
Architecture de réseaux et études de cas

Seconde édition



CampusPress France a apporté le plus grand soin à la réalisation de ce livre afin de vous fournir une information complète et fiable. Cependant, CampusPress France n'assume de responsabilités, ni pour son utilisation, ni pour les contrefaçons de brevets ou atteintes aux droits de tierces personnes qui pourraient résulter de cette utilisation.

Les exemples ou les programmes présents dans cet ouvrage sont fournis pour illustrer les descriptions théoriques. Ils ne sont en aucun cas destinés à une utilisation commerciale ou professionnelle.

CampusPress France ne pourra en aucun cas être tenu pour responsable des préjudices ou dommages de quelque nature que ce soit pouvant résulter de l'utilisation de ces exemples ou programmes.

Tous les noms de produits ou marques cités dans ce livre sont des marques déposées par leurs propriétaires respectifs.

Publié par CampusPress France
19, rue Michel Le Comte
75003 PARIS

Tél. : 01 44 54 51 10

Mise en pages : TyPAO
ISBN : 2-7440-0870-2
Copyright © 2000
CampusPress France

Tous droits réservés

Titre original : *CCIE Fundamentals : Network Design and Case Studies, Second Edition*

Traduit de l'américain par Christian Soubrier

ISBN original : 1-57870-167-8
Copyright © 2000 Cisco Systems, Inc.
Tous droits réservés

Macmillan Technical Publishing
201 West 103rd Street
Indianapolis, IN 46290 USA

Toute reproduction, même partielle, par quelque procédé que ce soit, est interdite sans autorisation préalable. Une copie par xérographie, photographie, film, support magnétique ou autre, constitue une contrefaçon passible des peines prévues par la loi, du 11 mars 1957 et du 3 juillet 1995, sur la protection des droits d'auteur.

Table des matières

Partie I. Architecture de réseaux

Chapitre 1. Introduction	3
Conception d'un réseau de campus	4
Tendances de conception	5
Conception d'un réseau étendu (WAN)	7
Tendances de conception d'un WAN	8
Conception pour les connexions distantes	9
Tendances de conception des connexions distantes	10
Tendances de l'intégration LAN/WAN	10
Solutions intégrées	11
Définition des exigences de réseau	12
Problèmes de conception : optimisation de la disponibilité et des coûts	12
Résumé	17
Chapitre 2. Notions essentielles sur la conception de réseaux	19
Concepts de base de la mise en œuvre de réseaux	20
Equipements de réseau	20
Introduction à la commutation	21
Identification et choix des fonctionnalités de réseau	23
Identification et choix d'un modèle de conception de réseau	23
Modèle de conception hiérarchique	24
Services du réseau fédérateur	25
Services de distribution	37
Services d'accès locaux	44
Choix des options de fiabilité de réseau	50

Identification et choix des équipements de réseau	57
Avantages des commutateurs (services de niveau 2)	58
Avantages des routeurs (services de niveau 3)	58
Types de commutateurs	60
Comparaison entre commutateurs et routeurs	62
Résumé	66
Chapitre 3. Conception de réseaux IP étendus avec protocoles de routage interne	67
Implémentation des protocoles de routage	67
Topologie de réseau	68
Adressage et synthèse de routage	68
Sélection d'itinéraire	70
Convergence	71
Evolutivité du réseau	72
Sécurité	74
Directives de conception d'un réseau EIGRP	75
Topologie de réseau EIGRP	75
Adressage EIGRP	75
Synthèse de routes EIGRP	76
Sélection de route EIGRP	76
Convergence EIGRP	77
Evolutivité d'un réseau EIGRP	81
Sécurité avec EIGRP	81
Directives de conception d'un réseau OSPF	81
Topologie de réseau OSPF	82
Adressage et synthèse de routes OSPF	84
Sélection de route OSPF	90
Convergence OSPF	91
Evolutivité d'un réseau OSPF	91
Sécurité avec OSPF	92
Fonctionnalités de la zone NSSA de OSPF	92
OSPF On-Demand Circuit	95
OSPF sur les réseaux non broadcast	98
Routage à la demande (ODR, On-Demand Routing)	101
Avantages de ODR	101
Remarques sur l'utilisation de ODR	102
Résumé	102

Chapitre 4. Conception de réseaux IP étendus avec BGP	103
Fonctionnement de BGP	103
BGP interne (IBGP)	105
BGP externe (EBGP)	107
BGP et cartes de routage	108
Annonces de réseaux	110
Attributs de BGP	113
Attribut de cheminement (AS_path)	113
Attribut d'origine (Origin)	114
Attribut de prochain saut (Next Hop)	114
Attribut de poids (Weight)	117
Attribut de préférence locale (Local Preference)	119
Attribut de préférence d'accès AS (Multi-Exit Discriminator)	121
Attribut de communauté (Community)	123
Critères de sélection de chemin BGP	124
Compréhension et définition des stratégies de routage BGP	125
Distances administratives	125
Filtrage BGP	125
Groupes d'homologues BGP	131
CIDR et agrégats d'adresses	133
Confédérations	134
Rélecteurs de route	136
Contrôle d'instabilité de route (Route Flap Dampening)	138
Résumé	138
Chapitre 5. Conception de réseaux ATM	139
Présentation d'ATM	139
Rôle d'ATM sur les réseaux	140
Couches fonctionnelles ATM	141
Adressage ATM	146
Médias ATM	147
Réseaux multiservices	148
Solutions intégrées	148
Types de commutateurs ATM	149
Commutateurs ATM de groupe de travail et de campus	150
Commutateurs et routeurs ATM d'entreprise	151
Commutateurs d'opérateur	152
Structure d'un réseau ATM	152
Fonctionnement d'un réseau ATM	153

Rôle de LANE	154
Composants LANE	155
Fonctionnement de LANE	156
Implémentation de LANE	161
Considérations sur la conception LANE	161
Redondance LANE	164
Résumé	170
Chapitre 6. Conception de réseaux à commutation de paquets et de réseaux Frame Relay	171
Conception de réseaux à commutation de paquets	171
Conception hiérarchique	172
Choix d'une topologie	173
Problèmes liés à la diffusion broadcast	176
Gestion des performances	177
Conception de réseaux Frame Relay	178
Conception hiérarchique	178
Topologies régionales	181
Problèmes liés à la diffusion broadcast	184
Gestion des performances	186
Configuration de l'adaptation de trafic Frame Relay	190
Conception de réseaux voix sur Frame Relay (VoFR)	190
Caractéristiques des communications humaines	191
Algorithmes de compression de la voix	192
Echo et annulation d'écho	193
Problèmes de délai et de variation de délai	194
Problèmes de perte de trames	195
Support pour fax et modem	195
Priorité de trafic sur le réseau Frame Relay	196
Contrôle de délai à l'aide de la fragmentation de trame	196
Suppression des silences à l'aide de l'interpolation de la parole numérique (DSI)	196
Optimisation de la bande passante à l'aide du multiplexage	197
Résumé	197
Chapitre 7. Conception de réseaux APPN	199
Evolution de SNA	200
Rôle d'APPN	200
Intégration d'APPN dans la conception d'un réseau	202
Noeud de réseau APPN au niveau de chaque site distant	204

APPN ou autres méthodes de transport SNA	205
Présentation d'APPN	206
Définition de noeuds	206
Etablissement de sessions APPN	207
Routage intermédiaire de session	208
Utilisation des DLUR/DLUS	209
Implémentation Cisco d'APPN	210
Problèmes d'évolutivité	210
Réduction des mises à jour de bases de données topologiques	211
Réduction des recherches LOCATE	217
Techniques de secours sur un réseau APPN	220
Ligne de secours	220
Redondance totale	221
Prise en charge SSCP	223
APPN dans un environnement multiprotocole	224
Gestion de bande passante et de file d'attente	225
Autres considérations relatives aux environnements multiprotocoles	228
Gestion de réseau	228
Exemples de configuration	230
Configuration d'un réseau APPN simple	230
Configuration d'un réseau APPN avec des stations terminales	233
Configuration d'APPN sur DLSw+	236
Migration d'une sous-zone vers APPN	239
APPN/CIP dans un environnement Sysplex	244
APPN avec FRAS BNN	252
Résumé	256
Chapitre 8. Interréseaux DLSw+	257
Introduction à DLSw+	257
Définition de DLSw+	257
Standard DLSw	258
Fonctionnalités DLSw+	261
Comment procéder	265
Débuter avec DLSw+	266
Configuration minimale requise	266
Token Ring	267
Ethernet	268
SDLC	268
QLLC	270

Fonctionnalités avancées de DLSw+	272
Etablissement de connexion par des homologues DLSw+	273
Equilibrage de charge et redondance	273
Contrôle de la sélection d'homologue	276
Homologues de secours	276
Homologues de secours versus homologues actifs multiples	278
Options d'encapsulation	278
Listes de ports	282
Groupes d'homologues, homologues interzones, homologues à la demande	283
Homologues dynamiques	284
Résumé	288
Chapitre 9. Conception et configuration avec CIP	289
Critères de conception	290
Concentration des fonctions sur un routeur CIP	291
Combinaison du CIP et de SNA	292
CIP en solo	292
Configurations de conception	293
Configurations avec PCA, ESCON et MPC	294
Chargement du microcode du CIP	298
Définition du support CSNA	300
Assignation de CSNA à une adresse de dispositif d'entrée/sortie	300
Définition du LAN virtuel interne	301
Définition du nœud principal VTAM XCA	302
Définition pour le support du serveur TN3270	303
Support de TN3270 Server avec DLUR/DLUS	306
Définition de la fonction CIP CMPC	307
Noeud principal VTAM TRL (Transport Resource List)	307
Définition du nœud principal SNA local	308
Définition des sous-canaux CMPC	308
Définition du groupe de transmission CMPC	309
Exemples de configuration CIP	309
Haute disponibilité en utilisant RSRB et deux routeurs CIP	309
Haute disponibilité et équilibrage de charge au moyen de DLSw+ et de deux routeurs CIP	310
Connectivité CMPC entre deux VTAM sur un seul routeur CIP	311
Commutation de sessions TN3270 avec DLUR/DLUS et la redondance d'hôte VTAM	312
VTAM vers nœud de réseau (NN) APPN avec HPR sur CMPC	313

Chapitre 10. Conception de réseaux DDR	315
Introduction au routage DDR	315
Pile de conception DDR	316
Nuage de numérotation	316
Trafic et topologie DDR	317
Topologies	317
Analyse du trafic	319
Interfaces de numérotation	320
Interfaces physiques supportées	320
Groupes de rotation de numérotation	322
Profils de numérotation	322
Méthodes d'encapsulation	323
Adressage de nuage de numérotation	323
Correspondances de numérotation	323
Stratégies de routage	326
Routage statique	326
Routage dynamique	327
Routage Snapshot	329
Secours communé pour liaisons louées	331
Filtrage d'appel	334
Filtrage par listes ACL	335
Paquets IPX	337
Filtrage AppleTalk	338
Paquets Banyan VINES, DECnet et OSI	340
Routage à la demande et PPP	340
Authentification	341
Authentification PPP	341
Protocole CHAP	341
Protocole PAP	342
Sécurité RNIS	343
Fonction de rappel DDR	343
Listes d'accès IPX	343
Résumé	343
Chapitre 11. Conception de réseaux RNIS	345
Applications de RNIS	346
Routage DDR	346
Liaison de secours par ligne commutée	347
Connectivité SOHO	347
Agrégation de modems	348

Elaboration de solutions RNIS	348
Connectivité RNIS	348
Encapsulation de datagrammes	349
Routage DDR	349
Problèmes de sécurité	349
Limitation des coûts	349
Problèmes de connectivité avec RNIS	350
Implémentation d'une interface d'accès de base BRI	350
Implémentation d'une interface d'accès primaire PRI	355
RNIS de bout en bout	358
Problèmes d'encapsulation de datagrammes	360
Sécurité RNIS	363
Evolutivité des réseaux RNIS	365
Nœuds distants virtuels	365
Profils virtuels	367
MultiLink PPP multichâssis (MMP)	367
Limitation des frais d'utilisation de RNIS	370
Analyse de trafic	370
Structure de tarification	371
Formation des utilisateurs	371
Exploitation de SNMP	371
Emploi de l'application CEA (Cisco Enterprise Accounting) pour RNIS	373
Comptabilité AAA	373
Dépannage de RNIS	373
Dépannage de la couche physique	374
Dépannage de la couche liaison de données	376
Dépannage de la couche réseau	378
Résumé	384
Chapitre 12. Conception de réseaux LAN commutés	385
Evolution des réseaux partagés vers des réseaux commutés	385
Technologies de conception de réseaux LAN commutés	387
Rôle de la commutation LAN sur les réseaux de campus	388
Solutions de réseaux commutés	389
Composants du modèle de réseau commuté	390
Plates-formes de commutation évolutives	390
Infrastructure logicielle commune	394
Outils et applications d'administration de réseau	396

Conception de réseaux LAN commutés	396
Modèle hub et routeur	397
Modèle de VLAN de campus	398
MPOA (Mutliprotocol over ATM)	400
Modèle multicouche	401
Augmentation de la bande passante	408
Organisation de la couche centrale	409
Positionnement des serveurs	410
Epine dorsale LANE ATM	411
Multicast IP	413
Problèmes d'évolutivité	415
Stratégies de migration	417
Sécurité dans le modèle multicouche	418
Pontage dans le modèle multicouche	418
Avantages du modèle multicouche	419
Résumé	420
Chapitre 13. Protocole PIM Sparse Mode	421
Modèle d'adhésion explicite	422
Arbres partagés PIM-SM	422
Adhésion à un arbre partagé	423
Elagage d'un arbre partagé	426
Arbres de plus court chemin PIM-SM	428
Adhésion à un arbre SPT	429
Elagage d'un arbre SPT	430
Messages Join/Prune PIM	433
Actualisation d'état PIM-SM (State-Refresh)	434
Enregistrement de source multicast	434
Messages Register PIM	435
Messages Register-Stop PIM	436
Exemple d'enregistrement de source	436
Basculement SPT	439
Exemple de basculement SPT	439
Elagage de source sur l'arbre partagé	441
Routeur DR PIM-SM	443
Rôle du routeur DR	443
Reprise de fonction du routeur DR	443
Découverte de RP	444
Evolutivité de PIM-SM	444
Résumé	445

Partie II. Etudes de cas

Chapitre 14. Gestion de réseau commuté	449
Présentation	450
Lectorat de ce chapitre	450
Termes et acronymes employés dans ce chapitre	450
Introduction à l'administration de réseau	452
Présentation technique des équipements Cisco	453
Introduction aux commutateurs	453
Introduction aux routeurs	457
Introduction aux commutateurs de niveau 3	457
Technologies communes aux commutateurs et aux routeurs	457
Protocole d'administration de réseau	459
Protocoles de base	459
Présentation du modèle d'événements	460
Directives d'administration de réseau	464
Conception efficace et armoires de câblage sécurisées	464
Identification des ports jugés "critiques"	465
Mise en place du suivi d'erreurs	466
Collecte de données de référence	467
Valeurs de seuils	469
Recommandations sur les commutateurs Cisco Catalyst	471
Recommandations de conception et de configuration	471
Etat des ressources de commutateur	482
Etat de châssis et d'environnement	486
Etat de modules de commutateur	489
Topologie STP	490
Informations de base de données de transmission de pont	492
Erreurs de port	493
Taux d'utilisation des ports, broadcast, multicast, et unicast	495
Utilisation client	496
Reporting de temps de réponse	497
Variables MIB pour les environnements commutés	497
Autres objets à surveiller	500
Recommandations sur les routeur Cisco	511
Gestion des erreurs	511
Gestion des performances	517

Scénarios de corrélation d'événements de réseau	524
Test d'accessibilité périodique	524
Base de données de topologie logique	525
Base de données de topologie physique	525
Elaboration de la base de référence	525
Personnalisation	525
Scénarios de situations à problèmes	525
Résumé	535
Chapitre 15. Architecture de commutation de paquets	537
Commutation par processus	538
Equilibrage de charge avec la commutation par processus	540
Inconvénients de la commutation par processus	541
Mise en cache avec la commutation rapide	543
Structure du cache rapide	545
Maintenance du cache rapide	548
Equilibrage de charge avec la commutation rapide	550
Commutation optimale	551
Transmission expresse Cisco (CEF)	553
Fonctionnement de la commutation CEF	553
Equilibrage de charge avec la commutation CEF	556
Révision de CEF	558
Résumé	559
Chapitre 16. Redistribution EIGRP et OSPF	561
Configuration de la redistribution mutuelle entre EIGRP et OSPF	561
Exemples de fichiers de configuration	563
Vérification de la redistribution de routes	565
Ajout d'une route dans une liste de redistribution	568
Résumé	569
Chapitre 17. Configuration de EIGRP sur des réseaux Novell et AppleTalk	571
Réseau Novell IPX	571
Configuration d'un réseau Novell IPX	572
Intégration de EIGRP sur un réseau Novell IPX	572
Réseau AppleTalk	582
Configuration d'un réseau AppleTalk	582
Intégration de EIGRP sur un réseau AppleTalk	583
Résumé	585

Chapitre 18. Conception, configuration et dépannage de MPOA	587
Introduction	587
MPOA avec AAL5 (RFC 1483)	588
Circuits virtuels permanents (PVC)	588
Circuits virtuels commutés (SVC)	594
Classical IP sur ATM (RFC 1577)	603
Considérations de conception	604
Topologie	604
Configuration	604
Dépannage	605
Introduction à LANE	609
Considérations de conception	610
Topologie	611
Configuration	611
Dépannage	614
Protocole MPOA (Multiprotocols Over ATM)	623
Considérations de conception	623
Topologie	624
Configuration MPOA	624
Dépannage	626
Résumé	631
Chapitre 19. Routage DDR	633
Configuration du site central pour les appels sortants	634
Configuration d'une interface pour chaque site distant	635
Configuration d'une seule interface pour plusieurs sites distants	638
Configuration de plusieurs interfaces pour plusieurs sites distants	640
Configuration du site central et des sites distants pour les appels entrants et sortants	643
Configuration d'une interface pour chaque site distant	643
Configuration d'une seule interface pour plusieurs sites distants	645
Configuration de plusieurs interfaces pour plusieurs sites distants	648
Configuration des sites distants pour les appels sortants	650
Configuration de plusieurs interfaces pour plusieurs sites distants	651
DDR : la solution de secours pour des liaisons louées	653
Routes statiques flottantes	654
Routes statiques flottantes sur interfaces partagées	656
Liaisons louées et secours commuté	657
Numérotation DTR	657
Numérotation V.25 bis	658

Scripts de dialogue (chat script)	660
Création et implémentation de scripts de dialogue	660
Scripts de dialogue et correspondances de numérotation	660
Résumé	661
Chapitre 20. Evolutivité du routage DDR	663
Conception du réseau	663
Modèles de trafic	664
Choix du média	664
Protocoles requis	664
Solution matérielle	665
Solution logicielle	666
Authentification	666
Adressage de la couche réseau	666
Stratégie de routage	668
Configuration des routeurs d'accès de site central	670
Configuration du nom d'utilisateur pour les sites distants	671
Configuration de la numérotation pour les sites distants	671
Configuration des interfaces de bouclage	672
Configuration des interfaces asynchrones	672
Configuration de l'interface de numérotation	673
Configuration du routage OSPF	674
Configuration du routage RIP	675
Configuration du routage statique	675
Problèmes de sécurité	676
Taille du fichier de configuration	676
Configuration des routeurs de site distant	676
Configuration de scripts de dialogue pour appeler le site central	677
Configuration des interfaces asynchrones	677
Commande site	677
Configuration du routage statique	678
Configuration complète	679
Configuration du routeur CENTRAL-1	679
Configuration de Router 2	681
Réseaux d'entreprise commutés	681
Réseaux de FAI commutés	683
Résumé	684

Chapitre 21. Emploi efficace de RNIS en milieu multiprotocole	685
Configuration de DDR sur RNIS	685
Interface pour RNIS natif	687
Configuration d'une interface RNIS	687
Configuration des numéros d'identification de lignes appelantes	691
Configuration du service de rappel (callback)	692
Configuration du routage Snapshot sur RNIS	694
Evolution du réseau de télétravail	696
Réseau Novell IPX avec routage Snapshot	698
Configuration d'AppleTalk sur RNIS	701
Configuration du routeur A	702
Configuration du routeur B	704
Configuration de IPX sur RNIS	705
Exemple de réseau pour la configuration de IPX sur RNIS	705
Configuration du routeur C2503	706
Explication de la configuration du routeur C2503	707
Configuration du routeur C4000	713
Résumé	714
Chapitre 22. Amélioration de la sécurité sur les réseaux IP	715
Services de sécurité Cisco	717
Evaluation de l'état de la sécurité	717
Contrôle et rétablissement après incident	719
La guerre de l'information a-t-elle lieu ?	720
Menaces de la guerre de l'information	720
Motivations des cyber-pirates	721
Vulnérabilité des réseaux	721
Vulnérabilité de l'authentification CHAP de Cisco	722
Attaques par déni de service avec boucle TCP (land.c)	722
Attaques par déni de service "smurf"	722
Attaques par déni de service vers port de diagnostic UDP	722
Cryptage des mots de passe Cisco IOS	722
Evaluation des besoins en sécurité	723
Stratégies de sécurité	723
Création d'une stratégie de sécurité	725
Documenter et analyser une stratégie de sécurité	726

Approche Cisco de la sécurité	726
Connaître son ennemi	726
Evaluer les coûts	726
Identifier les dangers potentiels	727
Contrôler les informations confidentielles	727
Considérer le facteur humain	727
Connaître les faiblesses du système de sécurité	728
Limiter l'étendue de l'accès	728
Comprendre son environnement	728
Limiter sa confiance	729
Penser à la sécurité physique	729
La sécurité est envahissante	729
Contrôle de l'accès aux routeurs Cisco	729
Accès par console	730
Accès Telnet	731
Accès SNMP	731
Techniques additionnelles de sécurisation d'un routeur	733
Listes de contrôle d'accès	736
Fonctionnement	736
Application de listes d'accès sur un routeur	738
Masque générique	739
Listes de contrôle d'accès standards	740
Listes de contrôle d'accès étendues	741
Listes de contrôle d'accès réflexives	743
Listes de contrôle d'accès dynamiques (sécurité Lock-and-Key)	749
Autres mesures de sécurité Cisco	756
Contrôle de l'accès aux serveurs de réseau hébergeant des fichiers de configuration ..	756
Messages de notification d'utilisations non autorisées	757
Sécurisation de services non standards	757
Sécurité avec niveaux de privilèges	757
Cryptage des données de réseau	758
Etude de cas 1 : authentification de protocole de routage	759
Authentification de routeur voisin OSPF	760
Avantages de l'authentification de voisin OSPF	760
Conditions de déploiement de l'authentification de voisin OSPF	761
Fonctionnement de l'authentification de voisin	761
Authentification en texte clair	761
Authentification MD5	762
Dépannage de OSPF et authentification	762

Etude de cas 2 : conception d'une architecture pare-feu	763
Contrôle du flux de trafic	764
Configuration du routeur pare-feu	765
Définition de listes d'accès de pare-feu	765
Application de listes d'accès sur des interfaces	768
Configuration du serveur de communication pare-feu	769
Définition de listes d'accès sur le serveur de communication	769
Listes d'accès en entrée et usurpation d'adresse (spoofing)	770
Assignation de numéros de ports	771
Suggestions de lectures	774
Livres et périodiques	774
RFC (Requests For Comments)	774
Sites Internet	775
Résumé	775
Chapitre 23. HSRP pour un routage IP avec tolérance aux pannes	777
Fonctionnement de HSRP	780
Configuration de HSRP	781
Configuration de groupes de secours Hot Standby	783
Suivi d'interface	785
Equilibrage de charge	787
Interaction de HSRP avec des protocoles routés	789
AppleTalk, Banyan VINES et Novell IPX	789
DECnet et XNS	789
Résumé	790

Partie III. Annexes

Annexe A. Segmentation d'un espace d'adresse IP	793
Annexe B. Implémentation de liaisons série IBM	807
Semi-duplex versus duplex	807
Liaisons asynchrones	807
SNA d'IBM	808
ETCD	808
Connexions multipoints	809
Annexe C. Configuration d'hôte SNA pour des réseaux SRB	811
Configuration FEP	811
Définitions de nœud principal commuté par VTAM	815
Exemple de configuration d'un contrôleur de cluster 3174	816

Annexe D. Configuration d'hôte SNA pour des réseaux SDLC	821
Configuration FEP pour liaisons SDLC	822
Tableau de configuration SDLC pour 3174	824
Annexe E. Diffusions broadcast sur des réseaux commutés	827
Multicast IP	827
Réseaux IP	828
Réseaux Novell	831
Réseaux AppleTalk	832
Réseaux multiprotocoles	834
Annexe F. Réduction du trafic SAP sur les réseaux Novell IPX	835
Listes d'accès de filtrage des mises à jour SAP	837
Site central	837
Sites distants	838
Mises à jour SAP incrémentielles	838
Site central	838
Sites distants	839
Résumé	840
Annexe G. Introduction au transport de la voix en paquets	841
Introduction	842
Codage de la voix	843
Standards de codage de la voix	844
Qualité de compression	846
Délai	846
Options et problèmes du transport de la voix par paquets	848
Réseaux synchrones à circuits commutés	849
Réseaux de trames/cellules	849
Réseaux de données en mode non connecté	850
Réseaux de paquets X.25	850
Réseaux de données privés	851
Signalisation : établissement de la connexion pour la voix	852
Signalisation externe	853
Signalisation interne	854
Applications de la voix par paquets	856
Résumé	857
Annexe H. Références et suggestions de lectures	859
Ouvrages et publications périodiques	859
Publications techniques et standards	862

Annexe I. Présentation de la technologie multicast IP	865
Avantages du multicast	865
Notions élémentaires sur le multicast	867
Adressage	867
Enregistrement dynamique	868
Livraison multicast	868
Routage multicast	868
Processus multicast	869
Exigences du multicast IP sur un réseau d'entreprise	870
Microsoft NetShow et réseau multicast Microsoft	872
Index	875

I

Architecture de réseaux

- | | |
|-----------|---|
| 1 | <i>Introduction</i> |
| 2 | <i>Notions essentielles sur la conception de réseaux</i> |
| 3 | <i>Conception de réseaux IP étendus avec protocoles de routage interne</i> |
| 4 | <i>Conception de réseaux IP étendus avec BGP</i> |
| 5 | <i>Conception de réseaux ATM</i> |
| 6 | <i>Conception de réseaux à commutation de paquets et de réseaux Frame Relay</i> |
| 7 | <i>Conception de réseaux APPN</i> |
| 8 | <i>Interréseaux DLSw+</i> |
| 9 | <i>Conception et configuration avec CIP</i> |
| 10 | <i>Conception de réseaux DDR</i> |
| 11 | <i>Conception de réseaux RNIS</i> |
| 12 | <i>Conception de réseaux LAN commutés</i> |
| 13 | <i>Protocole PIM Sparse Mode</i> |

1

Introduction

Par Atif Khan

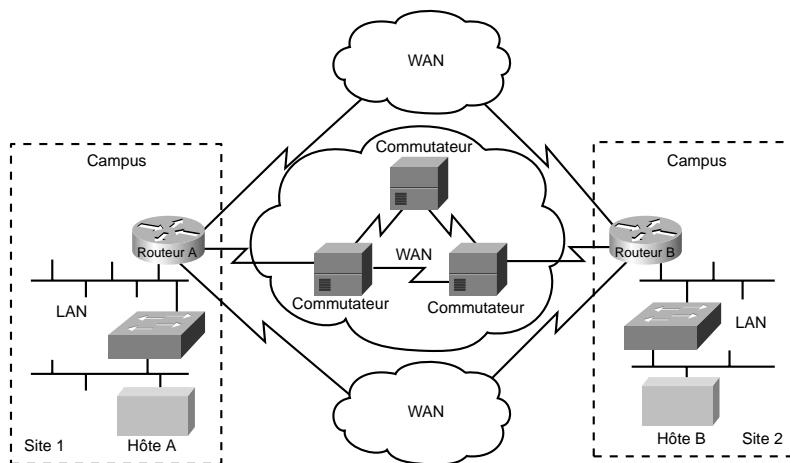
L’interconnexion de réseaux, qui permet à deux réseaux ou plus de communiquer, englobe tous les aspects de la connexion des ordinateurs entre eux. Les réseaux se sont développés pour pouvoir répondre à des exigences de communication entre systèmes terminaux très variés. Ils nécessitent la mise en œuvre de nombreux protocoles et fonctionnalités pour pouvoir rester évolutifs et être administrés sans qu’il soit nécessaire de recourir en permanence à des interventions manuelles. Les réseaux de grande taille peuvent se composer des trois éléments suivants :

- les réseaux de campus, qui comprennent les utilisateurs connectés localement, au sein d’un immeuble ou d’un groupe d’immeubles ;
- les réseaux étendus (*WAN, Wide Area Network*) qui relient des campus ;
- les technologies de connexion à distance, qui relient les bureaux de succursales et les utilisateurs isolés (itinérants et télétravailleurs) à un campus local ou à l’Internet.

La Figure 1.1 fournit un exemple type de réseau d’entreprise.

La conception d’un réseau peut se révéler une tâche ardue. Pour que le réseau soit fiable et capable d’évoluer, les concepteurs doivent garder à l’esprit que chacun des principaux composants précités possède ses exigences propres en matière de conception. Un réseau qui ne comprendrait que 50 nœuds de routage selon une structure maillée pourrait déjà poser de sérieux problèmes avec des résultats imprévisibles. Tenter d’optimiser un réseau qui comprendrait une centaine de nœuds serait encore plus difficile.

Figure 1.1
Un exemple de réseau d'entreprise type.



Malgré les améliorations constantes des performances des équipements et des capacités des médias de transmission, il est clair que la conception d'un réseau fait intervenir des environnements de plus en plus complexes, impliquant de nombreux types de supports de transmission, de protocoles et d'interconnexions à des réseaux qui, de plus, ne sont pas contrôlés par une seule organisation. Une approche prudente peut néanmoins aider le concepteur à éliminer une partie des difficultés liées à l'extension d'un réseau au fur et à mesure de son évolution.

Ce chapitre présente les technologies aujourd'hui disponibles pour la conception de réseaux. Voici les sujets généraux qui seront traités :

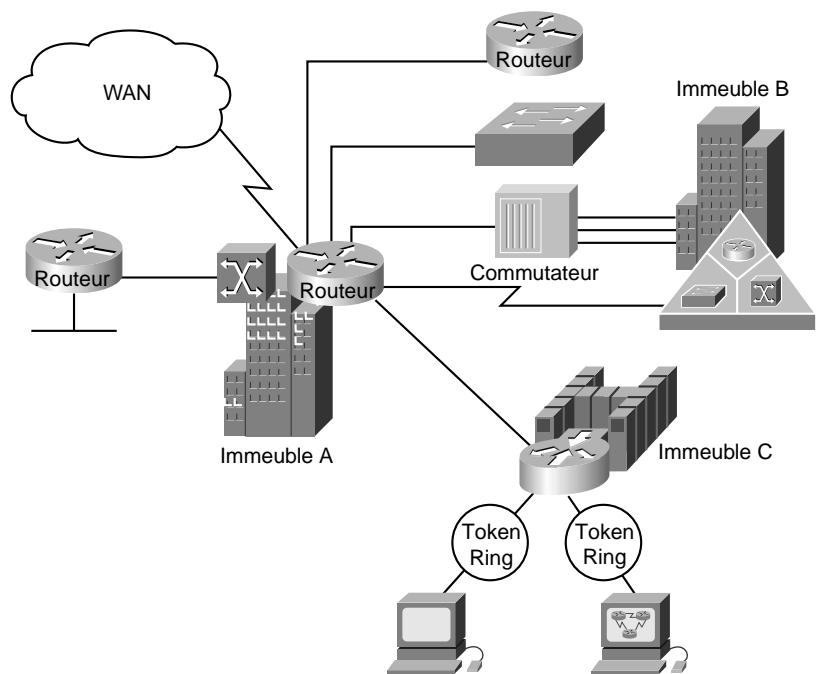
- la conception d'un réseau de campus ;
- la conception d'un réseau étendu (WAN) ;
- l'utilisation de connexions distantes ;
- la fourniture de solutions intégrées ;
- l'identification des exigences en matière de conception de réseaux.

Conception d'un réseau de campus

Un *réseau de campus* raccorde un immeuble ou un groupe d'immeubles à un réseau d'entreprise qui comprend plusieurs réseaux locaux (LAN, *Local Area Network*). Il concerne généralement une portion d'une entreprise (mais pourrait tout aussi bien en couvrir la totalité) limitée à une zone géographique fixe (voir Figure 1.2).

La caractéristique propre à un environnement de campus est que l'entreprise propriétaire du réseau possède en général également le câblage. Sa topologie suit principalement une technologie de réseau local qui interconnecte tous les systèmes terminaux au sein d'un immeuble, comme Ethernet, Token Ring, FDDI (*Fiber Distributed Data Interface*), Fast Ethernet, Gigabit Ethernet ou ATM (*Asynchronous Transfer Mode*).

Figure 1.2
Exemple de réseau de campus.



Un grand campus peut aussi exploiter une technologie de réseau étendu (WAN) pour raccorder des immeubles entre eux. Bien qu'il utilise le câblage et les protocoles propres à cette technologie, il échappe aux contraintes de coût élevé de la bande passante. Après l'installation du câblage, la bande passante se révèle peu coûteuse, car l'entreprise en est propriétaire et n'a donc pas à supporter les frais récurrents d'un fournisseur de services. Faire évoluer le câblage reste toutefois une opération onéreuse.

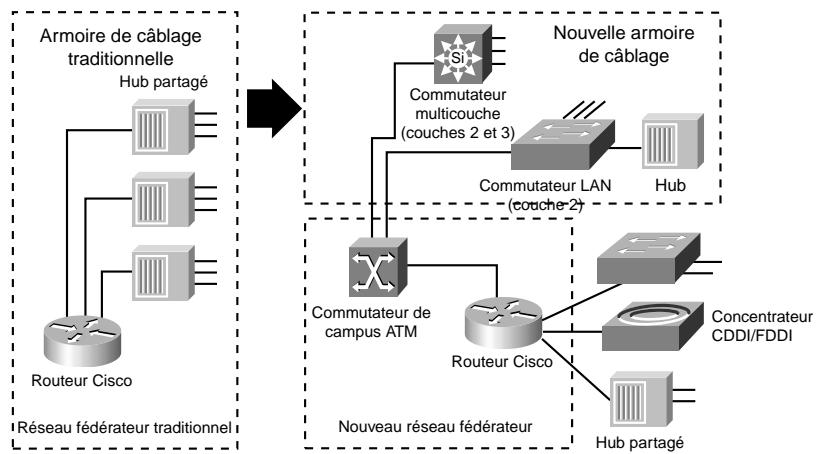
En conséquence, les concepteurs de réseaux adoptent généralement une conception optimisée en fonction de l'architecture la plus rapide pouvant fonctionner avec le câblage existant. Ils peuvent toutefois être confrontés à la nécessité de faire évoluer le câblage pour satisfaire aux exigences d'applications émergeantes. Par exemple, les technologies à haut débit, telles que Fast Ethernet, Gigabit Ethernet et ATM, en tant que réseau fédérateur, ainsi que la commutation au niveau de la couche 2, peuvent fournir une bande passante dédiée pour des applications de bureautique.

Tendances de conception

Par le passé, les concepteurs ne disposaient que d'un nombre limité d'options matérielles, à savoir routeurs ou hubs, lorsqu'ils devaient faire l'acquisition d'une technologie pour leurs réseaux de campus. Une erreur dans la conception matérielle était donc chose rare. Les hubs (concentrateurs) étaient prévus pour les armoires de câblage et les routeurs pour le centre de traitement des données ou les opérations principales de télécommunication.

Plus récemment, la technologie du réseau local a été révolutionnée par l'explosion de l'emploi de la commutation LAN au niveau de la couche 2 (liaison de données) afin d'augmenter les performances et fournir davantage de bande passante pour répondre à l'émergence de nouvelles applications de gestion de données en réseau. Grâce à ces avantages, les commutateurs LAN offrent à des groupes de travail et à des serveurs locaux un débit plus élevé. Ils se trouvent aujourd'hui placés en bordure du réseau dans les armoires de câblage et sont généralement prévus pour remplacer les hubs partagés et fournir à l'utilisateur des connexions à plus large bande passante (voir Figure 1.3).

Figure 1.3
Tendances de conception d'un réseau de campus.



Les fonctionnalités de réseau de la couche 3 sont nécessaires pour interconnecter les groupes de travail commutés et fournir des services qui incluent sécurité, qualité de service (*QoS, Quality of Service*) et gestion du trafic. Le routage intègre ces réseaux commutés et assure la sécurité, la stabilité ainsi que le contrôle nécessaires à l'élaboration de réseaux fonctionnels et évolutifs.

Traditionnellement, la commutation de couche 2 est assurée par des commutateurs LAN, et la commutation de couche 3 par des routeurs. On constate aujourd'hui que ces deux fonctions de réseau sont de plus en plus implémentées sur des plates-formes communes. Par exemple, des commutateurs multicouches assurant cette fonctionnalité aux deux niveaux apparaissent maintenant sur le marché.

Avec l'avènement de ces nouvelles fonctionnalités, telles que la commutation de couche 3, la commutation LAN, et les réseaux locaux virtuels ou VLAN (*Virtual Local Area Network*), la construction de réseaux de campus est devenue plus complexe que par le passé. Le Tableau 1.1 récapitule les diverses technologies LAN nécessaires à l'élaboration d'un réseau de campus. La société Cisco Systems propose des produits pour toutes ces technologies.

Les concepteurs créent maintenant des réseaux de campus en faisant l'acquisition de types d'équipements différents (par exemple, routeurs, commutateurs Ethernet et commutateurs ATM) et en les raccordant. Bien que des décisions d'achat isolées puissent sembler sans conséquences, les concepteurs ne doivent pas perdre de vue que tous ces équipements fonctionnent de concert pour former un réseau.

Tableau 1.1 : Récapitulatif des technologies LAN

Technologie LAN	Exploitation habituelle
Technologies de routage	Le routage est une technologie essentielle pour connecter des LAN dans un réseau de campus. Il peut consister en une commutation de couche 3 ou en un routage plus traditionnel incluant la commutation de couche 3 et des fonctionnalités de routeur supplémentaires.
Gigabit Ethernet	Cette solution est implémentée au-dessus du protocole Ethernet, mais offre un débit dix fois supérieur à celui du Fast Ethernet atteignant 1 000 Mbit/s ou 1 Gbit/s. Elle fournit une grande capacité de bande passante pour concevoir des réseaux fédérateurs tout en assurant une compatibilité avec les médias installés.
Technologies de commutation LAN — Commutation Ethernet	La commutation Ethernet assure la commutation de niveau 2 et offre des segments Ethernet dédiés pour chaque connexion. Elle représente la structure de base du réseau.
Technologies de commutation LAN — Commutation Token Ring	La commutation Token Ring propose les mêmes fonctionnalités que la commutation Ethernet, mais utilise une technologie propre à l'architecture d'anneau à jeton. Vous pouvez utiliser un commutateur Token Ring comme pont transparent ou pont à routage par la source.
Commutation ATM	Elle assure la commutation à haut débit pour transporter la voix, la vidéo et les données. Son fonctionnement est semblable à la commutation LAN pour les opérations sur les données, mais elle fournit toutefois une bande passante de plus grande capacité.

Il est possible de séparer ces technologies et d'installer des réseaux bien pensés exploitant chacune d'elles, mais les concepteurs doivent garder à l'esprit leur intégration générale. Si cette intégration de l'ensemble n'est pas prise en compte, les risques de pannes, d'immobilisation et de congestion du réseau seront plus nombreux qu'auparavant.

Conception d'un réseau étendu (WAN)

La communication WAN a lieu entre des zones géographiquement distantes. Sur un réseau d'entreprise, un réseau étendu relie des campus. Lorsqu'une station souhaite communiquer avec une autre station distante (située sur un site différent), les informations doivent transiter par une ou plusieurs liaisons WAN. Les routeurs situés sur les réseaux d'entreprise représentent les points de jonction LAN/WAN. Ils déterminent le chemin le plus approprié pour le transport des données.

La connexion de liaisons WAN est assurée par des commutateurs qui relaient les informations sur le réseau étendu et contrôlent le service que celui-ci fournit. La communication sur un réseau étendu est souvent appelée un *service*, car le fournisseur de réseau facture généralement aux utilisateurs les services qui sont assurés par les trois technologies de commutation principales suivantes :

- la commutation de circuits ;
- la commutation de paquets ;
- la commutation de cellules.

Chaque technique de commutation a ses avantages et ses inconvénients. Par exemple, la commutation de circuits offre à l'utilisateur une bande passante dédiée sur laquelle les connexions des autres utilisateurs ne peuvent empiéter. La commutation de paquets est connue pour offrir une plus grande souplesse et exploiter la bande passante avec plus d'efficacité. Quant à la commutation de cellules, elle combine certains aspects des deux types de commutation précédents pour autoriser l'installation de réseaux offrant une faible latence et un débit élevé. Elle a rapidement gagné en popularité, et ATM est actuellement la technologie de commutation de cellules la plus prisée. Voyez le Chapitre 2 pour plus d'informations sur les technologies de commutation des réseaux étendus et locaux.

Tendances de conception d'un WAN

Les réseaux étendus sont connus pour leur faible débit, leurs longs délais de transmission et leur taux d'erreur élevé. Ils se caractérisent également par un coût de location du média de transmission (le câblage) auprès d'un fournisseur de services. Puisque l'infrastructure d'un tel réseau est souvent louée, sa conception doit permettre d'optimiser le coût et l'efficacité de la bande passante utilisée. Par exemple, toutes les technologies et fonctionnalités mises en œuvre pour raccorder des campus par l'intermédiaire d'un réseau étendu sont développées pour répondre aux exigences de conception suivantes :

- optimisation de la bande passante WAN ;
- réduction maximale du coût des services ;
- optimisation du service effectif pour les utilisateurs finaux.

Depuis peu, les réseaux de médias partagés souffrent d'une surtaxe en raison des nouvelles exigences suivantes :

- nécessité de se connecter à des sites distants ;
- besoin croissant des utilisateurs de se connecter à distance à leur réseau d'entreprise ;
- croissance rapide des intranets d'entreprise ;
- utilisation accrue des serveurs d'entreprise.

Les concepteurs de réseaux se tournent vers la technologie WAN pour répondre à ces nouveaux besoins. Les connexions WAN transportent généralement des informations critiques et sont optimisées pour offrir un bon rapport performances/prix de la bande passante. Les routeurs qui relient des campus, par exemple, mettent en œuvre l'optimisation du trafic, la redondance d'itinéraires, l'ouverture de lignes commutées de secours en cas de sinistre, et améliorent la qualité de service pour les applications critiques.

Le Tableau 1.2 résume les diverses technologies WAN qui satisfont aux exigences des réseaux de grande envergure.

Tableau 1.2 : Récapitulatif des technologies WAN

Technologie WAN	Exploitation
ADSL (<i>Asymmetric Digital Subscriber Line</i>)	Variante du service DSL, ADSL permet d'utiliser les lignes téléphoniques existantes pour former des chemins d'accès plus rapides destinés au multimédia et aux communications de données à haute vitesse. L'utilisateur doit disposer d'un modem ADSL. Les vitesses supportées sont variables selon la distance ; elles peuvent être supérieures à 6 Mbit/s en réception et atteindre 640 Kbit/s en émission.
Modem analogique	Cet équipement peut être utilisé par les télétravailleurs et les utilisateurs itinérants qui accèdent au réseau moins de deux heures par jour, ou en tant que matériel de secours pour un autre type de liaison.
Lignes spécialisées louées	Elles peuvent être utilisées pour les réseaux PPP (<i>Point-to-Point Protocol</i>) et les topologies Hub-and-Spoke, ou comme ligne de secours pour un autre type de liaison.
RNIS	Cette technologie peut être utilisée pour fournir des accès distants rentables à des réseaux d'entreprise. Elle peut servir au transport de la voix et de la vidéo, et être utilisée comme moyen de communication de secours pour un autre type de liaison.
Frame Relay (relais de trames)	Le Frame Relay permet d'implémenter une topologie rentable à faible latence et à fort débit entre des sites distants. Il peut être utilisé à la fois pour des réseaux privés ou des réseaux d'opérateurs.
SMDS (<i>Switched Multimegabit Data Service</i>)	Ce service offre des connexions hautement performantes avec un débit élevé sur des réseaux de données publics. Il peut également être implémenté sur un réseau métropolitain (<i>MAN, Metropolitan Area Network</i>).
X.25	X.25 peut être utilisé pour fournir un circuit ou un réseau fédérateur WAN fiable. Il assure également le support des applications existantes.
ATM WAN	Cette technologie peut être utilisée pour devancer les exigences en bande passante. Elle assure également la gestion de plusieurs classes de qualité de service, afin de pouvoir distinguer les besoins des applications en cas de retards et de pertes.

Conception pour les connexions distantes

Les connexions distantes relient des utilisateurs isolés (itinérants ou télétravailleurs) et des succursales à un campus ou à l'Internet. Un site distant est généralement de petite taille, possède peu d'utilisateurs, et ne requiert par conséquent qu'une liaison WAN de faible étendue. Toutefois, les exigences d'un réseau en matière de communication distante impliquent habituellement un grand nombre d'utilisateurs isolés ou de sites distants, ce qui induit une augmentation de la charge WAN globale. Le nombre d'utilisateurs isolés ou de sites distants est tel que le coût total de la bande passante WAN est proportionnellement plus élevé sur les connexions distantes que sur les connexions LAN. Etant donné que le coût d'un réseau sur trois ans comprend les frais hors équipement, les frais de location du média WAN auprès d'un fournisseur de services représentent le

premier poste de dépenses d'un réseau distant. A la différence des connexions WAN, les petits sites ou les utilisateurs distants ont rarement besoin d'être connectés 24 h/24.

En conséquence, les concepteurs de réseaux choisissent habituellement entre la numérotation (*dial-up*) et les liaisons WAN dédiées comme solution de connexion à distance. Les connexions distantes fournissent généralement un débit de 128 Kbit/s ou inférieur. Un concepteur de réseau peut aussi employer des ponts sur un site distant pour leur facilité d'installation, leur topologie simple et leurs exigences de faible trafic.

Tendances de conception des connexions distantes

Il existe aujourd'hui un large éventail de médias pour les réseaux WAN distants, parmi lesquels :

- modem analogique ;
- ADSL (*Asymmetric Digital Subscriber Line*) ;
- ligne louée ;
- Frame Relay (relais de trames) ;
- X.25 ;
- RNIS.

Les connexions distantes permettent aussi un usage optimal de l'option WAN appropriée pour fournir une bande passante rentable, minimiser les coûts des services de numérotation et optimiser le service pour les utilisateurs finaux.

Tendances de l'intégration LAN/WAN

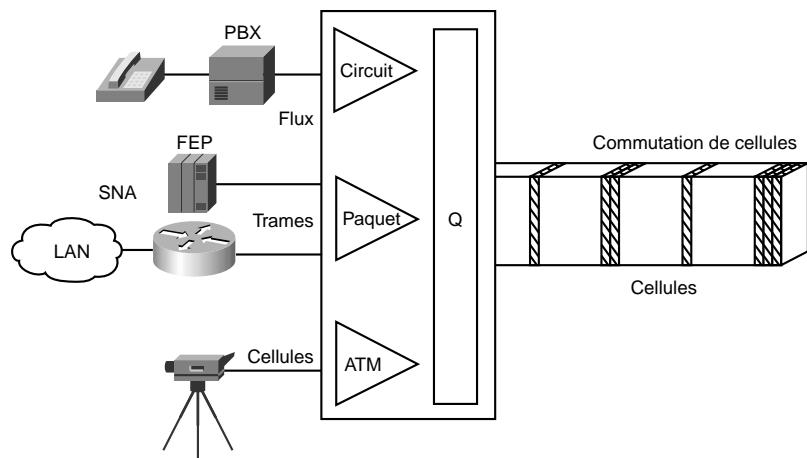
Aujourd'hui, 90 % de la puissance informatique se situe au niveau de l'ordinateur de bureau, et elle croît de façon exponentielle. Les applications distribuées sont de plus en plus gourmandes en bande passante et, avec l'avènement de l'Internet, bon nombre d'architectures LAN atteignent leurs limites. Les communications audio ont augmenté de façon significative et reposent de plus en plus sur des systèmes de messagerie vocale centralisés. Le réseau est crucial pour la circulation des informations. Les efforts convergent vers une tentative de réduction de ses coûts tout en permettant le support de nouvelles applications et d'un plus grand nombre d'utilisateurs avec des performances améliorées.

Jusqu'à présent, les communications de réseaux locaux et étendus sont restées logiquement séparées. Sur un réseau local, la bande passante est gratuite, la connectivité n'est limitée que par les coûts d'implémentation et de matériel, et seules des données sont transportées. Sur un réseau étendu, la bande passante représente le principal coût, et le trafic dont le temps de transmission est crucial, telle la voix, est séparé des données. Les nouvelles applications et les considérations financières liées à leur acceptation entraînent néanmoins des changements dans ces tendances.

L'Internet est la première source d'échange multimédia avec l'ordinateur personnel. Il a radicalement modifié la donne en matière d'échanges. Les applications concernées, transportant la voix ou la vidéo en temps réel, requièrent des performances accrues et plus prévisibles, que ce soit sur réseau local ou sur réseau étendu. Ces applications multimédias commencent à compter parmi les ingrédients essentiels à une bonne productivité d'entreprise. A mesure que les sociétés entrevoient d'implémenter sur IP de nouvelles applications multimédias consommatrices en bande passante et

basées sur des intranets — telles la formation par la vidéo, la vidéoconférence et la téléphonie —, l'impact de ces applications sur l'infrastructure de réseau existante constitue un vrai problème. Par exemple, si une société s'appuie sur son réseau d'entreprise pour l'acheminement du trafic SNA de première importance et souhaite installer une application de formation en ligne par la vidéo, le réseau doit être en mesure de fournir une garantie de qualité de service pour acheminer le trafic multimédia sans l'autoriser à interférer avec le flux des informations capitales de l'entreprise. ATM a été présenté comme l'une des technologies d'intégration de réseaux locaux et de réseaux étendus. La qualité des fonctionnalités de service d'ATM autorise le support de n'importe quel type de trafic en flux séparés ou mixtes, qu'ils soient sensibles au retard de livraison ou non (voir Figure 1.4).

Figure 1.4
Support ATM de divers types de trafics.



ATM peut également s'adapter pour fournir aussi bien des faibles débits que des débits élevés. Il a été adopté par tous les fabricants d'équipements de l'industrie, des réseaux locaux au commutateur privé (PBX, *Private Branch eXchange*).

Solutions intégrées

Concernant la mise en œuvre de réseaux, la tendance actuelle est d'apporter aux concepteurs une plus grande souplesse dans la résolution de problèmes, sans qu'ils aient besoin de créer de multiples réseaux ou de faire une croix sur les investissements existants en matière de communication de données. Les routeurs peuvent permettre l'installation de réseaux fiables et sûrs, et servir de barrières contre les tempêtes de broadcast sur les réseaux locaux. Des commutateurs, que l'on peut diviser en deux catégories principales, LAN et WAN, peuvent être déployés aux niveaux groupe de travail, épine dorsale de campus ou WAN. Les sites distants peuvent employer des routeurs d'entrée de gamme pour se connecter au WAN.

Le support et l'intégration de tous les produits Cisco sont gérés par le système IOS (*Internet-working Operating System*, système d'interconnexion de réseaux) de Cisco. Il permet d'intégrer des groupes disparates, des équipements divers et de nombreux protocoles, afin de former un réseau très

évolutif et d'une grande fiabilité. Il garantit également au réseau un niveau élevé de sécurité, de qualité de service, et de services de trafic.

Définition des exigences de réseau

La conception d'un réseau peut être un véritable défi. La première étape consiste à bien en comprendre les exigences ; la suite de ce chapitre décrit comment procéder pour les identifier. Lorsque vous aurez défini ces exigences, reportez-vous au Chapitre 2, afin d'obtenir des informations sur le choix des fonctionnalités et des options de fiabilité qui permettent d'y répondre.

Les équipements de réseau choisis doivent refléter les objectifs, les caractéristiques et les règles des organisations dans lesquelles ils opèrent. La conception d'un réseau et son implémentation doivent prendre en compte deux paramètres principaux :

- **Disponibilité des applications.** Les réseaux transportent les informations d'applications entre les ordinateurs. Si les applications ne sont pas disponibles pour les utilisateurs du réseau, celui-ci ne remplit pas sa fonction.
- **Coût de possession d'un réseau.** Les budgets accordés aux systèmes d'informations se chiffrent aujourd'hui en millions de francs. Etant donné que l'exploitation de grandes organisations repose de plus en plus sur des données électroniques, les coûts associés aux ressources informatiques continueront à augmenter.

Un réseau bien conçu peut faciliter un équilibrage de ces deux paramètres. S'il est correctement implanté, son infrastructure peut optimiser la disponibilité des applications et permettre ainsi une exploitation rentable des ressources de réseau existantes.

Problèmes de conception : optimisation de la disponibilité et des coûts

En général, les problèmes liés à la conception de réseaux impliquent les trois types d'éléments généraux suivants :

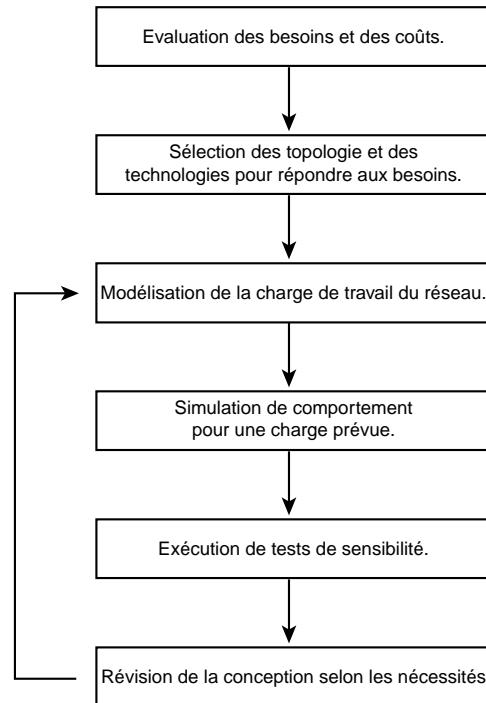
- **Eléments de l'environnement.** Ils comprennent l'emplacement des hôtes, des serveurs, des terminaux et autres nœuds d'extrémité ; les prévisions de trafic pour l'environnement ; les prévisions de coûts, afin de garantir différents niveaux de service.
- **Contraintes de performances.** Elles incluent la fiabilité du réseau, le débit des données transportées et les vitesses assurées par les ordinateurs hôtes/clients (par exemple, la vitesse des cartes réseau ou la vitesse d'accès aux disques durs).
- **Eléments variables de réseau.** Ils concernent la topologie du réseau, les capacités des lignes et les allocations de flux de paquets.

L'objectif est de réduire au maximum les coûts, en se basant sur ces éléments lors de la fourniture d'un service qui ne compromet pas les exigences de disponibilité définies. En tant que concepteur, vous êtes confronté à deux problèmes principaux : disponibilité et coût, bien qu'ils semblent incompatibles. En effet, toute augmentation de la disponibilité s'accompagne généralement d'une augmentation du coût. En conséquence, vous devez estimer avec prudence l'importance relative de la disponibilité d'une ressource et le coût global.

Comme l'illustre la Figure 1.5, la conception d'un réseau est une répétition de tâches. Les sections suivantes mettent en valeur plusieurs aspects qui sont à considérer avec prudence lors des prévisions d'implémentation.

Figure 1.5

Processus général de conception d'un réseau.



Evaluation des besoins de l'utilisateur

En général, les utilisateurs veulent pouvoir disposer à tout moment des applications du réseau. Les facteurs déterminants de cette disponibilité sont le *temps de réponse*, le *débit* et la *fiabilité* :

- Le temps de réponse est l'intervalle de temps compris entre l'entrée d'une commande ou l'activation d'une touche et l'exécution de ladite commande ou la réception d'une réponse émanant du système hôte. La satisfaction de l'utilisateur peut généralement être considérée comme une fonction *monotone*, croissante ou décroissante, mais il est primordial que ce paramètre ne s'approche pas du seuil minimal. Les services interactifs en ligne, tels les distributeurs automatiques de billets de banque, sont un exemple d'applications dont le temps de réponse est considéré comme capital.
- Les applications qui injectent un fort volume de trafic sur le réseau ont davantage d'effet sur le débit que celles qui connectent deux nœuds d'extrémité. Elles impliquent généralement des transferts de fichiers et de faibles exigences en termes de temps de réponse. En effet, leur exécution peut être programmée à des moments où le niveau de trafic sensible aux temps de réponse est faible, par exemple, après les heures de travail habituelles.

- Bien que la fiabilité soit toujours un facteur important, certaines applications sont particulièrement exigeantes en cette matière. Les organisations qui conduisent leur activité en ligne ou au moyen du téléphone requièrent une disponibilité du réseau avoisinant les 100 %. Les services financiers, d'échange de titres ou d'urgences en sont quelques exemples. Pour répondre à de tels besoins de disponibilité, un haut niveau de performance matérielle ou topologique est nécessaire. Déterminer le coût de l'immobilisation du réseau est une étape essentielle dans l'évaluation de l'importance de la fiabilité sur votre réseau.

Vous pouvez évaluer les besoins des utilisateurs de plusieurs façons, sachant que plus ils seront impliqués dans ce processus, plus votre évaluation sera proche de la réalité. Les méthodes suivantes devraient vous y aider :

- **Définition de profils de communautés d'utilisateurs.** Il s'agit de déterminer les besoins propres à différents groupes d'utilisateurs. C'est la première étape dans la définition des exigences du réseau. Bien que de nombreux utilisateurs aient des besoins similaires en matière de courrier électronique, ces exigences ne seront pas les mêmes pour des groupes d'ingénieurs qui exploitent des terminaux XWindow et des stations de travail Sun dans un environnement NFS que pour des groupes d'utilisateurs de PC qui se partagent des serveurs d'impression au sein d'un service financier.
- **Mise en place d'interviews, de groupes de discussion et d'études.** L'objectif est de créer une base de référence pour l'implémentation d'un réseau. En effet, certains groupes peuvent avoir besoin d'un accès à des serveurs communs, d'autres souhaiter autoriser un accès depuis l'extérieur à certaines ressources informatiques internes, et certaines organisations nécessiter que les systèmes d'information soient administrés d'une façon particulière, selon certains standards extérieurs. La méthode la moins formelle pour recueillir des informations est d'interroger des groupes d'utilisateurs clés. Des groupes de discussion peuvent également servir à collecter des informations et susciter des débats entre différentes organisations ayant des intérêts semblables ou différents. Enfin, des études formelles peuvent permettre de recueillir l'opinion des utilisateurs, considérée comme statistiquement valable, concernant un certain niveau de service ou une architecture de réseau proposée.
- **Tests de comportement.** La méthode la plus coûteuse en temps et en argent, mais peut-être aussi la plus révélatrice, consiste à conduire un test en laboratoire portant sur un groupe représentatif d'utilisateurs. Cette méthode est généralement la plus performante pour l'évaluation des exigences en temps de réponse. Par exemple, vous pourriez installer des systèmes formant un environnement de travail et demander aux utilisateurs de réaliser les tâches habituelles d'interrogation de l'hôte à partir du laboratoire. En évaluant les réactions des utilisateurs par rapport aux variations de temps de réponse du serveur, vous pourriez établir des seuils de référence représentatifs des performances acceptables.

Evaluation de solutions propriétaires et ouvertes

La compatibilité, la conformité et l'interopérabilité sont liées au problème de l'équilibrage des fonctionnalités propriétaires et de la souplesse des réseaux ouverts. En tant que concepteur de réseau, vous pouvez être forcé de choisir entre l'implémentation d'un environnement multifabricant et une fonctionnalité propriétaire bien spécifique. Par exemple, le protocole IGRP (*Interior Gateway Routing Protocol*) offre de nombreuses fonctionnalités dont certaines sont prévues pour

améliorer sa stabilité, telles les fonctions de retenue de modifications (*holddown*), d'horizon éclaté (*split horizon*) ou encore de mise à jour corrective (*poison reverse updates*).

L'inconvénient est que IGRP est un protocole de routage propriétaire, alors que IS-IS (*Intermediate System-to Intermediate System*) est une solution d'interconnexion ouverte qui fournit également un environnement de routage avec convergence rapide. Toutefois, l'implémentation d'un protocole de routage ouvert peut conduire à une complexité croissante de configuration de matériels provenant de plusieurs fabricants.

Vos décisions peuvent avoir des effets divers sur l'ensemble de la conception de votre réseau. Supposez que vous décidiez d'intégrer IS-IS plutôt que IGRP. Vous gagnez en interopérabilité, mais perdez certaines fonctionnalités. Par exemple, vous ne pouvez pas équilibrer la charge de trafic sur des chemins parallèles inégaux. De la même manière, certains modems fournissent d'importantes capacités de diagnostic propriétaires, mais nécessitent pour un réseau donné d'être tous du même fabricant pour que ces fonctionnalités propriétaires puissent être pleinement exploitées.

Les prévisions et les investissements passés ont une influence considérable sur les choix d'implementations pour le projet en cours. Vous devez prendre en considération les équipements de réseau déjà installés, les applications exploitées (ou à exploiter) sur le réseau, les modèles de trafic, l'emplacement physique des sites, des hôtes et des utilisateurs, le taux de croissance de la communauté des utilisateurs, et le tracé physique et logique du réseau.

Evaluation des coûts

Le réseau est une composante stratégique de la conception globale de votre système d'information. A ce titre, son coût total représente bien plus que le seul total des bons de commande d'équipements. Vous devez prendre en compte le cycle de vie intégral de votre environnement de réseau. Voici une liste des coûts associés à sa mise en œuvre :

- **Coûts des équipements matériels et logiciels.** Intégrez les coûts réels lors de l'acquisition de vos systèmes initiaux : ils doivent inclure les achats et les installations de départ, la maintenance et les mises à jour programmées.
- **Coûts de performances.** Estimez le coût requis pour passer d'un temps de réponse de 5 secondes à une demi-seconde. De telles améliorations peuvent nécessiter des dépenses en médias de transmission, cartes réseau, nœuds d'interconnexion, modems et services WAN.
- **Coûts d'installation.** L'implantation du câblage sur un site est parfois l'opération la plus coûteuse pour un grand réseau. Les coûts comprennent la main d'œuvre, la modification du site et les frais supplémentaires de mise en conformité eu égard à la législation locale et aux restrictions environnementales (par exemple, la suppression de l'amiant). Mais d'autres facteurs importants peuvent concourir à maintenir un niveau minimal de dépenses, par exemple une bonne planification du tracé de l'armoire de câblage et des conventions de couleurs pour les segments de câble.
- **Coûts d'expansion.** Calculez les frais à engager pour le retrait de la totalité d'un câblage Ethernet épais, l'ajout de fonctionnalités supplémentaires ou un changement d'emplacement. Une prévision des besoins futurs permettra aussi d'économiser du temps et de l'argent.
- **Coûts d'assistance.** Les réseaux complexes engendrent davantage de frais d'analyse, de configuration et de maintenance. Par conséquent, il est conseillé de limiter la complexité au strict

nécessaire. Incluez les coûts de formation, de personnel qualifié (responsables et administrateurs de réseau) et de remplacement de matériel. Prenez également en compte la gestion des services hors bande, les stations d'administration SNMP et la consommation d'énergie.

- **Coûts d'improductivité.** En évaluant le coût de chaque échec d'accès à un serveur de fichiers ou à une base centralisée, vous obtiendrez le coût d'improductivité. Lorsque ce dernier atteint un niveau élevé, il faut envisager de recourir à un réseau totalement redondant.
- **Coûts de renonciation.** Chaque choix implique une solution de rechange. Qu'il s'agisse de plate-forme matérielle, de topologie, de niveau de redondance ou d'intégration de système, il existe toujours plusieurs options. Les coûts de renonciation représentent la perte financière liée à un choix non adopté. Par exemple, négliger les technologies récentes peut entraîner la perte d'une position concurrentielle sur le marché, une baisse de la productivité et une diminution des performances. Essayez d'intégrer ces coûts dans vos calculs afin de réaliser des comparaisons précises en début de projet.
- **Coûts irrécupérables.** Ils concernent vos investissements en équipements : câblage, routeurs, concentrateurs, commutateurs, hôtes, ainsi que divers équipements matériels ou logiciels. Si les coûts sont élevés, vous devrez peut-être modifier votre réseau afin qu'il puisse continuer à être exploité. Bien que de faibles coûts différentiels d'exploitation semblent comparativement plus intéressants que des frais de reconception, ne pas faire évoluer le matériel peut, à long terme, se révéler plus coûteux pour l'organisation. Une stratégie qui accorderait trop d'importance à ces coûts peut entraîner, au bout du compte, des ventes insuffisantes, voire des pertes de parts de marché.

Estimation du trafic : modélisation de la charge de travail

La *modélisation de la charge de travail* consiste, d'un point de vue empirique, à organiser un environnement de travail en réseau et à analyser le trafic généré par un certain nombre d'utilisateurs et d'applications, avec une topologie de réseau donnée. Essayez de caractériser l'activité d'une journée de travail ordinaire en termes de type et de niveau de trafic, de temps de réponse, de temps d'exécution de transferts de fichiers, etc. Vous pouvez également analyser l'exploitation des équipements de réseau existants pendant la période de test.

Si les caractéristiques du réseau testé sont semblables à celles du futur réseau, vous pouvez tenter une extrapolation du nombre d'utilisateurs, des applications utilisées et de la topologie de ce dernier. Il s'agit de l'approche par déduction la plus réaliste possible pour évaluer le trafic, en l'absence d'outils plus précis qui permettraient d'en caractériser le comportement de façon plus détaillée.

Outre la surveillance passive d'un réseau existant, vous pouvez mesurer l'activité et le trafic générés par un nombre connu d'utilisateurs rattachés à un réseau de test représentatif, afin de tenter d'estimer par anticipation la communauté des utilisateurs futurs.

Un problème lié à la modélisation de la charge de travail sur un réseau est la difficulté de définir avec exactitude la charge imposée à un équipement donné, ainsi que ses performances, en fonction du nombre d'utilisateurs, des types d'applications et de l'emplacement géographique. Cela est particulièrement vrai s'il n'y a pas de réseau réel installé.

Prenez en compte les facteurs suivants, qui influencent la dynamique du réseau :

- **La nature temporelle des accès au réseau.** Les périodes de trafic intense peuvent varier ; les mesures doivent refléter un ensemble d'observations incluant les moments d'affluence.
- **Les différences associées au type de trafic.** Selon qu'un trafic est routé ou ponté, les exigences en matière d'équipements et de protocoles de réseau seront différentes. Certains protocoles réagissent aux paquets perdus, certains types d'applications nécessitent davantage de bande passante, etc.
- **La nature aléatoire du trafic de réseau.** Le moment exact d'arrivée des données et les effets spécifiques au trafic sont imprévisibles.

Test de sensibilité du réseau

D'un point de vue pratique, le test de sensibilité implique la rupture de liens stables et l'observation des répercussions. Procéder au test sur un réseau de test est relativement facile. Provoquez un dysfonctionnement en retirant une carte active, puis analysez de quelle façon le réseau gère la situation. Observez la manière dont le trafic est rerouté, la vitesse de convergence, la perte éventuelle de connectivité, et les problèmes éventuels de gestion de types spécifiques de trafic. Vous pouvez également modifier le niveau de trafic sur un réseau afin d'observer les réactions lorsque le média de transmission est proche de la saturation. Ce test simule une sorte de *régession* : une série de modifications spécifiques (test) sont répétées sur différentes versions de configuration du réseau. En analysant les effets des différentes variations de la conception, vous pouvez en évaluer la résistance.

NOTE

La modélisation des tests de sensibilité au moyen d'un ordinateur sort du cadre de cet ouvrage. L'ouvrage de A.S. Tannenbaum (paru en langue anglaise), *Computer Networks* (Upper Saddle River, New Jersey : Prentice Hall, 1996) constitue une bonne source d'informations sur la conception et la simulation de réseaux d'ordinateurs.

Résumé

Après avoir déterminé les besoins de votre réseau, vous devez identifier puis sélectionner les fonctionnalités spécifiques qui correspondent à votre environnement informatique. Le Chapitre 2 fournit davantage d'informations de base sur les différents types d'équipements de réseaux, ainsi qu'une description de l'approche hiérarchique pour la mise en œuvre de réseaux.

Les Chapitre 2 à 13 de ce livre donnent des renseignements détaillés sur les technologies impliquées dans l'implémentation de réseaux de grande taille dans les environnements suivants :

- Réseaux IP (*Internet Protocol*) étendus :
 - conception avec le protocole EIGRP (ou IGRP étendu) (*Enhanced Interior Gateway Routing Protocol*) ;
 - conception avec le protocole OSPF (*Open Shortest Path First*).
- Réseaux SNA (*System Network Architecture*) d'IBM :
 - conception avec pont à routage par le source, ou SRB (*Source-Routing Bridge*) ;

- conception avec SDLC (*Synchronous Data Link Control*) et STUN (*Serial Tunneling*), SDLLC (*SDLC Logical Link Control type 2*) et QLLC (*Qualified Logical Link Control*) ;
 - conception avec APPN (*Advanced Peer-to-Peer Networking*) et DLSw (*Data Link Switching*).
- Réseaux ATM.
 - Réseaux avec services de paquets :
 - conception avec Frame Relay.
 - Réseaux avec routage par ouverture de ligne à la demande, ou DDR (*Dial-on Demand Routing*).
 - Réseaux RNIS.

Outre ces chapitres, d'autres concernent la conception de réseaux LAN commutés, de réseaux locaux de campus, et de réseaux destinés aux applications multimédias. Les dix derniers chapitres du livre incluent des études de cas qui concernent les concepts décrits dans les chapitres précédents.

2

Notions essentielles sur la conception de réseaux

Par Atif Khan

Mettre en place un réseau peut-être un vrai défi. Un réseau formé d'un maillage de 50 nœuds de routage seulement peut déjà générer des problèmes complexes, aux conséquences imprévisibles. Lorsque l'on tente d'optimiser plusieurs réseaux, composés de milliers de nœuds, les difficultés sont encore plus grandes.

En dépit de l'amélioration des performances des équipements et des caractéristiques fonctionnelles des médias de transmission, la conception d'un réseau tend à se complexifier. La tendance est à des environnements de plus en plus hétérogènes, qui associent de nombreux médias et protocoles, et impliquent pour n'importe quelle organisation une interconnexion à des réseaux extérieurs. L'observation de certaines règles de prudence dans l'élaboration d'un réseau permet de limiter les problèmes qui pourraient apparaître dans le futur, à mesure que le réseau se développera.

Ce chapitre présente les grandes lignes de la planification et de la conception d'un réseau. Trois sujets d'ordre général y sont traités :

- compréhension des concepts de base de la mise en œuvre de réseaux ;
- identification et choix des fonctionnalités nécessaires à cette mise en œuvre ;
- identification et sélection des équipements de réseau.

Concepts de base de la mise en œuvre de réseaux

Cette section expose les concepts de base qui interviennent dans la conception de réseaux :

- les équipements de réseau ;
- la commutation.

Equipements de réseau

Les concepteurs de réseaux disposent de quatre types d'équipements de base :

- les hubs (concentrateurs) ;
- les ponts ;
- les commutateurs ;
- les routeurs.

Le Tableau 2.1 en récapitule les caractéristiques.

Tableau 2.1 : Récapitulatif des caractéristiques des équipements de réseau

<i>Equipement</i>	<i>Description</i>
Hubs (concentrateurs)	Les hubs servent à relier plusieurs utilisateurs à un seul équipement physique, lui-même connecté au réseau. Ils agissent comme des répéteurs, régénérant le signal qui transite par eux.
Ponts	Les ponts servent à séparer logiquement des segments d'un même réseau. Ils opèrent au niveau de la couche Liaison de données du modèle OSI (couche 2) et sont indépendants des protocoles de couche supérieure.
Commutateurs	Les commutateurs sont semblables aux ponts, mais ils possèdent généralement un plus grand nombre de ports. Chaque port dessert un seul segment de réseau, séparant de ce fait les domaines de collision (<i>collision domain</i>). Aujourd'hui, dans les armoires de câblage, les concepteurs de réseaux remplacent les hubs par des commutateurs afin d'augmenter les performances ainsi que la bande passante du réseau, tout en préservant les investissements existants en matière de câblage.
Routeurs	Les routeurs séparent les domaines de broadcast (diffusion générale) et sont utilisés pour connecter des réseaux différents. Ils aiguillent le trafic en utilisant l'adresse du réseau de destination (couche 3) et non l'adresse MAC de la station de travail (couche 2). Les routeurs sont dépendants des protocoles.

Les experts en transmission de données s'accordent pour dire que les concepteurs de réseaux préfèrent aujourd'hui l'utilisation de routeurs et de commutateurs à celle de ponts et de concentrateurs pour créer des réseaux. Par conséquent, ce chapitre est plus spécialement consacré au rôle des routeurs et des commutateurs dans la conception de réseaux.

Introduction à la commutation

Dans les transmissions de données, tous les équipements de commutation et de routage exécutent les deux opérations de base suivantes :

- **Commutation de trames de données.** Il s'agit généralement d'une opération en mode différé (*store-and-forward*) dans laquelle une trame atteint un canal d'entrée, pour être ensuite transmise vers un canal de sortie.
- **Maintenance des opérations de commutation.** Les commutateurs construisent et maintiennent des tables de commutation et recherchent les boucles. Les routeurs maintiennent à la fois des tables de routage et des tables de services.

Il existe deux méthodes de commutation de trames de données : au niveau de la couche 2 et au niveau de la couche 3.

Commutations de niveau 2 et de niveau 3

Le processus de commutation consiste à recevoir une trame entrante au niveau d'une interface, puis à la retransmettre en sortie par une autre interface. Les routeurs s'appuient sur la commutation de niveau 3 pour aiguiller un paquet alors que les commutateurs emploient la commutation de niveau 2 pour transmettre les trames.

La différence entre ces deux méthodes de commutation réside dans le type d'informations situées à l'intérieur de la trame, utilisées pour déterminer l'interface de sortie appropriée. La commutation de niveau 2 se fonde sur les informations d'adresse MAC pour acheminer les trames, alors que celle de niveau 3 utilise les informations de la couche réseau.

La commutation de niveau 2 ne recherche donc pas dans un paquet les informations de la couche réseau, comme c'est le cas de la commutation de niveau 3. A la place, elle examine l'adresse MAC de destination de la trame pour l'envoyer vers l'interface correspondante, si elle connaît son emplacement. Pour cela, elle élabore et maintient une table de commutation qui permet de savoir à quel port ou à quelle interface appartiennent les adresses MAC.

Si le commutateur de niveau 2 ne sait pas dans quelle direction envoyer la trame, il l'envoie sur le réseau en diffusion broadcast sur tous ses ports afin de connaître la destination correcte. Lorsqu'il reçoit la réponse, il prend connaissance de l'emplacement de la nouvelle adresse, puis ajoute les informations nécessaires dans sa table de commutation.

Les adresses de la couche 2 sont définies par le fabricant de l'équipement de communication utilisé. Il s'agit d'adresses uniques, composées de deux éléments : le code du fabricant, ou code MFG (*Manufacturing*), et un identifiant unique. Le code MFG est attribué à chaque fabricant par l'IEEE (*Institute of Electrical and Electronics Engineers*), alors que l'identifiant unique est assigné par le fabricant à chaque carte qu'il produit. A l'exception des réseaux SNA (*Systems Network Architecture*), les utilisateurs ne disposent d'aucun contrôle sur les adresses de niveau 2, car elles sont figées pour un matériel de réseau donné, tandis que les adresses de la couche 3 peuvent être modifiées. De plus, les adresses de la couche 2 impliquent l'emploi d'un espace d'adressage linéaire, avec des adresses uniques, au plan mondial.

La commutation de niveau 3 a lieu au niveau de la couche Réseau. Elle examine les informations contenues dans les paquets afin de les acheminer en fonction de leur adresse de réseau de destination. Elle supporte également les fonctionnalités de routeurs.

Les adresses de la couche 3 sont définies, pour la plupart, par l'administrateur de réseau qui établit une hiérarchie sur le réseau. Des protocoles tels que IP, IPX et AppleTalk utilisent les informations d'adressage de cette couche. L'administrateur réseau peut ainsi former des entités locales représentant des unités d'adressage uniques (semblables aux rues, villes, états et pays), et leur assigner une adresse. Si des utilisateurs changent d'immeuble, leurs stations de travail reçoivent une nouvelle adresse de niveau 3, mais conservent leur adresse de niveau 2.

Les routeurs opèrent au niveau de la couche 3 du modèle OSI, ils participent donc à l'établissement de cette structure d'adressage hiérarchique à laquelle ils peuvent en même temps se conformer. Par conséquent, un réseau routé associe une structure d'adressage logique à une infrastructure physique, par exemple par le biais de sous-réseaux TCP/IP ou de réseaux IPX pour chaque segment. L'écoulement du trafic sur un réseau commuté (linéaire) diffère fondamentalement de celui d'un réseau routé (hiérarchique). Ce dernier offre une plus grande souplesse d'écoulement, grâce à l'exploitation de cette hiérarchie, qui lui permet de déterminer les meilleurs chemins à emprunter et de former des domaines de broadcast.

Implications des commutations de niveau 2 et de niveau 3

La puissance toujours croissante des ordinateurs et des applications client/serveur et multimédias nécessite davantage de bande passante dans les environnements traditionnels où le média est partagé. Cela a amené les concepteurs de réseaux à remplacer, dans les armoires de câblage, les hubs par des commutateurs.

Bien que les commutateurs de niveau 2 utilisent la microsegmentation pour faire face à cet accroissement de la demande en bande passante et en performances, les concepteurs sont maintenant confrontés aux problèmes que pose la nécessité grandissante d'une communication entre sous-réseaux interconnectés. Par exemple, chaque fois qu'un utilisateur accède à des serveurs, ou à d'autres ressources, situés sur des sous-réseaux différents, le trafic doit transiter par un équipement qui opère au niveau de la couche 3. La Figure 2.1 illustre le cheminement du trafic à travers deux sous-réseaux, au moyen de commutateurs (niveau 2) et d'un routeur (niveau 3).

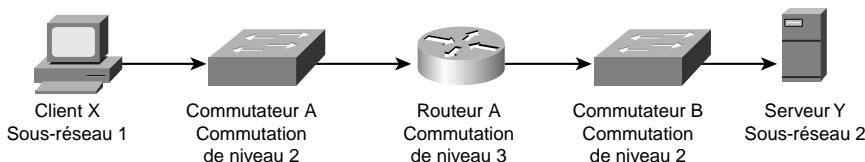


Figure 2.1

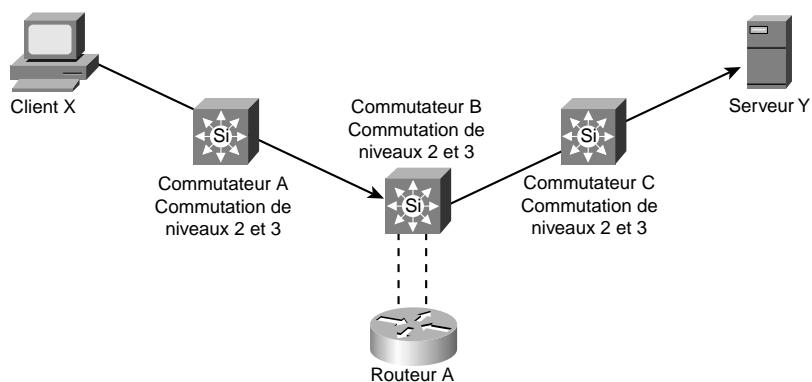
Circulation du trafic entre deux sous-réseaux, avec des commutateurs de niveau 2 et un routeur de niveau 3.

A la Figure 2.1, Client X doit emprunter le chemin suivant pour communiquer avec Serveur Y qui se trouve sur un sous-réseau différent : il doit passer par Commutateur A (commutation de niveau 2),

puis par Routeur A (commutation de niveau 3) et enfin par Commutateur B (commutation de niveau 2). Cette situation présente un risque de goulet d'étranglement très important et donc de réduction des performances, car le trafic doit passer d'un sous-réseau à un autre.

Pour éviter cela, les concepteurs peuvent ajouter des fonctionnalités de commutation de niveau 3 à travers le réseau. Elles sont implémentées sur les équipements en bordure de réseau afin de réduire la charge des routeurs centralisés. La Figure 2.2 illustre le déploiement de cette commutation, qui permet à Client X de communiquer directement avec Serveur Y, sans passer par Routeur A.

Figure 2.2
Déploiement de la commutation de niveau 3 à travers tout le réseau.



Identification et choix des fonctionnalités de réseau

Une fois les exigences de réseau définies, vous devez identifier, puis choisir, les fonctionnalités spécifiques qui correspondent à votre environnement. Les sujets traités dans les sections suivantes vous apportent les éléments de départ utiles à la prise de décision :

- identification et choix d'un modèle de conception de réseau ;
- choix des options de fiabilité de réseau.

Identification et choix d'un modèle de conception de réseau

Les modèles de conception hiérarchiques autorisent une organisation des réseaux en couches. Pour mieux saisir l'importance de ce concept, prenons l'exemple du modèle de référence OSI (*Open System Interconnection*, interconnexion de systèmes ouverts), qui sert à comprendre et à implémenter la communication entre ordinateurs. L'utilisation de couches lui permet de simplifier les tâches requises entre deux ordinateurs pour communiquer. Les modèles hiérarchiques font également appel à ce concept afin de faciliter la mise en œuvre de réseaux. Chaque couche peut être dédiée à des fonctions spécifiques, autorisant de ce fait le concepteur à choisir les systèmes et les fonctionnalités appropriés pour chacune d'elles.

Une conception hiérarchique facilite également les modifications dans un réseau. Le principe de modularité permet de créer des éléments qui peuvent être reproduits au fur et à mesure que le réseau se développe. Lorsqu'un élément doit être mis à jour, le coût et la complexité associés ne portent

alors que sur une petite portion du réseau. Au sein d'architectures linéaires ou maillées importantes, les modifications ont tendance à affecter un grand nombre de systèmes. Avec une structuration modulaire en petits éléments de réseau, plus faciles à maîtriser, les incidents sont également plus faciles à localiser et à isoler. Les administrateurs sont à même d'identifier les points de transition du réseau, ce qui les aide à identifier les pannes.

Modèle de conception hiérarchique

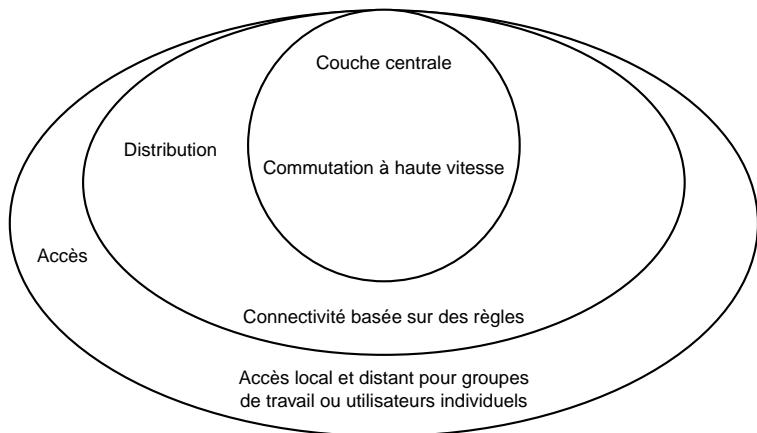
Une conception hiérarchique implique la présence des trois couches suivantes :

- l'épine dorsale, appelée aussi réseau fédérateur, qui représente la couche centrale assurant le transport optimal des données entre les sites ;
- la couche de distribution, qui fournit une connectivité basée sur des règles ;
- la couche d'accès local, qui offre aux groupes de travail et aux utilisateurs individuels un accès au réseau.

La Figure 2.3 est une représentation d'ensemble qui montre les diverses facettes d'un réseau hiérarchique. Chaque couche (centrale, distribution et accès) offre des fonctionnalités différentes.

Figure 2.3

Modèle de conception de réseau hiérarchique.



Fonctions de la couche centrale

Cette couche est un réseau fédérateur de commutation à haute vitesse qui devrait être conçu pour commuter les paquets le plus rapidement possible. Elle n'est censée opérer aucune manipulation des paquets, telle que les listes d'accès ou le filtrage, afin de ne pas ralentir leur commutation.

Fonctions de la couche de distribution

Cette couche représente la frontière entre la couche d'accès et la couche centrale, et aide à déterminer les caractéristiques distinctives de cette dernière. Son objectif est d'offrir une définition des limites. La manipulation des paquets a lieu à ce niveau.

Dans un environnement de réseau de campus, cette couche peut assurer plusieurs fonctions :

- regroupement d'adresses ou de zones ;
- accès au réseau pour les départements ou groupes de travail ;
- définition de domaines de broadcast (diffusion générale) ou multicast (diffusion restreinte) ;
- routage sur des réseaux locaux virtuels ou VLAN (*Virtual Local Area Network*) ;
- toute transition de médias nécessaire ;
- sécurité.

Dans les autres environnements, cette couche peut faire office de point de redistribution entre des domaines de routage, ou bien de frontière entre des protocoles de routage statique ou dynamique. Les sites distants peuvent également s'en servir de point d'accès au réseau d'entreprise. Sa principale fonctionnalité est d'offrir une connectivité basée sur des règles.

Fonctions de la couche d'accès

Cette couche représente le point d'accès local au réseau pour les utilisateurs finaux. Elle utilise parfois des listes d'accès ou des filtres afin de mieux servir les besoins d'un ensemble d'utilisateurs donné. Dans un environnement de réseau de campus, elle offre les fonctions suivantes :

- bande passante partagée ;
- bande passante commutée ;
- filtrage au niveau de la couche MAC ;
- microsegmentation.

Dans les autres environnements, cette couche peut autoriser des sites distants à accéder au réseau d'entreprise par le biais de certaines technologies longue distance, comme le Frame Relay (relais de trames), RNIS ou des lignes louées.

Certains pensent parfois que ces trois couches (centrale, distribution et accès) existent en tant qu'entités physiques clairement définies, ce qui n'est pas le cas. Elles ont été définies pour aider à la conception de réseaux et représenter les fonctionnalités qui doivent être implémentées. L'instanciation de chaque couche peut se faire au niveau de routeurs ou de commutateurs distincts, être représentée par un média physique, combinée en un seul équipement, ou encore être complètement omise. La façon dont ces couches sont mises en œuvre dépend des besoins du réseau en cours de conception. Il faut noter toutefois que la structure hiérarchique doit être préservée pour que le fonctionnement du réseau soit optimal.

Services du réseau fédérateur

Cette section couvre les fonctionnalités de réseau qui gèrent les services du réseau fédérateur. Les sujets suivants y sont traités :

- optimisation du chemin ;
- priorité du trafic ;
- équilibrage de charge ;
- chemins alternatifs ;

- accès commuté ;
- encapsulation (mise en œuvre d'un tunnel).

Optimisation du chemin

L'un des principaux avantages des routeurs est qu'ils permettent d'implémenter un environnement logique dans lequel les chemins les plus efficaces sont automatiquement sélectionnés pour faire circuler le trafic. Ils s'appuient pour cela sur les protocoles de routage associés aux différentes couches du réseau.

Selon les protocoles installés, les routeurs permettent d'implémenter un environnement de routage adapté à des exigences spécifiques. Par exemple, sur un réseau IP, les routeurs Cisco sont aptes à gérer tous les protocoles largement utilisés, tels que OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*), IGRP (*Interior Gateway Routing Protocol*, version améliorée de RIP, créée par Cisco), EIGRP (*Enhanced IGRP*), IS-IS (*Intermediate System-to Intermediate System*), BGP (*Border Gateway Protocol*), et EGP (*Exterior Gateway Protocol*). Les fonctionnalités intégrées essentielles qui favorisent l'optimisation du chemin incluent la convergence rapide et gérable des routes, ainsi que les métriques et temporiseurs de routage configurables.

La *convergence* est le processus par lequel tous les routeurs s'accordent pour choisir les routes les plus fiables. Lorsqu'un événement interrompt ou, à l'inverse, ouvre la circulation sur certaines routes, les routeurs s'envoient des messages de mise à jour des itinéraires. Ils peuvent ainsi recalculer les routes optimales et décider de celles à emprunter. Les algorithmes de routage qui offrent une convergence lente peuvent provoquer des boucles de routage ou des pannes sur le réseau.

Les algorithmes de routage utilisent de nombreuses métriques différentes. Certains, plus sophistiqués, s'appuient sur une forme hybride de mesure calculée à partir d'une combinaison de différentes métriques. EIGRP, par exemple, utilise l'un des algorithmes à vecteur de distance (*distance vector routing*) les plus perfectionnés. Il combine des valeurs de bande passante, de charge et de temps d'acheminement, afin de créer une métrique composée. Les protocoles par informations d'état de lien (*link state routing*), tels OSPF et IS-IS, emploient une métrique qui représente le coût associé à un chemin donné.

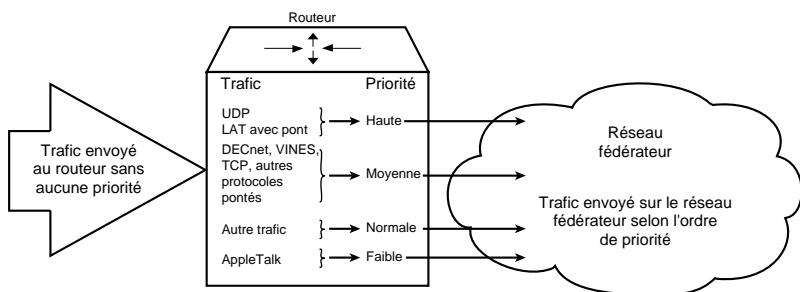
Priorité du trafic

Bien que certains protocoles de réseau gèrent la priorité du trafic homogène interne, celle de flux hétérogènes est à la charge des routeurs. Une telle gestion du trafic permet un routage basé sur des règles et garantit que les données de première importance seront prioritaires sur celles de moindre importance.

Mise en file d'attente de priorité

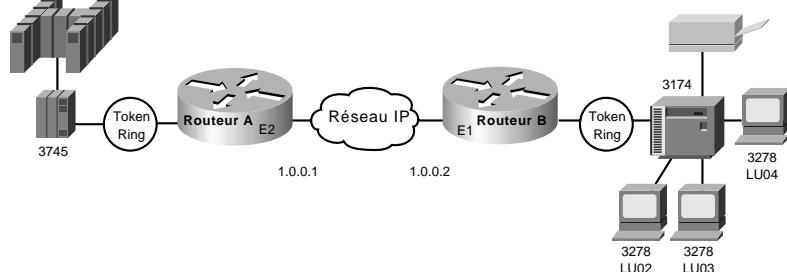
La mise en file d'attente de priorité permet à l'administrateur réseau d'attribuer au trafic des degrés de priorité. Celui-ci peut être classé selon différents critères, comme le type de protocole ou de sous-protocole, puis placé dans l'une des quatre files d'attente (priorités haute, moyenne, normale ou faible). Le trafic IP autorise une définition plus poussée du niveau de priorité. Cette fonctionnalité est la plus utile pour les liaisons série à faible vitesse. La Figure 2.4 illustre l'utilisation d'une file d'attente pour répartir le trafic par niveau de priorité, accélérant ainsi l'acheminement de certains paquets à travers le réseau.

Figure 2.4
File d'attente de priorité.



Il existe également certaines techniques intraprotocoles de gestion de priorité du trafic, utilisées pour obtenir de meilleures performances sur les réseaux. Par exemple, les fonctionnalités de type de service du protocole IP (ToS, *Type of Service*) et la priorité des unités logiques d'IBM ou LU (*Logical Unit*) peuvent être implémentées afin d'améliorer la gestion du trafic au niveau des routeurs. La Figure 2.5 illustre la gestion de priorité des unités logiques.

Figure 2.5
Mise en œuvre de la gestion de priorité des unités logiques.



Dans cette figure, l'ordinateur central IBM est relié par canal à un contrôleur de transmissions 3745, lui-même connecté à un contrôleur de cluster 3174 par le biais d'un système de ponts distants à routage par la source (RSRB, *Remote Source-Routing Bridge*). Plusieurs terminaux et imprimantes 3270, possédant chacun une adresse LU locale et unique, sont reliés au contrôleur de cluster. Avec la gestion de priorité des adresses LU, un niveau de priorité peut être accordé à chaque unité logique associée à un terminal ou à une imprimante, c'est-à-dire que certains terminaux peuvent bénéficier d'un temps de réponse plus rapide que d'autres, et les imprimantes peuvent recevoir une priorité inférieure. Dans certaines situations où les utilisateurs exploitent des applications extrêmement importantes, leur disponibilité peut être améliorée par cette fonctionnalité.

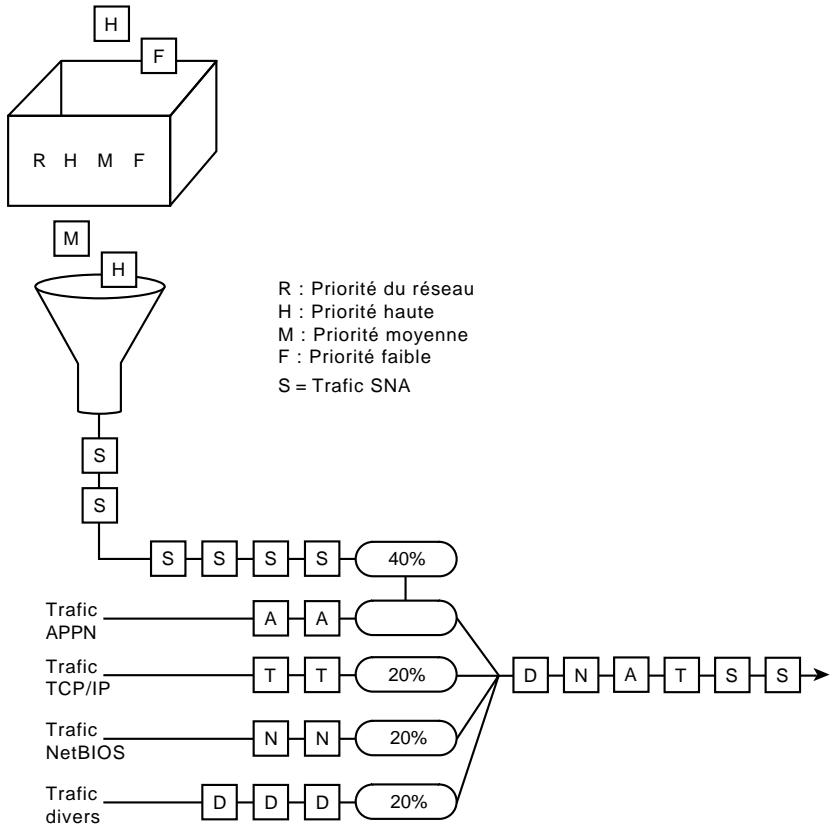
Pour finir, la plupart des protocoles routés (AppleTalk, IPX et DECnet) font appel à un protocole de routage qui se fonde sur le coût pour évaluer l'efficacité des différents chemins menant à une destination donnée. Grâce à la configuration de certains paramètres associés, il est possible de forcer un type spécifique de paquets à emprunter certaines routes, et réaliser ainsi une forme de gestion manuelle de la priorité.

Mise en file d'attente personnalisée

Le problème que pose la mise en file d'attente de priorité est que les paquets placés dans les files de faible priorité ne sont parfois pas délivrés en temps voulu, ou même pas délivrés du tout. La mise en file d'attente personnalisée est prévue pour résoudre ce problème, en offrant une plus grande granularité. En fait, cette fonctionnalité est couramment employée dans des environnements de réseau qui gèrent plusieurs protocoles de couche supérieure. Elle dédie une certaine quantité de bande passante à des protocoles spécifiques, permettant ainsi au trafic de première importance de pouvoir disposer du média de transmission à n'importe quel moment.

Le but est de réserver de la bande passante pour des types de trafic particuliers. Par exemple, à la Figure 2.6, SNA dispose de 40 % de la bande passante, TCP/IP de 20 %, NetBIOS de 20 %, et l'ensemble des protocoles restants de 20 %. Le protocole APPN (*Advanced Peer-to-Peer Networking*) met en œuvre le concept de classe de service (CoS, *Class of Service*) pour déterminer le degré de priorité de chaque message. Il définit la priorité du trafic avant de l'envoyer sur la file d'attente de transmission DLC.

Figure 2.6
File d'attente personnalisée.



La mise en file d'attente personnalisée permet de définir la priorité d'un trafic multiprotocole ; elle autorise un maximum de 16 files d'attente. Chaque file est servie de façon séquentielle, jusqu'à ce que le nombre d'octets envoyés dépasse le compte d'octets configurable, ou que la file soit vide. Un aspect important de cette fonctionnalité est la réallocation de la bande passante restante en cas de non-utilisation. Par exemple, si SNA n'exploite que 20 % de la quantité qui lui a été octroyée, les autres protocoles peuvent alors se partager les 20 % restants.

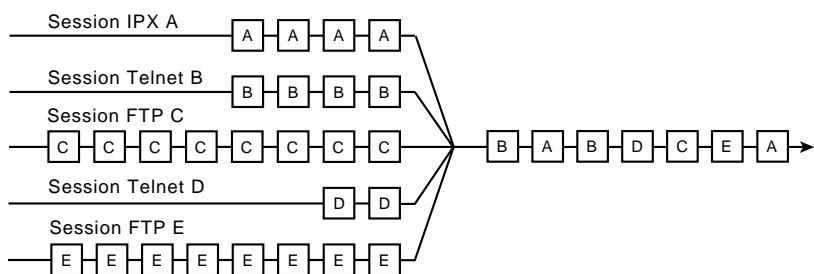
Cette fonctionnalité est prévue pour des environnements où un niveau de service minimal doit être assuré pour chaque protocole. Dans les environnements multiprotocoles actuels, elle permet à des protocoles possédant des caractéristiques différentes de partager le même média.

Mise en file d'attente équitable pondérée

La *mise en file d'attente équitable pondérée* est un algorithme de gestion de la priorité, qui utilise le multiplexage temporel (TDM, *Time-division Multiplexing*) pour répartir la bande passante entre des clients qui se partagent une même interface. Dans le multiplexage temporel, les clients reçoivent une tranche de temps, à tour de rôle. Avec la mise en file d'attente équitable pondérée, la bande passante est répartie équitablement entre les clients, afin que ceux qui possèdent la même charge de travail en reçoivent une quantité identique. Il est possible de spécifier différentes charges de travail, par exemple par l'intermédiaire du type de service, lorsque davantage de bande passante doit être attribuée.

Si chaque client reçoit la même quantité de bande passante, indépendamment du débit généré, le trafic de faible volume se voit avantageé par rapport à celui de fort volume. La possibilité de définir différentes charges de travail permet au trafic qui ne supporte pas de retard de bénéficier d'une plus grande bande passante, et garantit ainsi un temps de réponse approprié en cas de trafic dense. Différents types de flux de données peuvent converger sur un même câble (voir Figure 2.7).

Figure 2.7
File d'attente pondérée.



C et E sont deux sessions FTP à fort trafic. A, B et D sont des sessions interactives à faible trafic. Chaque session, dans ce cas, est appelée une *conversation*. Si chaque conversation est desservie de façon cyclique et reçoit une tranche de temps indépendamment de son débit d'arrivée, les sessions FTP ne monopolisent pas la bande passante. Par conséquent, le délai d'attente qui précède la transmission du trafic interactif devient prévisible.

La mise en file d'attente équitable pondérée fournit un algorithme qui identifie dynamiquement les flux de données au moyen d'une interface, puis les sépare en files logiques distinctes. Cet algorithme

utilise divers critères de distinction, en fonction des informations de protocole de la couche réseau qui sont disponibles, puis fait le tri parmi eux. Par exemple, dans le cas de trafic IP, les critères sont les adresses source et de destination, le type de protocole, les numéros de sockets et le type de service. C'est pourquoi les deux sessions Telnet (B et D) de la Figure 2.7 se trouvent aiguillées vers deux files logiques différentes.

Idéalement, l'algorithme devrait pouvoir faire la distinction entre toutes les conversations qui se partagent le média, afin que chacune reçoive sa juste part de bande passante. Malheureusement, avec des protocoles tel SNA, il est impossible de distinguer une session SNA d'une autre. Avec DLSw+ (*Data Link Switching Plus*), par exemple, le trafic SNA est multiplexé en une session TCP unique. De la même manière, dans le cas d'APPN, les sessions SNA sont multiplexées en une seule session LLC2 (*Logical Link Control, Type 2*).

Cet algorithme considère toutes ces sessions comme une seule et même conversation. Lorsqu'il y a de nombreuses sessions TCP/IP, elles obtiennent la majorité de la bande passante, et le trafic SNA le minimum. Pour cette raison, cet algorithme n'est pas recommandé pour l'utilisation de SNA avec une encapsulation TCP/IP au moyen de DLSw+, ou avec APPN.

La gestion de priorité avec file d'attente équitable pondérée présente néanmoins de nombreux avantages par rapport aux gestions par file d'attente de priorité ou personnalisée. Ces dernières requièrent la définition de listes d'accès ; la bande passante doit être allouée à l'avance, et les priorités prédéfinies. Cette caractéristique entraîne une charge supplémentaire. Il est parfois impossible aux administrateurs de réseau d'identifier et d'assigner un niveau de priorité au trafic en temps réel. La mise en file d'attente équitable pondérée est à même de distinguer les différents flux de données sans requérir une telle charge administrative.

Equilibrage de charge

La meilleure façon d'ajouter de la bande passante sur un réseau fédérateur est d'implémenter des liaisons supplémentaires. Les routeurs possèdent des fonctionnalités intégrées d'équilibrage de la charge sur de multiples liaisons et chemins. Il est possible d'emprunter jusqu'à quatre chemins vers un réseau de destination. Dans certaines situations, il n'est pas nécessaire que leur coût soit équivalent.

Avec IP, les routeurs assurent une répartition de la charge, à la fois par paquets et par destinations. Lorsqu'ils se fondent sur la destination, ils utilisent les informations d'itinéraire contenues dans leur cache respectif afin de déterminer l'interface de sortie. Dans le cas d'un routage IGRP ou EIGRP, l'équilibrage peut se faire à travers des chemins de coût différent. Les routeurs emploient des métriques pour décider des itinéraires que les paquets doivent suivre ; le niveau de l'équilibrage de charge peut être défini par l'utilisateur.

L'équilibrage d'un trafic ponté sur des lignes séries est également assuré. Des lignes série peuvent être assignées à des groupes de circuits. Si l'une des liaisons d'un groupe fait partie de l'arbre recouvrant (*spanning tree*) d'un réseau, toutes ses liaisons peuvent alors être utilisées pour l'équilibrage de charge. Afin de contourner les problèmes de séquencement des données, chaque destination est associée à une liaison. Lorsqu'une interface tombe en panne ou, à l'inverse, entre en service, la réaffectation est effectuée dynamiquement.

Chemins alternatifs

Les épines dorsales de réseau sont nombreuses à transporter des données critiques. Les organisations exploitantes souhaitent généralement protéger l'intégrité de ces informations, et cela pratiquement à n'importe quel prix. Les routeurs doivent donc être suffisamment fiables afin de ne pas représenter le point faible dans la chaîne des équipements de réseau. La solution consiste à fournir des chemins alternatifs pouvant être empruntés lorsque des liaisons sur les réseaux actifs deviennent impraticables.

Il ne suffit pas de mettre en œuvre une tolérance aux pannes au niveau de l'épine dorsale pour assurer une fiabilité de bout en bout. Si la communication était pour une raison quelconque interrompue sur un segment local au sein d'un immeuble, les informations ne pourraient pas atteindre l'épine dorsale. Seule la redondance à travers tout le réseau peut permettre une fiabilité de bout en bout. Etant donné que le coût associé est habituellement prohibitif, la plupart des sociétés choisissent d'utiliser des chemins redondants uniquement sur les segments qui transportent des données sensibles.

Comment peut-on garantir la fiabilité d'une épine dorsale ? Les routeurs sont la clé d'un réseau fiable. En fonction de ce que l'on entend par fiabilité, cela peut signifier la duplication de chaque système important de routeur et, si possible, de chaque composant. Toutefois, cette solution n'est pas complète dans la mesure où tous ces composants doivent aussi être reliés par des circuits supplémentaires pour pouvoir communiquer. Ce choix se révèle généralement très coûteux, mais surtout, il ne résout pas entièrement le problème. En supposant que tous les routeurs d'un réseau soient totalement fiables, des liaisons défectueuses entre des nœuds de l'épine dorsale peuvent invalider la solution de redondance matérielle.

Pour véritablement garantir la fiabilité d'un réseau, les *liaisons* doivent être redondantes. Par ailleurs, il ne suffit pas de les dupliquer toutes. En effet, les liaisons doubles doivent se terminer sur plusieurs routeurs, à moins que tous ceux de l'épine dorsale n'offrent une parfaite tolérance aux pannes (risque de panne nul). Par conséquent, la solution la plus efficace au problème de fiabilité n'est pas la redondance totale des routeurs, car elle est coûteuse et n'apporte rien à la fiabilité des liaisons.

La plupart des concepteurs choisissent d'implémenter des réseaux qui ne sont que partiellement redondants, et non totalement. La section "Choix des options de fiabilité de réseau", plus loin dans ce chapitre, présente plusieurs types de réseaux communément mis en œuvre dans le cadre d'une recherche de fiabilité.

Accès commuté

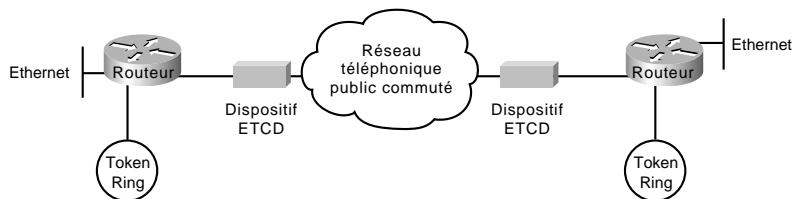
L'accès commuté permet de bénéficier de liaisons WAN sur la base de besoins ponctuels, par l'intermédiaire de contrôles de routeur automatisés. Un modèle de réseau fédérateur fiable consiste en des liaisons dupliquées et dédiées, ainsi qu'une liaison commutée inactive, capable d'assurer un secours dynamique en cas de besoin. Dans des conditions normales d'exploitation, la charge peut être répartie sur les liaisons dédiées, et la liaison commutée n'est exploitée que si l'une d'elles tombe en panne.

Les connexions WAN sur le réseau téléphonique public commuté (RTC) utilisent traditionnellement des lignes dédiées. Lorsque les applications ne requièrent que des connexions périodiques à faible débit, cela peut se révéler très onéreux. Afin de limiter les besoins en circuits dédiés, on emploie

une fonctionnalité appelée *routage par ouverture de ligne à la demande*, ou DDR (*Dial-on-Demand Routing*). La Figure 2.8 illustre une connexion DDR.

Figure 2.8

L'environnement de routage par ouverture de ligne à la demande, ou DDR.



Grâce à cette fonctionnalité, les connexions de réseau ponctuelles à faible trafic peuvent s'appuyer sur le réseau RTC. Lorsqu'un routeur reçoit un paquet IP ponté ou routé, dont la destination se trouve de l'autre côté de la ligne téléphonique, il active la fonction DDR. Une fois qu'il a composé le numéro de téléphone du réseau destinataire et établi la connexion, les paquets des protocoles supportés peuvent être transmis. Dès que l'envoi est terminé, la ligne est automatiquement libérée. Avec cette faculté de libération des connexions devenues inutiles, DDR permet de réduire le coût d'un réseau.

Encapsulation (mise en œuvre d'un tunnel)

Le processus d'*encapsulation* place les paquets ou trames d'un type de réseau dans les trames d'un autre type de réseau. On parle parfois de *technique du tunnel* (*tunneling*). Un tunnel permet d'encapsuler des paquets dans un protocole routable, par l'intermédiaire d'interfaces virtuelles. Le transport SDLC (*Synchronous Data Link Control*) consiste également en une encapsulation de paquets dans un protocole routable. De plus, il apporte des améliorations à la technique du tunnel, telles que la terminaison locale de la couche liaison de données, le blocage des diffusions broadcast, la conversion de médias, ainsi que d'autres optimisations qui autorisent une certaine évolutivité.

Les routeurs Cisco supportent les techniques d'encapsulation et de mise en œuvre de tunnel suivantes :

■ Méthodes proposées par la technologie IBM :

- STUN (*Serial Tunneling*) ou transport SDLC (*Synchronous Data Link Control*) ;
- SRB (*Source Routing Bridge*) avec encapsulation directe ;
- SRB avec encapsulation FST (*Fast Sequenced Transport*) ;
- SRB avec encapsulation TCP/IP (*Transmission Control Protocol/Internet Protocol*) ;
- DLSw+ (*Data Link Switching Plus*) avec encapsulation directe ;
- DLSw+ avec encapsulation TCP/IP ;
- DLSw+ avec encapsulation FST/IP (*Fast Sequenced Transport/Internet Protocol*) ;
- DLSw+ avec encapsulation DLSw Lite (*Logical Link Control Type 2 [LLC2]*).

- Protocole GRE (*Generic Routing Encapsulation*) de Cisco.

Avec GRE, Cisco gère l’encapsulation des protocoles IPX (*Internetwork Packet Exchange*) de Novell, IP (*Internet Protocol*), CLNP (*Connectionless Network Protocol*), AppleTalk, DECnet Phase IV, XNS (*Xerox Network Systems*), VINES (*Virtual Network System*) de Banyan, ainsi que des paquets Apollo pour le transport sur IP.

- Techniques de tunnel à protocole unique : Cayman (AppleTalk sur IP), AURP (AppleTalk sur IP), EON (CLNP sur IP) et NOS (IP sur IP).

Les sections suivantes traitent des différents types d’encapsulations IBM et de la technique de tunnel multiprotocole de GRE.

Types d’encapsulations IBM

La mise en œuvre d’un tunnel sur une ligne série, *via* STUN, permet à deux équipements normalement reliés par une liaison série directe d’être connectés par le biais d’un ou de plusieurs routeurs, au moyen de protocoles compatibles avec SDLC ou HDLC (*High-level Data Link Control*). Ces routeurs peuvent être connectés *via* un réseau multiprotocole de topologie quelconque. STUN permet aussi l’intégration de réseaux SNA et non SNA, au moyen de routeurs et de liaisons existantes. Le transport à travers le réseau multiprotocole qui relie les routeurs peut utiliser TCP/IP. Ce type de transport autorise un routage fiable et intelligent, par l’intermédiaire de n’importe quel protocole de routage pour IP supporté. Une configuration STUN est illustrée à la Figure 2.9.

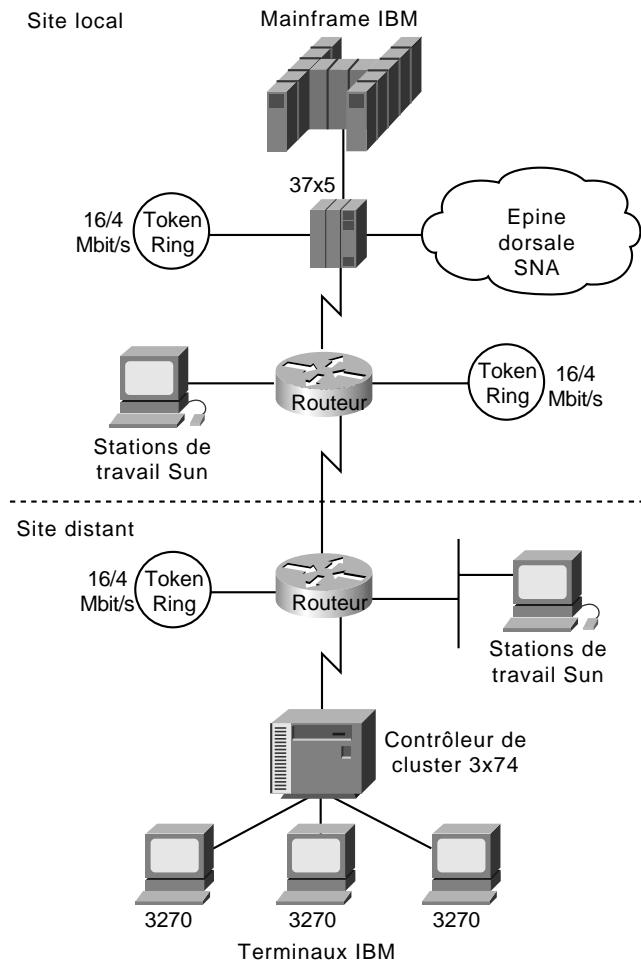
Le transport SDLC est une variante de STUN qui permet à des sessions utilisant des protocoles SDLC et une encapsulation TCP/IP d’être terminées au niveau local. Il permet aussi une participation aux opérations de fenêtrage SDLC et aux activités de retransmission.

Lorsqu’il s’agit de relier des équipements distants utilisant SRB (*Source Routing Bridge*, pont à routage par la source) sur une liaison série à faible vitesse, la plupart des concepteurs de réseaux choisissent d’implémenter RSRB (système de ponts distants à routage par la source) avec une encapsulation HDLC directe. Dans ce cas, les trames SRB sont encapsulées dans un en-tête HDLC. Cette solution n’ajoute qu’une légère surcharge de service, économisant ainsi la précieuse bande passante de la ligne série. L’encapsulation HDLC directe ne se limite pas aux liaisons séries (elle peut également être utilisée sur des liaisons Ethernet, Token Ring et FDDI), mais convient mieux lorsque le réseau qui procède à l’encapsulation ne peut tolérer une surcharge de contrôle additionnelle.

Si une certaine surcharge de service est tolérée et que le séquencement des trames soit important, mais qu’une livraison extrêmement fiable ne soit pas nécessaire, les paquets SRB peuvent être envoyés par le biais de liaisons série sur des réseaux Token Ring, Ethernet et FDDI, en utilisant l’encapsulation FST (*Fast Sequenced Transport*). FST est semblable à TCP dans le sens où il effectue le séquencement des paquets, mais s’en distingue par le fait qu’il n’assure pas leur acquittement.

Afin de bénéficier d’une remise extrêmement fiable dans des environnements pouvant supporter une surcharge moyenne, il est possible d’encapsuler les trames SRB dans des paquets TCP/IP. Cette solution n’est pas seulement fiable, elle permet également de tirer parti de fonctionnalités de routage, telles que la manipulation de paquets par des protocoles de routage, le filtrage de paquets et le routage multichemin.

Figure 2.9
Une configuration STUN.



GRE (Generic Routing Encapsulation)

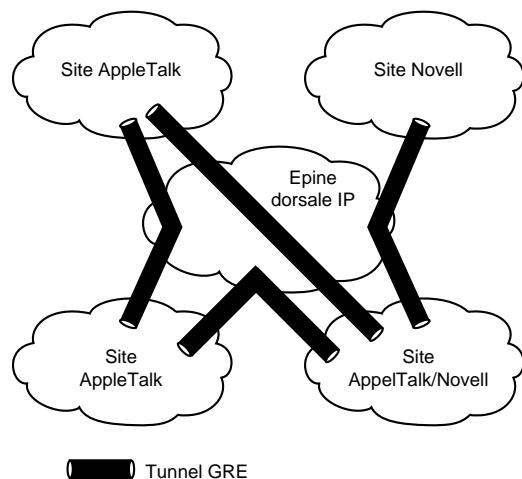
Le protocole GRE de transport multiprotocole de Cisco encapsule des paquets IP, CLNP, IPX, AppleTalk, DECnet Phase IV, XNS, VINES et Apollo dans des tunnels IP. Dans la technique de tunnel GRE, un routeur Cisco sur un site encapsule les paquets d'un protocole donné dans un en-tête IP afin de les envoyer à un autre routeur Cisco, situé sur un site de l'autre côté du nuage IP, où l'en-tête sera supprimé, créant ainsi une liaison point-à-point virtuelle entre les deux sites. La technique du tunnel IP permet ainsi l'extension de réseaux, en reliant des sous-réseaux de protocoles divers à travers un environnement fédérateur à protocole unique. La technique du tunnel GRE implique trois types de protocoles :

- **Passager.** Le protocole est encapsulé (IP, CLNP, IPX, AppleTalk, DECnet Phase IV, XNS, VINES et Apollo).
- **Opérateur.** Le protocole GRE offre des services d'opérateur.

■ **Transport.** IP transporte le protocole encapsulé.

Grâce au tunnel GRE, les protocoles de bureau peuvent bénéficier des fonctionnalités avancées de sélection de route d'IP. De nombreux protocoles de LAN, tels AppleTalk et IPX, ont été optimisés pour une utilisation locale. Ils disposent d'un faible choix de métriques de sélection de route et souffrent de limitations au niveau des comptes de sauts (*hop count*). Les protocoles de routage IP permettent une sélection de route plus souple et s'adaptent mieux aux grands réseaux. La Figure 2.10 illustre la technique du tunnel GRE à travers une épine dorsale IP reliant plusieurs sites. Quel que soit le nombre de routeurs et de chemins associés au nuage IP, le tunnel est vu comme un seul saut.

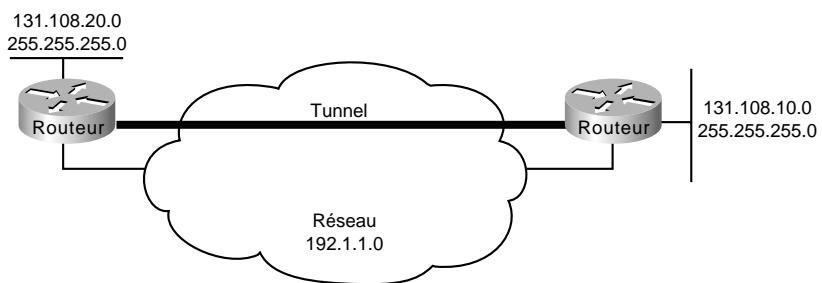
Figure 2.10
Utilisation d'une épine dorsale à protocole unique.



GRE possède des fonctionnalités essentielles — le séquencement des paquets et la possibilité de transporter des données par tunnel à des vitesses élevées — qui font défaut aux autres protocoles d'encapsulation. Certains protocoles de plus haut niveau nécessitent que les paquets soient livrés dans le bon ordre. La fonction de séquencement de GRE répond à cette nécessité. GRE dispose également en option d'une fonction importante qui permet d'éviter les erreurs de configuration, en exigeant qu'une même clé soit fournie à chaque extrémité du tunnel avant que les données transportées ne soient traitées. Le tunnel IP autorise aussi les concepteurs de réseaux à organiser diverses stratégies, telles l'association de types de trafics à des routes données ou l'assignation de niveaux de priorité ou de sécurité à certains types de trafics. Bon nombre de protocoles de LAN, dans leur forme native, ne possèdent pas ces fonctionnalités.

Le tunnel IP permet à des sous-réseaux non contigus ou dotés d'adresses invalides de communiquer, en leur assignant des adresses de réseau virtuelles. La Figure 2.11 montre de quelle manière deux sous-réseaux faisant partie du réseau 131.108.0.0 peuvent dialoguer grâce à GRE, alors qu'ils sont physiquement séparés par un autre réseau.

Figure 2.11
Connexion de deux sous-réseaux non contigus, à l'aide d'un tunnel.



Puisque l'encapsulation requiert la manipulation de paquets, il est généralement plus rapide de les router de façon native plutôt que d'utiliser des tunnels. La vitesse de commutation du trafic qui transite par des tunnels est deux fois inférieure à celle du processus de commutation classique, c'est-à-dire que chaque routeur traite environ 1 000 paquets par seconde. La technique du tunnel est coûteuse en ressources processeur ; son activation doit donc faire l'objet d'une certaine prudence. Chaque interface de tunnel peut avoir à véhiculer des informations de mise à jour de routage, de mise à jour SAP, ainsi que d'autres types de trafics administratifs. Lorsque plusieurs tunnels sont configurés sur une même liaison physique, celle-ci peut rapidement se retrouver saturée d'informations de routage. Les performances dépendent alors du protocole passager, des diffusions broadcast, des mises à jour d'informations de routage et de la bande passante des interfaces physiques. En cas de défaillance, le dépannage d'une liaison physique peut également se révéler difficile. Il existe cependant plusieurs moyens de dépannage en cas de problème avec le lien physique. Dans un environnement IPX, des filtres de routage et des filtres SAP réduisent la quantité de trafic de mise à jour qui circule sur les tunnels. Sur un réseau AppleTalk, le maintien de petites zones et l'emploi de filtres de route peuvent limiter les exigences excessives en bande passante.

Un tunnel peut également masquer la véritable nature d'une liaison, la rendant plus lente, plus rapide, ou plus ou moins coûteuse qu'elle ne l'est en réalité. Il peut en résulter une sélection de route imprévue ou malencontreuse. Les protocoles de routage qui se fondent uniquement sur le compte de sauts pour décider de la route à emprunter préfèrent généralement utiliser un tunnel plutôt qu'une liaison réelle. Mais ce n'est pas toujours la meilleure solution, car un nuage IP peut être constitué de divers médias dont les qualités sont très différentes. Par exemple, le trafic peut être acheminé sur des lignes Ethernet à 100 Mbit/s et sur des lignes séries à 9,6 Kbit/s. Avant d'implémenter un tunnel, il faut penser à vérifier le type de média sous-jacent et les métriques utilisées par chaque protocole.

Etant donné que les tunnels encapsulent des protocoles passagers non contrôlés, lorsqu'un réseau comporte des sites qui mettent en œuvre un filtrage de paquets fondé sur des protocoles dans le cadre d'un système de sécurité avec pare-feu, il faut implémenter le filtrage sur le routeur pare-feu afin que seuls les tunnels autorisés puissent accéder au réseau. S'il est prévu que des tunnels en provenance de réseaux non sécurisés soient acceptés, il est conseillé d'activer le filtrage au niveau de la sortie de ces tunnels, ou bien de placer celle-ci à l'extérieur de la zone sécurisée du réseau, afin de préserver l'intégrité du système de sécurité.

Lors de la mise en œuvre d'un tunnel IP sur IP, il faut veiller à ne pas configurer par mégarde une boucle de routage. Une telle situation se produit lorsque le protocole passager et le protocole de transport sont identiques, car le meilleur chemin vers la destination du tunnel passe par l'interface du tunnel. Voici comment survient une boucle de routage avec un tunnel IP sur IP :

1. Le paquet est placé en file d'attente de sortie de l'interface du tunnel.
2. L'interface du tunnel ajoute un en-tête GRE, puis place le paquet dans la file d'attente du protocole de transport (IP) afin qu'il soit acheminé vers l'adresse de destination du tunnel.
3. IP recherche la route vers l'adresse de destination du tunnel et apprend que le chemin passe par l'interface du tunnel elle-même.
4. De nouveau, le paquet est placé dans la file d'attente de sortie de l'interface du tunnel, comme décrit à l'étape 1. La boucle est ainsi provoquée.

Lorsqu'un routeur détecte une boucle de routage, il désactive l'interface du tunnel pendant une ou deux minutes, puis émet un message d'avertissement avant de s'engager dans la boucle. On peut également conclure qu'une boucle a été détectée lorsque l'interface du tunnel est active et que le protocole de ligne est inactif.

Afin d'éviter ces boucles, il faut séparer les informations de protocole passager et de routage du protocole de transport, en suivant ces instructions :

- Utiliser des identifiants de protocole de routage différents (par exemple, IGRP 1 et IGRP 2).
- Utiliser des protocoles de routage différents.
- Attribuer à l'interface du tunnel une très faible quantité de bande passante, afin que les protocoles de routage, tel IGRP, lui reconnaissent une très haute métrique et choisissent par conséquent le prochain saut approprié (c'est-à-dire l'interface physique la plus efficace plutôt que celle du tunnel).
- Faire en sorte que les deux plages d'adresse IP soient distinctes. Pour cela, utiliser une adresse principale pour le tunnel différente de celle du réseau IP réel. Une telle mesure facilite également le dépannage, car il est plus aisés de déterminer l'appartenance de chaque adresse.

Services de distribution

Cette section couvre les fonctionnalités de réseau qui supportent des services de distribution. Les sujets suivants y sont traités :

- gestion de la bande passante du réseau fédérateur ;
- filtrage de zones et de services ;
- distribution stratégique ;
- services de passerelle ;
- redistribution de routes interprotocoles ;
- traduction du format de trame.

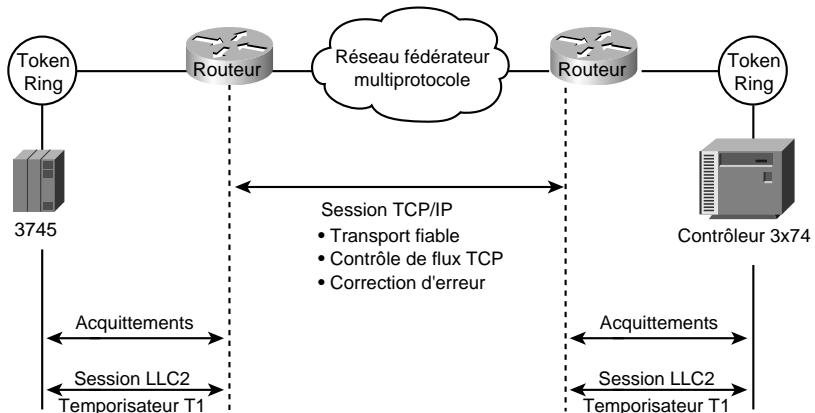
Gestion de la bande passante du réseau fédérateur

En vue d'optimiser le fonctionnement du réseau fédérateur, les routeurs offrent plusieurs options de mise au point des performances, telles la mise en file d'attente de priorité, l'utilisation de métriques par les protocoles de routage et la terminaison locale de session.

Il est possible d'ajuster la longueur des files d'attente de priorité. Si une file déborde, les paquets supplémentaires sont supprimés et des messages de notification de congestion (*quench*) sont envoyés, si nécessaire, afin de stopper le flux de paquets du protocole concerné. On peut également adapter les métriques de routage afin de mieux contrôler les chemins empruntés par le trafic à travers le réseau.

La terminaison locale de session permet à des routeurs de jouer le rôle de proxy pour des systèmes distants qui représentent les points d'extrémité de session (un *proxy* est un agent intermédiaire qui effectue certaines opérations pour le compte d'un autre). La Figure 2.12 illustre un exemple de terminaison locale de session dans un environnement IBM.

Figure 2.12
Terminaison locale de session sur un réseau fédérateur multiprotocole.



A la Figure 2.12, les routeurs terminent localement les sessions de contrôle LLC2 (*Logical Link Control Type 2*) de liaison de données. Plutôt que mettre en place des sessions de bout en bout où toutes les informations de contrôle sont transmises sur l'épine dorsale multiprotocole, les routeurs prennent en charge l'acquittement des paquets qui proviennent des hôtes de réseaux locaux (LAN) qui leur sont directement rattachés. L'acquittement au niveau local permet d'économiser la bande passante du WAN (et, par conséquent, de limiter les frais liés à son exploitation), d'éviter les problèmes de dépassement de temporisation, et d'offrir un meilleur temps de réponse aux utilisateurs.

Filtrage de zones et de services

Les filtres de trafic qui s'appuient sur le type de *zone* ou de *service* sont les principaux outils des services de distribution utilisés afin d'assurer un contrôle d'accès au niveau des services du réseau fédérateur. Ils sont implantés au moyen de *listes d'accès* (*access list*). Celles-ci sont constituées de séquences d'instructions, chacune d'elle autorisant ou refusant certaines conditions ou adresses.

Elles peuvent servir à accepter ou à rejeter les messages qui proviennent de nœuds de réseau spécifiques ou envoyés à l'aide de protocoles ou de services particuliers.

Ces filtres sont utilisés afin d'assurer une transmission sélective du trafic, basée sur l'adresse de réseau. Ils peuvent être mis en œuvre au niveau des ports d'entrée ou de sortie. Les filtres de service emploient des listes d'accès appliquées à des protocoles (tel UDP pour IP), des applications (telle SMTP, *Simple Mail Transfer Protocol*) et des protocoles spécifiques.

Supposons que vous disposiez d'un réseau connecté à l'Internet. Vous souhaitez que tous les hôtes d'un réseau Ethernet soient en mesure d'établir des connexions TCP/IP avec n'importe quel hôte sur l'Internet, mais que l'inverse ne soit pas possible. La seule exception est la connexion d'un hôte Internet sur le port SMTP d'un hôte de messagerie dédié.

SMTP utilise le port TCP 25 à l'une des extrémités de la connexion, et un numéro de port aléatoire de l'autre côté. Ces deux numéros sont conservés tout au long de la connexion. Les paquets de messages en provenance de l'Internet sont envoyés sur le port 25, tandis que ceux à destination de l'extérieur sont envoyés vers l'autre numéro de port. Le fait que le système de sécurité implémenté par le routeur accepte toujours les connexions de messagerie sur le port 25 permet de contrôler séparément les services entrants et sortants. La liste d'accès peut être configurée au niveau de l'interface d'entrée ou de sortie.

Dans l'exemple suivant, le réseau Ethernet est de classe B. Son adresse est 128.88.0.0 ; celle de l'hôte de messagerie est 128.88.1.2. Le mot clé **established** sert uniquement au protocole TCP pour indiquer une connexion établie. Une correspondance se produit si les bits ACK ou RST du data-gramme TCP sont activés, signifiant que le paquet appartient à une connexion existante :

```
access-list 102 permit tcp 0.0.0.0 255.255.255.255
    128.88.0.0 0.0.255.255 established
access-list 102 permit tcp 0.0.0.0 255.255.255.255
    128.88.1.2 0.0.0.0 eq 25
interface ethernet 0
ip access-group 102
```

Distribution stratégique

La distribution stratégique part du principe que plusieurs départements d'une organisation peuvent observer des règles différentes de distribution du trafic à travers tout le réseau. Cette forme de distribution vise à satisfaire des exigences différentes, sans pour autant provoquer de répercussions négatives quant aux performances et à l'intégrité des informations.

Une *stratégie* dans ce contexte est une règle ou un ensemble de règles qui gouvernent la distribution du trafic, de bout en bout, en direction d'un réseau fédérateur, puis sur ce réseau. Un département pourrait injecter vers cette épine dorsale un trafic composé de trois protocoles différents, mais souhaiter que celui d'un protocole spécifique transite également à travers cette artère, car il transporte des données critiques. Un autre département pourrait également vouloir réduire un trafic interne déjà excessif en interdisant à tout trafic en provenance de l'épine dorsale de pénétrer sur son segment de réseau, excepté celui de courrier électronique et d'applications personnalisées essentielles.

Ces exemples reflètent des stratégies propres à certains départements. Toutefois, elles pourraient correspondre à l'ensemble des objectifs de l'organisation. Par exemple, celle-ci pourrait souhaiter réglementer le trafic sur l'épine dorsale en se fondant sur un maximum de 10 % d'utilisation de la

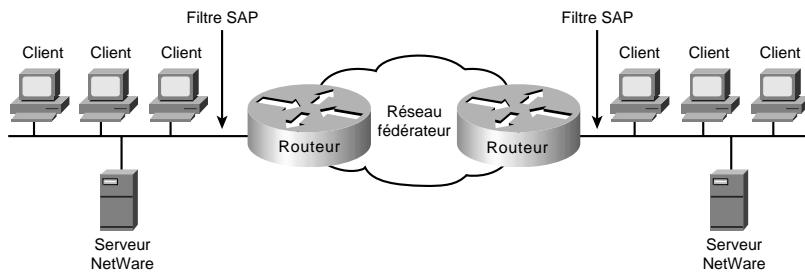
bande passante en moyenne durant la journée, avec des crêtes d'une minute où la consommation passe à 30 %. Une autre stratégie d'entreprise pourrait garantir que deux départements distants peuvent communiquer à n'importe quel moment, malgré des technologies de réseau différentes.

Diverses stratégies requièrent souvent l'emploi de technologies différentes au niveau des groupes de travail ou des départements. Par conséquent, la mise en œuvre de la distribution stratégique implique le support du large éventail de technologies actuellement en place. En retour, le fait de pouvoir implémenter des solutions qui supportent de nombreuses stratégies permet d'accroître la souplesse de l'organisation et la disponibilité des applications.

Outre la gestion de ces différentes technologies de réseau, des moyens doivent être mis en œuvre pour, à la fois les séparer, et les intégrer de façon appropriée. Elles doivent pouvoir coexister ou, au besoin, être combinées intelligemment selon les situations.

Observez la situation illustrée à la Figure 2.13. Une entreprise souhaite limiter le trafic inutile sur l'épine dorsale. Une solution serait de réduire la transmission des messages du protocole d'annonces SAP (Service Advertisement Protocol) qui permettent à des serveurs NetWare d'annoncer les services proposés aux clients. L'entreprise pourrait donc définir une stratégie stipulant que tous les services NetWare doivent être assurés localement. Dans ce cas, il n'y a aucune raison pour que des services soient annoncés à distance. L'organisation pourrait donc mettre en œuvre des filtres SAP pour empêcher que ce type de trafic ne quitte une interface de routeur, satisfaisant ainsi aux exigences de circulation de trafic sur l'épine dorsale.

Figure 2.13
Distribution stratégique avec filtrage SAP.



Services de passerelle

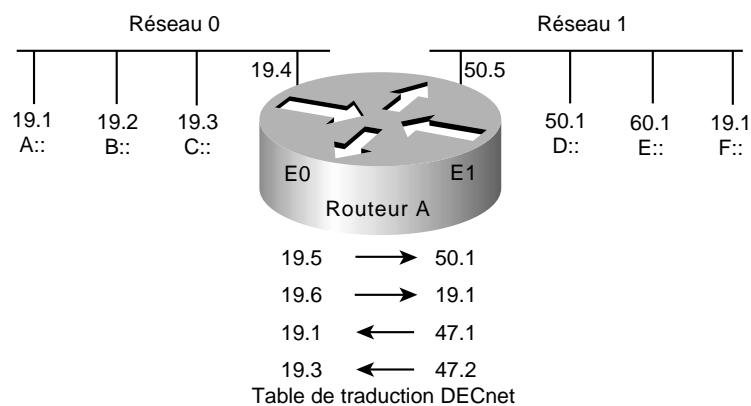
Les fonctions de passerelle de protocole font partie de la panoplie logicielle standard de chaque routeur. Par exemple, au moment de l'élaboration de cet ouvrage, Digital Equipment commercialisait DECnet Phase V. Les adresses de cette version sont différentes de celles utilisées par DECnet Phase IV. Pour les réseaux qui nécessitent la cohabitation des deux types d'hôtes, la traduction bidirectionnelle Phase IV/Phase V est conforme aux directives de Digital. Les routeurs Digital interagissent avec d'autres routeurs, et les hôtes Digital ne font aucune distinction entre les différents équipements.

La connexion de plusieurs réseaux DECnet indépendants peut conduire à la nécessité de résoudre certains problèmes. Rien n'empêche deux administrateurs d'assigner tous deux la même adresse de noeud 10 à un hôte sur leur réseau respectif. Toutefois, lorsque les deux réseaux se connecteront

ultérieurement, des conflits naîtront. DECnet fournit des passerelles de traduction d'adresses (ATG, *Address Translation Gateway*) pour régler ce problème. La solution ATG gère, au niveau routeur, la traduction des adresses de deux réseaux DECnet différents unis par un routeur. La Figure 2.14 illustre un exemple de cette opération.

Sur le Réseau 0, le routeur est configuré avec l'adresse 19.4 ; c'est un routeur de niveau 1. Sur le Réseau 1, le routeur est configuré avec l'adresse 50.5 ; c'est un routeur de zone. A ce stade, aucune information de routage n'est échangée entre les deux réseaux. Le routeur maintient une table de routage séparée pour chaque réseau. En établissant une carte de traduction, les paquets du Réseau 0 envoyés à l'adresse 19.5 seront routés sur le Réseau 1 avec l'adresse de destination 50.1, et les paquets envoyés vers l'adresse 19.6 seront routés vers le Réseau 1 avec l'adresse de destination 19.1. De la même manière, les paquets transmis sur le Réseau 1 vers l'adresse 47.1 seront aiguillés vers le Réseau 0 avec 19.1 comme adresse de destination, et les paquets expédiés vers l'adresse 47.2 seront acheminés vers le Réseau 0 avec l'adresse 19.3.

Figure 2.14
Exemple d'implémentation
de la traduction ATG de
DECnet.



AppleTalk est un autre exemple de protocole ayant fait l'objet de plusieurs révisions, chacune comportant des caractéristiques d'adressage quelque peu différentes. Les adresses d'AppleTalk Phase 1 suivent une forme locale simple, celles d'AppleTalk Phase 2 emploient une structure étendue (multiréseau). Normalement, des informations expédiées à partir d'un nœud Phase 2 ne peuvent pas être comprises par un nœud Phase 1 si l'adressage étendu Phase 2 est utilisé. Les routeurs gèrent l'acheminement du trafic entre ces deux types de nœuds sur un même câble, au moyen d'un routage transitoire.

Le routage transitoire peut être réalisé en reliant deux ports de routeur au même câble. Configurez un port pour gérer l'adressage non étendu et l'autre port pour l'adressage étendu. Ils doivent chacun disposer d'une adresse de réseau unique. Les paquets sont ensuite traduits, puis envoyés sur l'un ou l'autre des deux ports, selon les nécessités.

Redistribution de routes interprotocoles

La section précédente relative aux services de passerelle a décrit de quelle manière des passerelles de protocole *routé* peuvent permettre à deux nœuds d'extrémité d'implémentations différentes de communiquer. Les routeurs peuvent également agir en tant que passerelle pour les protocoles de *routage*. Les informations en provenance d'un protocole de routage tel que IGRP peuvent être transmises et utilisées par un autre protocole de routage, tel RIP. Cela peut se révéler utile lorsque plusieurs protocoles de routage sont utilisés sur un même réseau.

Les informations de routage peuvent être échangées entre n'importe quels protocoles de routage pour IP supportés : RIP, IGRP, OSPF, EIGRP, IS-IS, EGP ou BGP. De la même manière, la redistribution de route est supportée par ISO CLNS entre ISO IGRP et IS-IS. Les informations de routage statiques peuvent également être redistribuées. Des paramètres par défaut peuvent être assignés afin qu'un protocole de routage puisse utiliser la même métrique pour toutes les routes redistribuées, ce qui simplifie le mécanisme.

Traduction du format de trame

Les techniques de traduction du média permettent de convertir les trames d'un système de réseau vers un autre. Ce type de traduction est rarement efficace à 100 %, car un système peut utiliser des attributs qui ne trouvent pas leur corollaire dans un autre système. Par exemple, les réseaux Token Ring mettent en œuvre une gestion de priorité et de réservation intégrée, que les réseaux Ethernet n'assurent pas. Les traductions qui interviennent entre ces deux architectures doivent d'une façon ou d'une autre pouvoir prendre en compte ces différences. Il arrive qu'elles ne soient pas traitées de la même manière selon les fabricants, bloquant ainsi toute interopérabilité.

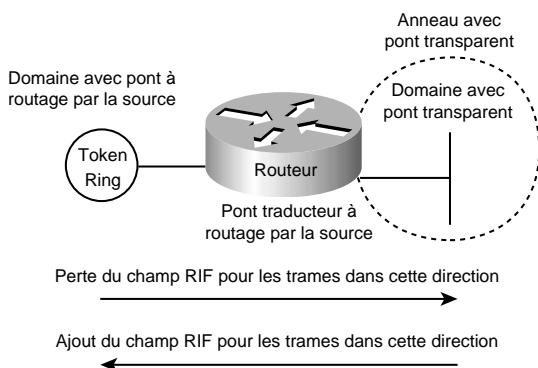
Dans des situations où la communication entre des stations situées sur des médias différents doit être autorisée, les routeurs peuvent procéder à la traduction des trames. Pour implémenter un pont direct entre des environnements Ethernet et Token Ring, utilisez soit un pont traducteur à routage par la source, soit un pont transparent à routage par la source (SRT). La première solution permet d'obtenir une traduction du format des trames de ces deux architectures, la seconde permet aux routeurs d'utiliser les algorithmes de pont SRB ou de pont transparent qui sont utilisés dans les systèmes de pontage Ethernet standard.

Lors du passage d'un domaine SRB à un domaine à pont transparent, les champs SRB des trames sont supprimés. Les champs RIF sont placés en cache pour être utilisés par le trafic en retour. Lors du pontage dans le sens opposé, le routeur vérifie le paquet afin de déterminer s'il fait partie d'une diffusion broadcast, multicast, ou unicast. Dans les deux premiers cas, il est envoyé en tant que paquet d'exploration d'arbre recouvrant. Dans le troisième cas, le routeur recherche le chemin de destination du paquet dans le cache RIF, et l'utilise s'il le trouve. Sinon, il l'envoie en tant que paquet d'exploration d'arbre recouvrant. Un exemple simple de cette topologie est illustré à la Figure 2.15.

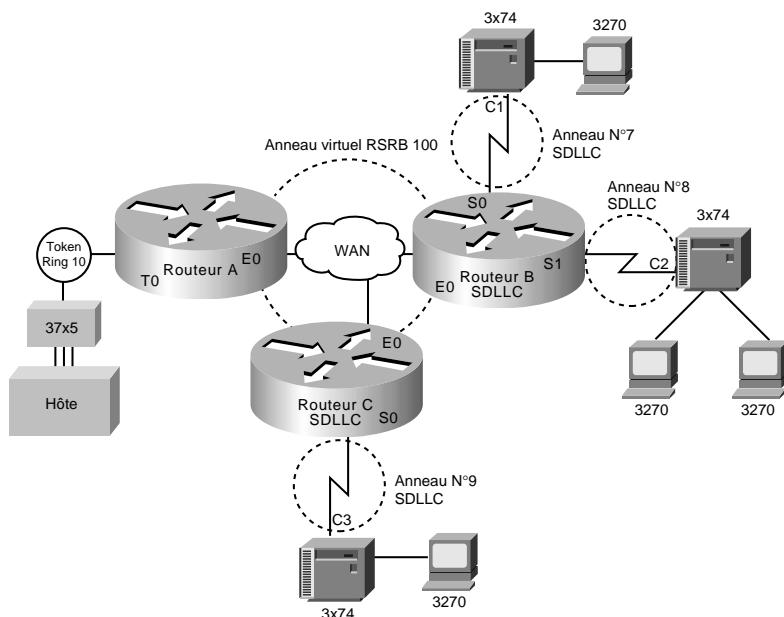
Les routeurs supportent SRT lorsque les deux algorithmes de pontage, SRB et transparent, sont implantés sur chaque interface SRT. Si une interface détecte la présence d'un champ RIF, elle utilise l'algorithme SRB, sinon elle utilise l'autre algorithme.

Figure 2.15

Topologie de pont traducteur à routage par la source.

**Figure 2.16**

Une configuration SDLLC complexe.



La traduction entre des lignes série qui exploitent le protocole SDLC et des anneaux Token Ring qui exploitent LLC2 est aussi possible. Elle est connue sous la désignation de *traduction de trame SDLLC* et autorise les connexions entre des lignes série et des réseaux Token Ring. Cela peut se révéler utile pour consolider des réseaux SNA/SDLC, traditionnellement disparates, en un réseau fédérateur multimédia, multiprotocole, fondé sur un LAN. Avec SDLLC, les routeurs peuvent terminer les sessions SDLC, traduire les trames SDLC en trames LLC2, puis transmettre ces dernières par voie de pontage RSRB sur une liaison point-à-point ou un réseau IP. Puisqu'un réseau IP fondé sur des routeurs peut utiliser un média quelconque (FDDI, Frame Relay ou X.25), ou encore des lignes louées, les routeurs gèrent SDLLC au-dessus de ces technologies, au moyen d'une encapsulation IP.

Une configuration SDLLC complexe est illustrée à la Figure 2.16.

Services d'accès locaux

La section suivante traite des fonctions de réseaux qui gèrent les services d'accès locaux. Voici les sujets qui y sont abordés :

- adressage de réseau à valeur ajoutée ;
- segmentation de réseau ;
- diffusion broadcast et diffusion multicast ;
- services de noms, de proxy et de cache local ;
- sécurité de l'accès au média ;
- découverte de routeurs.

Adressage de réseau à valeur ajoutée

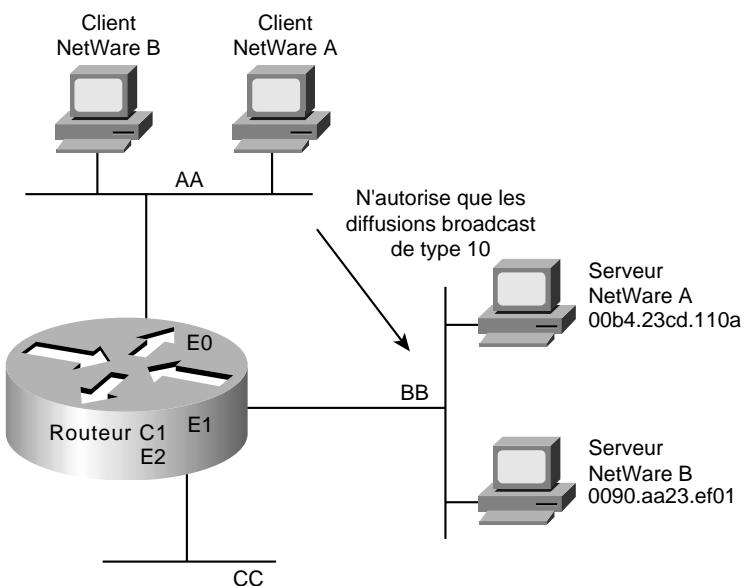
Les politiques d'adressage sur des réseaux fondés sur des LAN, tels que les réseaux NetWare, ne s'adaptent pas toujours parfaitement à une utilisation sur des réseaux multisegments locaux ou étendus. Un outil que les routeurs implémentent afin d'assurer le fonctionnement de ces règles est *l'adressage de soutien* pour un protocole donné. Il s'agit d'un mécanisme d'assistance qui permet de faire transiter un trafic spécifique à travers un réseau sur lequel il ne circuleraient pas autrement.

L'utilisation de cet adressage auxiliaire sera mieux illustrée par un exemple. Imaginons son emploi sur les réseaux IPX de Novell. Les clients Novell envoient des messages broadcast lorsqu'ils recherchent un serveur. Si celui-ci n'est pas local, le trafic broadcast doit être retransmis par l'intermédiaire de routeurs. Les adresses auxiliaires et les listes d'accès peuvent être utilisées ensemble pour permettre aux diffusions broadcast de certains nœuds d'un réseau d'être dirigées précisément vers certains serveurs sur un autre réseau. Chaque interface gère plusieurs de ces adresses, afin que les paquets broadcast puissent être transmis à plusieurs hôtes. La Figure 2.17 illustre l'emploi de cet adressage avec NetWare.

Les clients NetWare sur le Réseau AA sont autorisés à émettre des messages broadcast vers n'importe quel serveur sur le Réseau BB. Une liste d'accès applicable spécifierait que les paquets broadcast de type 10 sont autorisés à partir de tous les nœuds sur le Réseau AA. Grâce à la configuration d'un adressage auxiliaire, on identifie les adresses sur le Réseau BB vers lesquelles les diffusions broadcast sont dirigées. Aucun autre nœud sur le Réseau BB ne reçoit ces diffusions. Les diffusions broadcast de type autre que 10 ne seront pas routées.

Aucune diffusion broadcast en provenance d'un réseau en aval du Réseau AA (par exemple un Réseau AA1 quelconque) ne sera retransmise vers le Réseau BB par l'intermédiaire du Routeur C1, à moins que les routeurs séparant les Réseaux AA et AA1 ne soient configurés pour le faire, au moyen de paramètres prévus à cet effet. Dans un tel cas, ces paramètres doivent être appliqués aux interfaces d'entrée, et configurés pour autoriser l'acheminement des diffusions broadcast entre les réseaux directement connectés. De cette façon, le trafic est retransmis, mais de manière dirigée, de réseau en réseau.

Figure 2.17
Illustration du contrôle de diffusion broadcast avec adressage de soutien.



Segmentation de réseau

La division de réseaux en sous-éléments plus faciles à gérer est le rôle essentiel des routeurs d'accès local. Ils permettent en particulier d'implémenter des stratégies locales et de limiter le trafic inutile. Parmi les moyens mis à la disposition des concepteurs pour exploiter ces routeurs à des fins de segmentation, on trouve les sous-réseaux IP, l'adressage de zone DECnet et les zones AppleTalk.

Vous pouvez utiliser des routeurs d'accès local pour implémenter des stratégies locales, en les plaçant à des endroits stratégiques et en les configurant de façon à suivre des règles spécifiques. Par exemple, vous pouvez définir une série de segments LAN avec des adresses de sous-réseaux différentes ; les routeurs seraient configurés avec des adresses d'interface et des masques de sous-réseau appropriés. En général, le trafic sur un segment donné est limité aux diffusions broadcast locales, aux messages à destination d'une station sur le même segment ou à destination d'un autre routeur. En répartissant les hôtes et les clients ingénierusement, vous pouvez employer cette méthode simple de division d'un réseau pour réduire l'ensemble de la congestion.

Diffusions broadcast et multicast

De nombreux protocoles exploitent les possibilités de diffusions broadcast et multicast. Une diffusion *broadcast* (diffusion générale) consiste en l'envoi d'un paquet vers toutes les destinations possibles du réseau. Une diffusion *multicast* (diffusion restreinte, multidestinataire ou encore multipoint) est l'émission d'un paquet à destination d'un sous-ensemble spécifique de nœuds du réseau. Les routeurs sont dotés d'un comportement par défaut qui limite la prolifération des diffusions broadcast, mais ils peuvent aussi être configurés pour les relayer, si nécessaire. Dans certaines situations, la retransmission de ce type d'envoi est souhaitable, voire nécessaire. L'essentiel est de pouvoir contrôler à la fois les diffusions broadcast et multicast au moyen de routeurs.

Dans le monde IP, à l'instar d'autres technologies d'ailleurs, les requêtes broadcast sont chose courante. A moins qu'elles ne soient contrôlées, la bande passante peut s'en trouver sérieusement affectée. Les routeurs proposent plusieurs fonctions qui permettent de réduire ce type de trafic et, du même coup, les risques de tempêtes de broadcast. Par exemple, la diffusion broadcast dirigée permet d'envoyer les paquets concernés vers un réseau ou une série de réseaux spécifiques, au lieu de les transmettre sur l'ensemble du réseau. Lorsque les diffusions broadcast par inondation (envoyées sur tout le réseau) sont nécessaires, les routeurs Cisco s'appuient sur une technique dans laquelle les paquets suivent un arbre recouvrant le réseau. L'arbre recouvrant assure une couverture complète, sans trafic excessif, car un paquet unique est envoyé sur chaque segment de réseau.

Comme on l'a vu dans la section consacrée à l'adressage de réseau à valeur ajoutée, le contrôle du trafic broadcast est pris en charge par les mécanismes de l'adressage auxiliaire. Avec ce soutien, vous pouvez également autoriser un routeur ou une série de routeurs à relayer ce trafic, qui autrement serait bloqué. Par exemple, grâce à l'acheminement des diffusions broadcast SAP, les clients sur différents segments de réseau peuvent être avertis de la disponibilité de certains services NetWare assurés par des serveurs distants donnés.

La fonctionnalité de diffusion multicast IP de Cisco autorise le trafic IP à être acheminé à partir d'une source vers un nombre spécifique de destinations. A la différence de la diffusion broadcast qui transmet un paquet vers toutes les destinations, la diffusion multicast s'adresse à un groupe identifié par une seule adresse IP. Ce type d'envoi offre un excellent support pour des applications telles que la vidéo, l'audioconférence, la découverte de ressources et la distribution des résultats de marchés boursiers.

Pour que la diffusion multicast IP soit possible, les hôtes IP doivent exploiter le protocole IGMP (*Internet Group Management Protocol*). Ils peuvent ainsi signaler leur appartenance à un groupe auprès d'un routeur multicast situé dans un voisinage immédiat. L'enregistrement d'appartenance à un tel groupe est un processus dynamique. Les routeurs qui gèrent ce mode de diffusion envoient des messages de requête IGMP sur les réseaux locaux auxquels ils sont connectés. Les membres d'un groupe y répondent par l'émission de rapports IGMP sur les groupes auxquels ils appartiennent. Un routeur prend en compte le rapport d'enregistrement envoyé par le premier hôte abonné à un groupe, puis supprime tous les rapports identiques d'autres hôtes qui appartiendraient au même groupe.

Le routeur multicast connecté au réseau local a pour responsabilité de transmettre les datagrammes d'un groupe vers tous les autres réseaux qui comportent un hôte membre de ce groupe. Les routeurs élaborent des arbres de distribution multicast (tables de routage) afin que les paquets puissent emprunter des routes exemptes de boucles jusqu'à leur destination, sans être dupliqués. Si aucun rapport n'est reçu pour un groupe après un nombre défini de requêtes IGMP, le routeur multicast concerné supposera qu'aucun membre local n'en fait partie, et stoppera l'acheminement des diffusions multicast concernant ce groupe.

Les routeurs Cisco gèrent aussi le protocole PIM (*Protocol Independent Multicast*).

Services de noms, de proxy et de cache local

Trois fonctions essentielles du routeur participent également à la réduction du trafic et au fonctionnement efficace du réseau. Il s'agit des services de gestion de noms, de proxy, et de cache local d'informations de réseau.

Les applications de réseau et les services de connexion exploités sur des réseaux segmentés requièrent l'emploi de méthodes rationnelles pour résoudre les noms en adresses. Divers services concourent à cela. N'importe quel routeur doit pouvoir gérer les services de noms implémentés pour divers environnements de systèmes terminaux. Parmi les services de noms supportés, on trouve NetBIOS, DNS (*Domain Name System*), IEN-116 pour IP et NBP (*Name Binding Protocol*) d'AppleTalk.

Un routeur peut également fournir des services de *proxy* pour un serveur de noms. La gestion par le routeur d'un cache de noms NetBIOS en est un exemple. Il n'a ainsi pas besoin de transmettre toutes les requêtes broadcast entre les ordinateurs NetBIOS client ou serveur (IBM PC ou PS/2) dans un environnement SRB. Lorsqu'un tel cache est activé, le routeur procède de la façon suivante :

- Il détecte un hôte qui envoie une série de trames de requête dupliquées et limite la retransmission à une trame par période ; un intervalle de temps est défini au préalable.
- Il conserve en cache une table de correspondances entre les noms de serveurs et de clients NetBIOS et leurs adresses MAC. Grâce à ce mécanisme, les requêtes broadcast envoyées par les clients afin de rechercher des serveurs peuvent être directement dirigées vers leurs destinataires au lieu d'être diffusées en mode broadcast sur l'ensemble du réseau ponté.

Lorsque la gestion de noms NetBIOS en cache est activée et que les paramètres par défaut sont définis sur le routeur, sur les serveurs de noms NetBIOS, et sur les clients NetBIOS, environ vingt paquets broadcast par ouverture de session sont conservés sur l'anneau local où ils ont été générés.

Dans la plupart des cas, l'utilisation du cache est optimale lorsqu'une grande quantité du trafic broadcast généré par les requêtes NetBIOS provoque des goulets d'étranglement sur un WAN qui relie des réseaux locaux à des environnements distants.

Les routeurs peuvent également permettre une économie de bande passante (ou gérer des protocoles de résolution de noms non compatibles) au moyen d'un éventail d'autres services de proxy. En les utilisant comme agents exécutant des services pour le compte d'autres équipements, vous pourrez plus facilement adapter votre réseau. Au lieu de se trouver dans l'obligation d'ajouter de la bande passante lorsqu'un nouveau groupe de travail est ajouté dans un environnement, il est possible d'utiliser un routeur afin de gérer la résolution d'adresse et contrôler les services de messages. Parmi les exemples de ce type d'exploitation, on trouve la fonction d'exploration de proxy de SRB et la fonction de sondage de proxy dans les implémentations de STUN.

Parfois, des portions de réseau ne peuvent pas participer à l'activité de routage ou n'implémentent pas des logiciels conformes aux protocoles généralement installés pour la résolution d'adresse. Les implémentations de proxy sur les routeurs permettent alors aux concepteurs de réseaux de supporter ces réseaux ou hôtes sans avoir à reconfigurer un réseau. Par exemple, les fonctionnalités de proxy gèrent la résolution d'adresse ARP sur les réseaux IP ou NBP sur les réseaux AppleTalk.

Les caches locaux servent à mémoriser des informations recueillies sur le réseau afin d'éviter que de nouvelles requêtes aient besoin d'être transmises chaque fois que les mêmes éléments d'informations sont demandés. Un cache ARP de routeur stocke les correspondances entre adresses physiques et adresses de réseaux, empêchant qu'une requête ARP ne soit envoyée plusieurs fois en mode broadcast pour une même adresse, dans une période donnée. Des caches d'adresses sont également mis en œuvre pour d'autres protocoles, tels DECnet, Novell IPX et SRB, où les informations du champ RIF sont conservées.

Sécurité de l'accès au média

Si toutes les informations d'une entreprise sont disponibles pour tous les employés, des violations de sécurité et des accès indésirables aux ressources de fichiers peuvent se produire. Pour empêcher cela, les routeurs doivent :

- éviter que le trafic local n'atteigne de façon inappropriée l'épine dorsale ;
- empêcher que le trafic sur l'épine dorsale pénètre de façon inappropriée sur un segment de réseau de département ou de groupe de travail.

Ces deux fonctions nécessitent la mise en place d'un filtrage de paquets. Les services de filtrage doivent être personnalisés afin de s'adapter à différentes stratégies d'entreprise. Les méthodes mises en œuvre à cet effet peuvent réduire le trafic sur un réseau et permettre à une entreprise de poursuivre l'exploitation d'une technologie en place plutôt que d'avoir à investir dans davantage de matériels de réseau. De plus, le filtrage améliore la sécurité en empêchant les utilisateurs non autorisés d'accéder aux informations, mais réduit aussi les problèmes de communication provoqués par une congestion excessive.

Les routeurs acceptent de nombreuses stratégies de filtrage différentes pour assurer un contrôle sur le trafic qui pénètre sur une épine dorsale. Le plus puissant de ces mécanismes est sans doute la liste d'accès. Elle permet de mettre en œuvre les services d'accès local suivants :

- Vous exploitez un réseau avec routage Ethernet vers l'Internet et souhaitez que tout hôte sur le réseau Ethernet soit capable d'établir une connexion TCP avec n'importe quel hôte sur l'Internet. Toutefois, vous ne voulez pas que l'inverse soit possible, sauf au niveau du port SMTP sur un serveur de courrier dédié.
- Vous souhaitez émettre des annonces pour un seul réseau, par l'intermédiaire d'un processus de routage RIP.
- Vous voulez empêcher des paquets émis par une station de travail Sun de traverser un pont sur un segment Ethernet particulier.
- Vous voulez interdire à un protocole donné fondé sur Novell IPX d'établir une connexion entre un réseau source (ou une combinaison de ports source) et un réseau de destination (ou une combinaison de ports de destination).

La liste d'accès empêche logiquement certains paquets de traverser une interface de routeur particulière, et fournit ainsi un outil général qui permet de mettre en place une sécurité de réseau. Outre cette méthode, il existe également de nombreux autres systèmes de sécurité. Par exemple, le gouvernement américain a préconisé l'emploi d'un champ optionnel dans l'en-tête de paquets IP afin d'implémenter un système de sécurité de paquets hiérarchiques, désigné par IPSO (*Internet Protocol Security Option*).

Le support d'IPSO au niveau des routeurs inclut les deux options de sécurité (de base et étendue) décrites dans un projet d'étude sur ce système, communiqué par les bureaux de la DCA (*Defense Communications Agency*). Ce document est une première version du RFC 1108 (*Request for Comments*). L'IPSO définit des niveaux de sécurité tels TOP SECRET, SECRET, etc. pour une interface, et accepte ou rejette les messages selon qu'ils contiennent ou non l'autorisation adéquate.

Certains systèmes de sécurité sont conçus afin d'empêcher les utilisateurs distants d'accéder au réseau, à moins de disposer d'une autorisation appropriée. Par exemple, le système TACACS

(*Terminal Access Controller Access Control System*) est un moyen de protéger les accès par modem sur un réseau. Le DDN (*Defense Data Network*) américain a développé ce système afin de contrôler l'accès à ses serveurs de terminaux TAC.

Le support de TACACS sur un routeur suit un modèle d'application présenté par le DDN. Lorsqu'un utilisateur tente de démarrer un interpréteur de commandes EXEC sur une ligne de commande protégée par mot de passe, ce dernier est requis. En cas de non-conformité du mot de passe, l'accès est refusé. Les administrateurs de routeurs peuvent contrôler divers paramètres du système TACACS, tels que le nombre de tentatives autorisées, le délai d'expiration et l'activation de la comptabilité TACACS.

Le protocole CHAP (*Challenge Handshake Authentication Protocol*) est un autre moyen de contrôler l'accès à un réseau. Il est également couramment utilisé pour les communications entre deux routeurs. Lorsqu'il est activé, un équipement distant (un PC, une station de travail, un routeur ou un serveur de communication) qui tente de se connecter à un routeur local est "mis au défi" de fournir une réponse appropriée. En cas d'échec, l'accès est refusé.

CHAP devient populaire, car il ne recourt pas à l'envoi d'un mot de passe sur le réseau. Il est supporté sur toutes les lignes série de routeurs qui exploitent l'encapsulation PPP (*Point-to-Point Protocol*).

Découverte de routeurs

Les hôtes doivent être en mesure de localiser des routeurs lorsqu'ils ont besoin d'accéder à des équipements extérieurs au réseau local. Lorsque plusieurs routeurs sont connectés au segment local d'un hôte, ce dernier doit déduire quel routeur représente le point d'accès au chemin optimal vers une destination donnée. Ce processus est appelé *découverte de routeurs*.

Voici les protocoles de découverte de routeurs :

- **ES-IS (*End System-to-Intermediate System*)**. Ce protocole a été défini dans la suite de protocoles OSI de l'ISO. Il est dédié à l'échange d'informations entre des systèmes intermédiaires (routeurs) et des systèmes terminaux (hôtes). Les systèmes terminaux envoient des messages "ES hello" à tous les systèmes intermédiaires situés sur le segment local. En réponse, ces derniers renvoient des messages "IS hello" à tous les systèmes terminaux situés sur le sous-réseau local. Les deux types de messages véhiculent les adresses de sous-réseau et de couche réseau des systèmes qui les ont générés. Grâce à ce protocole, ces systèmes peuvent se localiser mutuellement.
- **IRDP (*ICMP Router Discovery Protocol*)**. Il n'existe actuellement aucune méthode standard qui permette aux stations terminales de localiser les routeurs dans l'environnement IP. Le problème est à l'étude. Dans de nombreuses situations, les stations sont simplement configurées manuellement avec l'adresse d'un routeur local. Toutefois, le RFC 1256 mentionne un protocole de découverte de routeur qui utilise ICMP (*Internet Control Message Protocol*) : IRDP.
- **Proxy ARP (*Proxy Address Resolution Protocol*)**. Ce protocole utilise les messages broadcast pour déterminer l'adresse de la couche MAC qui correspond à une adresse de réseau donnée. Il est suffisamment générique pour permettre l'emploi d'IP avec la quasi totalité des types de mécanismes d'accès au média sous-jacent. Un routeur sur lequel Proxy ARP est activé répond

aux requêtes d'adresse concernant les hôtes dont il connaît l'itinéraire, ce qui permet aux émetteurs des requêtes de supposer que les autres hôtes se trouvent en fait sur le même réseau.

- **RIP (Routing Internet Protocol).** Ce protocole est généralement disponible sur les hôtes IP. De nombreux utilisateurs s'en servent afin de rechercher une adresse de routeur sur un LAN ou, lorsqu'il y a plusieurs routeurs, afin de déterminer celui qui est le plus approprié pour une adresse de réseau donnée.

Les routeurs Cisco gèrent tous les protocoles de découverte de routeur listés. Vous pouvez ainsi choisir le mécanisme qui convient le mieux à votre environnement.

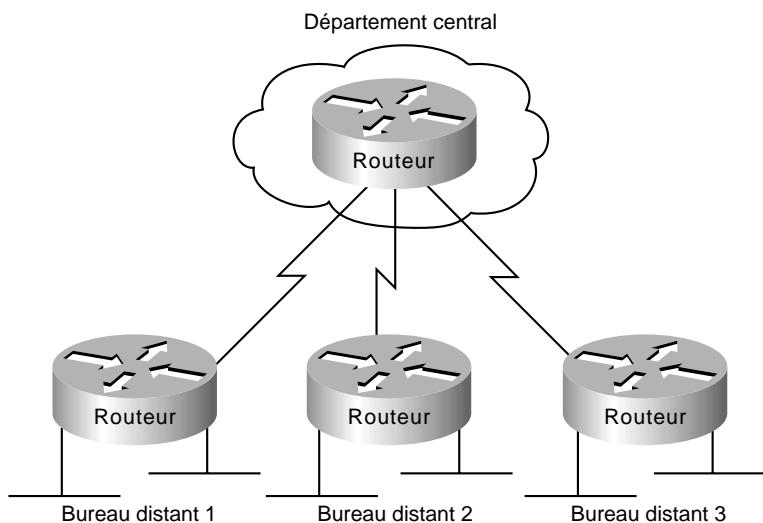
Choix des options de fiabilité de réseau

L'une des principales préoccupations de la plupart des concepteurs de réseaux est de déterminer le niveau de disponibilité requis des applications. En général, la disponibilité est mise en opposition avec le coût d'implémentation qu'elle induit. Pour la plupart des organisations, le coût de la transformation d'un réseau pour atteindre une totale tolérance aux pannes est prohibitif. Définir le niveau de résistance souhaité et le niveau auquel la redondance doit être assurée n'est pas une tâche à prendre à la légère.

La Figure 2.18 montre une conception de réseau non redondant qui illustre les points à considérer afin d'améliorer le niveau de résistance d'un réseau.

Ce réseau présente deux niveaux hiérarchiques : un département central et des bureaux distants. Supposons que le département central possède huit segments Ethernet auxquels sont connectés environ quatre cents utilisateurs (une moyenne de cinquante par segment). Chaque segment est connecté à un routeur. Dans les bureaux distants, deux segments Ethernet sont connectés au département central par l'intermédiaire d'un routeur. Chaque routeur des bureaux distants est relié au routeur du département central par une liaison T1.

Figure 2.18
Conception type d'un réseau
non redondant.



Les quatre sections suivantes traitent des différentes approches qui permettent de créer des réseaux redondants, et décrivent, pour chaque cas, un certain contexte qui permet de souligner leurs différents avantages et inconvénients :

- liens redondants versus topologies maillées ;
- systèmes d'alimentation redondants ;
- implémentations d'un média avec tolérance aux pannes ;
- matériel de secours.

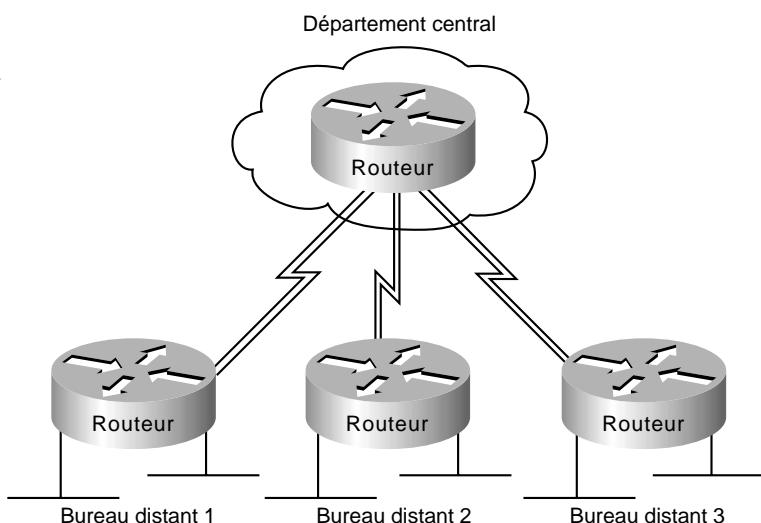
Liens redondants versus topologies maillées

En général, les liaisons WAN sont les composantes les moins fiables d'un réseau, en raison des problèmes que pose la boucle locale. Outre ce défaut, elles représentent aussi un facteur de ralentissement par rapport aux réseaux locaux qu'elles interconnectent. Toutefois, comme elles peuvent relier des sites géographiquement distants, elles forment souvent le réseau fédérateur, et sont par conséquent vitales pour une entreprise. La combinaison de ces facteurs de fiabilité médiocre, de manque de rapidité et de haute importance fait de la liaison WAN un bon candidat à la redondance.

Dans la première étape de renforcement de ce réseau face aux pannes, une liaison WAN est ajoutée entre chaque bureau distant et le département central, ce qui donne la topologie illustrée à la Figure 2.19. Cette nouvelle structure a plusieurs avantages. Tout d'abord, elle fournit un lien de secours qui peut être utilisé si un lien principal entre n'importe quel bureau distant et le département central est défaillant. Ensuite, si les routeurs gèrent l'équilibrage de la charge, la bande passante se trouve augmentée, ce qui réduit les temps de réponse pour les utilisateurs et augmente la fiabilité des applications.

Figure 2.19

Un réseau doté de liaisons doubles entre les sites distants et le site central.



L'équilibrage de la charge dans les environnements qui exploitent un système de pont transparent et IGRP constitue également un autre outil qui permet d'augmenter la résistance aux pannes. Les routeurs supportent également l'équilibrage de charge par paquets ou par destinations, dans tous les environnements IP. La répartition de la charge par paquets est recommandée si les liaisons WAN sont relativement lentes (inférieures à 56 Kbit/s, par exemple). Au-delà de ce débit, il est recommandé d'activer la commutation rapide sur les routeurs. Lorsque cette forme de commutation est possible, l'équilibrage de la charge est réalisé par destinations.

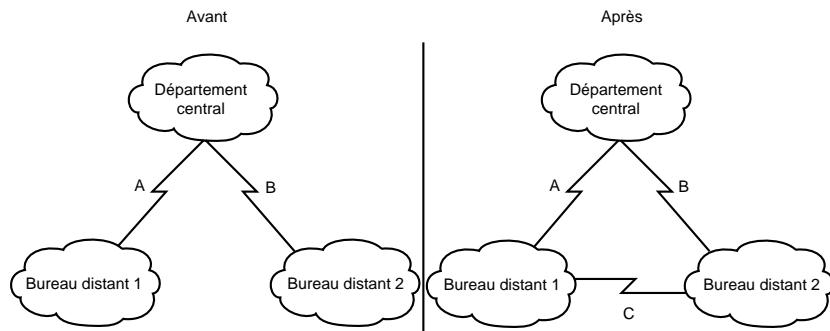
Les routeurs peuvent automatiquement pallier le dysfonctionnement d'une liaison WAN au moyen d'algorithmes de routage de protocoles, tels que IGRP, EIGRP, OSPF et IS-IS. Si un lien n'est plus utilisable, l'application de routage recalcule les itinéraires et achemine tout le trafic par l'intermédiaire d'un autre circuit. Cela permet d'augmenter la disponibilité des applications qui peuvent ainsi continuer à fonctionner, même en cas de rupture sur un réseau étendu.

Le principal inconvénient de la duplication de liaisons WAN vers chaque bureau distant est le coût. Dans l'exemple de la Figure 2.19, trois nouveaux liens ont été nécessaires. Sur de grands réseaux structurés en étoile, avec plusieurs sites distants, dix voire vingt nouvelles liaisons pourraient se révéler nécessaires, ainsi que de nouveaux équipements (y compris de nouvelles interfaces de routeur WAN). Une solution moins coûteuse, qui devient de plus en plus populaire, consiste à relier des sites distants au moyen d'une topologie maillée (voir Figure 2.20).

Dans la partie "Avant" de la Figure 2.20, toute panne associée à l'un des liens A ou B bloque les échanges entre le département central et le site distant concerné. La panne pourrait impliquer le matériel de connexion de la liaison — une unité de services de données (DSU, *Data Service Unit*) ou une unité de services de canal (CSU, *Channel Service Unit*), par exemple —, le routeur (dans sa totalité, ou uniquement un port) ou la liaison elle-même. L'ajout de la liaison C dans la partie "Après" de la figure permet de remédier à toute panne de l'un des liens principaux. Le site concerné pourra toujours accéder au département central par l'intermédiaire du nouveau lien et de celui de l'autre bureau distant. Notez que, si une rupture a lieu sur le nouveau lien, la communication entre les deux sites distants et le département central se poursuit normalement, avec leurs liaisons respectives vers ce dernier.

Figure 2.20

Evolution d'une topologie en étoile vers une topologie maillée.



Une topologie maillée possède trois avantages distincts par rapport à une topologie en étoile redondante :

- Elle est généralement un peu moins coûteuse (puisque elle compte au minimum une liaison WAN de moins).
- Elle fournit une communication plus directe (et éventuellement plus rapide) entre des sites distants, ce qui se traduit par une plus grande disponibilité des applications. Cette solution peut être utile si de forts volumes de trafic sont transmis directement entre deux sites distants.
- Elle favorise une exploitation distribuée, prévient les goulets d'étranglement au niveau du routeur du département central et augmente la disponibilité des applications.

Une topologie en étoile redondante convient dans les situations suivantes :

- Le volume de trafic qui circule entre les sites distants est relativement faible.
- Le trafic qui transite entre le site central et les bureaux distants est constitué de données critiques, sensibles au délai de livraison. Le délai et les problèmes éventuels de fiabilité qui résulteraient du passage par un saut supplémentaire en cas de liaison défective entre un site distant et le site central pourraient ne pas être acceptables.

Systèmes d'alimentation redondants

Les coupures d'alimentation sont courantes sur les réseaux étendus. Elles peuvent se produire à un niveau local ou étendu, il est donc difficile de s'en protéger. Les cas d'interruption de courant simples sont provoqués par un cordon d'alimentation déplacé ou débranché, un disjoncteur activé, ou une panne au niveau du fournisseur. Les cas plus complexes peuvent être provoqués par une surtension ou des phénomènes naturels, tel la foudre. Chaque organisation doit évaluer la probabilité de chaque type de panne avant de déterminer les actions préventives à entreprendre par rapport à ses besoins.

De nombreuses précautions peuvent être prises pour éviter que certains problèmes (le débranchement de cordons par exemple) se produisent trop souvent. Ce sujet dépasse le cadre de cet ouvrage et ne sera pas abordé. Ce chapitre se consacre aux difficultés qui peuvent être résolues par des équipements de réseau.

Sur le plan des équipements de réseau, les systèmes d'alimentation double peuvent jouer un rôle préventif en cas de ruptures qui risqueraient d'être préjudiciables. Prenons le cas d'un réseau fédérateur centralisé (*collapsed backbone*). Cette configuration implique la connexion de plusieurs réseaux à un routeur faisant également office de *hub central d'entreprise*. Les avantages qui en découlent sont une épine dorsale à haut débit (en fait, la plaque principale de connexion du routeur) et une rentabilité accrue (moins de médias). Malheureusement, si le système d'alimentation du routeur fait l'objet d'une panne, aucun des réseaux qui y sont connectés ne peut plus communiquer avec les autres.

Dans cette position de réseau fédérateur centralisé, certains routeurs peuvent faire face à ce problème grâce à la redondance du système d'alimentation. De plus, de nombreux sites raccordent un système d'alimentation à l'armoire électrique locale et un autre à un onduleur. En cas de panne, le routeur peut ainsi assurer la communication entre les réseaux connectés.

Les coupures d'alimentation générale sont plus courantes que les pannes de systèmes d'alimentation de routeur. Imaginez l'impact d'une panne de courant sur l'ensemble d'un site doté d'une topologie

en étoile redondante ou maillée. Si le site central d'une entreprise est victime d'une rupture de courant, la topologie peut être sérieusement touchée, d'autant que les applications de réseau essentielles sont souvent centralisées à ce niveau. L'entreprise pourrait subir des pertes financières pour chaque minute d'immobilisation du réseau. Dans une telle situation, une configuration maillée se révélerait plus adaptée, car les liaisons entre sites distants seraient toujours disponibles, permettant la communication.

Si une panne d'alimentation survient sur un site distant, toutes les connexions établies avec ce site seront interrompues, à moins qu'elles soient protégées d'une manière ou d'une autre. Dans ce cas, ni une topologie en étoile redondante, ni une structure maillée ne pourraient se prévaloir d'une quelconque supériorité. Dans les deux cas, tous les autres bureaux distants pourront continuer à communiquer avec le site central. Généralement, les pannes d'alimentation sur un site distant sont plus sérieuses lorsque les services de réseau sont largement distribués.

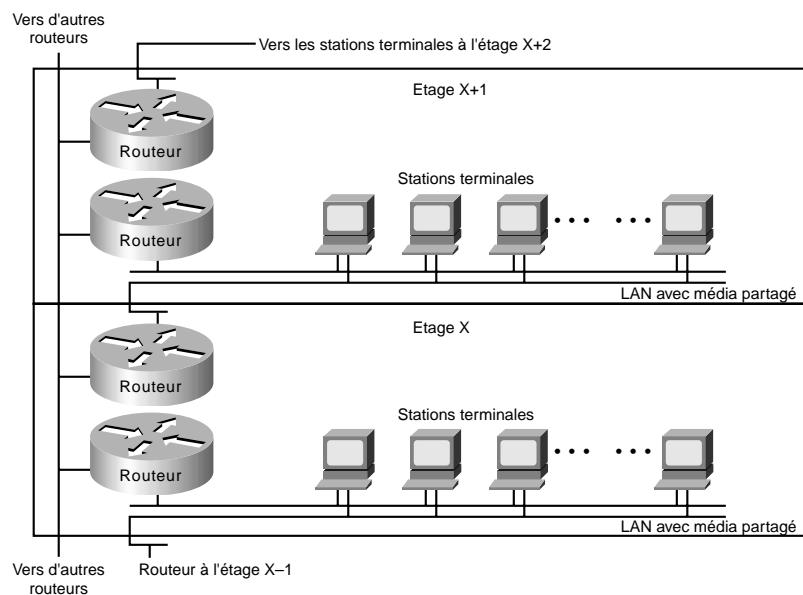
Pour se protéger des coupures de courant au niveau local ou sur l'ensemble d'un site, certaines entreprises négocient des dispositions spéciales avec les compagnies d'électricité, afin de pouvoir utiliser plusieurs armoires électriques au sein de leur organisation. Une rupture au niveau d'une armoire électrique n'affectera pas le réseau si tous les composants essentiels sont reliés à plusieurs armoires. Malheureusement, ce genre d'arrangement se révèle très coûteux et ne devrait être envisagé que dans le cas où l'entreprise dispose d'importantes ressources informatiques, est engagée dans des opérations extrêmement critiques, et est exposée à un risque relativement élevé en cas de panne de courant.

L'impact des coupures de courant très localisées peut être limité si l'on est assez prudent lors de la planification du réseau. Lorsque cela est possible, les composants redondants devraient être alimentés par des circuits différents et ne devraient pas partager un même emplacement physique. Par exemple, si des routeurs redondants sont employés pour toutes les stations d'un étage donné dans un immeuble d'entreprise, ils peuvent être physiquement raccordés à des armoires de câblage situées à des étages différents. Cela évitera que des problèmes d'alimentation au niveau d'une armoire de câblage n'empêchent la communication entre toutes les stations d'un même étage. La Figure 2.21 illustre une telle configuration.

Pour certaines entreprises, le besoin de se protéger d'une éventuelle panne de courant est tellement vital qu'elles recourent à la mise en œuvre d'un centre de données d'entreprise dupliqué. Les organisations qui ont de telles exigences créent souvent un centre redondant dans une autre ville ou à une certaine distance du centre principal dans la même ville, afin de se prémunir contre une panne de secteur. Tous les services de soutien sont dupliqués, et les transactions en provenance de sites distants sont envoyées vers les deux centres de données. Une telle configuration nécessite des liaisons WAN dupliquées à partir de tous les bureaux distants, des équipements de réseau dupliqués, des serveurs et des ressources de serveurs dupliqués, et la location d'un autre immeuble. Une telle approche se révèle si onéreuse que les entreprises désireuses d'implémenter un système de tolérance sans faille y font appel en dernier recours.

La duplication partielle d'un centre de traitement des données est également une solution envisageable. On peut dupliquer plusieurs serveurs et liaisons indispensables qui y sont raccordés. Il s'agit là d'un compromis que les entreprises acceptent couramment pour faire face à ces problèmes.

Figure 2.21
Composants redondants sur différents étages.



Implémentation d'un média avec tolérance aux pannes

La défaillance d'un média est l'un des problèmes qui peut se produire sur un réseau. On trouve dans cette catégorie de dysfonctionnements les problèmes liés au média et aux composants qui interviennent dans son raccordement à chaque station terminale. Ils peuvent être provoqués par des contrôleurs de cartes, des cordons AUI (*Attachment Unit Interface*) de raccordement, ou cordons de descente, des transceivers, des hubs, ou encore le câble lui-même, des terminateurs ou d'autres éléments. De nombreuses pannes de média sont dues à une négligence de l'opérateur ; elles sont difficiles à résoudre.

Une façon de réduire les désagréments causés par le dysfonctionnement du média est de le diviser en segments plus petits et d'utiliser un équipement différent pour chacun d'eux. Cela permet de limiter l'impact d'une panne à un segment particulier. Par exemple, si vous disposez de cent stations connectées à un seul commutateur, raccordez certaines d'entre elles à d'autres commutateurs. Les effets seront ainsi limités en cas de défaillance d'un hub ou de certaines défaillances de sous-réseau. En utilisant un équipement de réseau (un routeur, par exemple) pour séparer les segments, vous vous protégez contre d'éventuels problèmes supplémentaires et réduisez le trafic transitant sur le sous-réseau.

Comme illustré à la Figure 2.21, la redondance peut être exploitée pour réduire les risques de panne de média. Chaque station de cette figure est reliée à deux segments de média différents. Les cartes, les ports de hub et les câbles d'interface sont tous redondants. Cette mesure double le coût de la connectivité pour chaque station terminale, ainsi que le niveau d'utilisation des ports sur tous les équipements de réseau. Par conséquent, elle est recommandée uniquement dans les situations où une redondance totale est requise. Elle suppose également que les logiciels de stations terminales,

incluant ceux de réseau et d'applications, puissent gérer et utiliser de façon efficace les composants dupliqués pour être en mesure de détecter les défaillances au niveau d'un réseau et d'initier une convergence vers le réseau de secours.

Certains protocoles d'accès au média sont dotés de fonctionnalités intégrées de tolérance aux pannes. Les concentrateurs de câblage pour les réseaux Token Ring, appelés MAU (*Multistation Access Unit*), peuvent détecter certaines défaillances de connexion du média et les contourner en interne. L'anneau double FDDI (contrarotatif) permet de contourner une portion du réseau qui pose problème, en faisant transiter le trafic sur le second anneau.

Sur le plan du routage, de nombreuses défaillances du média peuvent être contournées sous réserve que des chemins alternatifs existent et soient disponibles. Diverses techniques de détection de défaillances matérielles permettent aux routeurs de révéler certains problèmes de média. Si les mises à jour de routage ou les messages d'activité (*keepalive messages*) n'ont pas été reçus de la part d'équipements normalement accessibles par l'intermédiaire d'un port de routeur donné, le routeur déclare le chemin impraticable et recherche des itinéraires de remplacement. Les réseaux maillés fournissent des routes alternatives, ce qui permet aux routeurs de compenser les défaillances du média.

Matériel de secours

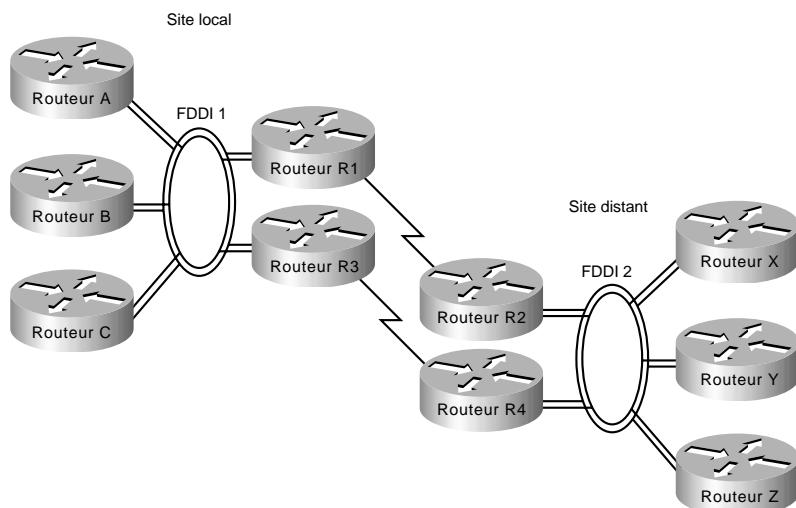
A l'instar de tous les dispositifs complexes, les routeurs, commutateurs et autres équipements de réseau peuvent souffrir de problèmes matériels. Lorsque de sérieuses défaillances se produisent, l'utilisation d'équipements en double peut réduire de façon efficace les effets négatifs. En cas de panne, des protocoles de découverte de chemin peuvent aider les stations terminales à localiser de nouveaux itinéraires, au moyen desquels elles pourront communiquer sur le réseau. Si chaque réseau connecté à l'équipement défaillant possède un chemin alternatif pour sortir de la zone locale, l'intégralité de la connectivité est préservée.

Par exemple, lorsque des routeurs de secours sont mis en œuvre, des métriques de routage peuvent être définies de façon à garantir qu'ils ne pourront pas être utilisés si les routeurs principaux fonctionnent. En cas de problème, la convergence est automatique et rapide. Considérons la situation illustrée à la Figure 2.22. Sur ce réseau, des routeurs dupliqués sont utilisés sur tous les sites dotés de liaisons WAN en double. Si le routeur R1 subit une panne, les routeurs sur FDDI 1 la détecteront en raison de l'absence de messages en provenance du routeur défaillant. Au moyen de n'importe lequel des nombreux protocoles de routage dynamiques, les routeurs A, B et C désigneront le routeur R3 comme le prochain saut sur l'itinéraire menant aux ressources distantes accessibles *via* le routeur R4.

Afin d'assurer une certaine redondance, de nombreux réseaux sont dotés de plusieurs routeurs qui interconnectent des LAN particuliers. Par le passé, l'efficacité de ce type de conception était limitée, en raison de la vitesse à laquelle les hôtes sur ces réseaux locaux détectaient une mise à jour de topologie et changeaient de routeur. En particulier, les hôtes IP sont souvent configurés avec une passerelle par défaut ou pour utiliser le protocole Proxy ARP, afin de localiser un routeur sur leur réseau local. Pour qu'un hôte IP change de routeur, il fallait généralement recourir à une intervention manuelle visant à mettre à jour le cache ARP ou à modifier la passerelle par défaut.

Figure 2.22

Configuration FDDI avec routeurs redondants.



Le protocole HSRP (*Hot Standby Router Protocol*) est une solution qui rend les changements de topologie de réseau transparents pour les hôtes. Ce protocole autorise les hôtes à changer de route en dix secondes environ. Il est supporté sur Ethernet, Token Ring, FDDI, Fast Ethernet et ATM.

Un groupe HSRP peut être défini sur chaque réseau local. Tous les membres du groupe connaissent l'adresse IP et l'adresse MAC de secours. Un membre est élu pour faire office de routeur leader. Il traite tous les paquets envoyés vers l'adresse du groupe HSRP. Les autres routeurs surveillent le routeur leader et agissent en tant que routeurs HSRP. Si le leader devient inutilisable pour une raison quelconque, un nouveau leader est élu et hérite des adresses MAC et IP HSRP.

Les routeurs Cisco haut de gamme (des familles 4500, 7000, et 7500) peuvent supporter plusieurs adresses MAC sur la même interface Ethernet ou FDDI, ce qui leur permet de gérer simultanément le trafic envoyé vers l'adresse MAC de secours et l'adresse MAC privée. Les commandes qui permettent d'activer HSRP et de configurer un groupe HSRP sont : **standby ip** et **standby group**.

Identification et choix des équipements de réseau

Les concepteurs de réseaux disposent de quatre types d'équipements de réseau de base :

- les hubs (concentrateurs) ;
- les ponts ;
- les commutateurs ;
- les routeurs.

Pour obtenir une synthèse de leurs caractéristiques, reportez-vous au Tableau 2.1, présenté plus haut dans ce chapitre. Les experts en communication de données s'accordent pour dire que les concepteurs de réseaux privilient principalement l'utilisation de routeurs et de commutateurs à celle de

ponts pour créer des réseaux. C'est pourquoi cette section se consacre au rôle des commutateurs et des routeurs.

Les commutateurs peuvent, sur le plan fonctionnel, être divisés en deux groupes principaux : les commutateurs de niveau 2 et les commutateurs multicouches, qui offrent des services de commutation des niveaux 2 et 3. Aujourd'hui, les concepteurs ont tendance à remplacer les hubs dans les armoires de câblage par des commutateurs, dans le but d'améliorer les performances de réseau et de préserver les investissements existants au niveau du câblage.

Les routeurs permettent de segmenter le trafic du réseau en se fondant sur l'adresse de destination de la couche réseau (niveau 3) à la place de l'adresse MAC. En conséquence, les routeurs sont dépendants des protocoles.

Avantages des commutateurs (services de niveau 2)

Un commutateur de niveau 2 peut présenter certains des avantages suivants, voire tous :

- **Bande passante.** Les commutateurs de réseaux locaux permettent aux utilisateurs de bénéficier d'excellentes performances, en allouant une bande passante dédiée à chaque port de commutation. Chacun de ces ports représente un segment de réseau différent. Cette technique est connue sous l'appellation *microsegmentation*.
- **VLAN.** Les commutateurs de réseaux locaux peuvent regrouper des ports individuels en groupes de travail logiques commutés, appelés VLAN (*Virtual LAN*), qui permettent de réduire le domaine de broadcast à certains ports membres du réseau virtuel. Ces réseaux virtuels sont également connus sous l'appellation *domaines commutés* ou *domaines de commutation autonomes*. La communication entre deux réseaux virtuels nécessite l'emploi d'un routeur.
- **Reconnaissance et traduction automatiques de paquets.** Cette fonctionnalité permet aux commutateurs de traduire automatiquement le format des trames, tel que MAC Ethernet vers SNAP FDDI.

Avantages des routeurs (services de niveau 3)

Puisque les routeurs utilisent les adresses de niveau 3, qui respectent généralement une certaine structure, ils peuvent utiliser des techniques (telles que la synthèse d'adressage) pour construire des réseaux pouvant maintenir un certain niveau de performances et de réactions, au fur et à mesure qu'ils se développent. Imposant une structure (généralement hiérarchique) sur un réseau, les routeurs peuvent utiliser efficacement des chemins redondants et choisir les routes optimales, même dans un environnement changeant dynamiquement.

Les routeurs sont nécessaires pour garantir l'évolutivité du réseau, au fur et à mesure qu'il s'étend. Ils assurent les services suivants, qui sont essentiels pour la conception de réseaux :

- contrôle de la diffusion broadcast et multicast ;
- segmentation de domaines de broadcast ;
- sécurité ;
- qualité de service (QoS) ;
- multimédia.

Options de routage du réseau fédérateur

Dans un monde idéal, un réseau d'entreprise parfait implémenterait un seul protocole de réseau robuste et capable de transporter tous types de données facilement, sans erreur, et avec suffisamment de souplesse pour pouvoir s'adapter à toute interruption de connectivité imprévue. Toutefois, il existe dans le monde réel de nombreux protocoles qui présentent divers niveaux de souplesse de réaction.

Afin de concevoir un réseau fédérateur pour votre entreprise, vous devez considérer plusieurs options. Elles sont généralement réparties dans les deux principales catégories suivantes :

- épine dorsale avec routage multiprotocole ;
- épine dorsale monoprotocole.

Les sections suivantes présentent les caractéristiques et les propriétés propres à ces deux orientations.

Epine dorsale avec routage multiprotocole

Un environnement dans lequel plusieurs protocoles de couche réseau sont routés à travers une épine dorsale commune sans encapsulation est appelé *épine dorsale à routage multiprotocole* (ou routage en mode *natif*). Un tel environnement peut adopter l'une des deux stratégies de routage suivantes, ou les deux à la fois, selon le protocole routé impliqué :

- **Routage intégré.** Le routage intégré implique l'emploi d'un seul protocole de routage (par exemple, par état de lien) qui détermine le chemin de plus faible coût pour différents protocoles routés.
- **Routage séparé.** Cette approche implique l'utilisation d'un protocole de routage différent pour chaque protocole de réseau routé. Par exemple, sur certains réseaux étendus composés de plusieurs protocoles, le trafic Novell IPX est routé au moyen d'une version propriétaire du protocole RIP, IP est routé au moyen de IGRP, et le trafic de DECnet Phase V est routé via le protocole IS-IS compatible ISO CLNS.

Ces protocoles de couche réseau sont routés indépendamment les uns des autres, avec des processus de routage distincts, qui gèrent leurs trafics respectifs et des chemins calculés séparés. Combiner des routeurs au sein d'un réseau qui supporte différentes associations de plusieurs protocoles peut conduire à une situation confuse, plus particulièrement dans le cas du routage intégré. En général, ce type de routage est plus facile à gérer si tous les routeurs raccordés au réseau fédérateur qui assure le routage intégré acceptent le même plan de routage. Pour des protocoles différents, les routes peuvent être calculées séparément. Une autre solution consiste à utiliser l'encapsulation pour acheminer un trafic via des routeurs qui ne supportent pas un protocole particulier.

Epine dorsale monoprotocole

Avec un réseau fédérateur à protocole unique, tous les routeurs sont supposés gérer le même protocole de routage pour un seul protocole de réseau. Dans ce type d'environnement, tous les autres protocoles de routage sont ignorés. Si plusieurs protocoles doivent être transportés sur le réseau, ceux qui ne sont pas acceptés doivent être encapsulés à l'intérieur du protocole géré, sous peine d'être ignorés par les nœuds de routage.

Peut-être vous demandez-vous pourquoi implémenter une épine dorsale monoprotocole ? Le choix de se limiter à un réseau fédérateur à protocole unique convient lorsqu'un nombre relativement faible de protocoles différents doit être géré, sur un nombre réduit de réseaux isolés. Toutefois, l'encapsulation ajoutera une surcharge de trafic. En revanche, si plusieurs protocoles sont largement utilisés sur l'ensemble du réseau, un réseau fédérateur multiprotocole donnera vraisemblablement les meilleurs résultats.

En général, vous devriez gérer tous les protocoles de couche réseau au sein d'un réseau adoptant un routage natif et en implémenter un nombre aussi faible que possible.

Types de commutateurs

Les commutateurs peuvent être classés de la façon suivante :

- **Commutateurs LAN.** Les commutateurs de cette catégorie peuvent encore être classés dans deux sous-catégories, à savoir les commutateurs de niveau 2 et les commutateurs multicouches.
- **Commutateurs ATM.** La commutation ATM et les routeurs ATM fournissent une bande passante de réseau fédérateur plus importante, afin de satisfaire aux exigences des services de données à haut débit.

Les administrateurs de réseau ajoutent des commutateurs LAN dans leurs armoires de câblage, afin d'augmenter la bande passante et de réduire la congestion au niveau des hubs de média partagé existants, tout en exploitant de nouvelles technologies au niveau de l'épine dorsale, telles que Fast Ethernet et ATM.

Commutateurs LAN

Les commutateurs LAN, hautement performants et rentables, procurent aujourd'hui aux administrateurs de réseau les avantages suivants :

- une meilleure microsegmentation ;
- une meilleure transmission des agrégats de données ;
- davantage de bande passante sur les réseaux fédérateurs d'entreprise.

Les commutateurs LAN répondent aux besoins des utilisateurs en matière de bande passante. En déployant des commutateurs plutôt que des hubs partagés traditionnels, les concepteurs de réseaux peuvent améliorer les performances et accroître la rentabilité des investissements existants au niveau du média et des cartes LAN. Ces équipements proposent également des fonctionnalités jusqu'alors inexistantes, tels les réseaux locaux virtuels (VLAN), qui apportent une certaine souplesse, car ils permettent d'utiliser des logiciels pour déplacer, ajouter, et modifier des utilisateurs à travers le réseau.

Les commutateurs LAN conviennent également pour fournir un service de commutation de segments et une bande passante évolutive au niveau des centres de traitement de données de réseau, en implantant des liaisons commutées pour interconnecter les hubs existants dans les armoires de câblage, les hubs locaux et les fermes de serveurs. Cisco commercialise une famille de commutateurs multicouches, appelée Catalyst, qui permet de relier plusieurs commutateurs d'armoires de câblage ou hubs partagés dans une configuration de réseau fédérateur.

Commutateurs ATM

Même si tous les commutateurs ATM assurent le relais de trames, ils diffèrent sensiblement par les caractéristiques suivantes :

- variété des interfaces et services supportés ;
- redondance ;
- étendue des applications de réseau ATM ;
- sophistication des mécanismes de gestion de trafic.

De la même façon qu'il existe des routeurs et des commutateurs LAN qui possèdent des caractéristiques diverses en termes de prix, de performances et de niveau de fonctionnalités, les commutateurs ATM peuvent être classés en quatre types distincts, qui reflètent les besoins d'applications et de marchés particuliers :

- commutateurs ATM de groupe de travail ;
- commutateurs ATM de campus ;
- commutateurs ATM d'entreprise ;
- commutateurs d'accès multiservices.

Cisco propose un éventail complet de commutateurs ATM.

Commutateurs ATM de groupe de travail et de campus

Les *commutateurs ATM de groupe de travail* disposent de ports de commutation Ethernet et d'une liaison montante ATM pour se connecter à un commutateur ATM de campus. Un exemple de commutateur ATM de groupe de travail chez Cisco est le Catalyst 5000.

Les *commutateurs ATM de campus* sont généralement utilisés sur les réseaux fédérateurs ATM de faible étendue (par exemple, pour y connecter des routeurs ATM ou des commutateurs LAN). L'exploitation de ce type de commutateurs ATM permet de réduire les congestions sur l'épine dorsale existante et de déployer de nouveaux services, tels que les réseaux virtuels (VLAN). Les commutateurs de campus doivent accepter une large variété de réseaux fédérateurs locaux et de types de WAN, mais être optimisés afin d'offrir un bon rapport prix/performances en ce qui concerne la fonction d'épine dorsale locale. Dans cette catégorie de commutateurs, les fonctionnalités de routage ATM qui permettent à plusieurs commutateurs d'être reliés entre eux sont très importantes. Les mécanismes de contrôle de congestion optimisant les performances du réseau fédérateur jouent également un rôle primordial. La famille de commutateurs ATM LightStream 1010 est un exemple de commutateurs ATM de campus. Pour plus d'informations sur le déploiement de ces deux catégories de commutateurs ATM sur un réseau, reportez-vous au Chapitre 12.

Commutateurs ATM d'entreprise

Les *commutateurs ATM d'entreprise* sont des équipements multiservices sophistiqués conçus pour constituer l'épine dorsale centrale des grands réseaux d'entreprise. Ils ont pour fonction de compléter les services des routeurs multiprotocoles haut de gamme actuels, et sont utilisés pour interconnecter des commutateurs ATM de campus. Ils peuvent non seulement servir d'épines dorsales ATM, mais aussi de points uniques d'intégration pour tous les services et toutes les technologies disparates que

l'on peut rencontrer sur les réseaux fédérateurs d'entreprise à l'heure actuelle. L'intégration de tous ces services au niveau d'une plate-forme et d'une infrastructure de transport ATM communes offre aux concepteurs de réseaux une plus grande aisance pour administrer le réseau et élimine le besoin de superposer de multiples réseaux.

Le BPX/IGX de Cisco est un puissant commutateur ATM à large bande, conçu pour répondre aux exigences de trafic élevé de grandes entreprises privées ou de fournisseurs de services publics. Pour plus d'informations sur le déploiement des commutateurs ATM d'entreprise sur un réseau, reportez-vous au Chapitre 5.

Commutateurs d'accès multiservices

Au-delà des réseaux privés, les plates-formes ATM sont également largement déployées par les fournisseurs de services sous forme d'équipements de télécommunication CPE (*Customer Premises Equipment*) et également sur les réseaux publics. Elles sont exploitées pour gérer plusieurs services de réseaux métropolitains (MAN) et étendus (WAN) — par exemple, la commutation Frame Relay, l'interconnexion de LAN, et les services ATM publics — sur une infrastructure ATM commune. Les commutateurs ATM d'entreprise sont souvent utilisés avec ces applications de réseaux publics en raison de leurs atouts en termes de disponibilité, de redondance, de support d'interfaces multiples, et de capacité à intégrer la voix et les données.

Comparaison entre commutateurs et routeurs

Pour souligner les différences qui existent entre les commutateurs et les routeurs, les sections suivantes examinent les rôles respectifs de ces équipements dans les situations suivantes :

- implémentation de VLAN ;
- implémentation de réseaux commutés.

Rôle des commutateurs et des routeurs sur les VLAN

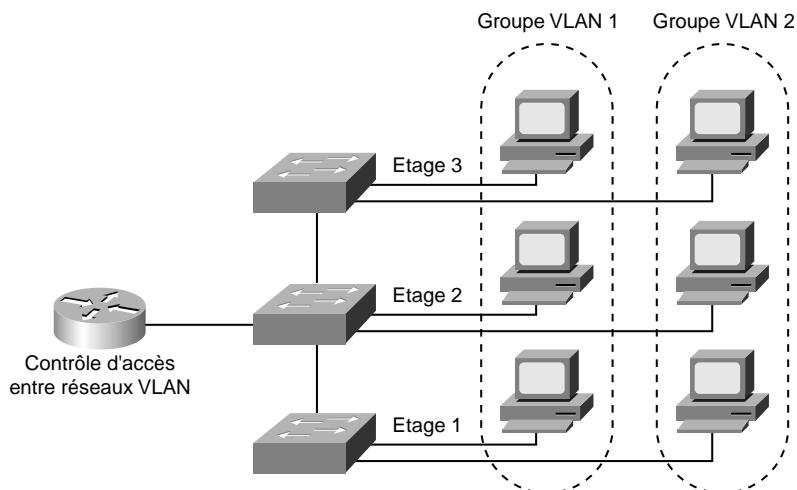
Les VLAN, ou LAN virtuels, apportent une solution aux deux problèmes suivants :

- évolutivité d'une topologie de réseau linéaire ;
- simplification de la gestion de réseau par une plus grande facilité de reconfiguration (déplacements et changements).

Un VLAN consiste en un seul domaine de diffusion. Il résout les problèmes d'évolutivité des grands réseaux linéaires en scindant un seul domaine de broadcast en plusieurs domaines plus petits, ou VLAN. Il facilite la modification de la conception d'un réseau par rapport aux réseaux traditionnels. Les commutateurs LAN peuvent servir à segmenter des réseaux en groupes de travail virtuels logiquement définis. Cette segmentation logique, couramment appelée *communication VLAN*, introduit un changement fondamental dans la conception, l'administration et la gestion des LAN. Bien que la segmentation apporte des avantages substantiels dans l'administration, la sécurité et la gestion des diffusions broadcast sur le réseau d'entreprise, les nombreuses composantes de la solution VLAN doivent être examinées avant de décider de les déployer à grande échelle.

Les commutateurs et les routeurs ont chacun un rôle important dans la conception d'un VLAN. Le commutateur représente le dispositif central qui contrôle les VLAN individuels, alors que le routeur leur permet de communiquer entre eux (voir Figure 2.23).

Figure 2.23
Rôle des commutateurs et des routeurs sur les VLAN.



Les commutateurs éliminent les contraintes physiques associées à une structure avec hubs partagés, car ils relient logiquement les utilisateurs et les ports au niveau de l'entreprise. En tant que dispositifs de remplacement des hubs, ils suppriment les barrières physiques imposées au niveau de chaque armoire de câblage. De plus, le rôle du routeur évolue au-delà des services traditionnels de pare-feu et de suppression des diffusions broadcast, pour offrir un contrôle fondé sur des règles, une gestion du trafic broadcast, ainsi que le traitement et la distribution des routes. Tout aussi important, le routeur conserve une place vitale au sein d'architectures configurées en réseaux VLAN, car il permet à ces derniers de communiquer. Il représente également le point d'accès VLAN aux ressources partagées, tels que serveurs et hôtes. Pour plus d'informations sur le déploiement de réseaux VLAN, reportez-vous au Chapitre 12.

Exemples de conception de réseaux de campus commutés

Un réseau de campus commuté bien implémenté doit combiner les avantages des routeurs et ceux des commutateurs dans chaque partie du réseau, et permettre à un réseau à média partagé d'évoluer aisément vers un grand réseau commuté.

Par exemple, l'incorporation de commutateurs dans un réseau de campus offre habituellement les avantages suivants :

- bande passante élevée ;
- amélioration des performances ;
- faible coût ;
- configuration facile.

Cependant, si vous avez besoin de services de réseau avancés, les routeurs sont nécessaires. Ils fournissent les services suivants :

- protection par pare-feu contre les diffusions broadcast ;
- adressage hiérarchique ;
- communication entre réseaux locaux de types différents ;
- convergence rapide ;
- routage fondé sur des règles ;
- routage avec qualité de service (QoS) ;
- sécurité ;
- redondance et équilibrage de charge ;
- gestion de flux du trafic ;
- gestion d'appartenance à un groupe multimédia.

Certains de ces services de routeur seront assurés à l'avenir par des commutateurs. Par exemple, le support du multimédia nécessite souvent un protocole tel IGMP pour permettre aux stations de travail d'adhérer à un groupe qui reçoit des paquets multimédias multidestinataires. Les commutateurs Cisco peuvent participer à ce processus au moyen du protocole CGMP (*Cisco Group Management Protocol*). Les commutateurs CGMP communiquent avec le routeur pour savoir si l'un de leurs utilisateurs connectés fait ou non partie d'un groupe multicast.

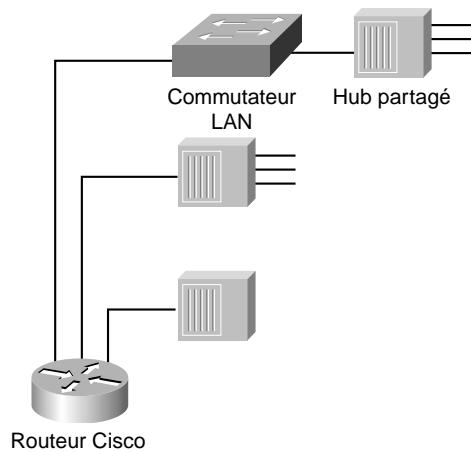
Le traitement assuré par les commutateurs et les ponts peut parfois entraîner un routage non optimal des paquets, car chaque paquet doit passer par le pont racine de l'arbre recouvrant. Lorsque des routeurs sont utilisés, le routage peut être contrôlé et élaboré à travers des chemins optimaux. Cisco fournit maintenant un support pour un routage et une redondance améliorés dans les environnements commutés, grâce à la gestion d'une instance de l'arbre recouvrant par VLAN.

Les Figures 2.24 à 2.27 illustrent la façon dont les concepteurs de réseaux peuvent utiliser les commutateurs et les routeurs afin de faire évoluer leurs réseaux de média partagé en réseaux de commutation. En général, l'évolution vers une architecture de réseau de campus commuté comprend quatre phases :

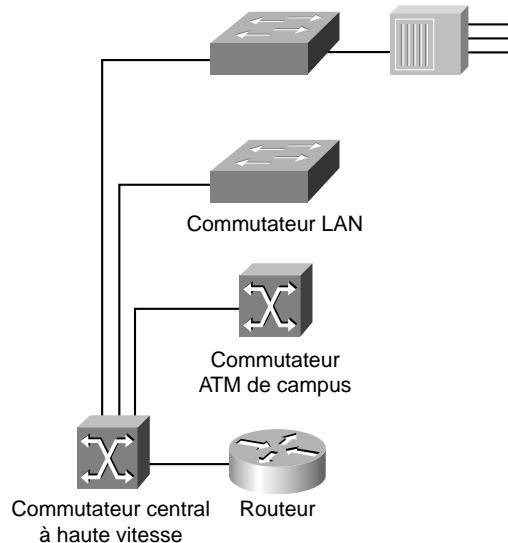
- La phase 1 concerne la microsegmentation, au cours de laquelle les concepteurs de réseaux conservent leurs hubs et routeurs, mais ajoutent un commutateur LAN, afin d'améliorer les performances. La Figure 2.24 fournit un exemple de l'utilisation d'un commutateur LAN pour segmenter un réseau.
- La phase 2 est l'ajout d'une technologie d'épine dorsale à haute vitesse et du routage entre commutateurs. Les commutateurs assurent la commutation et fournissent une bande passante dédiée aux ordinateurs et aux hubs partagés. Les routeurs d'épine dorsale sont connectés à des commutateurs Fast Ethernet ou ATM. L'augmentation de bande passante sur l'épine dorsale correspond à celle de la bande passante au niveau de l'armoire de câblage. La Figure 2.25 illustre de quelle façon vous pouvez implémenter une technologie de réseau fédérateur à haute vitesse, et le routage entre commutateurs existants.

Figure 2.24

L'emploi de commutateurs pour la microsegmentation.

**Figure 2.25**

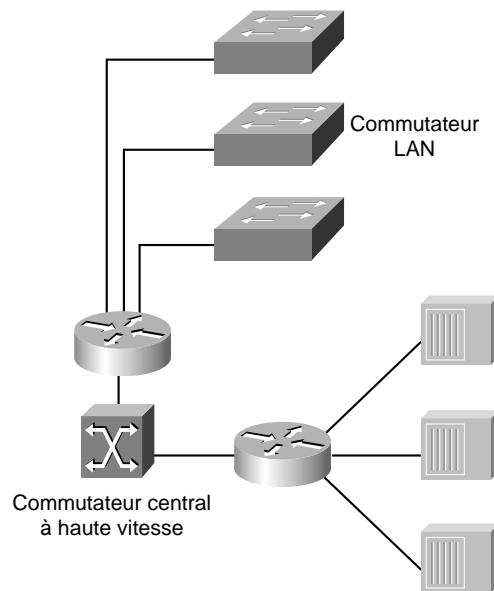
L'ajout d'une technologie d'épine dorsale à haute vitesse et du routage entre les commutateurs.



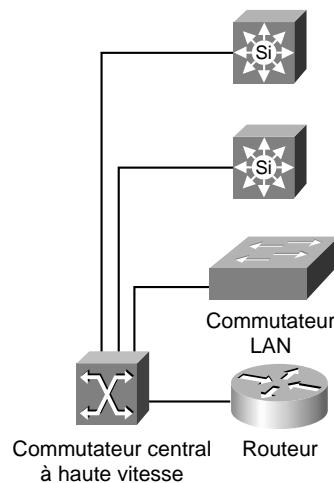
- Dans la phase 3, les routeurs sont distribués entre les commutateurs LAN dans l'armoire de câblage et le commutateur central à haute vitesse. L'épine dorsale du réseau n'est plus qu'un mécanisme de transport à haute vitesse, avec tous les autres équipements, tels les routeurs distribués, à la périphérie. La Figure 2.26 illustre un tel réseau.
- La phase 4, la phase finale, implique la commutation de bout en bout avec des fonctionnalités complètes de commutation VLAN et multicouche. A ce stade, les équipements de commutation intégrés de niveau 2 et 3 sont distribués sur tout le réseau et connectés au commutateur central à haute vitesse. La Figure 2.27 illustre la phase finale.

Figure 2.26

Distribution des routeurs entre le commutateur central à haute vitesse et les commutateurs LAN.

**Figure 2.27**

Commutation de bout en bout, avec fonctionnalités de commutation VLAN et multicouche.



Résumé

Ce chapitre vous a présenté les principes de conception générale de base des réseaux, ainsi que les équipements nécessaires. Les prochains chapitres de cette partie sont consacrés aux différentes technologies disponibles pour les concevoir.

3

Conception de réseaux IP étendus avec protocoles de routage interne

Par Atif Khan

Ce chapitre décrit les implications de l'utilisation des protocoles EIGRP (*Enhanced Interior Gateway Routing Protocol*), OSPF (*Open Shortest Path First*) et ODR (*On-Demand Routing*) lors de la conception de réseaux IP étendus, à travers l'étude des éléments suivants :

- topologie de réseau ;
- adressage et synthèse de routage ;
- sélection de route ;
- convergence ;
- évolutivité du réseau ;
- sécurité.

EIGRP et OSPF sont des protocoles de routage pour IP (*Internet Protocol*). Nous commencerons par une introduction aux problèmes d'ordre général concernant les protocoles de routage et poursuivrons avec les directives de conception permettant la mise en œuvre de protocoles spécifiques pour IP.

Implémentation des protocoles de routage

La section suivante présente les décisions essentielles devant être prises lors du choix et du déploiement des protocoles de routage. Elle introduit les notions élémentaires nécessaires à une bonne

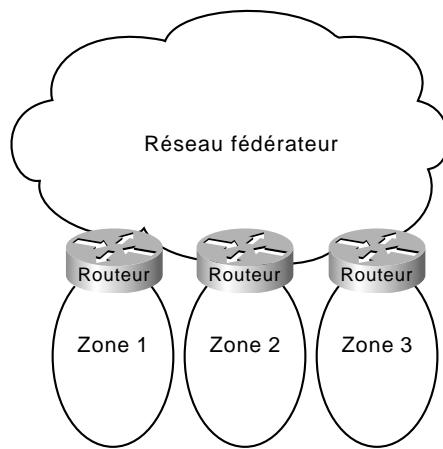
compréhension du contenu des prochaines sections qui examinent les caractéristiques spécifiques de ces protocoles.

Topologie de réseau

La topologie physique d'un réseau est représentée par l'ensemble complet des routeurs et des réseaux qu'ils relient. Les divers protocoles de routage apprennent différemment les informations de topologie. Certains requièrent une notion de hiérarchie et d'autres pas. Cette hiérarchie est nécessaire aux réseaux pour être évolutifs. Par conséquent, les protocoles ne requérant pas de hiérarchie devraient néanmoins l'implémenter à un certain degré, au risque de ne pas être évolutifs.

Certains protocoles exigent la création explicite d'une topologie hiérarchique par l'établissement d'un réseau fédérateur et de zones logiques (voir Figure 3.1). Les protocoles OSPF et IS-IS (*Intermediate System-to-Intermediate System*) sont des exemples de protocoles de routage qui utilisent une telle structure. Une topologie explicite selon un schéma hiérarchique est prioritaire sur une topologie créée par un système d'adressage.

Figure 3.1
Un réseau hiérarchique.



Quel que soit le protocole de routage utilisé, la topologie d'adressage devrait être définie de façon à refléter la hiérarchie. Deux méthodes sont recommandées pour assigner les adresses sur un réseau hiérarchique. La plus simple est d'attribuer à chaque zone, y compris au réseau fédérateur, une adresse de réseau unique. L'autre solution consiste à réservier des plages d'adresse pour chaque zone.

Une *zone* est un ensemble logique de réseaux et d'hôtes contigus. Elle comprend aussi tous les routeurs dotés d'une interface sur l'un des réseaux inclus. Chaque zone exécute une copie distincte de l'algorithme de routage de base, et possède, par conséquent, sa propre base de données topologique.

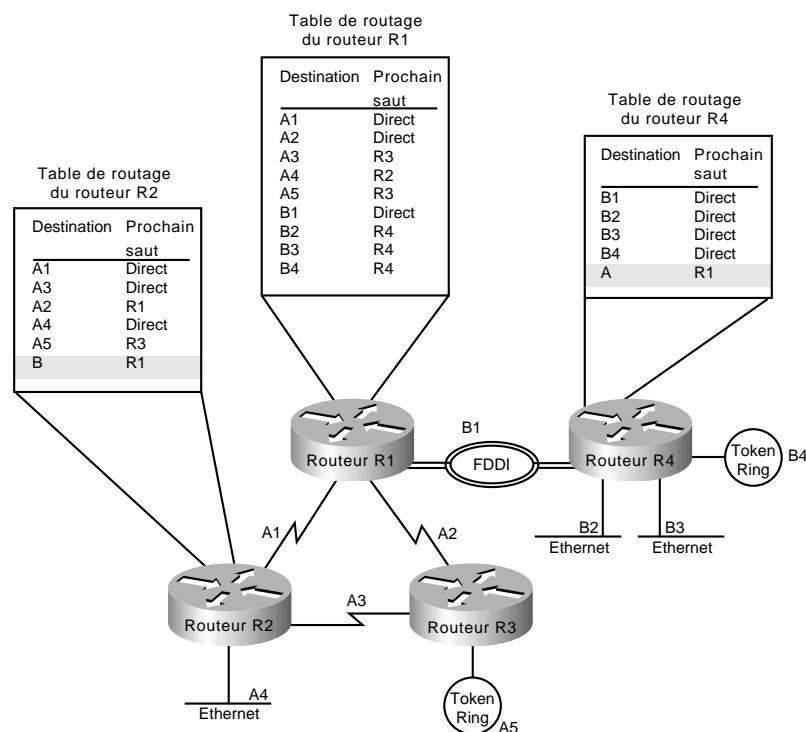
Adressage et synthèse de routage

Le processus de synthèse de routes condense les informations de routage. Il permet aux routeurs de résumer un certain ensemble d'itinéraires en une seule annonce, réduisant ainsi la charge qu'ils

doivent gérer et la complexité apparente du réseau. L'importance de ce processus croît avec la taille du réseau. Lorsqu'il n'est pas utilisé, chaque routeur sur un réseau doit mémoriser un chemin vers chaque sous-réseau.

La Figure 3.2 illustre un exemple de la synthèse de routes. Dans cet environnement, le routeur R2 mémorise un seul chemin vers tous les réseaux commençant par la lettre B. Le routeur R4 fait de même pour les réseaux commençant par la lettre A. C'est la base de la synthèse de routage. Le routeur R1 conserve tous les chemins, car il se trouve à la lisière des réseaux A et B.

Figure 3.2
Exemple de synthèse
de routage.

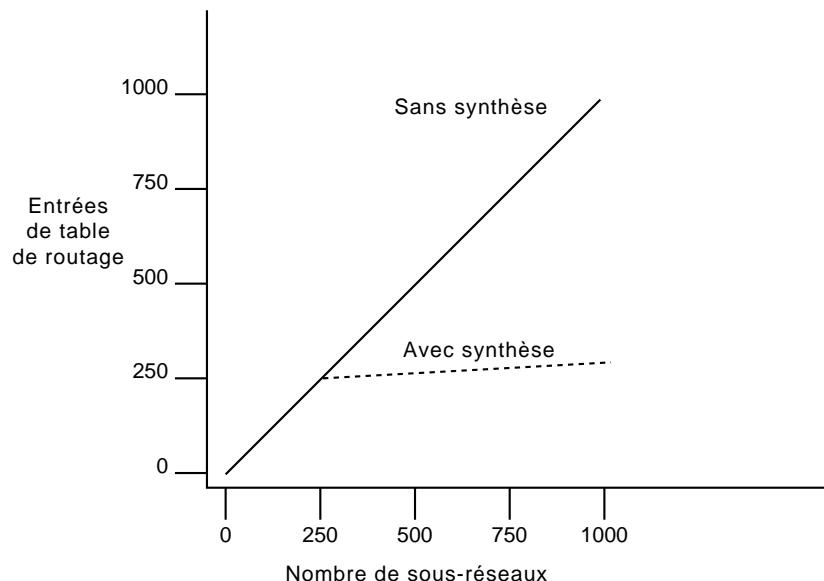


La réduction de la surcharge liée aux informations de routage et à leur propagation peut être significative. La Figure 3.3 illustre les économies potentielles. L'axe vertical dans l'illustration indique le nombre d'entrées dans la table de routage et l'axe horizontal représente le nombre de sous-réseaux. Sans le processus de synthèse, chaque routeur situé sur un réseau composé de mille sous-réseaux devrait mémoriser autant de routes. Avec la synthèse, le résultat est très différent. Si vous prenez, par exemple, un réseau de classe B avec huit bits d'espace d'adresse de sous-réseau, chaque routeur doit connaître tous les itinéraires vers les sous-réseaux de son adresse de réseau — 250 routes si l'on suppose que 1 000 sous-réseaux s'intègrent dans une structure de 4 réseaux principaux de 250 sous-réseaux chacun — plus une route pour chacun des autres réseaux (trois), ce qui donne un total de 253 routes à mémoriser par routeur. Cela représente à peu près une réduction de 75 % de la taille de la table de routage.

L'exemple précédent illustre le type de synthèse de routage le plus simple, où tous les accès aux sous-réseaux sont ramenés à un seul chemin vers un réseau donné. Certains protocoles de routage supportent également la synthèse de routes au niveau de n'importe quelle limite binaire (plutôt que seulement au niveau des limites principales des adresses de réseaux). Un protocole de routage ne peut réaliser une synthèse au niveau bit que s'il supporte les *masques de sous-réseau de longueur variable* (VLSM, Variable-Length Subnet Mask).

Certains protocoles de routage effectuent une synthèse automatique et d'autres nécessitent une configuration manuelle (voir Figure 3.3).

Figure 3.3
Avantages de la synthèse de routage.

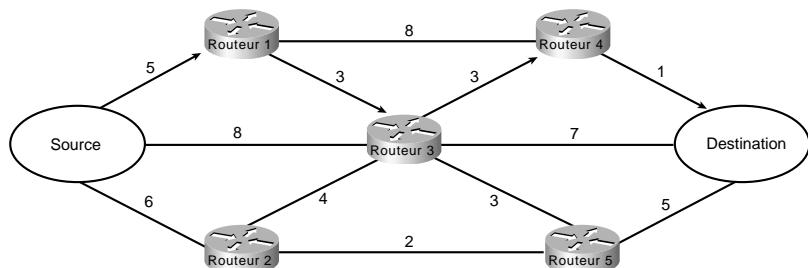


Sélection d'itinéraire

La sélection de route est insignifiante lorsqu'il n'existe qu'un seul chemin vers la destination. Cependant, si une section du chemin unique devient impraticable, aucun rétablissement n'est possible. Par conséquent, la plupart des réseaux sont conçus avec des chemins multiples pour qu'une autre solution puisse être envisagée en cas de défaillance d'un lien.

Les protocoles de routage comparent les métriques de distance pour sélectionner le meilleur chemin parmi plusieurs solutions. Elles sont calculées en se fondant sur une caractéristique ou sur un ensemble de caractéristiques définies pour chaque réseau. Une métrique est donc un agrégat des caractéristiques de chaque réseau physique rencontré sur une route. La Figure 3.4 illustre un réseau maillé avec une métrique assignée à chaque lien avec le meilleur itinéraire identifié pour aller de la source à la destination.

Figure 3.4
Métriques de routage et sélection d'itinéraire.



Les protocoles de routage utilisent diverses techniques pour attribuer une métrique à un réseau et chaque protocole possède une manière propre de former un agrégat métrique. La plupart d'entre eux sont capables d'utiliser plusieurs chemins lorsqu'ils sont de même coût. Seuls certains protocoles peuvent exploiter plusieurs chemins de coût inégal. Dans tous les cas, cet équilibrage de charge contribue à améliorer l'allocation globale de la bande passante du réseau.

Lorsque plusieurs itinéraires sont utilisés, il est possible de distribuer les paquets de différentes façons. Les deux mécanismes les plus courants sont *l'équilibrage de charge par paquet* et *l'équilibrage de charge par destination*. Le premier répartit les paquets sur tous les itinéraires possibles proportionnellement aux métriques de distance. Lorsque les chemins ont des coûts égaux, la répartition s'apparente à une distribution où chacun est servi à tour de rôle. Un paquet (ou une destination selon le mode de commutation) est alors distribué à chaque itinéraire possible. Le second mécanisme répartit les paquets sur toutes les routes possibles pour une destination donnée. Chaque nouvelle destination se voit assigner la route suivante disponible. Cette technique tend à préserver l'ordre des paquets.

NOTE

La plupart des implémentations TCP peuvent gérer les paquets sans prendre en compte leur ordre. Toutefois, cela peut entraîner des dégradations de performances.

Lorsque la commutation rapide est activée sur un routeur (par défaut), la sélection de route est effectuée en se fondant sur la destination. Dans le cas contraire, le choix s'effectue par rapport aux paquets. Pour des vitesses de liaison de 56 Kbit/s ou plus, la commutation rapide est recommandée.

Convergence

Lorsque la topologie de réseau change, le trafic doit être réaiguillé rapidement. L'expression "temps de convergence" désigne le délai nécessaire à un routeur pour prendre en compte une nouvelle route. Un routeur réagit en trois temps suite à un changement de topologie :

- Il détecte le changement.
- Il choisit un nouvel itinéraire.
- Il retransmet les informations de changement d'itinéraire.

Certains changements sont immédiatement détectables. Par exemple, la défaillance d'une ligne série entraînant la perte de la porteuse est immédiatement détectée par un routeur. D'autres problèmes sont plus difficiles à découvrir, comme une ligne série qui n'est plus fiable alors que la porteuse n'est pas perdue. De plus, certains médias comme Ethernet ne fournissent pas d'indications physiques telles que la perte de la porteuse. Lorsqu'un routeur est réinitialisé, les autres routeurs ne le voient pas non plus immédiatement. En général, la capacité des routeurs à détecter les problèmes dépend du média et du protocole de routage exploités.

Lorsqu'une rupture de lien est détectée, le protocole doit choisir un nouvel itinéraire puis propager l'information de changement de route. Dans les deux cas, les mécanismes employés dépendent du protocole.

Evolutivité du réseau

La capacité à faire évoluer un réseau est liée en partie aux propriétés d'adaptabilité des protocoles de routage utilisés et à la qualité de conception du réseau.

Deux facteurs limitent les possibilités d'évolution d'un réseau : les problèmes fonctionnels et les problèmes techniques. Les premiers sont généralement plus significatifs que les seconds. Les considérations liées à l'aspect fonctionnel encouragent l'emploi de grandes zones ou de protocoles qui ne requièrent pas de structure hiérarchique. Lorsque des protocoles hiérarchiques sont nécessaires, les considérations concernant l'aspect technique favorisent l'exploitation de zones dont la taille est basée sur les ressources disponibles (CPU, mémoire, etc.). Rechercher l'équilibre approprié, voilà tout l'art de la conception de réseau.

D'un point de vue technique, on peut dire que les protocoles de routage s'adaptent bien lorsque leur consommation en ressources ne croît pas proportionnellement au développement du réseau. Trois ressources essentielles sont exploitées par les protocoles de routage : mémoire, processeur et bande passante.

Mémoire

Les protocoles de routage utilisent la mémoire pour y stocker des tables de routage et des informations sur la topologie. La synthèse de routage permet à tous ces protocoles de réaliser des économies de mémoire. Maintenir des zones de petit taille permet de réduire la consommation de mémoire dans le cas de protocoles de routage hiérarchiques.

Processeur

L'utilisation du processeur est dépendante du protocole. Les protocoles de routage exploitent les cycles processeur pour calculer les routes. Le fait de limiter au minimum les informations de routage au moyen de la synthèse de routage permet de réduire cette consommation, car les effets d'un changement de topologie ont une portée limitée et le nombre de routes devant être recalculées après un changement est plus faible.

Bande passante

La consommation de la bande passante est également dépendante du protocole. Trois facteurs influent sur la quantité de bande passante utilisée par les protocoles de routage :

- **Le moment où les informations de routage sont envoyées.** Des mises à jour périodiques sont émises à intervalles réguliers. Les mises à jour flash ne sont transmises que lorsqu'un changement a eu lieu.
- **Les informations de routage elles-mêmes.** Les mises à jour complètes contiennent toutes les informations de routage. Les mises à jour partielles ne contiennent que les informations modifiées.
- **La destination des informations de routage.** Les mises à jour *par inondation* sont envoyées à tous les routeurs. Les mises à jour *liées* ne sont transmises qu'aux routeurs qui sont concernés par un changement.

NOTE

Les trois facteurs précités affectent également l'utilisation des ressources du processeur.

Les protocoles par vecteur de distance tels que RIP (*Routing Information Protocol*) et IGRP (*Interior Gateway Routing Protocol*) diffusent de façon périodique la totalité de leur table de routage en mode broadcast, indépendamment du fait qu'elle ait changé ou non. L'intervalle d'annonce varie entre 10 secondes pour RIP et 90 secondes pour IGRP. Lorsque le réseau est stable, les protocoles par vecteur de distance fonctionnent bien, mais gâchent de la bande passante en raison de leurs annonces périodiques. Lorsqu'une défaillance se produit sur un lien du réseau, ils ne provoquent pas une charge supplémentaire excessive sur le réseau, mais sont longs à converger vers un nouvel itinéraire ou à éliminer le lien défectueux.

Les protocoles de routage par état de lien tels que OSPF, IS-IS et NLSP (*NetWare Link Services Protocol*) ont été conçus pour apporter une solution aux limitations des protocoles par vecteur de distance (convergence lente et utilisation inutile de la bande passante). Ils sont plus complexes et exploitent davantage les ressources processeur et la mémoire. Cette surcharge additionnelle détermine le nombre de voisins qu'un routeur peut supporter et qui peuvent se trouver dans une zone. Ce nombre varie d'un réseau à un autre et dépend de variables comme la puissance du processeur, le nombre de routes et la stabilité des liens.

Lorsque le réseau est stable, les protocoles par état de lien minimisent l'exploitation de la bande passante en transmettant des mises à jour uniquement dans le cas de changements. Un mécanisme de signalisation Hello vérifie l'accessibilité des voisins. Lorsqu'une panne se produit sur le réseau, ce type de protocole inonde la zone concernée avec des annonces d'état de lien LSA (*Link-State Advertisement*). Dans ce cas, tous les routeurs au sein de la zone défaillante doivent recalculer leurs itinéraires. Le fait que les annonces doivent être envoyées par inondation sur la totalité de la zone et que tous les routeurs doivent mettre à jour leur table de routage limite le nombre des voisins pouvant se trouver dans une zone.

EIGRP est un protocole par vecteur de distance avancé qui possède certaines des propriétés des protocoles par état de lien. Il apporte une solution aux limitations vues plus haut relatives aux protocoles plus conventionnels de sa catégorie. Lorsque le réseau est stable, il envoie des mises à jour

uniquement en cas de changement sur le réseau. A l'instar des protocoles par état de lien, il utilise un mécanisme de signalisation Hello pour déterminer l'accessibilité de ses voisins. En cas de dysfonctionnement, il recherche de nouveaux successeurs lorsqu'il n'en existe aucun de disponible dans sa table topologique, en envoyant des messages à ses voisins. Cette recherche de nouveaux successeurs peut engendrer un fort trafic (mises à jour, requêtes et réponses) avant d'aboutir à une convergence. Un tel comportement limite le nombre de voisins possibles.

Sur les réseaux étendus, la question de la bande passante est capitale. Par exemple, la technologie Frame Relay, qui multiplexe de façon statistique de nombreuses connexions logiques (circuits virtuels) sur un seul lien physique, permet la création de réseaux qui se partagent la bande passante. Les réseaux publics intégrant cette technologie exploitent le partage de bande passante à tous les niveaux du réseau. C'est-à-dire qu'il peut être mis en œuvre aussi bien sur le réseau Frame Relay d'une entreprise qu'entre les réseaux de deux entreprises.

Deux facteurs influent considérablement sur la conception des réseaux publics Frame Relay :

- Les utilisateurs sont facturés pour chaque circuit virtuel permanent (PVC, *Permanent Virtual Circuit*), ce qui pousse les concepteurs de réseaux à réduire le nombre de ces circuits.
- Les réseaux des opérateurs publics incitent parfois les utilisateurs à éviter l'utilisation des circuits CIR (*Committed Information Rate*), qui reposent sur un contrat de débit moyen que les utilisateurs doivent respecter. Bien que les fournisseurs de services tentent de garantir une bande passante suffisante, la perte de paquets reste possible.

En général, les paquets peuvent être perdus sur les réseaux étendus en raison d'une bande passante insuffisante. Pour les réseaux Frame Relay, ce risque est aggravé, car il n'existe pas de service de reproduction de diffusions broadcast. Aussi chaque paquet envoyé en diffusion broadcast sur une interface Frame Relay doit être reproduit par le routeur au niveau de cette interface pour chaque circuit virtuel permanent. Cette exigence limite le nombre de circuits pouvant être gérés efficacement par un routeur.

Outre le problème de la bande passante, les concepteurs doivent considérer la question de la taille des tables de routage qui doivent être propagées. En clair, les considérations de conception pour une interface comptant 50 voisins et 100 routes de propagation sont très différentes de celles envisagées pour une interface avec 50 voisins et 10 000 routes.

Sécurité

Le contrôle de l'accès aux ressources d'un réseau est essentiel. Certains protocoles de routage fournissent des techniques pouvant être exploitées dans le cadre d'une stratégie de sécurité. Avec certains protocoles, il est possible de placer un filtre pour que des itinéraires spécifiques ne soient pas annoncés dans certaines parties du réseau.

Certains protocoles de routage peuvent authentifier les routeurs qui utilisent le même protocole. Les mécanismes d'authentification sont spécifiques aux protocoles et généralement insuffisants. Malgré cela, il est néanmoins conseillé de tirer profit des techniques qui existent. L'authentification peut améliorer la stabilité du réseau en empêchant des routeurs ou des hôtes non autorisés de participer au protocole de routage, que la tentative de participation soit accidentelle ou délibérée.

Directives de conception d'un réseau EIGRP

EIGRP (*Enhanced Interior Gateway Routing Protocol*) est un protocole de routage développé par Cisco Systems qui a été introduit avec la version 9.21 de System Software et la version 10.0 de Cisco IOS (*Internetworking Operating System*). Il combine les avantages des protocoles par vecteur de distance tels que IGRP avec ceux des protocoles par état de lien comme OSPF. Il utilise l'algorithme DUAL (*Diffusing Update ALgorithm*) pour permettre une convergence rapide.

Il inclut le support des protocoles de réseau IP, Novell NetWare et AppleTalk. Les prochaines sections traitent des sujets suivants :

- Topologie de réseau EIGRP ;
- Adressage EIGRP ;
- Synthèse de routes EIGRP ;
- Sélection de route EIGRP ;
- Convergence EIGRP ;
- Evolutivité d'un réseau EIGRP ;
- Sécurité avec EIGRP.

NOTE

Bien que les informations de cette section s'appliquent à IP, IPX et AppleTalk EIGRP, il sera davantage question de IP. Reportez-vous au Chapitre 17 pour les études de cas sur la façon d'intégrer EIGRP avec les réseaux IP, IPX et AppleTalk et obtenir des exemples de configuration détaillés ainsi que des informations sur les problèmes spécifiques aux protocoles.

Topologie de réseau EIGRP

Le protocole EIGRP peut utiliser une topologie non hiérarchique (ou linéaire). Toutefois, pour concevoir un réseau qui soit évolutif, il faut disposer d'un certain degré de hiérarchie. EIGRP assure la synthèse automatique des routes de sous-réseaux de réseaux directement connectés, réduisant les informations de routage au niveau de l'adresse de réseau (voir section "Synthèse de routes EIGRP" plus loin dans ce chapitre).

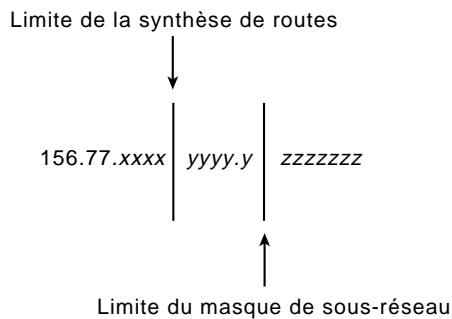
Adressage EIGRP

La première étape dans la conception d'un réseau EIGRP consiste à décider de la façon dont son adressage doit être réalisé. Dans de nombreuses situations, une entreprise reçoit une seule adresse du NIC (*Network Information Center*), comme une adresse de Classe B, qu'elle doit allouer à son réseau. La division en sous-réseaux et les masques de sous-réseaux de longueur variable (VLSM) servent à optimiser l'exploitation de l'espace d'adresse. EIGRP pour IP supporte l'utilisation de VLSM.

Imaginez un réseau sur lequel une adresse de Classe B a été divisée en sous-réseaux, et supposez que des groupes contigus de ces sous-réseaux aient été synthétisés par EIGRP. Un réseau de Classe B 156.77.0.0 pourrait être subdivisé (voir Figure 3.5).

Figure 3.5

Masques de sous-réseaux VLSM et limites utilisées par la synthèse de routes.



Dans la Figure 3.5, les lettres x , y et z représentent les bits des deux derniers octets du réseau de Classe B :

- Les quatre bits x représentent la limite de la synthèse de routes.
- Les cinq bits y représentent jusqu'à 32 sous-réseaux par route synthétisée.
- Les sept bits z permettent d'adresser jusqu'à 126 (128 – 2) hôtes par sous-réseau.

L'Annexe A fournit un exemple complet de subdivision d'une adresse 150.100.0.0 de Classe B en sous-réseaux.

Synthèse de routes EIGRP

Avec ce protocole, les adresses des sous-réseaux de réseaux directement connectés sont automatiquement ramenées aux limites de l'adresse de réseau. De plus, un administrateur de réseau peut configurer la synthèse de routes sur une interface, au niveau de n'importe quelle limite binaire, permettant aux plages d'adresse de réseaux d'être résumées de façon arbitraire.

Sélection de route EIGRP

Les protocoles de routage comparent les métriques de route pour sélectionner le meilleur chemin à partir d'un groupe d'itinéraires possibles. La compréhension des points suivants est importante pour la conception d'un réseau EIGRP. Ce protocole utilise le même vecteur de métriques que IGRP. Des valeurs de métriques distinctes sont assignées pour la bande passante, le délai, la fiabilité et la charge. Par défaut, EIGRP calcule la métrique d'une route en utilisant la bande passante minimale de chaque saut emprunté sur l'itinéraire et en ajoutant un délai spécifique au média pour chaque saut. Voici les métriques qu'il utilise :

- **Bandé passante.** La bande passante est déduite d'après le type d'interface. Elle peut être modifiée avec la commande `bandwidth`.
- **Délai.** Chaque type de média comporte un délai de propagation qui lui est associé. Cette valeur peut être modifiée avec la commande `delay`.
- **Fiabilité.** La fiabilité est définie dynamiquement sous la forme d'une moyenne pondérée calculée sur 5 secondes.

- **Charge.** La charge est définie dynamiquement sous la forme d'une moyenne pondérée calculée sur 5 secondes.

Lorsque EIGRP synthétise un groupe de routes, il utilise la métrique de la meilleure route incluse dans la synthèse comme métrique pour la synthèse.

Convergence EIGRP

Le protocole EIGRP implémente un nouvel algorithme de convergence appelé DUAL. Celui-ci utilise deux techniques qui permettent au protocole de converger très rapidement. Tout d'abord, chaque routeur EIGRP crée une table topologique EIGRP à partir des tables de routage reçues de ses voisins. Un routeur peut ainsi emprunter instantanément un nouvel itinéraire vers une destination donnée, à condition qu'il en existe un, connu d'après les informations recueillies au préalable auprès de ses voisins. S'il n'en existe pas, un routeur exploitant EIGRP devient *actif* pour cette destination et envoie une requête vers chacun de ses voisins, demandant une autre route possible vers la destination en question. Ces requêtes se propagent jusqu'à ce qu'un autre chemin soit localisé. Les routeurs qui ne sont pas affectés par le changement de topologie demeurent *passifs* et n'ont pas besoin d'être impliqués dans ce processus de recherche.

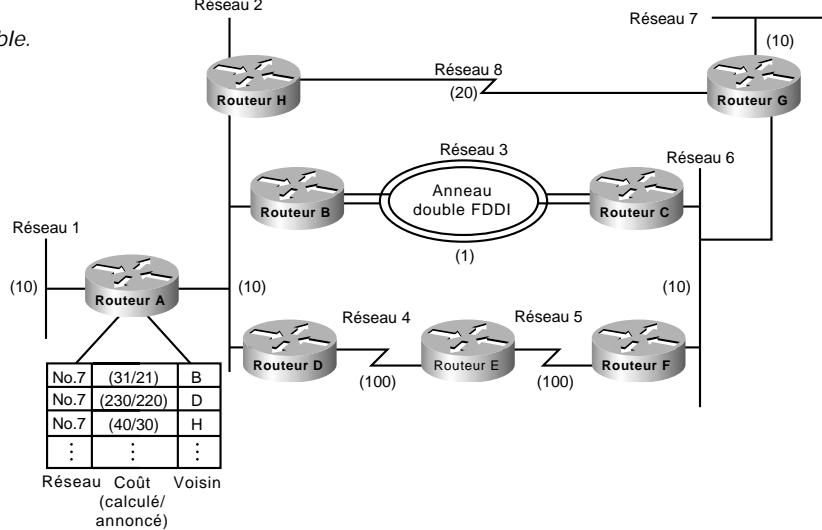
Un routeur qui utilise EIGRP reçoit les tables de routage complètes de la part de ses voisins lorsqu'il communique la première fois avec eux. Ensuite, seuls les changements apportés dans les tables sont envoyés, et uniquement aux routeurs affectés par ces changements. Un successeur est un routeur voisin actuellement utilisé pour la transmission de paquets qui fournit la route de plus faible coût vers une destination donnée, et qui n'est pas impliqué dans une boucle de routage. Lorsque la route passant par ce routeur est perdue, le successeur possible, s'il en existe un pour cette route, devient le successeur.

La table de routage maintient une liste des coûts calculés pour atteindre différents réseaux. La table topologique maintient toutes les routes annoncées par les voisins. Pour chaque réseau, un routeur conserve le coût réel qui lui est associé, ainsi que celui annoncé par son voisin. En cas de panne, la convergence est instantanée si un successeur possible peut être localisé. Un voisin peut accéder au rang de successeur possible s'il satisfait aux conditions de faisabilité définies par l'algorithme DUAL. L'algorithme identifie un successeur possible au moyen de la procédure suivante :

- Il détermine l'appartenance à un ensemble V1. V1 représente tous les voisins dont la distance annoncée vers le réseau x est inférieure à DP — DP est la distance possible et est définie comme étant la métrique la plus intéressante durant une transition d'état, actif vers passif.
- Il calcule D_{min} qui est le coût minimal calculé pour joindre le réseau x .
- Il détermine l'appartenance à V2. V2 est l'ensemble des voisins qui appartiennent à V1 et qui offrent un coût calculé vers le réseau x égal à D_{min} .

La condition de faisabilité est satisfaite lorsque V2 possède un ou plusieurs membres. Le concept de successeur possible est illustré Figure 3.6. Observez les entrées de la table de topologie du routeur A pour le réseau 7. Le routeur B est le *successeur* avec un coût calculé de 31 pour atteindre le réseau 7, comparé aux coûts des routeurs D (230) et H (40).

Figure 3.6
Successeur DUAL possible.



Si le routeur B devient indisponible, le routeur A réalise les trois étapes suivantes pour localiser un successeur possible pour le réseau 7 :

- Il détermine quels sont les voisins qui ont annoncé une distance vers le réseau 7 inférieure à la distance possible (DP) du routeur A, qui est égale 31. Comme le routeur H remplit cette condition, il est membre de V1.
- Il calcule le coût minimal calculé vers le réseau 7. Le routeur H fournit un coût de 40, et le routeur D un coût de 230. La valeur de Dmin est par conséquent de 40.
- Il détermine l'ensemble des voisins appartenant à V1 et qui offrent un coût calculé vers le réseau 7 égal à Dmin (40). Le routeur H satisfait à cette condition.

Le successeur possible est le routeur H qui offre un accès de plus faible coût (40) vers le réseau 7 à partir du routeur A. Si pour une raison quelconque il devenait également inutilisable, le routeur A procéderait à l'évaluation suivante :

- Il détermine les voisins qui possèdent une distance annoncée vers le réseau 7 inférieure à la valeur de DP pour ce réseau. Comme les routeurs B et H ne sont plus accessibles, seul le routeur D reste utilisable. Toutefois, le coût offert par ce routeur pour le réseau en question est de 220, une valeur supérieure à celle de DP (31) enregistrée par A. Le routeur D ne peut donc pas être un membre de V1. DP reste à 31, car sa valeur ne peut changer que durant une transition d'état, actif vers passif, ce qui n'est pas le cas ici. Le réseau 7 n'a connu aucune transition vers un état actif, une situation qui est désignée par le terme *calcul local*.
- Comme il n'existe aucun membre de V1, il n'y a aucun successeur possible. Le routeur A passe alors dans une phase de transition d'état, passif vers actif, pour le réseau 7 et interroge ses voisins à son sujet. Cette phase transitoire vers un état actif est connue sous l'appellation *calcul par diffusion*.

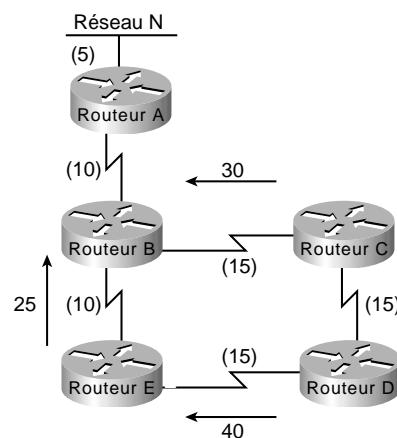
NOTE

Reportez-vous à l'Annexe H pour obtenir une liste de sources d'informations sur la convergence EIGRP.

L'exemple et les graphiques suivants illustrent la façon dont EIGRP supporte la convergence quasi-instantanée dans un environnement de réseau changeant. Dans la Figure 3.7, tous les routeurs communiquent entre eux et avec le réseau N. Le coût calculé pour atteindre les autres routeurs et le réseau N est indiqué. Par exemple, le coût pour aller du routeur E au routeur B est 10 et le coût entre le routeur E et le réseau N est 25 (coût calculé $10 + 10 + 5$).

Figure 3.7

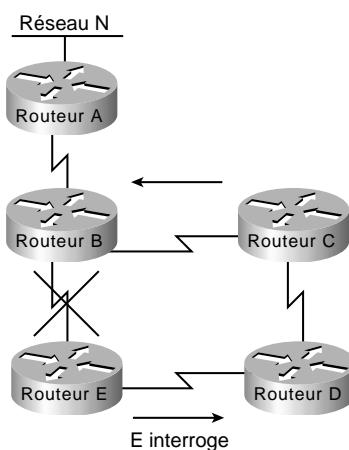
Exemple de procédure avec DUAL
(phase 1) : connectivité réseau initiale.



Dans la Figure 3.8, la connexion entre les routeurs B et E est interrompue. Le routeur E envoie une requête multidestinataire à tous ses voisins et place le réseau N dans un état actif.

Figure 3.8

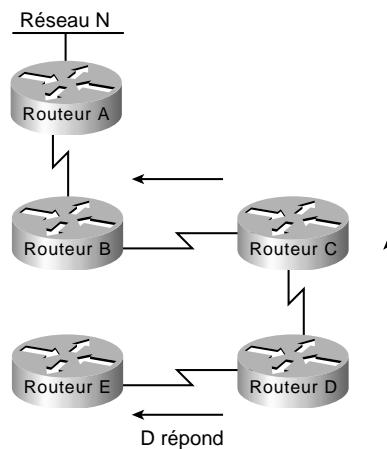
Exemple de procédure avec DUAL
(phase 2) : envoi de requêtes.



Ensuite, comme illustré Figure 3.9, le routeur D détermine un successeur possible. Il transfère la succession du routeur E sur le routeur C et envoie une réponse au routeur E.

Figure 3.9

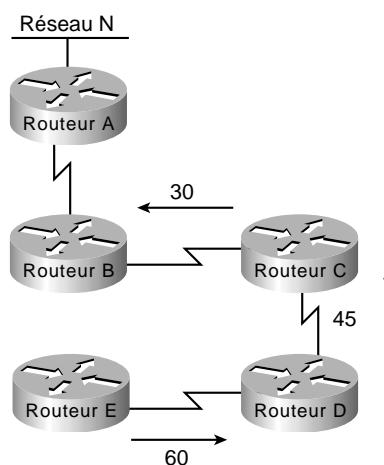
Exemple de procédure avec DUAL (phase 3) : transfert vers un successeur possible.



Dans la Figure 3.10, le routeur E a reçu les réponses de la part de ses voisins et fait passer le réseau N dans un état passif. Le routeur E place le réseau N dans sa table de routage avec une distance de 60.

Figure 3.10

Flux d'un trafic entre sous-réseaux avec la commutation de niveau 3.



NOTE

Les routeurs A, B et C n'ont pas été impliqués dans le calcul de route. Le routeur D a recalculé son chemin vers le réseau N sans avoir à obtenir de nouvelles informations de la part de ses voisins en aval.

Evolutivité d'un réseau EIGRP

L'aptitude d'un réseau à évoluer est limitée par deux facteurs : les problèmes fonctionnels et les problèmes techniques. Sur le plan fonctionnel, EIGRP est facile à configurer. Sur le plan technique, sa consommation des ressources n'augmente pas proportionnellement avec le développement du réseau, s'il est conçu correctement. La notion de hiérarchie, à la fois logique et physique, est essentielle pour concevoir un réseau EIGRP évolutif.

Mémoire

Un routeur exécutant EIGRP stocke les routes annoncées par ses voisins afin de pouvoir s'adapter rapidement à tout changement de topologie et exploiter les itinéraires alternatifs. Plus un routeur a de voisins, plus il consomme de mémoire. La fonction d'agrégation automatique de routes de EIGRP limite de façon naturelle la taille de la table de routage. Une limitation supplémentaire est possible avec une configuration manuelle de cette fonction.

Processeur

EIGRP utilise l'algorithme DUAL pour fournir une convergence rapide. Il ne recalcule que les routes qui sont affectées par un changement de topologie. DUAL n'entraîne pas de calcul complexe, mais le pourcentage d'utilisation du processeur dépend de la stabilité du réseau, des limites des requêtes et de la fiabilité des liens.

Bandé passante

EIGRP utilise des mises à jour partielles. Elle ne sont générées que lorsqu'un changement se produit ; seules les informations modifiées sont envoyées, et uniquement aux routeurs concernés par le changement. En raison de ce comportement, ce protocole est très efficace dans son utilisation de la bande passante. Le protocole Hello de EIGRP induit une consommation supplémentaire de la bande passante pour maintenir les informations d'activité des routeurs voisins.

Pour créer un réseau EIGRP évolutif, il est conseillé d'implémenter la synthèse de routage. Pour qu'un environnement soit capable de supporter cette fonction, l'implémentation d'un schéma d'adressage hiérarchique efficace est nécessaire. La raison est que les performances et l'évolutivité d'un réseau EIGRP peuvent être considérablement affectées par la structure d'adressage mise en œuvre.

Sécurité avec EIGRP

Le protocole EIGRP n'est disponible que sur les routeurs Cisco. Cela prévient tout risque d'interruption de routage, accidentelle ou malveillante, pouvant être provoquée par un hôte du réseau. De plus, des filtres de route peuvent être mis en place sur n'importe quelle interface pour empêcher que les informations de routage ne soient recueillies ou propagées de façon inappropriée.

Directives de conception d'un réseau OSPF

OSPF est un protocole de routage interne, ou IGP (*Interior Gateway Protocol*), qui a été développé pour être utilisé sur les réseaux s'appuyant sur le protocole IP. En tant que protocole de routage interne, il ne distribue les informations de routage qu'entre les routeurs d'un système autonome

(AS, *Autonomous System*). Un système autonome est un groupe de routeurs qui échangent des informations de routage via un protocole de routage commun. OSPF s'appuie sur un algorithme de routage par le plus court chemin (SPF, *Shortest Path First*) ou par état de lien.

Il a été développé par le groupe de travail OSPF de l'IETF (*Internet Engineering Task Force*). Il a été conçu expressément pour être exploité dans un environnement IP, avec un support explicite des sous-réseaux IP et du marquage des informations de routage provenant de l'extérieur. La version 2 du protocole est documentée dans le RFC 1247.

Si vous concevez un réseau OSPF en partant de rien ou faites migrer votre réseau existant vers OSPF, les directives suivantes vous aideront à mettre en œuvre un environnement OSPF fiable et évolutif.

L'implémentation réussie d'un environnement OSPF implique deux phases importantes :

- la définition des limites de zones ;
- l'assignation des adresses.

Une planification et une exécution efficaces de ces deux phases garantiront le succès de votre implémentation. Elles sont détaillées dans les sections suivantes :

- Topologie de réseau OSPF ;
- Adressage et synthèse de routes OSPF ;
- Sélection de route OSPF ;
- Convergence OSPF ;
- Evolutivité d'un réseau OSPF ;
- Sécurité avec OSPF ;
- Fonctionnalités NSSA (*Not-So-Stubby Area*) de OSPF;
- OSPF ODC (*On-Demand Circuit*) ;
- OSPF sur les réseaux non broadcast (sans diffusion).

NOTE

Reportez-vous au Chapitre 16 pour travailler sur une étude de cas concernant la définition et la configuration de la redistribution OSPF.

Topologie de réseau OSPF

C'est dans un environnement de routage hiérarchique que le protocole OSPF fonctionne le mieux. La première décision — et la plus importante — lors de la conception d'un réseau OSPF consiste à déterminer les routeurs et les liens qui doivent faire partie de l'épine dorsale et ceux qui doivent être inclus dans chaque zone. Voici plusieurs directives importantes à considérer lors de la conception d'une topologie OSPF :

- **Le nombre de routeurs dans une zone.** OSPF utilise un algorithme gourmand en ressources processeur. Le nombre de calculs qui doivent être exécutés, étant donné un nombre n de paquets d'état de lien, est proportionnel à $n \log n$. En conséquence, plus la zone est grande et instable,

plus grandes sont les chances de rencontrer des problèmes de performances lors des calculs du protocole de routage. Le nombre de routeurs dans une zone dépend de leur processeur, de leur mémoire et du nombre de liens dans la zone.

- **Le nombre de voisins pour chaque routeur.** OSPF envoie par inondation tous les changements d'état de lien à tous les routeurs d'une zone. Les routeurs dotés de nombreux voisins ont le plus de travail à accomplir lorsque des modifications ont lieu. Le nombre de voisins par routeur dépend du processeur de celui-ci, du nombre de liens dans une zone, du processeur des routeurs voisins, et de la bande passante des liens menant vers les voisins.
- **Le nombre de zones supportées par chaque routeur.** Un routeur doit exécuter l'algorithme LSA pour chaque changement d'état de lien qui intervient dans une zone à laquelle il participe. Chaque routeur interzones (*Area Border Router*) est impliqué dans au moins deux zones (celle de l'épine dorsale et celle qu'il connecte à l'épine dorsale).
- **Choix du routeur désigné.** En général, le routeur désigné et le routeur désigné de secours sur un LAN sont voisins de tous les autres routeurs. Ils sont chargés de générer les inondations LSA sur les routes adjacentes et de définir l'état des liens pour le compte du réseau. Il est donc conseillé de choisir pour ces rôles des routeurs qui ne sont pas déjà fortement sollicités par des activités consommatrices en ressources processeur.

Les explications qui suivent traitent des problèmes de topologie en rapport avec l'épine dorsale et les zones.

Considérations liées à l'épine dorsale

La *stabilité* et la *redondance* sont deux caractéristiques importantes de l'épine dorsale. La stabilité est meilleure si la taille de l'épine dorsale reste raisonnable. Une des raisons est que tous les routeurs qui y participent doivent recalculer leurs routes après chaque changement d'état de lien. Une épine dorsale de petite taille limite les probabilités de changements et la consommation de cycles du processeur nécessaires pour recalculer les itinéraires. La redondance est importante au niveau de l'épine dorsale afin d'éviter tout partitionnement lorsqu'un lien est coupé. Les épingles dorsales bien conçues sont prévues pour pallier cela en cas de défaillance d'une liaison.

Une épine dorsale OSPF doit être continue. Pour cela, OSPF supporte l'utilisation de liaisons virtuelles. Une telle liaison crée un chemin entre deux routeurs interzones (un routeur de ce type relie une zone à l'épine dorsale) qui ne sont pas directement connectés. Un lien virtuel peut être utilisé pour soutenir une épine dorsale morcelée. Toutefois, ne concevez pas un réseau OSPF de manière qu'il nécessite l'emploi de liaisons virtuelles. La stabilité d'une liaison virtuelle est déterminée par celle de la zone sous-jacente. Cette dépendance peut compliquer les tâches de dépannage. De plus, elles ne peuvent pas traverser les zones *stub* (voir section "Annonces de routage dans le sens épine dorsale-zone" plus loin dans ce chapitre).

Evitez de placer les hôtes (tels que des stations de travail, des serveurs de fichiers ou d'autres ressources) dans la zone de l'épine dorsale. L'extension du réseau est plus simple s'ils sont maintenus en dehors, en outre, l'environnement est aussi plus stable.

Considérations liées aux zones

Une zone individuelle doit être continue. Elle peut être partitionnée, mais cela n'est pas recommandé. Dans ce contexte, cela signifie qu'elle doit pouvoir présenter un chemin continu reliant tous les routeurs entre eux. Cela ne signifie pas que tous les routeurs doivent partager un média de réseau commun. La conception de zones implique deux tâches essentielles :

- déterminer l'adressage de la zone ;
- déterminer comment connecter la zone à l'épine dorsale.

Les zones devraient posséder un ensemble continu d'adresses de réseaux ou de sous-réseaux. Sans un espace d'adressage continu, il n'est pas possible d'implémenter la synthèse de routes. Les routeurs qui relient une zone à l'épine dorsale sont appelés routeurs interzones (*Area Border Router*). Une zone peut disposer d'un ou de plusieurs de ces routeurs. En général, il est souhaitable d'en avoir plus d'un par zone pour réduire les risques de rupture de liaison avec l'épine dorsale.

Lors de la création d'un réseau OSPF étendu, la définition des zones et l'assignation des ressources qu'elles contiennent doivent s'appuyer sur une approche pragmatique du réseau. Les deux règles générales suivantes permettent de s'assurer que le réseau reste souple et offre les performances requises pour un accès fiable aux ressources :

- **Prendre en compte la proximité physique lors de la définition des zones.** Si un emplacement donné présente une connectivité dense, créez une zone spécifique pour les nœuds qui le forment.
- **Réduire la taille maximale des zones si les liaisons sont instables.** Si votre réseau comprend des liens instables, envisagez l'implémentation de zones plus petites pour réduire les risques d'instabilité de route. Lorsqu'une route est perdue ou, au contraire, entre en activité, chaque zone affectée doit converger vers une nouvelle topologie. L'algorithme Dykstra est exécuté sur tous les routeurs concernés. En segmentant votre réseau en zones plus petites, vous isolez les liens instables et fournissez un service global plus fiable.

Adressage et synthèse de routes OSPF

L'assignation d'adresses et la synthèse de routes sont étroitement liées lorsqu'il s'agit de concevoir un réseau OSPF. Pour créer un réseau OSPF évolutif, implémentez la synthèse de routes. Celle-ci requiert la mise en œuvre d'une stratégie d'adressage hiérarchique efficace pour pouvoir être supportée par l'environnement développé. La structure de cet adressage peut avoir un impact profond sur les performances et l'aptitude à évoluer de votre réseau. Les sections suivantes traitent de la synthèse de routes OSPF et de trois options d'adressage :

- adresses de réseau distinctes pour chaque zone ;
- zones d'adresse NIC créées avec masques de sous-réseaux binaires et VLSM ;
- adressage privé, avec une *zone démilitarisée* (DMZ, *Demilitarized Zone*) tampon vers l'Internet.

NOTE

Maintenez une stratégie d'adressage aussi simple que possible, mais veillez à ne pas exagérer dans ce sens. Bien que cette simplicité puisse vous faire gagner du temps lors de l'exploitation ou du dépannage de votre réseau, l'utilisation de certains raccourcis peut avoir des conséquences graves. Lors de l'élaboration d'un environnement d'adressage évolutif, adoptez une approche structurée. Si nécessaire, utilisez des masques de sous-réseaux binaires, mais assurez-vous que la synthèse de routes peut être accomplie par les routeurs interzones.

Synthèse de routes OSPF

L'utilisation de la synthèse de routes est fortement recommandée pour obtenir un réseau OSPF fiable et évolutif. L'efficacité de cette fonctionnalité et l'implémentation de votre réseau OSPF en général s'appuient sur la stratégie d'adressage que vous adoptez. Cette synthèse se produit entre chaque zone et la zone d'épine dorsale. Elle doit être configurée manuellement avec OSPF. Lors de la planification de votre réseau, examinez les points suivants :

- Veillez à ce que votre stratégie d'adressage soit configurée de telle sorte que la plage des adresses de sous-réseaux assignées au sein d'une zone soit continue.
- Créez un espace d'adresse qui vous permette par la suite de diviser les zones plus facilement lorsque le réseau s'étendra. Si possible, assignez les sous-réseaux en vous fondant sur des limites simples au niveau octet. Si vous ne pouvez pas suivre des règles de division simples et faciles à mémoriser, veillez à disposer d'une structure d'adressage bien détaillée. Mieux vous connaîtrez la répartition de votre espace d'adresse, mieux vous pourrez prévoir certains changements.
- Prévoyez l'ajout de nouveaux routeurs dans votre environnement. Le moment venu, veillez à les installer de façon appropriée comme routeurs intrazone, d'épine dorsale, ou interzones. Ce type de changements provoque la création d'une nouvelle topologie et, en conséquence, des modifications éventuelles au niveau du routage (peut-être aussi au niveau des performances) lorsque la topologie OSPF est recalculée.

Structure d'adressage séparée pour chaque zone

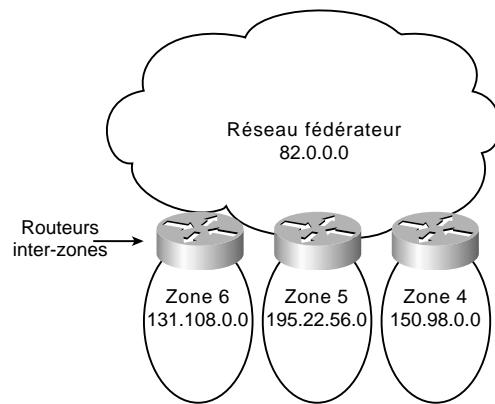
L'une des méthodes d'allocation d'adresses les plus simples avec OSPF consiste à assigner une adresse de réseau distincte à chaque zone. Selon cette procédure, vous créez une épine dorsale et plusieurs zones, et attribuez une adresse de réseau IP différente à chacune des zones. La Figure 3.11 illustre ce type de stratégie.

Voici les principales étapes de la création d'un tel réseau :

1. Définissez votre structure (identifiez les zones et allouez leur des nœuds).
2. Assignez des adresses aux réseaux, sous-réseaux et stations terminales.

Dans le réseau illustré Figure 3.11, chaque zone possède sa propre adresse unique. Il peut s'agir d'une adresse de Classe A (l'épine dorsale, voir Figure 3.11), de Classe B (zones 4 ou 6), ou de Classe C (zone 5).

Figure 3.11
Exemple d'attribution d'adresses NIC.



Voici quelques avantages liés à l'attribution d'une adresse unique à chaque zone :

- L'attribution des adresses est relativement facile à mémoriser.
- La configuration des routeurs est assez simple — ce qui limite le risque d'erreur.
- L'exploitation du réseau est simplifiée, car chaque zone possède une adresse de réseau unique et simple.

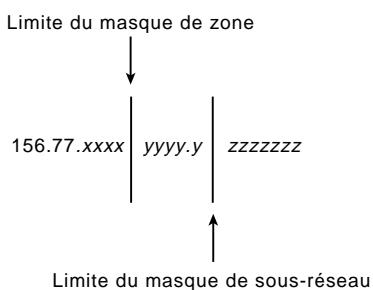
Dans l'exemple illustré Figure 3.11, la configuration de la synthèse de routes au niveau des routeurs interzones est grandement simplifiée. Les routes de la zone 4 qui convergent vers l'épine dorsale peuvent être synthétisées de la manière suivante : *toutes les routes commençant avec 150.98 se trouvent dans la zone 4*.

Le principal inconvénient de cette approche est un gaspillage de l'espace d'adresse. Si vous adoptez cette mesure, veillez à ce que les routeurs interzones soient configurés pour assurer la synthèse de routes. Celle-ci doit être explicitement définie.

Sous-réseaux avec masques binaires et VLSM

Les masques de sous-réseaux binaires et de longueur variable peuvent être combinés pour économiser de l'espace d'adresse. Imaginez un réseau sur lequel une adresse de Classe B est divisée au moyen d'un masque binaire pour être répartie sur seize zones. Elle pourrait être subdivisée comme illustré Figure 3.12.

Figure 3.12
Zones et masques de sous-réseaux.



Dans la Figure 3.12, les lettres x , y et z représentent les bits des deux derniers octets du réseau de Classe B :

- Les quatre bits x sont utilisés pour identifier 16 zones.
- Les cinq bits y représentent jusqu'à 32 sous-réseaux par zone.
- Les sept bits z permettent d'adresser jusqu'à 126 ($128 - 2$) hôtes par sous-réseau.

L'Annexe A fournit un exemple complet de subdivision d'une adresse 150.100.0.0 de Classe B en sous-réseaux. Elle décrit le concept de masques de zones et la division de grands sous-réseaux en sous-réseaux plus petits au moyen de masques VLSM.

Adressage privé

L'adressage privé est une autre option souvent citée comme étant plus simple que le développement d'une stratégie d'adressage de zone au moyen de masques de sous-réseaux binaires. Bien que l'adressage privé apporte un excellent niveau de souplesse et ne limite pas la croissance d'un réseau OSPF, il s'accompagne de certains inconvénients. Par exemple, le développement d'un réseau très étendu composé de nœuds dotés d'adresses IP privées empêche toute connexion à l'Internet et nécessite l'implémentation d'une *zone démilitarisée* (DMZ). Lorsque vous avez besoin de vous connecter à l'Internet, la Figure 3.13 illustre de quelle façon une zone démilitarisée peut fournir un tampon de nœuds d'adresses NIC valides entre le réseau mondial et un réseau privé.

NOTE

Reportez-vous au Chapitre 22 pour travailler sur une étude de cas concernant la sécurité de réseau et incluant des informations sur la façon d'installer des routeurs pare-feu et des serveurs de communication.

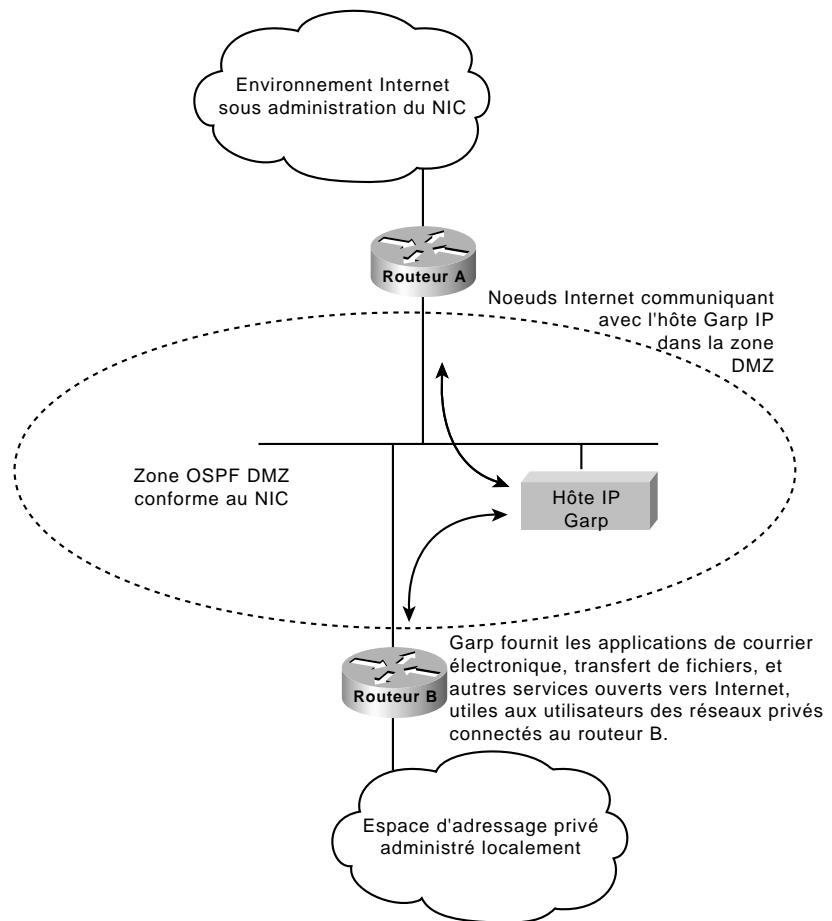
Techniques de synthèse de routes

La synthèse de routes est une fonction particulièrement importante dans un environnement OSPF, car elle améliore la stabilité du réseau. Lorsqu'elle est utilisée, les modifications qui portent sur des routes au sein d'une zone n'ont pas besoin d'être répercutées au niveau de l'épine dorsale ou des autres zones. Cette fonctionnalité renvoie à deux questions importantes concernant la distribution d'informations de routage :

- Quelles sont les informations que l'épine dorsale doit connaître à propos de chaque zone ? La réponse implique les informations de routage transmises des zones vers l'épine dorsale.
- Quelles sont les informations que chaque zone doit connaître à propos de l'épine dorsale et des autres zones ? La réponse concerne les informations de routage transitant de l'épine dorsale vers les zones.

Figure 3.13

Connexion à l'Internet à partir d'un réseau avec adressage privé.



Annonces de routage dans le sens zone-épine dorsale

Plusieurs points essentiels doivent être considérés lors de la définition de la synthèse de routes pour une zone OSPF :

- La synthèse de routes a lieu au niveau des routeurs interzones.
- OSPF supporte VLSM. Il est donc possible d'effectuer une synthèse de routes au niveau d'un bit d'adresse de réseau ou de sous-réseau.
- OSPF nécessite une configuration manuelle de la synthèse. Lorsque vous concevez les zones, vous devez déterminer la synthèse à appliquer sur chaque routeur interzones.

Annonces de routage dans le sens épine dorsale-zone

Il existe quatre types possibles d'informations de routage dans une zone :

- **Par défaut.** Si une route explicite ne peut pas être localisée pour un réseau ou un sous-réseau IP donné, le routeur transmet le paquet vers la destination spécifiée en utilisant l'itinéraire par défaut.

- **Routes intrazone.** Des informations explicites de routes de réseaux ou de sous-réseaux doivent être propagées pour tous les réseaux ou les sous-réseaux se trouvant à l'intérieur d'une zone.
- **Routes interzones.** Une zone peut transporter des informations de routes explicites de réseaux ou de sous-réseaux pour tous les réseaux ou les sous-réseaux qui font partie du système autonome, mais pas de la zone.
- **Routes externes.** Il s'agit des routes dont les informations de routage sont échangées par différents systèmes autonomes.

En général, il est souhaitable de restreindre les informations de routage de n'importe quelle zone à l'ensemble minimal dont elle a besoin. Il existe trois types de zones définies conformément aux informations de routage qu'elles utilisent en interne :

- **Zones non stub.** Les zones non stub transportent une route par défaut, ainsi que des routes statiques, intrazone, interzones et externes. Une zone doit être non stub lorsqu'elle contient un routeur qui utilise à la fois OSPF et n'importe quel autre protocole, tel que RIP. Un tel routeur est appelé routeur intersystèmes autonomes (ASBR, *Autonomous System Border Router*). Une zone doit aussi être non stub lorsqu'un lien virtuel est configuré à travers elle. Ce type de zone consomme davantage de ressources comparé aux autres.
- **Zones stub.** Les zones stub transportent une route par défaut, ainsi que des routes intrazone et interzones, mais pas de routes externes. (Reportez-vous à la section "Contrôle du trafic interzones" plus loin dans ce chapitre pour plus de renseignements sur les compromis de conception de zones avec plusieurs routeurs interzones). L'utilisation de zones stubs est soumise à deux restrictions : les liens virtuels ne peuvent pas être configurés à travers elles et elles ne peuvent pas comprendre de routeur intersystèmes.
- **Zones stub sans synthèse de routes.** Les versions 9.1(11) et 9.2(2) de System Software ainsi que les versions 10.0(1) et plus de Cisco IOS supportent les zones stub sans synthèse de routes, permettant de créer des zones qui ne transportent qu'une route par défaut et des routes intrazone. Les zones stub sans synthèse ne transportent pas d'informations de routes interzones ou externes. Ce type de zone est recommandé pour les configurations simples dans lesquelles un seul routeur connecte une zone à l'épine dorsale.

Le Tableau 3.1 présente les différents types de zones selon les informations de routage qu'elles utilisent :

Tableau 3.1 : Informations de routage utilisées dans les zones OSPF

Type de zone	Route par défaut	Routes intrazone	Routes interzones	Routes externes
Non stub	Oui	Oui	Oui	Oui
Stub	Oui	Oui	Oui	Non
Stub sans synthèse	Oui	Oui	Non	Non

NOTE

Les zones stub sont configurées au moyen de la commande de configuration de routeur : **area id-zone stub**. Les routes sont synthétisées au moyen de la commande de configuration de routeur : **area id-zone range masque_adresse**. Reportez-vous aux manuels *Router Products Configuration Guide* et *Router Products Command Reference*, pour plus d'informations concernant l'utilisation de ces commandes.

Sélection de route OSPF

Lors de la conception d'un réseau OSPF, considérez les trois aspects importants suivants qui contribuent à l'obtention d'une fonction de sélection de route efficace :

- Optimisation des métriques OSPF ;
- Contrôle du trafic interzones ;
- Equilibrage de charge sur un réseau OSPF.

Optimisation des métriques OSPF

La valeur par défaut des métriques utilisées par OSPF se base sur la bande passante. Les caractéristiques suivantes illustrent de quelle façon les métriques sont générées :

- Chaque lien reçoit une valeur de métrique basée sur sa bande passante. La valeur de métrique d'un lien spécifique est l'inverse de celle de sa bande passante. La métrique d'un itinéraire est la somme des métriques de tous les liens traversés.
- Lorsque la synthèse de route est activée, OSPF utilise la métrique du plus mauvais itinéraire dans la synthèse.
- Il existe deux formes de métriques externes : type 1 et type 2. L'utilisation des métriques de type 1 provoque l'ajout de la métrique interne OSPF à la métrique de route externe. Les métriques de type 2 n'ont pas cet effet. La métrique externe de type 1 est généralement utilisée de préférence. Si vous disposez de plus d'une connexion externe, les deux métriques peuvent affecter la façon dont les chemins multiples sont utilisés.

Contrôle du trafic interzones

Lorsqu'une zone ne possède qu'un seul routeur interzones, tout le trafic qui n'appartient pas à la zone passe par lui. Dans les zones comprenant plusieurs routeurs interzones, deux options s'offrent au trafic qui doit quitter la zone :

- Le routeur interzones le plus proche de l'origine du trafic est utilisé (le trafic quitte la zone le plus tôt possible).
- Le routeur interzones le plus proche de la destination du trafic est utilisé (le trafic quitte la zone le plus tard possible).

Si les routeurs interzones n'injectent que la route par défaut, le trafic est transmis au routeur interzones qui est le plus proche de la source. Ce comportement est le plus souvent souhaitable, car l'épine dorsale possède généralement des lignes disponibles avec une bande passante plus élevée. Toutefois, pour que le trafic utilise le routeur interzones situé le plus près de la destination (pour que le

trafic quitte la zone le plus tard possible), les routeurs interzones doivent injecter les synthèses dans la zone au lieu de ne lui transmettre que la route par défaut.

La plupart des concepteurs de réseaux préfèrent éviter un routage asymétrique (c'est-à-dire l'utilisation d'un chemin pour les paquets passant de A vers B différent de celui qu'empruntent les paquets allant de B vers A). Il est important de comprendre de quelle façon le routage se produit entre des zones pour éviter un routage asymétrique.

Equilibrage de charge sur un réseau OSPF

Les topologies de réseau sont généralement conçues pour fournir des routes redondantes afin d'éviter un morcellement du réseau. La redondance permet aussi de bénéficier d'une bande passante supplémentaire dans les zones à fort trafic. S'il existe des chemins de coût égal en direction d'une destination, les routeurs Cisco équilibrivent automatiquement la charge dans un environnement OSPF.

Les routeurs Cisco utilisent jusqu'à quatre chemins de coût égal pour une destination donnée. Le trafic est distribué par rapport à la destination (avec la commutation rapide) ou par rapport aux paquets. L'équilibrage de charge par destination représente le comportement par défaut.

Convergence OSPF

L'une des fonctionnalités les plus attrayantes de OSPF est sa capacité à s'adapter rapidement aux changements de topologie. Deux composantes du protocole participent à la convergence des informations de routage :

- **Détection des changements de topologie.** OSPF utilise deux mécanismes pour détecter les changements qui interviennent au niveau de la topologie. La surveillance des changements d'état d'interface (tels qu'un problème de porteur sur une ligne série) constitue le premier mécanisme. Le second mécanisme est la surveillance de l'échec de réception d'un paquet Hello de la part du voisin au sein d'une fenêtre de temporisation appelée *temporisateur d'inactivité*. Après expiration du temporisateur, le routeur suppose que le routeur voisin est inactif. Le temporisateur est configuré au moyen de la commande de configuration d'interface `ip ospf dead-interval`. La valeur par défaut de ce temporisateur est de quatre fois la valeur de l'intervalle Hello. Cela nous donne une valeur par défaut de 40 secondes pour les réseaux broadcast et de deux minutes pour les réseaux non broadcast.
- **Calcul de routes.** Après qu'un routeur a détecté une panne, il envoie un paquet d'état de lien avec les informations de changement à tous les routeurs situés dans la zone. Tous les routeurs procèdent à un nouveau calcul des itinéraires au moyen de l'algorithme Dykstra (ou SPF). Le temps requis pour l'exécution de l'algorithme dépend d'une combinaison qui prend en compte la taille de la zone et le nombre de routes dans la base de données.

Evolutivité d'un réseau OSPF

L'aptitude d'un réseau OSPF à évoluer dépend de l'ensemble de sa structure et de la stratégie d'adressage utilisée. Comme il a été indiqué dans les sections précédentes concernant la topologie de réseau et la synthèse de routes, l'adoption d'un environnement d'adressage hiérarchique et le respect de règles d'assignation d'adresses structurées représentent les facteurs déterminants de la

capacité de votre réseau à évoluer. Cette adaptabilité est affectée par des considérations fonctionnelles et techniques :

- Sur un plan fonctionnel, un réseau OSPF devrait être conçu de manière que les zones n'aient pas besoin d'être divisées pour s'adapter à sa croissance. L'espace d'adresse devrait être réservé pour autoriser l'ajout de nouvelles zones.
- Sur le plan technique, l'adaptabilité est conditionnée par l'utilisation de trois ressources : mémoire, processeur et bande passante. Ces trois éléments sont traités ci-dessous.

Mémoire

Un routeur OSPF conserve tous les états de liens pour toutes les zones dans lesquelles il se trouve. De plus, il stocke également les synthèses et les routes externes. Un emploi prudent de la synthèse de routes et des zones stub permet de réduire de façon substantielle l'utilisation de la mémoire.

Processeur

Un routeur OSPF utilise les cycles du processeur chaque fois qu'un changement d'état de lien se produit. Le maintien de zones de petite taille et l'emploi de la synthèse de routes réduit de façon considérable l'utilisation des ressources processeur et permet d'obtenir un environnement plus stable.

Bande passante

OSPF envoie des mises à jour partielles chaque fois qu'un changement d'état de lien intervient. Les mises à jour sont envoyées par inondation vers tous les routeurs de la zone. Sur un réseau stable, OSPF est stable lui aussi. Sur un réseau changeant fréquemment, le protocole minimise la quantité de bande passante utilisée.

Sécurité avec OSPF

Deux types de sécurité peuvent être appliqués aux protocoles de routage :

- **Contrôle des routeurs qui participent à un réseau OSPF.** OSPF contient un champ d'authentification optionnel. Tous les routeurs au sein d'une zone doivent s'accorder sur la valeur de ce champ. Comme OSPF est un protocole standard disponible sur de nombreuses plates-formes, y compris sur certains hôtes, l'emploi du champ d'authentification empêche le démarrage accidentel de OSPF sur une plate-forme non contrôlée de votre réseau et réduit le potentiel d'instabilité.
- **Contrôle des informations de routage échangées par les routeurs.** Tous les routeurs doivent détenir les mêmes données au sein d'une zone OSPF. En conséquence, il n'est pas possible d'utiliser des filtres de routes sur un réseau OSPF pour en assurer la sécurité.

Fonctionnalités de la zone NSSA de OSPF

Avant NSSA (*Not-So-Stubby Area*), il fallait définir une zone comme zone stub pour lui éviter de recevoir des annonces d'état de lien (LSA, *Link-State Advertisement*) externes (Type 5). Les routeurs interzones (ABR, *Area Border Router*) qui connectent des zones stub ne les inondent pas avec les informations de routes externes qu'ils reçoivent. Pour renvoyer des paquets vers des destinations en dehors de la zone stub, une route par défaut passant par le routeur interzones est utilisée.

La RFC 1587 définit une zone hybride appelée NSSA. Une telle zone est semblable à une zone stub, mais autorise les fonctionnalités suivantes :

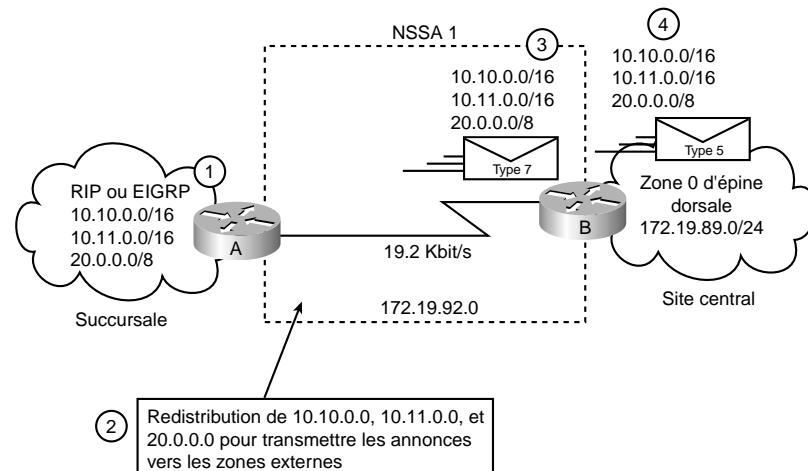
- importation (redistribution) de routes externes en tant qu'annonces LSA Type 7 dans les zones NSSA par les routeurs intersystèmes autonomes (ASBR) de ces zones ;
- traduction d'annonces de routes spécifiques LSA Type 7 en LSA Type 5 par les routeurs interzonaux NSSA.

Utilisation des zones NSSA de OSPF

Utilisez les zones NSSA de OSPF pour synthétiser ou filtrer les annonces LSA Type 5 avant qu'elles ne soient transmises dans une zone OSPF. La spécification de OSPF (RFC 1583) interdit la synthèse ou le filtrage des annonces LSA Type 5. C'est une exigence de OSPF que les annonces de Type 5 soient toujours transmises par inondation à travers le domaine de routage. Lorsque vous définissez une zone NSSA, importez-y des informations de routes externes spécifiques en tant qu'annonces de Type 7. De plus, lors de la traduction des annonces de Type 7 devant être importées dans des zones non stub, synthétisez-les ou filtrez-les avant leur exportation en tant qu'annonces de Type 5.

Dans la Figure 3.14, le site central et la succursale sont interconnectés par l'intermédiaire d'une liaison WAN lente. Le site central utilise OSPF, mais pas la succursale. Au lieu de définir un domaine RIP pour connecter les deux sites, définissez une zone NSSA.

Figure 3.14
Exploitation de zones
NSSA de OSPF.



Dans ce scénario, le routeur A est défini en tant que routeur intersystèmes autonomes. Il est configuré pour redistribuer toutes les routes du domaine RIP/EIGRP vers la zone NSSA. Lorsque la zone entre les deux routeurs de connexion est définie en tant que zone NSSA, voici ce qui se produit :

1. Le routeur A reçoit les informations de routes pour RIP ou EIGRP pour les réseaux 10.10.0.0/16, 10.11.0.0/16 et 20.0.0.0/8.

2. Comme le routeur A est aussi connecté à une zone NSSA, il redistribue les routes RIP ou EIGRP en tant qu'annonces LSA Type 7 vers la zone NSSA.
3. Le routeur B, un routeur interzones entre la zone NSSA et la zone 0 d'épine dorsale, reçoit les annonces LSA Type 7.
4. Après le calcul SPF, le routeur B traduit les annonces Type 7 en annonces Type 5 et les envoie par inondation à travers la zone 0 d'épine dorsale. A cette étape, le routeur B synthétise les routes 10.10.0.0/16 et 10.11.0.0/16 en tant que 10.0.0.0/8 ou filtre les informations d'une ou plusieurs routes.

Caractéristiques des annonces d'état de lien LSA Type 7

Les annonces LSA Type 7 possèdent les caractéristiques suivantes :

- Elles ne sont émises que par les routeurs intersystèmes connectés entre la zone NSSA et le domaine du système autonome.
- Elles incluent un champ d'adresse de transmission. Ce champ est retenu lorsqu'une annonce de Type 7 est traduite en Type 5.
- Elles ne sont transmises qu'au sein d'une zone NSSA.
- Elles ne sont pas envoyées par inondation au-delà d'une zone NSSA. Le routeur interzones qui est connecté à une autre zone non stub, reconvertit les annonces de Type 7 en annonces de Type 5 avant de les envoyer.
- Les routeurs interzones NSSA peuvent être configurés pour synthétiser ou filtrer les annonces de Type 7 et les convertir en annonces de Type 5.
- Les routeurs interzones NSSA transmettent des annonces Type 7 de route par défaut dans la zone NSSA.
- Les annonces Type 7 possèdent une priorité inférieure à celle des annonces Type 5. Aussi, lorsque des informations de route sont recueillies par des annonces Type 5 et Type 7, la route définie dans l'annonce Type 5 est sélectionnée en premier.

Configuration de NSSA de OSPF

La procédure suivante permet de configurer NSSA :

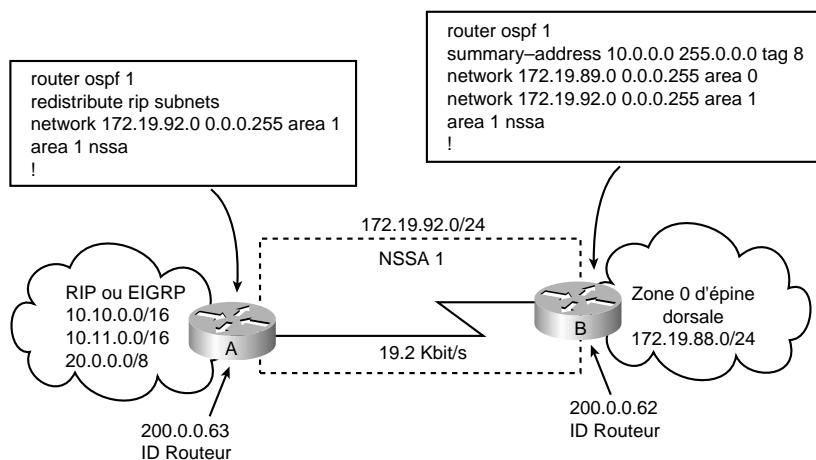
1. Configurez OSPF pour une exploitation standard sur l'interface ou les interfaces qui seront connectées aux zones NSSA.
2. Configurez une zone NSSA au moyen des commandes suivantes :

```
router(config)#area id-zone nssa
```

3. (Optionnel). Contrôlez la synthèse ou le filtrage durant la traduction. La Figure 3.15 illustre de quelle façon un routeur synthétise les routes au moyen de la commande suivante :

```
router(config)#summary-address préfixe masque
[not-advertise] [tag indicateur]
```

Figure 3.15
Configuration de NSSA de OSPF.



Considérations d'implémentation de NSSA

Veillez à examiner ces considérations avant d'implémenter NSSA. Définissez une annonce Type 7 de route par défaut qui peut être utilisée pour atteindre les destinations externes (voir Figure 3.15). Pour cela, la commande à émettre est :

```
router(config)#area id-zone nssa [default-information originate]
```

Lorsqu'il est configuré, le routeur génère une annonce Type 7 de route par défaut dans la zone NSSA via le routeur interzones NSSA. Tous les routeurs d'une même zone doivent accepter la zone NSSA, sinon ils ne seront pas capables de communiquer entre eux.

Si possible, évitez une redistribution explicite sur le routeur interzones NSSA, car vous pourriez ne plus distinguer quels sont les paquets traduits par tel ou tel routeur.

OSPF On-Demand Circuit

OSPF *On-Demand Circuit* (ODC) est une amélioration du protocole OSPF qui est efficace sur les circuits à la demande tels que RNIS, les circuits virtuels commutés (SVC, *Switched Virtual Circuit*) de X.25 et les lignes commutées. Cette fonctionnalité supporte les spécifications du RFC 1793, *Extending OSPF to Support On-Demand Circuits*. Ce RFC est utile pour en comprendre le fonctionnement. Il contient de bons exemples et explique l'exploitation de OSPF dans ce type d'environnement.

Avant l'introduction de OSPF ODC, des messages Hello et LSA périodiques étaient échangés entre des routeurs qui connectaient une ligne à la demande même lorsque aucun changement n'avait lieu.

Avec OSPF ODC, les messages Hello périodiques sont supprimés et les mises à jour d'annonces LSA n'inondent plus les circuits à la demande. Ces paquets provoquent l'ouverture des lignes uniquement lorsqu'il sont échangés la première fois ou lorsqu'il y a une modification dans les informations qu'ils contiennent, permettant ainsi de libérer la connexion au niveau de la couche liaison

de données sous-jacente, lorsque la topologie de réseau est stable, et de maintenir des coûts minimaux pour un circuit à la demande.

OSPF ODC est un mécanisme fondé sur des standards semblables à la fonction Snapshot de Cisco utilisée pour les protocoles à vecteur de distance tels que RIP.

Pourquoi utiliser OSPF On-Demand Circuit ?

Cette fonction est utile pour disposer d'une épine dorsale OSPF sur un site central et permettre à des succursales ou à des travailleurs distants de s'y connecter. Dans ce cas, ODC permet de tirer profit des avantages de OSPF sur l'intégralité du domaine sans entraîner de coûts de connexion excessifs. Les mises à jour périodiques Hello et LSA, ou autres surcharges de protocole, ne sont pas autorisées à déclencher l'activation d'un circuit à la demande lorsqu'il n'y a pas de véritables données à transmettre.

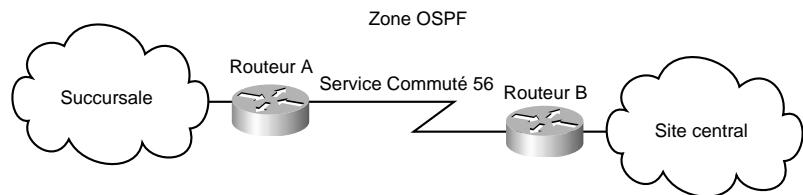
Les protocoles générant des surcharges, du genre paquets Hello et LSA, sont transmis sur le circuit à la demande uniquement lors du démarrage initial et lorsqu'ils reflètent un changement dans la topologie. Cela signifie que les modifications essentielles qui nécessitent de nouveaux calculs SPF sont transmises afin de permettre la maintenance de l'intégrité du réseau, mais les mises à jour périodiques qui n'incluent pas de modifications ne sont pas envoyées sur la ligne.

Fonctionnement de OSPF On-Demand Circuit

La Figure 3.16 illustre le réseau qui servira de base pour la description du fonctionnement général de OSPF sur les circuits à la demande.

Figure 3.16

Zone OSPF.



Les étapes suivantes décrivent la procédure illustrée Figure 3.16 :

1. A l'initialisation, le routeur A établit le circuit à la demande pour échanger les messages Hello et synchroniser les bases de données LSA avec le routeur B. Comme les deux routeurs sont configurés pour gérer OSPF ODC, le bit de circuit à la demande DC (*Demand Circuit*) est activé dans chaque paquet Hello et de description de base de données. En conséquence, les deux routeurs savent qu'ils doivent supprimer les mises à jour de paquets Hello périodiques. Lorsque chaque routeur inonde le réseau de paquets LSA, leur bit DNA (*DoNotAge*) est activé, signifiant que les annonces n'expireront pas. Elles peuvent être mises à jour si de nouvelles annonces sont reçues avec des informations modifiées, mais les mises à jour périodiques ne seront pas transmises sur le circuit à la demande.
2. Lorsque le routeur A reçoit des annonces LSA actualisées pour des entrées existantes dans la base de données, il détermine si elles contiennent des informations modifiées. Si ce n'est pas le

cas, il met à jour les entrées LSA existantes, mais ne transmet pas les informations au routeur B. Par conséquent, les deux routeurs ont les mêmes entrées, mais leurs numéros de séquence d'entrées peuvent ne pas être identiques.

3. Lorsque le routeur A reçoit une annonce LSA pour une nouvelle route, ou qui contient des données modifiées, il met à jour sa base de données LSA, établit le circuit à la demande et envoie les informations vers le routeur B. A cette étape, les deux routeurs possèdent des numéros de séquence identiques pour cette entrée LSA.
4. Lorsqu'il n'y a pas de données à transférer alors que la ligne est ouverte pour des mises à jour, elle est libérée.
5. Lorsqu'un hôte d'un côté ou de l'autre doit transférer des données à un autre hôte sur le site distant, la ligne est établie.

Configuration de OSPF On-Demand Circuit

Les étapes de configuration de OSPF ODC se résument comme suit :

1. Configurez votre circuit à la demande. Par exemple :

```
interface bri 0
ip address 10.1.1.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 3600
dialer map ip name rtra 10.1.1.2 broadcast 1234
dialer group 1
ppp authentication chap
dialer list 1 protocol ip permit
```

2. Activez OSPF de la manière suivante :

```
router(config)#router ospf process-id
```

3. Configurez OSPF ODC avec la commande d'interface suivante :

```
interface bri 0
ip ospf demand-circuit
```

Si le routeur fait partie d'une topologie point-à-point, seule une extrémité du circuit à la demande doit être configurée avec cette commande, mais les deux routeurs doivent avoir la fonctionnalité chargée. Tous les routeurs qui font partie d'une topologie point-multipoint doivent être configurés avec cette commande.

Considérations d'implémentation pour OSPF On-Demand Circuit

Considérez les points suivants avant d'implémenter OSPF ODC :

1. Comme les annonces LSA indiquant des changements de topologie inondent un circuit à la demande, il est conseillé de placer les circuits à l'intérieur de zones stub OSPF ou de zones NSSA afin de les isoler le plus possible des changements de topologie.
2. Pour tirer profit des fonctionnalités d'un circuit à la demande au sein une zone stub ou d'une zone NSSA, chaque routeur dans la zone doit avoir cette fonctionnalité chargée. Si la fonctionnalité est déployée à l'intérieur d'une zone normale, toutes les autres zones normales doivent aussi la supporter pour qu'elle puisse être effective. La raison en est que les annonces LSA inondent l'ensemble des zones.

3. N'activez pas cette fonction sur une topologie de réseau broadcast, car les messages Hello ne peuvent pas être supprimés de façon efficace, ce qui signifie que la ligne sera toujours active.

OSPF sur les réseaux non broadcast

Les réseaux NBMA (*Non Broadcast Multiple Access*) supportent de nombreux routeurs, mais ils ne disposent pas de fonctions broadcast. Sur ce type de réseau, les routeurs voisins sont déterminés au moyen du protocole Hello de OSPF. Toutefois, en raison de cette absence de fonctions broadcast, certaines informations de configuration pourraient se révéler nécessaires pour permettre la découverte des voisins. Les paquets du protocole OSPF qui sont normalement multidestinataires doivent être envoyés tour à tour vers chaque routeur voisin. Un réseau de données public X.25 est un exemple de réseau non broadcast. Notez les points suivants :

- **OSPF s'exécute dans un des deux modes disponibles sur un réseau non broadcast.** Le premier mode, appelé accès multiple non broadcast (sans diffusion) ou NBMA, simule le fonctionnement de OSPF sur un réseau broadcast. Le second mode, appelé point-multipoint, gère le réseau non broadcast comme un ensemble de liens point-à-point. Les réseaux non broadcast sont donc appelés réseaux NBMA ou réseaux point-multipoint, selon le mode OSPF exploité.
- **En mode NBMA, OSPF émule le fonctionnement d'un réseau broadcast.** Un routeur désigné est élu et génère une annonce LSA pour le réseau. La représentation graphique pour les réseaux broadcast et les réseaux non broadcast est identique.

Mode NBMA

Le mode NBMA représente la méthode la plus efficace d'exploitation de OSPF sur un réseau non broadcast, aussi bien en termes de taille de base de données d'état de liens qu'en termes de quantité de trafic généré par le protocole de routage. Toutefois, ce mode souffre d'une restriction significative ; il nécessite que tous les routeurs soient connectés au réseau NBMA pour pouvoir communiquer entre eux. Bien que cette restriction peut être rencontrée sur certains réseaux non broadcast tels qu'un sous-réseau ATM utilisant des circuits virtuels commutés (SVC), on ne la rencontre pas souvent sur les réseaux Frame Relay à circuits virtuels permanents (PVC).

Sur les réseaux non broadcast, les routeurs ne communiquent pas tous directement. Pour permettre une communication directe, divisez le réseau en sous-réseaux logiques. Chaque sous-réseau peut ensuite être exploité comme réseau NBMA ou point-à-point si chaque circuit virtuel est défini en tant que sous-réseau logique séparé. Cette configuration entraîne toutefois une certaine surcharge administrative, et est propice aux erreurs de configuration. Il est probablement préférable d'exploiter un tel réseau non broadcast en mode point-multipoint.

Mode point-multipoint

Les réseaux point-multipoint ont été conçus pour fonctionner simplement et naturellement lorsqu'ils reposent sur une connectivité partiellement maillée. Dans ce mode, OSPF traite toutes les connexions de routeur à routeur sur le réseau non broadcast comme si elles représentaient des liaisons point-à-point. Aucun routeur désigné n'est élu et aucune annonce LSA n'est générée pour le réseau. Il peut se révéler nécessaire de configurer l'ensemble des voisins qui sont directement accessibles à travers le réseau point-multipoint. Sur ce type de réseau, chaque voisin est identifié

par son adresse IP. Comme aucun routeur désigné n'est élu, l'éligibilité des routeurs voisins configurés est indéfinie.

Alternativement, des voisins peuvent être dynamiquement découverts par des protocoles d'un niveau inférieur comme ARP inverse. A la différence des réseaux NBMA, les réseaux point-multipoint présentent les caractéristiques suivantes :

1. Des dépendances sont établies entre tous les routeurs voisins. Il n'y a pas de routeur désigné ou de routeur désigné de secours. Aucune annonce LSA n'est générée pour le réseau. La priorité de routage n'est pas configurée pour les interfaces, ni pour les voisins.
2. Lors de la génération d'une annonce LSA de routeur, l'interface point-multipoint est présentée comme un ensemble de "liens point-à-point" vers l'interface de tous ses voisins adjacents, et possédant en même temps un seul lien stub annonçant l'adresse IP de l'interface avec un coût de 0.
3. Lors d'une inondation sur une interface non broadcast (en mode NBMA ou point-multipoint), le paquet de mise à jour ou d'acquittement d'état de lien doit être reproduit afin d'être envoyé à chacun des voisins de l'interface.

Voici un exemple de configuration de réseau point-multipoint sur un réseau NBMA (*Frame Relay* dans ce cas). La table de routage résultante et les informations d'état de lien de routeur, ainsi que d'autres données pertinentes suivent également :

```

interface Ethernet0
  ip address 130.10.6.1 255.255.255.0
!
interface Serial0
  no ip address
  encapsulation frame-relay
  frame-relay lmi-type ansi
!
interface Serial0.1 multipoint
  ip address 130.10.10.3 255.255.255.0
  ip ospf network point-to-multipoint
  ip ospf priority 10
  frame-relay map ip 130.10.10.1 140 broadcast
  frame-relay map ip 130.10.10.2 150 broadcast
!
router ospf 2
  network 130.10.10.0 0.0.0.255 area 0
  network 130.10.6.0 0.0.0.255 area 1

R6#sh ip ospf int s 0.1
Serial0.1 is up, line protocol is up
  Internet Address 130.10.10.3/24, Area 0
  Process ID 2, Router ID 140.10.1.1, Network Type POINT_TO_MULTIPOINT,
    Cost: 6,
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
  Hello due in 00:00:18
  Neighbor Count is 2, Adjacent neighbor count is 2
  Adjacent with neighbor 130.10.10.2
  Adjacent with neighbor 130.10.5.129

R6#sh ip ospf ne
      Neighbor ID      Pri      State     Dead Time     Address          Interface
  130.10.10.2        0      FULL/   00:01:37    130.10.10.2

```

```

130.10.5.129      0          FULL/ -00:01:53      130.10.10.1      Serial0.1
R6#


R6#sh ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
      U - per-user static route

Gateway of last resort is not set

130.10.0.0/16 is variably subnetted, 9 subnets, 3 masks
O    130.10.2.32 [110/64] via 130.10.10.2, 00:03:28, Serial0.1
C    130.10.10.0/24 is directly connected, Serial0.1
O    130.10.10.1/32 [110/64] via 130.10.10.1, 00:03:28, Serial0.1
O IA  130.10.0.0/22 [110/74] via 130.10.10.1, 00:03:28, Serial0.1
O    130.10.4.0/24 [110/74] via 130.10.10.2, 00:03:28, Serial0.1
C    130.10.6.0/24 is directly connected, Ethernet0

R6#sh ip ospf data router 140.10.1.1

OSPF Router with ID (140.10.1.1) (Process ID 2)

Router Link States (Area 0)

LS age: 806
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 140.10.1.1
Advertising Router: 140.10.1.1
LS Seq Number: 80000009
Checksum: 0x42C1
Length: 60
Area Border Router
Number of Links: 3

Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 130.10.10.2
(Link Data) Router Interface address: 130.10.10.3
Number of TOS metrics: 0
TOS 0 Metrics: 64

Link connected to: another Router (point-to-point)
(Link ID) Neighboring Router ID: 130.10.5.129
(Link Data) Router Interface address: 130.10.10.3
Number of TOS metrics: 0
TOS 0 Metrics: 64

Link connected to: a Stub Network
(Link ID) Network/subnet number: 130.10.10.3
(Link Data) Network Mask: 255.255.255.255
Number of TOS metrics: 0
TOS 0 Metrics: 0

```

Routage à la demande (ODR, On-Demand Routing)

Le mécanisme de routage à la demande, ou ODR (*On-Demand Routing*), permet de router IP avec une surcharge minimale au niveau des sites stub. La surcharge liée à un protocole de routage dynamique typique est ainsi évitée, sans pour autant entraîner une surcharge additionnelle due à la configuration et la gestion du routage statique.

Le terme *routeur stub* désigne un routeur de périphérie sur une topologie de réseau hub-and-spoke. Un routeur stub possède généralement une connexion WAN vers le routeur hub et un petit nombre de segments LAN (réseaux stub) qui lui sont directement connectés. Pour mettre en œuvre une connectivité totale, configurez statiquement un routeur hub afin de lui indiquer un réseau stub particulier accessible par l'intermédiaire d'un routeur d'accès spécifié. Lorsqu'il existe plusieurs routeurs hub, de nombreux réseaux stub, ou des connexions asynchrones entre les sites centraux (*hubs*) et les sites distants (*spokes*), la surcharge induite par la configuration statique des informations de réseaux stub sur les routeurs hub devient trop importante.

ODR autorise les routeurs stub à annoncer leurs réseaux stub connectés au moyen du protocole CDP (*Cisco Discovery Protocol*).

ODR requiert que les routeurs stub soient configurés statiquement avec des routes par défaut pointant vers les routeurs hub. Ces derniers sont configurés pour accepter les réseaux stub distants *via* CDP. Une fois que ODR a été activé sur un routeur hub, celui-ci commence à enregistrer les routes de réseaux stub dans la table de transmission IP. Le routeur hub peut également être configuré pour redistribuer ces routes dans n'importe quel protocole de routage pour IP dynamique configuré. Aucun protocole de routage pour IP n'est configuré sur les routeurs stub. Avec ODR, un routeur est automatiquement considéré comme étant un routeur stub lorsque aucun protocole de routage pour IP n'a été configuré dessus. Voici une commande de configuration ODR requise sur un routeur hub :

```
router odr
```

Aucune configuration n'est nécessaire sur les routeurs distants, car CDP est activé par défaut.

Avec la technologie Frame Relay, une configuration de sous-interface point-à-point peut être utilisée sur le nuage Frame Relay, car les routeurs distants sont configurés avec des routes statiques pointant de l'autre côté du nuage, c'est-à-dire vers l'adresse IP du routeur hub. Lorsque le circuit virtuel permanent entre le routeur distant et le routeur hub devient inactif, la sous-interface point-à-point n'est plus exploitable et la route statique par défaut n'est plus valide. Si une configuration point-multipoint est utilisée, l'interface sur le nuage reste accessible lorsqu'un circuit virtuel permanent est inactif et la route statique par défaut reste valide.

Avantages de ODR

ODR présente les avantages suivants :

- ODR est un mécanisme qui permet de router IP avec une surcharge minimale au niveau des sites stub. La surcharge liée à un protocole de routage dynamique typique est ainsi évitée, sans pour autant entraîner une surcharge additionnelle due à la configuration et la gestion du routage statique.
- ODR simplifie l'implémentation de réseaux stub IP puisque les routeurs hub maintiennent dynamiquement des routes vers ces réseaux. Pour cela, il n'est pas nécessaire de configurer un protocole de routage pour IP sur les routeurs stub. Avec ODR, le routeur stub annonce les préfixes IP

correspondant aux réseaux IP configurés sur les interfaces qui lui sont directement connectées. Comme ODR annonce les préfixes IP à la place des adresses de réseau IP, il peut transporter des informations de masques de sous-réseaux de longueur variable (VLSM).

- ODR limite la surcharge de configuration et de bande passante liée à une connectivité de routage totale. De plus, il élimine le besoin de configurer un protocole de routage pour IP sur les routeurs stub.

Remarques sur l'utilisation de ODR

Tenez compte des éléments suivants lorsque vous utilisez ODR :

- ODR propage les routes entre les routeurs au moyen du protocole CDP. Par conséquent, ODR est partiellement contrôlé par la configuration de CDP. Si CDP est désactivé, la propagation des informations de routage par ODR cesse.
- Par défaut, CDP envoie des mises à jour toutes les 60 secondes. Cet intervalle n'est parfois pas assez court pour permettre une convergence rapide, auquel cas il faut envisager de modifier sa valeur.
- Il est conseillé de limiter le nombre d'interfaces sur le hub.
- Au moment de l'écriture de cet ouvrage, CDP n'était pas supporté sur les réseaux ATM.

Résumé

Nous avons vu dans ce chapitre que les implications de l'utilisation des protocoles EIGRP et OSPF pour la conception de réseaux IP étendus portent sur les aspects suivants :

- topologie de réseau ;
- adressage et synthèse de routage ;
- sélection de route ;
- convergence ;
- évolutivité du réseau ;
- sécurité.

Ce chapitre a également abordé le mécanisme de routage à la demande, ou ODR, qui présente le principal avantage d'éliminer une grande partie de la surcharge liée au routage du protocole IP.

4

Conception de réseaux IP étendus avec BGP

Par Atif Khan

Le protocole BGP (*Border Gateway Protocol*) est un protocole de routage intersystème autonome (AS, *Autonomous System*). La principale fonction d'un système qui utilise ce protocole est d'échanger des informations d'accessibilité de réseau avec d'autres systèmes BGP. Ces informations incluent la liste des systèmes autonomes qu'elles traversent. BGP 4 fournit un ensemble de mécanismes permettant de supporter le routage interdomaine sans distinction de classe ou CIDR (*Classless InterDomain Routing*). Ces mécanismes comprennent la gestion d'annonce de préfixe IP et éliminent le concept de *classe* de réseau au sein de BGP. BGP 4 introduit aussi des fonctionnalités qui permettent la formation d'agrégats de routes, incluant les agrégats de chemins d'AS. Ces changements permettent de supporter la stratégie de super-réseau proposée. Ce chapitre décrit le fonctionnement de BGP et la façon dont il peut être utilisé pour participer au processus de routage avec d'autres réseaux qui l'exploitent également. Les sujets suivants seront abordés :

- fonctionnement de BGP ;
- attributs de BGP ;
- critères de sélection de chemin BGP ;
- compréhension et définition des stratégies de routage BGP.

Fonctionnement de BGP

A travers les sujets suivants, cette section présente les informations de base relatives à BGP :

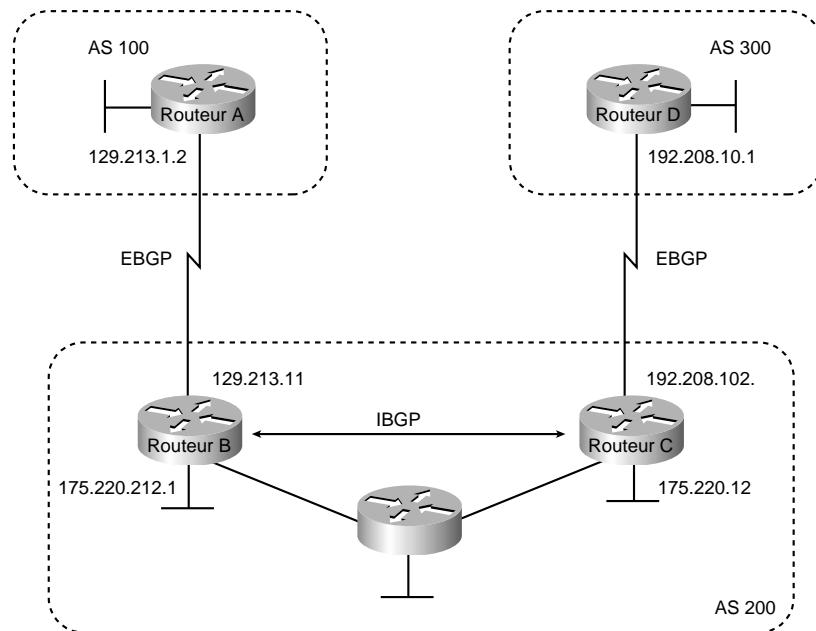
- BGP interne (IBGP) ;

- BGP externe (EBGP) ;
- BGP et cartes de routage ;
- annonces de réseaux.

Les routeurs qui appartiennent au même système autonome et qui échangent des mises à jour BGP exécutent le protocole BGP interne (IBGP, *Internal BGP*) et ceux qui appartiennent à des systèmes autonomes différents et qui échangent également des mises à jour BGP exécutent le protocole BGP externe (EBGP, *External BGP*).

A l'exception de la commande de voisin **ebgp-multihop**, les commandes de configuration de EBGP et IBGP sont identiques. Ce chapitre utilise les termes EBGP et IBGP pour rappeler que, dans un contexte particulier, les mises à jour sont échangées entre plusieurs AS (EBGP) ou à l'intérieur d'un même AS (IBGP). La Figure 4.1 présente un réseau qui illustre la différence entre ces deux protocoles.

Figure 4.1
EBGP, IBGP et
plusieurs systèmes
autonomes.



Avant d'échanger des informations avec un AS externe, BGP s'assure que les réseaux qu'il inclut sont accessibles. Pour cela, il s'appuie sur le peering des routeurs IBGP au sein de l'AS et sur la redistribution des informations de routage BGP vers les protocoles de routeurs internes (IGP, *Interior Gateway Protocol*) qui s'exécutent au sein de l'AS, tels que IGRP (*Interior Gateway Routing Protocol*), IS-IS (*Intermediate System-to-Intermediate System*), RIP (*Routing Information Protocol*), et OSPF (*Open Shortest Path First*).

BGP utilise TCP (*Transmission Control Protocol*) comme protocole de transport (plus précisément, le port 179). Deux routeurs ayant établi une connexion TCP afin d'échanger des informations de

routage sont désignés par le terme *homologues (peer)* ou *voisins (neighbor)*. Dans le cas de la Figure 4.1, les routeurs A et B sont des homologues BGP, de même que les routeurs B et C, ou C et D. Les informations de routage consistent en une série de numéros de AS qui décrivent le chemin complet vers le réseau de destination. BGP les exploite pour construire une carte exempte de boucle de AS. Notez que, au sein d'un AS, les homologues BGP n'ont pas besoin d'être directement connectés.

Les homologues BGP échangent au départ leurs tables de routage BGP complètes. Ensuite, seules les mises à jour différentielles sont envoyées. Ils échangent aussi des messages *keepalive* pour vérifier l'activité des lignes ainsi que des messages de notification en réponse à des erreurs ou des conditions spéciales.

NOTE

A la Figure 4.1, les routeurs A et B exécutent EBGP et les routeurs B et C utilisent IBGP. Notez que les homologues EBGP sont directement connectés, mais pas les homologues IBGP. Dès lors qu'un protocole IGP est exécuté, permettant ainsi à deux voisins de communiquer, les homologues IBGP n'ont pas besoin d'être directement connectés.

Tous les nœuds supportant BGP au sein d'un AS doivent établir une relation d'homologues entre eux, c'est-à-dire qu'ils doivent être totalement maillés logiquement. Pour cela, BGP 4 fournit deux méthodes : les *confédérations* et les *réflecteurs de routes*. Pour plus d'informations sur ces sujets, reportez-vous aux sections "Confédérations" et "Réflecteurs de routes" de ce chapitre.

L'AS 200 est un système autonome de transit pour les AS 100 et 300. Il sert en fait à transférer des paquets entre ces deux derniers.

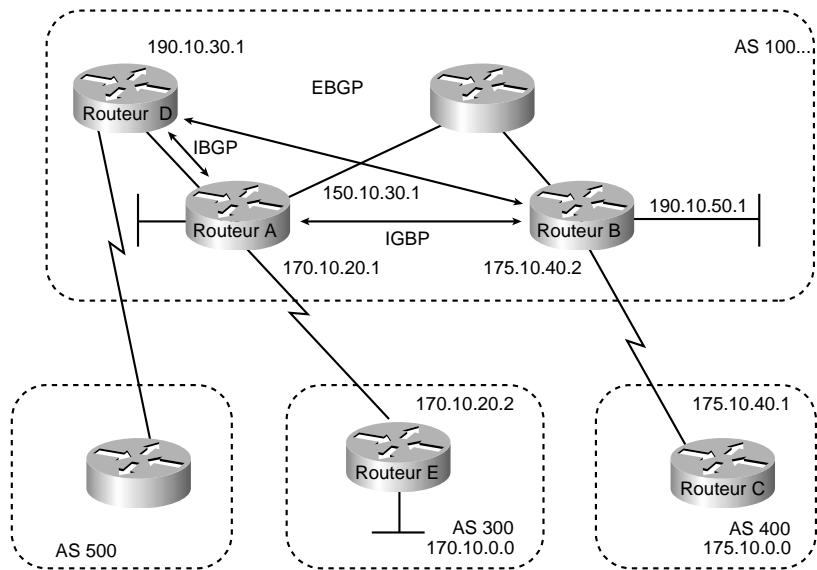
BGP interne (IBGP)

Le protocole IBGP est une forme de BGP qui échange des mises à jour BGP au sein d'un AS. Au lieu de passer par IBGP, les informations de routes recueillies via EBGP pourraient être redistribuées vers IGP dans l'AS puis à nouveau redistribuées dans un autre AS. Mais IBGP est plus souple et évolutif et fournit davantage de mécanismes pour contrôler efficacement l'échange d'informations dans l'AS. Il présente aussi une vue cohérente de l'AS aux voisins externes. Par exemple, il fournit des méthodes pour contrôler le point de sortie d'un AS. La Figure 4.2 présente une topologie qui illustre le fonctionnement de ce protocole.

Lorsqu'un routeur BGP reçoit une mise à jour de la part d'autres routeurs BGP de son propre AS (c'est-à-dire via IBGP), il utilise EBGP pour la transmettre aux routeurs BGP externes seulement. Ce comportement de IBGP justifie la nécessité d'un maillage total des routeurs BGP au sein d'un même AS.

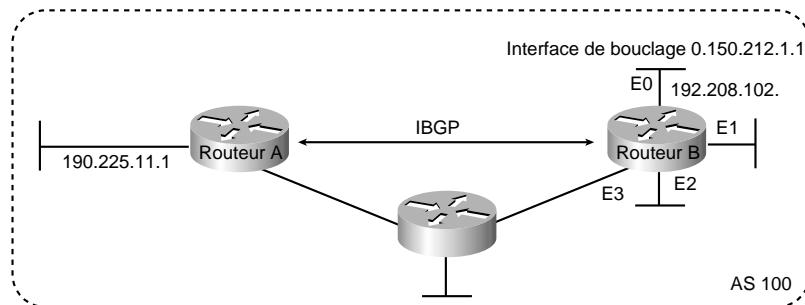
Par exemple, examinez la Figure 4.2. S'il n'existe pas de session IBGP entre les routeurs B et D, le routeur A enverrait les mises à jour provenant du routeur B vers le routeur E, mais pas vers le routeur D. Pour que D reçoive les mises à jour en provenance de B, ce dernier doit être configuré pour reconnaître D comme homologue BGP.

Figure 4.2
Exemple d'exploitation de IBGP.



Les interfaces de bouclage sont souvent utilisées par les homologues IBGP. L'avantage de ces interfaces est qu'elles permettent d'éliminer une dépendance qui, sinon, pourrait se produire lorsque vous employez l'adresse IP d'une interface physique pour configurer BGP. La Figure 4.3 illustre un réseau dans lequel l'utilisation d'une interface de bouclage est avantageuse.

Figure 4.3
L'emploi d'interfaces de bouclage.



Dans le cas de la Figure 4.3, les routeurs A et B exécutent IBGP dans l'AS 100. Si le routeur A devait spécifier l'adresse IP de l'interface Ethernet 0, 1, 2, ou 3 dans la commande **neighbor remote-as**, et que l'interface en question ne soit pas disponible, le routeur A ne serait pas en mesure d'établir une connexion TCP avec le routeur B. Au lieu de cela, A spécifie l'adresse IP de l'interface de bouclage définie par B. Lorsque l'interface de bouclage est utilisée, BGP n'a pas besoin de s'appuyer sur la disponibilité d'une interface particulière pour établir des connexions TCP.

NOTE

Les interfaces de bouclage sont rarement utilisées entre des homologues EBGP, car ils sont généralement directement connectés et dépendent par conséquent d'une interface spécifique pour la connectivité.

BGP externe (EBGP)

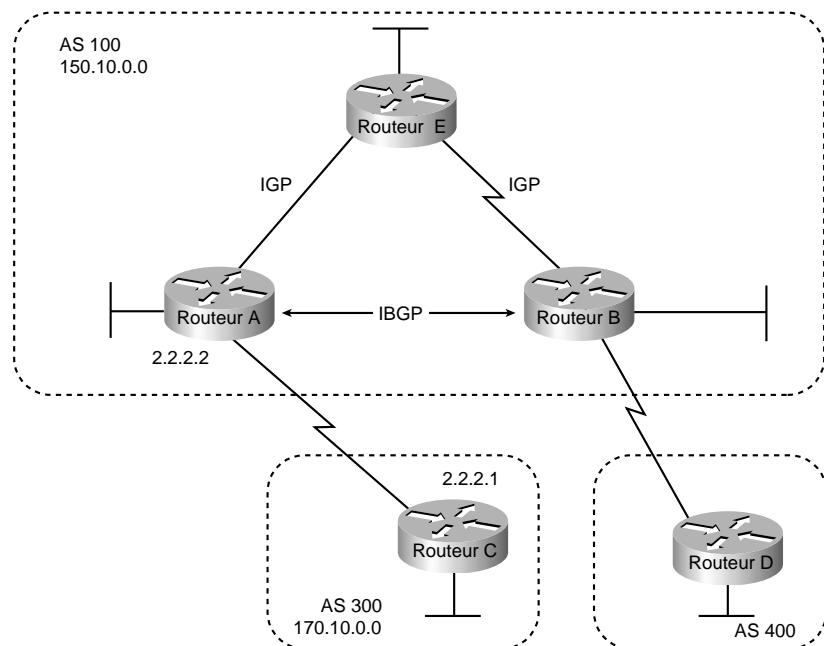
Lorsque deux routeurs BGP situés dans des systèmes autonomes différents échangent des informations de routage BGP, ils utilisent EBGP.

Synchronisation

Lorsqu'un AS assure un service de transit pour d'autres AS alors que ses routeurs ne supportent pas BGP, le trafic de transit risque d'être ignoré, si ces routeurs intermédiaires n'ont pas pris connaissance d'itinéraires praticables pour ce trafic *via* un protocole IGP. La règle de synchronisation de BGP stipule que, si un AS fournit un service de transit à un autre AS, BGP ne devrait pas annoncer de route tant que tous les routeurs au sein de l'AS de transit n'ont pas pris connaissance de la route *via* un protocole IGP. La topologie de la Figure 4.4 illustre cette règle de synchronisation.

A la Figure 4.4, le routeur C envoie des mises à jour concernant le réseau 170.10.0.0 au routeur A. Les routeurs A et B exécutent IBGP, aussi B peut recevoir des mises à jour à propos du réseau en question *via* IBGP. Si le routeur B souhaite atteindre ce réseau, il envoie le trafic au réseau E. Si A ne redistribuait pas les informations concernant ce réseau *via* un protocole IGP, le routeur E n'aurait aucun moyen de connaître l'existence du réseau et ignorerait par conséquent les paquets.

Figure 4.4
Règle de
synchronisation
EBGP.



Si le routeur B annonce au système autonome 400 qu'il peut atteindre le réseau 170.10.0.0 avant que le routeur E n'en prenne connaissance *via* IGP, le trafic en provenance de D vers B à destination 170.10.0.0 circulera vers E et sera ignoré.

La situation est gérée par la règle de synchronisation de BGP décrite précédemment. Dans le cas de notre figure, comme l'AS 100 est le système autonome de transit, le routeur B doit attendre de recevoir des informations concernant le réseau 170.10.0.0 *via* un IGP avant d'envoyer une mise à jour au routeur D.

Désactivation de la synchronisation

Dans certains cas, vous pourriez avoir besoin de désactiver la synchronisation. Cette action permet au protocole BGP de converger plus rapidement, mais peut également entraîner la perte de paquets en transit. Vous pouvez la désactiver dans l'une des situations suivantes :

- Votre AS ne sert pas de système de transit entre deux autres AS.
- Tous les routeurs de transit dans l'AS exécutent BGP.

BGP et cartes de routage

Les cartes de routage sont utilisées avec le protocole BGP pour contrôler et modifier les informations de routage et pour définir les conditions suivant lesquelles les routes sont redistribuées entre les domaines de routage. La configuration d'une carte de routage implique la syntaxe suivante :

```
route-map nom-carte [[permit | deny] | [numéro-séquence]]
```

L'argument *nom-carte* est un nom qui identifie la carte de routage et l'argument *numéro-séquence* indique la position qu'une instance de carte de routage doit avoir par rapport aux autres instances de la même carte, les instances étant ordonnées séquentiellement. Par exemple, vous pouvez utiliser les commandes suivantes pour définir une carte de routage nommée MACARTE :

```
route-map MACARTE permit 10
! Place du premier ensemble de conditions.
route-map MACARTE permit 20
! Place du second ensemble de conditions.
```

Lorsque BGP applique MACARTE aux mises à jour de routage, il applique d'abord la première instance (dans ce cas, l'instance 10). Si le premier ensemble de conditions n'est pas satisfait, le deuxième est appliqué, et ainsi de suite jusqu'à ce qu'un ensemble de conditions soit satisfait ou qu'il n'y en ait plus à appliquer.

Les commandes de configuration **match** et **set route map** servent à définir la portion conditionnelle de la carte. La commande **match** spécifie un critère pour lequel une correspondance doit être trouvée, et la commande **set** spécifie une action qui doit être exécutée si la mise à jour de routage satisfait aux conditions définies par la commande **match**. Voici un exemple de configuration d'une carte de routage simple :

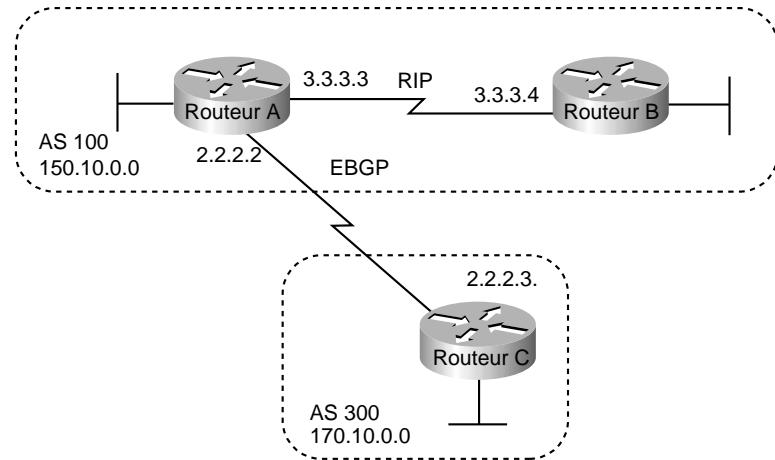
```
route-map MACARTE permit 10
match ip address 1.1.1.1
set metric 5
```

Si une mise à jour correspond à l'adresse 1.1.1.1, BGP définit la métrique de la mise à jour à 5, transmet cette dernière (en raison du mot clé **permit**), puis interrompt l'évaluation des instances de la liste. Comme indiqué précédemment, le protocole BGP applique les instances les unes après les

autres jusqu'à ce qu'une action soit entreprise ou qu'il n'y ait plus d'instances de carte de routage à appliquer. Si la mise à jour ne correspond à aucun critère, elle n'est ni redistribuée ni contrôlée.

Quand une mise à jour satisfait à une condition et que la carte de routage spécifie le mot clé **deny**, BGP interrompt l'évaluation de la liste d'instances et la mise à jour n'est ni redistribuée ni contrôlée. La Figure 4.5 présente une topologie qui illustre l'utilisation d'une carte de routage.

Figure 4.5
Exemple de carte de routage.



A la Figure 4.5, les routeurs A et B communiquent *via* RIP et les routeurs A et C *via* BGP. Si vous voulez que le routeur A redistribue les routes du réseau 170.10.0.0 avec une métrique de 2, et toutes les autres routes avec une métrique de 5, utilisez les commandes suivantes sur le routeur A :

```

!Routeur A
router rip
network 3.0.0.0
network 2.0.0.0
network 150.10.0.0
passive-interface serial 0
redistribute bgp 100 route-map SETMETRIC
!
router bgp 100
neighbor 2.2.2.3 remote-as 300
network 150.10.0.0
!
route-map SETMETRIC permit 10
match ip-address 1
set metric 2
!
route-map SETMETRIC permit 20
set metric 5
!
access-list 1 permit 170.10.0.0 0.0.255.255

```

Lorsqu'une route correspond à l'adresse IP 170.10.0.0, elle est redistribuée avec une métrique de 2. Lorsqu'il n'y a pas de correspondance, sa métrique est définie à 5 et la route est redistribuée.

Supposez que vous vouliez définir à 300 l'attribut de communauté des mises à jour sortantes concernant le réseau 170.10.0.0 sur le routeur C. Les commandes suivantes appliquent une carte de routage aux mises à jour sortantes sur le routeur C :

```
!Routeur C
router bgp 300
network 170.10.0.0
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 route-map SETCOMMUNITY out
!
route-map SETCOMMUNITY permit 10
match ip address 1
set community 300
!
access-list 1 permit 0.0.0.0 255.255.255.255
```

La liste d'accès 1 rejette toutes les mises à jour pour le réseau 170.10.0.0 et les autorise pour tout autre réseau.

Annonces de réseaux

Un réseau situé sur un système autonome est dit originaire de ce réseau. Pour informer les autres AS de l'existence de ses réseaux, un AS les annonce. Pour cela, BGP offre trois méthodes :

- redistribution de routes statiques ;
- redistribution de routes dynamiques ;
- utilisation de la commande **network**.

Cette section utilise la topologie illustrée Figure 4.6 pour démontrer de quelle façon les réseaux originaires d'un système autonome peuvent être annoncés.

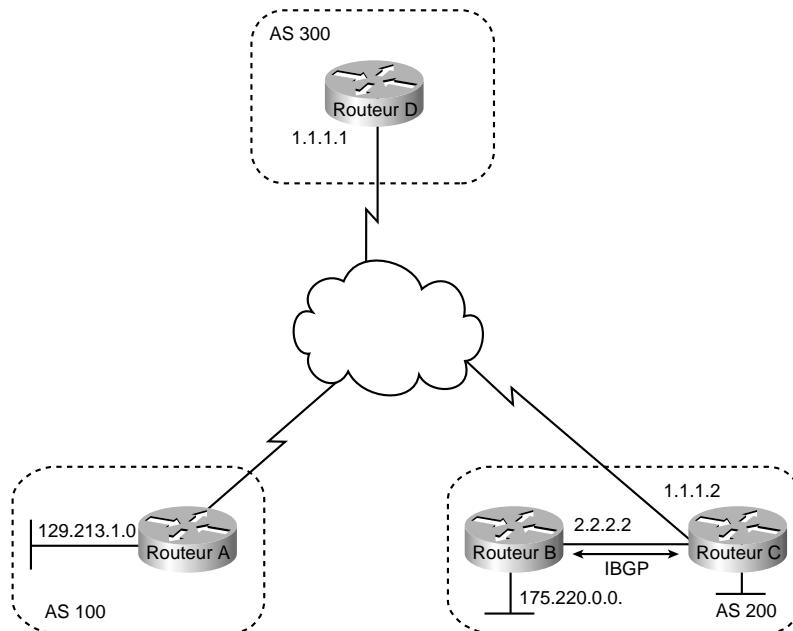
Redistribution de routes statiques

Une façon d'annoncer qu'un réseau ou un sous-réseau est originaire d'un AS est de redistribuer les routes statiques dans BGP. La seule différence entre l'annonce d'une route statique et celle d'une route dynamique se situe au niveau de la redistribution. Dans le cas d'une route statique, BGP définit l'attribut d'origine des mises à jour pour cette route avec la valeur **Incomplete** (pour plus d'informations sur les autres valeurs qui peuvent être assignées à un attribut d'origine, reportez-vous à la section "Attribut d'origine" de ce chapitre). Pour configurer le routeur C de la Figure 4.6 afin d'annoncer l'origine du réseau 175.220.0.0 dans BGP, utilisez les commandes suivantes :

```
!Routeur C
router bgp 200
neighbor 1.1.1.1 remote-as 300
redistribute static
!
ip route 175.220.0.0 0.0.255.255 null 0
```

La commande **redistribute** et le mot clé **static** provoquent la redistribution de toutes les routes statiques dans BGP. La commande **ip route** établit une route statique pour le réseau 175.220.0.0. En théorie, la spécification de l'interface **null 0** entraînerait la suppression d'un paquet à destination du réseau 175.220.0.0. Dans la pratique, il y aurait une correspondance plus spécifique pour le paquet que cette adresse et le routeur l'enverrait sur l'interface appropriée. La redistribution d'une route statique est la meilleure méthode pour annoncer l'origine d'un réseau, car elle prévient l'instabilité de route.

Figure 4.6
Exemple 1 d'annonce de réseau.



NOTE

En dépit du type de route (statique ou dynamique), la commande **redistribute** est la seule méthode permettant d'injecter les informations de route BGP dans un IGP.

Redistribution de routes dynamiques

Une autre méthode permettant d'annoncer des réseaux consiste à redistribuer des routes dynamiques. Généralement, vous redistribuez des routes IGP (telles que les routes EIGRP, IGRP, IS-IS, OSPF, et RIP) dans BGP. Comme certaines des informations de routes IGP peuvent avoir été reçues de BGP, vous devez utiliser des listes d'accès pour empêcher la redistribution en amont vers la source BGP. Dans le cas de la Figure 4.6, supposez que les routeurs B et C exécutent IBGP, que le routeur C prenne connaissance du réseau 129.213.1.0 via BGP et que le routeur B redistribue en amont dans EIGRP les informations concernant le réseau 129.213.1.0. Les commandes suivantes configurent le routeur C :

```

!Routeur C
router eigrp 10
network 175.220.0.0
redistribute bgp 200
redistributed connected
default-metric 1000 100 250 100 1500
!
router bgp 200
neighbor 1.1.1.1 remote-as 300
neighbor 2.2.2.2 remote-as 200

```

```

neighbor 1.1.1.1 distribute-list 1 out
redistribute eigrp 10
!
access-list 1 permit 175.220.0.0 0.0.255.255

```

La commande **redistribute** avec le mot clé **eigrp** redistribue les routes EIGRP pour l'identifiant de processus 10 dans BGP (normalement, la distribution de BGP dans IGP devrait être évitée, car trop d'informations de routes seraient injectées dans le système autonome). La commande **neighbor** **distribute-list** applique la liste d'accès 1 aux annonces sortantes en direction du voisin dont l'adresse IP est 1.1.1.1 (c'est-à-dire, le routeur D). La liste d'accès 1 spécifie que le réseau 175.220.0.0 doit être annoncé. Tous les autres réseaux, comme celui d'adresse 129.213.1.0, sont empêchés implicitement d'être annoncés. La liste d'accès empêche ainsi le réseau 129.213.1.0 d'être réinjecté en amont dans BGP comme s'il provenait de l'AS 200 et permet à BGP d'annoncer le réseau 175.220.0.0 comme étant originaire de cet AS.

Utilisation de la commande *network*

Une autre méthode d'annonce des réseaux consiste à utiliser la commande **network**. Lorsqu'elle est utilisée avec BGP, elle spécifie les réseaux originaires du système autonome. En comparaison, lorsqu'elle est employée avec un protocole de routage interne (IGP), comme RIP, elle permet d'identifier les interfaces sur lesquelles le protocole IGP doit être exécuté. Cette commande fonctionne pour les réseaux dont les informations sont acquises dynamiquement par le routeur ou qui sont configurés sous forme de routes statiques. L'attribut d'origine des routes qui sont injectées dans BGP au moyen de cette commande est défini avec la valeur **IGP**. Les commandes suivantes configurent le routeur C pour annoncer le réseau 175.220.0.0 :

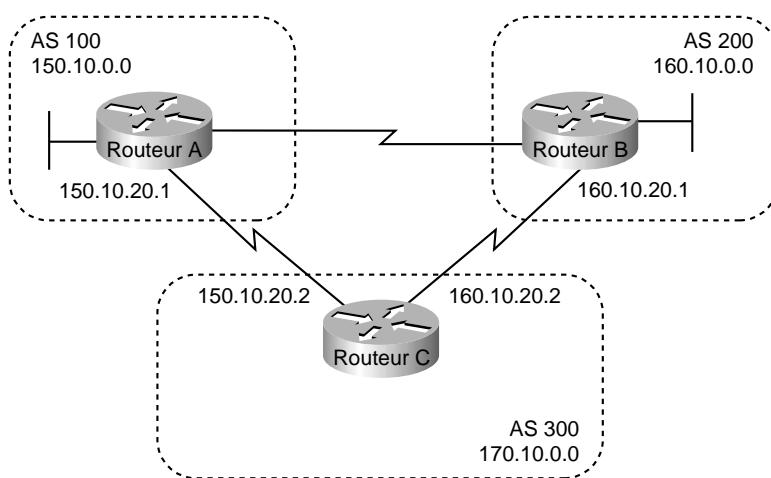
```

!Routeur C
router bgp 200
neighbor 1.1.1.1 remote-as 300
network 175.220.0.0

```

Avec la commande **network**, le routeur C génère une entrée pour le réseau 175.220.0.0 dans la table de routage BGP. La Figure 4.7 présente une autre topologie qui illustre les effets de cette commande.

Figure 4.7
Exemple 2 d'annonce de réseau.



La commande **network** est utilisée ici pour configurer les routeurs présentés à la Figure 4.7 :

```
!Routeur A
router bgp 100
neighbor 150.10.20.2 remote-as 300
network 150.10.0.0
!Routeur B
router bgp 200
neighbor 160.10.20.2 remote-as 300
network 160.10.0.0
!Routeur C
router bgp 300
neighbor 150.10.20.1 remote-as 100
neighbor 160.10.20.1 remote-as 200
network 170.10.0.0
```

Pour garantir une topologie interdomaine exempte de boucle, BGP n'accepte pas les mises à jour qui proviennent de son propre AS. Par exemple, à la Figure 4.7, si le routeur A génère une mise à jour pour le réseau 150.10.0.0 avec comme origine l'AS 100 et l'envoie au routeur C, celui-ci la transmettra au routeur B avec la même origine. Le routeur B enverra la mise à jour, toujours avec la même origine, vers le routeur A, qui reconnaîtra son propre AS et l'ignorera.

Attributs de BGP

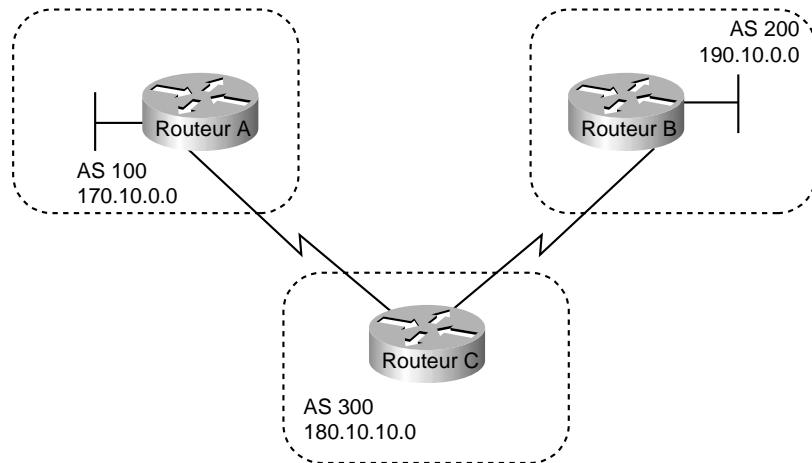
Lorsqu'un routeur BGP reçoit des mises à jour en provenance de plusieurs systèmes autonomes qui décrivent différents chemins vers une même destination, il doit choisir le meilleur et unique itinéraire pour l'atteindre, puis le propager vers ses voisins. La décision est fondée sur la valeur des attributs (comme le prochain saut, les poids administratifs, la préférence locale, l'origine de la route et la longueur du chemin) que la mise à jour contient, ainsi que sur d'autres facteurs configurables par BGP. Cette section décrit les attributs et les facteurs que ce protocole utilise dans son processus de prise de décision :

- attribut de chemin de système autonome (AS_path) ;
- attribut d'origine (Origin) ;
- attribut de prochain saut (Next Hop) ;
- attribut de poids (Weight) ;
- attribut de préférence locale (Local Preference) ;
- attribut de préférence d'accès AS (Multi-Exit Discriminator) ;
- attribut de communauté (Community).

Attribut de cheminement (AS_path)

Chaque fois qu'une mise à jour transite par un AS, BGP y ajoute son numéro d'AS. L'attribut AS_path de la mise à jour représente une liste des numéros de tous les AS qu'elle a traversés pour atteindre une destination. Un AS-SET est un ensemble mathématique de tous les AS qui ont été traversés. Observez cela sur le réseau illustré Figure 4.8.

Figure 4.8
Attribut de cheminement AS_path.



Attribut d'origine (Origin)

Cet attribut donne des informations sur l'origine de la route. Il peut prendre l'une des valeurs suivantes :

- **IGP.** La route se trouve au sein de l'AS d'origine. Cette valeur est définie lorsque la commande **network** est utilisée pour injecter la route dans BGP. Le type d'origine **IGP** est représenté par la lettre **i** dans la sortie de la commande EXEC **show ip bgp**.
- **EGP.** La route est apprise *via* le protocole de routage externe EGP. Le type d'origine **EGP** est représenté par la lettre **e** dans la sortie de la commande EXEC **show ip bgp**.
- **Incomplete.** L'origine de la route est inconnue ou apprise d'une manière quelconque. Cette valeur est utilisée lorsqu'une route est redistribuée dans BGP. Le type d'origine **Incomplete** est représenté par le symbole **?** dans la sortie de la commande EXEC **show ip bgp**.

La Figure 4.9 illustre l'emploi de l'attribut d'origine sur un réseau.

Attribut de prochain saut (Next Hop)

Cet attribut stipule l'adresse IP du prochain saut qui sera utilisé pour atteindre une destination donnée. Pour EBGP, le prochain saut est généralement l'adresse IP du voisin spécifié par la commande **neighbor remote-as**, sauf lorsque le prochain saut se trouve sur un média multiaccès. Dans ce cas, le prochain saut pourrait être l'adresse IP du routeur sur le même sous-réseau. Examinez le réseau illustré Figure 4.10.

A la Figure 4.10, le routeur C annonce le réseau 170.10.0.0 au routeur A avec un attribut de prochain saut indiquant 170.10.20.2, et le routeur A annonce le réseau 150.10.0.0 au routeur C avec un attribut de prochain saut de 170.10.20.1.

Figure 4.9
Attribut d'origine.

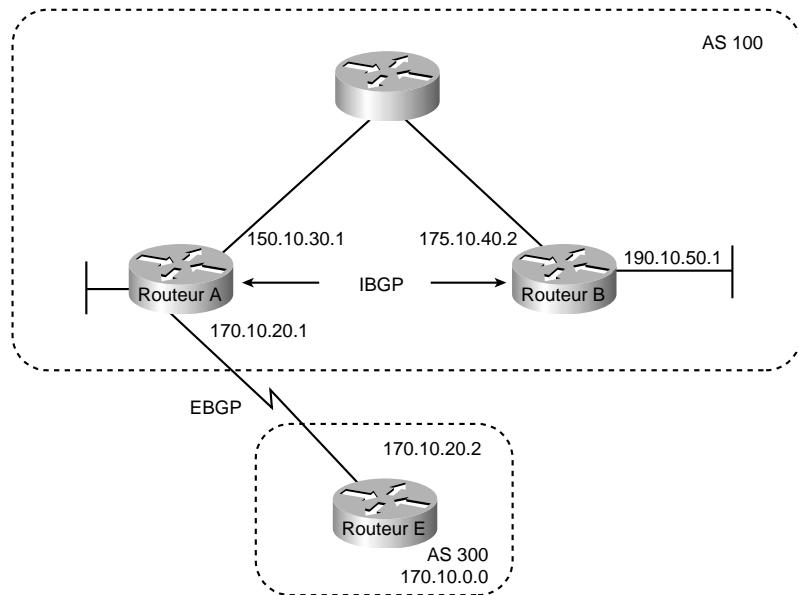
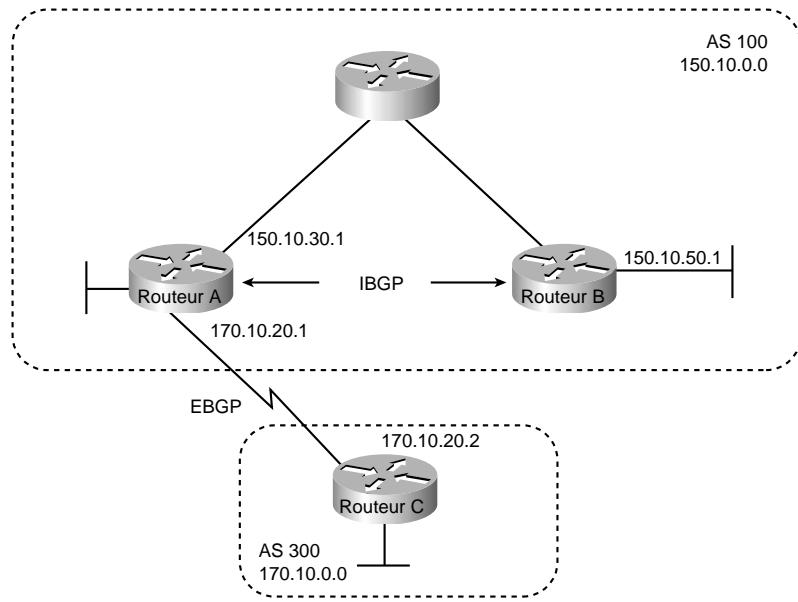


Figure 4.10
Attribut de prochain saut.



BGP spécifie que le prochain saut vers une destination apprise *via* EBGP devrait être acheminé sans modification dans IBGP. Selon cette règle, le routeur A annonce le réseau 170.10.0.0 au routeur B, son homologue IBGP, avec un attribut de prochain saut spécifiant 170.10.20.2. En conséquence,

selon le routeur B, le prochain saut pour atteindre l'adresse 170.10.0.0 est 170.10.20.2, au lieu de 150.10.30.1. Pour cette raison, la configuration doit s'assurer que le routeur B peut atteindre 170.10.20.2 *via* un IGP. Sinon, le routeur B ignorera les paquets à destination de 170.10.0.0, car l'adresse de l'attribut de prochain saut est inaccessible.

Par exemple, si le routeur B exécute IGRP, le routeur A devrait exécuter IGRP sur le réseau 170.10.0.0. Si vous le souhaitez, vous avez la possibilité de désactiver IGRP sur le lien vers le routeur C afin que seules les mises à jour BGP soient échangées.

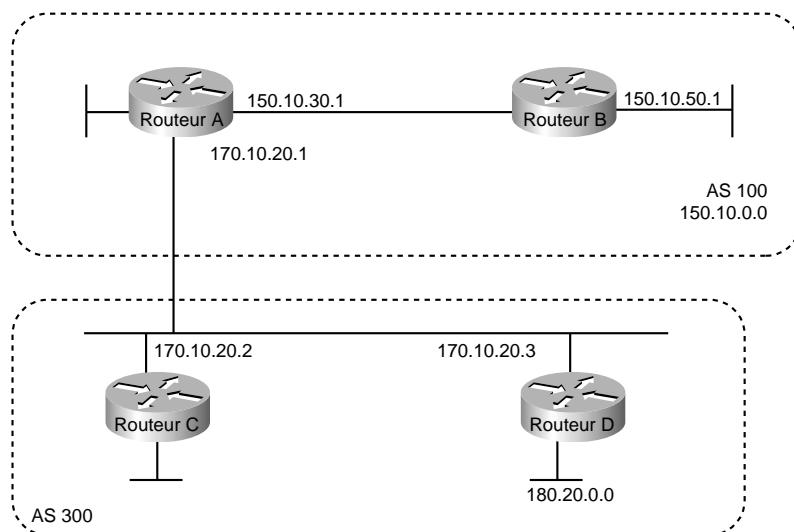
Attribut de prochain saut et média multiaccès

BGP pourrait définir différemment la valeur de l'attribut de prochain saut sur un média multiaccès tel qu'Ethernet. Considérez le réseau illustré Figure 4.11.

Dans le cas de la Figure 4.11, les routeurs C et D dans l'AS 300 exécutent OSPF. Le routeur C communique avec le routeur A *via* BGP. C peut atteindre le réseau 180.20.0.0 *via* 170.10.20.3. Lorsque C envoie une mise à jour BGP à A concernant le réseau 180.20.0.0, il spécifie 170.10.20.3 comme attribut de prochain saut au lieu de sa propre adresse IP (170.10.20.2). La raison en est que les routeurs A, B et C se trouvent dans le même sous-réseau, et il semble plus logique que A utilise D comme prochain saut plutôt que de passer par un saut supplémentaire, à savoir C.

Figure 4.11

Réseau avec média multiaccès.

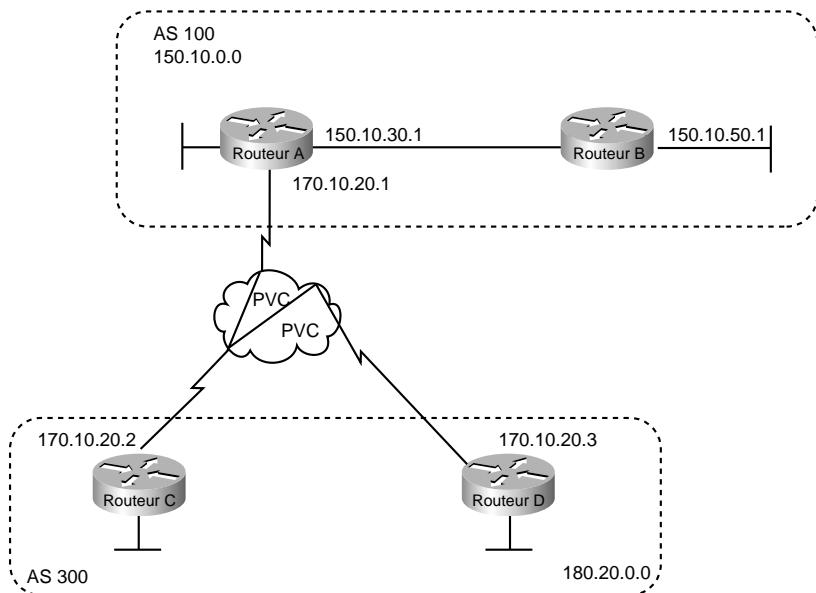


Attribut de prochain saut et accès au média non broadcast

A la Figure 4.12, trois réseaux sont reliés par un nuage NBMA (avec accès au média non broadcast), tel que le Frame Relay.

Figure 4.12

Attribut de prochain saut et accès au média non broadcast.



Si les routeurs A, C et D utilisent un média commun tel que le Frame Relay (ou n'importe quel nuage NBMA), C annonce 180.20.0.0 à A avec 170.10.20.3 comme prochain saut, comme il le ferait si le média partagé était Ethernet. Le problème est que A ne dispose pas d'une connexion virtuelle permanente (PVC, Permanent Virtual Connection) vers le routeur D et ne peut donc pas atteindre l'adresse stipulée par l'attribut de prochain saut, ce qui se traduit par un échec de routage. Pour remédier à cette situation, utilisez la commande **neighbor next-hop-self**, comme illustré dans la configuration suivante pour le routeur C :

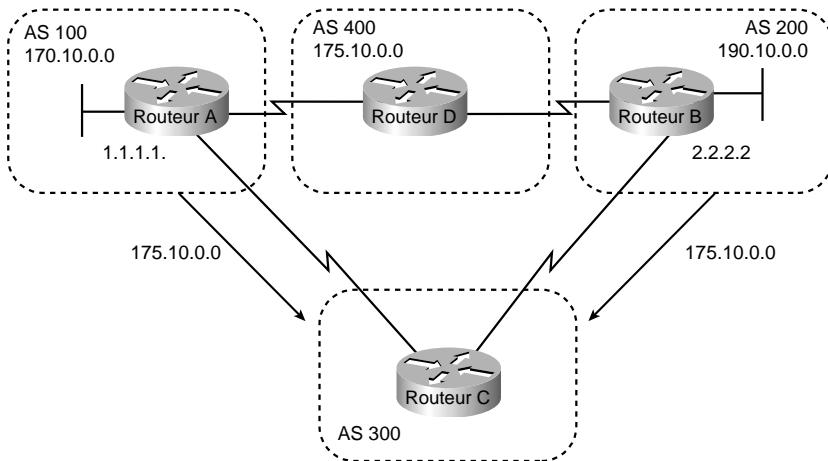
```
!Routeur C
router bgp 300
neighbor 170.10.20.1 remote-as 100
neighbor 170.10.20.1 next-hop-self
```

Avec la commande **neighbor next-hop-self**, le routeur C annonce le réseau 180.20.0.0 avec 170.10.20.2 comme attribut de prochain saut.

Attribut de poids (Weight)

L'attribut de poids est un attribut Cisco spécial qui est utilisé dans le processus de sélection de chemin lorsqu'il existe plus d'une route vers la même destination. Cet attribut est local au routeur sur lequel il est assigné et n'est pas propagé dans les mises à jour de routage. Par défaut, sa valeur est 32768 pour les chemins provenant du réseau du routeur et zéro pour les autres chemins. Les routes de poids plus élevé emportent la préférence lorsqu'il y a plusieurs chemins vers la même destination. Considérez le réseau illustré Figure 4.13.

Figure 4.13
Exemple d'attribut de poids.



A la Figure 4.13, les routeurs A et B prennent connaissance du réseau 175.10.0.0 du système autonome 400 et propagent chacun la mise à jour vers le routeur C. Ce dernier dispose donc de deux routes pour atteindre 175.10.0.0 et doit décider de celle à emprunter. Si, sur C, le poids des mises à jour en provenance de A est supérieur à celui des mises à jour de B, C utilisera alors A comme prochain saut pour atteindre le réseau 175.10.0.0. Il existe trois méthodes pour définir l'attribut de poids pour les mises à jour provenant de A :

- liste d'accès ;
- carte de routage ;
- commande **neighbor weight**.

Utilisation d'une liste d'accès pour définir l'attribut de poids

Les commandes suivantes sur le routeur C utilisent des listes d'accès et la valeur de l'attribut AS_path pour assigner un poids aux mises à jour de route :

```

!Routeur C
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 filter-list 5 weight 2000
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 filter-list 6 weight 1000
!
ip as-path access-list 5 permit ^100$
ip as-path access-list 6 permit ^200$
```

Dans cet exemple, 2000 est la valeur assignée à l'attribut de poids des mises à jour provenant du voisin situé à l'adresse IP 1.1.1.1, et qui sont autorisées par la liste d'accès 5. Celle-ci accepte les mises à jour dont l'attribut de cheminement AS_path commence par 100 (comme spécifié par le symbole ^) et se termine par 100 (comme spécifié par le symbole \$). Ces deux symboles sont utilisés pour former des expressions régulières. Cet exemple assigne également la valeur 1000 à l'attribut de poids des mises à jour transmises par le voisin situé à l'adresse IP 2.2.2.2, et qui sont

acceptées par la liste d'accès 6. Celle-ci accepte les mises à jour dont l'attribut de cheminement commence par 200 et se termine par 200.

Dans la pratique, cette configuration assigne la valeur 2000 à l'attribut de poids de toutes les mises à jour de route reçues de l'AS 100, et la valeur 1000 à l'attribut de poids de toutes les mises à jour transmises par l'AS 200.

Utilisation d'une carte de routage pour définir l'attribut de poids

Les commandes suivantes sur le routeur C utilisent une carte de routage pour assigner un poids à des mises à jour de routage :

```
!Routeur C
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 route-map SETWEIGHTIN in
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 route-map SETWEIGHTIN in
!
ip as-path access-list 5 permit ^100$*
!
route-map SETWEIGHTIN permit 10
match as-path 5
set weight 2000
route-map SETWEIGHTIN permit 20
set weight 1000
```

La première instance de la carte de routage SETWEIGHTIN assigne 2000 à n'importe quelle mise à jour de routage provenant de l'AS 100 et la seconde instance de la carte de routage SETWEIGHTIN assigne 1000 aux mises à jour de n'importe quel autre AS.

Utilisation de la commande *neighbor weight* pour définir l'attribut de poids

La configuration suivante pour le routeur C utilise la commande **neighbor weight** :

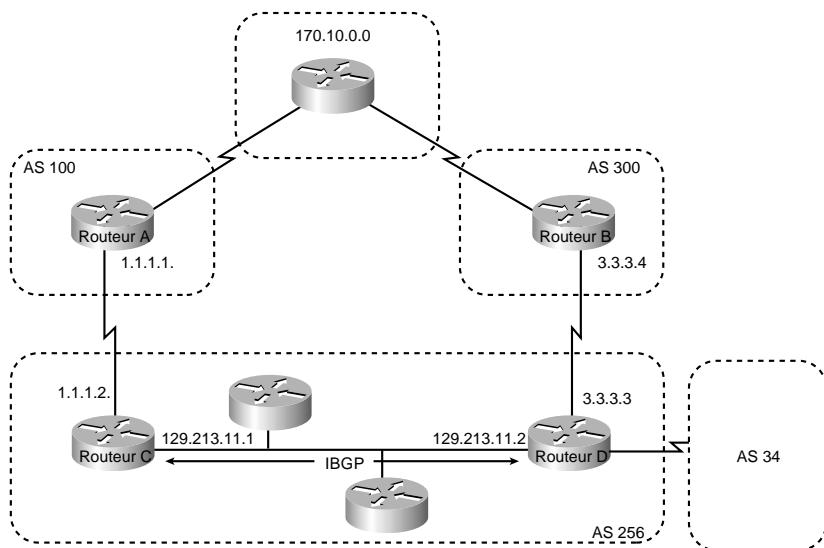
```
!Routeur C
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 weight 2000
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 weight 1000
```

Cette configuration définit un poids de 2000 pour toutes les mises à jour de routage provenant de l'AS 100 et un poids de 1000 pour toutes celles provenant de l'AS 200. Etant donné le poids plus élevé assigné aux mises à jour provenant de l'AS 100, C envoie donc tout le trafic par l'intermédiaire de A.

Attribut de préférence locale (Local Preference)

Lorsqu'il existe plusieurs chemins vers une même destination, l'attribut de préférence locale permet d'indiquer l'itinéraire préféré. Le chemin comprenant la valeur de préférence la plus haute est choisi (la valeur par défaut de l'attribut étant 100). A la différence de l'attribut de poids, qui n'est pertinent que pour le routeur local, l'attribut de préférence locale fait partie des informations de mises à jour de routage et est échangé entre les routeurs d'un même système autonome. Le réseau de la Figure 4.14 en illustre l'emploi.

Figure 4.14
Exemple d'emploi
de l'attribut de
préférence locale.



A la Figure 4.14, l'AS 256 reçoit des mises à jour de route pour le réseau 170.10.0.0 de la part des AS 100 et 300. Il existe deux façons de définir l'attribut de préférence locale :

- commande **bgp default local-preference** ;
- carte de routage.

Utilisation de la commande *bgp default local-preference*

Les configurations suivantes utilisent cette commande pour définir l'attribut de préférence locale sur les routeurs C et D :

```

!Routeur C
router bgp 256
neighbor 1.1.1.1 remote-as 100
neighbor 128.213.11.2 remote-as 256
bgp default local-preference 150
!Routeur D
router bgp 256
neighbor 3.3.3.4 remote-as 300
neighbor 128.213.11.1 remote-as 256
bgp default local-preference 200

```

La configuration du routeur C assigne une préférence locale de 150 pour toutes les mises à jour provenant de l'AS 100 et la configuration du routeur D assigne une préférence locale de 200 pour toutes les mises à jour transmises par l'AS 300. Comme les informations de préférence locale sont échangées au sein de l'AS, les routeurs C et D déterminent que les mises à jour concernant le réseau 170.10.0.0 possèdent une valeur de préférence locale plus intéressante lorsqu'elles transitent par l'AS 300. Résultat : tout le trafic dans l'AS 256 à destination du réseau 170.10.0.0 est envoyé vers le routeur D comme point de sortie.

Utilisation d'une carte de routage pour définir la préférence locale

Les cartes de routage offrent davantage de souplesse que la commande **bgp default local-preference**. Lorsque cette commande est utilisée sur le routeur D de la Figure 4.14, l'attribut de préférence locale de toutes les mises à jour qu'il reçoit, y compris celles provenant de l'AS 34, est défini avec la valeur 200.

La configuration suivante utilise une carte de routage définissant cet attribut sur le routeur D, spécifiquement pour les données de routage provenant de l'AS 300 :

```
!Routeur D
router bgp 256
neighbor 3.3.3.4 remote-as 300
route-map SETLOCALIN in
neighbor 128.213.11.1 remote-as 256
!
ip as-path 7 permit ^300$
route-map SETLOCALIN permit 10
match as-path 7
set local-preference 200
!
route-map SETLOCALIN permit 20
```

Avec cette configuration, n'importe quelle mise à jour provenant de l'AS 300 reçoit une valeur de préférence locale de 200. L'instance 20 de la carte de routage SETLOCALIN accepte toutes les autres routes.

Attribut de préférence d'accès AS (Multi-Exit Discriminator)

L'attribut MED (*Multi-Exit Discriminator*) est une indication à l'attention des routeurs voisins externes concernant le chemin préféré vers un AS lorsqu'il présente plusieurs points d'entrée. Une valeur MED faible reçoit la préférence par rapport à une valeur MED plus élevée. La valeur par défaut de l'attribut MED est 0.

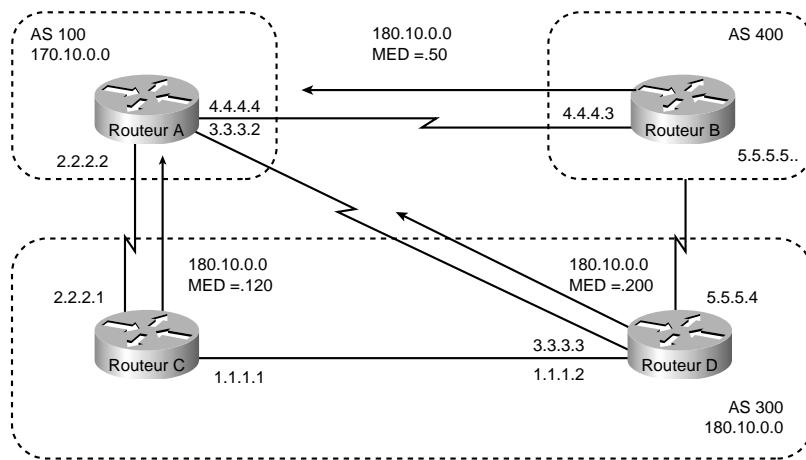
NOTE

Dans la version 4 de BGP, l'attribut MED est connu sous l'appellation Inter-AS_Metric.

A la différence de l'attribut de préférence locale, l'attribut MED est échangé entre les AS et, une fois arrivé dans un AS, il n'est pas retransmis. Lorsqu'une mise à jour pénètre dans un AS avec une certaine valeur d'attribut MED, cette dernière est utilisée pour effectuer les prises de décision au sein de l'AS. Lorsque BGP renvoie cette mise à jour à un autre AS, l'attribut est réinitialisé avec la valeur 0.

Sauf s'il est explicitement configuré, le routeur d'un AS compare les attributs MED des itinéraires provenant de voisins externes situés dans un même AS. Si vous voulez forcer la comparaison des attributs MED de voisins d'AS différents, vous devez configurer le routeur avec la commande **bgp always-compare-med**. Le réseau de la Figure 4.15 illustre l'emploi de l'attribut MED.

Figure 4.15
Exemple d'emploi
de l'attribut MED.



A la Figure 4.15, l'AS 100 reçoit des mises à jour concernant le réseau 180.10.0.0 de la part des routeurs B, C et D. C et D se trouvent dans l'AS 300 et B dans l'AS 400. Les commandes suivantes permettent de configurer les routeurs A, B, C et D :

```

!Routeur A
router bgp 100
neighbor 2.2.2.1 remote-as 300
neighbor 3.3.3.3 remote-as 300
neighbor 4.4.4.3 remote-as 400

!Routeur B
router bgp 400
neighbor 4.4.4.4 remote-as 100
neighbor 4.4.4.4 route-map SETMEDOUT out
neighbor 5.5.5.4 remote-as 300
!
route-map SETMEDOUT permit 10
set metric 50

!Routeur C
router bgp 300
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 route-map SETMEDOUT out
neighbor 1.1.1.2 remote-as 300
!
route-map SETMEDOUT permit 10
set metric 120

!Routeur D
router bgp 300
neighbor 3.3.3.2 remote-as 100
neighbor 3.3.3.2 route map SETMEDOUT out
neighbor 5.5.5.5 remote-as 400
neighbor 1.1.1.1 remote-as 300
route-map SETMEDOUT permit 10
set metric 200

```

Par défaut, BGP compare les attributs MED des routes provenant de voisins situés dans un même AS externe (tel que l'AS 300 à la Figure 4.15). Le routeur A peut comparer uniquement les attributs MED provenant des routeurs C (120) et D (200), même si la mise à jour transmise par le routeur B possède la valeur MED la plus faible.

Le routeur A choisira le routeur C comme meilleur chemin pour atteindre le réseau 180.10.0.0. Pour obliger le routeur A à inclure dans cette comparaison les mises à jour acheminées par B pour le même réseau, utilisez la commande **bgp always-compare-med**, comme dans l'exemple suivant de configuration modifiée pour le routeur A :

```
!Routeur A
router bgp 100
neighbor 2.2.2.1 remote-as 300
neighbor 3.3.3.3 remote-as 300
neighbor 4.4.4.3 remote-as 400
bgp always-compare-med
```

Le routeur A choisira le routeur B comme le meilleur prochain saut pour atteindre le réseau 180.10.0.0 (en supposant que tous les autres attributs soient restés identiques).

Vous pouvez aussi définir l'attribut MED lorsque vous configurez la redistribution de routes dans BGP. Sur le routeur B, vous pouvez par exemple injecter dans BGP une route statique avec un attribut MED de 50, comme dans l'exemple de configuration suivant :

```
!Routeur B
router bgp 400
redistribute static
default-metric 50
!
ip route 160.10.0.0 255.255.0.0 null 0
```

La configuration précédente provoque l'envoi par le routeur B de mises à jour pour le réseau 160.10.0.0 avec un attribut MED de 50.

Attribut de communauté (Community)

L'attribut de communauté représente un moyen de grouper des destinations (appelées communautés) auxquelles des décisions de routage (telles que l'acceptation, la préférence et la redistribution) peuvent être appliquées. Les cartes de routage sont utilisées pour définir un attribut de communauté. Le Tableau 4.1 présente quelques communautés prédéfinies.

Tableau 4.1 : Communautés prédéfinies

Communauté	Signification
no-export	Ne pas annoncer cette route aux homologues EBGP.
no-advertise	N'annoncer cette route à aucun homologue.
internet	Annoncer cette route à la communauté Internet ; tous les routeurs sur le réseau en font partie.

Les cartes de routage suivantes définissent la valeur de l'attribut de communauté :

```
route-map COMMUNITYMAP
match ip address 1
set community no-advertise
!
route-map SETCOMMUNITY
match as-path 1
set community 200 additive
```

Si vous spécifiez le mot clé **additive**, la valeur spécifiée est ajoutée à la valeur existante de l'attribut de communauté. Autrement, la valeur de communauté spécifiée remplace toute valeur définie précédemment. Pour envoyer l'attribut de communauté à un voisin, vous devez utiliser la commande de **neighbor send-community**, comme dans l'exemple suivant :

```
router bgp 100
neighbor 3.3.3.3 remote-as 300
neighbor 3.3.3.3 send-community
neighbor 3.3.3.3 route-map setcommunity out
```

Reportez-vous à la section "Filtrage de communauté" de ce chapitre pour obtenir des exemples d'utilisation de l'attribut de communauté pour filtrer des mises à jour.

Critères de sélection de chemin BGP

BGP ne sélectionne qu'un seul chemin comme meilleur itinéraire. Après l'avoir sélectionné, il le place dans sa table de routage et le transmet à ses voisins. Il suit la procédure de sélection ci-dessous pour choisir un itinéraire :

1. Si le chemin spécifie un prochain saut qui est inaccessible, il ignore la mise à jour.
2. Il donne la préférence au chemin comprenant le poids le plus élevé.
3. Si les poids sont identiques, il donne la préférence au chemin qui a la plus grande valeur de préférence locale.
4. Si les valeurs de préférence locale sont les mêmes, il choisit le chemin qui a été transmis par le BGP exécuté sur le présent routeur.
5. Si aucune route ne provient du présent routeur, il choisit le chemin d'attribut AS_path le plus court.
6. Si tous les chemins possèdent la même longueur d'attribut AS_path, il choisit le chemin avec le type d'origine le plus faible (où IGP est inférieur à EGP, qui est lui-même inférieur à Incomplete).
7. Si les codes d'origine sont les mêmes, il choisit le chemin dont l'attribut MED est le plus faible.
8. Si les itinéraires possèdent le même attribut MED, le chemin externe a l'avantage sur le chemin interne.
9. Si les chemins sont toujours les mêmes, il choisit celui passant par le voisin IGP le plus proche.
10. Il choisit le chemin avec l'adresse IP la plus faible, comme spécifié par l'ID du routeur BGP.

Compréhension et définition des stratégies de routage BGP

Cette section décrit de quelle manière aborder et définir les stratégies BGP permettant de contrôler le flux des mises à jour de ce protocole. Ces techniques incluent :

- les distances administratives ;
- le filtrage BGP ;
- les groupes d'homologues BGP ;
- le routage CIDR et les agrégats d'adresses ;
- les confédérations ;
- les réflecteurs de route ;
- le contrôle d'instabilité de route.

Distances administratives

Normalement, les informations de routage peuvent être communiquées par plusieurs protocoles. La distance administrative est utilisée pour faire un choix entre les routes transmises par différents protocoles. Celle qui comprend la distance administrative la plus faible est placée dans la table de routage IP. Par défaut, BGP utilise les distances administratives illustrées au Tableau 4.2.

Tableau 4.2. Distances administratives de BGP

<i>Distance</i>	<i>Valeur par défaut</i>	<i>Fonction</i>
Externe	20	Appliquées aux routes transmises par EBGP
Interne	200	Appliquées aux routes transmises par IBGP
Locale	200	Appliquées aux routes provenant du présent routeur

NOTE

La distance n'a aucun effet sur l'algorithme de sélection de chemin BGP, mais elle influe sur la décision de placer ou non les routes communiquées par BGP dans la table de routage.

Filtrage BGP

Vous pouvez contrôler l'envoi et la réception des mises à jour au moyen des méthodes de filtrage suivantes :

- filtrage de préfixe ;
- filtrage d'attribut de cheminement AS_path ;
- filtrage par carte de routage ;
- filtrage de communauté.

Ces méthodes conduisent toutes au même résultat. Le choix de la méthode appropriée dépend de votre configuration de réseau spécifique.

Filtrage de préfixe

L'implémentation d'une liste de préfixes vise à améliorer l'efficacité du filtrage de route (actuellement seulement avec BGP). En comparaison avec l'utilisation de listes d'accès (étendues), une liste de préfixes présente les avantages suivants :

- une amélioration significative des performances lors du chargement et du contrôle de route dans le cas de longues listes ;
- un support des mises à jour incrémentielles ;
- une plus grande convivialité de l'interface en lignes de commande.

Plusieurs fonctionnalités essentielles des listes d'accès sont reprises par les listes de préfixes :

- possibilité de configurer l'acceptation (**permit**) ou le rejet (**deny**) ;
- dépendance de l'ordre des entrées (l'évaluation s'arrête à la première correspondance trouvée) ;
- possibilité de filtrer un préfixe exact ou une plage de préfixes.

Toutefois, les listes de préfixes ne supportent pas l'utilisation de masques non contigus.

La syntaxe complète pour configurer une liste de préfixes est la suivante :

```
ip prefix-list [seq] deny|permit préfixe le|ge valeur
```

La commande suivante peut être utilisée pour supprimer une liste de préfixes :

```
no ip prefix-list
```

L'argument *seq* est optionnel et peut servir à spécifier le numéro de séquence d'une entrée dans une liste de préfixes.

Par défaut, les entrées d'une liste de préfixes reçoivent successivement les valeurs 5, 10, 15, etc., comme numéros de séquence. Si aucune valeur de séquence n'est spécifiée, l'entrée reçoit un numéro égal à (Max_Actuel + 5).

Si un préfixe donné correspond à plusieurs entrées dans une liste de préfixes, celle possédant le numéro de séquence le plus faible est considérée comme correspondante.

Les instructions **deny** ou **permit** spécifient l'action à exécuter lorsqu'une correspondance est trouvée.

Plusieurs stratégies (correspondance exacte ou de plage) avec différents numéros de séquence peuvent être configurées pour un même préfixe.

L'attribut **ge** signifie supérieur ou égal à et **le** signifie inférieur ou égal à. Ces deux attributs sont optionnels et peuvent être utilisés pour spécifier la plage de préfixes évaluée pour trouver une correspondance. En l'absence de ces attributs, une correspondance exacte est présumée.

La plage est censée s'étendre de **ge valeur** à 32, mais seulement si l'attribut **ge** est spécifié. La plage est censée s'étendre de **longueur à le valeur**, mais seulement si l'attribut **le** est spécifié.

A l'instar des listes d'accès, une liste de préfixes se termine par une instruction implicite de rejet de tout le trafic.

Voici deux exemples de configuration pour une correspondance de préfixe exacte :

```
ip prefix-list aaa deny 0.0.0.0/0
ip prefix-list aaa permit 35.0.0.0/8
```

La liste suivante présente des commandes de configuration pour une correspondance de plages de préfixes :

Dans 192/8, accepter jusqu'à /24 :

```
ip prefix-list aaa permit 192.0.0.0/8 le 24
```

Dans 192/8, rejeter /25+ :

```
ip prefix-list aaa deny 192.0.0.0/8 ge 25
```

Dans tout l'espace d'adresse, rejeter de /0 à /7 :

```
ip prefix-list aaa deny 0.0.0.0/0 le 7
```

Dans tout l'espace d'adresse, rejeter /25+ :

```
ip prefix-list aaa deny 0.0.0.0/0 ge 25
```

Dans 10/8, rejeter tout :

```
ip prefix-list aaa deny 10.0.0.0/8 le 32
```

Dans 204.70.1/24, rejeter /25+ :

```
ip prefix-list aaa deny 204.70.1.0/24 ge 25
```

Accepter tout :

```
ip prefix-list aaa permit 0.0.0.0/0 le 32
```

Les mises à jour incrémentielles sont supportées par les listes de préfixes. Contrairement aux listes d'accès normales dans lesquelles la commande **no** efface la liste complète, une liste de préfixes peut être progressivement modifiée. Par exemple, pour adapter la liste de préfixes du routeur A pour le routeur B, il suffit de changer les points de divergence :

Depuis A :

```
ip prefix-list aaa deny 0.0.0.0/0 le 7
ip prefix-list aaa deny 0.0.0.0/0 ge 25
ip prefix-list aaa permit 35.0.0.0/8
ip prefix-list aaa permit 204.70.0.0/15
```

Vers B :

```
ip prefix-list aaa deny 0.0.0.0/0 le 7
ip prefix-list aaa deny 0.0.0.0/0 ge 25
ip prefix-list aaa permit 35.0.0.0/8
ip prefix-list aaa permit 198.0.0.0/8
```

En apportant les modifications suivantes :

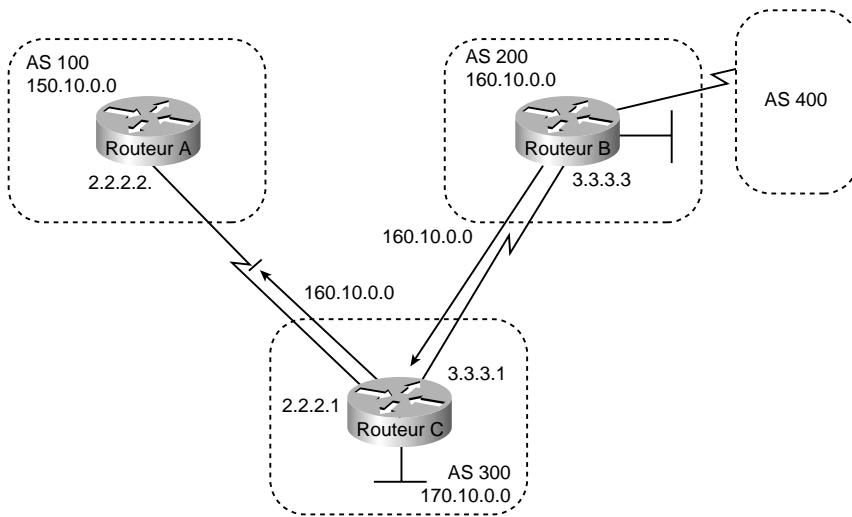
```
no ip prefix-list aaa permit 204.70.0.0/15
ip prefix-list aaa permit 198.0.0.0/8
```

Filtrage d'attribut de cheminement AS_path

Vous pouvez spécifier une liste d'accès pour les mises à jour entrantes et sortantes basée sur la valeur de l'attribut AS_path. Le réseau de la Figure 4.16 illustre l'utilité d'un tel filtre :

```
!Routeur C
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 filter-list 1 out
!
ip as-path access-list 1 deny ^200$
ip as-path access-list 1 permit .*
```

Figure 4.16
Filtrage d'attribut AS_path.



Dans cet exemple, la liste d'accès 1 rejette toutes les mises à jour dont l'attribut AS_path commence par 200 (comme spécifié par le symbole ^) et se termine par 200 (comme spécifié par le symbole \$). Comme le routeur B envoie des mises à jour concernant le réseau 160.10.0.0 dont les attributs AS_path correspondent aux valeurs stipulées dans la liste d'accès, elles seront détectées et rejetées. En spécifiant que la mise à jour doit aussi se terminer par 200, la liste d'accès autorise les mises à jour de l'AS 400 (dont l'attribut AS_path est 200,400). Si elle spécifiait ^200 comme expression, les informations de l'AS 400 seraient aussi rejetées.

Dans la seconde instruction de la liste d'accès, le point (.) désigne n'importe quel caractère et l'astérisque (*) signifie une répétition de ce caractère. Combinés (*), ces caractères correspondent à n'importe quelle valeur de l'attribut AS_path qui, en pratique, autorise toute mise à jour qui n'aura pas été rejetée par l'instruction précédente de la liste d'accès. Si vous voulez vérifier que vos expressions fonctionnent comme prévu, utilisez la commande EXEC suivante :

```
show ip bgp regexp expression-régulière
```

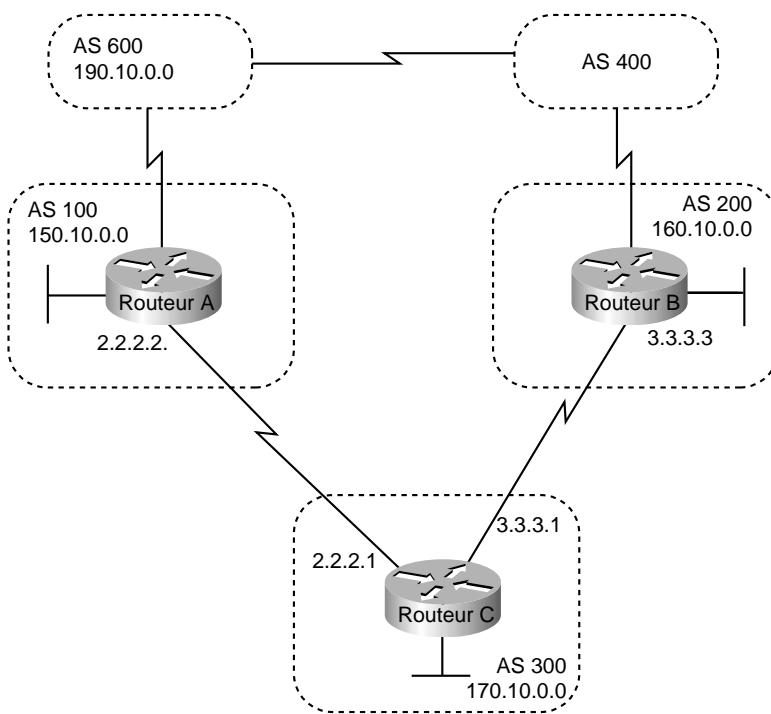
Le routeur affiche tous les chemins qui correspondent à l'expression régulière spécifiée.

Filtrage par carte de routage

La commande **neighbor route-map** peut être utilisée pour appliquer une carte de routage aux informations de mise à jour entrantes et sortantes. Le réseau de la Figure 4.17 illustre l'utilisation des cartes de routage pour filtrer les mises à jour BGP.

A la Figure 4.17, supposez que vous vouliez que le routeur C prenne connaissance des réseaux qui sont locaux par rapport à l'AS 200 seulement : autrement dit, vous ne voulez pas qu'il recueille des informations sur les AS 100, 400 ou 600 de la part de l'AS 200. De plus, vous voudriez définir un attribut de poids à 20 pour les routes pour lesquelles le routeur C accepte des informations de la part de l'AS 200.

Figure 4.17
Filtrage BGP par cartes de routage.



Pour cela, vous pourriez utiliser la configuration suivante :

```
!Router C
router bgp 300
network 170.10.0.0
neighbor 3.3.3.3 remote-as 200
neighbor 3.3.3.3 route-map STAMP in
!
route-map STAMP permit 10
match as-path 1
set weight 20
!
ip as-path access-list 1 permit ^200$
```

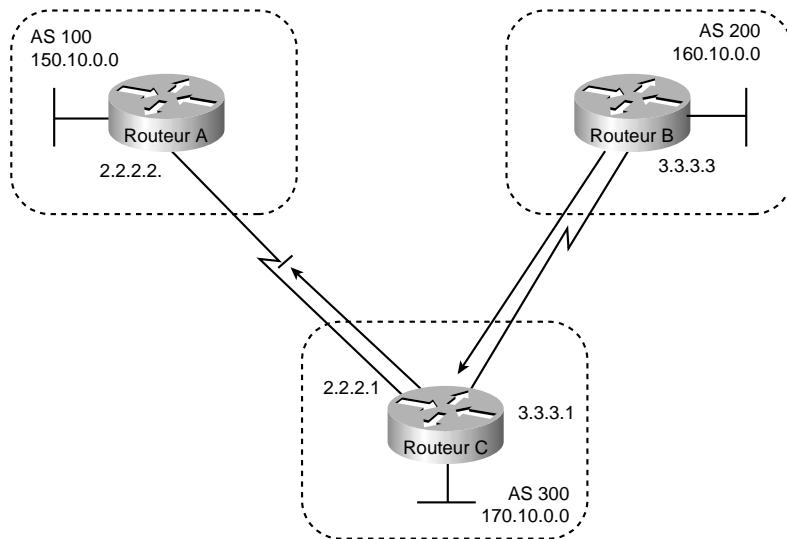
Dans la configuration précédente, la liste d'accès 1 autorise toutes les mises à jour dont l'attribut AS_path commence par 200 et se termine par 200 (c'est-à-dire qu'elle autorise les mises à jour provenant de l'AS 200). L'attribut de poids des mises à jour autorisées est défini avec la valeur 20. Toutes les autres informations de routage sont rejetées et supprimées.

Filtrage de communauté

Le réseau illustré Figure 4.18 démontre l'utilité des filtres de communauté.

Supposez que vous ne vouliez pas que le routeur C propage vers le routeur A les routes communiquées par le routeur B.

Figure 4.18
Filtrage de communauté.



Vous pourriez réaliser cela en définissant l'attribut de communauté des mises à jour que C reçoit de B, comme dans la configuration suivante pour le routeur B :

```
!Routeur B
router bgp 200
network 160.10.0.0
neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 send-community
neighbor 3.3.3.1 route-map SETCOMMUNITY out
!
route-map SETCOMMUNITY permit 10
match ip address 1
set community no-export
!
route-map SETCOMMUNITY permit 20
!
access list 1 permit 0.0.0.0 255.255.255.255
```

Pour les routes qui sont envoyées au voisin situé à l'adresse IP 3.3.3.1 (routeur C), le routeur B applique la carte de routage nommée SETCOMMUNITY. Cette carte spécifie une valeur d'attribut de communauté **no-export** (au moyen de la liste d'accès 1) pour toutes les mises à jour à destination de 3.3.3.1. La commande **neighbor send-community** est nécessaire pour inclure l'attribut de communauté dans les mises à jour envoyées au voisin situé à l'adresse IP 3.3.3.1. Lorsque C reçoit des mises à jour de routage de la part de B, il ne les propage pas vers A, car la valeur de l'attribut de communauté est **no-export**.

Une autre méthode de filtrage des mises à jour basée sur la valeur de l'attribut de communauté consiste à utiliser la commande de configuration globale **ip community-list**. Supposez que le routeur B ait été configuré de la manière suivante :

```
!Routeur B
router bgp 200
```

```

network 160.10.0.0
neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 send-community
neighbor 3.3.3.1 route-map SETCOMMUNITY out
!
route-map SETCOMMUNITY permit 10
match ip address 2
set community 100 200 additive
route-map SETCOMMUNITY permit 20
!
access list 2 permit 0.0.0.0 255.255.255.255

```

Dans la configuration précédente, le routeur B ajoute 100 et 200 à la valeur de communauté de toutes les mises à jour à destination du voisin situé à l'adresse IP précitée, à savoir 3.3.3.1. Pour configurer le routeur C afin qu'il utilise la commande **ip community-list**, il faut définir la valeur de l'attribut de poids. La configuration suivante se base sur la valeur de l'attribut de communauté 100 ou 200 pour assigner une valeur d'attribut de poids :

```

!Routeur C
router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 3.3.3.3 route-map check-community in
!
route-map check-community permit 10
match community 1
set weight 20
!
route-map check-community permit 20
match community 2 exact
set weight 10
!
route-map check-community permit 30
match community 3
!
ip community-list 1 permit 100
ip community-list 2 permit 200
ip community-list 3 permit internet

```

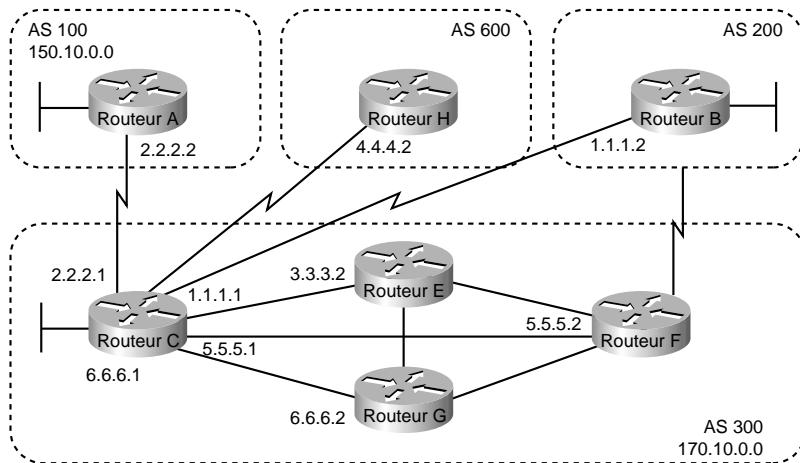
Dans la configuration précédente, toutes les routes dont l'attribut de communauté est égal à 100 correspondent à la liste d'accès 1 et reçoivent 20 comme valeur de poids. Toutes celles dont la valeur de communauté n'est que de 200 (en raison du mot clé **exact**) correspondent à la liste d'accès 2 et reçoivent la valeur 10 comme attribut de poids. Dans la liste d'accès de la dernière communauté (liste 3), l'emploi du mot clé **internet** autorise toutes les autres mises à jour sans modifier de valeur d'attribut. Ce mot clé spécifie toutes les routes, car elles sont toutes membres de la communauté Internet.

Groupes d'homologues BGP

Un *groupe d'homologues BGP* (*peer group*) est un groupe de voisins BGP qui partagent les mêmes stratégies de mises à jour. Celles-ci sont généralement définies au moyen de cartes de routage, de listes de distributions et de listes de filtres. Au lieu de définir les mêmes règles pour chaque voisin, il suffit de définir un nom de groupe d'homologues et d'assigner des règles à ce groupe.

Les membres d'un groupe d'homologues héritent de toutes les options de configuration définies pour le groupe, mais ils peuvent aussi être configurés pour redéfinir les options qui n'affectent pas les mises à jour sortantes. Autrement dit, vous pouvez redéfinir les options qui sont configurées uniquement pour les informations entrantes. L'emploi des groupes d'homologues BGP est illustré à la Figure 4.19.

Figure 4.19
Groupes
d'homologues BGP.



Les commandes suivantes configurent un groupe d'homologues BGP nommé INTERNALMAP sur le routeur C et l'appliquent aux autres routeurs dans l'AS 300 :

```
!Routeur C
router bgp 300
neighbor INTERNALMAP peer-group
neighbor INTERNALMAP remote-as 300
neighbor INTERNALMAP route-map INTERNAL out
neighbor INTERNALMAP filter-list 1 out
neighbor INTERNALMAP filter-list 2 in
neighbor 5.5.5.2 peer-group INTERNALMAP
neighbor 6.6.6.2 peer-group INTERNALMAP
neighbor 3.3.3.2 peer-group INTERNALMAP
neighbor 3.3.3.2 filter-list 3 in
```

La configuration précédente définit les stratégies suivantes pour le groupe d'homologues INTERNALMAP :

- Une carte de routage nommée INTERNALMAP
- Une liste de filtrage pour les mises à jour sortantes (filter-list 1)
- Une liste de filtrage pour les mises à jour entrantes (filter-list 2)

La configuration applique le groupe d'homologues à tous les voisins internes, c'est-à-dire aux routeurs E, F, et G. Elle définit aussi une liste de filtrage pour les mises à jour entrantes reçues du voisin à l'adresse IP 3.3.3.2, le routeur E. Cette liste peut être uniquement utilisée pour redéfinir les options qui affectent les mises à jour entrantes.

Les commandes suivantes configurent un groupe d'homologues BGP nommé EXTERNALMAP sur le routeur C et l'appliquent aux routeurs des AS 100, 200 et 600 :

```
!Routeur C
router bgp 300
neighbor EXTERNALMAP peer-group
neighbor EXTERNALMAP route-map SETMED
neighbor EXTERNALMAP filter-list 1 out
neighbor EXTERNALMAP filter-list 2 in
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 peer-group EXTERNALMAP
neighbor 4.4.4.2 remote-as 600
neighbor 4.4.4.2 peer-group EXTERNALMAP
neighbor 1.1.1.2 remote-as 200
neighbor 1.1.1.2 peer-group EXTERNALMAP
neighbor 1.1.1.2 filter-list 3 in
```

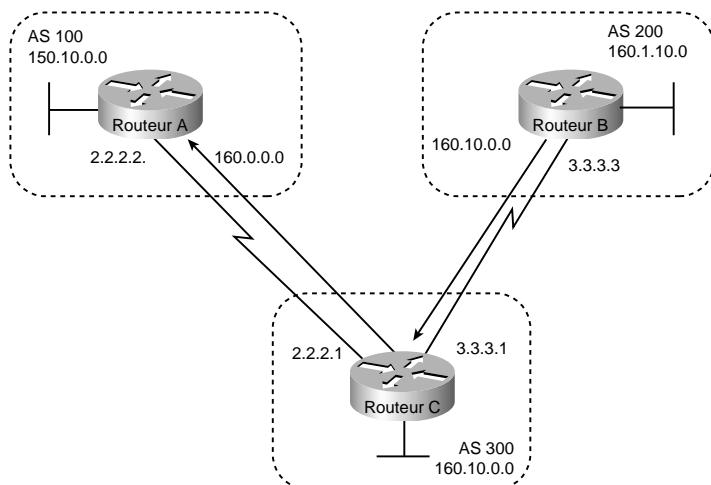
Dans la configuration précédente, les commandes **neighbor remote-as** sont placées en dehors des commandes **neighbor peer-group**, car différents AS externes doivent être définis. Notez également que cette configuration définit la liste de filtrage 3, qui peut être utilisée pour redéfinir les options de configuration pour les mises à jour entrantes de la part du voisin à l'adresse IP 1.1.1.2 (routeur B).

CIDR et agrégats d'adresses

BGP4 supporte le routage interdomaine sans classe (CIDR, *Classless InterDomain Routing*). La fonctionnalité CIDR est une nouvelle approche de l'adressage IP qui élimine le concept de classe (Classe A, Classe B, etc.). Par exemple, le réseau 192.213.0.0, qui représente une adresse de réseau de Classe C illégale, est un super-réseau légal lorsque cette adresse est exprimée en notation CIDR 192.213.0.0/16. Le /16 indique que le masque de sous-réseau se compose de 16 bits (en comptant à partir de la gauche). Par conséquent, 192.213.0.0/16 est semblable à 192.213.0.0 255.255.0.0.

CIDR facilite la formation d'agrégats de routes. L'agrégation est un processus qui combine plusieurs itinéraires différents de façon à pouvoir les annoncer en une seule route, ce qui réduit la taille des tables de routage. Examinez le réseau illustré Figure 4.20.

Figure 4.20
Exemple de formation d'agrégat.



A la Figure 4.20, le routeur B dans l'AS 200 annonce le réseau 160.11.0.0 au routeur C dans l'AS 300. Pour configurer le routeur C afin qu'il propage l'agrégat d'adresse 160.0.0.0 vers le routeur A, utilisez les commandes suivantes :

```
!Routeur C
router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
network 160.10.0.0
aggregate-address 160.0.0.0 255.0.0.0
```

La commande **aggregate-address** spécifie un préfixe d'adresse (dans ce cas, 160.0.0.0/8) et toutes les routes plus spécifiques. Si vous voulez que le routeur C propage seulement le préfixe sans transmettre de route plus spécifique, utilisez la commande suivante :

```
aggregate-address 160.0.0.0 255.0.0.0 summary-only
```

Cette commande transmet le préfixe (160.0.0.0/8) et supprime toutes les routes plus spécifiques que le routeur peut avoir dans sa table de routage BGP. Si vous voulez éliminer des routes spécifiques lors de la formation d'agrégats de routes, vous pouvez définir une carte de routage et l'appliquer à un agrégat. Par exemple, si vous voulez que le routeur C de la Figure 4.20 forme un agrégat 160.0.0.0 et supprime la route 160.20.0.0, mais propage la route 160.10.0.0, utilisez les commandes suivantes :

```
!Routeur C
router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
network 160.10.0.0
aggregate-address 160.0.0.0 255.0.0.0 suppress-map CHECK
!
route-map CHECK permit 10
match ip address 1
!
access-list 1 deny 160.20.0.0 0.0.255.255
access-list 1 permit 0.0.0.0 255.255.255.255
```

Si vous souhaitez que le routeur définitte la valeur d'un attribut lorsqu'il distribue l'agrégat de routes, utilisez une carte d'attribut comme l'illustrent les instructions suivantes :

```
route-map SETORIGIN permit 10
set origin igp
!
aggregate-address 160.0.0.0 255.0.0.0 attribute-map SETORIGIN
```

NOTE

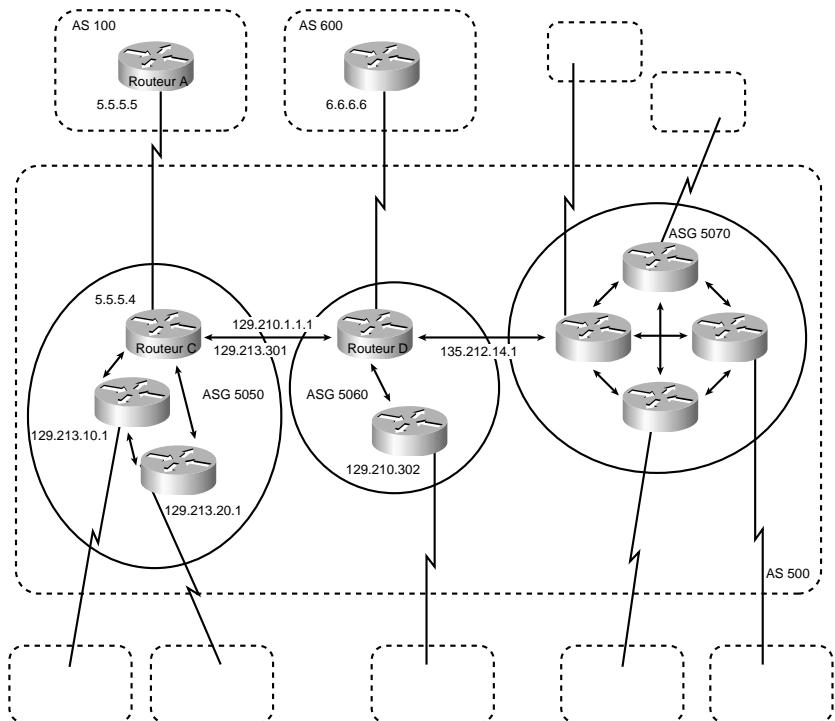
Lorsque des agrégats sont générés à partir de routes plus spécifiques, leurs attributs AS_path sont combinés pour former un ensemble appelé AS-SET. Il est utile pour prévenir les boucles de routage.

Confédérations

Une *confédération* est une technique permettant de réduire un maillage IBGP au sein d'un AS. Examinez le réseau illustré Figure 4.21.

L'AS 500 consiste en neuf routeurs BGP (bien qu'il puisse y en avoir d'autres non configurés pour BGP). En l'absence de confédération, BGP exigerait que les routeurs de l'AS 500 soient totalement maillés. Ce qui signifie que chaque routeur devrait communiquer avec les huit autres *via* IBGP, être connecté à un AS externe et exécuter EBGP. Ce qui donnerait un total de neuf homologues pour chaque routeur.

Figure 4.21
Exemple de confédérations.



Les confédérations réduisent le nombre d'homologues au sein d'un AS, comme le montre la Figure 4.21. Elles servent à diviser un AS en plusieurs mini-AS et à assigner ces derniers à une confédération. Chaque mini-AS est totalement maillé et ses membres utilisent IBGP pour communiquer entre eux. Tous les mini-AS possèdent une connexion vers les autres mini-AS dans le cadre de la confédération. Même si ces mini-AS comprennent des homologues EBGP reliés à des AS au sein même de la confédération, ils échangent des mises à jour de routage comme s'ils utilisaient IBGP. Autrement dit, les informations d'attributs de prochain saut, MED et de préférence locale sont préservées. Pour le monde extérieur, la confédération apparaît comme un seul AS. Les commandes suivantes configurent le routeur C :

```
!Routeur C
router bgp 65050
bgp confederation identifier 500
bgp confederation peers 65060 65070
neighbor 128.213.10.1 remote-as 65050
```

```

neighbor 128.213.20.1 remote-as 65050
neighbor 128.210.11.1 remote-as 65060
neighbor 135.212.14.1 remote-as 65070
neighbor 5.5.5.5 remote-as 100

```

La commande **router bgp** spécifie que le routeur C appartient à l'AS 50.

La commande **bgp confederation identifier** stipule que le routeur C appartient à la confédération 500. Les deux premières instructions **neighbor remote-as** établissent les connexions IBGP avec les deux autres routeurs dans l'AS 65050. Les deux instructions **neighbor remote-as** qui suivent établissent les connexions avec les homologues de confédérations 65060 et 65070. La dernière commande **neighbor remote-as** établit une connexion EBGP avec l'AS 100. Les commandes suivantes configurent le routeur D :

```

!Routeur D
router bgp 65060
bgp confederation identifier 500
bgp confederation peers 65050 65070
neighbor 129.210.30.2 remote-as 65060
neighbor 128.213.30.1 remote-as 65050
neighbor 135.212.14.1 remote-as 65070
neighbor 6.6.6.6 remote-as 600

```

La commande **router bgp** spécifie que le routeur D appartient à l'AS 65060. La commande **bgp confederation identifier** indique que le routeur D appartient à la confédération 500.

La première commande **neighbor remote-as** établit une connexion IBGP vers l'autre routeur au sein de l'AS 65060. Les deux commandes **neighbor remote-as** suivantes établissent les connexions BGP avec les homologues 65050 et 65070. La dernière commande **neighbor remote-as** établit une connexion EBGP avec l'AS 600. Les commandes suivantes configurent le routeur A :

```

!Routeur A
router bgp 100
neighbor 5.5.5.4 remote-as 500

```

La commande **neighbor remote-as** établit une connexion EBGP avec le routeur C. Le routeur A n'a pas connaissance des AS 65050, 65060, et 65070 et ne connaît que l'AS 500.

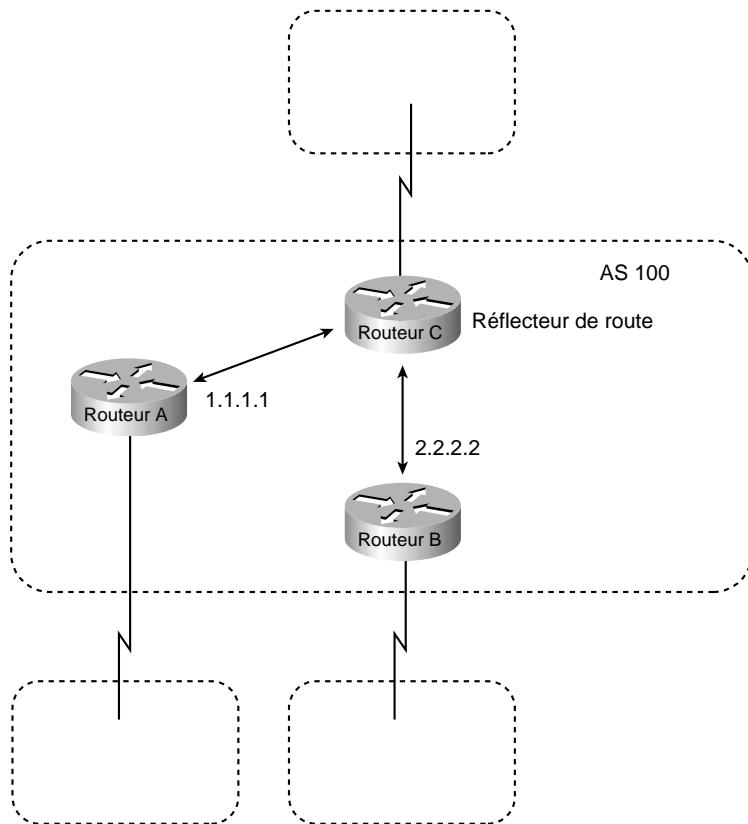
Rélecteurs de route

Les rélecteurs de route (*route reflector*) représentent une autre solution permettant de limiter le peering de routeurs IBGP dans un système autonome. Comme décrit plus haut à la section "Synchronisation", un routeur BGP ne fait pas l'annonce d'une route vers un routeur IBGP s'il en a pris connaissance par l'intermédiaire d'un autre routeur IBGP. Les rélecteurs de route atténuent cette limitation et autorisent un routeur à annoncer (réfléter) les routes reçues via IBGP vers d'autres routeurs IBGP, réduisant du même coup le nombre d'homologues IBGP au sein d'un AS. La Figure 4.22 illustre le fonctionnement des rélecteurs de route.

En l'absence de rélecteur de route, le réseau de cette figure nécessiterait un réseau IBGP totalement maillé : le routeur A devrait aussi être homologue du routeur B. Si le routeur C est configuré en tant que rélecteur de route, le peering IBGP entre A et B n'est pas nécessaire, car C reflétera vers B les mises à jour reçues de la part de A.

Figure 4.22

Exemple de réflecteur de route.



Pour configurer C comme réflecteur de route, utilisez les commandes suivantes :

```
!Routeur C
router bgp 100
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 route-reflector-client
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 route-reflector-client
```

Le routeur dont la configuration inclut les commandes **neighbor route-reflector-client** est le réflecteur de route. Les routeurs identifiés par les commandes **neighbor route-reflector-client** sont les clients du réflecteur de route. Le réflecteur de route et ses clients forment un *cluster*. Les autres homologues IBGP du réflecteur de route qui ne sont pas clients sont simplement appelés non-clients.

Un AS peut comprendre plusieurs réflecteurs de route. Dans ce cas, ils se comportent entre eux comme des routeurs IBGP ordinaires. Il peut également exister plusieurs réflecteurs de route dans un cluster et plusieurs clusters dans un AS.

Contrôle d'instabilité de route (Route Flap Dampening)

La fonctionnalité de contrôle d'instabilité de route (*Route Flap Dampening*), introduite avec Cisco IOS 11.0, est un mécanisme qui permet de réduire les variations du réseau provoquées par une ligne instable. Les termes suivants sont utilisés pour décrire le contrôle d'instabilité :

- **Penalty (pénalité).** Une valeur numérique qui est assignée à une route instable.
- **Half-life time (demi-durée de vie).** Une valeur numérique configurable qui spécifie le temps nécessaire pour réduire la pénalité de moitié.
- **Suppress limit (limite de suppression).** Une valeur numérique qui est comparée avec celle de pénalité. Si celle de pénalité est supérieure à la limite de suppression, la route est supprimée.
- **Suppressed (supprimée).** Une route qui ne fait pas l'objet d'une annonce, même si elle est active. Une route est supprimée si la pénalité est supérieure à la limite de suppression.
- **Reuse limit (limite de réutilisation).** Une valeur numérique configurable qui est comparée avec celle de pénalité. Si celle de pénalité est inférieure à la limite de réutilisation, une route supprimée active est replacée en activité.
- **History entry (entrée d'historique).** Une entrée qui est utilisée pour stocker des informations d'instabilité sur une route inutilisable.

Une route qui est instable reçoit une pénalité de 1000 pour chaque variation d'état. Lorsque la pénalité cumulée atteint une limite configurable, BGP n'en fait plus l'annonce, même si elle est active. La pénalité cumulée est diminuée par la valeur du paramètre Half-life time. Lorsque la pénalité cumulée est inférieure à la limite de réutilisation, la route est à nouveau annoncée (si elle est toujours active).

Résumé

La fonction principale d'un système BGP est d'autoriser l'échange d'informations d'accessibilité avec d'autres systèmes BGP. Ces informations sont utilisées pour élaborer une représentation de la connectivité de système autonome (SA) à partir de laquelle les boucles sont éliminées et permettent l'application des décisions stratégiques au niveau SA. BGP fournit un certain nombre de techniques pour contrôler le flux des mises à jour, telles que le filtrage de route ou de communauté. Il offre aussi des fonctionnalités de regroupement d'informations de routage telles que les agrégats d'adresses CIDR, les confédérations et les réflecteurs de route. BGP est un outil puissant de routage inter-domaine permettant d'éviter les boucles au sein d'un AS ou entre plusieurs AS.

5

Conception de réseaux ATM

Par Ron McCarty

Ce chapitre décrit la technologie ATM (*Asynchronous Transfer Mode*, mode de transfert asynchrone) actuelle sur laquelle les concepteurs peuvent s'appuyer pour construire leurs réseaux, mais aborde également son futur. Il couvre aussi les considérations d'implémentation pour une exploitation optimale des produits Cisco lors du déploiement de solutions ATM dans des environnements LAN et WAN existants.

Présentation d'ATM

ATM est une technologie arrivée à maturité, mais néanmoins en constante évolution, conçue pour assurer un transport rentable de la voix, de la vidéo et des données sur des réseaux publics et privés.

Elle est le résultat des travaux du groupe d'étude XVIII de l'UIT-T (Union internationale des télécommunications, section normalisation), autrefois connu sous le nom de CCITT (*Consultative Committee for International Telegraph and Telephone*, Comité consultatif international pour la télégraphie et la téléphonie) et de l'ANSI (*American National Standards Institute*, Institut national de standards américain), visant à appliquer la technologie VLSI (*Very Large Scale Integration*, intégration à très grande échelle) au transfert de données sur les réseaux publics.

Les efforts actuels pour porter ATM vers les réseaux privés et favoriser une interopérabilité entre ces réseaux et les réseaux publics sont l'œuvre du Forum ATM, fondé conjointement par Cisco Systems, NET/ADAPTIVE, Northern Telecom et Sprint, en 1991. Le Forum ATM compte actuellement plus de 600 organisations membres œuvrant pour la promotion de cette technologie et de solutions adaptées. Parmi ses membres figurent des fabricants de systèmes d'exploitation de réseau, des

fournisseurs de solutions de télécommunication, des fournisseurs de services à valeur ajoutée, ainsi que des constructeurs de matériels LAN/WAN.

Rôle d'ATM sur les réseaux

Le réseau est l'outil essentiel permettant la circulation des informations dans les environnements informatiques actuels. Les applications requièrent des canaux de données de plus grande capacité que les générations précédentes, et les réseaux doivent non seulement évoluer pour répondre aux besoins immédiats des entreprises, mais aussi offrir un certain niveau de redondance et assurer une reprise rapide en cas de défaillance.

L'émergence de l'Internet est la raison principale de l'apparition du multimédia sur l'ordinateur de bureau. Outre les possibilités multimédias infinies proposées par l'Internet, les connexions WAN sont aujourd'hui capables de transporter la voix et les flux de données. Les applications LAN sont également déployées sur les liaisons WAN et VPN (*Virtual Private Network*, réseau privé virtuel). De plus, il existe une demande pour des applications multimédias (voix et vidéo) fondées sur les besoins vitaux des entreprises, pouvant être exploitées sur l'ordinateur de bureau. Cette augmentation des besoins en bande passante et la disparition des limites des applications LAN/WAN traditionnelles encouragent l'exploitation de technologies qui ne sont pas soumises aux restrictions de conception LAN/WAN habituelles. L'intégration de la voix, de la vidéo et des données sur des circuits communs résulte également des réseaux — moins coûteux que des solutions comparables non intégrées —, qui assurent à la fois le support d'applications plus gourmandes et fournissent la bande passante nécessaire pour gérer la voix et la vidéo.

Cette intégration entraîne toutefois des problèmes de qualité de service (QoS, *Quality of Service*) que les concepteurs rencontraient déjà lors de la conception de réseaux basés sur TCP/IP, mais dans une moindre mesure. Soit la bande passante des réseaux LAN était appropriée, soit elle était augmentée de façon à fournir un environnement suffisamment efficace pour les programmes interactifs. Par exemple, la connectivité WAN, en dépit d'une bande passante limitée, était assurée au moyen du mécanisme de fenêtrage TCP (technique de la fenêtre "glissante") orienté connexion, fournissant ainsi une connexion suffisamment fiable pour les applications WAN non interactives. Dans les situations où la connexion était trop médiocre pour que TCP parvienne à la maintenir, la plupart des applications se rétablissaient d'elles-mêmes et tentaient de se reconnecter ultérieurement.

Les applications multimédias doivent disposer d'une bande passante ou d'une qualité de service minimale garantie pour être efficaces. Quant aux utilisateurs, ils toléreront un certain niveau de perte et de bruit. Toutefois, supporter une expiration de délai au cours d'une livraison, avec tentative de retransmission ultérieure, n'est habituellement pas acceptable. Les problèmes de qualité de service et d'intégration de services (voix, vidéo et données) sont les facteurs décisifs à prendre en compte lors de la conception ou de l'extension de réseaux impliquant la technologie ATM.

Cette section aborde les concepts ATM suivants :

- couches fonctionnelles ATM ;
- adressage ATM ;
- médias ATM ;
- réseaux multiservice.

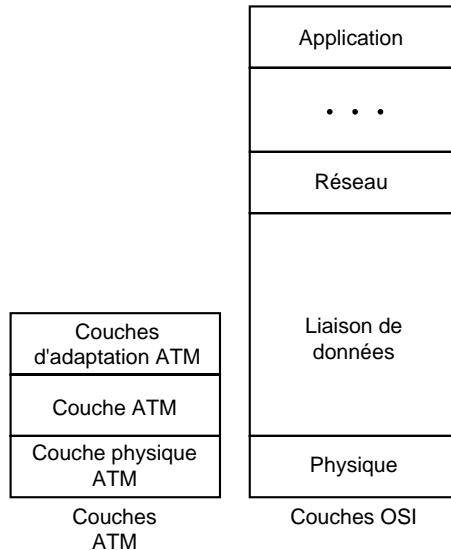
Couches fonctionnelles ATM

De même que le modèle de référence OSI (*Open System Interconnection*, interconnexion de systèmes ouverts) décrit comment deux ordinateurs communiquent par l’intermédiaire d’un réseau, le modèle de protocole ATM décrit de quelle façon deux systèmes terminaux communiquent par l’intermédiaire de commutateurs ATM. Ce modèle se compose des trois couches fonctionnelles suivantes :

- couche physique ATM ;
- couche ATM ;
- couche d’adaptation ATM.

Comme l’illustre la Figure 5.1, ces trois couches correspondent approximativement à la couche 1 et à une partie de la couche 2 (par exemple le contrôle d’erreur et la délimitation des trames de données) du modèle de référence OSI.

Figure 5.1
Relation entre les couches fonctionnelles ATM et le modèle de référence OSI.



Couche physique

La couche physique ATM contrôle la transmission et la réception des bits sur le média physique. Elle se charge également du suivi des limites des cellules ATM et les empaquette dans le type de trame approprié pour le support physique utilisé. Cette couche se décompose en deux parties :

- sous-couche de média physique ;
- sous-couche de convergence de transmission.

Sous-couche de média physique

Cette sous-couche est responsable de l’envoi et de la réception d’un flux continu de bits avec des informations de temporisation associées qui permettent la synchronisation de ces opérations. Puisqu’elle

inclut uniquement des fonctions dépendantes du média physique, sa spécification dépend donc du support physique utilisé. Parmi les standards qui transportent les cellules ATM figurent le câblage en cuivre de catégorie 5, SONET/SDH (*Synchronous Optical Network/Synchronous Digital Hierarchy*), DS-3/E3, la fibre locale à 100 Mbit/s (FDDI, *Fiber Distributed Data Interface*) et la fibre locale à 155 Mbit/s (*Fiber Channel*).

Sous-couche de convergence de transmission

La sous-couche de convergence de transmission est responsable des fonctions suivantes :

- **Délimitation des cellules.** Maintient des limites de cellules ATM.
- **Génération et vérification de code de contrôle d'erreur d'en-tête.** Génère et vérifie le code de contrôle d'erreur d'en-tête afin de garantir la validité des données.
- **Découplage de débit de cellules.** Insère ou supprime des cellules *idle* (non assignées) pour adapter le débit des cellules valides à la capacité acceptée par le système de transmission.
- **Adaptation de trames de transmission.** Empaque les cellules dans des trames acceptables pour l'implémentation spécifique de la couche physique.
- **Génération et récupération de trames de transmission.** Génère et maintient la structure appropriée de trames de la couche physique.

Couche ATM

La couche ATM établit des connexions virtuelles et transmet les cellules par l'intermédiaire du réseau ATM. Pour cela, elle utilise les informations contenues dans l'en-tête de chaque cellule. Cette couche est responsable de l'exécution des fonctions suivantes :

- Livraison de la charge utile de 48 octets sur une connexion ATM établie.
- Multiplexage et démultiplexage des cellules de différentes connexions virtuelles, celles-ci étant identifiées par les valeurs des champs VCI (*Virtual Channel Identifier*) et VPI (*Virtual Path Identifier*).
- Identification des cellules afin de déterminer leur type et leur niveau de priorité.

Cette couche est complexe pour les concepteurs de réseau habitués à d'autres principes essentiels de gestion de réseau. Cette complexité provient de problèmes de qualité de service généralement rencontrés avec les commutateurs de télécommunication uniquement, et a tendance à s'accentuer en raison du niveau de granularité nécessaire pour supporter les différents besoins QoS (allant des plus stricts à une absence de qualité de service).

La qualité de service est fondée sur des paramètres de performances initialement définis par le Forum ATM. Les paramètres suivants peuvent être négociés durant l'initialisation de session :

- **peak-to-peak CDV (peak-to-peak Cell Delay Variation, écart de délais de transfert de cellules entre pointes).** La différence entre le délai de transfert de cellules le plus élevé et le plus faible. Le plus faible est représenté par une valeur prédéfinie basée sur une probabilité.
- **maxCTD (Maximum Cell Transmission Delay, délai maximal de transmission de cellules).** Le délai maximal de transmission de cellules.

- **CLR (Cell Loss Ratio, pourcentage de perte de cellules).** Le pourcentage de perte de cellules sur le total des cellules. Un paramètre CLR peut être négocié pour chaque classe de cellules (priorité élevée ou faible) ou pour toutes les cellules.

Outre ces paramètres négociables, il en existe d'autres, fondés sur des données statistiques, et non négociables :

- **CER (Cell Error Ratio, pourcentage d'erreurs de cellules).** Le pourcentage d'erreurs de cellules sur le total de cellules.
- **CMR (Cell Misinsertion Rate, pourcentage d'erreurs d'insertion de cellules).** Le pourcentage de cellules mal insérées. Il s'agit du nombre de cellules reçues, mais qui auraient dû être transmises à un autre équipement ATM.
- **SECBR (Severely Errored Cell Block Ratio, pourcentage de blocs de cellules très altérés).** Le pourcentage de blocs de cellules qui contiennent de nombreuses erreurs sur le total des blocs de cellules.

Couche d'adaptation ATM

La couche d'adaptation ATM, ou couche AAL (*ATM Adaptation Layer*), est responsable de la segmentation et du râssemblage des données de couche supérieure. Elle doit fournir une charge utile de 48 octets à la couche ATM. Elle assure également des services spécifiques pour les couches supérieures. L'UIT-T recommande quatre classes de services : Classe A, Classe B, Classe C et Classe D. Ces classes se basent sur les caractéristiques de la session demandée :

- **Classe A.** Session orientée connexion, avec débit constant, sensible aux délais et au temps.
- **Classe B.** Session orientée connexion, avec débit variable, sensible aux délais et au temps.
- **Classe C.** Session orientée connexion, avec débit variable, non sensible aux délais et au temps.
- **Classe D.** Session sans connexion, avec débit variable, non sensible aux délais et au temps.

Pour implémenter ces quatre types de services, quatre couches AAL (protocoles) ont été spécifiées. Le Tableau 5.1 résume les caractéristiques de chacune.

Tableau 5.1 : Couches d'adaptation ATM

<i>Caractéristiques</i>	<i>AAL1</i>	<i>AAL2</i>	<i>AAL3/4</i>	<i>AAL5</i>
Requiert la synchronisation entre la source et la destination	Oui	Oui	Non	Non
Débit de données	Constant	Variable	Variable	Variable
Mode de connexion	Orienté	Orienté	Orienté	Orienté
Types de trafic	Voice et émulation de circuit	Voice (qualité téléphone)	Données	Données

AAL1

La couche AAL1 convient pour transporter le trafic téléphonique et vidéo non compressé. Comme elle nécessite une synchronisation entre la source et la destination, elle est dépendante d'un média qui supporte la temporisation, tel que SONET. Le rétablissement de la synchronisation est réalisé par le récepteur, au moyen du bit correspondant de l'en-tête.

AAL1 utilise les bits de la charge utile pour définir des champs supplémentaires. Les données de la charge utile consistent en un échantillon synchrone (par exemple, un octet de données généré à un taux d'échantillonnage de 125 microsecondes), un champ de numéro de séquence (SN, *Sequence Number*) et des champs de protection de numéro de séquence (SNP, *Sequence Number Protection*) qui fournissent les informations nécessaires à la couche AAL1 de destination, afin d'effectuer un rassemblement correct des données. Un contrôle de redondance cyclique (CRC, *Cyclic Redundancy Check*) sur 3 bits assure également la détection d'erreur et la récupération.

AAL2

La couche AAL2 offre des services pour des applications à faible débit et sensibles aux délais, telles que des services de voix avec qualité téléphone. Puisque les paquets sont de longueur variable avec ces types d'applications, les sous-couches de contrôle LLC (*Logical Link Control*) ont été conçues pour fournir des connexions virtuelles point-à-point qui utilisent le champ LLC et le champ de longueur afin d'assembler les paquets de longueur variable de plus petite taille en des cellules ATM.

AAL3/4

La couche AAL3/4 est dédiée aux fournisseurs de services de réseau et s'aligne étroitement sur les caractéristiques de SMDS (*Switched Multimegabit Data Service*, service de données multimégabit commuté). Elle est utilisée pour transmettre des paquets SMDS sur un réseau ATM. Cette couche utilise quatre identifiants de champs :

- **Type.** Détermine si la cellule représente le début, le corps ou la fin d'un message.
- **Numéro de séquence.** Détermine l'ordre dans lequel les cellules devraient être rassemblées.
- **Identifiant de multiplexage.** Identifie les cellules de différentes sources multiplexées sur la même connexion de circuit virtuel (VCC, *Virtual Circuit Connection*) afin que les cellules appropriées soient rassemblées sur la destination.
- **En-queue CRC.** Assure la détection et la correction d'erreurs.

La Figure 5.2 illustre la préparation de cellules, effectuée par la couche AAL3/4.

AAL5

La couche AAL5 prépare une cellule pour sa transmission (voir Figure 5.3).

Tout d'abord, la sous-couche de convergence (CS, *Convergence Sublayer*) de la couche AAL5 ajoute à la trame un bloc de remplissage de longueur variable et un suffixe de 8 octets. La partie de remplissage est suffisamment longue pour garantir que la PDU (*Protocol Data Unit*, unité de données de protocole) atteindra les 48 octets délimitant la cellule ATM. L'en-queue inclut un champ pour la longueur de la trame et un champ CRC de 32 bits calculé sur toute la longueur de la PDU, ce qui permet à la couche AAL5 de destination de détecter les erreurs, les cellules perdues ou les cellules désordonnées.

Figure 5.2
Préparation d'une cellule par la couche AAL3/4.

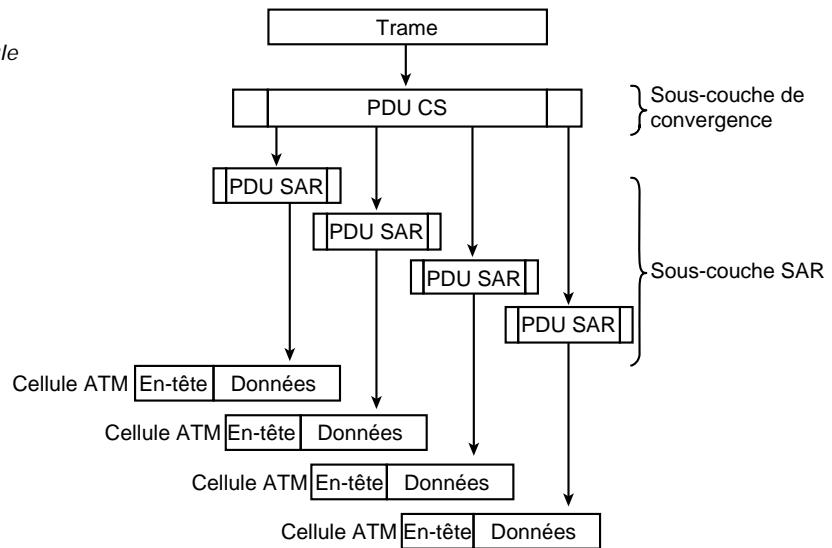
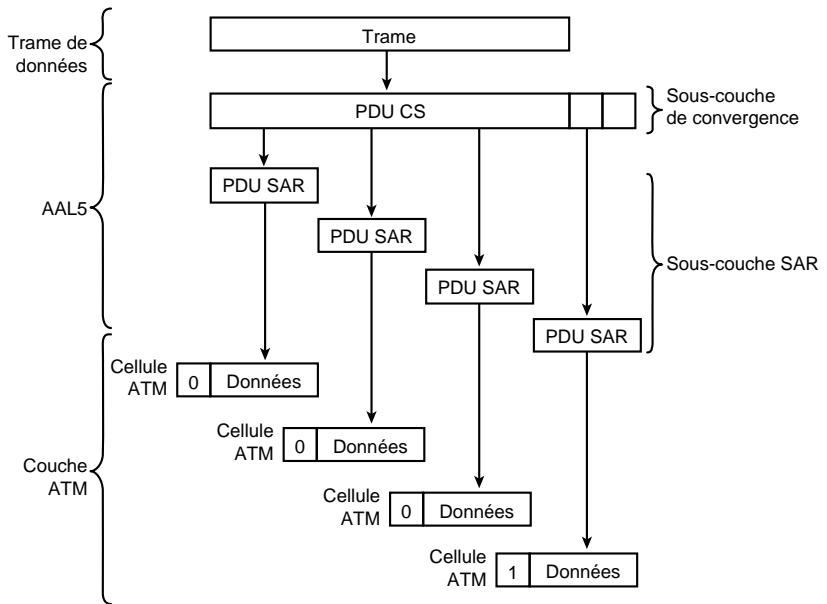


Figure 5.3
Préparation d'une cellule par la couche AAL5.



Ensuite, la sous-couche de segmentation et de réassemblage fragmente la PDU CS en blocs de 48 octets. La couche ATM place chaque bloc dans le champ de données d'une cellule ATM. Pour chaque cellule, excepté la dernière, un bit dans le champ PT (*Payload Type*, type d'informations) est mis à 0, ce qui indique que cette cellule n'est pas la dernière d'une série formant une seule trame.

Dans la dernière cellule, le champ PT est mis à 1. Lorsque la cellule arrive à destination, la couche ATM extrait le champ de données de la cellule, la sous-couche SAR (*Segmentation And Reassembly*) réassemble la PDU CS, puis la sous-couche CS utilise les champs CRC et de longueur afin de vérifier que la trame a été transmise et réassemblée correctement.

La couche AAL5 est la couche d'adaptation utilisée pour transférer la plupart des données non SMDS, comme dans le cas de IP sur ATM et de l'émulation LAN (LANE).

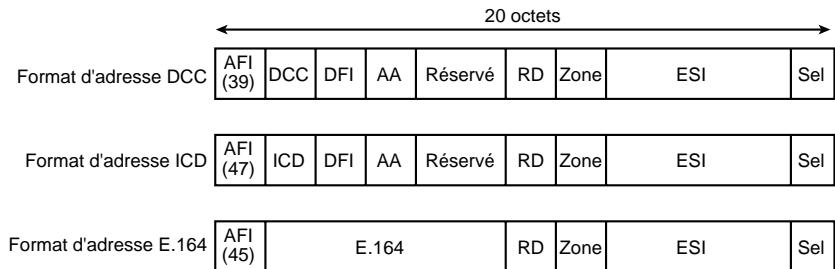
Adressage ATM

L'adressage ATM utilise la couche ATM. A l'inverse d'un nœud IP, cet adressage requiert que le nœud d'extrémité ATM connaisse le chemin complet vers la destination, ce qui évite la surcharge associée aux décisions de routage en cours de transmission. Toutefois, les équipements ATM, ou tout au moins les commutateurs ATM de frontière (*edge switch*), doivent assurer un adressage logique de niveau 3.

Plusieurs formats d'adresses ATM ont été développés. Les réseaux ATM publics utilisent généralement des adresses E.164, qui sont aussi utilisées par les réseaux RNIS à bande étroite.

La Figure 5.4 illustre le format des adresses ATM de réseau privé. Les trois formats sont DCC (*Data Country Code*, code de pays), ICD (*International Code Designator*, désignation de code international) et des adresses E.164 encapsulées NSAP (*Network Service Access Point*, point d'accès au service de réseau).

Figure 5.4
Formats d'adresses ATM.



Structure d'une adresse ATM

Les champs d'une adresse ATM sont les suivants :

- **AFI (Authority and Format Identifier)**. Un octet pour l'identifiant d'autorité et de format. Ce champ identifie le type d'adresse. Les valeurs définies sont 45, 47 et 39, respectivement pour les adresses E.164, ICD, et DCC.
- **DCC (Data Country Code)**. Deux octets pour les données de code pays.
- **DFI (DSP Format Identifier)**. Un octet pour l'identifiant de format DSP (*Domain Specific Part*, partie spécifique de domaine).
- **AA (Administrative Authority)**. Trois octets pour l'autorité administrative.
- **RD (Routing Domain)**. Deux octets pour le domaine de routage.

- **Zone.** Deux octets pour l'identifiant de zone.
- **ESI (End-System Identifier).** Six octets pour l'identifiant de système terminal, ce qui représente une adresse MAC (*Media Access Control*, contrôle d'accès au média) IEEE 802.
- **Sel.** Un octet pour le sélecteur NSAP.
- **ICD (International Code Designator).** Deux octets pour la désignation de code international.
- **E.164.** Huit octets pour le numéro de téléphone RNIS.

Les formats d'adresse ATM sont basés sur les adresses ISO NSAP, mais identifient les adresses SNPA (*Subnetwork Point of Attachment*, point d'attachement de sous-réseau). L'incorporation de l'adresse MAC dans l'adresse ATM facilite la mise en correspondance des adresses ATM avec les réseaux LAN existants.

Médias ATM

Le Forum ATM a défini plusieurs standards pour encoder ATM sur divers types de médias. Le Tableau 5.2 fournit le type de délimitation de trames et le débit pour différents médias, y compris le câble à paire torsadée non blindé (UTP, *Unshielded Twisted Pair*) supporté par les produits Cisco.

Tableau 5.2 : Débits physiques ATM

<i>Délimitation de trames</i>	<i>Média</i>						
	<i>Débit (Mbit/s)</i>	<i>Fibre multimode</i>	<i>Fibre monomode</i>	<i>Câble coaxial</i>	<i>UTP-3</i>	<i>UTP-5</i>	<i>STP</i>
DS-1	1,544			✓			
E1	2,048			✓			
DS-3	45			✓			
E3	34			✓			
STS-1	51				✓		
SONET STS3c	155	✓	✓	✓		✓	
SDH STM1							
SONET STS12c	622	✓	✓				
SDH STM4							
TAXI 4B/5B	100	✓					
8B/10B	155	✓				✓	
(Fiber Channel)							

Il existe deux standards qui permettent d'exploiter ATM sur du câble de cuivre : la catégorie 3 et la catégorie 5. La catégorie 5 supporte 155 Mbit/s avec l'encodage NRZI ; la catégorie 3 supporte 51 Mbit/s avec l'encodage CAP-16, qui est plus difficile à implémenter. Par conséquent, bien que la

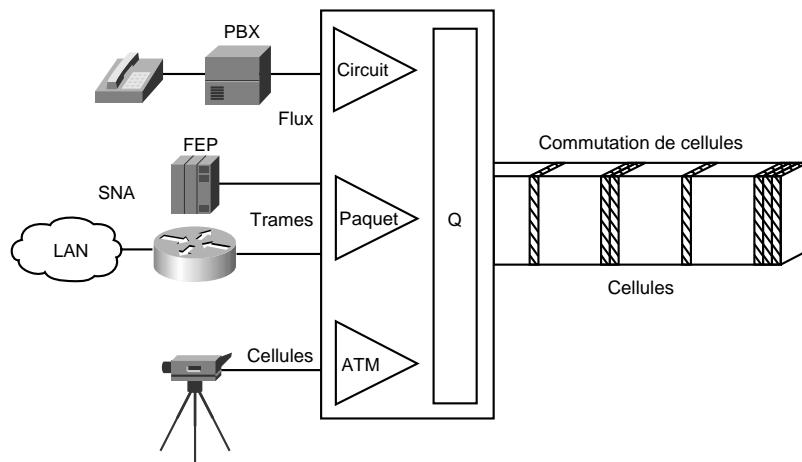
pose de câble UTP-3 puisse sembler moins coûteuse, les cartes de station de travail conçues pour du câble UTP-3 basé sur CAP-16 peuvent être plus chères et offrir moins de bande passante.

Le support ATM de la fibre et du câble de cuivre facilitera la migration future des entreprises ayant largement investi dans ces médias.

Réseaux multiservices

ATM est apparu comme l'une des technologies d'intégration de services et de fourniture de services WAN pour la connexion de réseaux LAN. ATM est également un LAN, mais son utilisation en tant que tel n'est pas largement répandue en raison de l'évolution continue d'Ethernet vers des débits atteignant des centaines de mégabits, voire de gigabits. ATM supporte divers types de trafics sur des flux séparés ou mixtes, ainsi que le trafic sensible ou non aux délais (voir Figure 5.5).

Figure 5.5
ATM supporte divers types de trafics.



ATM supporte également différentes vitesses, allant de 1,54 Mbit/s à 622 Mbit/s. Ce standard a été adopté par les constructeurs d'équipements industriels, du LAN au PBX (*Private Branch Exchange*, autocommutateur privé), en passant par les opérateurs internationaux. Grâce à ATM, aux commutateurs ATM de Cisco et aux commutateurs ATM de frontière, les concepteurs de réseaux peuvent intégrer des services, fournir une connectivité LAN-WAN et mettre en œuvre un support rentable pour les applications émergentes des entreprises.

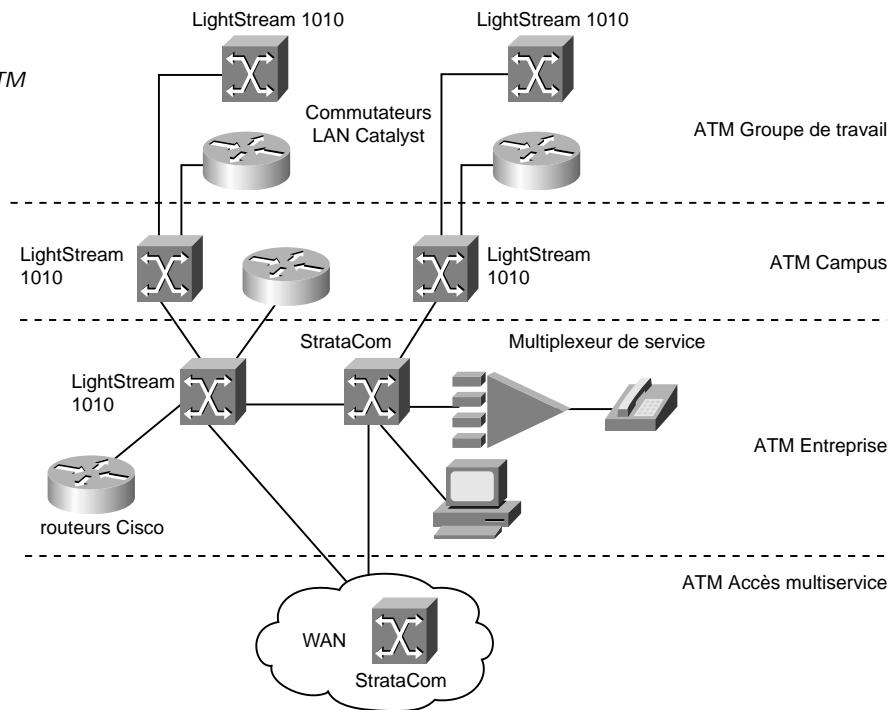
Solutions intégrées

La tendance de conception de réseaux est de fournir aux concepteurs une plus grande souplesse dans la résolution des problèmes de mise en réseau, sans avoir à créer plusieurs réseaux ou perdre les investissements existants en matière de communication de données. Les routeurs peuvent fournir un réseau fiable et sécurisé, et servir de protection contre les tempêtes de broadcast accidentelles sur les réseaux locaux. Les commutateurs (que l'on peut diviser en deux catégories principales :

LAN et WAN) peuvent être déployés aux niveaux groupe de travail, épine dorsale de campus ou WAN (voir Figure 5.6).

Figure 5.6

Le rôle des commutateurs ATM sur un réseau.



Le support et l'intégration de tous les produits Cisco sont gérés par le système IOS (*Internet-working Operating System*, système d'interconnexion de réseaux) de Cisco. Il permet d'intégrer des groupes disparates, des équipements divers et de nombreux protocoles, afin de former un réseau très fiable et évolutif.

Types de commutateurs ATM

Même si tous les commutateurs ATM supportent le Frame Relay, ils diffèrent de façon notable au niveau des caractéristiques suivantes :

- variété d'interfaces et de services supportés ;
- redondance ;
- étendue des applications de réseau ATM ;
- sophistication des mécanismes de gestion de trafic.

De même qu'il existe des routeurs et des commutateurs LAN qui présentent des caractéristiques variées en termes de prix, de performances et de fonctionnalités, il existe plusieurs configurations

de commutateurs ATM qui permettent de supporter l'intégration de la technologie ATM avec des groupes de travail, des campus et des entreprises.

Commutateurs ATM de groupe de travail et de campus

Les commutateurs ATM de groupe de travail sont souvent caractérisés par le fait qu'ils possèdent des ports de commutation Ethernet et une liaison montante (*uplink*) ATM pour se connecter à un commutateur ATM de campus. La série de Catalyst 5000 est un exemple de ce type de commutateurs. Toutefois, en raison de la popularité de l'Ethernet commuté à 100 Mbit/s, les commutateurs ATM de campus et d'entreprise supportent également des ports Ethernet.

Le commutateur Catalyst 5500 assure une commutation hautement performante dans les environnements de groupe de travail et de campus. Il dispose d'un châssis à 13 connecteurs. Le connecteur 1 est réservé au module de moteur superviseur (*Supervisor Engine*) qui assure la commutation, l'administration locale et distante, et qui fournit les liaisons montantes doubles Fast Ethernet. Le connecteur 2 est prévu pour pouvoir accepter un second moteur superviseur, ou n'importe lequel des autres modules gérés. Les connecteurs 3 à 12 supportent des modules Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, CDDI (*Copper Distributed Data Interface*) et ATM. Si un module ASP est présent sur le connecteur 13, les connecteurs 9 à 12 supportent n'importe lequel des modules PAM (*Port Adapter Module*) du commutateur ATM LightStream 1010 standard.

Le Catalyst 5500 dispose d'un circuit de commutation à 3,6 Gbit/s indépendant du média et d'un circuit de commutation de cellules à 5 Gbit/s. La plaque de connexion arrière permet de connecter les blocs d'alimentation, le moteur superviseur, les modules d'interface et le module d'épine dorsale. Le circuit indépendant du média à 3,6 Gbit/s supporte des modules Ethernet, Fast Ethernet, FDDI/CDDI, LANE ATM et RSM. La structure de commutation de cellules à 5 Gbit/s supporte un module ASP et les modules PAM ATM du LightStream 1010.

Les commutateurs ATM de campus sont généralement utilisés sur de petites épingles dorsales ATM (par exemple, pour relier des routeurs ATM ou des commutateurs LAN), ce qui permet de soulager les situations actuelles de congestion d'épine dorsale tout en autorisant le déploiement de LAN virtuels (VLAN). Les commutateurs de campus doivent supporter une grande variété de types d'épingles dorsales locales et de WAN, mais également être optimisés au plan prix/performances pour la fonction d'épine dorsale locale. Dans cette catégorie de commutateurs, les fonctionnalités de routage ATM qui autorisent plusieurs commutateurs à être reliés ensemble sont très importantes, de même que les mécanismes de contrôle de congestion qui visent à optimiser les performances de l'épine dorsale. L'extension de la gamme de commutateurs ATM de campus inclut la famille de produits Catalyst 8500.

Le Catalyst 8540 supporte les performances d'un circuit de commutation non bloquant à 40 Gbit/s. Les trois premiers connecteurs sont réservés aux modules processeur. Deux modules sont obligatoires ; le troisième module redondant peut être utilisé sur le troisième connecteur. Les dix ports restants supportent Ethernet, Fast Ethernet, Gigabit Ethernet, ainsi qu'ATM OC-3c (155 Mbit/s) et OC-12c (622 Mbit/s). Pour obtenir plus d'informations sur le déploiement de commutateurs ATM de groupe de travail et de campus, reportez-vous au Chapitre 12.

Commutateurs et routeurs ATM d'entreprise

Les commutateurs ATM d'entreprise sont des équipements sophistiqués multiservices, multimédias et multiprotocoles conçus pour former l'épine dorsale centrale de grands réseaux d'entreprise. Ils viennent compléter, et dans certains cas remplacer, la fonction des routeurs multiprotocoles haut de gamme actuels. Ces commutateurs ATM d'entreprise sont utilisés pour interconnecter des commutateurs ATM de campus. Outre leur rôle d'épines dorsales ATM, ils font aussi office de point unique d'intégration pour tous les services et technologies disparates que l'on rencontre aujourd'hui sur les réseaux fédérateurs d'entreprise. En intégrant tous ces services sur une plate-forme et une infrastructure de transport ATM communes, les concepteurs de réseaux peuvent améliorer l'administration de l'ensemble, sans avoir à recourir à la superposition de plusieurs réseaux.

Le LightStream 1010 ATM de Cisco est un commutateur de campus et d'entreprise pouvant supporter une épine dorsale d'entreprise ou assurer des services ATM de frontière pour l'entreprise. Il possède un châssis modulaire avec cinq connecteurs, qui accepte des alimentations doubles, assurant tolérance aux pannes et équilibrage de la charge. Le processeur est situé au niveau du connecteur central, et le circuit de commutation gère des vitesses allant jusqu'à 5 Gbit/s. Il autorise également le support de plusieurs segments ATM, avec un maximum de 32 ports ATM OC-3 commutés dans un rack standard de 48 centimètres.

Le commutateur Cisco BPX 8600 est un puissant commutateur ATM de frontière à large bande, conçu pour répondre aux besoins en fort trafic de grandes entreprises privées ou de fournisseurs de services publics. Ce commutateur possède 15 connecteurs, dont deux supportent les cartes de contrôle à large bande redondantes constituées du circuit de commutation et du système de contrôle. Un connecteur supplémentaire est utilisé par le moniteur d'état. Les 12 connecteurs restants peuvent être exploités pour supporter des interfaces BPX, IGX, MGX ou ATM UNI (*User-to-Network Interface*, interface utilisateur-réseau) et NNI (*Network-to-Network Interface*, interface réseau-réseau). Les performances du commutateur peuvent être optimisées au moyen de tampons de commutation en entrée et en sortie.

Les réseaux IP requièrent des performances de routeur élevées, ainsi que des services de commutation ATM. La famille de routeurs 7500 de Cisco intègre des fonctions de commutation distribuée qui permettent aux concepteurs de réseaux de mettre en œuvre le routage hautement performant nécessaire pour supporter des réseaux qui exploitent les technologies ATM, de commutation LAN multicouche, ELAN (*Emulated LAN*) et VLAN (*Virtual LAN*).

La famille de routeurs Cisco 7500 offre un support étendu des interfaces ATM et WAN à haute vitesse. Sa grande densité de ports permet de gérer facilement le grand nombre d'interfaces requis pour une connectivité de site distant. Les concepteurs de réseaux peuvent déployer ces routeurs dans un environnement WAN, afin de bénéficier des nombreux types d'offres de services des opérateurs, incluant les épines dorsales ATM. Ces routeurs offrent un débit de 2,1 Gbit/s.

En tant que routeurs haut de gamme, les routeurs de la série Cisco 7500 fournissent des alimentations redondantes, mais aussi un processeur de commutation de route (RSP, *Route Switch Processor*) redondant, et assurent un équilibrage de charge pour IP (d'autres protocoles sont prévus) lorsque ce processeur est présent. Le Cisco 7500 a été reconnu comme le routeur d'entreprise par excellence. Il peut également jouer le rôle de routeur ATM de frontière pour un campus ou une entreprise, grâce à son support de la technologie ATM.

Commutateurs d'opérateur

Au-delà des réseaux privés, les plates-formes ATM sont aussi largement déployées par les fournisseurs de services, à la fois au niveau de l'équipement de télécommunication du client (CPE, *Customer Premises Equipment*) et au sein de réseaux publics. Un tel équipement supporte plusieurs services WAN, incluant la commutation Frame Relay, les services fondés sur IP, l'interconnexion ATM NNI et les services ATM publics qui exploitent une infrastructure ATM commune. Ces commutateurs ATM d'entreprise haut de gamme, appelés également *commutateurs d'opérateur*, seront souvent utilisés pour ces applications de réseaux publics en raison de leurs grandes disponibilité et redondance, leur support de nombreuses interfaces et leur faculté à intégrer la voix et les données. Le Cisco BPX 8600, mentionné plus haut, est un exemple de commutateur ATM d'opérateur. Avec le développement de l'industrie des télécommunications, plus particulièrement en Europe, la demande pour ce type de commutateurs va augmenter.

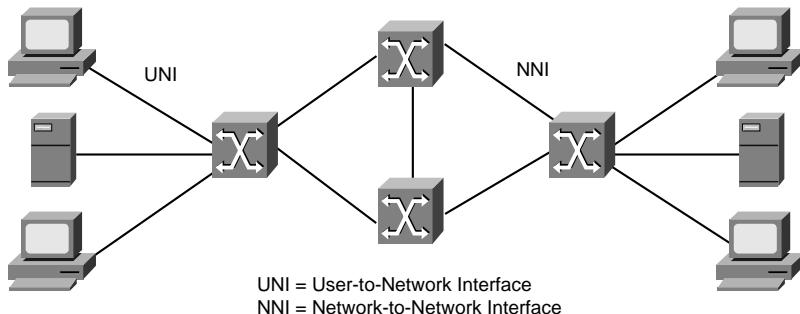
Structure d'un réseau ATM

ATM se fonde sur le concept de deux points d'extrémité qui communiquent au moyen de commutateurs intermédiaires. Comme l'illustre la Figure 5.7, un réseau ATM est constitué d'une série de commutateurs et d'équipements d'extrémité. Ces derniers peuvent être des stations terminales avec connexion ATM, des serveurs avec connexion ATM ou des routeurs avec connexion ATM.

Comme le montre la Figure 5.7, il existe deux types d'interfaces sur un réseau ATM :

- UNI (*User-to-Network Interface*, interface utilisateur-réseau) ;
- NNI (*Network-to-Network Interface*, interface réseau-réseau).

Figure 5.7
Composants
d'un réseau ATM.



La connexion UNI est constituée d'un équipement d'extrémité et d'un commutateur ATM privé ou public. Les premiers développeurs de la technologie ATM étaient principalement confrontés à cette interface lors de la conception de produits pour le marché. Quant à la connexion NNI, elle est établie entre deux commutateurs ATM. Ces deux interfaces peuvent être supportées par des connexions physiques différentes.

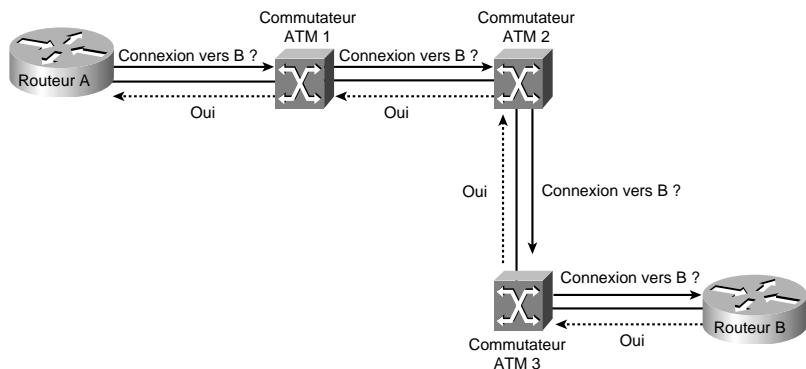
Outre les protocoles UNI et NNI, le Forum ATM a défini un ensemble de protocoles pour supporter l'émulation LAN, appelé LANE (*LAN Emulation*). LANE est une technologie de réseau employée

par les concepteurs afin de connecter des réseaux locaux existants, tels qu'Ethernet ou Token Ring, au moyen d'équipements reliés à ATM. La principale demande du marché en ce qui concerne les commutateurs ATM de frontière est née du besoin de relier des réseaux Ethernet et Token Ring à des réseaux ATM. Les premiers développeurs d'ATM pensaient qu'Ethernet et Token Ring seraient remplacés par ATM au fur et à mesure que cette technologie gagnerait en popularité, mais les technologies Ethernet commuté à 100 Mbit/s et Gigabit Ethernet ont assuré la continuité de ces réseaux.

Fonctionnement d'un réseau ATM

Sur un réseau ATM, une connexion doit avoir été établie entre deux points d'extrémité pour qu'un transfert de données puisse avoir lieu. Cette connexion est réalisée au moyen d'un protocole de signalisation (voir Figure 5.8).

Figure 5.8
Etablissement
d'une connexion
sur un réseau ATM.



Comme le montre la Figure 5.8, les étapes suivantes doivent être accomplies afin que le routeur A puisse se connecter au routeur B :

1. Le routeur A envoie un paquet de requête de signalisation vers le commutateur ATM auquel il est directement connecté (commutateur ATM 1).
Cette requête contient l'adresse ATM du routeur B, ainsi que tout paramètre de qualité de service (QoS) requis pour la connexion.
2. Le commutateur ATM 1 rassemble le paquet de signalisation du routeur A et l'examine.
3. Si le commutateur ATM 1 dispose d'une entrée pour l'adresse ATM du routeur B dans sa table de commutation et qu'il peut gérer la qualité de service demandée pour la connexion, il établit la connexion virtuelle et transmet la requête au commutateur suivant (commutateur ATM 2) sur le chemin.
4. Chaque commutateur le long de l'itinéraire vers le routeur B rassemble et examine le paquet de signalisation avant de le transmettre au commutateur suivant si les paramètres de qualité de service peuvent être gérés. Chaque commutateur établit également la connexion virtuelle lorsque le paquet de signalisation est transmis.

Si l'un des commutateurs sur le chemin ne peut pas gérer les paramètres de qualité de service demandés, la requête est rejetée et un message est renvoyé vers le routeur A, proposant une qualité de service disponible plus faible.

5. Lorsque le paquet de signalisation arrive sur le routeur B, celui-ci le réassemble et l'évalue. S'il peut gérer la qualité de service requise, il répond avec un message d'acceptation. Au fur et à mesure que ce message est retransmis vers le routeur A, les commutateurs établissent un circuit virtuel.

NOTE

Un *canal virtuel* est l'équivalent d'un *circuit virtuel*. Il désigne une connexion logique entre les deux extrémités d'une connexion. Un *chemin virtuel* est un groupement logique de circuits virtuels, qui permet à un commutateur ATM d'effectuer des opérations sur des groupes de circuits virtuels.

6. Le routeur A reçoit le message d'acceptation de la part du commutateur ATM auquel il est directement connecté (commutateur ATM 1), ainsi que les valeurs d'identifiant de chemin virtuel (VPI, *Virtual Path Identifier*) et d'identifiant de canal virtuel (VCI, *Virtual Channel Identifier*) qui doivent être utilisées avec les cellules envoyées vers le routeur B.

NOTE

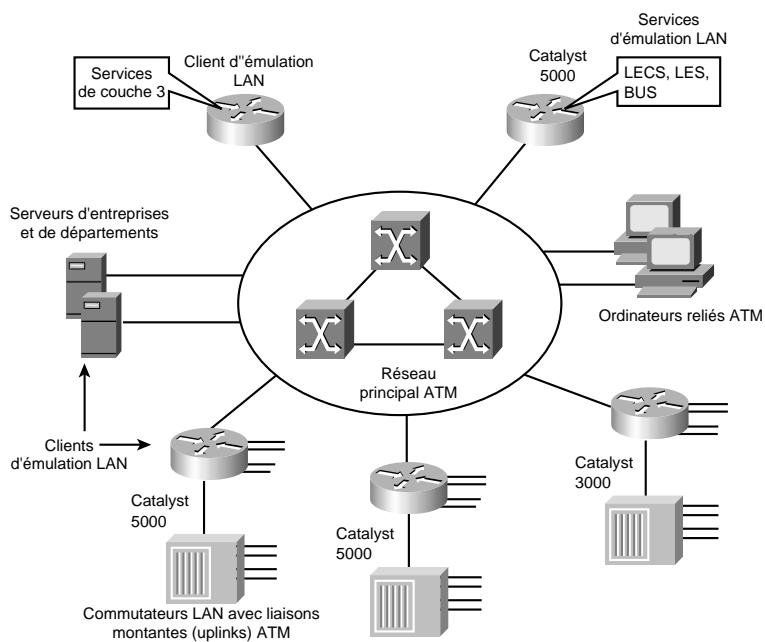
Les cellules ATM se composent de 5 octets d'informations d'en-tête et de 48 octets de données utiles. Les champs VPI et VCI dans l'en-tête sont utilisés pour router les cellules à travers les réseaux ATM. Ils permettent d'identifier le prochain segment de réseau qu'une cellule doit emprunter, en direction de sa destination finale.

Rôle de LANE

Le Forum ATM a défini un standard pour l'émulation LAN : LANE (*LAN Emulation*). Comme mentionné précédemment, LANE est une technologie que les concepteurs de réseaux peuvent déployer afin de relier des réseaux locaux Ethernet et Token Ring existants à des réseaux ATM. Elle utilise l'encapsulation MAC (couche 2 du modèle OSI) pour supporter le plus grand nombre possible de protocoles de couche 3 OSI. Le résultat final est que tous les équipements connectés à un LAN émulé (ELAN, *Emulated LAN*) semblent situés sur un seul segment ponté. De cette manière, AppleTalk, IPX, IP et d'autres protocoles peuvent présenter des caractéristiques de performances semblables à celle d'un environnement ponté traditionnel qui utilise le même média. Toutefois, les communications entre réseaux ELAN impliquent toujours l'utilisation de routeurs de niveau 3, ajoutant une latence inutile sur le réseau ATM qui n'aurait normalement jamais besoin des services de niveau 3, sauf pour supporter des réseaux LAN Ethernet et Token Ring existants. En réponse à ce problème, le Forum ATM a défini la spécification MPOA (*Multiprotocol over ATM*).

La Figure 5.9 illustre un exemple de réseau LANE ATM qui utilise des routeurs pour les communications inter-ELAN.

Figure 5.9
Composants d'un réseau LANE ATM.



Lorsque MPOA est utilisé, les stations ATM ont l'impression que les communications inter-ELAN mettent en œuvre un raccourci direct vers la station de destination, ce qui évite le phénomène de latence qui se produit sur la topologie illustrée.

Composants LANE

Les dispositifs suivants figurent parmi les composants LANE :

- **Client d'émulation LAN (LEC, LAN Emulation Client).** Systèmes ATM qui supportent à la fois les réseaux LAN, comme Ethernet et Token Ring, et les réseaux LANE ATM. Parmi eux figurent la famille de commutateurs Catalyst et les séries de routeurs Cisco 7500, 7000, 4500 et 4000, qui acceptent les connexions ATM. Le LEC émule une interface vers un LAN existant pour les protocoles de plus haut niveau, et assure la résolution d'adresse, la transmission de données et l'enregistrement d'adresses MAC auprès du serveur LANE (LES). Il communique avec d'autres LEC, via des connexions de canaux virtuels (VCC, Virtual Channel Connection) ATM.
- **Serveur de configuration d'émission LAN (LECS, LAN Emulation Configuration Server).** Les LECS maintiennent une base de données de réseaux locaux émulés (ELAN) et les adresses ATM des serveurs d'émission LAN (LES) qui contrôlent les ELAN. Ils acceptent les requêtes de la part de clients LEC et répondent avec l'adresse ATM du serveur LES qui sert le ELAN.
- **Serveur d'émission LAN (LES, LAN Emulation Server).** Le LES fournit un point de contrôle central pour tous les LEC. Les LEC maintiennent une connexion VCC Control Direct vers le LES afin de transmettre les informations d'enregistrement et de contrôle. Le LES maintient une connexion VCC point-multipoint, connue sous l'appellation Control Distribute, vers

tous les LEC. Cette connexion est utilisée uniquement pour transmettre des informations de contrôle. Lorsque de nouveaux LEC rejoignent le ELAN ATM, ils sont ajoutés en tant que feuilles à l'arbre *Control Distribute*.

- **Serveur BUS (*Broadcast and Unknown Server*)**. Le serveur BUS agit comme point central pour la distribution des diffusions broadcast (diffusions générales) et multicast (diffusions restreintes). ATM est une technologie point-à-point, sans support pour la communication broadcast. LANE résout ce problème en centralisant le support de la diffusion broadcast sur le BUS. Chaque LEC doit définir une connexion VCC *Multicast Send* vers le BUS. Celui-ci ajoute ensuite le LEC en tant que feuille à sa connexion VCC point-multipoint, également appelée VCC *Multicast Forward*.

Le BUS agit également comme serveur multicast. LANE est défini au niveau de la couche d'adaptation ATM ALL5, qui spécifie un suffixe simple devant être ajouté à une trame avant de la diviser en cellules ATM. Le problème est qu'il n'existe aucun moyen de distinguer les cellules qui proviennent de différents émetteurs lorsqu'elles sont multiplexées sur un canal virtuel. Puisque l'on suppose que les cellules sont reçues en séquences, lorsque la cellule de fin de message (EOM, *End Of Message*) arrive, toutes les cellules déjà arrivées devraient simplement être rassemblées.

Le BUS prélève les séquences de cellules sur chaque VCC *Multicast Send* et les réorganise en trames. Lorsqu'une trame complète est reçue, elle est placée en file d'attente afin d'être envoyée vers tous les clients LEC de la connexion VCC *Multicast Forward*. De cette manière, toutes les cellules d'une trame de données spécifique sont assurées d'être transmises dans l'ordre, et non intercalées avec des cellules d'autres trames sur la connexion VCC point-multipoint.

Etant donné que LANE est défini au niveau de la couche 2 du modèle OSI, le serveur LECS est le seul point de contrôle de sécurité disponible. Lorsqu'il sait où est situé le LES et qu'il a réussi à joindre le réseau ELAN, le LEC est libre d'envoyer n'importe quel trafic (malveillant ou non) sur le ELAN ponté. Des filtres de sécurité de niveau 3 peuvent être implémentés uniquement sur le routeur qui assure le routage de l'ELAN en question vers d'autres ELAN. Mais, une fois que MPOA a établi un raccourci pour contourner le routeur, cette sécurité n'est plus effective. Par conséquent, plus le ELAN est grand, plus il est exposé aux risques de violation de la sécurité.

Fonctionnement de LANE

Un ELAN fournit une communication de niveau 2 entre tous ses utilisateurs. Un ou plusieurs réseaux ELAN peuvent être exécutés sur le même réseau ATM. Toutefois, chaque ELAN est indépendant des autres, et leurs utilisateurs respectifs ne peuvent communiquer directement. Comme mentionné précédemment, la communication entre réseaux ELAN n'est possible que par l'intermédiaire de MPOA ou de routeurs.

Un ELAN fournit une communication de niveau 2, il peut donc être assimilé à un domaine de broadcast. De plus, les sous-réseaux IP et les réseaux IPX qui sont définis sur des équipements de niveau 3, tels que des routeurs, sont fréquemment mis en correspondance avec des domaines de broadcast (à l'exception de l'adressage secondaire). Cela permet d'assigner un sous-réseau IP ou un réseau IP à un ELAN.

Un ELAN est contrôlé par un seul couple de serveurs LES/BUS, et l'assignation de l'adresse ATM de son serveur d'émulation LES est définie dans la base de données LECS. Un ELAN se compose de plusieurs LEC ; il peut s'agir d'un réseau Ethernet ou Token Ring, mais non des deux à la fois.

Afin qu'un ELAN puisse fonctionner correctement, ses clients LEC doivent être opérationnels. Chaque LEC doit passer par une séquence d'initialisation, décrite dans les sections suivantes.

Mise en œuvre de LANE

Dans le cadre du fonctionnement normal de la technologie LANE, le LEC doit d'abord localiser le LECS afin de découvrir le réseau ELAN auquel il doit se joindre. Le LEC recherche spécifiquement l'adresse ATM du LECS qui sert le ELAN en question.

Recherche du serveur LECS

Pour résoudre l'adresse ATM du LECS, le LEC suit la procédure suivante :

1. Le LEC interroge le commutateur ATM, via l'interface ILMI (*Interim Local Management Interface*). Le commutateur dispose d'une variable MIB, définie avec l'adresse ATM du LECS. Le LEC peut ensuite utiliser la signalisation UNI pour contacter le LECS.
2. Le LEC recherche une adresse ATM permanente, spécifiée en tant qu'adresse ATM LECS par le Forum ATM.
3. Le LEC accède au circuit virtuel permanent (PVC, *Private Virtual Circuit*) 0/17, un PVC "connu".

Interrogation du LECS

Le LEC crée un paquet de signalisation avec l'adresse ATM du LECS. Il signale une connexion VCC *Configure Direct* et émet une requête LE_CONFIGURE_REQUEST sur cette connexion. Les informations contenues dans cette requête sont comparées à celles de la base de données du LECS. L'adresse ATM source est plus couramment utilisée pour placer un LEC dans un ELAN spécifique. Si une entrée correspondante est localisée, une réponse LE_CONFIGURE_RESPONSE est renvoyée avec l'adresse ATM du serveur LES qui sert le réseau ELAN recherché.

Configuration de la base de données LECS

Vous pouvez configurer la base de données LECS à l'aide de l'une des trois méthodes suivantes :

- **Configurer les noms ELAN sur le LEC.** Dans cette configuration, tous les clients LEC sont configurés avec un nom de ELAN qu'ils peuvent ajouter à leurs requêtes LE_CONFIGURE_REQUEST. C'est la forme la plus basique de la base de données LECS : il faut seulement qu'elle contienne la liste des réseaux ELAN, avec l'adresse ATM de leurs serveurs LES correspondants. Dans une telle configuration, tous les clients LEC qui demandent spécifiquement à joindre un ELAN donné reçoivent l'adresse ATM du LES correspondant. Un LEC qui ne sait pas quel ELAN joindre peut être assigné à un ELAN par défaut, si un tel réseau est configuré dans la base de données LECS.

Voici un exemple d'assignation LEC-ELAN sur un LEC :

```
lane database test-1
name finance server-atm-address 47.0091.8100.0000.0800.200c.1001.
```

```

0800.200c.1001.01
name marketing server-atm-address 47.0091.8100.0000.0800.200c.1001.
0800.200c.1001.02
default-name finance

```

- **Configurer une assignation LEC-ELAN dans la base de données LECS.** Dans cette configuration, toutes les informations sont centralisées dans la base de données LECS. Les clients LEC n'ont pas de manipulations à faire et peuvent simplement interroger le LECS pour déterminer quel ELAN joindre. Bien qu'il s'agisse d'une configuration plus coûteuse en temps, elle permet d'assurer un meilleur contrôle sur tous les réseaux ELAN. Par conséquent, elle peut être utile pour renforcer la sécurité.

Avec cette méthode, les clients LEC sont identifiés par leur adresse ATM ou leur adresse MAC. Puisque l'emploi de préfixes d'adresse ATM avec caractères de substitution est supporté, il peut être utile de prévoir des relations du type : "Pour tout LEC qui se joint, assigner un préfixe A à l'ELAN X". Voici un exemple d'assignation LEC-ELAN dans la base de données LECS :

```

lane database test-2
name finance server-atm-address 47.0091.8100.0000.0800.200c.1001.
0800.200c.1001.01
name marketing server-atm-address 47.0091.8100.0000.0800.200c.1001.
0800.200c.1001.02
default-name finance

client-atm-address 47.0091.8100.0000.08 name finance
client-atm-address 47.0091.8100.0000.09 name marketing

mac-address 00c0.0000.0100 name finance
mac-address 00c0.1111.2222 name marketing

```

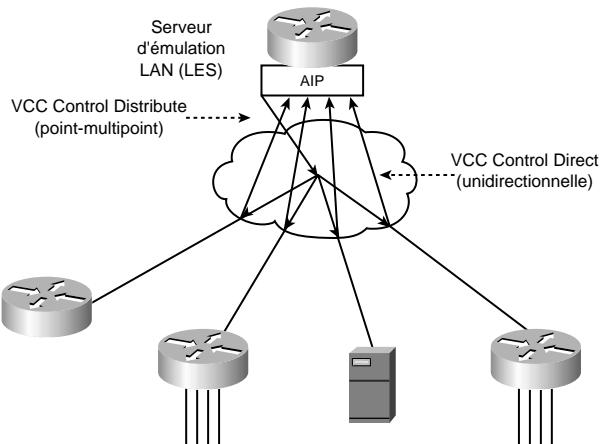
- **Combinaison hybride.** Vous pouvez configurer une combinaison des deux méthodes précédentes.

Enregistrement auprès du LES

Après que le LEC a découvert l'adresse ATM du LES désiré, il abandonne la connexion avec le serveur LECS, crée un paquet de signalisation avec l'adresse ATM du LES, puis signale une connexion VCC *Control Direct*. Après établissement de la connexion VCC, le LES envoie une requête LE_JOIN_REQUEST, qui contient l'adresse ATM du LEC ainsi que l'adresse MAC qu'il souhaite enregistrer avec le ELAN. Ces informations sont maintenues pour que deux LEC n'enregistrent pas la même adresse MAC ou ATM.

A réception de la demande d'enregistrement, le LES vérifie la requête, via une connexion propre avec le LECS, confirmant ainsi l'appartenance du client. Après une vérification réussie, le LES ajoute le LEC en tant que feuille à sa connexion VCC *Control Distribute*. Enfin, le LES envoie au LEC une réponse LE_JOIN_RESPONSE qui contient un identifiant unique de client LANE (LECID, *LAN Emulation Client ID*). Cet identifiant est utilisé par le LEC pour filtrer ses propres diffusions broadcast à partir du serveur BUS. La Figure 5.10 illustre des exemples de connexions LES.

Figure 5.10
Connexions LES.



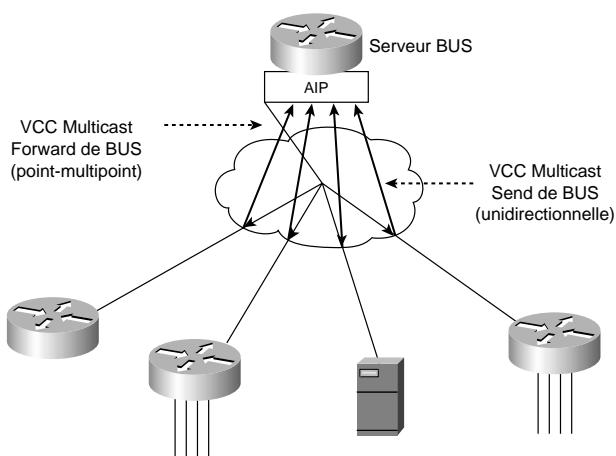
Recherche du serveur BUS

Après s'être enregistré avec succès auprès du LES, la première tâche du LEC consiste à trouver l'adresse ATM du serveur BUS, afin de rejoindre le groupe de broadcast. Le LEC crée une requête LE_ARP_REQUEST avec l'adresse MAC 0xFFFFFFFF. Ce paquet spécial est envoyé sur la connexion VCC *Control Direct* vers le LES. Le LES reconnaît que le client recherche le serveur BUS et envoie une réponse avec l'adresse ATM du BUS sur la connexion VCC *Control Distribute*.

Communication avec le serveur BUS

Lorsque le LEC possède l'adresse ATM du serveur BUS, il crée un paquet de signalisation avec cette adresse et signale une connexion VCC *Multicast Send*. A réception de la requête de signalisation, le BUS ajoute le LEC en tant que feuille à sa connexion point-multipoint VCC *Multicast Forward*. A ce stade, le LEC devient membre du ELAN. La Figure 5.11 illustre des exemples de connexions avec un serveur BUS.

Figure 5.11
Connexions BUS.



Résolution d'adresse

Le réel intérêt de LANE se situe au niveau du chemin de transmission ATM qu'il fournit pour le trafic dirigé (*unicast*) entre clients LEC. Lorsqu'un client LEC possède un paquet de données à envoyer vers une destination inconnue, il émet une requête LE_ARP_REQUEST vers le LES sur la connexion VCC *Control Direct*. Le LES transmet la requête sur la connexion VCC *Control Distribute* afin que toutes les stations LEC en prennent connaissance. En parallèle, les paquets de données unicast sont envoyés vers le BUS pour être transmis vers tous les points terminaux. Cette inondation ne représente pas un chemin optimal pour le trafic dirigé, et son débit est limité à 10 paquets par seconde (selon le standard LANE). Les paquets unicast continuent d'utiliser le serveur BUS, jusqu'à ce que la requête LE_ARP_REQUEST soit résolue.

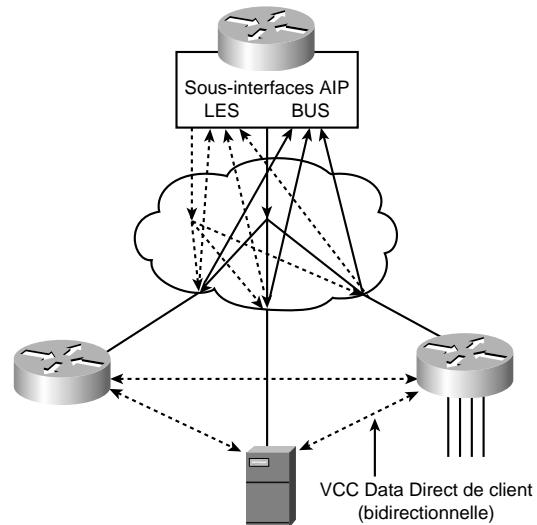
Si un équipement tel un pont ou un commutateur exécutant le client LEC participe au réseau ELAN, il traduit et transmet le protocole ARP sur son interface LAN. L'un des LEC devrait émettre une réponse LE_ARP_RESPONSE et l'envoyer vers le LES, qui le transmettrait sur la connexion VCC *Control Distribute* afin que tous les clients LEC prennent connaissance de la nouvelle association d'adresse MAC-ATM. L'inondation à raison de 10 paquets par seconde peut ensuite cesser.

Lorsque le LEC demandeur reçoit la réponse à la requête ARP, il possède l'adresse ATM du LEC qui représente l'adresse MAC recherchée. Il doit alors se signaler directement auprès de l'autre LEC et définir une connexion VCC *Data Direct* à utiliser ensuite pour le trafic dirigé entre les LEC.

En attendant la réponse de résolution à sa requête ARP, le LEC transmet le trafic unicast vers le BUS. En revanche, après résolution de la requête, un nouveau chemin optimal devient disponible. Mais si le LEC converge immédiatement vers ce nouveau chemin, les paquets risquent d'arriver dans le désordre. Pour prévenir une telle situation, le standard LANE prévoit un paquet de terminaison (*flush*).

Figure 5.12

Réseau ELAN entièrement relié.



Lorsque la connexion VCC *Data Direct* devient disponible, le LEC génère un paquet *flush* et l'envoie au serveur BUS. Lorsque le LEC reçoit son propre paquet *flush* sur la connexion VCC *Multicast Forward*, il en déduit que tous les paquets unicast précédemment envoyés ont déjà été transmis. Le nouveau chemin, *via* la connexion VCC *Data Direct*, peut alors être emprunté en toute sécurité. La Figure 5.12 présente un exemple de réseau ELAN entièrement relié.

Implémentation de LANE

Comme le montre le Tableau 5.3, les fonctionnalités de LANE (LECS, LEC, LES et BUS) peuvent être implémentées sur différents équipements Cisco.

Tableau 5.3 : Implémentation Cisco de LANE

Produits Cisco	Composants LANE disponibles	Version de logiciel requise
Série de commutateurs Catalyst 5000	LECS, LES, BUS, LEC	Module ATM version 2.0 ou ultérieure
Série de commutateurs Catalyst 3000	LECS, LES, BUS, LEC	Module ATM version 2.1 ou ultérieure
Série de routeurs Cisco 7000	LECS, LES, BUS, LEC	Cisco IOS version 11.0 ou ultérieure
Série de routeurs Cisco 7500	LECS, LES, BUS, LEC	Cisco IOS version 11.1 ou ultérieure
Série de routeurs Cisco 4500 et 4000	LECS, LES, BUS, LEC	Cisco IOS version 11.1 ou ultérieure

Ces fonctions seront définies sur les interfaces et sous-interfaces ATM. Une *sous-interface* est une interface logique qui fait partie d'une interface physique, comme la fibre optique Optical Carrier 3 (OC-3). Les interfaces ATM sur les routeurs Cisco et le module ATM sur le commutateur Catalyst 5000 peuvent être divisés logiquement en un maximum de 255 sous-interfaces logiques.

Cette section aborde donc l'implémentation de réseaux LANE ATM. Elle couvre les sujets suivants :

- considérations sur la conception LANE ;
- redondance LANE.

Considérations sur la conception LANE

Voici quelques considérations d'ordre général à prendre en compte lors de l'implémentation de la technologie LANE :

- L'AIP (*ATM Interface Processor*) sert d'interface au circuit de commutation ATM pour transmettre et recevoir des données. Le débit est déterminé par le module d'interface de la couche physique PLIM (*Physical Layer Interface Module*).
- Un serveur LECS actif supporte tous les réseaux ELAN.
- Chaque réseau ELAN est constitué d'un couple de serveurs LES/BUS et d'un certain nombre de clients LEC.

- Les fonctionnalités LES et BUS doivent être définies sur la même sous-interface et ne peuvent être séparées.
- Il ne peut y avoir qu'un seul couple de serveurs LES/BUS actif par sous-interface.
- Il ne peut y avoir qu'un seul couple de serveurs LES/BUS actif par ELAN.
- Le standard LANE Phase 1 actuel ne fournit pas de redondance LES/BUS.
- Les dispositifs LECS et LES/BUS peuvent être représentés par différents routeurs, ponts ou stations de travail.
- Les connexions VCC peuvent être, soit des circuits virtuels commutés (SVC), soit des circuits virtuels permanents (PVC), sachant que la configuration et la complexité de conception d'un PVC peuvent transformer un petit réseau en un environnement complexe et difficile à administrer.
- Si un LEC sur une sous-interface de routeur reçoit une adresse IP, IPX ou AppleTalk, le protocole en question est routable par l'intermédiaire de ce LEC. S'il y a plusieurs LEC sur un routeur et qu'ils reçoivent des adresses de protocoles, le routage interviendra entre les ELAN. Pour que le routage entre réseaux ELAN fonctionne correctement, un ELAN ne devrait se trouver que dans un seul sous-réseau pour un protocole particulier.

PNNI dans des réseaux LANE

Les concepteurs de réseaux peuvent déployer PNNI (*Private Network-to-Network Interface*) comme protocole de routage de niveau 2 pour la gestion de bande passante, la distribution de trafic et la redondance de chemins sur les réseaux LANE. PNNI est un protocole de routage ATM utilisé afin d'acheminer les demandes de connexion (*call setup*) ; il est implémenté sur les commutateurs ATM. La plupart des réseaux LANE se composent de plusieurs commutateurs ATM et emploient généralement le protocole PNNI.

NOTE

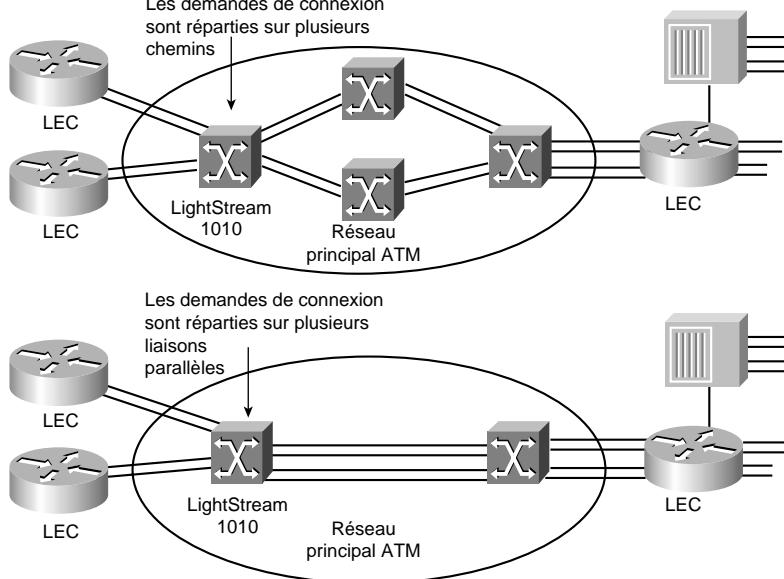
Bien que PNNI soit un protocole de routage avancé et qu'il supporte le routage fondé sur la qualité de service (QoS), cet aspect particulier de PNNI n'est pas traité dans ce chapitre, car la plupart des réseaux LANE sont basés sur un service de livraison "au mieux" (*best-effort delivery*).

PNNI présente certaines fonctionnalités qui peuvent permettre de faire évoluer les réseaux LANE, parmi lesquelles :

- support de l'équilibrage de charge des demandes de connexion sur plusieurs chemins situés entre deux stations terminales ;
- support de l'équilibrage de charge sur plusieurs liaisons parallèles ;
- support de la redondance de liaisons et de chemins avec convergence rapide ;
- excellentes performances pour les demandes de connexion à travers plusieurs tronçons, au moyen de la fonction de routage d'arrière-plan (*background routing*).

La Figure 5.13 illustre la façon dont le commutateur LightStream 1010 supporte l'équilibrage de charge.

Figure 5.13
Equilibrage de charge des demandes de connexion sur plusieurs chemins et liaisons.



Comme le montre la Figure 5.13, l'équilibrage de charge des appels est activé par défaut sur le commutateur LightStream 1010, à l'inverse du routage d'arrière-plan. Ce type de routage peut-être vu comme l'acheminement des demandes *via* un chemin choisi à partir d'une base d'itinéraires calculés au préalable. Le processus de routage d'arrière-plan établit une liste de tous les itinéraires possibles vers toutes les destinations, par le biais de toutes les catégories de service, par exemple CBR (*Constant Bit Rate*), VBR-RT (*Virtual Bit Rate-Real Time*), VBR-NRT (*Virtual Bit Rate-Non Real Time*) et ABR-UBR (*Available Bit Rate-Unspecified Bit Rate*).

Lorsqu'un appel a lieu depuis un point A vers un point B, le protocole PNNI choisit une route en cache à partir de la table de routage d'arrière-plan, au lieu de calculer une route à la demande. Ce procédé allège la charge du processeur et permet un traitement plus rapide des demandes de connexion.

Le routage d'arrière-plan peut être utile sur les réseaux qui possèdent une topologie stable quant à la qualité de service (QoS). Il n'est cependant pas efficace sur les réseaux dont la topologie change rapidement, tels les réseaux de fournisseurs de services Internet ou les réseaux d'opérateurs. Les réseaux LANE de campus peuvent exploiter efficacement cette fonctionnalité, car tous les SVC appartiennent aux catégories UBR ou ABR. Pour activer cette fonctionnalité, exécutez la commande suivante :

```
atm router pnni
node 1 level 56
bg-routes
```

L'implémentation actuelle de PNNI sur le commutateur LightStream 1010 est totalement conforme à la spécification PNNI version 1 du Forum ATM. La licence d'image PNNI par défaut du LightStream supporte un seul niveau de hiérarchie, dans lequel plusieurs groupes d'homologues peuvent être interconnectés par l'intermédiaire de IISP ou d'autres commutateurs gérant la hiérarchie PNNI.

Des licences d'image PNNI supplémentaires permettent de supporter plusieurs niveaux de hiérarchie de routage.

Les protocoles PNNI ont été conçus pour pouvoir s'adapter à différentes tailles de réseaux ATM, depuis les petits réseaux de campus qui comprennent quelques commutateurs jusqu'à l'ensemble du réseau Internet et ses millions de commutateurs. Ce degré d'évolutivité, supérieur à celui de n'importe quel protocole de routage existant, induit une très grande complexité au niveau du protocole PNNI.

Plus particulièrement, il exige le support de plusieurs niveaux de hiérarchie de routage basé sur l'emploi de préfixes de l'espace d'adresse ATM de 20 octets. Le niveau le plus bas de la hiérarchie consiste en un seul groupe d'homologues, au sein duquel tous les commutateurs se communiquent l'ensemble des métriques d'accessibilité et de qualité de service (QoS). Cette situation est analogue, par exemple, à une seule zone du protocole OSPF.

Ensuite, plusieurs groupes d'homologues à un certain niveau de la hiérarchie sont rassemblés en des groupes d'homologues de niveau supérieur, au sein desquels chaque groupe de niveau inférieur est représenté par un seul *leader de groupe d'homologues*. Toute la hiérarchie PNNI est ainsi formée par itérations de ce processus de rassemblement de groupes. Chaque niveau de la hiérarchie est identifié par un préfixe de l'espace d'adresse ATM, ce qui signifie que PNNI pourrait en théorie contenir plus de 100 niveaux de hiérarchie de routage. Toutefois, quelques niveaux suffisent pour la plupart des réseaux. Afin de bénéficier d'une telle évolutivité, il faut implémenter des mécanismes très complexes afin de supporter et mettre en œuvre les nombreux niveaux de hiérarchie, et d'élire les leaders de groupes d'homologues, au sein de chaque groupe, à chaque niveau.

Evolution d'un ELAN : problèmes engendrés par le protocole par arbre recouvrant

Le protocole par arbre recouvrant (*Spanning Tree*) est un protocole de niveau 2, supporté par les commutateurs et les ponts afin d'éviter les risques d'apparition de boucles temporaires sur les réseaux qui comprennent des liaisons redondantes. Etant donné qu'un LEC ponte le trafic Ethernet/TOKEN Ring au-dessus d'une épine dorsale ATM, les unités de données du protocole de pontage par arbre recouvrant (BPDU, *Bridge Protocol Data Units*) sont transmises sur la totalité de l'ELAN. Le réseau ATM apparaît comme un réseau Ethernet/TOKEN Ring partagé pour le processus d'arbre recouvrant à la frontière des commutateurs de niveau 2.

La topologie d'arbre recouvrant d'un réseau fondé sur la technologie LANE est beaucoup plus simple que celle d'un réseau à commutation de trames pur qui emploie le protocole Spanning Tree. Il s'ensuit que les temps de convergence avec un arbre recouvrant, qui peuvent constituer un problème majeur sur de grands réseaux à commutation de trames, ne présentent pratiquement aucune difficulté sur des réseaux LANE. Notez que le protocole Spanning Tree doit effectuer une reconvergence en cas de défaillance au niveau des dispositifs de frontière ou à l'intérieur du réseau ATM. S'il se révèle nécessaire d'optimiser le temps de convergence avec une valeur inférieure ou supérieure, le paramètre de délai de transmission peut être utilisé.

Redondance LANE

Bien que la technologie LANE permette aux concepteurs de connecter leurs réseaux locaux existants à un réseau ATM, la version 1.02 de LANE ne définit pas de mécanismes pour implémenter la redondance et la tolérance aux pannes au niveau des services LANE. En conséquence, ces services

peuvent représenter une source de pannes. De plus, la redondance de routeurs et des chemins-liaisons est également un facteur à prendre en compte.

Les concepteurs peuvent employer différentes techniques pour implémenter des réseaux LANE fiables et tolérants envers les pannes :

- Le protocole SSRP (*Simple Server Replication Protocol*) assure une redondance des services LANE avec Cisco et tout LEC d'un fabricant tiers.
- Le protocole HSRP (*Hot Standby Router Protocol*) sur LANE assure la redondance du routeur par défaut configuré sur les stations terminales IP.
- Des modules redondants supportés par les commutateurs ATM de Cisco.
- Le protocole d'arbre recouvrant Spanning Tree sur les commutateurs Ethernet-ATM.

Nous allons examiner ces différentes techniques, ainsi que les règles de conception et les problèmes à considérer lors de l'implémentation de réseaux LANE redondants. Nous commencerons par le protocole SSRP, qui a été développé pour fournir des services LANE redondants.

Bien que de nombreux fabricants proposent des implémentations de services LANE redondants depuis un certain temps, aucune ne respecte la spécification LANE 1.0. Elles ne peuvent donc pas interopérer avec d'autres implémentations tierces. Le protocole SSRP, qui respecte cette spécification, peut assurer l'interaction avec des implémentations tierces, garantissant ainsi l'interopérabilité des réseaux ATM.

Problèmes sur un réseau LANE

Le principal problème rencontré avec un réseau LANE 1.0 tient au fait qu'un LEC ne peut accéder à tout moment qu'à un seul ensemble de composants de services LANE. Il en résulte les limitations suivantes :

- un seul LECS supporte tous les ELAN ;
- il ne peut y avoir qu'un seul couple de serveurs LES/BUS par ELAN.

Une panne sur n'importe lequel de ces composants de service affecte le fonctionnement du réseau de la façon suivante :

- **Panne de LECS.** La panne d'un serveur LECS affecte tous les ELAN sous son contrôle, car il représente leur point de contrôle d'accès. Bien que les réseaux LANE existants puissent continuer à fonctionner normalement (en supposant la présence de clients LEC Cisco uniquement), aucun nouveau LEC ne peut rejoindre un ELAN situé sous le contrôle du LECS en panne. De plus, il est impossible pour un LEC de rejoindre son ELAN ou de modifier son appartenance, car le serveur LES ne peut procéder à la vérification du LEC.
- **Panne de LES/BUS.** Le couple de serveurs LES/BUS est nécessaire au bon fonctionnement d'un réseau ELAN. Le LES fournit le service LE_ARP pour les correspondances d'adresses ATM-MAC, tandis que le BUS fournit les services de diffusion broadcast et d'adresse inconnue pour un ELAN donné. Par conséquent, une panne sur l'un de ces deux serveurs affecte immédiatement la communication sur l'ELAN. Toutefois, seul l'ELAN servi par le couple de serveurs est touché.

Il est évident que ces problèmes peuvent constituer une limitation sur les réseaux qui requièrent résistance et fiabilité. Ils peuvent représenter un facteur déterminant dans le choix d'implémenter des

réseaux ATM basés sur la technologie LANE. De plus, d'autres considérations peuvent avoir des implications sur l'ensemble de la résistance d'un environnement LANE, comme le placement des composants de services LANE au sein du réseau ATM.

Résistance des réseaux LANE

L'augmentation de la résistance d'un réseau basé LANE implique essentiellement davantage de robustesse au niveau des composants de services LANE, tels que les serveurs LECS, LES et BUS. Cette résistance est assurée par le protocole SSRP, via une combinaison de dispositifs principal-secondaire pour les services LANE. En ce qui concerne la redondance du serveur LECS, un serveur principal est soutenu par plusieurs serveurs secondaires. La redondance LES/BUS est également gérée de façon semblable. Notez que les fonctions LES/BUS cohabitent toujours dans une implémentation Cisco et que le couple de serveurs est géré comme une seule unité en ce qui concerne la redondance.

Redondance LECS

Selon la spécification LANE 1.0, la première étape de l'initialisation d'un LEC est la connexion au LECS, afin d'obtenir l'adresse ATM du LES du réseau ELAN auquel le LEC souhaite se joindre. Pour que ce dernier puisse se connecter au LECS, plusieurs mécanismes sont définis. Tout d'abord, le LEC doit interroger le commutateur ATM auquel il est connecté, afin d'obtenir l'adresse du serveur LECS. Ce processus de découverte d'adresse est réalisé au moyen du protocole ILMI sur VPI, VCI - 0, 16.

Voici un exemple de commande de configuration qui permet d'ajouter une adresse de serveur LECS sur un commutateur LightStream 1010 :

```
atm lecs-address <adresse_NSAP_LECS> <index>
```

Avec SSRP, plusieurs adresses LECS sont configurées sur les commutateurs ATM. Un LEC qui demande l'adresse LECS d'un commutateur ATM obtient en réponse la table entière des adresses LECS. Le LEC doit ensuite tenter de se connecter à l'adresse de plus haut rang. En cas d'échec, il doit essayer l'adresse suivante dans la liste, et ainsi de suite jusqu'à la réussite de la connexion avec le serveur LECS.

Alors que le LEC tente toujours de se connecter au LECS de plus haut rang disponible, le protocole SSRP s'assure qu'un seul serveur principal répond aux requêtes de configuration provenant d'un LEC. L'établissement d'un serveur LECS principal et d'autres serveurs de secours est la fonction essentielle du protocole SSRP. Voyons comment procède SSRP pour établir un serveur LECS principal. A l'initialisation, un serveur LECS obtient la table d'adresses LECS auprès de son commutateur. Il tente ensuite de se connecter à tous les autres serveurs LECS dont le rang est inférieur au sien. Le rang est fonction de la valeur d'index dans la table d'adresses LECS.

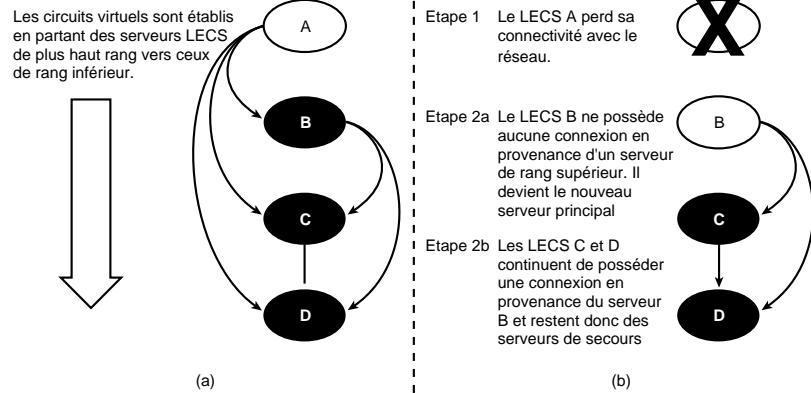
Si un serveur LECS dispose d'une connexion de circuit virtuel (VCC) en provenance d'un LECS dont le rang est supérieur au sien, il est dans le mode de secours. Aucun LECS provenant d'un rang supérieur n'est connecté au LECS de plus haut rang, lequel joue le rôle de serveur LECS principal.

La Figure 5.14 illustre la procédure de secours utilisée en cas de défaillance d'un serveur LECS principal. Le réseau LANE donné en exemple possède quatre serveurs LECS : A, B, C et D. Tous les commutateurs ATM du réseau sont configurés avec la même table d'adresses LECS. Après le

démarrage, le LECS A obtient la table d'adresses auprès du commutateur ATM qui lui est connecté, découvre qu'il possède trois serveurs LECS de rang inférieur et tente par conséquent de se connecter aux LECS B, C et D. Le serveur B se connecte aux serveurs C et D, et le serveur C au serveur D. Les connexions VCC sont établies vers le bas. Puisque le serveur A ne possède pas de connexion en provenance d'un serveur de rang supérieur, il devient le serveur LECS principal.

Figure 5.14

Redondance LECS.



Au cours du fonctionnement normal du réseau, le serveur A répond à toutes les requêtes de configuration, alors que les serveurs de secours, B, C et D, ne répondent à aucune requête. Si, pour une raison quelconque, le serveur principal tombe en panne, le serveur B perd sa connexion VCC avec le serveur A, et il en va de même pour les autres serveurs.

Dans ce cas, le serveur LECS B ne possède plus aucune connexion VCC en provenance d'un serveur de rang supérieur et devient donc le serveur LECS de plus haut rang disponible sur le réseau, c'est-à-dire le serveur principal. Les deux autres serveurs LECS, C et D, possèdent toujours des connexions en provenance de serveurs LECS de rang supérieur et continuent à fonctionner dans le mode de secours (voir l'étape 2b de la Figure 5.14).

Redondance LES/BUS

La partie du protocole SSRP qui assure la redondance du couple de serveurs LES/BUS supporte la configuration de plusieurs couples LES/BUS fonctionnant selon un modèle principal-secondaire. Toutefois, les mécanismes utilisés ici diffèrent de ceux qui servent à la redondance des serveurs LECS, décrite dans la section précédente.

Plusieurs couples de serveurs LES/BUS pour un ELAN donné sont d'abord configurés dans la base de données LECS. Chaque couple reçoit une priorité. Après l'initialisation, chaque couple établit une connexion VCC avec le LECS principal, au moyen du mécanisme de découverte d'adresse LECS. Le couple LES/BUS qui possède la priorité la plus haute et dispose d'une connexion VCC ouverte vers le LECS est désigné comme couple principal par le LECS principal.

Directives d'emploi de SSRP

Il n'y a, en théorie, aucune limite relative au nombre de serveurs LECS qui peuvent être configurés au moyen du protocole SSRP. Cependant, il est recommandé d'en configurer deux (un serveur principal et un serveur de secours) ou trois (un serveur principal et deux serveurs de secours). Une redondance supérieure ne devrait être envisagée qu'après une sérieuse analyse, car elle rendrait le réseau beaucoup plus complexe, engendrant une augmentation substantielle du temps nécessaire à son administration et à son dépannage.

Directives de configuration de SSRP

Pour supporter la stratégie de redondance de serveurs LECS, vous devez respecter les règles de configuration suivantes, sous peine de provoquer un dysfonctionnement du protocole et du réseau :

- Chaque LECS doit maintenir la même base de données de réseaux ELAN. Par conséquent, vous devez maintenir la même base de données sur tous les serveurs LECS.
- Vous devez configurer les adresses de serveurs LECS dans la table d'adressage LECS, en respectant le même ordre sur chaque commutateur ATM du réseau.
- Lors de l'utilisation du protocole SSRP avec l'adresse par défaut (*Well Known Address*), ne placez pas deux serveurs LECS sur le même commutateur ATM. Sinon, seul un serveur pourra enregistrer l'adresse par défaut auprès du commutateur (par l'intermédiaire de ILMI), ce qui pourrait entraîner des problèmes lors de l'initialisation.

Remarques sur l'interopérabilité de SSRP

SSRP peut être employé avec des LEC de fabricants tiers s'ils utilisent ILMI avec le processus de découverte d'adresse LECS et s'ils peuvent gérer de façon appropriée plusieurs adresses LECS renvoyées par le commutateur ATM. Par exemple, le LEC devra se connecter tour à tour avec tous les serveurs LECS dont l'adresse figure dans la liste retournée par le commutateur ATM. Le premier serveur LECS qui répondra à la requête de configuration sera le serveur principal.

Comportement de SSRP avec l'adresse LECS par défaut (Well Known Address)

SSRP fonctionne également avec l'adresse LECS par défaut (*Well Known Address*, 47.0079....), définie dans la spécification LANE 1.0. Le serveur LECS Cisco peut écouter au niveau de plusieurs adresses ATM en même temps. Par conséquent, il peut écouter au niveau de l'adresse par défaut et de l'adresse ATM autoconfigurée, adresses que vous pouvez afficher avec la commande **show lane default**.

Lorsque le LECS peut écouter au niveau de l'adresse par défaut, il l'enregistre auprès du commutateur ATM afin que les autres commutateurs ATM puissent annoncer des routes vers cette adresse et router toutes les demandes de connexion vers l'emplacement approprié.

Avec SSRP, il peut y avoir plusieurs LECS sur le réseau. Si chaque LECS enregistre l'adresse par défaut auprès des commutateurs auxquels il est connecté, les demandes de connexion sont routées vers les différents emplacements du réseau. Vous devez par conséquent définir une adresse autoconfigurée afin que la négociation du serveur LECS principal ait lieu en premier ; ensuite, le serveur principal enregistrera l'adresse par défaut auprès du commutateur ATM. S'il échoue, l'adresse par défaut sera modifiée avec le LECS principal.

Le code PNNI situé sur le commutateur LightStream 1010 se charge de l'annonce de la nouvelle route vers l'adresse par défaut lorsqu'intervient un changement de LECS en tant que serveur principal. Par conséquent, un LEC d'un fabricant tiers qui utilise uniquement l'adresse par défaut peut également interopérer avec SSRP. Ce protocole est la seule technique de redondance qui puisse être utilisée avec presque n'importe quel LEC commercialisé.

Pour implémenter SSRP avec l'adresse par défaut, utilisez la procédure suivante :

1. Configurez le LECS pour qu'il écoute sur l'adresse autoconfigurée (ou, si vous le souhaitez, une adresse ATM distincte que vous aurez déterminée au préalable). Cette adresse devrait être programmée sur les commutateurs ATM pour le mécanisme de découverte d'adresse du LECS.
2. Configurez chaque LECS au moyen de la commande **lane config fixed-config-atm-address** pour qu'il écoute sur l'adresse par défaut. Après avoir déterminé le LECS principal au moyen de la procédure de redondance, celui-ci enregistre l'adresse par défaut auprès des commutateurs ATM.

NOTE

L'emploi du protocole SSRP avec l'adresse par défaut (*Well Known Address*) ne donne pas de bons résultats dans certaines situations (lors d'une défaillance, par exemple) si deux LECS sont connectés au même commutateur ATM. La raison en est qu'un enregistrement d'adresse peut être dupliqué sur le même commutateur, ce qui n'est pas autorisé avec ILMI. Assurez-vous que chaque LECS soit situé sur un commutateur ATM séparé.

Comportement de SSRP en cas de partitionnement du réseau

Dans l'éventualité d'un morcellement du réseau en deux nuages ATM séparés, suite à une panne de liaison ou de commutateur d'interconnexion, chaque nuage devrait pouvoir disposer de son propre ensemble de services LANE si SSRP est configuré pour gérer les partitions de réseau.

Lors de la configuration de SSRP, aidez-vous des directives suivantes pour préparer le réseau à un éventuel partitionnement :

- Configurez chaque partition avec son propre ensemble de services LANE pouvant devenir actif en cas de morcellement du réseau. Par exemple, si vous voulez connecter deux sites ou campus par l'intermédiaire d'un réseau métropolitain (MAN) et souhaitez disposer du même réseau ELAN sur chaque site, configurez chacun d'eux avec son propre ensemble de services LANE.
- Le comportement du routage devrait être examiné attentivement lors du partitionnement d'un réseau dans le cas où un ELAN serait assigné à un réseau de niveau 3, par exemple un sous-réseau IP ou un réseau IPX, car il existe maintenant deux routes vers le même sous-réseau (en supposant qu'il existe des routeurs redondants sur le réseau). S'il n'y a pas de routeurs redondants, l'une des partitions sera effectivement isolée du reste du réseau. Le trafic intra-ELAN continuera à circuler correctement.

HSRP sur LANE

HSRP est un protocole que les concepteurs peuvent employer pour prévenir les pannes de routeurs sur le réseau. Ce protocole est échangé entre deux routeurs, dont l'un est élu pour assurer le rôle

d'interface de routage principale (ou sous-interface) pour un sous-réseau donné. L'autre routeur joue le rôle de routeur de secours dynamique (*hot standby*). Avec HSRP, une adresse IP par défaut et une adresse MAC virtuelle par défaut sont partagées par les deux routeurs qui s'échangent le protocole. Toutes les stations terminales IP utilisent cette adresse IP comme passerelle par défaut pour communiquer avec d'autres stations situées en dehors de leur sous-réseau immédiat. Par conséquent, en cas de panne du routeur principal, le routeur de secours prend en charge l'adresse de passerelle par défaut ainsi que l'adresse MAC, afin que la communication puisse se poursuivre avec les stations situées en dehors du sous-réseau.

Etant donné que HSRP est un protocole de niveau 2 qui nécessite un réseau de niveau 2 basé sur des adresses MAC, il est possible d'implémenter une récupération de type HSRP sur LANE. Les mécanismes employés sont identiques à ceux d'une interface Ethernet et peuvent être configurés au niveau sous-interface.

Modules redondants pour commutateurs ATM de Cisco

Une autre façon de répondre aux besoins d'un réseau physique en matière de redondance est d'ajouter des modules redondants sur les commutateurs ATM. Ceux de Cisco supportent des alimentations redondantes, ainsi que des modules redondants de commutation et d'interface.

Résumé

Ce chapitre a décrit la technologie ATM, les réseaux ATM et l'intégration d'ATM à des réseaux existants.

ATM possède trois couches fonctionnelles : la couche physique ATM, la couche ATM, et la couche d'adaptation ATM. ATM supporte de nombreux médias au niveau de la couche physique. La couche ATM est responsable de la livraison de la charge utile, des connexions virtuelles et de l'identification des cellules. La qualité de service est gérée au niveau de la couche d'adaptation ATM ; cette dernière offre quatre classes de trafic (AAL1, AAL2, AAL3/4 et AAL5) qui influent sur les décisions QoS.

Outre la technologie ATM, des considérations de conception concernant LANE ont été abordées, ainsi que l'offre ATM de Cisco.

6

Conception de réseaux à commutation de paquets et de réseaux Frame Relay

Par Christopher Beveridge

Ce chapitre traite de manière générale de la commutation de paquets et des réseaux Frame Relay. La technologie Frame Relay a été choisie ici, car elle illustre clairement les implications de l'interconnexion de services de commutation de paquets. Les informations fournies dans ce chapitre sont organisées autour des thèmes suivants :

- conception de réseaux hiérarchiques ;
- choix d'une topologie ;
- problèmes liés à la diffusion broadcast ;
- gestion des performances.

Ce chapitre aborde également les aspects de conception et de performances liés à l'intégration de données et de la voix sur un réseau Frame Relay.

Conception de réseaux à commutation de paquets

Lors de l'interconnexion de réseaux locaux (LAN) et de réseaux étendus (WAN) privés à l'aide de services de réseau à commutation de paquets (PSDN, *Packet Switched Data Network*), il faut trouver un compromis entre le coût et les performances. Une conception idéale optimise les services de

commutation de paquets, mais ne se traduit pas forcément par le choix de la combinaison de services la moins coûteuse. Une implémentation réussie repose sur deux règles essentielles :

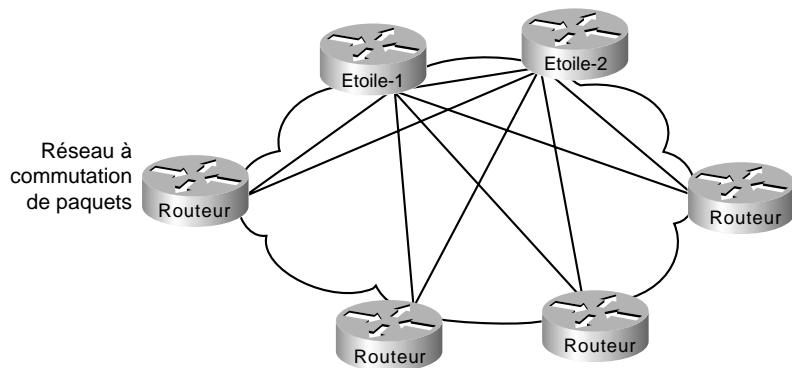
- Lorsque vous implémentez une solution à commutation de paquets, veillez à évaluer les économies potentielles, grâce aux interconnexions PSDN, en tenant compte des performances requises par votre communauté informatique.
- Créez un environnement qui soit facile à gérer, et qui puisse s'adapter au fur et à mesure que d'autres liaisons WAN se révéleront nécessaires.

Ces règles reviendront en tant que thèmes sous-jacents dans les sections suivantes.

Conception hiérarchique

L'objectif d'une conception hiérarchique est de rendre les éléments d'un grand réseau modulaires, grâce à une implémentation en couches. Le modèle global de cette organisation hiérarchique est décrit au Chapitre 2. Les couches fonctionnelles essentielles de ce modèle sont la couche d'accès local, la couche de distribution et la couche centrale (épine dorsale). Une approche hiérarchique tend essentiellement à diviser un réseau en sous-réseaux, afin de faciliter la gestion du trafic et des nœuds. Une telle conception facilite également l'évolutivité des réseaux, car elle permet d'intégrer de nouveaux modules de sous-réseaux, ainsi que de nouvelles technologies de connexion à la structure globale, sans pour autant perturber l'épine dorsale existante. La Figure 6.1 illustre l'approche de base d'une conception hiérarchique.

Figure 6.1
Interconnexion
hiérarchique avec
commutation de paquets.



Trois avantages majeurs font pencher les décisions de conception en faveur d'une solution hiérarchique :

- évolutivité ;
- facilité de gestion ;
- optimisation du trafic de contrôle broadcast et multicast.

Evolutivité des réseaux hiérarchiques

L'évolutivité est l'un des principaux avantages qui justifient l'adoption d'une approche hiérarchique pour les connexions de services de paquets. Les réseaux hiérarchiques sont plus évolutifs, car ils supportent l'ajout de modules supplémentaires, ce qui repousse les limites qui apparaissent rapidement sur des structures linéaires, non hiérarchiques.

Néanmoins, ils ont certains inconvénients qu'il faut prendre en compte : le coût des circuits virtuels, la complexité inhérente à une conception hiérarchique (particulièrement lorsqu'elle est intégrée à une topologie maillée), ainsi que les interfaces de routeur supplémentaires, nécessaires pour séparer les couches de votre hiérarchie.

Pour pouvoir tirer parti d'une conception hiérarchique, vous devez associer à votre hiérarchie de réseaux une approche complémentaire au niveau de vos topologies régionales. Les détails de conception dépendent des services de paquets implémentés, ainsi que de vos exigences en termes de tolérance aux pannes, de coût et de performances globales.

Facilité de gestion des réseaux hiérarchiques

Une conception hiérarchique présente plusieurs avantages en matière de gestion :

- **Simplicité de connexion.** Le fait d'opter pour une solution hiérarchique réduit la complexité globale d'un réseau, car, dans ce cas, il est scindé en unités plus petites. Cette subdivision facilite le dépannage, tout en offrant une protection contre la propagation de tempêtes de broadcast, boucles de routage et autres problèmes potentiels.
- **Souplesse de conception.** Les réseaux hiérarchiques offrent une plus grande souplesse d'utilisation des services de paquets WAN. La plupart d'entre eux gagnent à exploiter une approche hybride dans leur structure d'ensemble. Dans la majorité des cas, des liaisons louées peuvent être implémentées au niveau de l'épine dorsale avec des services de commutation de paquets exécutés au niveau des réseaux d'accès et de distribution.
- **Gestion de routeurs.** En choisissant une approche hiérarchique pour l'implémentation des routeurs, vous réduisez de beaucoup la complexité liée à leur configuration, chaque routeur ne possédant qu'un petit nombre de voisins ou homologues avec lesquels communiquer.

Optimisation du trafic de contrôle broadcast et multicast

Les effets des diffusions broadcast (diffusions générales) sur les réseaux de services de paquets (voir la section "Problèmes liés à la diffusion broadcast", plus loin dans ce chapitre) requièrent l'implémentation de groupes de routeurs plus petits. Des exemples types de trafic broadcast sont les mises à jour de routage et les mises à jour SAP (*Service Advertisement Protocol*) de Novell, qui sont échangées entre routeurs sur des réseaux PSDN. Un nombre excessif de routeurs dans n'importe quelle zone ou couche d'un réseau peut générer des goulets d'étranglement, en raison de la duplication des diffusions broadcast. Une organisation hiérarchique permet de limiter l'étendue de ces diffusions entre régions et au sein de l'épine dorsale.

Choix d'une topologie

Après avoir défini votre structure de réseau, vous devez définir une approche de gestion de l'interconnexion de sites au sein d'une même zone ou région administrative. Lors de la conception d'un

réseau étendu (WAN) à échelle régionale, que ce réseau repose sur des services de commutation de paquets ou sur des connexions point-à-point, vous disposez de trois approches de base :

- topologie en étoile ;
- topologie totalement maillée ;
- topologie partiellement maillée.

Les sections suivantes traitent des possibilités d'application de ces topologies pour des services de commutation de paquets spécifiques.

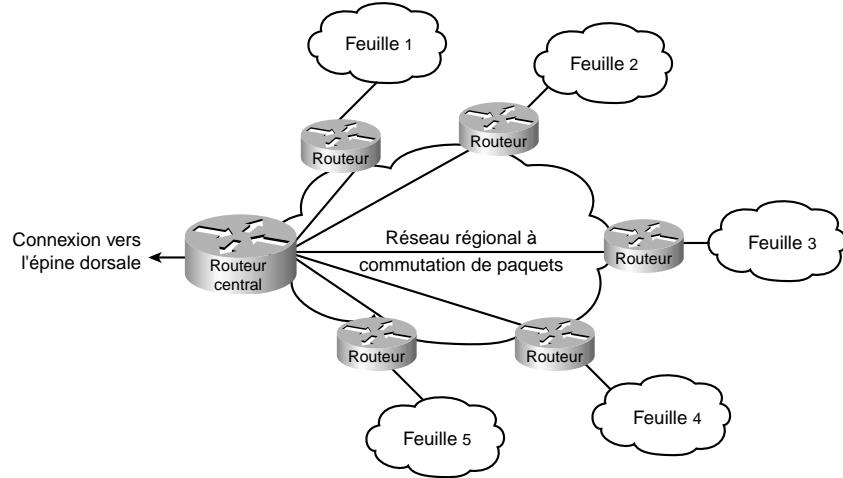
Les illustrations de ce chapitre utilisent des lignes, afin de représenter l'interconnexion de routeurs spécifiques sur le réseau PSDN. Il s'agit de connexions virtuelles, mises en œuvre par une association de fonctionnalités sur les routeurs. Les connexions physiques réelles sont généralement implémentées au niveau de commutateurs sur le réseau PSDN.

Topologie en étoile

Une topologie en étoile inclut un seul hub d'interconnexion, ou routeur central, qui fournit un accès à l'épine dorsale pour les réseaux feuilles, ainsi qu'un accès à ces derniers uniquement par son intermédiaire. La Figure 6.2 illustre la topologie en étoile d'un réseau régional à commutation de paquets.

Figure 6.2

Topologie en étoile
d'un réseau régional.

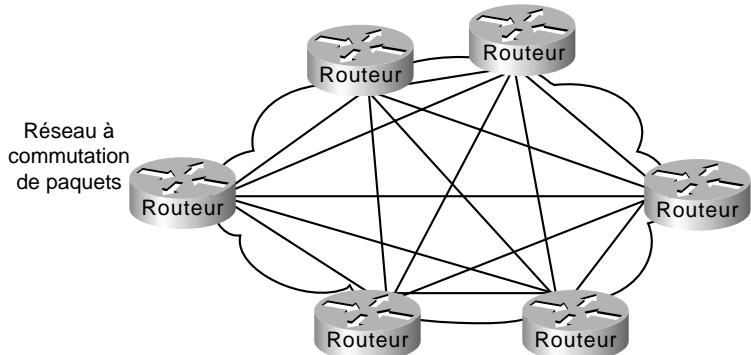


Une topologie en étoile offre les avantages d'une gestion simplifiée et d'une réduction maximale des coûts. Néanmoins, elle présente aussi des inconvénients non négligeables. Tout d'abord, le routeur central constitue une source de panne potentielle. Ensuite, ce routeur limite les performances globales d'accès aux ressources de l'épine dorsale, car le trafic qui circule dans cette direction (ou vers les autres routeurs régionaux) doit passer par ce seul canal. Enfin, cette topologie n'est pas évolutive.

Topologie totalement maillée

Une topologie totalement maillée implique un chemin direct entre chaque noeud de routage situé en périphérie d'un réseau à commutation de paquets et tous les autres noeuds situés au sein du nuage. La Figure 6.3 illustre ce type d'organisation.

Figure 6.3
Topologie totalement maillée.



L'objectif d'un environnement totalement maillé est de fournir un haut niveau de redondance. Bien qu'une telle topologie facilite le support de tous les protocoles de réseau, elle n'est pas rentable pour de grands réseaux à commutation de paquets. Les principaux problèmes qui se posent concernent le nombre important de circuits virtuels nécessaires (un pour chaque connexion entre routeurs), la duplication intensive de paquets et de diffusions broadcast, ainsi que la complexité de configuration des routeurs, en l'absence de support du mode multicast dans des environnements non broadcast.

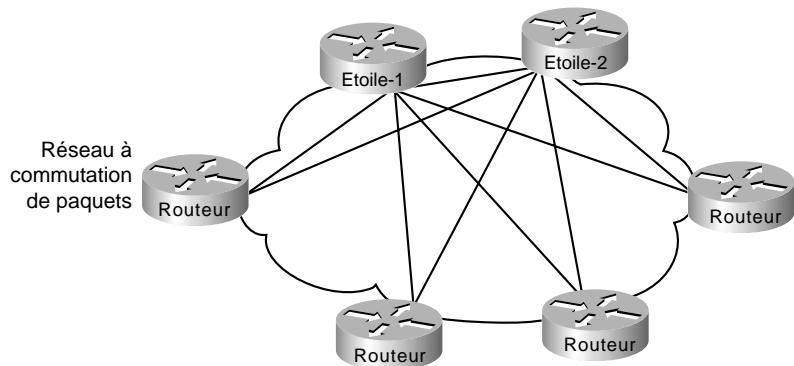
En combinant une topologie totalement maillée et une topologie en étoile, de façon à former un environnement partiellement maillé, on améliore le degré de tolérance aux pannes, sans rencontrer pour autant les problèmes de performances et de gestion associés à une approche totalement maillée.

Topologie partiellement maillée

Une topologie partiellement maillée limite, dans une région, le nombre de routeurs qui possèdent une connexion directe vers tous les autres nœuds ; les nœuds ne sont pas tous connectés entre eux. Pour qu'un nœud non maillé puisse communiquer avec un autre nœud non maillé, il doit envoyer le trafic *via* l'un des routeurs qui fait office de point de collecte (voir Figure 6.4).

Il existe de nombreuses variantes de cette topologie. Elle offre généralement le meilleur équilibre en termes de nombre de circuits virtuels, redondance et performances, pour les topologies régionales.

Figure 6.4
Topologie partiellement maillée.



Problèmes liés à la diffusion broadcast

Le trafic broadcast peut poser des problèmes lorsqu'il est introduit sur des réseaux de services de paquets. Une station doit exploiter la diffusion broadcast lorsqu'elle souhaite envoyer un paquet à plusieurs stations dont elle ignore l'adresse. Le Tableau 6.1 liste les protocoles de réseau courants et leur niveau général de trafic broadcast, dans le cas d'un grand réseau qui comprend de nombreux nœuds de routage.

Tableau 6.1 : Niveaux de trafic broadcast sur des réseaux étendus

Protocole de réseau	Protocole de routage	Niveau de trafic broadcast
AppleTalk	RTMP (<i>Routing Table Maintenance Protocol</i>) Enhanced IGRP (<i>Enhanced Interior Gateway Routing Protocol</i>)	Elevé Faible
Novell IPX (<i>Internetwork Packet Exchange</i>)	RIP (<i>Routing Information Protocol</i>) SAP (<i>Service Advertisement Protocol</i>) Enhanced IGRP	Elevé Elevé Faible
IP (<i>Internet Protocol</i>)	RIP IGRP (<i>Interior Gateway Routing Protocol</i>) OSPF (<i>Open Shortest Path First</i>) IS-IS (<i>Intermediate System-to-Intermediate System</i>) Enhanced IGRP BGP (<i>Border Gateway Protocol</i>) EGP (<i>Exterior Gateway Protocol</i>)	Elevé Elevé Faible Faible Faible Aucun Aucun
DECnet Phase IV	DECnet Routing	Elevé
DECnet Phase V	IS-IS	Faible

Tableau 6.1 : Niveaux de trafic broadcast sur des réseaux étendus (suite)

<i>Protocole de réseau</i>	<i>Protocole de routage</i>	<i>Niveau de trafic broadcast</i>
ISO (<i>International Organization for Standardization</i>) CLNS (<i>Connectionless Network Service</i>)	IS-IS ISO-IGRP	Faible Elevé
XNS (<i>Xerox Network Systems</i>)	RIP	Elevé
Banyan VINES (<i>Virtual Integrated Network Service</i>)	RTP (<i>Routing Table Protocol</i>) Sequenced RTP	Elevé Faible

Les valeurs relatives *Elevé* et *Faible* du Tableau 6.1 donnent une idée générale des niveaux de broadcast pour les protocoles répertoriés. La densité du trafic broadcast sera déterminée par vos situation et implémentation spécifiques. Par exemple, le niveau de trafic broadcast généré dans un environnement AppleTalk/Enhanced IGRP dépend de la valeur de l'intervalle du temporisateur Hello IGRP. La taille du réseau peut également poser problème. Sur un réseau de petite échelle, le niveau de trafic broadcast généré par les nœuds Enhanced IGRP peut être plus élevé que celui d'un réseau basé RTMP. Cependant, sur de grands réseaux, les nœuds Enhanced IGRP génèrent beaucoup moins de trafic broadcast que les nœuds RTMP.

La gestion de la duplication de paquets est un facteur de conception important, qui doit être pris en compte lors de l'intégration de réseaux locaux de type broadcast (tel Ethernet) avec des services de paquets non broadcast (tel X.25). Les connexions à des environnements de commutation de paquets se caractérisent par un nombre important de circuits virtuels. Par conséquent, les routeurs doivent reproduire les diffusions broadcast pour chaque circuit sur une liaison physique donnée.

Dans des environnements fortement maillés, la duplication des diffusions broadcast peut se révéler coûteuse en termes de bande passante et de cycles processeur. En dépit des avantages qu'offrent les topologies maillées, celles-ci ne conviennent généralement pas pour de grands réseaux à commutation de paquets. Toutefois, un certain niveau de maillage de circuits est essentiel, afin de garantir une tolérance aux pannes. La solution consiste donc à trouver un compromis entre les performances et les exigences en matière de redondance de circuits.

Gestion des performances

Lors de la conception d'un réseau étendu basé sur un type de service de paquets spécifique, vous devez prendre en considération les caractéristiques des circuits virtuels. Par exemple, dans certaines situations, les performances dépendront de la capacité d'un circuit virtuel donné à s'adapter à un trafic multiprotocole. Selon la manière dont ce trafic est placé en file d'attente et circule d'un nœud à l'autre, certains protocoles peuvent nécessiter une gestion particulière. On pourrait envisager d'assigner certains circuits virtuels à certains types de protocoles. Les performances des services de commutation de paquets dépendent du débit contractuel, ou CIR (*Committed Information Rate*) — le CIR correspond au débit moyen maximal autorisé par connexion, c'est-à-dire par PVC, pour

une période donnée —, sur les réseaux Frame Relay, et des limitations de taille de fenêtre sur les réseaux X.25.

Conception de réseaux Frame Relay

L'évolutivité est une préoccupation majeure lors de la conception d'un réseau Frame Relay. Au fur et à mesure que les exigences en matière d'interconnexions distantes augmentent, votre réseau doit être capable d'évoluer, afin de s'adapter aux changements. Il doit également offrir un niveau de performances acceptable, tout en réduisant le plus possible les besoins de maintenance et de gestion. Satisfaire tous ces objectifs simultanément peut se révéler une tâche ardue. Les sections suivantes examinent plusieurs facteurs importants, relatifs aux réseaux Frame Relay :

- conception hiérarchique ;
- topologies régionales ;
- problèmes de diffusion broadcast ;
- gestion des performances.

Les recommandations et suggestions suivantes ont pour objectif de jeter les bases de la conception de réseaux Frame Relay évolutifs, qui présentent un rapport équilibré entre les performances, la tolérance aux pannes et le coût.

Conception hiérarchique

En règle générale, les arguments en faveur d'une conception hiérarchique pour les réseaux à commutation de paquets, présentés plus haut dans ce chapitre, s'appliquent également à la conception hiérarchique de réseaux Frame Relay. Ils sont au nombre de trois :

- évolutivité ;
- facilité de gestion ;
- optimisation du trafic de contrôle broadcast et multicast.

De nombreux fournisseurs Frame Relay facturent leurs services en se fondant sur l'identifiant de connexion de liaison de données (DLCI, *Data Link Connection Identifier*), qui caractérise une connexion virtuelle permanente Frame Relay. Une telle connexion est équivalente à un circuit virtuel permanent X.25 qui, dans la terminologie X.25, est identifié par un numéro de canal logique (LCN, *Logical Channel Number*). L'identifiant DLCI définit l'interconnexion d'équipements Frame Relay. Quelle que soit l'implémentation d'un réseau, le nombre de connexions virtuelles permanentes Frame Relay dépend étroitement des protocoles utilisés, ainsi que des modèles de trafics existants.

Le nombre de DLCI configurables par port série dépend du niveau de trafic. Vous pouvez les utiliser tous (environ 1 000), mais 200 à 300 suffisent généralement pour une utilisation courante. Si vous envoyez des diffusions broadcast sur les DLCI, 30 à 50 DLCI sont des quantités plus现实的, eu égard à la surcharge de services générée au niveau du processeur. Il est difficile de fournir des recommandations spécifiques, car cette surcharge varie en fonction de la configuration. Néanmoins, sur des équipements bas de gamme, l'architecture est limitée par la quantité de mémoire d'entrée-sortie disponible. Le nombre de DLCI dépend de plusieurs facteurs, qui devraient être pris en compte conjointement :

- **Protocoles routés.** N'importe quel protocole qui utilise les diffusions broadcast de façon intensive limite le nombre de DLCI pouvant être assignés. Par exemple, AppleTalk est un protocole qui se caractérise par l'utilisation de huit niveaux de surcharge en diffusion broadcast. Un autre exemple est le protocole Novell IPX, qui envoie à la fois des mises à jour de routage et des mises à jour de service, ce qui entraîne une surcharge de trafic broadcast supérieure au niveau de la bande passante. A l'inverse, IGRP utilise moins la diffusion broadcast, car il envoie moins fréquemment des mises à jour de routage (toutes les 90 secondes, par défaut). Cependant, si ses temporisateurs sont modifiés, afin que les mises à jour soient envoyées à une fréquence plus élevée, il se mettra lui aussi à exploiter intensivement ce mode de diffusion.
- **Trafic broadcast.** Les diffusions broadcast, telles les mises à jour de routage, représentent le facteur le plus important à prendre en compte lors de la détermination du nombre de DLCI pouvant être définis. La quantité et le type de trafic broadcast requis vous guideront dans l'assignation des DLCI, tout en demeurant dans la plage générale recommandée. Revoyez le Tableau 6.1, plus haut dans ce chapitre, pour obtenir une liste des niveaux relatifs de trafic broadcast pour des protocoles courants.
- **Vitesse des lignes.** Si le niveau de trafic broadcast doit être élevé, vous devriez envisager l'utilisation de lignes plus rapides, ainsi que de DLCI dotées de valeurs supérieures pour les limites de CIR, et de salves en excès (B_e , *excess burst*). Vous devriez également implémenter un nombre moindre de DLCI.
- **Routes statiques.** Si le routage statique est implémenté, vous pouvez utiliser un plus grand nombre de DLCI par ligne, ce qui permet de réduire le niveau de diffusion broadcast.
- **Taille des mises à jour de protocoles de routage et des mises à jour SAP.** Plus le réseau est grand, plus la taille de ces mises à jour augmente. Plus les mises à jour sont importantes, plus le nombre de DLCI pouvant être assignés est limité.

Deux formes de conception hiérarchique Frame Relay peuvent être implémentées :

- réseaux Frame Relay maillés hiérarchiques ;
- réseaux Frame Relay maillés hybrides.

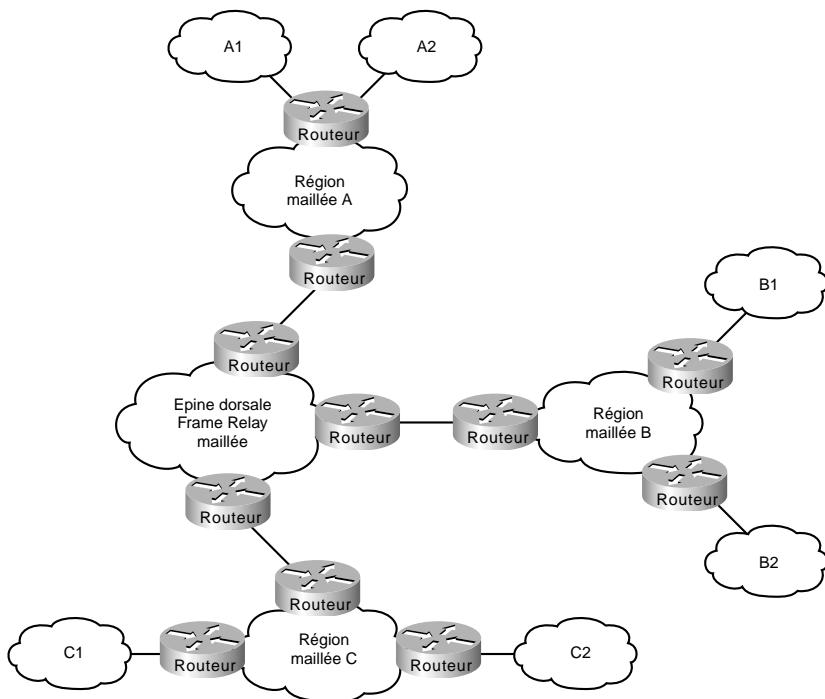
Ces deux approches présentent à la fois des avantages et des inconvénients, mis en évidence dans les sections suivantes.

Réseaux Frame Relay maillés hiérarchiques

L'objectif de l'implémentation d'un maillage hiérarchique pour des réseaux Frame Relay est d'éviter la définition d'un nombre excessif de DLCI, et de fournir un environnement segmenté facile à gérer. Un tel environnement présente un maillage total au niveau du réseau PSDN central et de tous les réseaux périphériques. La hiérarchie est créée en plaçant les routeurs de façon stratégique entre les éléments du réseau.

La Figure 6.5 illustre un maillage hiérarchique simple. Le réseau donné en exemple comprend une épine dorsale totalement maillée, ainsi que des réseaux régionaux et des réseaux broadcast maillés, situés en périphérie extérieure.

Figure 6.5
Environnement Frame Relay hiérarchique totalement maillé.



Les deux principaux avantages d'un maillage hiérarchique sont qu'il est relativement évolutif et qu'il permet d'isoler le trafic. En plaçant des routeurs entre des portions totalement maillées du réseau, vous limitez le nombre de DLCI par interface physique, segmentez votre réseau, et en facilitez la gestion. Toutefois, deux problèmes peuvent se présenter :

- **Duplication de diffusions broadcast et de paquets.** Dans un environnement où les interfaces de routeur sont nombreuses à supporter plusieurs DLCI, une reproduction excessive des diffusions broadcast et des paquets peut dégrader les performances globales. Il s'agit d'un problème majeur sur les réseaux hiérarchiques fortement maillés. Etant donné que les exigences en matière de débit sont généralement élevées sur l'épine dorsale, il est très important d'éviter de perdre de la bande passante.
- **Augmentation des coûts associés à des interfaces de routeur supplémentaires.** Comparé à une topologie totalement maillée, des routeurs supplémentaires sont nécessaires pour séparer l'épine dorsale maillée des réseaux maillés en périphérie. Néanmoins, l'utilisation de ces routeurs permet de créer des réseaux bien plus grands, qui peuvent évoluer presque indéfiniment, ce qui n'est pas le cas d'un réseau totalement maillé.

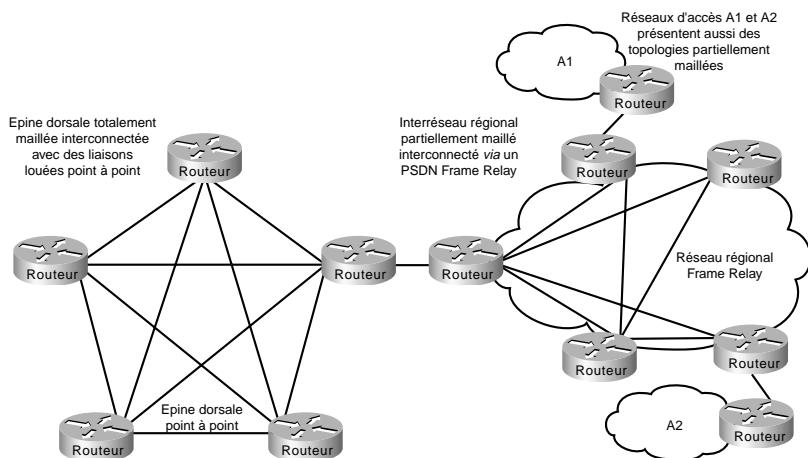
Réseaux Frame Relay maillés hybrides

L'importance économique et stratégique des environnements d'épine dorsale oblige souvent les concepteurs à implémenter une structure maillée hybride pour les réseaux WAN. Un réseau maillé

hybride comprend des liaisons louées maillées et redondantes au niveau de l'épine dorsale WAN, ainsi que des réseaux PSDN Frame Relay partiellement (ou totalement) maillés en périphérie. Des routeurs séparent l'épine dorsale des réseaux PSDN (voir Figure 6.6).

Figure 6.6

Réseau Frame Relay hiérarchique hybride.



Les maillages hybrides hiérarchiques ont pour avantages de fournir un niveau de performances supérieur sur l'épine dorsale, d'isoler le trafic et de simplifier l'évolution des réseaux. De plus, ce type de réseau, associé au Frame Relay, représente une solution intéressante, car il autorise un meilleur contrôle du trafic sur l'épine dorsale, et permet à celle-ci d'être constituée de liaisons dédiées, d'où une plus grande fiabilité.

Les inconvénients de ces maillages sont, entre autres, des coûts élevés associés aux liaisons louées, ainsi qu'une duplication de diffusions broadcast et de paquets, qui peut être intensive sur les réseaux d'accès.

Topologies régionales

Vous pouvez adopter l'une des trois approches de conception suivantes, pour un réseau régional de services de paquets fondé sur le Frame Relay :

- topologie en étoile ;
- topologie totalement maillée ;
- topologie partiellement maillée.

Ces trois approches sont présentées dans les prochaines sections. En règle générale, l'accent est placé sur les topologies partiellement maillées intégrées à un environnement hiérarchique. Les topologies en étoile et totalement maillées sont examinées pour leur contexte structurel.

Topologie en étoile

La structure générale d'une topologie en étoile a été décrite plus haut dans ce chapitre. Elle est intéressante, car elle réduit au maximum le nombre de DLCI nécessaires, et représente une solution peu coûteuse. Toutefois, elle est limitée en matière de bande passante. Considérons un environnement dans lequel un routeur d'épine dorsale est relié à un nuage Frame Relay à une vitesse de 256 Kbit/s, alors que les sites distants sont reliés à 56 Kbit/s. Une telle topologie ralentirait le trafic qui circule depuis l'épine dorsale jusqu'aux sites distants.

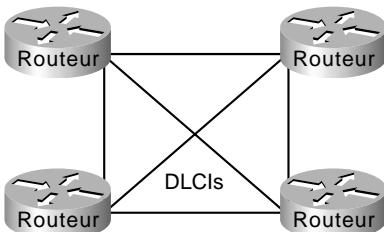
Nous l'avons vu, une topologie en étoile stricte n'offre pas le niveau de tolérance aux pannes requis dans de nombreuses situations. Si la liaison entre un routeur hub et un routeur feuille spécifique est perdue, c'est toute la connectivité vers ce dernier qui est perdue.

Topologie totalement maillée

Une topologie totalement maillée implique que chaque noeud de routage connecté à un réseau Frame Relay soit logiquement relié, *via* un DLCI assigné, à tous les autres noeuds du nuage. Cette topologie ne convient pas pour les réseaux Frame Relay plus grands, et ce pour plusieurs raisons :

- Les grands réseaux Frame Relay totalement maillés requièrent de nombreux DLCI, un pour chaque liaison logique entre les noeuds. Comme illustré à la Figure 6.7, une topologie entièrement connectée nécessite l'assignation de $[n(n - 1)]/2$ DLCI, où n est le nombre de routeurs qui doivent être directement connectés.

Figure 6.7
Réseau Frame Relay totalement maillé.



- La duplication de diffusions broadcast provoque des congestions sur les grands réseaux Frame Relay maillés. Les routeurs considèrent le Frame Relay comme étant un média de type broadcast. Chaque fois qu'un routeur envoie une trame multicast (une mise à jour de routage, une mise à jour d'arbre recouvrant ou une mise à jour SAP), il doit la copier sur chaque DLCI pour cette interface Frame Relay.

Ces problèmes combinés rendent les topologies totalement maillées inadaptées pour la quasi totalité des implémentations de Frame Relay, à l'exception de celles de petite taille.

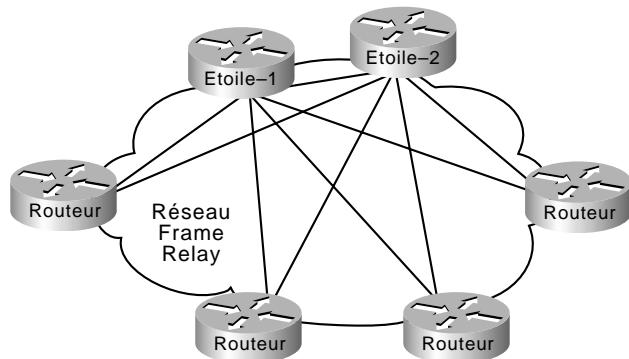
Topologie partiellement maillée

La combinaison d'une topologie en étoile et d'une topologie totalement maillée représente une topologie partiellement maillée. Cette solution est habituellement recommandée pour des environnements Frame Relay régionaux, car elle offre un niveau supérieur de tolérance aux pannes (par le

biais d'étoiles redondantes) et se révèle moins coûteuse qu'un environnement totalement maillé. En règle générale, vous devriez implémenter un maillage minimal, afin d'éliminer les risques de sources de pannes.

La Figure 6.8 illustre une topologie partiellement maillée, à deux étoiles. Cette organisation est supportée sur les réseaux Frame Relay qui exécutent IP, ISO CLNS, DECnet, Novell IPX, AppleTalk, ainsi que le pontage.

Figure 6.8
Réseau Frame Relay partiellement maillé, à deux étoiles.



Une fonctionnalité connue sous l'appellation *interfaces virtuelles* (introduite avec la version 9.21 de System Software) permet de créer des réseaux, à l'aide des topologies Frame Relay partiellement maillées (voir Figure 6.8).

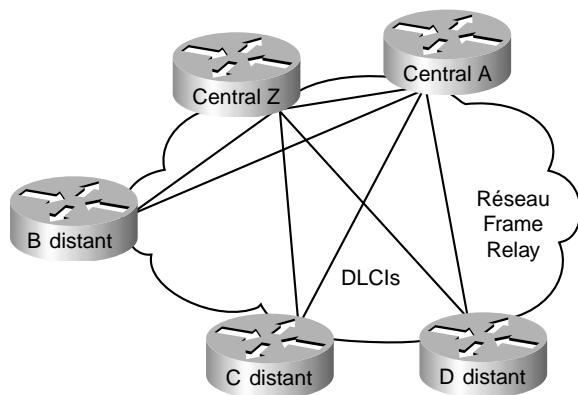
Pour créer ce type de réseau, des interfaces physiques individuelles sont divisées en plusieurs interfaces virtuelles (logiques). En ce qui concerne le Frame Relay, cela signifie que les DLCI peuvent être regroupés ou séparés, pour une exploitation optimale. Par exemple, des petits nuages totalement maillés de routeurs connectés Frame Relay peuvent transiter au-dessus d'un groupe de quatre DLCI concentrés sur une seule interface virtuelle, alors qu'un cinquième DLCI sur une autre interface virtuelle assure la connectivité vers un réseau complètement séparé. Toute cette connectivité a lieu au-dessus d'une seule interface physique connectée au service Frame Relay.

Dans la version 9.21 de System Software, les interfaces virtuelles n'étaient pas disponibles, et les topologies partiellement maillées pouvaient poser des problèmes selon les protocoles de réseau utilisés. Examinez la topologie illustrée à la Figure 6.9.

Eu égard à une configuration de routeur standard et à un logiciel de routeur antérieur à la version 9.21 de System Software, la connectivité disponible pour le réseau illustré à la Figure 6.9 peut être caractérisée comme suit :

- Les routeurs centraux A et Z peuvent joindre tous les routeurs distants.
- Les routeurs distants B, C et D ne peuvent pas communiquer entre eux.

Figure 6.9
Réseau Frame Relay
partiellement maillé.



En ce qui concerne les implémentations Frame Relay qui exécutent une version de System Software antérieure à la version 9.21, le seul moyen de mettre en œuvre une connectivité entre tous ces routeurs est d'utiliser un protocole par vecteur de distance, qui puisse désactiver la fonctionnalité d'horizon éclaté (*split horizon*), tels RIP ou IGRP pour IP. Tout autre protocole de réseau (AppleTalk ou ISO CLNS) ne sera pas opérationnel. Le code suivant illustre une configuration IGRP prévue pour supporter une organisation partiellement maillée :

```
router igrp 20
network 45.0.0.0
!
interface serial 3
encapsulation frame-relay
ip address 45.1.2.3 255.255.255.0
no ip split-horizon
```

Cette topologie fonctionne uniquement avec des protocoles de routage par vecteur de distance — en supposant que souhaitiez établir une connectivité entre les routeurs distants B, C et D et les routeurs centraux A et Z uniquement —, sans nécessiter de liaison directe entre les routeurs distants. Cette topologie ne fonctionne pas avec des protocoles de routage par informations d'état de lien, car le routeur n'est pas en mesure de vérifier la contiguïté de ses routeurs voisins. Notez que les routes et les services des nœuds feuilles qui ne peuvent pas être joints sont visibles.

Problèmes liés à la diffusion broadcast

Nous l'avons vu, les routeurs considèrent le Frame Relay comme étant un média de type broadcast. Par conséquent, chaque fois qu'un routeur envoie une trame multicast (une mise à jour de routage, une mise à jour d'arbre recouvrant ou une mise à jour SAP), il doit la copier sur chaque DLCI pour l'interface Frame Relay. La reproduction de trame entraîne une surcharge importante aux niveaux du routeur et de l'interface physique.

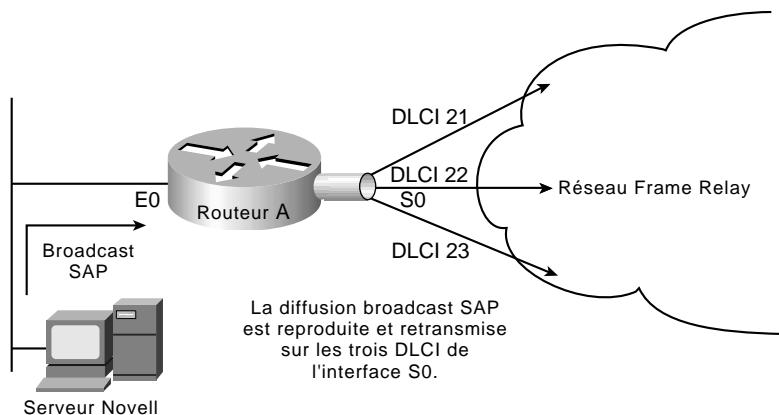
Prenons, par exemple, un environnement Novell IPX qui comprend plusieurs DLCI configurés sur une seule interface physique. Chaque fois qu'une mise à jour SAP est détectée — ce qui se produit toutes les 60 secondes —, le routeur doit la reproduire, puis l'envoyer sur l'interface virtuelle associée à

chaque DLCI. Chaque trame SAP contient jusqu'à sept entrées de service, et chaque mise à jour comprend 64 octets. La Figure 6.10 illustre cet exemple.

NOTE

L'une des méthodes de réduction des diffusions broadcast consiste à implémenter des protocoles de routage plus efficaces, tel Enhanced IGRP, et d'ajuster les intervalles des temporiseurs sur les services Frame Relay à faible vitesse.

Figure 6.10
Duplication SAP dans
un environnement
Frame Relay avec
interfaces virtuelles.



Création d'une file broadcast pour une interface

Les très grands réseaux Frame Relay peuvent rencontrer des problèmes de performances lorsque de nombreux DLCI se terminent sur un seul routeur, ou serveur d'accès, qui doit reproduire les mises à jour de routage ainsi que les mises à jour d'annonces de service sur chaque DLCI. Les mises à jour peuvent consommer la bande passante de la liaison d'accès et provoquer des variations importantes dans les délais de transport du trafic utilisateur. Elles peuvent également exploiter largement les tampons d'interface, ce qui entraîne une augmentation des pertes de paquets pour les données utilisateur aussi bien que pour les mises à jour de routage.

Afin d'éviter cela, vous pouvez créer une file broadcast spécifique pour une interface, file qui sera gérée indépendamment de la file d'interface normale. Cette file disposera de ses propres tampons ; sa taille et son débit de service pourront être configurés.

Une file broadcast se voit assigner une limite maximale de débit de transmission, exprimée à la fois en octets par seconde et en paquets par seconde. Elle est servie, de façon à garantir que cette limite ne sera pas dépassée. Elle est prioritaire lorsqu'elle transmet des données à un débit inférieur au maximum configuré, et dispose donc d'une allocation minimale de bande passante garantie. Les deux limites de débit de transmission sont prévues afin d'éviter d'inonder une interface avec des diffusions broadcast. La véritable limite est la première (celle exprimée en octets ou celle exprimée en paquets) atteinte à n'importe quel moment.

Gestion des performances

Deux facteurs importants relatifs aux performances doivent être pris en compte lors de l'implémentation d'un réseau Frame Relay :

- les métriques de coût des fournisseurs de services de commutation de paquets ;
- les exigences de gestion associées au trafic multiprotocole.

Chacun de ces facteurs doit être examiné au cours du processus de planification du réseau. Les sections suivantes traitent brièvement de l'effet qu'ils peuvent produire sur les performances Frame Relay globales.

Métriques de coût des fournisseurs de services de commutation de paquets

Lorsque vous passez un contrat avec un fournisseur de services de commutation de paquets Frame Relay, afin de bénéficier de certaines fonctionnalités, le CIR (débit contracté), mesuré en bits par seconde, est l'une des métriques de coût négociées essentielles. Le CIR représente le niveau de trafic maximal autorisé par l'opérateur sur un DLCI spécifique dans l'environnement de commutation de paquets. Ce débit garanti peut être équivalent ou inférieur à la capacité physique maximale de la ligne de connexion.

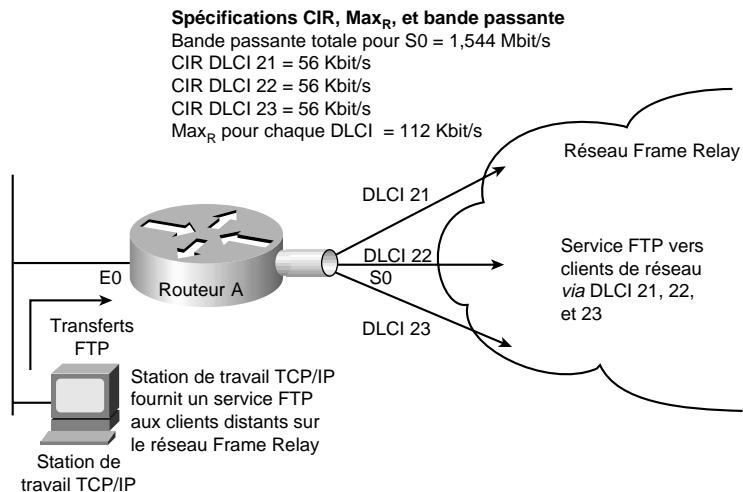
D'autres métriques essentielles sont représentées par les salves garanties (B_c , *committed burst*) et les salves en excès (B_e , *excess burst*). Les salves garanties représentent le nombre de bits que le réseau est censé accepter et transmettre au débit CIR. Les salves en excès définissent la limite absolue, en bits, d'un DLCI. Il s'agit du nombre de bits que le réseau Frame Relay tentera de transmettre une fois la métrique B_c définie. B_e détermine une pointe, ou débit maximal, Frame Relay (Max_R), où $\text{Max}_R = (B_c + B_e)/B_c \times \text{CIR}$, exprimé en bits par seconde.

Examinez l'exemple de la Figure 6.11. Dans cet environnement, les DLCI 21, 22 et 23 se voient assigner des CIR de 56 Kbit/s. Supposez que le Max_R pour chaque ligne soit de 112 Kbit/s (le double du CIR). La ligne série à laquelle le routeur A est connecté est une ligne T1, capable de fournir un débit total de 1 544 Mbit/s. Etant donné que le trafic envoyé sur le réseau Frame Relay est généré par des transferts de fichiers FTP, il est fort probable que le routeur tentera de transmettre à un débit supérieur au Max_R . Si cela se produit, le trafic risque d'être supprimé sans notification, en cas de débordement des tampons B_e (alloués au commutateur Frame Relay).

Malheureusement, il existe assez peu de techniques qui permettent d'éviter systématiquement que le trafic sur une ligne ne dépasse le Max_R . Bien que le Frame Relay emploie les protocoles FECN (*Forward Explicit Congestion Notification*, notification de congestion explicite en aval) et BECN (*Backward Explicit Congestion Notification*, notification de congestion explicite en amont) pour contrôler le trafic sur un réseau Frame Relay, il n'existe aucun standard de mise en correspondance entre le niveau Frame Relay (liaison) et la plupart des protocoles de couches supérieures. Aussi, lorsqu'un bit FECN est détecté par un routeur, il est associé à l'octet de notification de congestion pour le protocole DECnet Phase IV ou ISO CLNS. Aucun autre protocole n'est supporté.

Figure 6.11

Exemple de situation limitant le trafic CIR et CBR.



Les conséquences réelles du dépassement du CIR spécifié et des paramètres Max_R associés dépendent du type des applications qui sont exécutées sur le réseau. Par exemple, l'algorithme de temporisation (*back-off*) de TCP/IP interprétera les paquets supprimés en tant qu'indicateur de congestion ; les hôtes émetteurs pourront alors réduire l'émission de trafic. Néanmoins, étant donné que NFS ne possède aucun algorithme de ce type, les paquets supprimés résulteront en des connexions perdues. Lorsque vous déterminez les métriques CIR, B_c et B_e pour une connexion Frame Relay, vous devez prendre en compte la vitesse de liaison ainsi que les applications réelles qui doivent être supportées.

La plupart des opérateurs Frame Relay fournissent un niveau approprié de mise en mémoire tampon, afin de pouvoir gérer les situations où le trafic excède le CIR pour un DLCI donné. Ces tampons permettent aux paquets en excès d'être traités avec le débit CIR, et de limiter leur perte, dans le cas d'un protocole de transport robuste, tel que TCP. Néanmoins, il peut arriver que ces tampons débordent. Souvenez-vous que les routeurs sont capables de gérer la priorité du trafic, à l'inverse des commutateurs Frame Relay. Vous pouvez spécifier quels sont les paquets Frame Relay de plus faible priorité ou le moins sensibles aux délais de livraison ; ils seront supprimés en priorité si un commutateur Frame Relay est congestionné. Le mécanisme qui permet à un commutateur Frame Relay d'identifier ces paquets est le bit DE (*Discard Eligibility*).

Cette fonctionnalité nécessite que le réseau Frame Relay soit en mesure d'interpréter le bit DE. Certains réseaux n'exécutent aucune action lorsque ce bit est activé. D'autres l'utilisent afin de déterminer quels paquets supprimer. La meilleure approche consiste à utiliser ce bit afin de déterminer quels paquets doivent être supprimés en priorité, mais également quels sont les paquets le moins sensibles aux délais de livraison. Vous pouvez définir une liste de bits DE afin d'identifier les caractéristiques des paquets qui peuvent être supprimés, et également spécifier des groupes de bits DE, afin d'identifier le DLCI qui est affecté.

Vous pouvez établir des listes de DE en vous fondant sur le protocole ou l'interface, ainsi que sur certaines caractéristiques : la fragmentation du paquet, un port TCP ou UDP (*User Datagram Protocol*) spécifique, un numéro de liste d'accès ou une taille de paquet.

NOTE

Pour éviter de perdre des paquets, implémentez des protocoles d'application non acquittés, à l'image de la vidéo empaquetée (*packetized video*). Soyez prudent, ces protocoles accroissent le risque de dépassement de capacité des tampons.

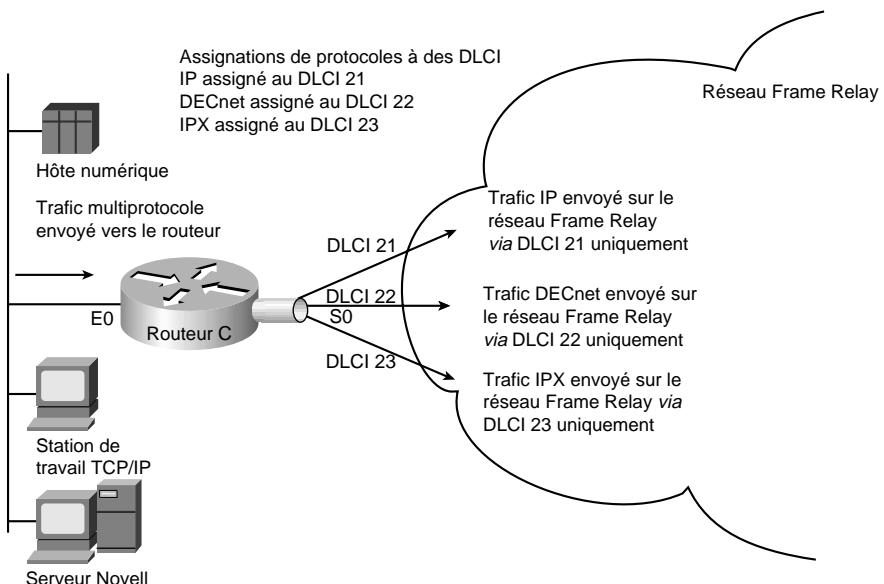
Exigences de gestion associées au trafic multiprotocole

Lorsque plusieurs protocoles sont transmis sur un réseau Frame Relay par le biais d'une seule interface physique, il peut être utile de répartir le trafic sur différents DLCI, en fonction du type de protocole. Pour diviser le trafic de cette manière, vous devez assigner des protocoles spécifiques à des DLCI spécifiques. Pour cela, vous pouvez spécifier une correspondance statique sur la base de chaque interface virtuelle ou seulement définir des types d'encapsulation pour certaines interfaces virtuelles.

La Figure 6.12 illustre l'utilisation d'interfaces virtuelles (assignées au moyen de commandes de configuration de sous-interface) afin d'attribuer le trafic à différents DLCI. Dans ce cas, le trafic de chaque protocole configuré est envoyé vers le DLCI qui lui est associé, et isolé sur un circuit. De plus, chaque protocole peut se voir assigner un CIR ainsi qu'un niveau de mise en mémoire tampon, séparés par le fournisseur de services Frame Relay.

Figure 6.12

Protocoles assignés à des interfaces virtuelles.



La Figure 6.13 présente un listing des commandes de configuration de sous-interface nécessaires pour pouvoir supporter la configuration de la figure précédente. Ce listing illustre l'activation des protocoles utiles, ainsi que leur assignation à des sous-interfaces spécifiques et aux DLCI Frame Relay qui leur sont associés. La version 9.1 de System Software, ainsi que les versions ultérieures, utilisent le protocole Frame Relay IARP (*Inverse Address Resolution Protocol*) afin de faire correspondre dynamiquement les adresses de protocoles aux DLCI Frame Relay. Pour cette raison, le listing n'illustre pas les correspondances Frame Relay.

Figure 6.13

Exemple de configuration d'interface virtuelle.

```

interface Ethernet0
ip address 192.198.78.9 255.255.255.0
ipx network AC
dnet cost 4
no mcp enabled
!
interface Serial0
no ip address
encapsulation frame-realy
!
interface Serial0.1 point-to-point
ip address 131.108.3.12.255.255.255.0
frame-relay interface-dlci 21 broadcast
no frame-relay inverse-arp IP 21
no frame-relay inverse-arp NOVELL 21
no frame-relay inverse-arp APPLETALK 21
no frame-relay inverse-arp INS 21
!
interface Serial0.2 point-to-point
no ip address
decnet cost 10
frame-relay interface-dlci 22 broadcast
no frame-relay inverse-arp IP 22
no frame-relay inverse-arp NOVELL 22
no frame-relay inverse-arp APPLETALK 22
no frame-relay inverse-arp INS 22
!
interface Serial0.3 point-to-point
no ip address
ipx network A3
frame-relay interface-dlci 23 broadcast
no frame-relay inverse-arp IP 23
no frame-relay inverse-arp NOVELL 23
no frame-relay inverse-arp APPLETALK 23
no frame-relay inverse-arp INS 23
!
router igrp 109
network 192.198.78.0
!
ip name-server 255.255.255.255
!
snmp-server community
!
line oon 0
line aux 0
line vty 0 4
end

```

Commandes de configuration de sous-interface définissant les DLCI Frame Relay et leur assignant des protocoles

Vous pouvez utiliser les commandes suivantes de System Software 9.1 afin de réaliser une configuration semblable à celle présentée à la Figure 6.13 :

```
Version 9.1
interface serial 0
ip address 131.108.3.12 255.255.255.0
decnet cost 10
novell network A3
frame-relay map IP 131.108.3.62 21 broadcast
frame-relay map DECNET 10.3 22 broadcast
frame-relay map NOVELL C09845 23 broadcast
```

Configuration de l'adaptation de trafic Frame Relay

Les fonctions d'adaptation (*traffic shaping*) du trafic Frame Relay sont supportées depuis la version 11.2 de Cisco IOS. Elles présentent les caractéristiques suivantes :

- **Imposition d'un débit par circuit virtuel.** Le débit du trafic de pointe sortant peut être configuré afin d'utiliser le débit CIR ou un autre débit configurable par l'utilisateur.
- **Ralentissement dynamique du trafic par circuit virtuel.** Lorsque les paquets BECN signalent une congestion sur le réseau, le débit du trafic sortant est automatiquement réduit. Lorsque la congestion cesse, il est rétabli. Cette fonction est activée par défaut.
- **Gestion avancée de file d'attente par circuit virtuel.** La gestion de file d'attente personnalisée, ou de file d'attente de priorité, peut être configurée au niveau de circuits virtuels individuels.

En définissant des circuits virtuels distincts pour différents types de trafics, et en spécifiant une file d'attente ainsi qu'un débit de trafic sortant pour chaque circuit virtuel, vous pouvez offrir une bande passante garantie pour chaque type de trafic. En spécifiant différents débits de trafic pour différents circuits virtuels pour une même période, vous pouvez réaliser un multiplexage temporel virtuel. En ralentissant le trafic sortant de lignes à haute vitesse au niveau des bureaux centraux en direction des lignes à faible vitesse de sites distants, vous pouvez réduire les risques de congestion et de perte de données sur le réseau. La gestion avancée de file d'attente permet également de prévenir les pertes de données dues aux congestions. Les fonctions d'adaptation de trafic s'appliquent à la fois au circuit virtuel permanent et au circuit virtuel commuté.

Conception de réseaux voix sur Frame Relay (VoFR)

A l'inverse de la majorité des applications de données, qui peuvent tolérer un certain retard, les communications qui utilisent la voix doivent avoir lieu en temps réel. Cela signifie que les délais de transmission et de réseau doivent être suffisamment faibles et constants pour demeurer imperceptibles aux utilisateurs. Par le passé, la transmission de la voix par paquets était impossible, en raison des exigences de bande passante de ce type de trafic et des délais de transmission associés aux réseaux de paquets. De plus, l'intégration de la voix sur des réseaux de données n'est réellement maîtrisée que depuis peu, car le transport de deux types de trafics différents (données et voix) sur un même réseau représente un réel défi de conception et d'implémentation. La suite de ce chapitre propose une introduction aux caractéristiques de conception et d'implémentation du trafic de type voix, et décrit son comportement sur un réseau Frame Relay.

Caractéristiques des communications humaines

La communication orale implique une certaine quantité d'informations redondantes, qui sont nécessaires au bon déroulement d'une conversation entre des personnes regroupées dans une salle ; ce n'est pas le cas sur un réseau. En règle générale, seulement 20 % d'une conversation consistent en des composants du langage essentiels à la compréhension, le reste étant formé de pauses, de bruits de fond, et de modèles répétitifs.

On peut aujourd'hui transporter la voix par paquets, avec une exploitation efficace de la bande passante, en analysant et en traitant uniquement les composants essentiels de l'échantillon de voix, au lieu de tenter une numérisation de l'échantillon tout entier (avec toutes les pauses et modèles répétitifs associés). Les technologies actuelles de traitement des signaux vocaux vont beaucoup plus loin dans le processus de numérisation de la voix que les méthodes de codage conventionnelles.

Suppression des répétitions dans des conversations orales

Les sons répétitifs font partie intégrante de la communication orale et peuvent être facilement compressés. Dans une conversation courante, la moitié seulement de ce qui est formulé atteint l'oreille de celui qui écoute. Sur un réseau de communication classique, tout le contenu de la conversation est codé et transmis. Néanmoins, une transmission exacte des sons n'est pas nécessaire, et la suppression des sons répétitifs peut permettre d'augmenter l'efficacité de la bande passante.

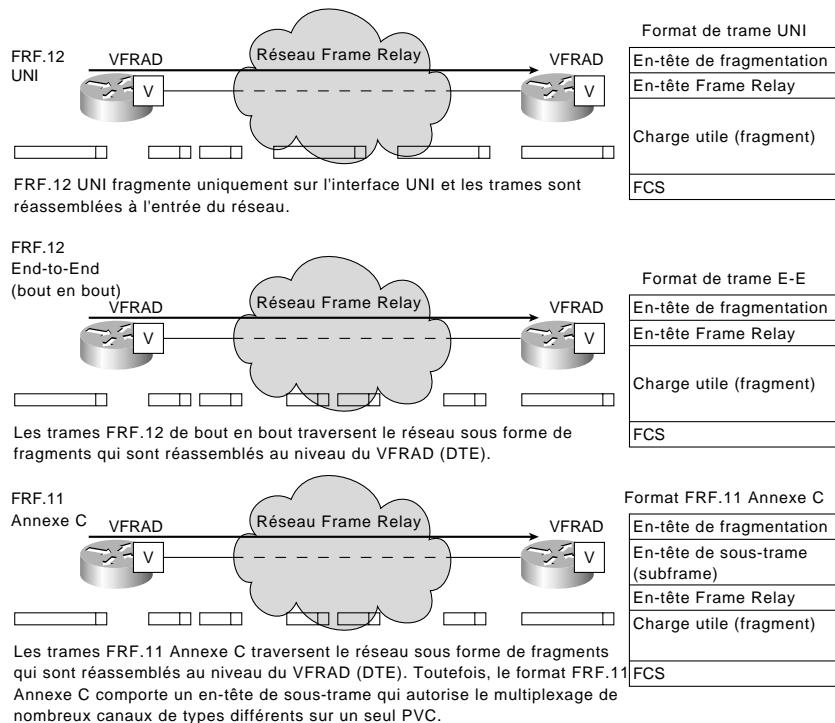
Suppression des silences dans des conversations orales

Quelqu'un qui parle n'émet pas un flot continu de paroles. Son discours est ponctué de pauses entre les mots et les phrases ; des temps morts peuvent également apparaître dans le cas où un tiers doit prendre la parole à sa suite. Ces silences peuvent être supprimés, afin d'optimiser l'efficacité de la bande passante. Les pauses peuvent être représentées sous une forme compressée, puis être régénérées sur la destination, afin de retranscrire la qualité naturelle de la communication orale.

Formation et fragmentation des trames de voix

Une fois que les modèles répétitifs ainsi que les silences ont été supprimés, les informations restantes peuvent être numérisées, puis placées dans des paquets de voix adaptés à la transmission de la voix sur les réseaux Frame Relay. Ces paquets ou trames ont tendance à être plus petits que la moyenne des trames de données. La taille de ces trames ainsi que les algorithmes de compression utilisés sont définis dans les spécifications du forum Frame Relay FRF.11 et FRF.12 (voir Figure 6.14).

La taille de trame est codée au moyen de l'algorithme de codage et de compression du standard UIT G.729, CS-CELP (*Conjugate-Structure-Algebraic Code-Excited-Linear-Predictive*). Ensuite, la trame est fragmentée afin de supprimer les composants de délai variable importants. L'utilisation de paquets plus petits permet de réduire les délais et les variations de délai de transmission sur le réseau Frame Relay ; l'algorithme de compression limite les exigences globales en bande passante.

Figure 6.14Spécifications
FRF.11 et FRF.12.

Algorithmes de compression de la voix

La compression de la voix implique la suppression des périodes de silence et des informations redondantes, ainsi que l'application d'algorithmes spécifiques aux flux de bits codés du trafic voix échantillonné. La voix numérisée non compressée, à l'image du fax, requiert une grande quantité de bande passante, généralement 64 Kbit/s. Ce débit est obtenu en multipliant la fréquence d'échantillonnage (8 000 échantillons par seconde) par le nombre de bits par échantillon (8). L'une des méthodes utilisées pour atteindre des débits plus faibles est de coder les sons sur un nombre inférieur de bits, c'est-à-dire 5, 4, 3, voire 2, par échantillon (tel que spécifié par le standard UIT G.726, ADPCM – *Adaptive Differential Pulse Code Modulation*). L'emploi d'algorithmes de compression de la voix à faibles débits offre une haute qualité d'écoute, ainsi qu'une exploitation efficace de la bande passante.

Plusieurs algorithmes sont utilisés afin d'échantillonner les modèles de la parole, et réduire ainsi la quantité d'informations envoyées, tout en assurant le meilleur niveau de qualité voix possible. Il existe trois types de codeurs de voix de base : les codeurs sous forme d'ondes (*waveform coder*), les codeurs de parole (*vocoder*), et les codeurs hybrides (*hybrid coder*). Le standard UIT G.711 PCM (*Pulse Code Modulation*) est un codeur sous forme d'ondes, qui opère à un débit de 64 Kbit/s, et qui est optimisé pour la qualité voix. Cet algorithme de codage de la voix est couramment utilisé sur les réseaux téléphoniques actuels. L'algorithme ADPCM est, lui aussi, un codeur sous forme d'ondes, qui permet de réduire de moitié le débit du codeur PCM ; il peut être utilisé à la place de ce

dernier, tout en assurant la même qualité voix. Le Tableau 6.2 présente différents algorithmes de compression, ainsi que leurs exigences en bande passante, extraites de la série de spécifications G de l'UIT.

Tableau 6.2 : Algorithmes de compression

<i>Codage/compression UIT</i>	<i>Débit</i>
G.711 PCM	64 Kbit/s (DS0) A-Law/Mu-Law
G.726 ADPCM	16, 24, 32, 40 Kbit/s
G.729 CS-ACELP	8 Kbit/s
G.728 LD-CELP	16 Kbit/s
G.723.1 CELP	6,3/5,3 Kbit/s variable

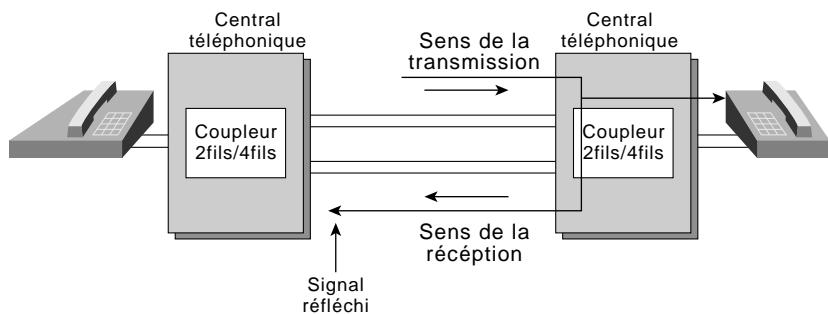
Afin de réduire au maximum les exigences en bande passante pour la parole, tout en préservant une bonne qualité voix grâce à l'utilisation de codeurs de parole et de codeurs hybrides, des algorithmes de compression avancée sont nécessaires. Pour pouvoir être exploités, ces algorithmes ont besoin de processeurs de signaux numériques (DSP, *Digital Signal Processor*). Un DSP est un microprocesseur conçu spécialement pour traiter les signaux numériques, tels ceux des applications de voix. Des avancées significatives dans la conception de ces microprocesseurs ont permis de développer des algorithmes de compression de la voix à très faibles débits. Par exemple, le codeur hybride G.729 de l'UIT réduit considérablement la quantité d'informations nécessaires à la compression et à la reproduction de la parole. Il parvient à générer un flux de 8 Kbit/s, à partir d'un flux PCM initial de 64 Kbit/s, ce qui donne un taux de compression 8:1. D'autres algorithmes, tel G.723 de l'UIT, offrent une compression qui atteint les 5,3 Kbit/s.

Au fur et à mesure que les débits disponibles passent de 64, à 32, 16, puis 8 Kbit/s, voire en deçà, les processeurs DSP et autres algorithmes de compression avancée permettent d'implémenter la compression de la voix à des débits de plus en plus faibles, sur des équipements qui supportent le Frame Relay.

Echo et annulation d'écho

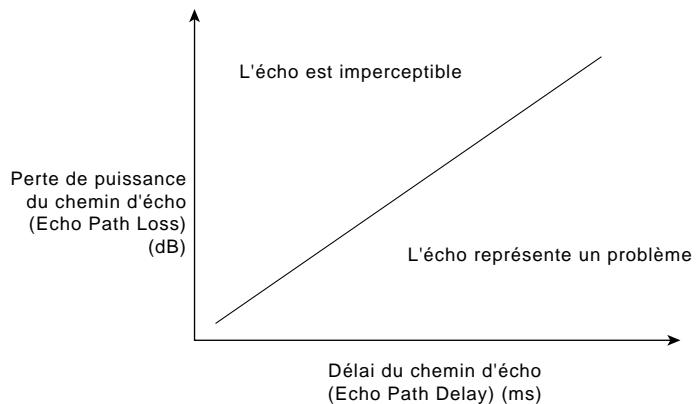
L'écho est un phénomène que l'on rencontre sur les réseaux qui transportent la voix, et qui se manifeste par la réflexion d'un signal vocal vers sa source. Cette réflexion du signal vocal se produit en général au niveau d'un équipement appelé coupleur, qui convertit une paire de fils de cuivre de boucle locale en une interface à quatre fils, pour une transmission longue distance. Lorsqu'une non-concordance de l'impédance se produit entre l'interface à deux fils et celle à quatre fils, les signaux qui ne peuvent pas être envoyés sur le chemin de transmission sont renvoyés vers la source (voir Figure 6.15).

Figure 6.15
Phénomène d'écho.



Sur des réseaux qui transportent la voix, les opérateurs utilisent des équipements qui supportent l'annulation d'écho, appelés *annulateurs d'écho* (*echo canceler*), lorsque les délais de transmission de la voix sur des conversations de bout en bout viennent amplifier l'écho. La Figure 6.16 indique que l'écho dépend des niveaux de délai et de puissance.

Figure 6.16
L'écho dépend des niveaux
de délai et de puissance.

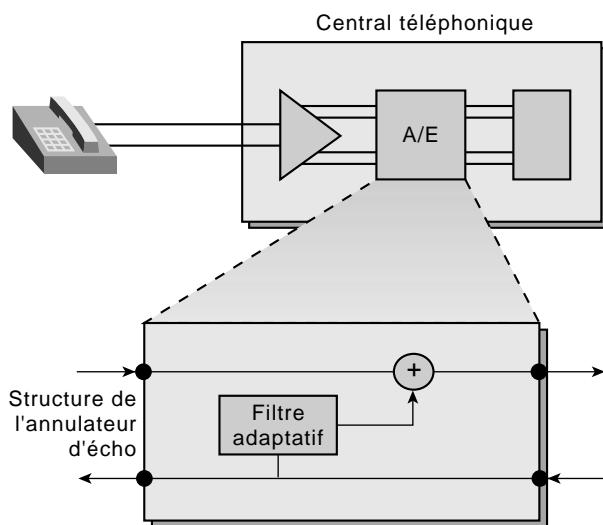


Plus la distance à parcourir est longue, plus le délai est allongé, par conséquent, plus l'écho augmente. La voix transmise sur un réseau Frame Relay doit également faire face à des délais de propagation. Au fur et à mesure que le délai de bout en bout augmente, l'écho devient perceptible pour l'utilisateur final s'il n'est pas annulé (voir Figure 6.17).

Problèmes de délai et de variation de délai

La nature morcelée du trafic Frame Relay, ainsi que la taille variable des trames transportées, peuvent engendrer des variations de délai de livraison entre les paquets d'un même flux. Cette variation est appelée *gigue* (*jitter*).

Figure 6.17
Annulation d'écho.



La gigue peut rendre difficile la régénération correcte de la voix, au niveau de l'équipement de télécommunication du client, situé à l'autre extrémité de la connexion. Etant donné que la voix est une forme d'onde continue, un intervalle trop long entre la régénération de chaque paquet de voix produit, en général, une distorsion du signal. Pour éviter que des trames soient supprimées, elles peuvent être placées dans un tampon, au niveau du décodeur de parole (*speech decoder*), afin de parer aux situations critiques de variation de délai sur le réseau.

Problèmes de perte de trames

La voix transportée sur les réseaux Frame Relay résiste habituellement mieux que les données à des pertes accidentnelles de paquets. Si un paquet de voix sur Frame Relay est perdu, l'utilisateur ne s'en rendra probablement pas compte. En revanche, des pertes de trames excessives seront inacceptables, pour la voix aussi bien que pour les données. Il arrive que des paquets soient perdus lors du débordement d'une file d'attente, ou lorsque le mécanisme CRC (*Cyclic Redundancy Check*) détecte des erreurs de bits, introduites dans une trame sur le chemin de transmission. Dans les deux cas, la transmission de la voix peut être suffisamment dégradée pour devenir inexploitable.

Support pour fax et modem

Un réseau voix sur Frame Relay doit fournir des services de modem fax et données. Les signaux de modem fax et données sur bande voix peuvent être démodulés, et transmis sous forme de données numériques au format paquet. Cette technique est généralement appelée *relais de fax (fax relay)* ; elle permet d'améliorer globalement l'efficacité de la gestion du trafic fax sur un réseau de données, sans impliquer de modulation/démodulation sur un canal de voix à 64 Kbit/s.

Il est cependant difficile de compresser de façon fiable les signaux de modem fax et données sur des canaux réservés à la voix, afin d'atteindre la faible utilisation de bande passante souvent essentielle pour une intégration efficace avec le Frame Relay. Les interfaces de commutateurs Frame Relay

classiques mettent en œuvre une technique dans laquelle la voix est compressée à un faible débit. Dès qu'un signal de fax est détecté, la bande passante est réallouée pour un débit de 64 Kbit/s, afin de pouvoir gérer une transmission de fax plus rapide. Pour cela, un canal de 64 Kbit/s (qui supporte fax groupe 3, à 14,4 Kbit/s) est généralement nécessaire. Si l'équipement supporte le relais de fax, le débit demeure à 14,4 Kbit/s tout le long du chemin de transmission.

Priorité de trafic sur le réseau Frame Relay

La voix, le fax, ainsi que certains types de données, sont sensibles aux délais de transmission. Cela signifie que, lorsque le délai ou les variations de délai de bout en bout excèdent une limite prédefinie, le niveau de service s'en trouve affecté. De nombreux mécanismes et techniques permettent de limiter les risques de dégradation des performances de service.

Pour réduire les délais de transmission de la voix, des mécanismes qui favorisent le trafic sensible aux délais peuvent être mis en œuvre. Des équipements capables d'intégrer la voix sur Frame Relay peuvent fournir une variété de mécanismes propriétaires, afin d'équilibrer les exigences de transmission de la voix et des données, parmi lesquels on trouve des fonctionnalités de file d'attente (personnalisée, de priorité et équitable pondérée). Ces mécanismes peuvent parfois différer dans leur implémentation, mais le concept sous-jacent demeure le même. Par exemple, chaque type de trafic en entrée peut être configuré afin d'être dirigé vers une ou plusieurs files d'attente de priorité. Le trafic de type voix et fax peut être placé dans la file d'attente de priorité la plus haute, alors que le trafic moins sensible aux délais est placé dans une file de priorité plus faible, en attendant que les paquets de voix et de données soient transmis.

La gestion de priorité permet de traiter le trafic sensible aux délais, tel que la voix, avant les transmissions de données de moindre priorité.

Contrôle de délai à l'aide de la fragmentation de trame

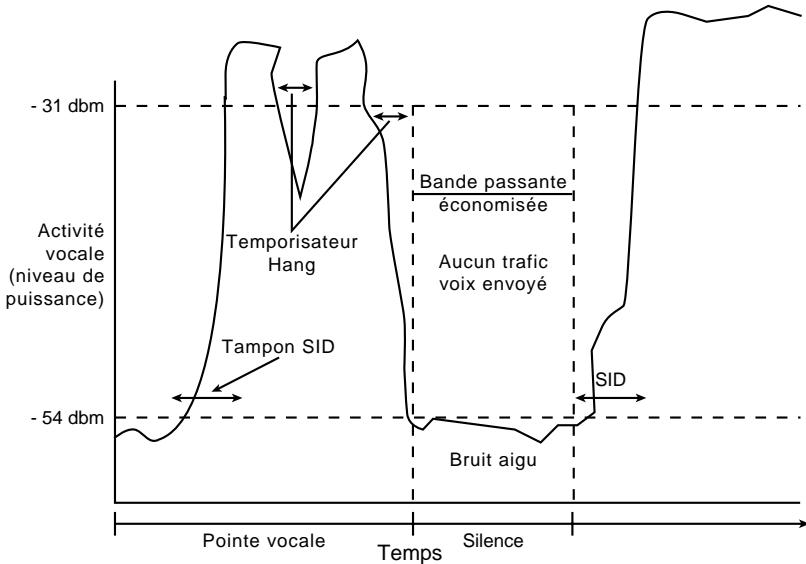
La fragmentation permet de diviser des paquets de données en trames plus petites, donc plus faciles à gérer. Elle tente de maintenir un flux continu de trames de voix sur le réseau, en limitant autant que possible les délais (voir Figure 6.14). Cette technique garantit que le trafic hautement prioritaire n'aura pas à subir d'attente avant d'être envoyé. Afin d'assurer une bonne qualité voix, la fragmentation affecte souvent toutes les données sur le réseau. En effet, même lorsque les informations de type voix sont fragmentées, une trame de voix peut être retardée par une trame de données plus grande, sur le chemin de transmission. En fragmentant également les paquets de données, il est possible d'assurer un transport des paquets de fax et de voix, sans avoir à subir de retards inacceptables. De plus, la fragmentation réduit la gigue, car les paquets de voix peuvent être échangés de façon plus régulière. Combinée aux techniques de gestion de priorité, la fragmentation offre toute l'efficacité requise. L'objectif de la fragmentation est de permettre aux réseaux voix sur Frame Relay de fournir des services qui approchent la qualité d'une ligne interurbaine, tout en autorisant la transmission de données, afin d'exploiter au mieux la bande passante.

Suppression des silences à l'aide de l'interpolation de la parole numérique (DSI)

La communication orale inclut des pauses entre les mots et entre les phrases. Les algorithmes de compression fondés sur la fonctionnalité de détection d'activité vocale (VAD, *Voice Activity Detection*) — également connue sous le nom d'interpolation de la parole numérique (DSI, *Digital Speech*

(Interpolation) — identifient et suppriment ces périodes de silence, ce qui réduit efficacement la quantité totale des informations vocales, en vue de leur transmission. DSI fait appel à des techniques de traitement de la voix avancées, afin de détecter les périodes de silence et éliminer leur transmission, ce qui limite la consommation en bande passante (voir Figure 6.18).

Figure 6.18
Suppression de silences par VAD.



Optimisation de la bande passante à l'aide du multiplexage

Certains fabricants proposent des équipements d'accès FRAD (*Frame Relay Access Device*) pour la voix sur Frame Relay, qui utilisent différentes techniques de multiplexage, afin d'optimiser l'exploitation de la bande passante. Parmi ces techniques, on trouve le multiplexage de liaison logique et le multiplexage de sous-canal. Le premier autorise des trames de voix et de données à partager le même circuit virtuel permanent (PVC), ce qui permet de réduire les coûts d'opérateur, et d'améliorer le niveau d'utilisation du circuit PVC.

Le multiplexage de sous-canal est une technique employée pour combiner les informations qui proviennent de plusieurs conversations de type voix dans une même trame. La transmission de plusieurs charges utiles dans une même trame de voix entraîne une réduction de la surcharge de paquets, et une amélioration des performances sur des liaisons lentes. Cette technique permet à des connexions lentes de transporter efficacement des petits paquets de voix sur un réseau Frame Relay.

Résumé

Ce chapitre a décrit l'implémentation de services de commutation de paquets. Nous avons traité des sujets tels que la conception de réseaux hiérarchiques, le choix d'une topologie, ainsi que les problèmes de diffusion broadcast et de performances. Nous avons également abordé les aspects liés à la conception de réseaux Frame Relay et voix sur Frame Relay.

7

Conception de réseaux APPN

Par Nicole Park

L'architecture APPN (*Advanced Peer-to-Peer Networking*) est vue comme une version de seconde génération de l'architecture SNA (*Systems Network Architecture*) d'IBM. Son objectif a été de faire passer SNA, un environnement centralisé autour d'un hôte, à un environnement d'homologues, le peer-to-peer. Elle apporte des fonctionnalités identiques à celles des protocoles de réseaux locaux, comme la définition dynamique des ressources ou la découverte d'itinéraires d'acheminement du trafic.

Ce chapitre étudie le développement d'un tracé de réseau existant et la planification de projets de migration vers APPN. Il traite des sujets suivants :

- évolution de SNA ;
- intégration d'APPN ;
- utilisation d'APPN ou d'autres méthodes de transport SNA ;
- présentation d'APPN ;
- implémentation Cisco d'APPN ;
- problèmes d'évolutivité ;
- techniques de communication de secours sur un réseau APPN ;
- intégration d'APPN dans un environnement multiprotocole ;
- gestion de réseau ;
- exemples de configuration.

Bien que ce chapitre traite aussi de l'exploitation d'APPN avec DLSw+, vous obtiendrez davantage d'informations sur l'emploi de DLSw+ en vous reportant au Chapitre 8.

Evolution de SNA

Introduit en 1974, le concept de sous-zone SNA a permis à un mainframe exécutant un dispositif ACF/VTAM (*Advanced Communications Function/Virtual Telecommunication Access Method*) d'assurer le rôle de hub du réseau. Le mainframe était responsable de l'établissement de toutes les sessions (une connexion entre deux ressources, à travers laquelle les données pouvaient être envoyées), ainsi que de l'activation et de la désactivation des ressources. L'objectif des sous-zones SNA était de permettre la livraison fiable d'informations sur des lignes analogiques à faible vitesse. Les ressources étaient clairement prédéfinies, ce qui éliminait le besoin de recourir à la diffusion broadcast et minimisait la surcharge liée à la gestion d'en-têtes.

De nombreuses entreprises maintiennent aujourd'hui deux réseaux : un réseau traditionnel hiérarchique de sous-zones SNA et un réseau de plusieurs LAN interconnectés, basé sur des protocoles dynamiques sans connexion. L'avantage du réseau de sous-zones est qu'il est maniable et fournit un temps de réponse prévisible. L'inconvénient est qu'il nécessite une définition étendue de l'organisation du système et ne tire pas profit des capacités d'équipements plus intelligents, comme les PC et les stations de travail.

Rôle d'APPN

Les deux types de réseaux précités, sous-zones SNA et LAN interconnectés, ont pu être intégrés au moyen d'APPN, car ce protocole possède de nombreuses caractéristiques propres aux réseaux LAN et offre en même temps les avantages de SNA. Ses principaux avantages sont :

- la possibilité d'établir des connexions entre homologues (peer-to-peer), ce qui permet à un utilisateur final d'initier une connexion avec n'importe quel autre utilisateur final sans l'intervention du mainframe (VTAM) ;
- le support d'applications de sous-zones ainsi que de nouvelles applications peer-to-peer sur un même réseau ;
- la fourniture d'un protocole de routage efficace pour permettre à un trafic SNA natif de circuler en même temps que d'autres protocoles sur un même réseau ;
- la maintenance de la traditionnelle classe de service (CoS) SNA/priorité de transmission.

A mesure que SNA a évolué, une fonctionnalité est restée cruciale pour bon nombre d'utilisateurs : la classe de service ou CoS (*Class of Service*). Elle permet une gestion de la priorité du trafic par session SNA sur l'épine dorsale. Cela permet en retour à un utilisateur de bénéficier de sessions avec plusieurs applications, chacune avec une classe de service différente. Avec APPN, cette fonctionnalité offre davantage de granularité et étend ses services jusqu'aux noeuds d'extrémité au lieu de s'arrêter aux contrôleurs de communication (FEP).

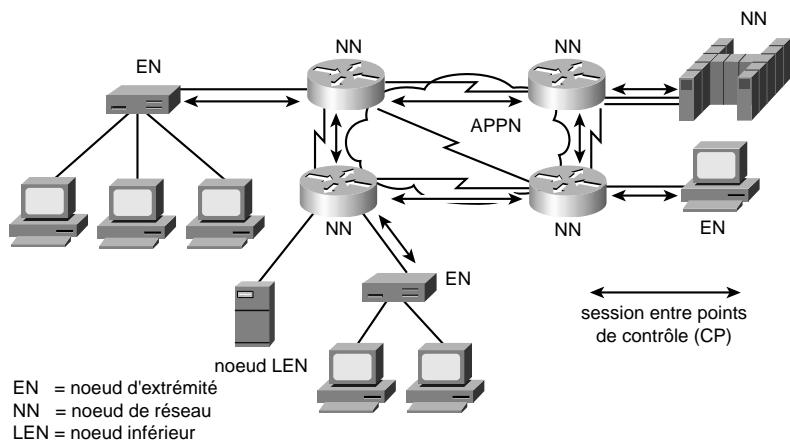
Types de nœuds APPN

Un réseau APPN possède les 3 types de nœuds suivants, décrits au Tableau 7.1 : le nœud de niveau inférieur ou LEN (*Low Entry Node*), le nœud d'extrême ou EN (*End Node*) et le nœud de réseau ou NN (*Network Node*), comme illustré Figure 7.1.

Le Tableau 7.1 décrit ces différents types de nœuds. Le point de contrôle ou CP (*Control Point*), qui est responsable de la gestion des ressources d'un nœud et de sa communication avec un nœud adjacent, est un élément essentiel d'un nœud APPN. Il est l'équivalent du SSCP (*System Services Control Point*) sur un hôte SNA.

Figure 7.1

Différents types de nœuds APPN.



SSCP : System Service Control Point

Dans la communication réseau SNA traditionnelle (également nommée routage de sous-zone), VTAM représente le composant principal qui contrôle toutes les ressources SNA, telles que les sous-systèmes applicatifs (CICS, TSO, et IMS), les unités de contrôle (3174, 3274), les FEP, les terminaux et les imprimantes. La fonction SSCP de VTAM assure la définition ainsi que l'activation et la désactivation de ces ressources.

Vous obtiendrez davantage d'informations sur APPN dans la section "Présentation d'APPN" de ce chapitre.

Tableau 7.1 : Différents types de nœuds APPN

Type de nœud APPN	Description
LEN (<i>Low Entry Node</i> *)	Ce nœud de niveau inférieur, antérieur à APPN, est un nœud de type homologue (peer-to-peer). Il peut participer sur un réseau APPN en utilisant les services fournis par un nœud de réseau adjacent (NN). Le point de contrôle (CP) du nœud LEN gère les ressources locales, mais n'établit pas de session CP-CP avec un nœud adjacent. Les partenaires d'une session doivent être prédéfinis au niveau du nœud LEN et celui-ci doit être prédéfini au niveau du nœud de réseau adjacent. Le nœud LEN est également appelé nœud SNA type 2.1, unité physique (PU) type 2.1 ou PU2.1.
EN (<i>End Node</i>)	Ce nœud d'extrême contient un sous-ensemble de fonctionnalités APPN. Il accède au réseau par l'intermédiaire d'un nœud de réseau (NN) adjacent et en utilise les services de routage. Il peut établir une session CP-CP avec un nœud NN et utilise cette session pour enregistrer des informations de ressources, réclamer des services d'annuaire et demander des données de routage.
NN (<i>Network Node</i>)	Ce nœud englobe toutes les fonctionnalités APPN. Le point de contrôle (CP) sur un nœud de réseau (NN) est responsable de la gestion des ressources de ce nœud, ainsi que des nœuds d'extrême (EN) et de niveau inférieur (LEN) qui sont reliés à son nœud de réseau. Le CP établit des sessions CP-CP avec des nœuds d'extrême et de réseau adjacents. Il maintient également les informations sur la topologie du réseau et les bases de données d'annuaire, qui sont créées et mises à jour grâce à une collecte dynamique de renseignements auprès de ces nœuds adjacents.

*NdT : On associe parfois dans la littérature la signification Local Entry Networking Node à ce sigle.

Intégration d'APPN dans la conception d'un réseau

L'architecture APPN présente deux avantages essentiels par rapport aux autres protocoles :

- routage SNA natif ;
- classe de service (CoS) offrant la garantie de livraison.

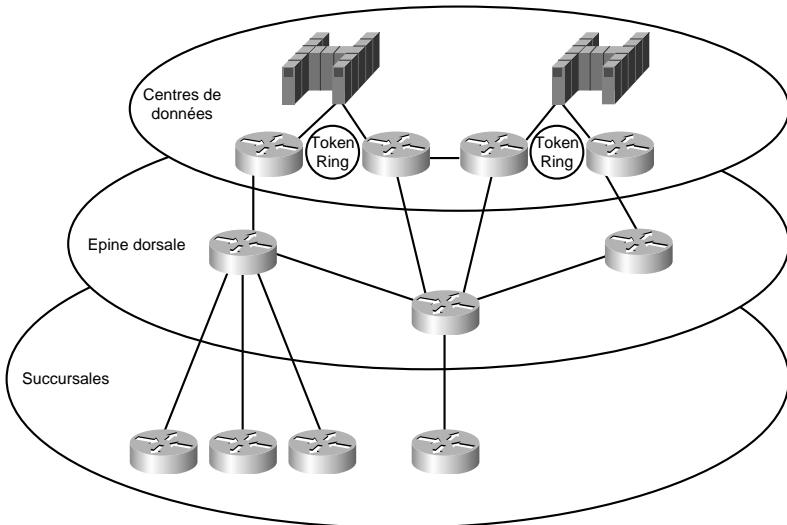
APPN, comme TCP/IP (*Transmission Control Protocol/Internet Protocol*), est un protocole routable, dont les décisions de routage sont prises au niveau des nœuds de réseau (NN). Bien que seul le nœud de réseau adjacent à l'initiateur de la session sélectionne le chemin de la session, tous les autres nœuds de réseau contribuent au processus de routage en se tenant informés de la topologie du réseau. Le nœud de réseau contigu à la destination y participe aussi en fournissant des données détaillées sur la destination. Seuls les routeurs fonctionnant en tant que nœuds de réseau APPN peuvent prendre des décisions de routage.

Les nœuds LEN et EN représentent toujours les points terminaux de sessions. Ils s'appuient sur les nœuds NN en ce qui concerne les décisions de routage, lesquels calculent les meilleurs itinéraires pour l'établissement des sessions.

Pour que les décisions de routage soient possibles (par exemple, choisir un centre de données ou un itinéraire), APPN doit être implémenté. La Figure 7.2 présente les critères sur lesquels se fonder pour savoir si APPN doit être utilisé ou non sur un réseau.

Figure 7.2

Choix du niveau d'intégration d'APPN.



A la Figure 7.2, un seul lien connecte chaque succursale à l'épine dorsale. Par conséquent, aucune décision de routage n'est nécessaire à leur niveau et un nœud de réseau APPN n'est donc pas utile sur ces sites.

Comme il y a néanmoins deux centres de données, une décision de routage doit pouvoir être prise pour déterminer vers quel centre diriger le trafic. Cette décision peut avoir lieu au niveau des routeurs des centres de données ou de ceux de l'épine dorsale. Si vous souhaitez que le routage soit décidé au niveau des centres, tout le trafic doit être expédié vers un seul d'entre eux, via DLSw+ par exemple, pour être ensuite routé vers le centre approprié, et ce en utilisant APPN uniquement au niveau des routeurs du centre voulu. Si, en revanche, vous voulez que les décisions d'acheminement aient lieu au niveau des routeurs de l'épine dorsale, placez les nœuds APPN sur ces derniers. Les décisions d'itinéraire seront alors effectuées en dehors des centres de données. Dans cet exemple, la seconde option est préférable, car elle permet de limiter la fonction des routeurs de centre de données à la connexion avec le canal, de réduire le nombre de sauts vers le second centre de données et de fournir un chemin vers un centre de secours en cas de sinistre.

Comme APPN nécessite davantage de ressources mémoire et logicielles, cette solution est généralement plus coûteuse. Les avantages du routage direct APPN et de la classe de service compensent toutefois souvent les frais supplémentaires engagés. Dans notre exemple, les coûts impliqués dans une solution de routage APPN au niveau de l'épine dorsale ou des centres de données seraient justifiés, alors qu'ils ne le seraient pas pour une stratégie de routage au niveau des succursales.

Nœud de réseau APPN au niveau de chaque site distant

Deux situations justifient l'ajout d'un nœud de réseau à chaque site distant de succursale :

- quand la classe de service est nécessaire ;
- quand le routage entre succursales est requis.

Impératif de classe de service

Comme la classe de service (CoS) implique que l'utilisateur accède à plusieurs applications, elle doit permettre l'attribution d'une priorité au trafic à un niveau application. Bien que d'autres stratégies, comme la gestion par file d'attente personnalisée, puissent assigner une priorité au niveau utilisateur, elles ne la gèrent pas entre plusieurs applications d'un même utilisateur. Si vous deviez absolument disposer de cette fonctionnalité, les nœuds de réseau APPN devraient alors être placés au niveau des sites de succursales pour consolider le trafic provenant de plusieurs utilisateurs utilisant la classe de service. Celle-ci pourrait, par exemple, garantir qu'une procédure de vérification de cartes de crédit obtienne toujours une priorité supérieure à celle d'une procédure de réception par un site central des lots d'une entreprise de détail.

Il est important de comprendre où la classe de service est utilisée sur le réseau aujourd'hui. S'il s'agit d'un réseau SNA de sous-zones, la classe de service n'est exploitée qu'entre dispositifs FEP et ACF/VTAM, ou entre dispositifs ACF/VTAM, ou entre contrôleurs FEP. A moins qu'il n'y ait déjà un FEP sur le site d'une succursale, aucune priorité n'est attribuée à partir de la succursale, encore que ce ne serait qu'en sortie de FEP. Dans ce cas, l'ajout d'un nœud de réseau APPN sur le site de la succursale pourrait assurer une priorité en amont pour le trafic à destination d'un centre de données, au lieu d'attendre qu'il atteigne le FEP.

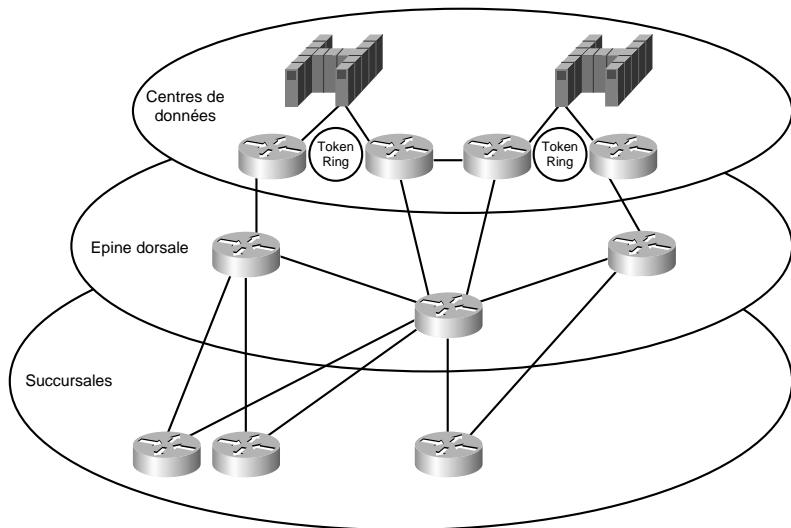
Impératif de routage entre succursales

Si maintenant le trafic doit aussi circuler entre les succursales, vous pouvez envoyer tout le trafic vers un site central et laisser ses nœuds de réseau APPN se charger de l'acheminement en direction des sites appropriés. C'est la solution la plus évidente lorsqu'il faut pouvoir gérer un trafic vers un centre de données et entre des succursales et que chacune de celles-ci n'est reliée à l'épine dorsale que par un seul lien. Toutefois, si le coût associé à la mise en place d'une liaison directe entre deux succursales est justifiable, router toutes les informations vers un centre de données est inacceptable. Dans cette nouvelle configuration, il est utile que les décisions de routage soient prises au niveau succursale. Avec l'ajout de nœuds de réseau APPN aux endroits stratégiques, le trafic se destinant aux centres de données serait ainsi transmis sur une liaison vers le centre approprié et celui inter-succursales pourrait être expédié via un lien direct.

A l'exemple de la Figure 7.3, chaque succursale possède deux liaisons en direction des routeurs alternatifs des centres de données. C'est une situation dans laquelle des nœuds de réseau APPN peuvent être nécessaires au niveau des succursales afin que les liaisons appropriées puissent être sélectionnées. Cela pourrait aussi être le tracé prévu pour le routage d'un trafic inter-succursales, avec l'ajout d'un seul saut (hop) plutôt que la création de tout un maillage. Le routage obtenu est plus direct que s'il fallait d'abord envoyer tout le trafic vers un centre de données décisionnaire.

Figure 7.3

Exemple de réseau sur lequel un routage de trafic inter-succursales est nécessaire.



Comme vous l'apprendrez plus loin, il vaut mieux maintenir un nombre de noeuds de réseau aussi faible que possible pour des questions d'évolutivité. Savoir discerner quand le routage natif et la classe de service sont nécessaires est essentiel pour pouvoir minimiser le nombre de noeuds de réseau.

En résumé, pour déterminer les points d'implémentation d'APPN, il faut évaluer certains critères comme le coût, l'évolution possible et les endroits où le routage natif et la classe de service sont requis. Intégrer APPN sur l'ensemble du réseau pourrait sembler être la solution évidente, même si cela n'était pas nécessaire. Il faut bien comprendre qu'un tel déploiement serait probablement plus coûteux par rapport à ce que les besoins réels entraîneraient et pourrait éventuellement, dans le futur, être une source d'obstacles à l'évolution du réseau. En conséquence, installez APPN là où ses fonctionnalités sont réellement requises.

APPN ou autres méthodes de transport SNA

APPN et les fonctions BNN/BAN (*Border Network Node/Border Access Node*, noeud de réseau de frontière/noeud d'accès de frontière) sur Frame Relay, selon le RFC 1490, représentent deux méthodes de transport de SNA natif, où SNA n'est pas encapsulé dans un autre protocole. BAN et BNN offrent une connexion directe à un FEP, en utilisant le réseau Frame Relay pour commuter les messages, à la place d'un routage SNA direct.

Bien que le routage en mode *natif* puisse sembler être la stratégie appropriée, APPN implique certains sacrifices en termes de coûts, mais aussi d'évolutivité, comme nous l'avons vu à la section précédente. Avec la solution BNN/BAN, un engagement financier supplémentaire est nécessaire pour mettre en œuvre une communication multiprotocole, car le FEP ne peut gérer plusieurs protocoles. Cela implique l'ajout de routeurs au niveau du centre de données, afin de gérer les autres protocoles, et la mise en place de circuits virtuels distincts pour offrir une garantie de livraison du trafic SNA ou APPN.

Le protocole DLSw+ permet d'encapsuler SNA en plaçant l'intégralité du message APPN dans le champ "données" du message TCP/IP. Les 40 octets supplémentaires d'en-tête associés à TCP/IP provoquent bien quelques inquiétudes. Toutefois, comme Cisco offre d'autres solutions telles que Data Link Switching Lite, Fast Sequenced Transport (FST) et Direct Transport, qui utilisent des en-têtes plus courts, cette partie du message ne sera pas considérée comme problématique dans le cadre de notre discussion.

DLSw+ est une solution intéressante pour les réseaux sur lesquels les stations et le centre de données sont implémentés avec SNA, mais où l'épine dorsale exploite TCP/IP. Cela permet d'avoir un seul protocole sur toute l'épine dorsale, tout en maintenant l'accès à toutes les applications SNA. DLSw+ ne fournit ni routage APPN natif, ni classe de service. Par conséquent, il est préférable d'employer DLSw+ sur des réseaux pour lesquels le coût est un facteur essentiel et possédant les caractéristiques suivantes :

- un seul centre de données ou mainframe ;
- des liens uniques à partir des succursales.

En général, DLSw+ offre une solution de moindre coût, qui nécessite moins de mémoire et de logiciels. Dans la grande majorité des réseaux, DLSw+ est combiné avec APPN, et ce dernier est utilisé uniquement là où les décisions de routage sont cruciales. Avec l'encapsulation TCP/IP, la couche TCP fournit une livraison aussi fiable que SNA/APPN, sans le routage natif et la classe de service.

TN3270 transporte les flots de données 3270 à l'intérieur d'un paquet TCP/IP sans les en-têtes SNA. Par conséquent, cette solution suppose que la station terminale ne dispose que d'une pile de protocoles TCP/IP et d'aucune pile SNA. TN3270 n'est donc pas une solution de remplacement à APPN, car celui-ci requiert que la station destinataire possède une pile SNA. A l'instar de DLSw+, APPN peut être utile sur le réseau pour assurer le routage entre des serveurs TN3270 et plusieurs mainframes ou centres de données.

En résumé, APPN sera fréquemment utilisé avec DLSW+ sur des réseaux lorsqu'un seul protocole est accepté sur l'épine dorsale. La solution BAN/BNN fournit une connectivité directe vers le FEP, mais il lui manque les fonctionnalités des autres solutions. TN3270 n'est utilisé que pour les stations finales TCP/IP.

Présentation d'APPN

Cette section introduit l'architecture d'APPN et traite des sujets suivants :

- définition de nœuds ;
- établissement de sessions APPN ;
- compréhension du routage de session intermédiaire ;
- utilisation de DLUR/DLUS (*Dependant Logical Unit Requester/Server*).

Définition de nœuds

Les nœuds, comme ACF/VTAM, OS/400 et Communication Server/2 (CS/2), peuvent être définis en tant que nœud de réseau (NN) ou nœud d'extrémité (EN). Si vous devez faire un choix, aidez-vous des points suivants :

- **Taille du réseau.** Déterminez la taille du réseau. La conception de réseaux APPN étendus peut parfois être une source d'obstacles pour une évolution future. Réduire le nombre de nœuds de réseau pourra apporter une solution à ce problème. Pour plus d'informations sur la réduction du nombre de nœuds de réseau, voyez la section "Réduction du nombre de nœuds de réseau" de ce chapitre.
- **Rôle du nœud.** Interrogez-vous sur les fonctions du nœud, à savoir s'il doit assurer des fonctions de routage en même temps que de traitement d'applications. Des nœuds de réseau distincts contribuent à une réduction des cycles de traitement et des exigences en termes de mémoire sur un contrôleur d'applications.

Généralement, vous devez définir un nœud de réseau partout où une décision de routage doit être prise.

Identificateurs de nœuds APPN

Un nœud APPN est identifié par son nom de réseau CP qualifié, qui suit le format *netid.nom*. La portion *netid* est un nom de huit caractères qui identifie le réseau ou le sous-réseau sur lequel la ressource est située. L'identifiant de réseau et le nom doivent être représentés sous forme d'une combinaison de lettres majuscules (A à Z), de chiffres (0 à 9) et de caractères spéciaux (\$, # ou @), où la première position ne doit pas être un chiffre.

Etablissement de sessions APPN

Une session APPN est établie selon la procédure suivante :

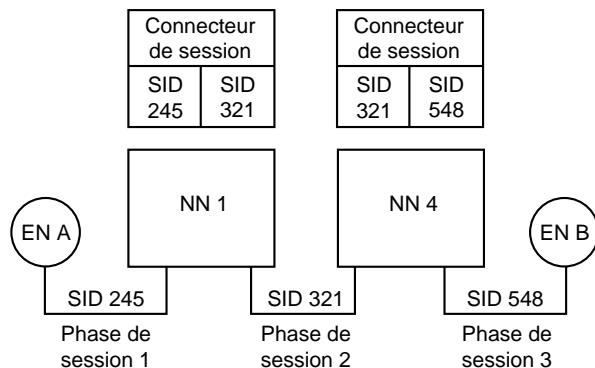
1. L'utilisateur final demande une session d'application qui entraîne l'initiation du processus d'établissement de la session par le nœud d'extrémité (EN), qui envoie un message LOCATE à son serveur nœud de réseau (NNS). Pour établir la session, le serveur fournit le chemin menant au nœud EN de destination, ce qui permet au nœud EN d'origine de lui envoyer directement des messages. Cela est vrai pour un nœud EN, mais pas pour un nœud LEN, qui envoie un message BIND à un serveur nœud de réseau (NNS). Ce dernier assure un service d'annuaire en envoyant des messages LOCATE aux autres nœuds NN et EN.
2. Le nœud NN source utilise les services d'annuaire pour localiser la destination en contrôlant d'abord son répertoire interne. Si la destination n'est pas incluse dans le répertoire interne, il envoie une requête LOCATE vers le serveur d'annuaire central ou CDS (*Central Directory Server*), s'il en existe un. S'il n'y a pas de serveur d'annuaire central disponible, le nœud NN envoie un message LOCATE en mode diffusion vers les nœuds NN adjacents qui, à leur tour, le propagent. Le nœud NN du destinataire renvoie une réponse indiquant l'emplacement de celui-ci. Le NN trouve l'emplacement du CDS dans la base de données topologiques.
3. Le nœud NN source choisit le chemin de plus faible coût capable d'offrir le service approprié en se basant sur l'emplacement de la destination, la classe de service demandée par l'initiateur de la session, la base de données topologique et les tables de classes de service.
4. Le serveur nœud de réseau d'origine envoie une réponse LOCATE au nœud EN source. La réponse donne le chemin jusqu'à la destination.

5. Le nœud EN source est alors responsable de l'initiation de la session. Un message BIND est envoyé du nœud EN source vers le nœud EN de destination, en demandant une session. Le destinataire répond au message BIND et le trafic de la session peut commencer à circuler.

Routage intermédiaire de session

Des connecteurs de session sont utilisés à la place de tables de routage avec APPN. Les identifiants uniques de session et ports respectifs de chacun des nœuds participant à une connexion sont mis en correspondance. Lorsque le trafic passe à travers un nœud, l'identifiant de session dans l'en-tête est remplacé par l'identifiant de sortie et envoyé sur le port approprié (voir Figure 7.4).

Figure 7.4
Echange d'étiquette de routage intermédiaire de session.



Cet algorithme de routage est appelé ISR (*Intermediate Session Routing*). Il offre un support pour la définition de route et incorpore les fonctionnalités traditionnelles suivantes :

- **Traitement d'erreur et contrôle du flux aux nœuds d'extrémité.** Cette fonction reflète la méthode de commutation de paquets des années 70, qui provoquait de nombreuses erreurs de ligne, imposant de ce fait le contrôle d'erreur et de flux sur chaque nœud. Etant donné la haute qualité des services numériques qui existent actuellement en de nombreux endroits, ce traitement redondant se révèle inutile et réduit de façon significative le débit entre les nœuds d'extrémité d'une communication. Le traitement de bout en bout fournit de meilleures performances tout en assurant le degré de fiabilité nécessaire.
- **Interruption de commutation de session en cas de panne de réseau.** Lorsqu'une liaison est interrompue sur le réseau, toutes les sessions qui l'utilisent le sont aussi et doivent être réinitialisées pour pouvoir emprunter un autre chemin.

Comme ces fonctionnalités sont aujourd'hui inacceptables sur la plupart des réseaux à grande vitesse, un nouvel algorithme de routage, HPR (*High Performance Routing*), a été ajouté à APPN afin de supporter le rerouting sans interruption pour contourner les pannes, ainsi que le contrôle d'erreur, le contrôle de flux et la segmentation de bout en bout. Les routeurs Cisco gèrent ISR et HPR.

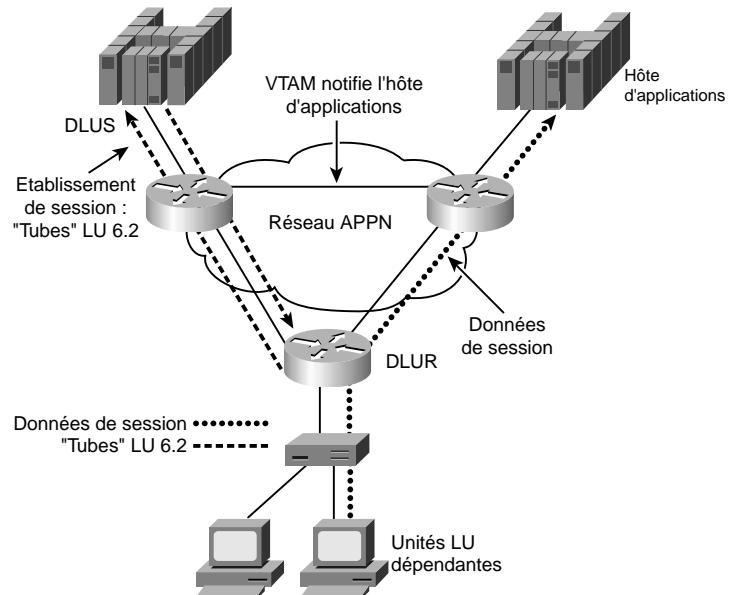
Utilisation des DLUR/DLUS

La gestion des DLUR/DLUS (*Dependent Logical Unit Requester/Server*) est une fonctionnalité APPN qui autorise le trafic de terminaux anciens à circuler sur un réseau APPN. Avant l'introduction de cette fonctionnalité, l'architecture APPN supposait que tous les nœuds sur un réseau pouvaient initier un trafic peer-to-peer (par exemple, l'envoi du message BIND pour débuter la session). De nombreux terminaux anciens, auxquels on se réfère par le terme DLU, ou unités logiques dépendantes, ne le peuvent pas et ont besoin que VTAM avertisse l'application, qui envoie ensuite le message BIND.

Pour que des sessions entre dispositifs anciens puissent être initiées, une relation client/serveur doit exister entre le ACF/VTAM (serveur de LU dépendant ou DLUS) et le routeur Cisco (demandeur de LU dépendant ou DLUR). Une paire de sessions LU type 6.2 est alors établie entre le DLUR et le DLUS (une session est établie par chaque point d'extrémité). Ces sessions servent à transporter les anciens messages de contrôle qui doivent circuler pour activer les anciennes ressources et initier leurs sessions LU-LU. Une session LU-LU est la connexion qui est initiée lorsque les cinq étapes décrites plus haut à la section "Etablissement de sessions APPN" sont réalisées.

Par exemple, pour activer une ancienne LU, un message d'activation d'unité logique (ACTLU, *Activate Logical Unit*) doit lui être envoyé. Comme ce message n'est pas reconnu dans un environnement APPN, il est transporté par encapsulation sur la session 6.2. Le DLUR le désencapsule à la réception et le passe à l'ancienne LU. De la même manière, la requête de session DLU est transmise au DLUS de l'ACF/VTAM où elle est traitée en tant que trafic hérité. Le DLUS envoie ensuite un message à l'hôte d'applications qui est responsable de l'envoi du message BIND. Après l'établissement de la session LU-LU, les données peuvent circuler en natif avec le trafic APPN, comme illustré Figure 7.5.

Figure 7.5
Traitement de session DLU.



Implémentation Cisco d'APPN

Cette section présente l'implémentation Cisco d'APPN et précise sa place dans le système d'exploitation Cisco IOS. Cisco a obtenu une licence d'exploitation auprès d'IBM pour le code source d'APPN et l'a porté dans son logiciel pour pouvoir utiliser les services de réseau de DLC (*Data Link Control*, contrôle de liaison de données).

Les applications utilisent APPN pour assurer le transport sur le réseau. Cette architecture s'exécute au-dessus du système Cisco IOS. APPN est un protocole de couche supérieure qui requiert les services de réseau de DLC. L'implémentation Cisco est conforme aux spécifications de l'architecture APPN. Lorsqu'il est utilisé avec d'autres fonctionnalités du système d'exploitation IOS, il présente les caractéristiques suivantes :

- APPN peut utiliser DLSw+ ou RSRB en tant que mécanisme de transport de réseau pour être supporté sur un réseau TCP/IP natif.
- APPN peut être utilisé avec un dispositif de concentration en aval d'unités physiques (DSPU, *Downstream Physical Unit*) afin de réduire le nombre de PU en aval visibles pour VTAM. Cela limite la définition de VTAM et le nombre de redémarrages du système.
- Avec la classe de service (CoS), les fonctionnalités de mise en files d'attente de priorité, personnalisée et équitable pondérée, peuvent être utilisées afin d'assurer la gestion de priorité et/ou la réservation de bande passante entre protocoles.
- Les options de gestion du réseau sont supportées et comprennent les services de gestion SNA natifs utilisant NSP (*Native Service Point*) sur les routeurs Cisco, et SNMP (*Simple Network Management Protocol*) par l'intermédiaire des applications Cisco Works Blue.
- Avec l'emploi d'un CIP (*Channel Interface Processor*) ou d'un CPA (*Channel Port Adapter*), le nœud APPN peut s'interfacer directement avec l'ACF/VTAM à travers le canal. VTAM peut être défini en tant que nœud EN ou nœud NN.

Problèmes d'évolutivité

En tant qu'architecture d'état des liens d'un réseau, la topologie est mise à jour chaque fois que des changements ont lieu. Il en résulte un trafic de réseau considérable en cas d'instabilité et une consommation importante des ressources mémoire et des cycles de traitement en vue de maintenir les grandes bases de données topologiques et les tables CoS. De la même manière, la découverte dynamique des ressources sur les réseaux étendus peut aussi être consommatrice en bande passante et en ressources de traitement. Pour toutes ces raisons, l'évolutivité devient un problème à mesure que la taille du réseau augmente. Les facteurs suivants influent sur la charge des nœuds :

- quantité du trafic ;
- stabilité du réseau ;
- nombre de techniques (décrisées dans cette section) utilisées pour contrôler le trafic et le traitement.

Fondamentalement, pour permettre aux réseaux APPN de s'étendre, la conception doit se focaliser sur la réduction du nombre des mises à jour de bases de données topologiques (TDU, *Topology Database Update*) et des requêtes de recherche LOCATE.

Réduction des mises à jour de bases de données topologiques

APPN est un protocole qui se base sur un algorithme de routage par état de lien. A l'instar des autres algorithmes de ce type, il maintient une base de données d'informations sur l'ensemble de la topologie du réseau. Chaque nœud de réseau APPN envoie des paquets TDU, qui décrivent l'état actuel de tous ses liens vers les nœuds de réseau adjacents. Un paquet TDU contient des informations qui identifient les éléments suivants :

- les caractéristiques du nœud émetteur ;
- les caractéristiques du nœud et des liaisons vers les diverses ressources sur son réseau ;
- le numéro de séquence de la mise à jour la plus récente pour chaque ressource décrite.

Un nœud de réseau qui reçoit un paquet TDU propage les informations qu'il contient vers les nœuds de réseau qui lui sont adjacents en utilisant une technique de réduction de flux. Chaque nœud de réseau maintient des informations complètes sur le réseau et la façon dont ses liens sont interconnectés. Lorsqu'un nœud de réseau détecte un changement (au niveau de la ligne ou du noeud), il inonde le réseau de paquets TDU pour assurer une convergence rapide. Si un lien instable existe sur le réseau, il représente une source potentielle d'importantes diffusions de TDU.

A mesure que le nombre de nœuds de réseau et de liaisons augmente, le nombre de paquets TDU augmente aussi. Ce type de distribution d'informations de topologie peut se révéler très consommateur en cycles de traitement, en mémoire et en bande passante. La maintenance des itinéraires et d'un grand sous-réseau de communication complet peut nécessiter une importante quantité de mémoire dynamique.

Vous pouvez utiliser les techniques suivantes pour diminuer la quantité de paquets TDU qui circulent sur le réseau :

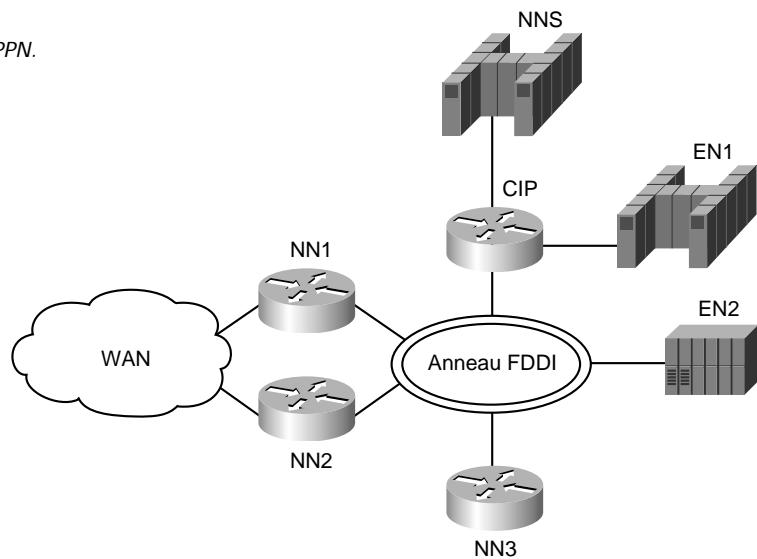
- Réduisez le nombre de liens.
- Réduisez le nombre de sessions CP-CP.
- Réduisez le nombre de nœuds de réseau.

Réduction du nombre de liens

La première méthode de limitation de la quantité de paquets TDU transitant sur le réseau consiste à réduire le nombre de liens du réseau. Dans certaines configurations, il est parfois possible de recourir au concept de *réseau de connexion* pour diminuer le nombre de liens prédefinis. Comme les nœuds de réseau échangent des informations sur leurs liaisons, moins vous aurez de liaisons et moins ils généreront de paquets TDU.

La Figure 7.6 illustre le tracé physique d'un réseau APPN. Les nœuds NN1, NN2 et NN3 représentent des routeurs connectés à un réseau local FDDI.

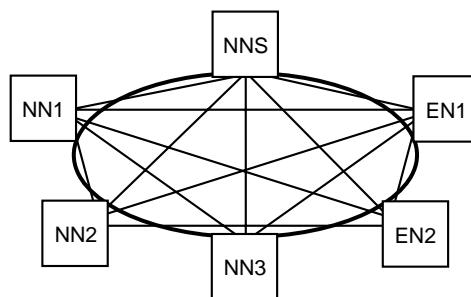
Figure 7.6
Tracé physique d'un réseau APPN.



Les hôtes des nœuds NNS (Network Node Server), EN1 et EN2 sont connectés au même réseau local FDDI via un routeur CIP ou un contrôleur de cluster. Ces nœuds sur le réseau FDDI sont reliés par une connectivité any-to-any. Pour refléter cette connectivité avec APPN, le nœud NN1 doit définir une liaison vers les nœuds NN2, NN3, NNS (hôte VTAM), EN1 (hôte de données VTAM) et EN2 (hôte de données EN). Les groupes de transmission interconnectant les nœuds de réseau sont contenus dans la base de données de topologie du réseau. Des paquets TDU sont diffusés pour chaque liaison qui est définie vers le nœud de réseau.

La Figure 7.7 illustre la vue logique du réseau APPN présenté à la Figure 7.6. Lorsque le nœud NN1 rejoint le réseau pour la première fois, il active les liaisons vers NN2, NN3, NNS, EN1 et EN2. Des sessions CP-CP sont établies avec les nœuds de réseau adjacents. Chaque nœud de réseau adjacent envoie une copie de la base de données de topologie actuelle à NN1.

Figure 7.7
Vue logique d'un réseau APPN sans déploiement d'un réseau de connexions.

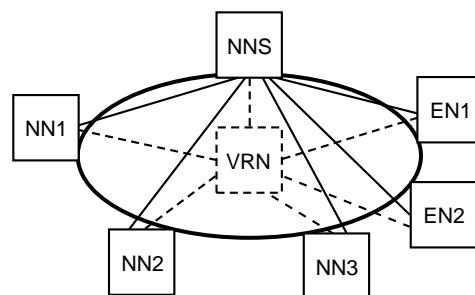


De la même manière, ce dernier crée un paquet TDU avec des informations le concernant ainsi que ses liens avec les autres nœuds et l'envoie vers les nœuds NN2, NN3 et NNS par l'intermédiaire des sessions CP-CP. Lorsque NN2 reçoit le TDU de NN1, il le retransmet vers ses nœuds de réseau adjacents, qui sont NN3 et NNS. Selon le même processus, ces derniers renvoient le TDU de NN1 vers leurs nœuds adjacents. Le résultat est que plusieurs copies du même TDU sont reçues par chaque nœud du réseau.

Les groupes de transmission qui interconnectent les nœuds d'extrémité ne sont pas contenus dans la base de données de topologie du réseau. En conséquence, aucun paquet TDU n'est diffusé pour les deux liaisons vers les nœuds EN1 et EN2.

Si le nombre de groupes de transmission reliant les nœuds de réseau pouvait être réduit, celui des paquets TDU le serait également. En utilisant le concept de réseau de connexions, vous pouvez éliminer les définitions de groupes de transmission et, par conséquent, limiter le trafic de paquets TDU. Un réseau de connexions est un nœud de routage virtuel unique (VRN, *Virtual Routing Node*) qui assure une connectivité any-to-any pour chacun de ses nœuds connectés. Le VRN n'est pas un nœud physique, mais une entité logique qui indique que les nœuds utilisent un réseau de connexions et qu'un itinéraire de routage direct peut être choisi.

Figure 7.8
Vue logique d'un réseau APPN avec déploiement d'un réseau de connexions.



Les nœuds NN1, NN2 et NN3 possèdent chacun une liaison vers le serveur nœud de réseau (NNS) et une liaison vers le VRN. Lorsque la liaison entre NN1 et NNS est activée, NNS envoie une copie de la base de données de topologie actuelle vers NN1. Ce dernier crée un TDU avec des renseignements le concernant et concernant ses liens vers NNS et le VRN, puis l'envoie vers NNS. Comme NN1 ne possède pas de liaison définie vers NN2 et NN3, il ne leur envoie aucun paquet TDU. Lorsque NNS reçoit le TDU de NN1, il l'envoie vers NN2 et NN3 qui ne le retransmettent pas, car ils possèdent seulement une liaison vers NNS. Cette configuration réduit de façon considérable le nombre de paquets TDU qui circulent sur le réseau.

Lorsqu'une session est activée entre des ressources situées sur le réseau de connexions, le serveur nœud de réseau reconnaît qu'il s'agit d'un réseau de connexions et sélectionne un chemin direct au lieu d'effectuer un routage au moyen de ses propres nœuds de réseau. Cisco recommande de mettre en œuvre le concept de réseau de connexions lorsque cela est possible, car il permet non seulement de diminuer le nombre de TDU transitant sur le réseau, mais aussi de réduire grandement les définitions de système.

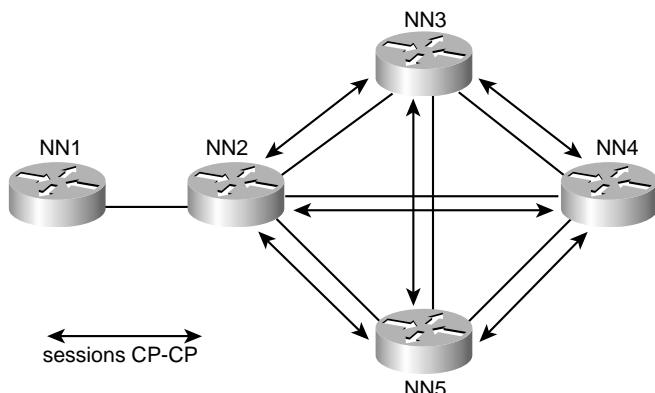
Comme illustré par l'exemple, un LAN (Ethernet, Token Ring ou FDDI) peut être défini en tant que réseau de connexions. Grâce aux services LANE (*LAN Emulation*, émulation LAN) d'ATM, vous pouvez interconnecter des réseaux ATM avec des réseaux locaux traditionnels. Pour APPN, comme un LAN émulé via ATM n'est rien d'autre qu'un LAN de plus, le concept de réseau de connexions peut être appliqué. Ce concept est aussi exploitable sur les réseaux X.25, Frame Relay et ATM. Il faut également noter que des technologies comme RSRB et DLSw sont vues comme des LAN pour APPN. Vous pouvez donc utiliser un réseau de connexions dans ces environnements. L'utilisation combinée d'APPN et des technologies RSRB et DLSw offre une synergie entre le routage et le pontage du trafic SNA.

Réduction du nombre de sessions CP-CP

La deuxième technique de limitation des paquets TDU sur le réseau consiste à réduire le nombre de sessions CP-CP sur le réseau. Les noeuds de réseau échangent des mises à jour de topologie au moyen de ces sessions. Leur nombre a donc un effet direct sur celui des TDU générés.

Par exemple, à la Figure 7.9, les noeuds NN2, NN3, NN4 et NN5 font partie d'un réseau totalement maillé. Chaque noeud établit des sessions CP-CP avec ses noeuds de réseau adjacents. Cela signifie que NN2 met en place des sessions CP-CP avec NN3, NN4 et NN5. De la même façon, NN3 établit des sessions CP-CP avec NN2, NN4, NN5, etc.

Figure 7.9
Sessions CP-CP totalement maillées.

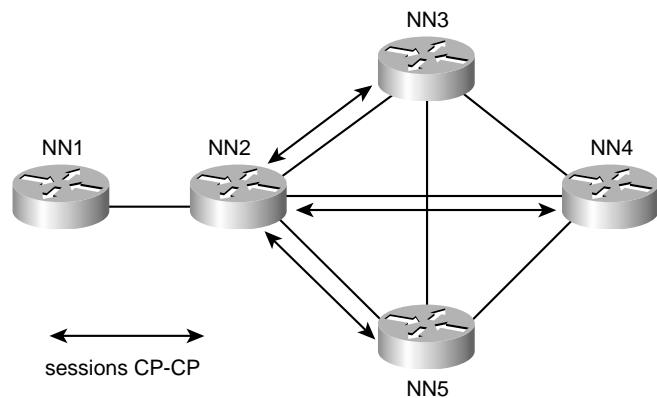


Si la liaison est interrompue entre NN1 et NN2, des mises à jour par TDU sont diffusées de NN2 vers NN3, NN4 et NN5. Lorsque NN3 reçoit le TDU, il le renvoie vers NN4 et NN5. De la même manière, lorsque NN5 le reçoit, il le retransmet vers NN3 et NN4. Cela signifie que NN4 recueille trois fois les mêmes renseignements. Vous devriez maintenir un nombre minimal de sessions CP-CP pour ne pas provoquer de duplication des informations de TDU.

A la Figure 7.10, des sessions CP-CP n'existent qu'entre NN2 et NN3, NN2 et NN4, et NN2 et NN5. Il n'y a aucune autre session CP-CP. Si la liaison est interrompue entre NN1 et NN2, ce

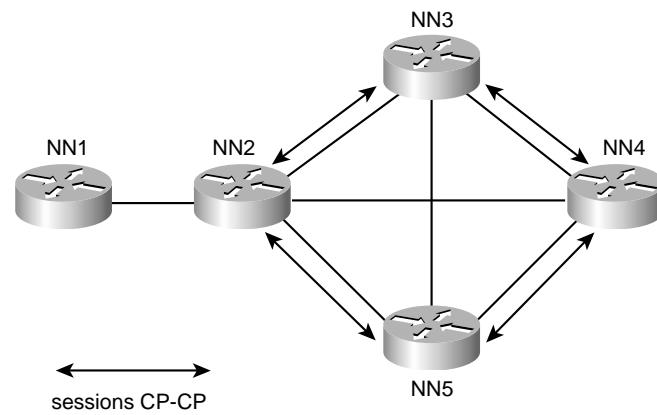
dernier diffuse des mises à jour de groupe de transmission vers NN3, NN4 et NN5. Aucun de ces trois noeuds ne retransmet ces informations au reste du réseau, car il n'existe pas d'autre session CP-CP. Bien que cette disposition permette de réduire le nombre de TDU, si la liaison entre NN2 et NN3 est interrompue, le réseau APPN se retrouve divisé et le noeud NN3 est isolé.

Figure 7.10
Une paire de sessions CP-CP.



La Figure 7.11 illustre une conception plus efficace qui fournit également une redondance. Chaque noeud de réseau possède des sessions CP-CP avec ses deux noeuds adjacents. NN2 possède des sessions CP-CP avec NN3 et NN5. Si la liaison entre NN2 et NN3 est interrompue, les TDU de mises à jour seront envoyés via NN5 et NN4.

Figure 7.11
Deux paires de sessions CP-CP.



A des fins de redondance, chaque noeud de réseau devrait disposer, si possible, de sessions CP-CP vers deux autres noeuds.

Réduction du nombre de noeuds de réseau

La troisième technique permettant de réduire la quantité de paquets TDU circulant sur le réseau consiste à diminuer le nombre de noeuds de réseau en définissant des noeuds APPN uniquement aux frontières du réseau. Cela permet également de limiter l'étendue de la topologie sous-jacente. Les technologies suivantes permettent d'atteindre cet objectif :

- APPN sur DLSw+ ;
- APPN sur Frame Relay Access Server (FRAS)/BNN ou BAN ;
- APPN sur RSRB.

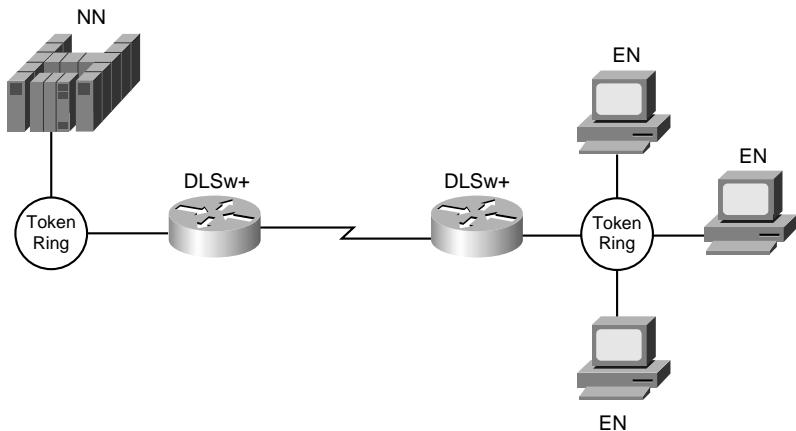
APPN sur DLSw+

La commutation de liaison de données est l'une des méthodes permettant de réduire le nombre de noeuds sur un réseau. DLSw+ permet de transporter le trafic APPN sur un réseau étendu, dans lequel les noeuds de réseau et/ou les noeuds d'extrémité APPN ne sont définis qu'aux frontières du réseau. Le routage intermédiaire est réalisé via DLSw+ et non via un trafic SNA natif.

DLSw+ définit un standard permettant d'intégrer SNA/APPN et des réseaux LAN en encapsulant ces protocoles à l'intérieur d'IP. L'implémentation Cisco de DLSw, connue sous la désignation de DLSw+, est un surensemble de l'architecture DLSw actuelle. DLSw+ possède de nombreuses fonctions utiles qui ne sont pas disponibles avec les versions de DLSw d'autres fabricants. Lorsque APPN est utilisé conjointement à DLSw+, il peut tirer profit des nombreuses améliorations offertes par ce dernier en matière d'évolutivité, comme les fonctions de routeur homologue interzone, d'ouverture de ligne à la demande, les algorithmes de gestion de cache et les pare-feu d'exploration.

A la Figure 7.12, les sessions entre les stations noeuds d'extrémité et l'hôte sont transportées sur le réseau DLSw+.

Figure 7.12
APPN avec DLSw+.

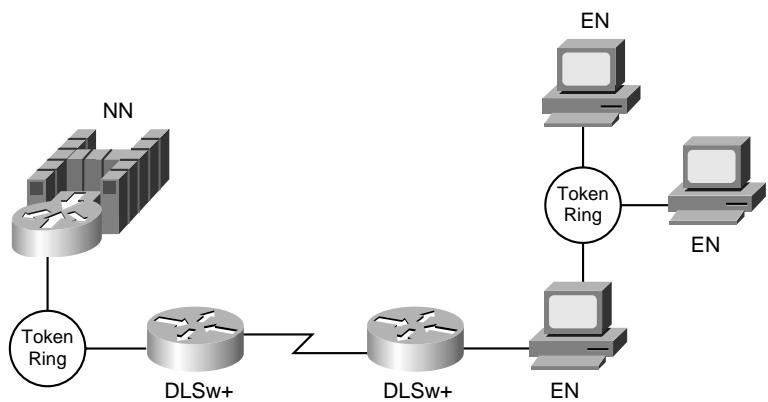


VTAM agit en tant que serveur noeud de réseau pour plusieurs stations noeuds d'extrémité. S'il existe plusieurs VTAM ou centres de données sur un réseau, l'implémentation d'APPN sur le

routeur (ou les routeurs) connecté via un canal à l'hôte ou sur les autres routeurs dans le centre de données peut permettre de décharger VTAM en offrant des fonctionnalités de routage SNA, comme illustré à la Figure 7.13.

Figure 7.13

APPN avec DLSw+ et l'utilisation d'un routeur connecté à l'hôte via un canal.



DLSw+ permet aussi un routage sans interruption en cas de panne sur le réseau étendu. L'utiliser comme système de transport réduit le nombre de nœuds sur le réseau. Un inconvénient est que les stations nœuds d'extrême nécessitent des connexions WAN pour accéder aux services du NNS. Un autre inconvénient est que, sans APPN sur les routeurs, la priorité de transmission APPN est perdue lorsque le trafic arrive sur le réseau DLSw+.

Pour plus d'informations sur DLSw et DLSw+, reportez-vous au Chapitre 8.

APPN sur FRAS BNN/BAN

Si le réseau APPN s'appuie sur un réseau Frame Relay, une option consiste à employer la fonction FRAS BNN/BAN pour accéder à l'hôte. Ces deux fonctions, BNN et BAN, permettent à un routeur Cisco d'être connecté directement à un FEP. Lorsque FRAS BNN est utilisé, cela suppose que le réseau Frame Relay assure la commutation et que le routage natif n'est pas utilisé au sein du réseau. Pour obtenir un exemple sur la façon dont APPN peut être utilisé avec FRAS BNN/BAN lors de la conception d'un réseau, voyez la section "APPN avec FRAS BNN".

APPN sur RSRB

Au moyen de RSRB, le trafic SNA peut être transmis à partir d'un site distant vers un centre de données via un pont. L'utilisation d'un pont distant à routage par la source peut réduire de façon significative le nombre total de nœuds du réseau et, du même coup, le nombre de paquets TDU devant y circuler. Un autre avantage lié à l'emploi de cette technique est qu'elle offre un routage sans interruption en cas de défaillance d'un lien.

Réduction des recherches LOCATE

Cette section décrit le trafic de diffusion sur un réseau APPN et précise en quoi les demandes de recherche LOCATE peuvent constituer un obstacle à l'évolutivité d'un tel réseau, sachant que leur

impact peut varier d'un réseau à un autre. Elle identifie certaines des causes qui sont à l'origine d'un nombre excessif de requêtes LOCATE et présente quatre techniques permettant d'y remédier :

- stockage sécurisé de cache d'annuaire ;
- entrées d'annuaire partielles ;
- serveur et client d'annuaire central ;
- enregistrement central de ressources.

Un nœud de réseau APPN autorise une localisation dynamique des ressources du réseau. Chaque nœud maintient dynamiquement des informations de ressources dans sa propre base de données d'annuaire. La base de données d'annuaire distribuée contient une liste de toutes les ressources du réseau. La requête de localisation LOCATE permet à un nœud de réseau d'effectuer une recherche dans la base de données d'annuaire de tous les autres nœuds de réseau.

Lorsqu'une ressource nœud d'extrémité demande l'établissement d'une session avec une autre ressource dont elle n'a pas connaissance, elle utilise les capacités de recherche de son serveur nœud de réseau pour localiser la ressource cible. Si le nœud de réseau ne possède aucune information sur la cible, il transmet une requête de localisation LOCATE à tous les nœuds de réseau qui lui sont adjacents en leur demandant d'aider le serveur nœud de réseau à identifier la ressource. Ces nœuds propagent à leur tour des requêtes de recherche vers leurs nœuds contigus. Ce processus de recherche est appelé *recherche par broadcast*.

Bien qu'il existe plusieurs mécanismes visant à réduire la quantité de recherches par diffusion (comme l'enregistrement ou la mise en cache de ressources), il peut néanmoins subsister une quantité excessive de flots de requêtes de localisation sur un réseau, en raison de ressources qui n'existent plus, d'une combinaison de réseaux de sous-zones et de réseaux APPN, ou bien de ressources indisponibles temporairement.

Stockage sécurisé de cache d'annuaire

La première technique que vous pouvez employer pour réduire la quantité de requêtes de localisation sur un réseau APPN est la fonction de stockage sécurisé de cache d'annuaire, qui est supportée par l'implémentation Cisco du nœud de réseau. Les entrées en cache dans la base de données d'annuaire d'un nœud de réseau peuvent être périodiquement écrites sur un support de stockage permanent : un hôte tftp. Ce processus permet d'accélérer le rétablissement en cas de défaillance d'un nœud de réseau. Les ressources n'ont pas besoin d'être redécouvertes par l'intermédiaire de requêtes de localisation. Cette fonctionnalité permet de réduire les pics de diffusion qui peuvent se produire lorsque le réseau APPN est remis en route.

Entrées d'annuaire partielles

La deuxième technique que vous pouvez utiliser pour limiter les requêtes de localisation sur un réseau APPN consiste à définir les ressources dans la base de données d'annuaire locale en identifiant le nœud d'extrémité ou le nœud de réseau lorsqu'une ressource particulière est repérée.

Voici un exemple de configuration :

```
appn partner-lu-location CISCO.LU21
owning-cp CISCO.CP2
complete
```

L'exemple précédent définit l'emplacement d'une LU nommée CISCO.LU21, qui est située au niveau du nœud d'extrémité ou du nœud de réseau CISCO.CP2. Cette commande améliore les performances du réseau en offrant la possibilité d'effectuer des recherches dirigées au lieu de recourir à une diffusion broadcast. L'inconvénient est qu'il faut créer des définitions. Pour contourner ce problème, il est possible d'utiliser des noms partiellement spécifiés pour définir plusieurs ressources.

Voici un exemple de configuration :

```
appn partner-lu-location CISCO.LU
  owning-cp CISCO.CP2
  wildcard
  complete
```

L'exemple précédent définit l'emplacement de toutes les unités LU comprenant un préfixe LU. L'observation d'une convention d'attribution de noms est évidemment essentielle à la réussite de ce type de définition de nœud.

Serveur et client d'annuaire central

La troisième technique sur laquelle vous pouvez vous appuyer pour minimiser les flots de requêtes de localisation sur un réseau APPN est la fonction de serveur/client d'annuaire central (CDS, *Central Directory Server/Client*). L'architecture APPN prévoit une fonction de serveur d'annuaire central qui permet à un nœud de réseau désigné d'agir en tant que point de centralisation servant à identifier les ressources du réseau. Sur les réseaux APPN actuels, chaque nœud de réseau est une source potentielle de diffusion de requêtes de localisation de ressources. La raison en est que la base de données des services d'annuaire n'est pas reproduite sur chaque nœud de réseau.

La fonction CDS permet à un nœud de réseau, associé à un logiciel client d'annuaire central, d'envoyer une requête dirigée vers un CDS. Si ce dernier n'a aucune connaissance de la ressource, il émet une requête en diffusion pour la localiser. Une fois qu'elle a été identifiée, le CDS place les informations correspondantes dans son cache d'annuaire. Par la suite, le CDS pourra indiquer l'emplacement de la ressource aux autres nœuds de réseau sans avoir à effectuer de recherche en diffusion. L'implémentation du nœud de réseau par Cisco supporte la fonction de client d'annuaire central. Le dispositif VTAM est actuellement le seul produit qui implémente la fonction CDS.

Cette fonction implique un maximum d'une seule requête en diffusion générale pour chaque ressource de réseau. Elle réduit donc de façon significative la quantité de trafic lié à la recherche d'entités. Vous pouvez définir plusieurs CDS sur un réseau APPN. Un nœud de réseau apprend l'existence d'un CDS par l'échange de TDU. S'il en existe plusieurs, celui qui se trouve le plus près (en fonction du nombre de sauts nécessaires pour l'atteindre) est utilisé. S'il est inaccessible, l'itinéraire vers le serveur alternatif le plus proche est calculé automatiquement.

Enregistrement central de ressources

La quatrième technique permettant de diminuer les flots de requêtes de localisation est la fonction d'enregistrement central de ressources. Un nœud d'extrémité enregistre ses ressources locales auprès de son serveur nœud de réseau. Si chaque ressource est ainsi enregistrée, tous les nœuds de réseau peuvent interroger le serveur d'annuaire central, ce qui élimine le besoin de générer des requêtes en mode broadcast.

L'activation de la session CP-CP et d'un nœud principal provoque l'enregistrement.

Les nœuds principaux qui incluent des ressources possèdent un paramètre d'enregistrement qui détermine si les ressources doivent être enregistrées avec le serveur nœud de réseau ou le serveur d'annuaire central, ou ne doivent pas du tout être enregistrées.

Techniques de secours sur un réseau APPN

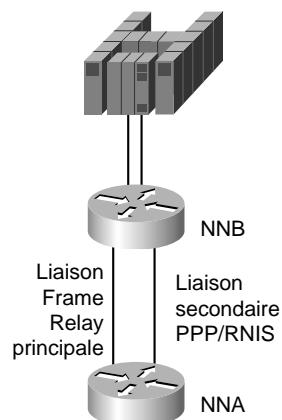
Cette section présente les diverses techniques de secours exploitables sur un réseau APPN. Les scénarios de soutien et de rétablissement sont représentatifs d'environnements et de besoins courants. Les trois scénarios suivants seront examinés :

- une liaison WAN secondaire en tant que lien de secours pour une liaison WAN principale ;
- des liaisons WAN doubles et des routeurs doubles assurant une redondance complète ;
- le support de secours de la fonctionnalité DLUR d'APPN au moyen d'un routeur CIP Cisco.

Ligne de secours

La première technique de secours que vous pouvez utiliser sur un réseau APPN est l'utilisation d'une liaison WAN secondaire en tant que solution de secours pour une liaison WAN principale. Grâce au concept d'auto-activation à la demande, vous pouvez assurer le soutien d'une liaison principale au moyen de n'importe quel protocole supporté — par exemple, PPP (*Point-to-Point Protocol*), SMDS (*Switched Multimegabit Data Service*), ou X.25 — comme illustré à la Figure 7.14.

Figure 7.14
Ligne de secours.



A la Figure 7.14, la liaison Frame Relay représente la liaison principale et la liaison RNIS représente la ligne de secours. La liaison RNIS doit être en mesure de fournir un soutien instantané de la liaison principale, mais doit demeurer inactive jusqu'à ce que cette dernière soit défaillante. Aucune intervention manuelle n'est nécessaire. Pour supporter cela, NNA doit définir deux groupes de transmission parallèles vers NNB.

La liaison principale est définie au moyen de la commande de configuration suivante :

```
appn link-station PRIMARY
port FRAME_RELAY
fr-dest-address 35
retry-limit infinite
complete
```

La liaison secondaire est définie pour supporter la fonction d'auto-activation au moyen de la commande de configuration suivante :

```
appn link-station SECONDARY
port PPP
no connect-at-startup
adjacent-cp-name NETA.NNB
activate-on-demand
complete
```

En spécifiant la commande **no connect-at-startup**, la liaison secondaire n'est pas activée au démarrage du nœud APPN. Pour spécifier le support de l'auto-activation, insérez la commande **adjacent-cp-name** et **activate-on-demand**.

En cas de rupture de la liaison principale, APPN détecte son dysfonctionnement ainsi que celui des sessions CP-CP. Ce dysfonctionnement interrompt toute session LU-LU existante. Comme il existe plusieurs liaisons de NNA vers NNB, NNA tente de rétablir les sessions sur la liaison secondaire. Cette requête active automatiquement la seconde liaison.

Pour s'assurer que la liaison Frame Relay est utilisée en tant que lien principal et que la liaison PPP sert de lien de secours, il faut définir les caractéristiques des groupes de transmission de façon appropriée. Par exemple, utilisez le paramètre **cost-per-connect-time** pour définir le coût relatif associé à l'utilisation de la liaison PPP/RNIS.

```
cost-per-connect-time 5
```

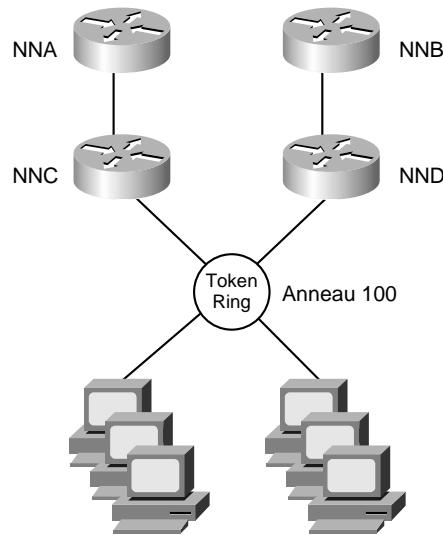
Dans ce cas, la liaison principale bénéficiera d'un coût d'itinéraire inférieur, car la valeur par défaut pour le paramètre est zéro. Elle représentera donc un chemin préférable par rapport à la liaison secondaire. Lors du rétablissement de la liaison principale, aucun mécanisme ne permet de rétablir automatiquement les sessions sur cette liaison. Une intervention manuelle est nécessaire.

Redondance totale

La seconde technique de secours que vous pouvez utiliser sur un réseau APPN est l'emploi de liaisons WAN doubles et de routeurs doubles afin d'obtenir une redondance complète. Dans certaines situations, une tolérance aux pannes totale est requise pour le transport de données cruciales. Une telle configuration permettra de parer à tous types de pannes de communication.

La Figure 7.15 illustre de quelle façon vous pouvez utiliser des adresses MAC virtuelles dupliquées via RSRB afin d'offrir une redondance totale et un équilibrage de charge.

Figure 7.15
Redondance totale.



Voici les commandes de configuration du routeur NNC :

```
source-bridge ring-group 200
!
interface TokenRing0
  ring-speed 16
  source 100 1 200
!
appn control-point NETA.NNC
  complete
!
appn port RSRB rsrb
  rsrb-virtual-station 4000.1000.2000 50 2 200
  complete
```

Voici les commandes de configuration du routeur NND :

```
source-bridge ring-group 300
!
interface TokenRing0
  ring-speed 16
  source 100 5 300
!
appn control-point NETA.NND
  complete
!
appn port RSRB rsrb
  rsrb-virtual-station 4000.1000.2000 60 3 300
  complete
```

Les deux nœuds NNC et NND définissent un port RSRB avec la même adresse virtuelle MAC. Chaque station définira l'adresse MAC virtuelle RSRB comme adresse MAC de destination pour le serveur nœud de réseau. Une station peut donc en pratique utiliser NNC ou NND comme serveur

nœud de réseau, selon le nœud qui répondra en premier au paquet d'exploration. La route vers NNC comprend les informations suivantes :

Ring 100 -> Bridge 1 -> Ring 200 -> Bridge 2 -> Ring 50

L'itinéraire vers NND se compose des informations de routage suivantes :

Ring 100 -> Bridge 5 -> Ring 300 -> Bridge 3 -> Ring 60

Lorsque NND tombe en panne, les sessions auxquelles il participe peuvent être rétablies instantanément sur NNC. Ce processus est analogue au support du coupleur d'interface Token Ring (TIC, *Token Ring Interface Coupler*) dupliqué sur le FEP, excepté qu'aucun équipement matériel n'est requis. Dans l'implémentation RSRB de Cisco (voir Figure 7.15), le segment 20 et le pont 1 ainsi que le segment 30 et le pont 2 sont virtuels. L'adressage MAC dupliqué peut être supporté sans recourir au matériel en place.

Prise en charge SSCP

La troisième technique de communication de secours implique l'utilisation de la fonction DLUR d'APPN avec un routeur CIP Cisco, afin de supporter le transfert de propriété de ressources d'un point de contrôle SSCP (*System Services Control Point*) (VTAM) vers un autre en cas de rupture de liaison. Le processus comprend le maintien des sessions existantes durant la panne. La fonction DLUS/DLUR peut assurer le transfert de propriété du SSCP principal vers le SSCP de secours. Elle examine ensuite les possibilités du DLUR d'obtenir les services du SSCP de secours sans mettre fin aux sessions LU-LU en cours.

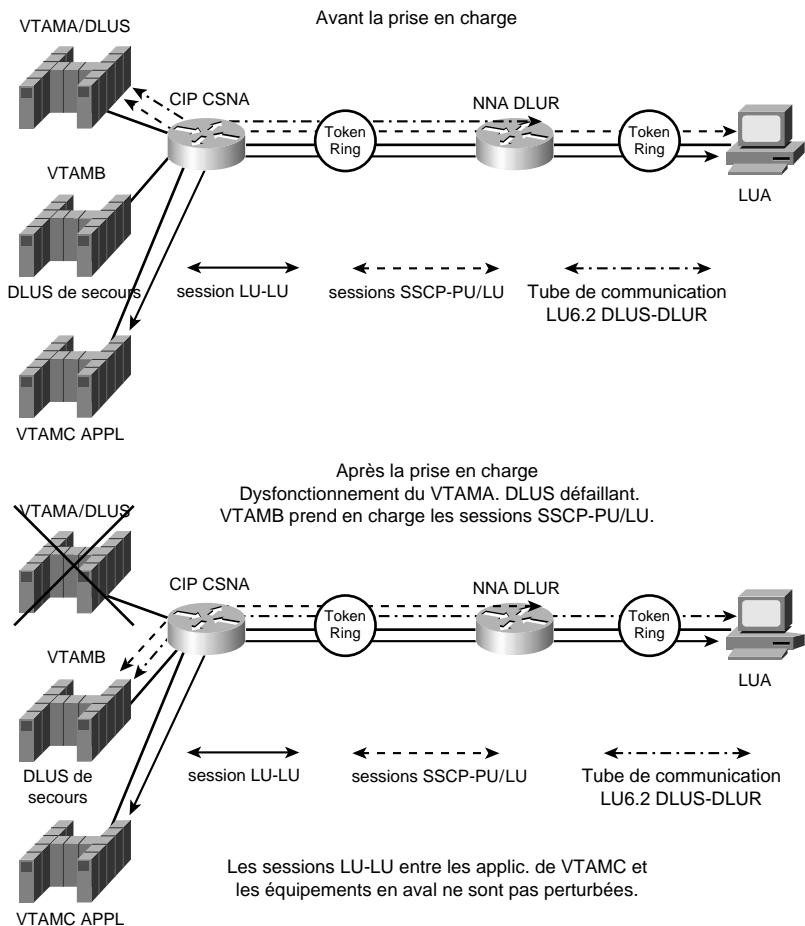
La Figure 7.16 illustre de quelle façon le FEP peut être remplacé par un routeur CIP exécutant CIP SNA (CSNA).

Dans cet exemple, VTAMA est le DLUS principal, VTAMB le DLUS de secours et NNA est configuré comme DLUR. Supposez que LUA demande à se connecter à une application située sur VTAMB. Si VTAMA ainsi que la connexion de DLUS vers DLUR présentent un dysfonctionnement, le nœud DLUR tente d'établir une session avec VTAMC qui est configuré en tant que DLUS de secours. Lorsque les sessions de contrôle vers le DLUS de secours sont actives, le nœud DLUR demande à VTAMB d'activer les unités physiques et logiques en aval en envoyant les requêtes REQACTPU et REQACTLU. VTAMB envoie vers ces unités des commandes d'activation d'unité physique (ACTPU) et d'unité logique (ACTLU). Cela permet de transférer la propriété de ressources de VTAMA vers VTAMB.

Après rétablissement des sessions SSCP-PU et SSCP-LU avec VTAMB, de nouvelles sessions LU-LU sont possibles. De plus, le nœud DLUR notifie à VTAMB toutes les unités logiques dépendantes qui possèdent une session active.

Le chemin LU-LU entre VTAMC et LUA serait VTAMB -> NNB -> NNA -> LUA. Lorsque VTAMA est inaccessible, les sessions LU-LU ne sont pas interrompues, car VTAMA ne fait pas partie du chemin de session LU-LU. En fait, LUA ne sait pas que le SSCP propriétaire (VTAMA) est défaillant et qu'un autre SSCP est devenu le nouveau propriétaire. Ce processus est transparent pour LUA.

Figure 7.16
Prise en charge SSCP avec APPN et CIP.



APPN dans un environnement multiprotocole

La tendance dans la conception de réseaux est de pouvoir fournir aux concepteurs une plus grande souplesse dans l'élaboration d'environnements supportant plusieurs protocoles. Cisco fournit les deux mécanismes suivants pour transporter le trafic SNA sur un réseau :

- l'encapsulation ;
- le transport natif via APPN.

La clé de la conception de réseaux multiprotocoles réside dans l'implémentation d'un mécanisme de gestion de priorité de trafic ou de réservation de bande passante, dans le dessein de garantir des temps de réponse acceptables pour le trafic de données critiques tout en conservant certaines ressources de réseau pour le trafic moins sensible aux délais de livraison.

Gestion de bande passante et de file d'attente

Voici quelques fonctions Cisco de gestion de bande passante et de file d'attente qui peuvent améliorer les performances globales du réseau :

- gestion de file d'attente de priorité ;
- gestion de file d'attente personnalisée ;
- gestion de file d'attente équitable pondérée ;
- gestion de tampon et de mémoire APPN.

Pendant de nombreuses années, le mainframe a été le support dominant des applications cruciales en entreprise. L'accroissement constant de la puissance des stations de travail, la création d'environnements informatiques client/serveur et l'émergence d'applications très exigeantes en bande passante sont des facteurs qui ont changé les topologies de réseaux. Avec la prolifération d'applications client/serveur au niveau réseau local, de nombreux réseaux d'entreprise ont amorcé une migration de leurs réseaux hiérarchiques purement SNA vers des réseaux multiprotocoles répondant aux exigences de communication en perpétuel changement. Il ne s'agit pas là d'une transition facile. Les concepteurs doivent comprendre l'adéquation selon laquelle les divers protocoles utilisent les ressources de réseau partagées sans provoquer de conflits excessifs entre eux.

Cisco a fourni pendant de nombreuses années des technologies permettant d'encapsuler le trafic SNA et de consolider l'architecture SNA avec des réseaux multiprotocoles. APPN sur le routeur Cisco introduit une option supplémentaire sur les réseaux multiprotocoles permettant au trafic SNA de circuler nativement en même temps que d'autres protocoles. En dépit de la technologie utilisée dans un environnement multiprotocole, les performances représentent le point essentiel.

Voici quelques-uns des principaux facteurs qui affectent les performances du réseau dans un environnement multiprotocole :

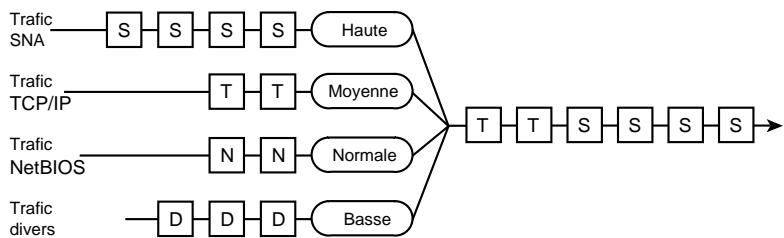
- **Vitesse d'accès au média.** Il s'agit du temps nécessaire à une trame pour être transmise sur une liaison. Les exigences doivent être bien cernées en ce qui concerne la capacité du réseau. Cette caractéristique est primordiale et une insuffisance de capacité serait une des principales causes de dégradation des performances. Que vous disposiez d'un réseau supportant un seul protocole ou d'un réseau multiprotocole, il est primordial que la quantité de bande passante soit suffisante.
- **Contrôle de congestion.** Le routeur doit posséder un tampon de capacité suffisante pour pouvoir gérer les rafales instantanées de données. Pour supporter un environnement multiprotocole, la gestion du tampon est un facteur important, car elle doit pouvoir garantir qu'un seul protocole ne monopolise pas toute la mémoire tampon.
- **Temps de latence sur les routeurs intermédiaires.** Ce temps inclut celui le traitement des paquets lorsqu'ils traversent un routeur et le délai de stationnement en file d'attente. Le temps de traitement ne représente qu'une faible partie du temps total tandis que le délai d'attente représente la part la plus importante, car le trafic client/serveur est généré en rafales.

Généralement, le trafic SNA de sous-zone est hautement prévisible et peu exigeant en bande passante. Comparé à ce trafic, celui des applications client/serveur a tendance à être émis en rafales et requiert davantage de bande passante. A moins de disposer d'un mécanisme protégeant le trafic SNA provenant d'applications cruciales, les performances du réseau peuvent en être affectées.

Cisco fournit aux entreprises de nombreuses solutions de connexion de réseaux en permettant à ces deux types de trafic, de caractéristiques différentes, de coexister et de partager une même bande passante, tout en assurant une protection des données SNA critiques par rapport aux données client/serveur qui sont moins sensibles aux délais de livraison. Cette gestion est réalisée par l'intermédiaire de mécanismes de mise en file d'attente de priorité ou de réservation de bande passante.

La mise en file d'attente de priorité de sortie d'interface fournit une méthode permettant de gérer la priorité des paquets transmis par rapport aux interfaces. Les quatre files d'attente possibles associées à cette gestion sont : haute priorité, priorité moyenne, priorité normale et basse priorité, comme illustré Figure 7.17. Les niveaux de priorité peuvent être accordés selon le type de protocole, l'interface, l'adresse SDLC, etc.

Figure 7.17
Les quatre files d'attente de la fonction de gestion de priorité.

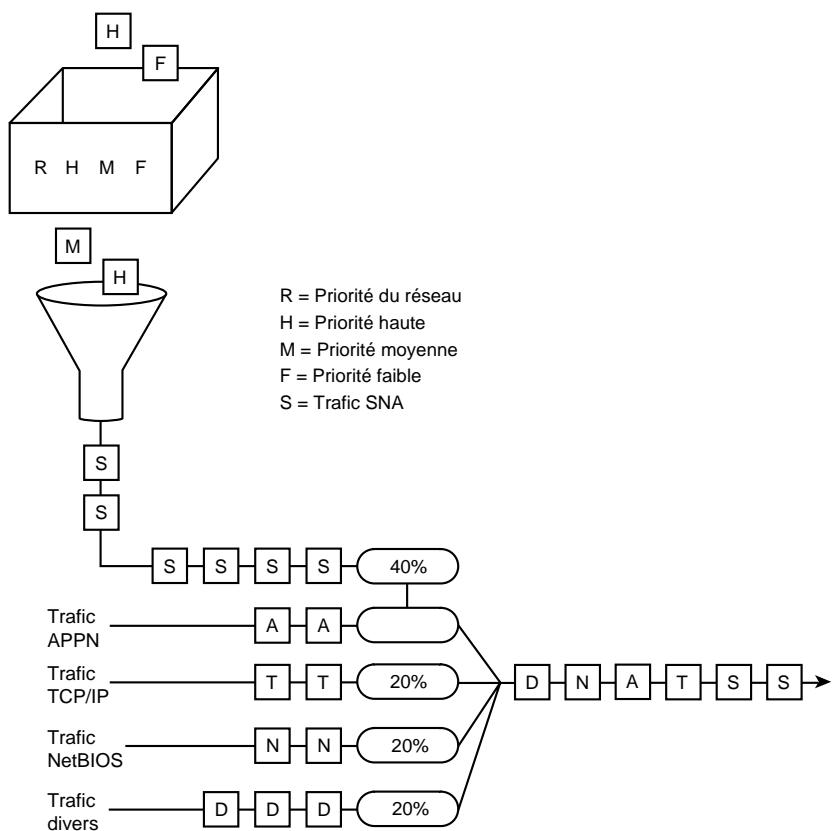


A la Figure 7.18, le trafic SNA, TCP/IP, NetBIOS et d'autres données diverses se partagent le média. Le trafic SNA est prioritaire sur tous les autres trafics, suivi par celui de TCP/IP, de NetBIOS et finalement celui de divers autres protocoles. Il n'existe aucun algorithme de calcul d'ancienneté des données associé à ce type de gestion de file d'attente. Les paquets placés dans la file d'attente de haute priorité sont toujours traités avant ceux de la file de moyenne priorité, qui sont eux-mêmes servis avant ceux de la file de priorité normale, etc.

La gestion de priorité introduit néanmoins un problème d'équité en ce sens que les paquets classés dans les files d'attente de faible priorité peuvent ne pas être servis à temps, ou ne pas être traités du tout. La gestion de file d'attente personnalisée a été prévue pour pallier ce problème, car elle offre une meilleure granularité. En fait, elle est couramment utilisée dans les environnements de réseaux supportant plusieurs protocoles de couches supérieures. Cette gestion de file d'attente peut réservé de la bande passante pour un protocole spécifique, ce qui permet de garantir à un trafic transportant des données critiques une quantité minimale de bande passante à n'importe quel moment.

Le but est de réserver de la bande passante pour des types de trafic particuliers. Par exemple, à la Figure 7.18, SNA dispose de 40 % de la bande passante, TCP/IP de 20 %, NetBIOS de 20 % et l'ensemble des protocoles restants de 20 %. Le protocole APPN intègre un concept de classe de service (CoS, *Class of Service*) pour déterminer le degré de priorité de chaque message. Il en définit la priorité avant de l'envoyer sur la file d'attente de transmission DLC.

Figure 7.18
Exemple de file d'attente personnalisée.



La mise en file d'attente personnalisée permet de définir la priorité d'un trafic multiprotocole et autorise un maximum de 16 files d'attente. Chaque file est servie de façon séquentielle jusqu'à ce que le nombre d'octets envoyés dépasse le compte d'octets configurable ou que la file soit vide. Un aspect important de cette fonctionnalité est la réallocation de la bande passante restante en cas de non-utilisation. Par exemple, si SNA n'exploite que 20 % de la quantité qui lui a été octroyée, les autres protocoles peuvent alors se partager les 20 % restants.

Cette fonctionnalité est prévue pour des environnements dans lesquels un niveau de service minimal doit être assuré pour chaque protocole. Dans les environnements multiprotocoles actuels, elle permet à des protocoles possédant des caractéristiques différentes de partager le même média. Pour une présentation d'autres types de gestion de files d'attente permettant à plusieurs protocoles de cohabiter sur un même routeur, revoyez le Chapitre 2.

Autres considérations relatives aux environnements multiprotocoles

Les exigences en mémoire pour le support d'APPN sont nettement plus élevées que pour celui des autres protocoles en raison de ses grandes tables de classes de service, de ses bases de données de topologie et de ses bases de données d'annuaire. Pour assurer une bonne cohabitation d'APPN avec d'autres protocoles dans un environnement multiprotocole, les utilisateurs peuvent définir la quantité maximale de mémoire mise à disposition d'APPN. Voici un exemple de commande de configuration :

```
appn control-point CISCONET.EARTH  
maximum-memory 16  
complete
```

La commande précédente spécifie qu'APPN n'utilisera pas plus de 16 Mo de mémoire. La mémoire est ensuite gérée localement par le protocole. Vous pouvez également spécifier la quantité de mémoire qui lui sera réservée en utilisant la commande suivante :

```
appn control-point CISCONET.EARTH  
minimum-memory 32  
complete
```

La mémoire qui est dédiée à APPN n'est pas disponible pour d'autres traitements. Utilisez donc cette commande avec prudence.

Bien que la mémoire détermine des facteurs comme le nombre de sessions pouvant être supportées par APPN, la mémoire tampon est nécessaire pour réguler le trafic échangé avec le routeur. Pour garantir qu'APPN dispose de suffisamment de mémoire tampon pour pouvoir supporter les flots de trafic, vous pouvez définir le pourcentage qui lui sera réservé. Cela l'empêchera de monopoliser la mémoire tampon disponible sur le routeur.

Voici un exemple de commande de configuration :

```
appn control-point CISCONET.EARTH  
buffer-percent 60  
complete
```

Le protocole APPN emploie un algorithme de gestion par statistiques pour contrôler l'utilisation du tampon. Lorsque la mémoire tampon est limitée, il utilise divers mécanismes de contrôle de flux pour se protéger de situations sévères de congestion ou de blocage (deadlock) qui pourraient être provoquées par un espace tampon insuffisant.

Gestion de réseau

A mesure que les réseaux augmentent en taille et en complexité, de nombreuses méthodes apparaissent pour permettre aux entreprises de gérer leur réseau. Le Tableau 7.2 résume les produits de gestion de réseau proposés par Cisco.

Tableau 7.2 : Outils de gestion de réseau disponibles pour des réseaux APPN

<i>Application</i>	<i>Description</i>
Commandes d'affichage	Sur les réseaux APPN, la compréhension de la topologie et de l'état des ressources du réseau relève du défi. Les commandes d'affichage tirent profit du fait que tous les nœuds de réseau ou de sous-réseau disposent d'une base de données complète de la topologie du réseau. Un seul nœud de réseau suffit à obtenir une vue du sous-réseau APPN ; peu importe le nœud choisi. Afin d'obtenir des informations plus détaillées, par exemple sur les nœuds d'extrémité (EN), les nœuds de niveau inférieur (LEN), les ports locaux ou les stations connectées, d'autres nœuds de réseau doivent être interrogés. Le routeur Cisco supporte RFC1593, APPN, MIB, qui sont utilisés par le routeur IBM 6611. Aussi peut-il être utilisé comme agent pour les applications APPN SNMP. La plupart des nœuds APPN peuvent afficher une grande partie de ces informations sous forme tabulaire. Sur le routeur Cisco, la commande show appn topo affiche la base donnée de topologie sous forme d'un tableau. La commande show appn? répertorie toutes les options disponibles.
Cisco Works Blue Maps	Une application Cisco Works, qui affiche les cartes logiques des réseaux APPN, RSRB et DLSw+. Elle s'exécute sur les systèmes d'exploitation HP/UX, SunOS et AIX. La carte APPN est un gestionnaire pour les agents APPN SNMP qui permet d'afficher un réseau APPN. L'application ne peut gérer qu'un seul agent de topologie de réseau. S'il existe plusieurs sous-réseaux, elle peut être démarrée plusieurs fois.
NSP (<i>Native Service Point</i>)	Sous SNA, une session entre un SSCP et une PU est appelée une session SSCP-PU. Les SSCP utilisent ces sessions pour envoyer des requêtes et recevoir des informations d'état de la part de nœuds individuels. Ces informations sont ensuite utilisées pour contrôler la configuration du réseau. Un point de service NSP sur le routeur peut être utilisé pour envoyer des alertes et répondre aux questions de NetView sur le mainframe. Un point de service permet à cette application d'établir une session vers un routeur à l'aide des applications Cisco qui s'exécutent sur NetView. Ces applications provoquent l'envoi des commandes vers le routeur, auxquelles celui-ci répond. Ce processus n'est actuellement supporté que sur une session SSCP-PU, mais la fonctionnalité DLUR peut être utilisée pour accomplir cela sur un réseau APPN.
Alertes et interceptions	NetView représente la destination principale des alertes. L'application peut recevoir des alertes de la part d'APPN ainsi que sur une session SSCP-PU utilisée par NSP. Le routeur Cisco peut émettre des alertes sur chaque session. A l'époque de la rédaction de cet ouvrage, deux sessions étaient requises : une pour les alertes APPN uniquement, et une seconde pour les autres alertes. La nouvelle MIB APPN permet aux alertes APPN d'être envoyées en tant qu'interceptions également, avec l'identifiant d'alerte et la ressource concernée inclus dans l'interception. Pour envoyer des alertes vers NetView, la commande suivante doit être entrée au niveau de NetView : FOCALPT CHANGE, FPCAT=ALERT, TARGET=NETA.ROUTER.

Exemples de configuration

Cette section fournit des exemples de configuration de réseau APPN :

- réseau APPN simple ;
- réseau APPN avec stations terminales ;
- APPN sur DLSw+.

Vous trouverez également des exemples de l'utilisation d'APPN lors de la conception d'un réseau :

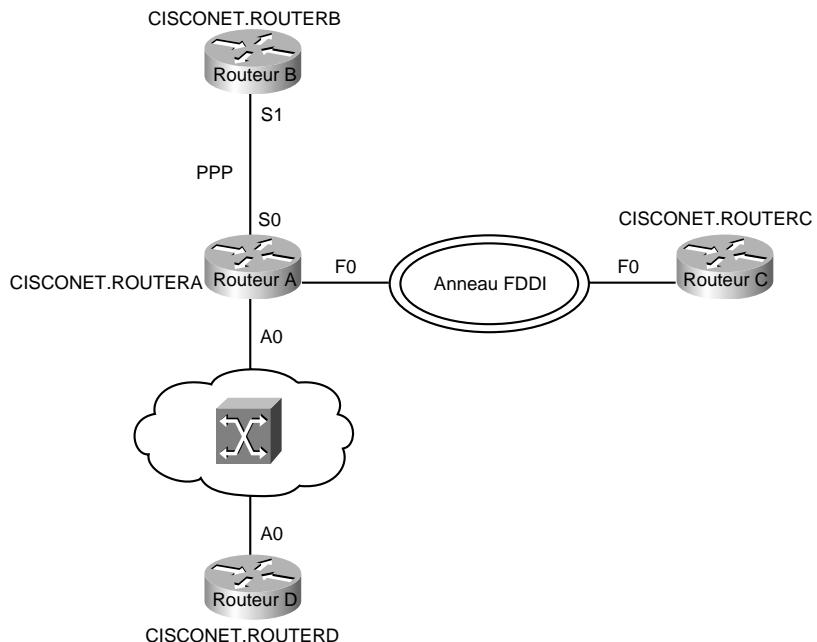
- migration de sous-zone vers APPN ;
- APPN/CIP dans un environnement Sysplex ;
- APPN avec FRAS BNN.

Comme le montrent les exemples suivants, la configuration minimale d'un nœud APPN inclut une instruction de point de contrôle APPN pour le nœud et une instruction de port pour chaque interface.

Configuration d'un réseau APPN simple

La Figure 7.19 illustre un exemple de réseau APPN simple qui se compose de quatre nœuds de réseau, les routeurs A, B, C et D. Le routeur A est responsable de l'initiation des connexions vers les routeurs B, C et D. En conséquence, il doit définir les liens logiques APPN en spécifiant l'adresse FDDI du routeur C, l'adresse ATM du routeur D, et ainsi de suite. En ce qui concerne les routeurs B, C et D, ils peuvent dynamiquement créer les définitions de stations de liaison lorsque le routeur A se connecte.

Figure 7.19
Exemple d'une configuration de réseau APPN simple.



Exemples de configuration

Cette section fournit des exemples de configuration pour chacun des quatre nœuds de réseau (routeurs A, B, C et D) illustrés Figure 7.19.

Configuration du routeur A

Dans cet exemple de configuration, notez que toutes les stations de liaison sont définies sur le routeur A (commande **appn link-station**) et découvertes dynamiquement par les autres routeurs. Une station de liaison connecte deux ressources et doit être définie avec l'adresse de destination sur l'une des ressources :

```
!
hostname routerA
!
interface Serial0
  ip address 10.11.1.1 255.255.255.0
  encapsulation ppp
  no keepalive
  no fair-queue
  clockrate 4000000
!
interface Fddi0
  no ip address
  no keepalive
!
interface ATM0
  no ip address
  atm clock INTERNAL
  atm pvc 1 1 32 aal5nlpid
!
appn control-point CISCONET.ROUTERA
  complete
!
appn port PPP Serial0
  complete
!
appn port FDDI Fddi0
  desired-max-send-btu-size 3849
  max-rcv-btu-size 3849
  complete
!
appn port ATM ATM0
  complete
!
appn link-station LINKTOB
  port PPP
  complete
!
appn link-station LINKTOC
  port FDDI
  lan-dest-address 0000.6f85.a8a5
  no connect-at-startup
  retry-limit infinite 5
  complete
!
appn link-station LINKTOD
  port ATM
  atm-dest-address 1
```

```

no connect-at-startup
retry-limit infinite 5
complete
!
```

Configuration du routeur B

Voici un exemple de configuration pour le routeur B de la Figure 7.19 :

```

!
hostname routerb
!
interface Serial1
  ip address 10.11.1.2 255.255.255.0
  encapsulation ppp
  no keepalive
  no fair-queue
!
appn control-point CISCONET.ROUTERB
  complete
!
appn port PPP Serial1
  complete
!
appn routing
!
end
```

Configuration du routeur C

Voici un exemple de configuration pour le routeur C de la Figure 7.19 :

```

!
hostname routerc
!
interface Fddi0
  no ip address
  no keepalive
!
appn control-point CISCONET.ROUTERC
  complete
!
appn port FDDI Fddi0
  desired-max-send-btu-size 3849
  max-rcv-btu-size 3849
  complete
!
appn routing
!
end
```

Configuration du routeur D

Voici un exemple de configuration pour le routeur D de la Figure 7.19 :

```

!
hostname routerd
!
interface ATM0
  ip address 100.39.15.3 255.255.255.0
  atm pvc 1 1 32 aal5nlpid
```

```

!
appn control-point CISCONET.ROUTERD
  complete
!
appn port ATM ATM0
  complete
!
appn routing
!
end

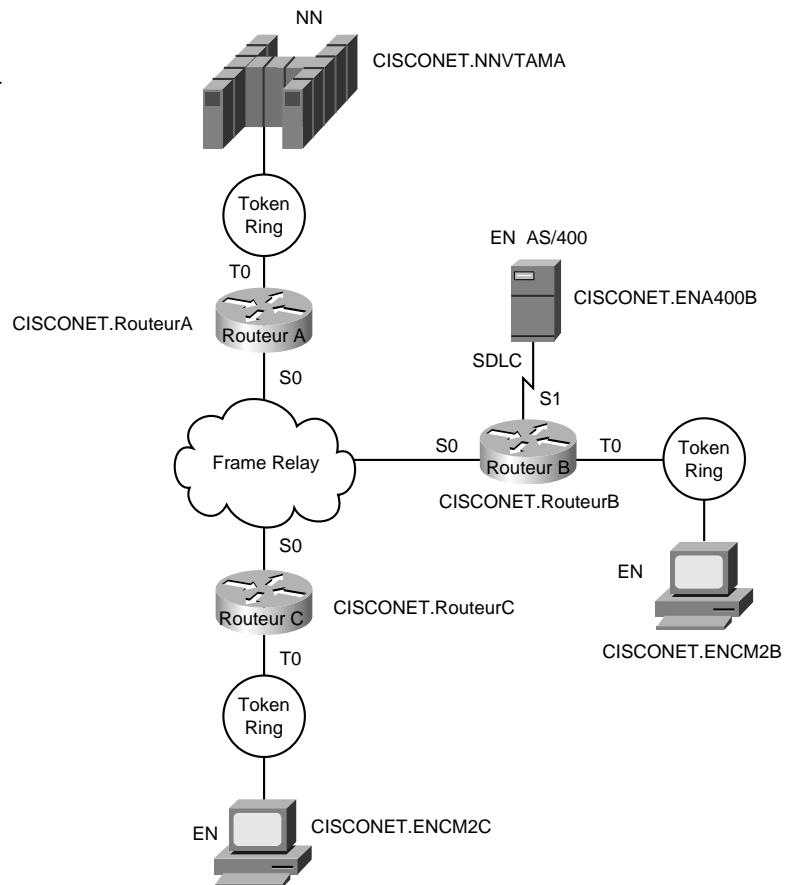
```

Configuration d'un réseau APPN avec des stations terminales

La Figure 7.20 illustre un exemple de réseau APPN comprenant des stations terminales. Sur le site distant, le routeur B initie la connexion APPN vers le routeur A sur le site du centre de données.

Figure 7.20

Exemple de réseau APPN avec des stations terminales.



Exemples de configuration

Cette section présente des exemples de configuration pour les routeurs A, B et C illustrés Figure 7.20.

Configuration du routeur A

Voici un exemple de configuration pour le routeur A de la Figure 7.20, qui est responsable de l'initiation de la connexion APPN vers l'hôte VTAM :

```
hostname routera
!
interface TokenRing0
  no ip address
  mac-address 4000.1000.1000
  ring-speed 16
!
interface Serial0
  mtu 4096
  encapsulation frame-relay IETF
  keepalive 12
  frame-relay lmi-type ansi
  frame-relay map llc2 35
!
appn control-point CISCONET.ROUTERA
  complete
!
appn port FR0 Serial0
  complete
!
appn port TR0 TokenRing0
  complete
!
appn link-station TOVTAM
  port TR0
  lan-dest-address 4000.3745.0000
  complete
!
end
```

Configuration du routeur B

Voici un exemple de configuration pour le routeur B illustré Figure 7.20. Sur le site distant, il initie la connexion APPN vers le routeur A sur le centre de données et le nœud d'extrémité EN AS/400. Comme aucune station de liaison n'est définie sur le routeur B pour CISCONET.ENCM2B, il faut en définir une pour le routeur B sur ENCM2B :

```
!hostname routerb
!
interface TokenRing0
  mac-address 4000.1000.2000
  no ip address
  ring-speed 16
!
interface Serial0
  mtu 4096
  encapsulation frame-relay IETF
  keepalive 12
  frame-relay lmi-type ansi
  frame-relay map llc2 35
```

```

!
interface Serial1
  no ip address
  encapsulation sdlc
  no keepalive
  clockrate 19200
  sdlc role prim-xid-poll
  sdlc address 01
!
appn control-point CISCONET.ROUTERB
  complete
!
appn port FR0 Serial0
  complete
!
appn port SDLC Serial1
  sdlc-sec-addr 1
  complete
!
appn port TR0 TokenRing0
  complete
!
appn link-station AS400
  port SDLC
  role primary
  sdlc-dest-address 1
  complete
!
appn link-station ROUTERA
  port FR0
  fr-dest-address 35
  complete
!
end

```

Configuration du routeur C

Voici un exemple de configuration pour le routeur C illustré Figure 7.20. Il initie une connexion APPN vers le routeur A. Comme il n'y a pas de station de liaison définie pour CISCONET.ENCNC2C, il faut en définir une pour le routeur C dans la configuration de ENCM2C :

```

hostname routerc
!
interface TokenRing0
  mac-address 4000.1000.3000
  no ip address
  ring-speed 16
!
interface Serial0
  mtu 4096
  encapsulation frame-relay IETF
  keepalive 12
  frame-relay lmi-type ansi
  frame-relay map llc2 36
!
appn control-point CISCONET.ROUTERC
  complete
!
appn port FR0 Serial0

```

```

        complete
!
appn port TR0 TokenRing0
    complete
!
appn link-station ROUTERA
    port FR0
    fr-dest-address 36
    complete
!
end

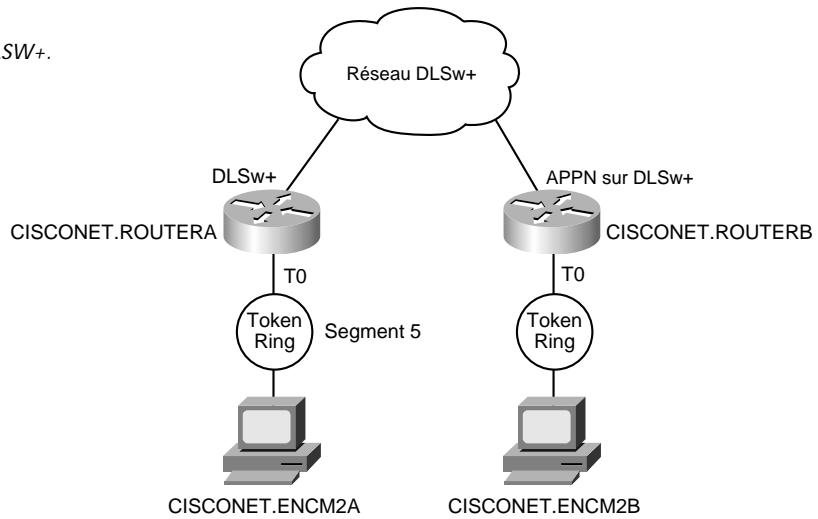
```

Configuration d'APPN sur DLSw+

La Figure 7.21 illustre un exemple de réseau utilisant APPN avec DLSw+. Le routeur A est un routeur DLSw+ sans fonction APPN alors que le routeur B exécute DLSw+ et APPN.

Figure 7.21

Exemple d'APPN avec DLSW+.



Exemple de configurations de DLSw+

La section suivante fournit des exemples de configuration pour les routeurs A et B et les deux stations de travail illustrées Figure 7.21.

Configuration DLSw+ du routeur A

Voici une configuration pour le routeur A illustré Figure 7.21 :

```

hostname routera
!
source-bridge ring-group 100
dlsw local-peer peer-id 10.4.21.3
dlsw remote-peer 0 tcp 10.4.21.1
!
interface Serial0

```

```

mtu 4096
ip address 10.4.21.3 255.255.255.0
encapsulation frame-relay IETF
keepalive 12
no fair-queue
frame-relay lmi-type ansi
frame-relay map llc2 56
!
interface TokenRing0
  ip address 10.4.22.2 255.255.255.0
  ring-speed 16
  multiring all
  source-bridge 5 1 100
!
```

Configuration pour la station de travail connectée au routeur A

Voici un exemple de configuration CS/2 pour la station de travail OS/2 nommée CISCO-NET.ENCM2A illustrée Figure 7.21. Cette station est connectée au routeur DLSw+ nommé routeur A. La station est configurée en tant que nœud d'extrémité et utilise le routeur B comme serveur nœud de réseau. L'adresse MAC de destination configurée sur cette station est l'adresse MAC virtuelle configurée sur le routeur B avec l'instruction **appn port**. Un exemple de configuration DLSw+ pour le routeur B est présenté à la prochaine section :

```

DEFINE_LOCAL_CP   FQ_CPN_NAME(CISCOENET.ENCM2A)
                  CP_ALIAS(ENCM2C)
                  NAU_ADDRESS(INDEPENDENT_LU)
                  NODE_TYPE(EN)
                  NODE_ID(X'05D00000')
                  NW_FP_SUPPORT(NONE)
                  HOST_FP_SUPPORT(YES)
                  MAX_COMP_LEVEL(NONE)
                  MAX_COMP_TOKENS(0);
DEFINE_LOGICAL_LINK  LINK_NAME(TORTRB)
                     ADJACENT_NODE_TYPE(LEARN)
                     PREFERRED_NN_SERVER(YES)
                     DLC_NAME(IBMTRNET)
                     ADAPTER_NUMBER(0)
                     DESTINATION_ADDRESS(X'400010001112')
                     ETHERNET_FORMAT(NO)
                     CP_CP_SESSION_SUPPORT(YES)
                     SOLICIT_SSCP_SESSION(YES)
                     NODE_ID(X'05D00000')
                     ACTIVATE_AT_STARTUP(YES)
                     USE_PUNAME_AS_CPNNAME(NO)
                     LIMITED_RESOURCE(NO)
                     LINK_STATION_ROLE(USE_ADAPTER_DEFINITION)
                     MAX_ACTIVATION_ATTEMPTS(USE_ADAPTER_DEFINITION)
                     EFFECTIVE_CAPACITY(USE_ADAPTER_DEFINITION)
                     COST_PER_CONNECT_TIME(USE_ADAPTER_DEFINITION)
                     COST_PER_BYTE(USE_ADAPTER_DEFINITION)
                     SECURITY(USE_ADAPTER_DEFINITION)
                     PROPAGATION_DELAY(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_1(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_2(USE_ADAPTER_DEFINITION)
                     USER_DEFINED_3(USE_ADAPTER_DEFINITION);
DEFINE_DEFAULTS   IMPLICIT_INBOUND_PLU_SUPPORT(YES)
                  DEFAULT_MODE_NAME(BLANK)
```

```

MAX_MC_LL_SEND_SIZE(32767)
DIRECTORY_FOR_INBOUND_ATTACHES(*)
DEFAULT_TP_OPERATION(NONQUEUED_AM_STARTED)
DEFAULT_TP_PROGRAM_TYPE(BACKGROUND)
DEFAULT_TP_CONV_SECURITY_RQD(NO)
MAX_HELD_ALERTS(10);
START_ATTACH_MANAGER;

```

Configuration DLSw+ du routeur B

Le routeur B illustré Figure 7.21 est un routeur APPN qui utilise la fonctionnalité APPN sur DLSw+. L'opérande VDLC de l'instruction de port indique qu'APPN est transporté au-dessus de DLSw+. Voici un exemple de configuration pour ce routeur :

```

hostname routerb
!
source-bridge ring-group 100
dlsw local-peer peer-id 10.4.21.1
dlsw remote-peer 0 tcp 10.4.21.3
!
interface Serial2/0
mtu 4096
ip address 10.4.21.1 255.255.255.0
encapsulation frame-relay IETF
keepalive 12
no fair-queue
frame-relay map llc2 35
!
interface TokenRing0
no ip address
ring-speed 16
mac-address 4000.5000.6000
source-bridge 10 1 100
!
appn control-point CISCONET.ROUTERB
complete
!
appn_port VDLC vdlc
vdlc 100 vmac 4000.1000.1112
complete
!
appn_port tr0 TokenRing 0
complete

```

Configuration pour la station de travail connectée au routeur B

Voici un exemple de configuration CS/2 pour la station de travail OS/2 nommée CISCONET.ENCM2B illustrée Figure 7.21. Cette station est connectée au routeur DLSw+ nommé routeur B.

```

DEFINE_LOCAL_CP FQ_C_P_NAME(CISCONET.ENCM2B)
CP_ALIAS(ENCM2C)
NAU_ADDRESS(INDEPENDENT_LU)
NODE_TYPE(EN)
NODE_ID(X'05D00000')
NW_FP_SUPPORT(NONE)
HOST_FP_SUPPORT(YES)
MAX_COMP_LEVEL(NONE)
MAX_COMP_TOKENS(0);

```

```

DEFINE_LOGICAL_LINK  LINK_NAME(TORTRB)
ADJACENT_NODE_TYPE(LEARN)
PREFERRED_NN_SERVER(YES)
DLC_NAME(IBMTRNET)
ADAPTER_NUMBER(0)
DESTINATION_ADDRESS(X'400050006000')
ETHERNET_FORMAT(NO)
CP_CP_SESSION_SUPPORT(YES)
SOLICIT_SSCP_SESSION(YES)
NODE_ID(X'05D00000')
ACTIVATE_AT_STARTUP(YES)
USE_PUNAME_AS_CPNAMES(NO)
LIMITED_RESOURCE(NO)
LINK_STATION_ROLE(USE_ADAPTER_DEFINITION)
MAX_ACTIVATION_ATTEMPTS(USE_ADAPTER_DEFINITION)
EFFECTIVE_CAPACITY(USE_ADAPTER_DEFINITION)
COST_PER_CONNECT_TIME(USE_ADAPTER_DEFINITION)
COST_PER_BYTE(USE_ADAPTER_DEFINITION)
SECURITY(USE_ADAPTER_DEFINITION)
PROPAGATION_DELAY(USE_ADAPTER_DEFINITION)
USER_DEFINED_1(USE_ADAPTER_DEFINITION)
USER_DEFINED_2(USE_ADAPTER_DEFINITION)
USER_DEFINED_3(USE_ADAPTER_DEFINITION);
DEFINE_DEFAULTS  IMPLICIT_INBOUND_PLU_SUPPORT(YES)
DEFAULT_MODE_NAME(BLANK)
MAX_MC_LL_SEND_SIZE(32767)
DIRECTORY_FOR_INBOUND_ATTACHES(*)
DEFAULT_TP_OPERATION(NONQUEUED_AM_STARTED)
DEFAULT_TP_PROGRAM_TYPE(BACKGROUND)
DEFAULT_TP_CONV_SECURITY_RQD(NO)
MAX_HELD_ALERTS(10);
START_ATTACH_MANAGER;

```

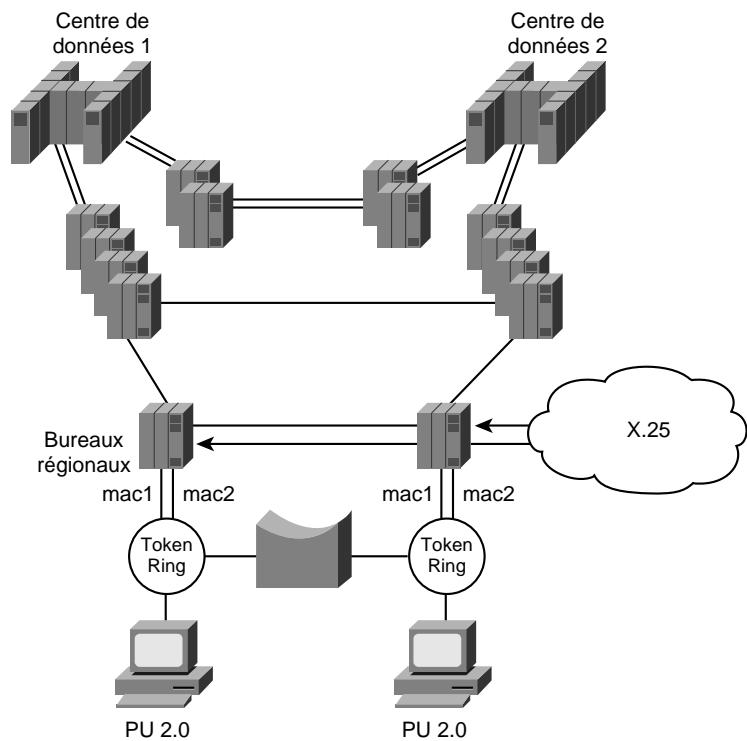
Pour plus d'informations sur DLSw+, voyez le Chapitre 8.

Migration d'une sous-zone vers APPN

Cette section présente l'implémentation et la conversion d'une sous-zone de réseau SNA basée sur un FEP en un réseau APPN reposant sur des routeurs. Elle explore l'utilisation de DLSw+ en tant que technologie de migration et présente les étapes à réaliser. Le scénario met en scène une grande compagnie d'assurance située en Europe. L'entreprise projette de remplacer les FEP par des routeurs Cisco et de migrer leur sous-zone vers un environnement de routage APPN.

La Figure 7.22 illustre le réseau SNA actuel de l'entreprise. Il se compose de deux sites avec mainframe exécutant quatre images VTAM avec un hôte CMC (*Communication Management Complex*) dans chaque centre de données, comme illustré Figure 7.22. Chaque centre de données possède aussi quatre FEP NCR Comten (compatibles IBM 3745) qui supportent le trafic provenant de plusieurs sites régionaux et deux FEP NCR Comten qui assurent la gestion de SNI (*SNA Network Interconnect*).

Figure 7.22
Réseau SNA basé sur
l'emploi de FEP.

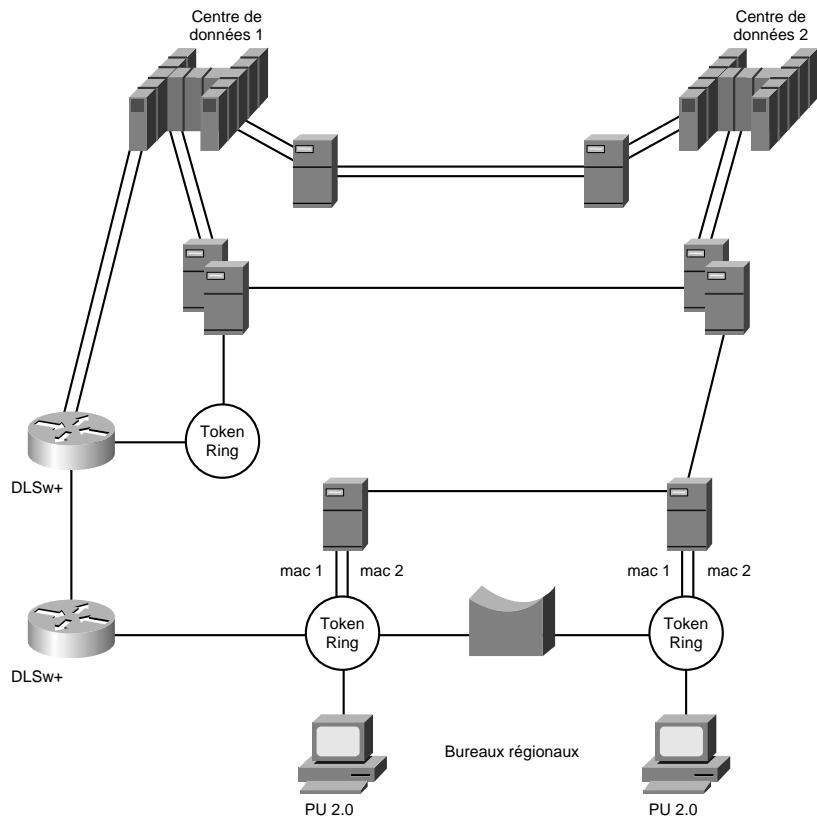


Il existe 22 bureaux régionaux à travers le pays. Chaque site régional possède deux FEP NCR Comten, l'un se connectant au centre de données 3 et l'autre au centre de données 2. Les FEP distants sont associés à des réseaux Token Ring doubles connectés par l'intermédiaire d'un pont ; le support d'adresse de coupleur TIC dupliquée est implémenté pour le secours et la redondance. Cela signifie qu'une station PU2.0 peut accéder à l'hôte par l'intermédiaire de n'importe lequel des deux FEP, au cas où l'un d'eux tomberait en panne.

Outre les dispositifs connectés au Token Ring (environ 15 par bureau régional), les deux FEP utilisent aussi NPSI (*NCP Packet-Switching Interface*) et supportent plus de 200 dispositifs connectés à distance via le réseau public X.25. Le nombre total de LU supportées par bureau régional est d'environ 1800, avec 1500 sessions LU-LU pouvant être actives à n'importe quel moment. Le débit du trafic est estimé à 15 transactions par seconde.

La première étape de migration consiste à implémenter un routeur CIP Cisco au niveau de l'un des centres de données, en remplaçant les FEP reliés par canaux. Un routeur Distant est ensuite installé sur l'un des sites régionaux. Les deux routeurs sont connectés au moyen de DLSw+, comme illustré Figure 7.23.

Figure 7.23
Migration de sous-zone vers APPN : phase 1.



Comme le montre la Figure 7.23, les FEP sur le site régional continuent à assurer les fonctions de liaison vers les dispositifs connectés au Token Ring et via X.25. Les deux routeurs DLSw+ gèrent le trafic entre le FEP du centre de données 1 et le FEP sur le site régional. La classe de service SNA est préservée dans cet environnement.

Après s'être assuré de la stabilité des routeurs, le concepteur du réseau passe à la phase suivante. Comme le montre la Figure 7.24, cette phase implique l'installation de deux autres routeurs, un sur le centre de données 2 et un autre sur le site régional. A ce point, les communications FEP-FEP entre sites régionaux et centres de données sont gérées par les routeurs via DLSw+.

En poursuivant le plan de migration, l'étape suivante du concepteur est d'installer un routeur CIP supplémentaire dans chaque centre de données pour gérer le trafic entre les deux centres. Comme illustré Figure 7.25, les liaisons qui connectent les FEP des centres de données 1 et 2 sont déplacées une par une vers les routeurs.

APPN sera activé pour supporter le trafic entre les centres de données 1 et 2. Finalement, le réseau basé sur FEP devient un réseau de routeurs. Les contrôleurs NCR Comten deviennent obsolètes. Deux d'entre eux seront conservés pour assurer le support de SNI pour les organisations externes. La Figure 7.26 illustre le nouveau réseau.

Figure 7.24
Migration de sous-zone
vers APPN : phase 2.

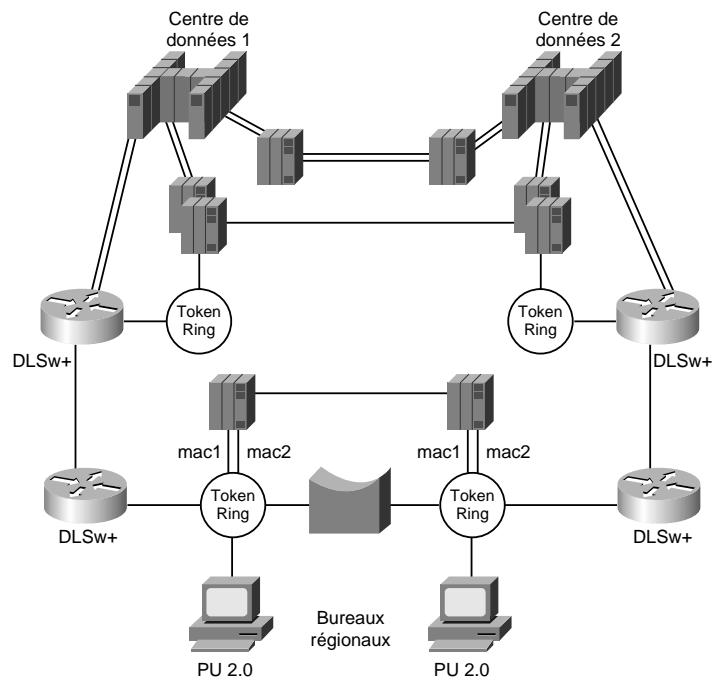


Figure 7.25
Migration de sous-zone
vers APPN : phase 3.

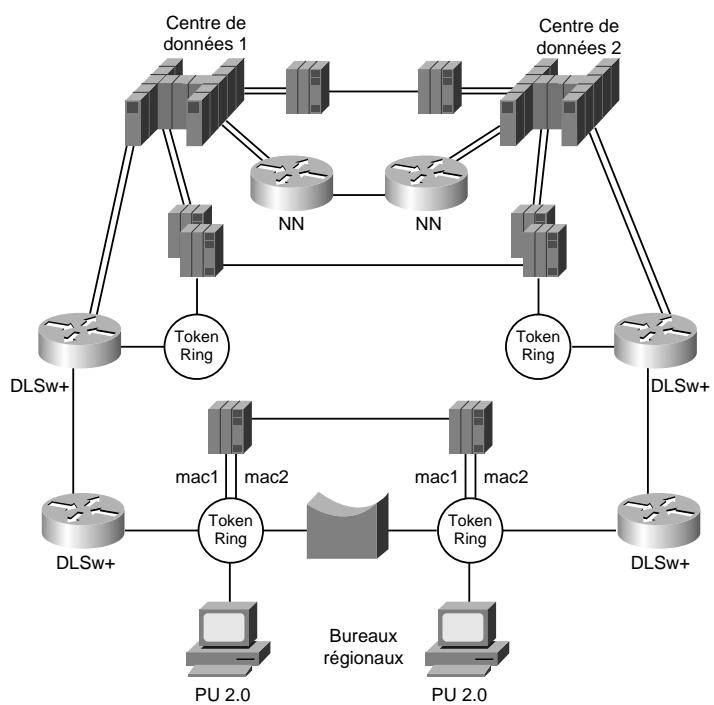
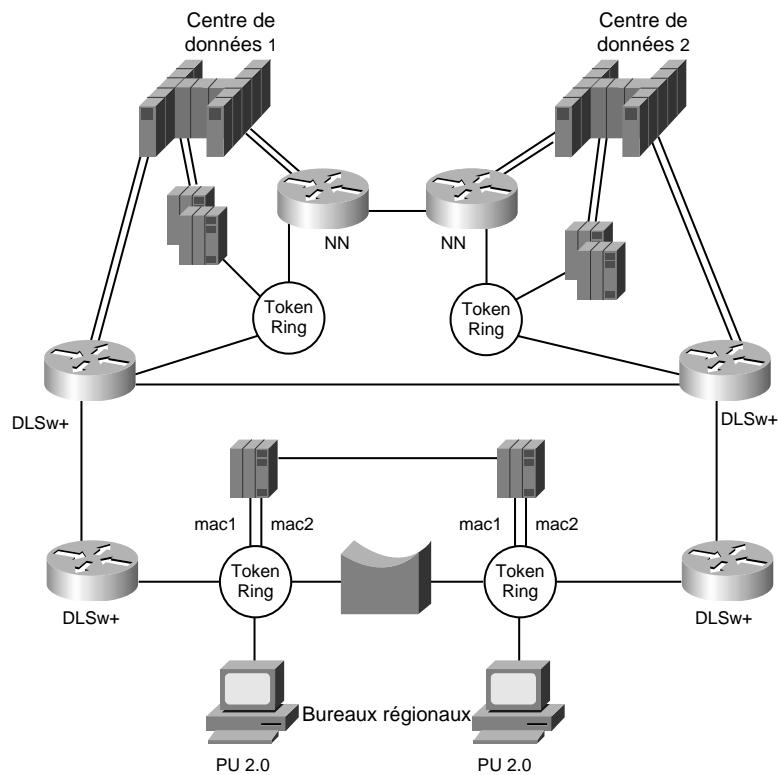


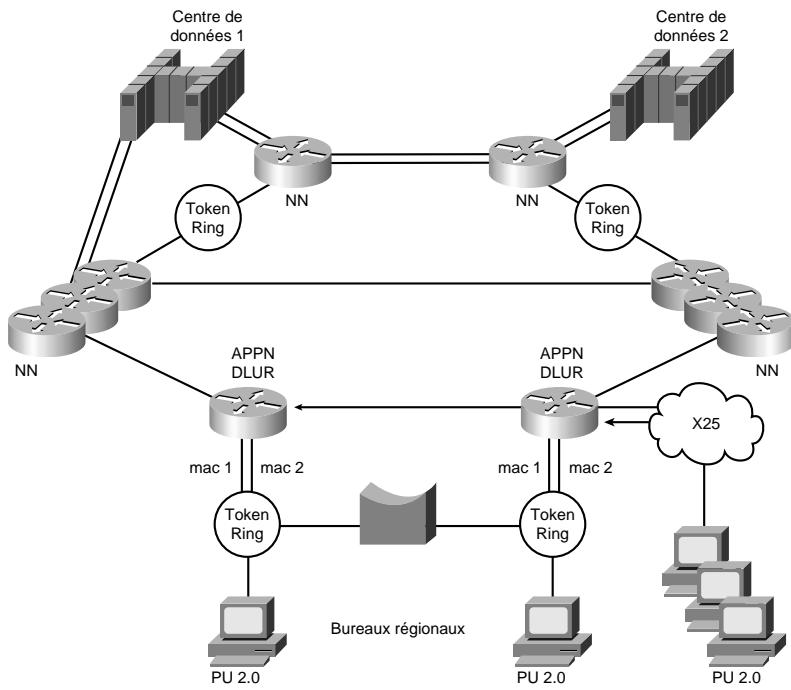
Figure 7.26
Migration de sous-zone vers APPN : phase 4.



Les liens de communication qui connectaient précédemment les FEP aux centres de données sont maintenant déplacés vers les routeurs. Les FEP des centres de données peuvent être éliminés. Ceux sur les sites régionaux jouent simplement le rôle de frontière pour les dispositifs LU dépendants, autorisant ainsi le maintien de la classe de service de SNA. La phase suivante consiste en la migration des fonctions de frontière SNA des FEP vers le routeur Distant sur le site régional en activant APPN et DLUR. Après cela, les FEP peuvent être éliminés.

L'étape suivante consiste en la migration de DLSw+ vers APPN entre les routeurs de centres de données et ceux des bureaux régionaux. Cette phase est réalisée région par région jusqu'à ce que la stabilité du réseau soit garantie. Comme l'illustre la Figure 7.27, le support DLUR est activé pour gérer les dispositifs PU dépendants sur les sites régionaux. Les dispositifs PU2.0 dépendants connectés via X.25 qui étaient précédemment connectés aux FEP par le biais de NPSI sont maintenant supportés via QLLC (*Qualified Logical Link Control*) sur le routeur. Il s'agit d'un standard pour l'encapsulation de SNA sur X.25.

Figure 7.27
Migration de sous-zone vers APPN : phase 5.



APPN/CIP dans un environnement Sysplex

Cette section étudie APPN et les routeurs CIP au sein d'un environnement Sysplex (*System Complex*). Elle présente cet environnement en relation avec APPN et décrit de quelle façon utiliser les trois approches suivantes pour implémenter l'environnement Sysplex :

- Sysplex avec APPN en utilisant le routage de sous-zone — option 1 ;
- Sysplex avec le routage sous-zone/APPN — option 2 ;
- Sysplex avec le routage APPN — option 3.

Cette section décrit également de quelle manière APPN peut offrir des fonctionnalités de tolérance aux pannes et d'équilibrage de charge au niveau des centres de données.

Présentation de l'environnement Sysplex

L'environnement Sysplex fournit un moyen d'exploiter et de gérer de façon centralisée un groupe de plusieurs systèmes de stockage virtuel (MVS, *Multiple Virtual Storage*) en couplant des éléments matériels et des services logiciels. De nombreuses entreprises équipent leurs centres de traitement de données de plusieurs de ces systèmes pour la gestion de leurs activités. Ces systèmes se partagent souvent des données et des applications. Sysplex a été conçu pour fournir une solution rentable, qui répond aux exigences d'expansion d'une entreprise en permettant aux systèmes MVS d'être ajoutés et gérés efficacement.

Un environnement Sysplex consiste en de nombreux processeurs CMOS 9672, chacun d'eux représentant un domaine VTAM. Le concept de multiprocesseur pose cependant un problème. Aujourd'hui, les utilisateurs sont habitués aux images uniques. Par exemple, le système IMS (*Information Management System*) qui s'exécute sur le mainframe peut servir la totalité de l'organisation au moyen d'une seule image hôte. Avec le concept de multiprocesseur, vous n'indiqueriez pas à un utilisateur d'établir une session avec IMS sur un système donné et à un autre utilisateur d'établir aussi une session avec IMS sur un autre système, car IMS pourrait être en cours d'exécution sur chaque système.

Pour résoudre cela, une fonction appelée *ressource générique* a été créée. Elle permet à plusieurs programmes qui fournissent la même fonction d'être connus et utilisés au moyen d'un seul nom générique. Cela signifie qu'un utilisateur peut parfois accéder à IMS à partir d'un système, et parfois à partir d'un autre. Comme ces deux systèmes ont accès aux mêmes données partagées dans le Sysplex, cette commutation entre systèmes est transparente pour les utilisateurs. VTAM est responsable de la résolution du nom générique et de l'identification du programme qui est utilisé pour établir la session. Cette fonction permet à VTAM d'assurer un équilibrage de charge en distribuant les initiations de sessions entrantes vers un certain nombre de programmes identiques exécutés sur différents processeurs.

La fonction de ressource générique ne s'exécute que sur un VTAM avec support APPN. Afin d'assurer l'équilibrage de charge de sessions sur différents processeurs, les utilisateurs doivent procéder à la migration de VTAM à partir d'une sous-zone SNA vers APPN. Le reste de cette section examine les trois options qui permettent de gérer un environnement Sysplex.

Sysplex avec APPN avec le routage de sous-zone — option 1

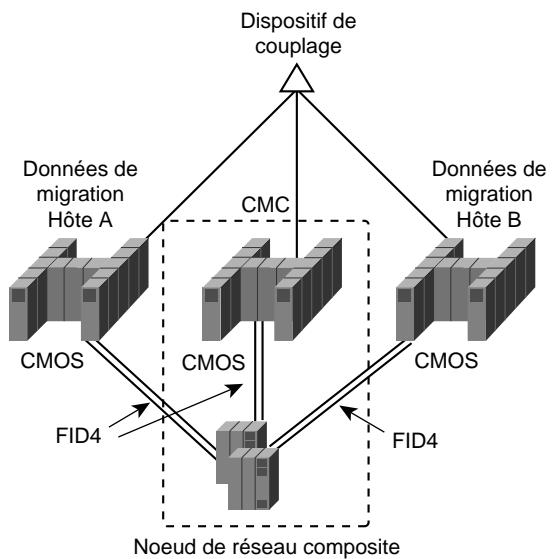
La première option permettant de supporter l'environnement Sysplex est de convertir l'hôte CMC en noeud de réseau composite (CNN, *Composite Network Node*). Traditionnellement, l'hôte CMC était représenté par le VTAM qui possédait toutes les ressources SNA du réseau. Avec cette approche, le noeud de réseau composite est utilisé pour décrire la combinaison de VTAM et de NCP (*Network Control Program*, programme de contrôle de réseau). Cela signifie que VTAM et NCP fonctionnent ensemble en tant que noeud de réseau unique. La Figure 7.28 illustre l'hôte CMC et les FEP configurés en tant que noeud de réseau composite.

L'hôte CMC VTAM possède les FEP. Chaque FEP est connecté aux processeurs CMOS 9672 par l'intermédiaire d'un canal parallèle. Chaque processeur CMOS 9672 est configuré en tant qu'hôte de données de migration et entretient les deux aspects, celui d'APPN et celui de sous-zone.

Chaque hôte de données de migration établit des connexions de sous-zone vers les FEP au moyen de la fonctionnalité de groupe de transmission de routes virtuelles, ou VRTG (*Virtual Route Transmission Group*), qui permet à APPN d'être transporté via un routage de sous-zone traditionnel. Les sessions CP-CP entre l'hôte CMC et les hôtes de données de migration 9672 sont établies au moyen de VRTG. La fonction de ressource générique est exécutée au niveau d'APPN, mais tout le routage est un routage de sous-zone. Il s'agit là de la façon la plus conservatrice de migrer vers un environnement Sysplex.

Figure 7.28

Nœud de réseau composite CMC avec routage de sous-zone — option 1.



L'inconvénient de cette approche est que l'emploi du routage de sous-zone ne fournit pas l'implémentation dynamique des changements de topologie sous APPN, qui est normalement disponible avec les connexions APPN. Si vous devez ajouter un processeur CMOS, des modifications de chemin de sous-zone (PATH) vers chaque nœud de sous-zone sont nécessaires. Un autre inconvénient de cette approche est que l'exécution d'APPN sur un routage de sous-zone introduit un certain niveau de complexité sur le réseau.

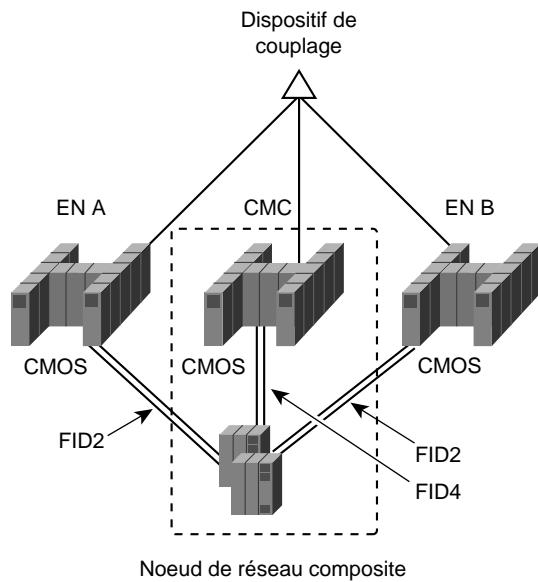
Sysplex avec le routage de sous-zone/APPN — option 2

La deuxième option permettant de supporter l'environnement Sysplex est d'utiliser le routage de sous-zone/APPN. Cette approche est similaire à l'option 1, décrite dans la section précédente. Avec cette seconde approche, l'hôte CMC et les FEP sont convertis en un nœud de réseau composite, comme illustré Figure 7.29.

Comme l'indique la figure, les deux processeurs CMOS 9672 sont convertis en nœuds d'extrémité purs (EN A et EN B). Les connexions APPN sont établies entre les processeurs 9672 et les FEP. Les sessions arrivent sur le CMC de façon habituelle et celui-ci procède à l'échange sous-zone/APPN. Cela signifie que des sessions sont converties du routage de sous-zone vers le routage APPN, sur les liaisons entre les FEP et les 9672.

Un inconvénient de cette deuxième approche est qu'elle entraîne des performances médiocres, car les FEP doivent réaliser une conversion supplémentaire. Elle requiert également davantage de cycles NCP et de mémoire. Bien qu'elle soit très facile à configurer et ne nécessite aucun changement au niveau du routage de sous-zone de base, le coût des mises à jour NCP peut être élevé.

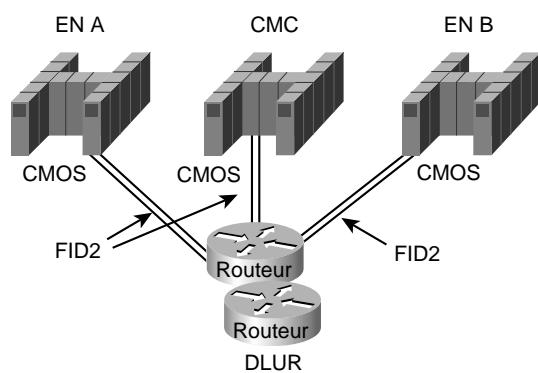
Figure 7.29
Nœud de réseau composite CMC avec routage APPN — option 2.



Sysplex avec le routage APPN — option 3

La troisième option permettant de supporter l'environnement Sysplex est d'utiliser le routage APPN. Vous devez utiliser un DLUR comme dispositif frontal vers les unités logiques du CMC. La Figure 7.30 illustre cette configuration.

Figure 7.30
Sysplex avec DLUR et l'emploi de CIP — option 3.



Comme le montre cette figure, il s'agit d'un réseau APPN pur avec routage APPN. Chaque processeur CMOS de nœud d'extrémité est relié aux routeurs du DLUR par l'intermédiaire d'APPN. Notez que ceux-ci pourraient être distants. Ils ne doivent pas obligatoirement se trouver à proximité des mainframes (il pourrait, par exemple, y avoir d'autres routeurs intermédiaires).

Cette approche sera choisie pour implémenter un environnement Sysplex dans notre exemple d'entreprise. La section suivante fournit davantage de détails sur cette implémentation.

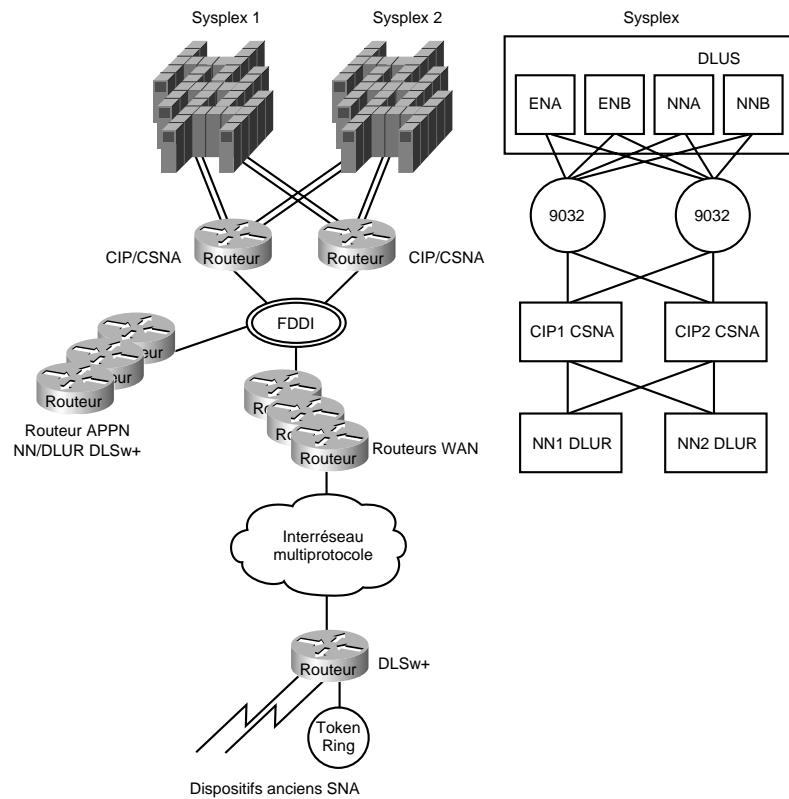
Réseau de l'entreprise

L'entreprise examinée dans cet exemple possède un très grand réseau fédérateur IP ainsi qu'un réseau SNA étendu. Aujourd'hui, les réseaux multiprotocoles et SNA sont séparés. L'objectif de l'entreprise est de consolider le trafic à travers l'interréseau multiprotocole. Elle a donc porté son choix sur le protocole IP pour son réseau fédérateur stratégique et sur une encapsulation DLSw+ pour transporter le trafic SNA.

Pour son centre de données, la société projette de gérer cinq environnements Sysplex IBM différents. Elle souhaite disposer du plus haut degré de redondance et de tolérance aux pannes. Les administrateurs ont donc décidé de ne pas exécuter APPN à travers le réseau multiprotocole existant, mais plutôt de l'implémenter au niveau du centre de données pour fournir le niveau de redondance requis.

La Figure 7.31 présente la configuration du centre de données de l'entreprise. Le diagramme figurant dans le coin supérieur droit représente une vue logique de l'environnement Sysplex et de la façon dont il est connecté au réseau multiprotocole par l'intermédiaire des routeurs CIP/CSNA et des routeurs APPN.

Figure 7.31
Exemple d'intégration
d'APPN dans le centre
de données.



Chaque routeur CIP/CSNA possède deux cartes pour les canaux parallèles vers chaque hôte Sysplex (Sysplex 1 et Sysplex 2) par l'intermédiaire de directeurs ESCON séparés. Pour satisfaire aux exigences très fortes de la société en matière de disponibilité, cette configuration ne présente aucun élément unique pouvant immobiliser l'ensemble du système (*Single Point of Failure*).

Dans chaque environnement Sysplex, au moins deux nœuds de réseau agissent comme DLUS. Le VTAM NNA est désigné comme nœud DLUS principal et NNB est désigné comme DLUS de secours. Les hôtes restants sont des hôtes de données configurés en tant que nœuds d'extrémité. Ils utilisent NNA comme serveur nœud de réseau.

Chaque environnement Sysplex est supporté par deux routeurs CIP et au moins deux routeurs APPN exécutant DLUR fournissent des fonctions de liaison de frontière pour servir les dispositifs distants. Il est prévu que le trafic soit équilibré entre les deux routeurs CIP. Par conséquent, APPN fournit l'équilibrage de charge et la redondance dans cet environnement.

Exemple de configuration

En ce qui concerne APPN, NNA à la Figure 7.31 peut être configuré comme serveur DLUS principal, et NNB comme DLUS de secours. Voici un exemple de configuration pour NN1, sachant que NN2 serait configuré de la même manière :

```
!
appn control-point CISCONET.NNA
  dlus CISCONET.NNA
  backup-dlus CISCONET.NNB
  dlur
  complete
```

Lorsque l'hôte DLUS principal est inaccessible, le nœud DLUR en est déconnecté. Le DLUR essaye à nouveau le tube DLUS/DLUR avec NNA. En cas d'échec, il se tourne vers le DLUS de secours.

Pour assurer l'équilibrage de charge, chaque routeur DLUR définit deux groupes de transmission APPN parallèles, de poids égal pour chaque hôte VTAM, en utilisant la configuration suivante :

```
!
! Lien vers VTAM ENA via routeur CIP 1
!
appn link-station LINK1ENA
  port FDDI0
  lan-dest-address 4000.3000.1001
  complete
!
! Lien vers VTAM ENA via routeur CIP 2
!
appn link-station LINK2ENA
  port FDDI0
  lan-dest-address 4000.3000.2001
  complete
!
! Lien vers VTAM ENB via routeur CIP 1
!
appn link-station LINK1ENB
  port FDDI0
  lan-dest-address 4000.3000.1002
  complete
```

```

!
! Lien vers VTAM ENB via routeur CIP 2
!
appn link-station LINK2ENB
  port FDDI0
  lan-dest-address 4000.3000.2002
  complete
!
! Lien vers NNA DLUS principal via routeur CIP 1
!
appn link-station LINK1NNA
  port FDDI0
  lan-dest-address 4000.3000.1003
  complete
!
! Lien vers NNA DLUS principal via routeur CIP 2
!
appn link-station LINK2NNA
  port FDDI0
  lan-dest-address 4000.3000.2003
  complete
!
! Lien vers NNB DLUS de secours via routeur CIP 1
!
appn link-station LINK1NNB
  port FDDI0
  lan-dest-address 4000.3000.1004
  complete
!
! Lien vers NNB DLUS de secours via routeur CIP 2
!
appn link-station LINK2NNB
  port FDDI0
  lan-dest-address 4000.3000.2004
  complete

```

Comme illustré dans la configuration précédente, NN1 définit deux groupes de transmission APPN vers ENA, ENB, NNA et NNB. Il existe deux liens par canal vers chaque hôte, chaque lien étant connecté à un dispositif matériel distinct (par exemple, une carte CIP, un routeur CIP, un directeur ESCON). La duplication du matériel s'explique en partie par la prévision d'un risque éventuel de perte d'un composant physique. Dans notre cas, si cela se produisait, l'hôte serait toujours accessible par l'autre chemin.

En ce qui concerne APPN, deux groupes de transmission connectent un routeur DLUR à chaque hôte. L'un des deux groupes traverse le routeur CIP 1, et l'autre traverse le routeur CIP 2. Lorsqu'un chemin est impraticable, le groupe concerné devient inopérant. Le second groupe fournit une autre route pour permettre la connexion vers l'hôte par l'intermédiaire de l'itinéraire de secours.

Toutes les sessions SSCP/PU et SSCP/LU de sous-zone circulent sur l'un des groupes de transmission entre le routeur DLUR et l'hôte DLUS principal. Comme pour les sessions LU-LU, les deux routes possibles entre le routeur DLUR et un hôte VTAM sont disponibles. Le routeur DLUR et un hôte VTAM sélectionnent de façon aléatoire l'une de ces deux routes pour les sessions LU-LU. Ce choix arbitraire provoque une certaine distribution de charge sur les deux routeurs CIP, bien qu'il ne s'agisse pas nécessairement d'un équilibrage statistique.

De nombreux routeurs DLUR supportent les dispositifs SNA en aval. Voici un exemple de configuration pour le routeur DLUR NN1 :

```
source-bridge ring-group 100
dlsw local-peer peer-id 172.18.3.111 promiscuous
!
interface FDDI0
  ip address 172.18.3.111 255.255.255.0
!
appn control-point CISCONET.NN1
dlus CISCONET.NNA
backup-dlus CISCONET.NNB
dlur
complete
!
appn port VDLC1 vdlc
  vdlc 100 4000.1000.2000
  complete
```

Voici un exemple de configuration pour le routeur DLUR NN2 :

```
source-bridge ring-group 200
dlsw local-peer peer-id 172.18.3.112 promiscuous
!
interface FDDI0
  ip address 172.18.3.112 255.255.255.0
!
appn control-point CISCONET.NN2
  complete
!
appn port VDLC2 vdlc
  vdlc 200 4000.1000.2000
  complete
```

Chaque station de travail accède à l'hôte par l'intermédiaire du routeur DLUR et doit définir 4000.1000.2000 comme adresse MAC de destination dans le logiciel d'émulation. Cette adresse virtuelle est définie pour atteindre chaque routeur DLUR. Lors de l'initiation d'une connexion, une station envoie en diffusion une trame TEST toutes routes vers l'adresse MAC à laquelle elle souhaite se connecter. Le routeur DLSw+ distant envoie une trame d'exploration à ses homologues, les nœuds NN1 et NN2, qui répondent par un message ICANREACH. Le routeur DLSw+ est configuré pour utiliser l'équilibrage de charge. Cela signifie qu'il place en cache NN1 et NN2 comme homologues pouvant atteindre l'hôte. Les sessions d'hôte sont établies en alternance via NN1 et NN2. Cela permet à l'entreprise de répartir le trafic SNA sur deux ou plusieurs routeurs DLUR. Si NN1 devient indisponible, les sessions qui le traversent sont interrompues, mais elles peuvent être rétablies par l'intermédiaire de NN2 avec un impact négligeable.

Cette conception améliore la disponibilité générale du système au moyen d'un adressage MAC virtuel dupliqué sur le routeur DLUR. Les chemins doubles donnent la possibilité d'emprunter un chemin secondaire lorsque le chemin principal est interrompu. Un autre avantage de cette conception est qu'elle peut facilement évoluer. Par exemple, lorsque le nombre de dispositifs SNA augmente, la mémoire tampon peut devenir un facteur limitant au niveau des routeurs DLUR. L'entreprise peut alors ajouter un routeur DLUR afin de supporter la charge des sessions supplémentaires. Cette modification de topologie n'implique aucune administration de réseau au niveau des routeurs distants ou du centre de données.

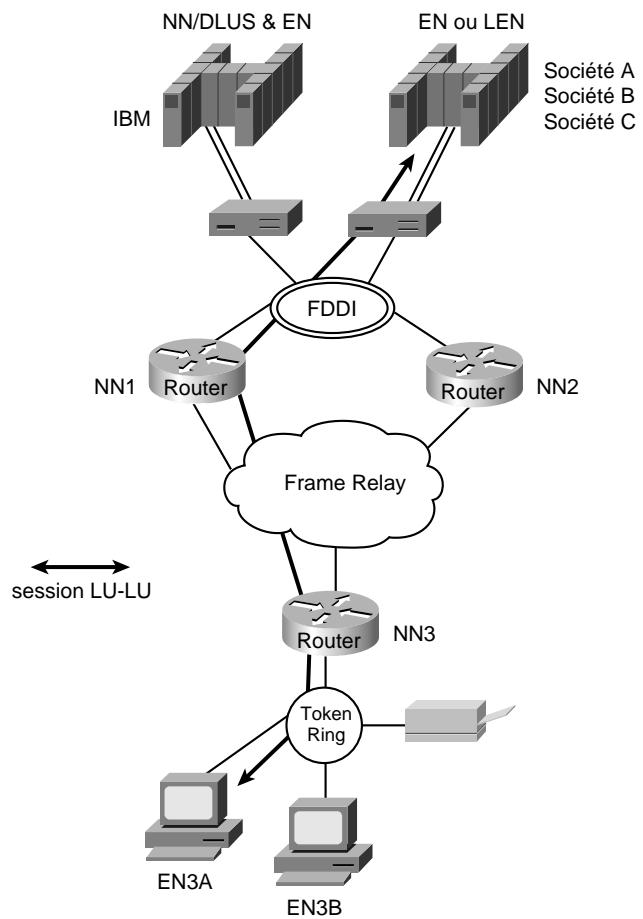
APPN avec FRAS BNN

Cette section décrit les éléments à prendre en compte lors de la conception d'un grand réseau APPN d'entreprise. Elle répertorie les techniques actuelles qui permettent sa réalisation. Chaque option y est traitée en détail. Le système FRAS BNN est choisi comme solution d'évolutivité provisoire pour réduire le nombre de nœuds de réseau, ce qui permet au réseau de s'adapter aux exigences d'expansion de la société.

Dans cet exemple, une agence gouvernementale possède un réseau avec un centre de données et environ 100 sites distants. Dans les prochaines années, elle prévoit d'étendre le réseau jusqu'à 500 sites distants.

La Figure 7.32 illustre une version simplifiée du réseau APPN actuel de l'agence.

Figure 7.32
Exemple de réseau APPN pour
une agence gouvernementale.



Le centre de données comprend 20 mainframes de chez IBM et d'autres fabricants. Les mainframes IBM tournent sur MVS et exploitent la technologie VTAM. Ils sont également configurés en tant que nœud NN/DLUS et hôtes de données EN. Aucun protocole de sous-zone n'existe sur ce réseau. Les autres mainframes non-IBM sont configurés en tant que nœuds EN ou LEN.

La plate-forme utilisateur est OS/2 exploitant Communications Server sur tous les sites distants qui ont des besoins de connectivité avec les mainframes du centre de données. Initialement, il n'est pas nécessaire de disposer d'une connectivité any-to-any. Les applications supportées sont LU type 2 et LU6.2.

APPN dans le centre de données

Les hôtes mainframes à la Figure 7.32 sont connectés au moyen d'une carte de communication externe (XCA, *External Communication Adapter*) par l'intermédiaire des contrôleurs d'interconnexion 3172. Les hôtes de données non-IBM (sociétés A, B et C) utilisent le mainframe IBM VTAM en tant que serveur nœud de réseau. Pour limiter au minimum les flots TDU, les sessions CP-CP existent uniquement entre VTAM et les routeurs du centre de données, mais pas entre ces derniers.

Pour bénéficier d'un calcul de routes optimal sans définir de façon explicite des connexions maillées, tous les nœuds d'extrémité et de réseau sur le centre de données sont reliés au même réseau de connexions. Cela permet à une session d'être directement établie entre deux ressources de centre de données sans avoir à traverser le nœud de réseau VTAM. Comme le montre la Figure 7.32, lorsqu'une session LU-LU est établie entre des ressources de mainframe (entre EN3A et la société A), la route optimale passe directement par l'anneau FDDI en direction de NN1 et NN3.

Pour réduire le nombre de requêtes de localisation en diffusion à un minimum d'une par ressource, VTAM est configuré en tant que CDS (serveur d'annuaire central) pour ce réseau. La fonction CDS est ici très efficace, car les ressources sur le réseau ont seulement besoin d'accéder à celles situées sur les hôtes du centre de données. Ces mainframes hôtes enregistrent leurs ressources avec VTAM, qui représente leur serveur nœud de réseau. Par conséquent, VTAM dispose toujours d'informations de localisation sur chaque ressource du centre de données, ce qui veut dire qu'il n'a jamais besoin de diffuser de requêtes de localisation.

APPN sur le site distant

Le réseau illustré Figure 7.32 comprend environ 30 à 40 stations de travail CS/2 sur chaque site distant. Chacune d'elles est configurée en tant que nœud d'extrémité. Chacun de ces nœuds supporte huit sessions LU6.2 indépendantes et quatre sessions LU dépendantes. Un routeur Cisco sur chaque site transmet le trafic vers le centre de données. La fonction de nœud de réseau de ces routeurs gère le routage intermédiaire pour les unités LU indépendantes et la fonction DLUR gère le routage pour les LU dépendantes.

Configuration future

Il est prévu que ce réseau s'étende pour comprendre jusqu'à 500 routeurs distants nœud de réseau, 100 routeurs de centre de données et huit mainframes. Généralement, un réseau APPN de 600 nœuds

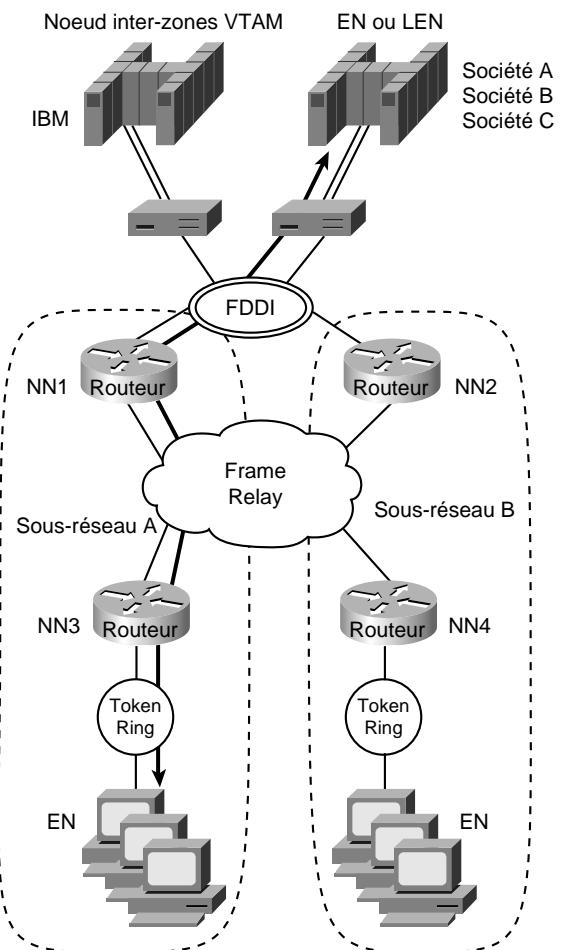
rencontrera des problèmes d'évolutivité. La suite de cette section examine les deux options que vous pouvez exploiter pour contourner ces problèmes sur un réseau APPN :

- implémentation de nœuds interzones sur VTAM pour segmenter le réseau en sous-réseaux ;
- utilisation de la fonction FRAS BNN pour réduire le nombre de nœuds de réseau.

Emploi de nœuds interzones sur VTAM pour segmenter le réseau en sous-réseaux

En implémentant le concept de nœuds interzones sur VTAM, une frontière de sous-réseau est introduite en périphérie entre le nœud NN1 et VTAM, et le nœud NN2 et VTAM, comme illustré Figure 7.33.

Figure 7.33
Réseau APPN avec nœud interzone VTAM étendu.



Aucun échange d'informations de topologie n'aurait lieu entre VTAM et les routeurs NN du centre de données. Les huit mainframes seraient dans le même sous-réseau. Chaque routeur de centre de données supporterait plusieurs routeurs d'accès et ils formeraient leur propre sous-réseau (chaque sous-réseau étant limité à un maximum de 100 nœuds de réseau). Cette configuration empêcherait que des informations de topologie soient envoyées d'un sous-réseau vers un autre et permettrait au réseau d'évoluer au-delà des 600 nœuds de réseau.

Bien que cette approche gère le problème des flots de paquets TDU, la configuration de VTAM en tant que nœud interzone dans cet environnement entraîne une perte de fonctions très importante. Tout d'abord, deux sous-réseaux APPN ne peuvent pas être interconnectés par l'intermédiaire d'un réseau de connexions. Les sessions LU-LU entre les ressources situées sur l'hôte de la société A et celles de sites distants seraient établies par l'intermédiaire d'un itinéraire indirect passant par le nœud interzone VTAM. Cette route n'est évidemment pas optimale. Deuxièmement, la fonction de serveur d'annuaire central est perdue, car le nœud interzone VTAM présente une image de nœud d'extrémité à NN1. Cela empêche NN1 de découvrir le serveur d'annuaire central sur le réseau.

La section suivante étudie une autre approche mettant en œuvre la technologie FRAS BNN pour réduire le nombre de nœuds de réseau.

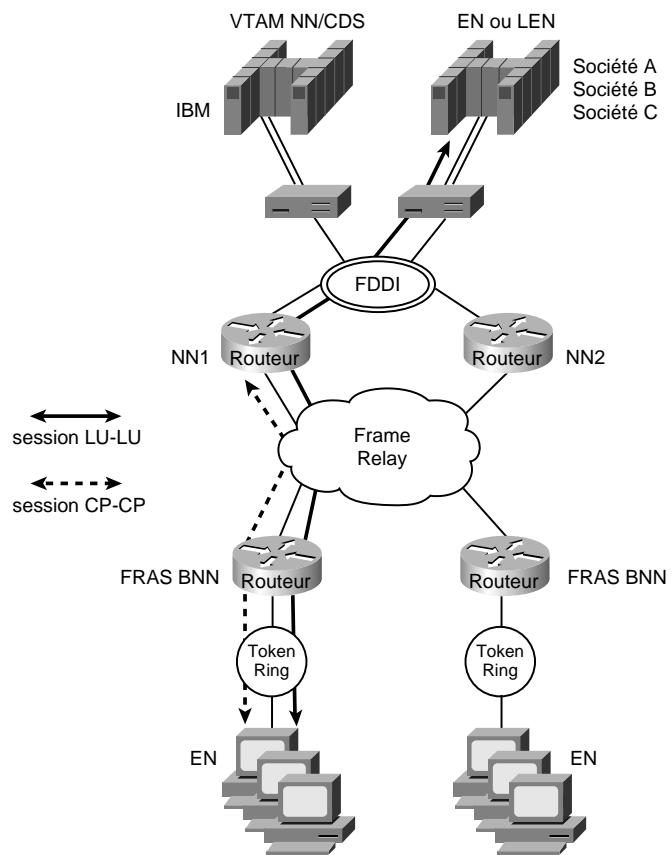
Utilisation de FRAS BNN pour réduire le nombre de nœuds de réseau

La Figure 7.34 illustre de quelle façon FRAS BNN peut être utilisé pour diminuer le nombre de nœuds du réseau de l'entreprise. Toutes les applications serveur sont situées sur les mainframes et les dispositifs de réseau ont uniquement besoin d'accéder à l'hôte. Le routage APPN n'est pas essentiel pour cette entreprise.

L'implémentation de FRAS BNN à la place d'un nœud de réseau APPN complet sur les routeurs d'accès diminue directement le nombre de nœuds de réseau. Cela permet au réseau de s'adapter sans être confronté aux problèmes de flots de TDU. Cette approche s'est révélée viable pour l'entreprise à ce stade d'évolution, car la connectivité LAN-LAN n'est pas une exigence immédiate. Les routeurs distants pourront faire l'objet d'une migration pour supporter un nœud interzone APPN lorsqu'il sera disponible.

Dans cet environnement, les sessions CP-CP sont supportées sur le réseau Frame Relay. Le serveur d'annuaire central et le concept de réseau de connexions sont totalement supportés. Les sessions LU-LU peuvent être établies en utilisant la route directe sans traverser VTAM, comme l'illustre la Figure 7.34. La seule fonction qui est perdue avec FRAS BNN est celle de classe de service pour le trafic circulant à partir du routeur Distant FRAS BNN vers le centre de données.

Figure 7.34
Réseau APPN avec FRAS BNN.



Résumé

Ce chapitre a traité du développement d'un tracé de réseau existant et de la planification d'une migration réussie vers APPN. Les sujets suivants ont été étudiés :

- évolution de SNA ;
- intégration d'APPN ;
- utilisation d'APPN ou d'autres méthodes de transport SNA ;
- présentation d'APPN ;
- implémentation Cisco d'APPN ;
- problèmes d'évolutivité ;
- techniques de communication de secours sur un réseau APPN ;
- intégration d'APPN dans un environnement multiprocole ;
- gestion de réseau ;
- exemples de configuration.

8

Interréseaux DLSw+

Ce chapitre comporte les sections suivantes :

- Introduction à DLSw+
- Débuter avec DLSw+
- Fonctionnalités avancées de DLSw+

Introduction à DLSw+

Cette section décrit la technologie de commutation de liaison de données DLSw+ (*Data Link Switching Plus*) et présente des exemples de configuration permettant de concevoir et configurer rapidement des réseaux DLSw+. Elle passe en revue les composants essentiels de cette technologie et décrit les extensions qu'elle propose par rapport au standard. Elle étudie également les fonctionnalités avancées de DLSw+, leur contexte d'utilisation, et donne des exemples de leur exploitation. Elle aborde ensuite des thèmes comme l'optimisation, la conception hiérarchique, la conception maillée, le débogage et les directives de migration, pour finir par des recommandations sur la façon de concevoir votre réseau. Cette section peut être utilisée comme un simple guide de référence (pour les exemples de configuration), comme guide d'optimisation, ou comme guide de conception d'un réseau DLSw+.

Définition de DLSw+

DLSw+ est un système de transport pour le trafic SNA (*Systems Network Architecture*) et NetBIOS sur un réseau de campus ou un réseau étendu (WAN). Les systèmes terminaux peuvent se connecter au réseau par l'intermédiaire de technologies de réseau diverses telles que Token Ring, Ethernet, SDLC (*Synchronous Data Link Control*), QLLC (*Qualified Logical Link Control*), ou FDDI (*Fiber Distributed Data Interface*) — FDDI n'est supporté que sur la série de routeurs Cisco 7000 et requiert la version 11.2 ou ultérieure du système Cisco IOS. DLSw+ opère une commutation entre ces divers médias et termine localement les liaisons de données, ce qui permet de maintenir la surcharge liée aux messages d'acquittement, au contrôle d'activité (*keepalive*) et au sondage, en dehors du réseau étendu. La terminaison locale des liaisons de données permet aussi d'éliminer les dépassements de délai au niveau du contrôle de ces liaisons, qui peuvent se produire en cas de

congestion du réseau ou de reroutage (lorsqu'il faut contourner une liaison inexploitable). Finalement, DLSw+ fournit un mécanisme de recherche dynamique des ressources SNA ou NetBIOS sur le réseau et intègre des algorithmes de gestion de cache qui minimisent les diffusions générales.

Dans cet ouvrage, un routeur DLSw+ est désigné par le terme *routeur homologue* (routeur peer), *homologue* (peer), ou *partenaire* (partner). La connexion entre deux routeurs DLSw+ est appelée *connexion d'homologues*. Un circuit DLSw+ offre un compromis de dénomination qui désigne la relation entretenue par la connexion de contrôle de liaison de données entre le système terminal et le routeur D'origine, la connexion entre les deux routeurs — généralement une connexion TCP (*Transport Control Protocol*) —, et la connexion de contrôle de liaison de données entre le routeur et le système terminal de destination. Une seule connexion d'homologues peut transporter plusieurs circuits.

DLSw+ gère les circuits entre les unités physiques SNA (PU), ou entre les clients et les serveurs NetBIOS. La connectivité de PU SNA supportée est PU 2.0/2.1 vers PU 4 (reliée par n'importe quel type de contrôle de liaison de données supporté), PU 1 vers PU 4 (*via SDLC seulement*), PU 4 vers PU 4 (Token Ring seulement), et PU 2.1 vers PU 2.1 (n'importe quel contrôle de liaison de données supporté).

NOTE

La connectivité PU 4 vers PU 4 n'accepte qu'un seul chemin entre les ordinateurs frontaux (FEP), car ils traitent les chemins passant par un pont à routage par la source d'une façon particulière. De plus, le chargement distant n'est pas accepté.

Standard DLSw

Le standard DLSw a été défini par l'atelier AIW (*APPN Implementers Workshop*) du groupe d'intérêt travaillant sur DLSw. Au moment de la rédaction de cet ouvrage, ce standard en était à sa version 1. Il a été documenté dans le RFC 1795, qui rend de fait obsolète le RFC 1434 décrivant l'implémentation 6611 originale de DLSw par IBM.

Le standard DLSw décrit le protocole SSP (*Switch-to-Switch*) utilisé entre les routeurs (appelés commutateurs de liaison de données) pour établir des connexions d'homologues DLSw, localiser des ressources, transmettre des données, gérer le contrôle de flux, et assurer la reprise après erreur. Le RFC 1795 stipule que les connexions de la couche liaison de données doivent se terminer au niveau des routeurs homologues, c'est-à-dire qu'elles doivent être localement acquittées et, dans le cas d'un réseau Token Ring, que le champ d'informations de routage (RIF) doit se terminer au niveau d'un anneau virtuel sur le routeur homologue.

En terminant localement les connexions, le standard DLSw élimine le besoin de faire traverser les messages d'acquittement et *keepalive* (de contrôle d'activité de ligne) de la couche liaison de données sur le réseau étendu. Par conséquent, il ne devrait plus y avoir d'expiration de délai de réponse au niveau de cette couche. Il incombe aux routeurs DLSw de multiplexer le trafic de plusieurs liaisons de données vers le tube TCP approprié et d'assurer le transport fiable des données à travers une épine dorsale IP.

Avant que toute communication de système terminal puisse avoir lieu sur DLSw, les actions suivantes doivent être entreprises :

- établissement de connexions d'homologues ;
- échange d'informations de services ;
- établissement d'un circuit.

Etablissement de connexions d'homologues

Pour que deux routeurs puissent gérer la commutation d'un trafic SNA ou NetBIOS, ils doivent au préalable établir deux connexions TCP entre eux. Le standard autorise l'abandon de l'une de ces connexions si elle n'est pas nécessaire, ce que font les routeurs Cisco sauf s'ils doivent communiquer avec le routeur D'un autre fabricant qui requerrait deux connexions TCP. Le standard permet également l'établissement de connexions TCP supplémentaires pour pouvoir assurer différents niveaux de priorité.

Echange d'informations de services

Après établissement des connexions TCP, les routeurs échangent des informations sur les services qu'ils assurent. Cet échange inclut le numéro de version de DLSw, les fenêtres initiales de régulation (taille de la fenêtre de réception), le support NetBIOS, la liste des points d'accès aux services de liaison supportés (SAP), et le nombre de sessions TCP acceptées. Les listes d'adresses de la sous-couche MAC (*Media Access Control*, contrôle d'accès au média) et celles de noms NetBIOS peuvent également être communiquées durant cette phase. Si nécessaire, un partenaire DLSw peut spécifier qu'il ne souhaite pas recevoir certains types de trames de recherche. Il est possible de configurer les adresses MAC et les noms NetBIOS de toutes les ressources qui utiliseront DLSw de façon à éviter toute diffusion générale de requêtes. Après cet échange d'informations, les partenaires DLSw sont prêts à établir des circuits entre les systèmes terminaux SNA ou NetBIOS.

Etablissement d'un circuit

L'établissement d'un circuit entre une paire de systèmes terminaux inclut la localisation de la ressource cible (basée sur l'adresse MAC ou le nom NetBIOS de la destination) et l'établissement des connexions de la liaison de données entre chaque système terminal et son commutateur de liaison de données (routeur local). SNA et NetBIOS sont gérés différemment. Un dispositif SNA sur un LAN recherche un autre dispositif SNA en émettant une trame d'exploration (une trame TEST ou une trame d'échange d'identification XID) avec l'adresse MAC du dispositif SNA cible. Lorsqu'un routeur DLSw reçoit une telle trame de recherche, il envoie une trame d'interrogation CANUREACH vers chacun des partenaires DLSw. Si l'un de ses partenaires dispose d'un accès vers l'adresse spécifiée, il l'indique en renvoyant une trame de confirmation ICANREACH. La séquence spécifique comprend une trame CANUREACH *ex* (*explorer*) pour localiser la ressource et une trame ICANREACH *cs* (*circuit setup*) qui déclenche l'établissement du circuit entre les routeurs homologues.

A cette étape, les partenaires DLSw mettent en place un *circuit* qui comprend trois connexions : les deux connexions de contrôle de liaison de données entre chaque routeur et son système terminal

local, et la connexion TCP entre les partenaires DLSw. Ce circuit est identifié de façon unique par des identifiants de circuit source et de destination qui sont transportés dans toutes les trames de données constantes à la place des adresses de contrôle de liaison, telles que les adresses MAC. Chaque identifiant de circuit est défini par les adresses MAC de destination et de source, les points d'accès aux services de liaison de destination et de source (LSAP), et un identifiant de port de liaison de données. Le concept de circuit simplifie la gestion et a son importance dans le processus de traitement des erreurs et de nettoyage. Une fois le circuit établi, les trames d'informations peuvent circuler.

La procédure d'établissement d'un circuit NetBIOS est similaire, sauf qu'au lieu de transmettre une trame CANUREACH qui spécifie une adresse MAC, les routeurs DLSw envoient une requête de nom (NetBIOS NAME-QUERY) spécifiant un nom NetBIOS. De la même manière, une trame de nom reconnu (NetBIOS NAME-RECOGNIZED) est envoyée en réponse au lieu d'une trame ICANREACH.

La plupart des implémentations DLSw placent en cache les informations recueillies au cours des processus d'exploration, afin que les recherches suivantes pour une même ressource ne provoquent pas l'envoi de trames d'exploration supplémentaires.

Contrôle de flux

Le standard DLSw décrit un mécanisme de régulation adaptable pour la transmission entre routeurs homologues, mais n'indique pas comment établir une correspondance avec le contrôle de flux natif de la liaison de données aux extrémités. Le contrôle de flux est spécifié par le standard sur la base d'un circuit et implique l'utilisation de deux mécanismes indépendants de contrôle de flux de circuit unidirectionnel. Ce contrôle est géré par un mécanisme de fenêtrage capable de s'adapter dynamiquement à la disponibilité du tampon, à la profondeur de la file d'attente de transmission TCP, et aux mécanismes de contrôle de flux au niveau des stations terminales. Les fenêtres peuvent être augmentées, diminuées, divisées, ou réinitialisées à zéro.

Les unités accordées (le nombre d'unités que l'émetteur est autorisé à transmettre) sont augmentées selon une indication de contrôle de flux de la part du récepteur (procédure similaire à la régulation classique de niveau de session SNA). Les indicateurs de contrôle de flux peuvent être de l'un des types suivants :

- **Répéter.** Augmente les unités accordées de la valeur de la taille de la fenêtre actuelle.
- **Incrémenter.** Incrémente la taille de la fenêtre de 1 et augmente les unités accordées de la valeur de la nouvelle taille de fenêtre.
- **Décrémenter.** Réduit la taille de la fenêtre de 1 et augmente les unités accordées de la valeur de la nouvelle taille de fenêtre.
- **Réinitialiser.** Réduit la taille de la fenêtre à zéro et définit les unités accordées à zéro pour mettre fin à toutes les transmissions dans une direction, jusqu'à ce qu'un indicateur d'incrémantation soit envoyé.
- **Diminuer de moitié.** Diminue de moitié la taille actuelle de la fenêtre et augmente les unités accordées de la valeur de la nouvelle taille de fenêtre.

Les indicateurs et les acquittements de contrôle de flux peuvent être annexés aux trames d'informations par *piggybacking* ou envoyés en tant que messages de contrôle de flux indépendants, alors que les indicateurs de réinitialisation sont toujours transmis comme messages indépendants.

Fonctionnalités DLSw+

DLSw+ est l'implémentation Cisco de DLSw. Elle va au-delà du standard pour inclure la fonctionnalité avancée de pont distant à routage par la source de Cisco, dit RSRB (*Remote Source Route Bridge*), ainsi que des fonctionnalités supplémentaires permettant d'augmenter le niveau d'adaptabilité générale de DLSw. DLSw+ offre une amélioration des caractéristiques suivantes :

- **Evolutivité.** Il permet d'élaborer des interréseaux IBM de telle façon que la quantité de trafic généré par les diffusions générales s'en trouve réduite, ce qui améliore par conséquent leur évolutivité.
- **Disponibilité.** Il permet de rechercher dynamiquement et rapidement des chemins alternatifs, et peut optionnellement équilibrer la charge sur plusieurs homologues, ports, et passerelles de canal (channel gateway) actifs.
- **Souplesse de transport.** Il offre des possibilités de transport hautement performant lorsqu'il y a suffisamment de bande passante pour gérer la charge sans risque d'expiration de délais, et permet de choisir des solutions entraînant moins de surcharge lorsque la bande passante doit être protégée et qu'un rerouting sans interruption n'est pas requis.
- **Modes d'opération.** Il détecte dynamiquement les services du routeur homologue pour les prendre en compte dans son fonctionnement.

Evolutivité améliorée de DLSw+

L'un des principaux facteurs limitant la taille des interréseaux de LAN est la quantité de trafic d'exploration qui traverse le réseau étendu. DLSw+ comprend plusieurs mécanismes d'optimisation permettant de le réduire.

Concept de groupes d'homologues

L'amélioration la plus importante dans DLSw+ est sans doute le concept de *groupes d'homologues*. Il a été conçu pour s'attaquer au problème de reproduction des trames de diffusion sur les réseaux totalement maillés. Lorsqu'une communication any-to-any est nécessaire (par exemple, dans les environnements NetBIOS ou APPN), les implémentations de RSRB ou du standard DLSw nécessitent l'établissement de connexions d'homologues entre tous les routeurs pris deux à deux.

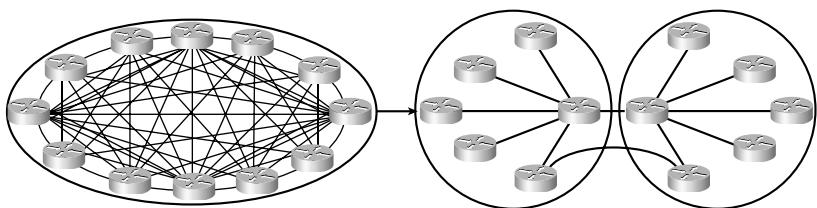
De telles implémentations sont non seulement difficiles à configurer, mais elles obligent les routeurs d'accès d'agence à reproduire les requêtes de recherche pour chaque connexion d'homologues. Il en résulte un gaspillage de la bande passante et des cycles de traitement des routeurs. Une meilleure approche serait de grouper les routeurs en clusters et d'en désigner un qui soit responsable de la reproduction des diffusions. Cette fonctionnalité est incluse dans DLSw+.

Avec DLSw+, un cluster de routeurs dans une région ou un département d'une entreprise peut être combiné avec un groupe d'homologues. A l'intérieur d'un tel groupe, un ou plusieurs routeurs sont désignés en tant qu'homologues interzones (border peer). Au lieu d'assister à une prolifération d'échanges de messages entre tous les routeurs pris deux à deux, chaque routeur dans un groupe

émet vers son homologue interzone ; les homologues interzones établissent entre eux des connexions d'homologues (voir Figure 8.1). Lorsqu'un routeur DLSw+ reçoit une trame TEST ou de requête de nom (NetBIOS NAME-QUERY), il envoie une seule trame d'exploration à son homologue interzone. Celui-ci retransmet la trame de recherche au nom du membre du groupe d'homologues. Cette configuration élimine les trames dupliquées sur les liaisons d'accès et limite le traitement nécessaire au niveau des routeurs d'accès.

Figure 8.1

Le concept de groupes d'homologues peut être utilisé pour simplifier et adapter les réseaux any-to-any.



Lorsque le routeur De destination correct est trouvé, une connexion d'homologues de bout en bout (TCP ou IP) est établie pour transporter le trafic entre systèmes terminaux. Cette connexion demeure active aussi longtemps que du trafic de système terminal est transporté et elle est dynamiquement libérée lorsqu'elle n'est plus utilisée. Cela permet de bénéficier d'une communication any-to-any ponctuelle sans le souci de devoir spécifier par avance les connexions d'homologues. Cette fonctionnalité permet également le routage any-to-any sur de grands interréseaux, sur lesquels les connexions TCP permanentes entre tous les routeurs pris deux à deux ne seraient pas possibles.

Pare-feu d'exploration

Afin de réduire davantage la quantité de trafic d'exploration qui pénètre sur le réseau étendu, un certain nombre de techniques de filtrage et de pare-feu permettent de stopper ce trafic au niveau du routeur DLSw+. L'une des techniques essentielles est le pare-feu d'exploration.

Un pare-feu d'exploration n'autorise la traversée du réseau étendu qu'à une seule trame d'exploration en direction d'une adresse MAC de destination spécifique. Lorsqu'une trame d'exploration est en suspens et attend une réponse de la part de la destination, les trames suivantes pour cette même adresse ne sont pas propagées. Une fois que le routeur DLSw+ d'origine a reçu la réponse, toutes les trames d'exploration pour la même destination reçoivent une réponse au niveau local. Cela élimine les tempêtes de trames d'exploration qui se produisent sur de nombreux réseaux en début de journée.

Disponibilité améliorée de DLSw+

DLSw+ offre une meilleure disponibilité grâce à la gestion d'un cache d'accessibilité contenant de multiples chemins vers des adresses MAC ou vers des noms NetBIOS locaux et distants. Dans le cas d'une ressource distante, le chemin indique l'homologue à utiliser pour pouvoir l'atteindre. Si la ressource est locale, le chemin spécifie un numéro de port. Lorsqu'il existe plusieurs itinéraires permettant d'atteindre une destination, le routeur marquera l'un des chemins comme route préférée et les autres comme routes possibles. Si le chemin préféré n'est pas disponible, le chemin suivant

possible sera élu chemin préféré et la convergence sera immédiatement initiée. La façon dont DLSw+ gère plusieurs chemins possibles peut être influencée (mot clé **bias**) pour répondre aux besoins du réseau :

- **Tolérance aux pannes.** Dans ce mode, un circuit est établi sur un chemin préféré, mais également rapidement dirigé sur un chemin alternatif actif en cas de perte de la liaison préférée.
- **Équilibrage de charge.** Dans ce mode, l'établissement du circuit est réparti sur plusieurs homologues DLSw+ du réseau ou ports du routeur.

La configuration par défaut de DLSw+ lui indique d'utiliser le mode de tolérance aux pannes. Dans cette configuration, lorsqu'un homologue DLSw+ reçoit une trame TEST pour une ressource distante, il consulte son cache. S'il trouve une entrée correspondante et que celle-ci est récente (c'est-à-dire qu'elle n'a pas été vérifiée durant le dernier intervalle de vérification), il répond immédiatement sans diffuser de trame d'interrogation CANUREACH sur le réseau. Si, en revanche, l'entrée est obsolète, l'homologue DLSw+ d'origine envoie une trame CANUREACH directement à chaque homologue figurant dans son cache pour en valider les entrées (ce processus est connu sous le nom de vérification dirigée). En l'absence de réponse de la part d'un homologue, celui-ci est supprimé de la liste. Cette procédure peut provoquer le réordonnancement des entrées du cache. Le paramètre configurable SNA-VERIFY-INTERVAL spécifie le délai d'attente observé par un routeur avant de marquer une entrée du cache comme étant obsolète. Le paramètre SNA-CACHE-TIMEOUT indique la durée de conservation des entrées dans le cache avant leur suppression. La valeur par défaut est de 16 minutes et peut être modifiée.

Le routeur DLSw+ de destination suit une procédure légèrement différente en utilisant les entrées du cache local. Si l'entrée dans le cache est récente, il envoie la réponse immédiatement. Si elle est obsolète, il diffuse une seule trame TEST à route unique sur tous les ports spécifiés dans le cache. Si une réponse positive est reçue, il envoie une trame ICANREACH au routeur D'origine. Les trames de TEST sont envoyées toutes les 30 secondes (paramètre SNA-RETRY-INTERVAL) durant une période de 3 minutes (paramètre SNA-EXPLORER-TIMEOUT). Ces temporiseurs sont configurables.

Vous pouvez aussi configurer DLSw+ pour qu'il utilise l'équilibrage de charge lorsqu'il existe plusieurs itinéraires permettant d'atteindre une destination. Dans ce cas, les nouvelles requêtes d'établissement de circuit utilisent à tour de rôle tous les homologues ou ports possibles listés.

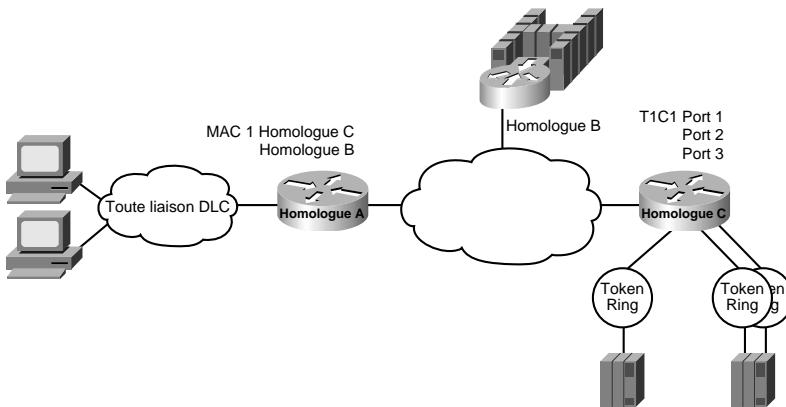
Cette fonction est particulièrement intéressante sur les réseaux SNA. Une pratique très courante dans cet environnement hiérarchique consiste à assigner la même adresse MAC à différentes passerelles de canal de mainframe, comme des FEP ou des routeurs Cisco avec plusieurs CIP (*Channel Interface Processor*). Si une passerelle de canal est indisponible, d'autres sont dynamiquement localisées sans intervention de l'opérateur. L'adressage MAC dupliqué permet également d'assurer l'équilibrage de charge sur plusieurs passerelles ou cartes Token Ring actives.

DLSw+ garantit la localisation des adresses MAC dupliquées, et peut placer en cache jusqu'à quatre homologues DLSw+ ou ports d'interface pouvant être utilisés pour trouver une adresse MAC. Cette technique peut être appliquée dans le cadre de la tolérance aux pannes et de l'équilibrage de charge. Dans le premier cas, elle facilite une reconnexion dans les temps suite à une interruption de circuit, et, dans le second, elle améliore les performances SNA globales en répartissant le trafic sur plusieurs composants actifs (routeurs, cartes Token Ring ou FDDI, ou passerelles de canal), comme illustré Figure 8.2. L'équilibrage de charge améliore non seulement les performances, mais aussi la vitesse

de rétablissement en cas de perte d'un composant sur un itinéraire, car seule une portion limitée du réseau est affectée.

Figure 8.2

Les techniques de mise en cache de DLSw+ permettent d'équilibrer la charge sur plusieurs routeurs de site central, anneaux Token Ring et passerelles de canal.



Outre le support de plusieurs homologues actifs, DLSw+ supporte des *homologues de secours* qui sont connectés uniquement lorsque l'homologue principal est inaccessible.

Souplesse de transport de DLSw+

La connexion de transport entre les routeurs DLSw+ peut varier selon les besoins du réseau et n'est pas liée à TCP/IP, contrairement au standard DLSw. Cisco supporte quatre protocoles de transport sur les routeurs DLSw+ :

- **TCP/IP.** Ce protocole transporte le trafic SNA et NetBIOS sur des liaisons WAN lorsque l'acquittement local est nécessaire pour minimiser le trafic inutile et empêcher les expirations de délai du contrôle de liaison de données, et lorsque le reroutage sans interruption permettant de contourner une liaison défaillante est crucial. Cette option de transport est requise lorsque DLSw+ opère dans le mode DLSw standard.
- **FST/IP.** Ce protocole transporte le trafic SNA et NetBIOS sur des liaisons WAN de topologie quelconque. Cette solution autorise le reroutage pour contourner des liaisons impraticables, mais un rétablissement peut être source d'interruption selon le temps qui sera nécessaire à l'identification d'un chemin alternatif. Cette option n'offre pas le support de l'acquittement local des trames.
- **Directe.** Ce protocole transporte le trafic SNA ou NetBIOS sur une connexion point-à-point ou Frame Relay lorsque les avantages offerts par une topologie quelconque ne sont pas nécessaires et que le reroutage sans interruption n'est pas requis. Cette option n'offre pas le support de l'acquittement local des trames.
- **DLSw Lite.** Ce protocole transporte le trafic SNA et NetBIOS sur une connexion point-à-point (actuellement, seule la technologie Frame Relay est acceptée) lorsque l'acquittement local et le

transport fiable sont requis, mais que le reroutage sans interruption n'est pas une nécessité. Ce protocole utilise l'encapsulation de LLC2 (*Logical Link Control type 2*) décrite dans le RFC 1490.

Modes de fonctionnement de DLSw+

Cisco commercialise depuis de nombreuses années des produits d'interconnexion pour les réseaux IBM. Il existe aujourd'hui une base substantielle de routeurs Cisco exploitant RSRB. Par conséquent, il est essentiel que DLSw+ et RSRB puissent cohabiter sur le même réseau et sur le même routeur. De plus, comme DLSw+ est basé sur le nouveau standard DLSw, il doit aussi pouvoir interopérer avec les implémentations d'autres fabricants qui se basent également sur ce standard.

DLSw+ possède trois modes de fonctionnement :

- **Mode double.** Un routeur Cisco peut communiquer avec certains homologues distants au moyen de RSRB et avec d'autres homologues au moyen de DLSw+, en fournissant un chemin de transition sans difficultés de RSRB vers DLSw+. En mode double, RSRB et DLSw+ peuvent cohabiter sur la même machine, l'homologue local devant être configuré pour les deux protocoles et les homologues distants soit pour RSRB soit pour DLSw+, mais pas pour les deux.
- **Mode conforme au standard.** DLSw+ peut détecter automatiquement (*via* le processus DLSw d'échange d'informations de services) que le routeur participant a été produit par un autre fabricant, et qu'il fonctionne par conséquent en mode DLSw standard.
- **Mode étendu.** DLSw+ peut détecter automatiquement que le routeur participant est un autre routeur DLSw+, et qu'il fonctionne par conséquent en mode étendu, pouvant offrir aux systèmes terminaux SNA et NetBIOS toutes les fonctionnalités de DLSw+.

Certaines fonctions avancées de DLSw+ sont également disponibles lorsqu'un routeur Cisco interact en mode standard avec le routeur d'un autre fabricant. En particulier, les améliorations que l'on retrouve sous forme d'options contrôlées localement au niveau d'un routeur sont accessibles même si le routeur distant n'exécute pas DLSw+. Ces fonctions étendues incluent l'équilibrage de charge, l'apprentissage local (la faculté de déterminer si une destination se trouve sur un LAN avant d'envoyer des trames de recherche sur le réseau étendu), le pare-feu d'exploration et la conversion de média.

Comment procéder

Si vous disposez d'un réseau hiérarchique simple ne traitant qu'un faible volume de trafic SNA, lisez la section "Débuter avec DLSw+" qui décrit les commandes de configuration requises pour toutes les implémentations de DLSw+ et donne des exemples de configuration pour SDLC, Token Ring, Ethernet et QLLC. Une fois que vous l'aurez lue, vous pourrez étudier les fonctionnalités avancées, la personnalisation, et la gestion de la bande passante.

Ce chapitre décrit de quelle façon utiliser DLSw+ avec des dispositifs de concentration en aval (DSPU, *Downstream Physical Unit*), LAN Network Manager, APPN et l'architecture d'interface client native (NCIA, *Native Client Interface Architecture*).

Débuter avec DLSw+

Cette section décrit les commandes de configuration de base nécessaires à l'implémentation d'un réseau DLSw+. Elle commence pour une description de la configuration minimale requise, puis donne des exemples d'intégration avec les environnements Token Ring, Ethernet, SDLC et QLLC. Si la configuration des routeurs est un sujet qui ne vous est pas familier, vous pouvez également étudier les exemples de l'Annexe A. Ils illustrent la configuration des routeurs, mais aussi des systèmes terminaux qui y sont connectés, et montrent comment configurer des adresses canoniques, des routes statiques et des adresses de bouclage.

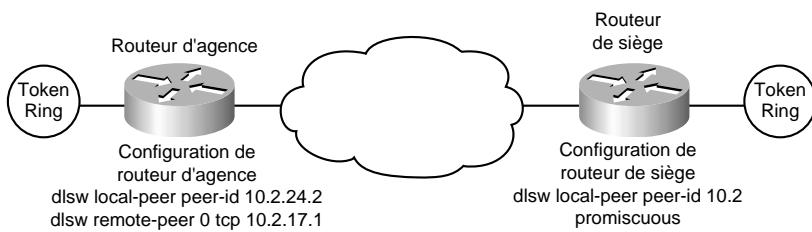
Configuration minimale requise

La configuration de DLSw+ n'est pas une opération difficile sur la plupart des réseaux. Chaque routeur qui supporte ce protocole doit avoir été configuré à l'aide de la commande **dlsw local-peer** ; les commandes **dlsw remote-peer** sont optionnelles mais, généralement, au moins un côté de la connexion d'homologues doit prévoir la configuration d'un homologue distant. Si une configuration d'homologue omet la commande **dlsw remote-peer**, la commande **dlsw local-peer** doit spécifier le mot clé **promiscuous**. Les routeurs fonctionnant en mode transparent (promiscuous) accepteront des requêtes de connexion d'homologues de la part de routeurs qui ne sont pas préconfigurés. Cette fonction permet de limiter les changements au niveau des routeurs de sites centraux lorsque des bureaux régionaux sont ajoutés ou supprimés. Elle permet également de réduire les tâches nécessaires à la coordination des configurations.

Si vous avez utilisé RSRB par le passé, vous devez savoir ce qui *ne doit pas* être configuré. Avec DLSw+, vous n'avez pas besoin d'explorateur proxy, de cache de noms NetBIOS, de conversion SDLC vers LLC2 (SDLLC), ou de pont traducteur avec routage par la source (SR/TLB). Toutes ces fonctions sont intégrées dans DLSw+.

Dans la Figure 8.3, le routeur D'agence spécifie à la fois la commande **dlsw local-peer** et la commande **dlsw remote-peer**. Le routeur De siège ne spécifie que la commande **dlsw local-peer**, mais précise le mot clé **promiscuous** pour pouvoir accepter dynamiquement les connexions de la part de routeurs d'agences. L'identifiant d'homologue spécifié avec cette commande est l'adresse IP du routeur. Il pourrait s'agir d'une adresse de bouclage configurée via la commande **interface loop-back 0** ou de l'adresse IP associée à une interface LAN ou WAN spécifique. Toutefois, si vous utilisez une adresse IP de réseau local ou étendu, l'interface doit être active pour que DLSw puisse fonctionner.

Figure 8.3
Exemple des commandes **dlsw local-peer** et **dlsw remote-peer**.



L'adresse qui suit la commande **dlsw remote-peer** est celle de la liste de l'anneau. Comme les listes d'anneaux représentent un sujet avancé, il vaut mieux pour l'instant spécifier zéro dans cet espace pour indiquer qu'elles ne sont pas utilisées. Il existe d'autres options pour ces deux commandes, mais elles ne sont pas nécessaires. Elles seront traitées à la section "Fonctionnalités avancées de DLSw+", plus loin dans ce chapitre.

Outre la spécification des homologues locaux et distants, vous devez établir des correspondances entre les types de contrôles de liaison de données locaux suivants et DLSw :

- **Token Ring.** Définissez un anneau virtuel en utilisant la commande **source-bridge ring-group** et incluez une commande **source-bridge** pour indiquer au routeur De diriger le trafic à travers le pont du Token Ring externe vers cet anneau virtuel.
- **Ethernet.** Faites correspondre un groupe spécifique de ponts Ethernet avec DLSw.
- **SDLC.** Définissez les dispositifs SDLC et établissez une correspondance entre les adresses SDLC et les adresses MAC virtuelles DLSw+.
- **QLLC.** Définissez les dispositifs X.25 et établissez une correspondance entre les adresses X.25 et les adresses MAC virtuelles DLSw+.
- **FDDI.** Définissez un anneau virtuel en utilisant la commande **source-bridge ring-group** et incluez une instruction SRB qui indique au routeur De ponter le trafic du réseau FDDI externe vers cet anneau virtuel. FDDI est supporté par le système Cisco IOS version 11.2 sur la série de routeurs Cisco 7000.

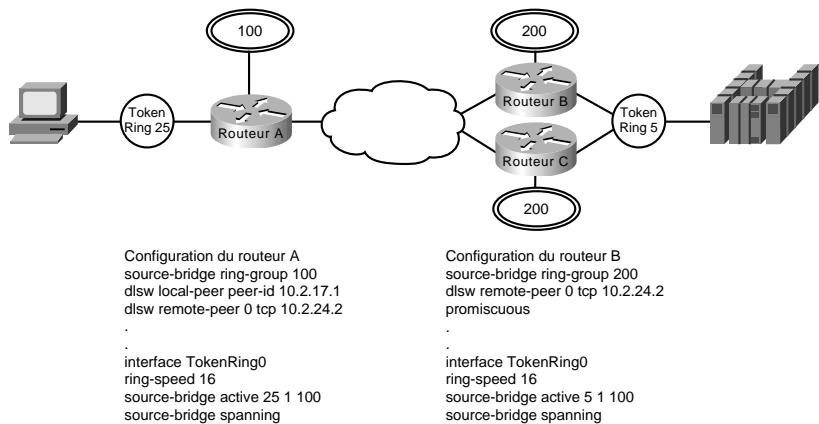
Le reste de cette section donne des exemples de configuration pour les environnements Token Ring, Ethernet, SDLC et QLLC.

Token Ring

La Figure 8.4 illustre un exemple de configuration de DLSw+ pour Token Ring. Le trafic provenant de Token Ring est acheminé par le pont à routage par la source de l'anneau local, vers un groupe d'anneaux avec pont à routage par la source, pour être ensuite pris en charge par DLSw+. Vous devez inclure une commande **source-bridge ring-group** qui spécifie une adresse d'anneau virtuel, ainsi qu'une commande **source-bridge** qui indique aux routeurs de transmettre le trafic par le pont du réseau Token Ring physique vers l'anneau virtuel.

DLSw+ supporte la terminaison du champ RIF, ce qui signifie que tous les dispositifs distants apparaissent comme étant connectés à l'anneau virtuel spécifié dans la commande **source-bridge**. Dans la Figure 8.4, tous les dispositifs connectés au routeur A apparaissent à l'hôte comme étant situés sur l'anneau virtuel 200. A l'inverse, le FEP apparaît au site distant comme étant situé sur l'anneau virtuel 100. Comme illustré dans cette figure, les anneaux virtuels spécifiés sur les routeurs homologues n'ont pas besoin de correspondre. Si plusieurs routeurs sont connectés au même anneau physique, comme c'est le cas pour les routeurs B et C, vous pouvez empêcher les paquets d'exploration en provenance du WAN de pénétrer sur l'anneau virtuel et d'être réinjectés sur le WAN, en spécifiant la même adresse de groupe d'anneaux sur chacun des routeurs.

Figure 8.4
Configuration simple de DLSw+ pour Token Ring.



Ethernet

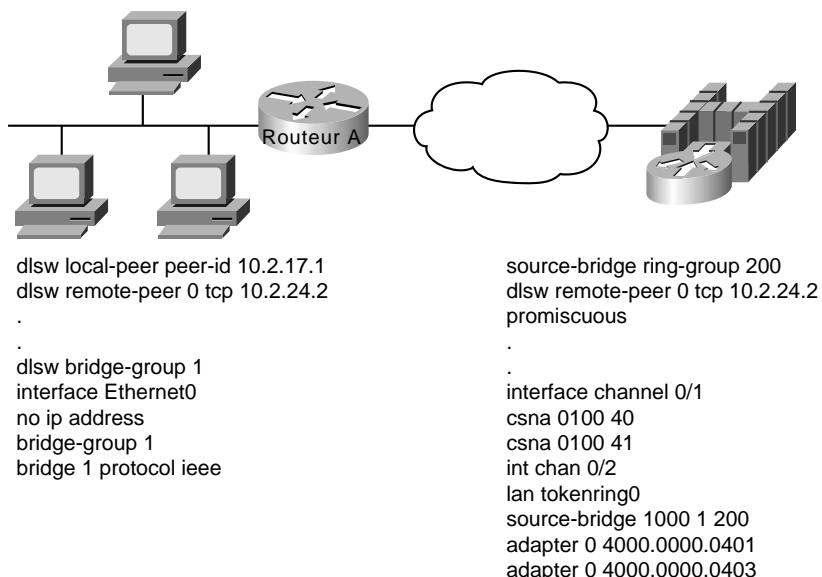
Le trafic qui provient d'un réseau Ethernet est pris en charge à partir du groupe de pont (bridge group) Ethernet local et transporté sur le réseau DLSw. DLSw transfère toujours les données dans un format non canonique. Dans la Figure 8.5, vous n'avez pas besoin de configurer le routeur gauche pour un pontage avec traduction ou de vous demander quel est le média situé de l'autre côté du WAN. DLSw procédera automatiquement à la conversion d'adresse MAC correcte pour le média de destination. Lorsque DLSw+ reçoit une adresse MAC de la part d'un dispositif connecté *via* Ethernet, il suppose qu'il s'agit d'une adresse canonique et la convertit dans un format non canonique pour le transport vers l'homologue distant. Sur ce dernier, l'adresse est transmise telle quelle au système terminal connecté *via* Token Ring, ou bien reconvertisse dans un format canonique si le média de destination est Ethernet. Lorsqu'une ressource SNA réside sur un réseau Ethernet, si vous configurez une adresse SNA de destination sur ce dispositif vous devez utiliser un format canonique. Par exemple, un dispositif 3174 connecté *via* Ethernet doit spécifier l'adresse MAC du FEP dans un format canonique. Si le format Token Ring ou non canonique de l'adresse MAC du FEP est 4000.3745.0001, le format canonique est 0200.4C12.0080.

Dans la Figure 8.5, les données sont transférées directement vers un routeur Cisco avec CIP, mais il pourrait s'agir de n'importe quel routeur compatible DLSw, et le système terminal SNA en amont pourrait être situé sur n'importe quel média supporté.

SDLC

La configuration de dispositifs SDLC est un peu plus complexe. Vous devez savoir s'il s'agit d'unités physiques PU 1, PU 2.0 ou PU 2.1. Pour un dispositif PU 2.0, vous devez connaître les identifiants IDBLK et IDNUM qui ont été spécifiés sur VTAM (*Virtual Telecommunication Access Method*) pour le dispositif en question, car le routeur joue un rôle plus important dans le traitement XID lorsqu'une unité PU 2.0 SDLC est impliquée. Vous devez savoir si le routeur représente l'extrémité principale ou secondaire de la ligne SDLC. De plus, si le raccordement vers le dispositif SNA en amont passe par un LAN, vous devez configurer l'adresse MAC de ce dispositif. Dans tous les cas, vous devez configurer une adresse MAC virtuelle qui sera mise en correspondance avec une adresse de sondage (polling) SDLC.

Figure 8.5
Configuration simple de DLSw+ pour Ethernet.



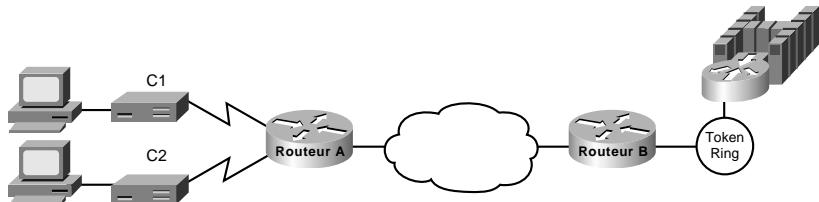
Dans la Figure 8.6, les dispositifs connectés *via* SDLC reçoivent chacun l'adresse 4000.3174.0000 comme adresse MAC virtuelle de base. Le routeur remplacera les deux derniers chiffres de l'adresse par l'adresse SDLC du dispositif. Le dispositif situé à l'adresse SDLC C1 présente l'adresse MAC 4000.3174.00C1, et le dispositif situé à l'adresse SDLC C2 présente l'adresse MAC 4000.3174.00C2. Comme dans cet exemple il s'agit de deux dispositifs PU 2.0, leur XID doit être configuré et correspondre aux identifiants IDBLK et IDNUM sur VTAM. De plus, le routeur assume toujours le rôle principal lorsqu'il est connecté en amont des dispositifs PU 2.0.

Le routeur peut être l'extrémité secondaire d'une ligne SDLC (par exemple, lorsqu'il se connecte à un FEP par l'intermédiaire de SDLC). Dans ce cas, spécifiez le mot clé **secondary** dans la commande **sdlc role**, et indiquez pour les dispositifs PU 2.1 le mot clé **xid-passthru** dans la commande **sdlc address**. Dans la version 11.0 ou ultérieure du système Cisco IOS, DLSw+ supporte les PU 2.0/2.1 multipoint. Dans la Figure 8.7, la configuration PU 2.0 multipoint inclut une commande **sdlc xid** pour chaque dispositif PU 2.0.

Pour les lignes multipoint avec une combinaison de dispositifs PU 2.0 et 2.1, spécifiez le mot clé **primary** dans la commande **sdlc role**. Pour les dispositifs PU 2.0, vous devez coder les références IDBLK et IDNUM dans la commande **sdlc xid**. Pour les dispositifs PU 2.1, vous pouvez omettre cette commande. Toutefois, dans la commande **sdlc address**, vous devez spécifier **xid-poll**. Sinon, lorsque tous les dispositifs sur une ligne sont de type PU 2.1, vous pouvez spécifier la commande **sdlc role prim-xid-poll**, et dans ce cas vous n'avez pas besoin de spécifier **xid-poll** pour chaque commande **sdlc address**.

Figure 8.6

Configuration simple de DLSw+ pour SDLC.

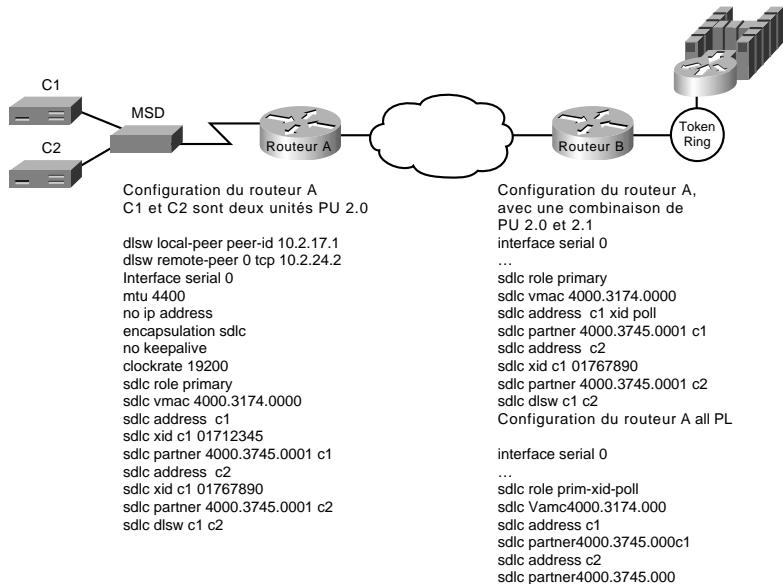


Configuration du routeur A
 dlsw local-peer peer-id 10.2.17.1
 dlsw remote-peer 0 tcp 10.2.24.2
 Interface serial 0
 encapsulation sdlc
 sdlc role primary
 sdlc vmac 4000.3174.0000
 sdlc address c1
 sdlc xid c1 01712345
 sdlc partner 4000.3745.0001 c1
 sdlc dlsw c1

interface serial1
 encapsulation sdlc
 sdlc role primary
 sdlc vmac 4000.3174.1000
 sdlc address c2
 sdlc xid c1 01767890
 sdlc partner 4000.3745.0001 c2
 sdlc dlsw c2

Figure 8.7

Configuration multipoint de DLSw+ pour SDLC.



Configuration du routeur A
 C1 et C2 sont deux unités PU 2.0
 dlsw local-peer peer-id 10.2.17.1
 dlsw remote-peer 0 tcp 10.2.24.2
 Interface serial 0
 mtu 4400
 no ip address
 encapsulation sdlc
 no keepalive
 clockrate 19200
 sdlc role primary
 sdlc vmac 4000.3174.0000
 sdlc address c1
 sdlc xid c1 01712345
 sdlc partner 4000.3745.0001 c1
 sdlc address c2
 sdlc xid c1 01767890
 sdlc partner 4000.3745.0001 c2
 sdlc dlsw c1 c2

Configuration du routeur A, avec une combinaison de PU 2.0 et 2.1
 interface serial 0
 ...
 sdlc role primary
 sdlc vmac 4000.3174.0000
 sdlc address c1 xid poll
 sdlc partner 4000.3745.0001 c1
 sdlc address c2
 sdlc xid c1 01767890
 sdlc partner 4000.3745.0001 c2
 sdlc dlsw c1 c2
 Configuration du routeur A all PL
 interface serial 0
 ...
 sdlc role prim-xid-poll
 sdlc Vamc4000.3174.000
 sdlc address c1
 sdlc partner4000.3745.000c1
 sdlc address c2
 sdlc partner4000.3745.000

QLLC

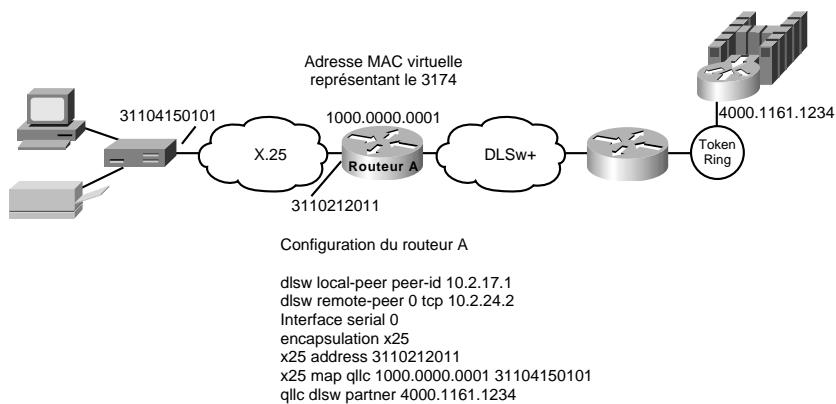
QLLC est le protocole de liaison de données utilisé par les dispositifs SNA pour se connecter aux réseaux X.25. Il s'agit d'un protocole ancien, qui a été développé par IBM pour permettre au NCP (*Network Control Program*, programme de contrôle de réseau) de supporter les connexions distantes sur X.25. La fonction logicielle sur le NCP qui supporte ce protocole est appelée Network Packet Switching Interface. Ce protocole tire son nom du bit Q utilisé dans l'en-tête X.25 pour identifier ses primitives. QLLC émule essentiellement SDLC sur X.25. Ainsi, DLSw+ réalise la conversion QLLC de façon semblable à la conversion SDLC. L'implémentation Cisco de DLSw+ a

prévu un support pour QLLC dans le système Cisco IOS version 11.0. Comme QLLC est plus complexe que Token Ring, Ethernet ou SDLC, nous en étudierons trois exemples dans cette section.

La Figure 8.8 illustre l'emploi de DLSw+ pour permettre aux dispositifs distants de se connecter à un réseau DLSw+ à travers un réseau public de commutation de paquets X.25. Dans cet exemple, tout le trafic QLLC est envoyé à l'adresse de destination 4000.1161.1234, qui représente l'adresse MAC du FEP. Le dispositif 3174 distant connecté *via* X.25 s'est vu attribuer une adresse MAC virtuelle 1000.0000.0001 qui a été associée à l'adresse X.121 du 3174 (31104150101) sur le routeur connecté au réseau X.25.

Figure 8.8

Configuration de DLSw+ pour QLLC, pour un seul dispositif de LAN en amont.



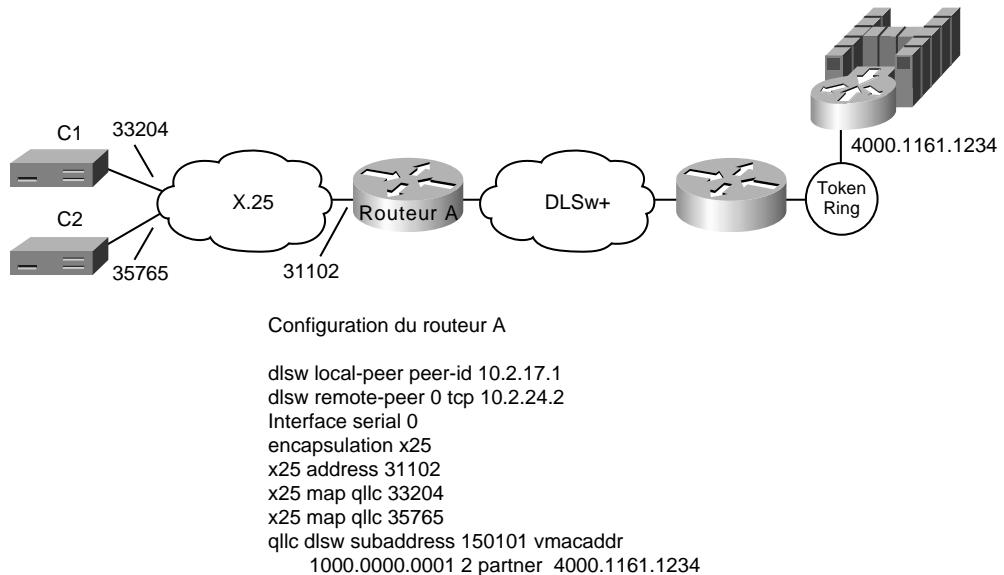
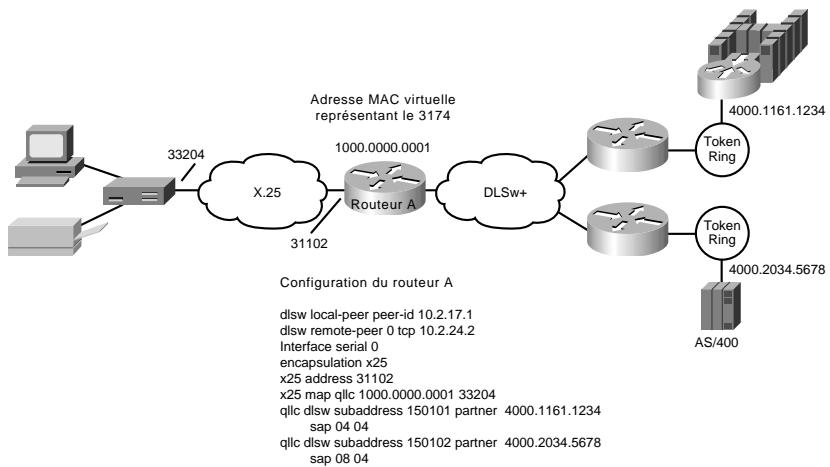
Dans la Figure 8.9, un seul 3174 doit pouvoir communiquer avec un AS/400 et un FEP. La sous-adresse 150101 est associée au FEP, et la sous-adresse 150102 est associée à l'AS/400. Si un appel X.25 arrive pour l'adresse 33204150101, il est mis en correspondance avec le FEP et transmis à l'adresse MAC 4000.1161.1234. Le 3174 apparaît au FEP comme étant une ressource de réseau Token-Ring possédant l'adresse MAC 1000.0000.0001. Il utilise un SAP source de 04 lorsqu'il communique avec le FEP.

Si un appel X.25 est reçu pour l'adresse 33204150102, il est associé à l'AS/400 et transmis en direction de l'adresse MAC 4000.2034.5678. Le 3174 apparaît à l'AS/400 comme étant une ressource Token Ring portant l'adresse MAC 1000.0000.0001. Le 3174 utilise un SAP source 08 lorsqu'il communique avec l'AS/400.

Dans la Figure 8.10, deux ressources X.25 souhaitent communiquer *via* leur réseau avec le même FEP. Sur le routeur connecté au nuage X.25, chaque requête de connexion X.25 pour l'adresse X.121 31102150101 est dirigée vers DLSw+. La commande **qllc dlsw** crée un pool de deux adresses MAC virtuelles, en commençant par 1000.0000.0001. Le premier circuit virtuel commuté ou CVC (Switched Virtual Circuit) établi sera associé à cette première adresse MAC virtuelle, et le second CVC sera mis en correspondance avec l'adresse MAC virtuelle 1000.0000.0002.

Figure 8.9

Configuration de DLSw+ pour QLLC, pour supporter plusieurs dispositifs de LAN en amont.

**Figure 8.10**

Configuration de DLSw+ pour QLLC offrant le support de plusieurs dispositifs en aval connectés via X.25 et communiquant par l'intermédiaire d'un réseau DLSw+ en amont.

Fonctionnalités avancées de DLSw+

Cette section présente les fonctionnalités avancées de DLSw+ ainsi que les avantages qu'elles procurent, et décrit dans quel contexte les employer. Exploitez les informations fournies ici pour déterminer les options que vous devez utiliser et apprendre à les configurer afin de répondre à vos besoins.

DLSw+ inclut des fonctionnalités permettant d'améliorer la disponibilité du réseau (équilibrage de charge, redondance et routeurs homologues de secours), d'optimiser les performances (options d'encapsulation), de réduire les diffusions générales (listes d'anneaux), et de construire des réseaux maillés (homologues interzones et groupes d'homologues). DLSw+ fournit aussi une fonctionnalité permettant d'exploiter au maximum les ressources du site central tout en limitant le coût associé aux services d'opérateur (homologues dynamiques). Les fonctionnalités avancées sont optionnelles et ne s'appliquent pas à tous les réseaux. Chacune d'elles inclut une indication stipulant son contexte d'utilisation.

Etablissement de connexion par des homologues DLSw+

Pour comprendre l'équilibrage de charge, il faut également savoir de quelle façon les routeurs homologues DLSw+ établissent des connexions et recherchent des ressources. Lorsqu'un routeur DLSw+ est activé, il établit tout d'abord une connexion avec chaque homologue distant configuré (à moins que le mot clé **passive** n'ait été spécifié, auquel cas il attend que l'homologue distant initie une connexion). Les routeurs homologues échangent ensuite des informations sur les services qu'ils offrent. Ces services comprennent aussi toutes les ressources configurées avec les commandes **dlsw icanreach** ou **dlsw icannotreach**. Après cet échange, les homologues DLSw+ demeurent inactifs jusqu'à ce qu'un système terminal envoie une trame d'exploration — une telle trame peut être du type SNA TEST ou XID, ou du type NetBIOS NAME-QUERY ou ADD NAME-QUERY. Cette trame est ensuite retransmise vers tous les homologues actifs et les ports locaux (à l'exception du port par lequel la trame est arrivée). Il est possible qu'un système terminal puisse être localisé par l'intermédiaire de plusieurs homologues distants ou ports locaux. Le chemin sélectionné pour un circuit dépend de certaines options de configuration avancées décrites dans cette section.

Équilibrage de charge et redondance

Si vous disposez de plusieurs routeurs de site central supportant DLSw+ pour l'équilibrage de charge ou la redondance, cette section contient d'importantes informations à ce sujet. Elle décrit de quelle façon équilibrer le trafic sur plusieurs routeurs de site central ou sur plusieurs ports d'un seul routeur. Cet équilibrage-ci ne se réfère pas à une répartition du trafic sur plusieurs liaisons WAN ou chemins IP. Il est réalisé par le protocole IP sous-jacent et est transparent pour DLSw+.

Si DLSw+ reçoit plusieurs réponses positives suite à une trame d'exploration, il peut placer en cache jusqu'à quatre homologues permettant d'atteindre un système terminal distant et jusqu'à quatre ports par l'intermédiaire desquels un système terminal local peut être joint. L'utilisation de ces entrées en cache est influencée par la commande **dlsw duplicate-path-bias**, qui spécifie si l'équilibrage de charge est réalisé ou non. Si c'est le cas, les chemins placés en cache (homologues distants ou ports locaux) sont choisis à tour de rôle par le processus d'établissement de circuit.

Si l'équilibrage de charge n'est pas spécifié, l'homologue sélectionne le premier chemin dans le cache et établit tous les circuits *via* cet itinéraire, sauf s'il est inaccessible. Le premier chemin dans la liste du cache peut être l'un des suivants :

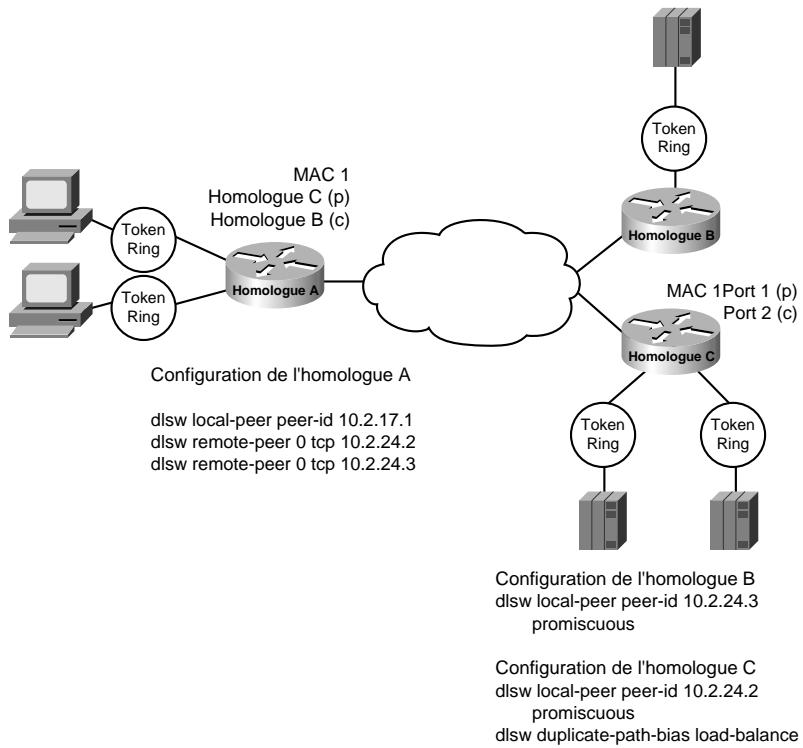
- l'homologue par lequel la première réponse positive a été reçue ;
- l'homologue représentant le coût le plus faible ;
- le port par lequel la première réponse positive a été reçue.

Le coût peut être spécifié au moyen de l'une de ces deux commandes : **dlsw local-peer** ou **dlsw remote-peer**. Lorsque la première commande est utilisée, le coût est communiqué aux homologues distants lors du processus d'échange des informations de services. L'exemple suivant illustre la manière dont cette information peut être exploitée pour contrôler les chemins empruntés par les sessions.

Dans la Figure 8.11, il y a deux passerelles de canal et trois cartes Token Ring qui peuvent être utilisées pour accéder aux applications sur le mainframe. Les trois cartes ont reçu la même adresse MAC. L'attribution d'adresses dupliquées est une technique courante permettant d'assurer l'équilibrage de charge et la redondance dans un environnement SRB. Elle fonctionne, car SRB suppose qu'il existe trois chemins menant au même dispositif et ne voit pas cela comme une duplication d'adresses de LAN. Par contre, cette technique ne fonctionne pas dans un environnement avec pont transparent.

Figure 8.11

Exemple de configuration avec entrées de cache créées lorsque toutes les passerelles de canal possèdent la même adresse MAC.



Dans cet exemple, l'homologue A est configuré avec deux commandes **dlsw remote-peer** pour les homologues B et C. L'homologue B spécifie un coût de 4 dans sa commande **dlsw local-peer** et l'homologue C indique un coût de 2. Ces informations de coût sont échangées avec A lors de l'échange des informations de services.

Lorsque le système terminal SNA (c'est-à-dire la PU) situé sur la gauche envoie un paquet d'exploration, A le transmet à B et à C. Ces derniers le retransmettent sur leurs réseaux locaux respectifs. B reçoit une réponse positive, et renvoie donc une réponse positive à A. C reçoit deux réponses positives (provenant de chacun des deux ports) et transmet une réponse positive à A. C prend note qu'il possède deux ports qu'il peut utiliser pour atteindre l'adresse MAC de la passerelle de canal, et A prend note qu'il possède deux homologues qu'il peut utiliser pour atteindre l'adresse MAC de la passerelle de canal.

L'homologue A transmet ensuite une réponse positive à la PU SNA et établit un circuit de bout en bout en utilisant C. Ce dernier est sélectionné parce qu'il possède le coût le plus faible. Lorsque la prochaine unité PU demandera une connexion avec la même adresse MAC, elle sera établie avec C, s'il est disponible. Il s'agit de la méthode utilisée par défaut pour gérer les chemins dupliqués avec DLSw+.

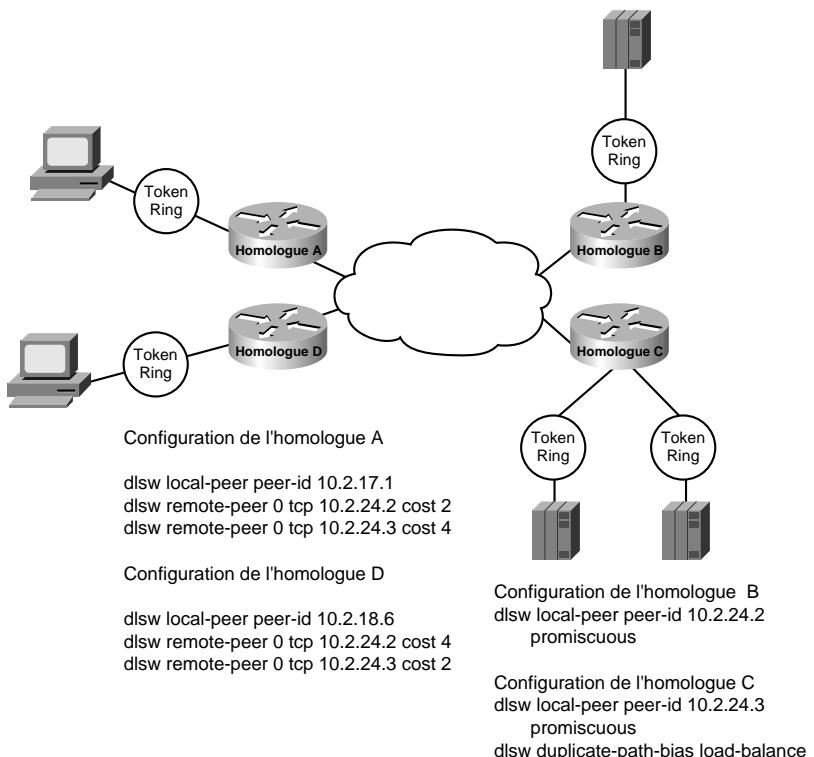
Sur l'homologue C, le premier circuit est établi en utilisant le port 1, mais le circuit suivant empruntera le port 2, car l'équilibrage de charge a été spécifié sur ce routeur à l'aide de la commande **dlsw duplicate-path-bias**. Chaque nouvelle PU SNA utilisera le chemin suivant dans la liste en cache.

La Figure 8.11 illustre la façon de privilégier un homologue par rapport à un autre lors de l'établissement de connexions distantes ; cependant, le site central équilibre le trafic sur toutes les cartes LAN d'une passerelle de canal donnée. Autrement, l'équilibrage peut être spécifié n'importe où pour répartir la charge sur tous les routeurs de site central, les passerelles de canal et les LAN. Notez que cette fonction n'exige pas que les systèmes terminaux soient connectés *via* Token Ring. Ils pourraient se connecter par l'intermédiaire de SDLC, Ethernet ou QLLC, et la fonctionnalité serait toujours opérante. La passerelle de canal du site central doit être connectée *via* un LAN (de préférence Token Ring). Les adresses MAC dupliquées pour les passerelles de canal sur Ethernet fonctionneront uniquement : 1) si vous disposez d'un segment unique Ethernet avec pont et d'un seul routeur DLSw+ pour chaque adresse MAC dupliquée ; 2) si vous utilisez l'équilibrage de charge à partir des sites distants. Ethernet ne disposant d'aucune fonctionnalité pour empêcher les bouclages, il faudra être prudent lors de la construction de réseaux redondants avec des réseaux locaux Ethernet. Les réseaux Token Ring peuvent s'appuyer sur SRB pour éviter les boucles.

Une autre méthode qui permet de spécifier le coût consiste à utiliser la commande **dlsw remote-peer**, comme illustré Figure 8.12. L'utilisation du mot clé **cost** au niveau de cette commande autorise différentes régions d'un pays à favoriser diverses passerelles de site central. De plus, vous devez indiquer ce mot clé si vous souhaitez répartir le trafic SNA sur plusieurs routeurs de site central, mais chaque site distant ne possède qu'une seule PU SNA (toutes les sessions logiques circulent sur le même circuit que celui de la session PU). Dans la Figure 8.12, l'homologue A favorise toujours l'homologue B et l'homologue D favorise toujours l'homologue C.

Figure 8.12

Configuration où le coût est spécifié avec la commande `dlsw remote-peer` au lieu de la commande `dlsw local-peer`.



Contrôle de la sélection d'homologue

Un homologue de coût plus élevé peut être utilisé pour une connexion, même lorsque celui de moindre coût est actif, s'il a répondu avant l'autre au paquet d'exploration. Si votre configuration de réseau dispose de cette possibilité, vous pouvez l'empêcher en définissant un temporisateur.

La spécification de la commande **dlsw explorer-wait-time** oblige DLSw+ à attendre le délai spécifié (par exemple, 1 seconde) avant de sélectionner un homologue pour établir les connexions. Ce temporisateur peut être défini sur le système Cisco IOS version 11.0, ou ultérieure. Avant cette version, il n'existe pas.

Homologues de secours

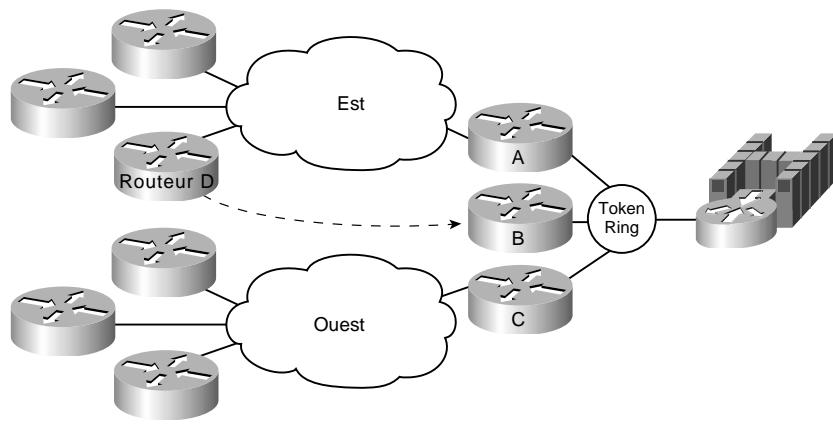
Disposer de plusieurs homologues actifs est un moyen de garantir un rétablissement dynamique et immédiat après la perte d'un routeur De site central. Toutefois, dans certaines configurations, il est préférable que l'homologue de secours ne soit actif que lorsqu'il est requis. Cela peut être le cas si le routeur De secours est situé sur un site redondant prévu pour une récupération après sinistre, ou lorsqu'il existe plus de 300 à 400 sites distants et qu'un seul routeur De site central représente la solution de secours pour plusieurs routeurs de site central.

Dans ce cas, utilisez la fonctionnalité d'homologue de secours (introduite avec Cisco IOS version 10.3, mais étendue avec la version 11.1). La Figure 8.13 illustre de quelle façon configurer un homologue de secours. Si vous souhaitez exploiter cette fonctionnalité, il faut employer la méthode d'encapsulation TCP ou FST (*Fast-Sequenced Transport*) pour accéder à l'homologue principal.

Cet exemple suppose l'existence de 400 sites distants. Tous les routeurs sur la côte est utilisent le routeur A comme routeur principal, et tous les routeurs sur la côte ouest utilisent C comme routeur principal. Dans les deux cas, le routeur De secours est B. La configuration illustrée est celle du routeur D, un des routeurs de la côte est. Ces derniers sont tous configurés avec les mêmes commandes **dlsw remote-peer**. Le routeur principal A et le routeur De secours B sont chacun configurés avec une commande **dlsw remote-peer**. B est configuré uniquement en tant que routeur De secours, et l'adresse IP du routeur qu'il soutient est spécifiée.

Dans l'éventualité d'une panne au niveau du routeur A, toutes les sessions SNA sont terminées, puis rétablies par l'intermédiaire du routeur B. Lorsque A redéveloppe disponible, toutes les nouvelles sessions sont établies à son niveau, mais celles déjà existantes passant par B sont maintenues jusqu'à ce que le temporisateur **linger** expire. L'omission du mot clé **linger** provoquera le maintien de ces sessions sur le routeur B jusqu'à ce qu'elles se terminent d'elles-mêmes. Ce mot clé peut être utilisé pour minimiser les coûts de liaison si le routeur De secours est accessible par l'intermédiaire d'une ligne commutée, mais laissera suffisamment de temps pour qu'un avertissement de l'opérateur puisse être envoyé à tous les utilisateurs finaux SNA.

Figure 8.13
Comment utiliser les homologues de secours pour améliorer la disponibilité d'un grand réseau DLSw+.



Configuration du routeur D

```

dlsw local-peer peer-id 10.2.17.1
dlsw remote-peer 0 tcp 10.2.24.2
dlsw remote-peer 0 tcp 10.2.24.3 backup-peer 10.2.24.2 linger 20
  
```

NOTE

Avant l'introduction de Cisco IOS version 11.1, lorsque l'homologue principal était à nouveau actif après une défaillance, toutes les sessions qui utilisaient le routeur De secours étaient immédiatement terminées, puis rétablies sur le routeur principal. Si ce n'est pas le comportement que vous souhaitez et que vous utilisez une version du système antérieure à la version 11.1, envisagez à la place l'emploi d'homologues actifs dupliqués (procédure décrite dans la section précédente).

Homologues de secours versus homologues actifs multiples

Les homologues de secours et les homologues actifs multiples (avec un homologue désigné comme routeur préféré et les autres comme routeurs possibles) représentent deux solutions de secours en cas de panne d'un routeur principal. L'une des principales différences de la solution d'homologues de secours est que les connexions ne sont pas actives tant qu'elles ne sont pas nécessaires. Supposez que vous ayez 1 000 bureaux d'agence, et que vous souhaitiez concevoir un réseau pour un coût minimal pouvant se rétablir dynamiquement en cas de défaillance de n'importe quel routeur De site central. Supposez aussi que quatre routeurs sur le site central soient suffisants pour traiter toute la charge de travail. Vous pouvez donc les installer en tant que routeurs principaux sur le site central et les définir pour qu'ils communiquent chacun avec 250 agences.

Pour satisfaire aux besoins en matière de disponibilité, une solution serait de recourir à plusieurs connexions d'homologues actives simultanément. Dans ce cas, il faut configurer chaque routeur Distant avec deux connexions d'homologues : l'une vers un routeur préféré et l'autre vers un routeur possible. Le premier est celui qui est configuré avec le coût le plus faible. Le second peut être le même routeur pour tous les sites distants, mais il doit dans ce cas avoir 1 000 connexions d'homologues. Le plus grand nombre de routeurs homologues qu'il nous a été donné de rencontrer est 400, et il s'agissait d'un environnement où le trafic était extrêmement lent. Bien que 1 000 connexions d'homologues inactives soient envisageables, elles pourraient imposer une forte charge sur le routeur Dès qu'il prend le relais d'un autre routeur. Une autre solution serait de disposer de plusieurs routeurs de site central comme routeurs possibles, mais ce ne serait pas la conception la plus rentable.

En utilisant un homologue de secours sur chaque site distant à la place d'une paire de connexions concurrentes vers deux routeurs, un routeur De secours sur un site central peut aisément soutenir n'importe quel autre routeur De site central. Aucune charge ne pèse sur le routeur De secours tant qu'un routeur principal n'est pas défaillant.

Options d'encapsulation

DLSw+ propose quatre options d'encapsulation qui varient en termes de chemin de traitement utilisé, de surcharge sur le réseau étendu et de média supporté. Ces solutions d'encapsulation sont TCP, FST, l'encapsulation directe et LLC2.

Encapsulation TCP

TCP est la méthode d'encapsulation du standard DLSw. C'est la seule à être spécifiée dans le RFC 1795 et à offrir autant de fonctionnalités. Elle assure une livraison fiable des trames ainsi qu'un acquittement local. C'est aussi la seule option qui propose un reroutage sans interruption après

panne. Vous pouvez tirer profit de la fonction d'ouverture de ligne à la demande qui permet d'ajouter dynamiquement de la bande passante si des liaisons principales atteignent un seuil de saturation préconfiguré. Cette méthode est recommandée pour la plupart des environnements, car ses performances sont généralement plus que suffisantes ; elle propose la plus haute disponibilité, et la surcharge de service générée n'a en principe aucun impact négatif sur les temps de réponse ou le débit.

TCP est commuté par processus et requiert donc plus de cycles de traitement que FST et que l'encapsulation directe. Un routeur Cisco 4700 exécutant DLSw+ avec l'encapsulation TCP peut commuter jusqu'à 8 Mbit de données par seconde. Cette solution peut donc répondre aux exigences de traitement de la plupart des environnements SNA. Lorsqu'un débit supérieur est requis, des routeurs supplémentaires ou d'autres options d'encapsulation peuvent être utilisés.

L'encapsulation TCP est la solution qui génère le plus de surcharge de service au niveau de chaque trame (20 octets pour TCP et 20 octets pour IP, en plus des 16 octets de l'en-tête DLSw). La compression d'en-tête TCP ou de la zone de données (payload) peut être utilisée pour réduire la quantité de bande passante requise, si nécessaire. Sur des liaisons à 56 Kbit/s ou plus, les 40 octets de surcharge rallongent de moins de 5,7 ms le délai d'un échange aller-retour ; l'impact est donc négligeable.

DLSw+ avec l'encapsulation TCP fournit l'acquittement local et le sondage local, et réduit également le trafic *keepalive* (contrôle d'activité de ligne) sur le réseau étendu. Cette solution supporte n'importe quel média de réseau local et étendu. L'équilibrage de charge sur plusieurs liaisons WAN ou chemins IP est possible, car TCP réorganise le trafic avant de le transmettre.

Quand vous utilisez l'encapsulation TCP, vous pouvez assigner différents types de trafic à différents ports afin de pouvoir gérer de façon précise la mise en file d'attente. On peut distinguer le trafic LLC2 en se basant sur les SAP (pour identifier le trafic NetBIOS et SNA), et les dispositifs SNA peuvent recevoir une priorité sur la base des adresses LOCADDR ou MAC/SAP. Voici un exemple de commande **dlsw remote-peer** spécifiant l'encapsulation TCP :

```
dlsw remote-peer 0 tcp 10.2.24.3
```

Encapsulation FST

FST est une option hautement performante utilisée sur les liaisons à grande vitesse (256 Kbit/s ou plus) lorsqu'un débit élevé est requis. Cette solution utilise un en-tête IP avec des numéros de séquence pour garantir que toutes les trames sont livrées dans l'ordre (les trames reçues dans le désordre sont ignorées et le système terminal doit les retransmettre).

Cette solution utilise la commutation rapide et non celle par processus, ce qui permet à DLSw+ de traiter davantage de paquets par seconde qu'avec l'encapsulation TCP. Comme FST n'utilise pas TCP, la taille de son en-tête est plus petite de 20 octets par rapport à celui de TCP.

Cependant, FST n'offre aucune fonctionnalité de livraison fiable des trames et d'acquittement local. Toutes les trames *keepalive* circulent de bout en bout. FST est supporté uniquement lorsque les systèmes terminaux se trouvent sur un réseau Token Ring. Deux homologues FST peuvent communiquer sur une liaison HDLC (*High-Level Data Link*), Ethernet, Token Ring, FDDI, ATM (*Asynchronous Transfer Mode*), ou Frame Relay. Certains médias de transport ne sont pas supportés avec les premières versions de maintenance FST peut assurer le reroutage pour contourner une ligne

défaillante, mais avec un risque d'interruption. De plus, l'équilibrage de charge sur plusieurs liaisons WAN ou chemins IP n'est pas recommandé avec FST, car les trames peuvent être délivrées dans le désordre, provoquant leur abandon. Les systèmes terminaux doivent alors retransmettre, ce qui réduit les performances globales du réseau.

Pour finir, la gestion de mise en file d'attente n'est pas aussi précise avec FST, car vous ne pouvez pas assigner différents types de trafics à différents ports TCP. Cela signifie que les algorithmes de gestion de files d'attente ne peuvent pas prendre en compte les SAP (le trafic NetBIOS et SNA est traité en tant que trafic LLC2), ni les adresses LOCADDR ou MAC. Voici un exemple de la commande **dlsw remote-peer fst** qui spécifie une encapsulation FST :

```
dlsw remote-peer 0 fst 10.2.24.3
```

Encapsulation directe

L'encapsulation directe est une option à faible surcharge de service pour le transport du trafic sur des liaisons point-à-point lorsque le reroutage n'est pas requis. Cette option est supportée sur des liaisons HDLC et Frame Relay. Elle inclut un en-tête DLSw de 16 octets et un en-tête de contrôle de liaison de données. Elle utilise la commutation rapide et non la commutation par processus, ce qui permet à DLSw+ de traiter davantage de paquets par seconde qu'avec l'encapsulation TCP.

Cette solution n'assure ni la livraison fiable des trames, ni l'acquittement local. Toutes les trames *keepalive* circulent de bout en bout. Elle est supportée uniquement lorsque les systèmes terminaux sont situés sur un réseau local Token Ring. Le reroutage n'est pas assuré.

Finalement, la gestion de mise en file d'attente n'est pas aussi précise avec cette solution, car vous ne pouvez pas assigner différents types de trafic à différents ports TCP. Cela signifie que lorsque vous utilisez l'encapsulation directe, les algorithmes de mise en files d'attente ne peuvent pas prendre en compte les SAP (le trafic NetBIOS et SNA est traité en tant que trafic LLC2), ni les adresses SDLC ou MAC.

Cette solution est parfois envisagée sur des lignes à très faible vitesse afin de réduire au minimum la surcharge de service, mais l'encapsulation TCP avec compression de la zone de données (payload) peut garantir une surcharge WAN inférieure sans les limitations liées à l'encapsulation directe. Voici un exemple de commande **dlsw remote-peer** spécifiant l'encapsulation directe sur une ligne HDLC :

```
dlsw remote-peer 0 interface serial 01
```

Voici un exemple de commande **dlsw remote-peer frame-relay** spécifiant l'encapsulation directe sur une ligne Frame Relay :

```
dlsw remote-peer 0 frame-relay interface serial 01 33 pass-thru
frame-relay map dlsw 33
```

Dans cet exemple, l'identifiant de connexion de liaison de données (DLCI) 33 sur l'interface série 1 est utilisé pour transporter le trafic DLSw. Le mot clé **pass-thru** indique que le trafic n'est pas acquitté localement. S'il n'est pas spécifié, le trafic est acquitté localement, ce qui implique qu'il est transporté par LLC2 pour garantir une livraison fiable. La section suivante décrit l'encapsulation LLC2.

Encapsulation LLC2 (DLSw Lite)

La solution d'encapsulation DLSw+ avec LLC2 est également connue sous le nom de DLSw Lite. Elle supporte de nombreuses fonctionnalités de DLSw+, dont l'acquittement local, la conversion de média, la réduction du trafic *keepalive* et la livraison fiable des trames, mais entraîne moins de surcharge de service (16 octets d'en-tête DLSw et 4 octets d'en-tête LLC2). Elle est actuellement supportée sur Frame Relay et suppose une configuration point-à-point sur Frame Relay (c'est-à-dire que le routeur homologue sur le site central est également le routeur WAN). Elle supporte les systèmes terminaux connectés *via* Token Ring, SDLC, QLLC ou Ethernet. Cette solution est commutée par processus et traite environ le même volume de trafic que l'encapsulation TCP.

Avec cette solution, les ruptures de liaison provoquent une interruption. Afin de garantir une meilleure disponibilité, il faut disposer de plusieurs homologues actifs de site central, ce qui permet d'assurer un rétablissement dynamique sans interruption en cas de perte d'un lien ou d'un homologue principal. Les homologues de secours ne sont pas encore supportés.

La gestion de files d'attente n'est pas aussi précise qu'avec l'encapsulation TCP, car il n'est pas possible d'assigner différents types de trafics à différents ports TCP. Cela signifie qu'avec DLSw Lite, les algorithmes de mise en files d'attente ne peuvent pas prendre en compte les SAP (le trafic NetBIOS et SNA est traité comme un trafic LLC2), ni les adresses SDLC ou MAC. Voici un exemple de commande **dlsw remote-peer frame-relay** spécifiant l'encapsulation LLC2 sur une ligne Frame Relay :

```
dlsw remote-peer 0 frame-relay interface serial 01 33  
frame-relay map llc2 33
```

NOTE

La commande **frame-relay map llc2 33** ne fonctionnera pas sur les sous-interfaces point-à-point. Il faut spécifier à la place le numéro DLCI dans la commande **frame-relay interface-dlci** et spécifier le même numéro dans la commande **dlsw remote-peer frame-relay**.

Voici un exemple de la commande **dlsw remote-peer** pour des sous-interfaces point-à-point :

```
dlsw remote-peer 0 frame-relay interface serial 0.1 60  
interface s0.1 point-to-point  
frame-relay interface-dlci 60
```

Surcharge de service liée à l'encapsulation

Les divers types d'encapsulations provoquent une surcharge de service différente au niveau de chaque trame. Avec TCP et LLC2, le trafic d'acquittement et *keepalive* est maintenu hors du réseau étendu, ce qui réduit le nombre de paquets. De plus, des techniques telles que la compression des données ou de l'en-tête, ainsi que l'empaquetage de plusieurs trames SNA dans un seul paquet TCP, peuvent réduire encore davantage la surcharge de service. Le pourcentage de surcharge généré par DLSw dépend de la méthode d'encapsulation utilisée.

La Figure 8.14 illustre le format de trame pour l'encapsulation TCP, FST, DLSw Lite, et directe. Le pourcentage indiqué représente la quantité de surcharge, en supposant des transactions SNA de 40 in, 1 920 out (un rafraîchissement d'écran) et de 40 in, 1 200 out. Avec des transactions plus petites, la surcharge est plus importante. Les chiffres de l'encapsulation TCP représentent les cas les plus

pessimistes, car ils supposent que chaque unité d'information de chemin SNA (PIU) est encapsulée dans un paquet TCP distinct. En fait, s'il y a plus d'une PIU SNA dans la file de sortie, plusieurs trames seront encapsulées dans un seul paquet TCP, ce qui réduit la surcharge de service. Les chiffres ne prennent pas en compte le fait que DLSw+ élimine les paquets *keepalive* de contrôle d'activité de ligne et ceux d'acquittement.

Figure 8.14
Format de trame et surcharge de service par paquet pour divers types d'encapsulations et tailles de transaction.

	Encapsulation	40/1920		40/1200	
		SDLC	LAN	SDLC	LAN
TCP	DLC IP TCP DLSw Données	5.7%	4.5%	9%	7%
FST	DLC IP DLSw Données	3.7%	2.4%	5.8%	3.9%
Lite	FR LLC2 DLSw Données	2%	1%	3.2%	1.3%
Directe	FR DLSw Données	1.8%	.6%	2.9%	1%

La surcharge effective par paquet de DLSw pour le trafic LAN est inférieure à celle de SDLC, car DLSw+ élimine le besoin de transporter les adresses MAC et les informations RIF dans chaque trame. DLSw ne transporte pas ces données, car l'identifiant de circuit DLSw (portion de l'en-tête DLSw de 16 octets) est utilisé pour la correspondance de circuit. La surcharge liée aux adresses MAC et aux informations RIF peut sinon représenter de 12 à 28 octets de données. Les pourcentages de la figure supposent une surcharge minimale (c'est-à-dire informations RIF non comprises).

Listes de ports

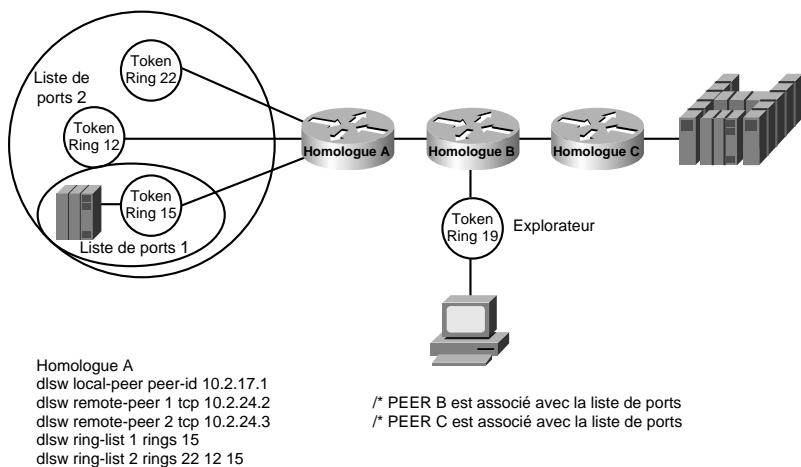
Les listes de ports vous permettent de créer des anneaux virtuels ou des domaines de diffusion sur un réseau DLSw+. Vous pouvez les utiliser pour contrôler vers quelle destination les messages en diffusion générale sont transmis. Par exemple, dans la Figure 8.15, il y a trois anneaux sur le site de distribution (où se situe l'homologue A).

Tous les anneaux comportent des systèmes terminaux SNA, mais l'anneau 15 est le seul qui connecte des serveurs NetBIOS. L'agence reliée à l'homologue B a besoin d'accéder aux serveurs NetBIOS, mais pas aux autres anneaux. La fonction de listes de ports permet de maintenir les diffusions générales provenant de l'homologue B en dehors des anneaux 12 et 22 (l'empêchant de communiquer avec les dispositifs situés sur ces deux anneaux).

A l'aide de ces listes, vous pouvez opérer une distinction entre les différents ports Token Ring et ports série, mais tous les ports Ethernet sont traités comme une seule entité (groupe de pont Ethernet).

Figure 8.15

Listes d'anneaux utilisées pour limiter des domaines de diffusion sur un réseau DLSw+.



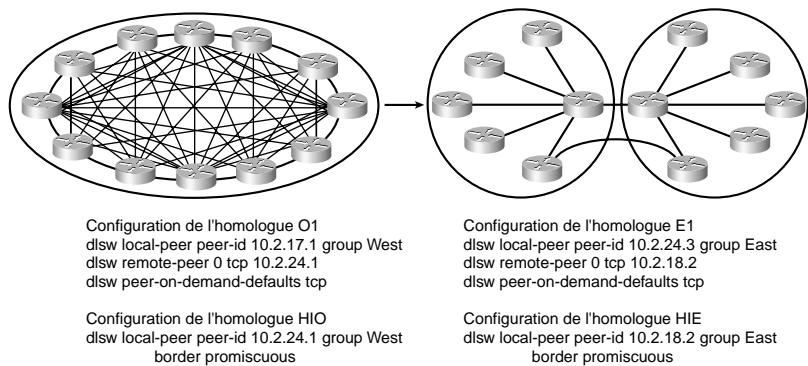
Groupes d'homologues, homologues interzones, homologues à la demande

Les groupes d'homologues et les homologues interzones peuvent être utilisés pour minimiser le nombre de connexions d'homologues requises pour établir une communication any-to-any. Avant l'introduction des homologues interzones, deux routeurs DLSw qui avaient besoin de communiquer devaient posséder une connexion d'homologues active en permanence. Cette connexion est exploitée pour rechercher des ressources et transporter le trafic. Sur un réseau totalement maillé de n routeurs, cela nécessite $n(n - 1) / 2$ connexions TCP. La configuration est complexe et génère un trafic d'exploration superflu. Pour régler ce problème, DLSw+ supporte le concept de groupe d'homologues et d'homologues interzones. Un groupe d'homologues est un groupe arbitraire de routeurs comprenant un ou plusieurs homologues interzones désignés. Ces derniers sont reliés à chaque routeur de leur groupe et à des homologues interzones situés dans d'autres groupes. Le rôle d'un tel homologue est de transmettre les paquets d'exploration au nom des autres routeurs.

Utilisez les groupes d'homologues et les homologues interzones uniquement lorsque vous avez besoin d'une communication agence vers agence entre des systèmes terminaux NetBIOS ou APPN. Dans la Figure 8.16, le réseau "avant" illustre les connexions TCP requises pour obtenir une connectivité totalement maillée sans l'utilisation d'homologues interzones. Sans ce type d'homologues, chaque fois qu'un routeur ne trouve pas une ressource dans son cache il doit créer une trame d'exploration et la reproduire pour chaque connexion TCP. Il en résulte un trafic d'exploration excessif sur les liaisons WAN et une charge de traitement importante au niveau du routeur.

Après avoir configuré les homologues interzone et les groupes d'homologues, il est possible d'obtenir une même connectivité totalement maillée, mais cette fois sans surcharge. Dans le réseau "après", les deux groupes d'homologues sont définis en tant que groupes Ouest et Est. Au sein de chaque groupe, un ou plusieurs routeurs sont configurés en tant qu'homologues interzone. Chaque routeur homologue au sein du groupe Ouest établit une connexion d'homologues avec l'homologue interzone Ouest (HIO). De la même manière, chaque routeur du groupe Est établit une connexion d'homologues avec l'homologue interzone Est (HIE).

Figure 8.16
Utilisation d'homologues interzones et de groupes d'homologues pour réduire le nombre de connexions TCP requises tout en maintenant une connectivité any-to-any totale.



Les homologues interzone établissent une connexion d'homologues entre eux. Lorsqu'un routeur Du groupe Ouest doit trouver une ressource, il envoie un seul paquet d'exploration à son homologue interzone. Celui-ci transmet le paquet d'exploration à chaque homologue membre de son groupe et à tous les autres homologues interzone. Le HIE qui reçoit le paquet le transmet à chaque routeur De son groupe. Lorsque la ressource est trouvée (dans ce cas sur E1), une réponse positive est envoyée vers l'origine (O1) via les deux homologues interzones. A cette étape, O1 établit une connexion d'homologues directe vers E1. Les connexions d'homologues qui sont établies par l'intermédiaire d'homologues interzones sans l'avantage de la préconfiguration sont appelées *connexions d'homologues à la demande*. Les règles gérant l'établissement d'homologues à la demande sont définies par les commandes **dlsw peer-on-demand-defaults tcp** sur chaque routeur.

Homologues dynamiques

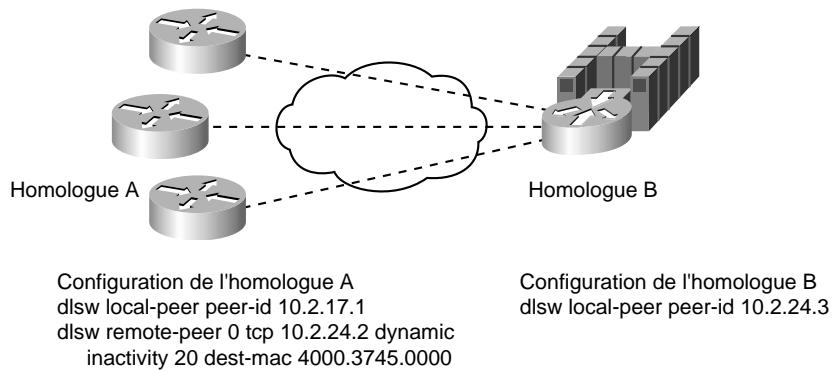
Les homologues dynamiques (fonction introduite avec Cisco IOS version 11.1) sont configurés en tant qu'homologues distants uniquement connectés lorsque des circuits les utilisent. Quand une commande **dlsw remote-peer** spécifie le mot clé **dynamic**, l'homologue distant n'est activé que si un système terminal envoie une trame d'exploration qui satisfait à toutes les conditions de filtrage spécifiées par la commande. Une fois la connexion dynamique établie, le paquet d'exploration est transmis à l'homologue distant. Si la ressource est localisée, un circuit est établi et l'homologue distant demeure actif jusqu'à ce que tous les circuits qui l'utilisent se terminent et que cinq minutes se soient écoulées. Vous pouvez spécifier le mot clé **no-lrc** pour modifier le délai à observer en choisissant une valeur autre que cinq minutes. Optionnellement, l'homologue distant peut être configuré pour être déconnecté lorsqu'il n'y a aucune activité sur les circuits pendant un certain temps préconfiguré (temporisateur d'inactivité).

Des filtres permettant de réduire le nombre de paquets d'exploration envoyés vers un homologue distant peuvent être inclus dans les commandes **dlsw remote-peer**. Ces filtres servent également à empêcher l'activation d'un homologue dynamique. Cette commande permet de pointer vers des listes de SAP, d'adresses MAC, de noms NetBIOS, ou de filtres de déplacement binaire (byte offset). Avec cette commande, vous pouvez aussi prévoir une adresse MAC pour un homologue dynamique qui ne sera activé que si un paquet d'exploration est envoyé vers l'adresse spécifiée. La Figure 8.17 illustre l'utilisation de cette fonction. L'homologue dynamique n'est connecté que si

une trame d'exploration est reçue à destination de l'adresse MAC du FEP. Après l'établissement de la connexion, celle-ci sera libérée, ainsi que les circuits qui l'utilisent, si aucune activité n'est détectée pendant 20 minutes, en raison du paramètre **inactivity 20** spécifié.

Figure 8.17

Des routeurs DLSw+ configurés pour tirer profit de la fonction d'homologue dynamique.



Contexte d'utilisation des homologues dynamiques

Vous pouvez utiliser des homologues dynamiques si vous disposez d'un grand réseau sans pour autant avoir besoin que tous les sites distants soient connectés en même temps. Cela vous permet ainsi de réduire le nombre de routeurs de site central nécessaires pour supporter le réseau. Vous pouvez également recourir aux homologues dynamiques pour établir des communications occasionnelles entre sites distants. Ces homologues diffèrent des homologues à la demande en ce qu'ils doivent être préconfigurés. Pour finir, ils peuvent aussi être utilisés sur des réseaux de petite taille pour ouvrir une ligne lors d'un processus de reprise après erreur.

Routage SNA par ouverture de ligne à la demande

Le routage SNA par ouverture de ligne à la demande (DDR, *Dial-on-Demand Routing*) désigne la fonctionnalité de DLSw+ qui permet de transférer des données SNA sur une ligne commutée et de la libérer automatiquement lorsqu'il n'y a plus de données à transférer. La session SNA demeure active. Pour utiliser cette fonctionnalité, configurez la commande **dlsw remote-peer** de la façon suivante :

```
dlsw remote-peer adresse-liste tcp adresse-ip dynamic keepalive 0
    timeout secondes
```

Le mot clé **dynamic** est optionnel, mais recommandé, car il empêche l'établissement d'une connexion inutile par l'homologue distant. L'option **dynamic** a été décrite dans la section précédente et peut être combinée avec les options **dmac-out** ou **dmac-output-list** pour la commande **dlsw remote-peer** afin de garantir que les connexions d'homologues sont activées uniquement lorsqu'elles sont souhaitées (par exemple, lorsqu'un dispositif tente de localiser le FEP).

Le mot clé **keepalive** est requis. DLSw+ acquitte localement le trafic SNA (ou plus précisément, SDLC ou LLC2) pour qu'aucune trame d'acquittement de contrôle de liaison de données ou de surveillance RR "receveur prêt" (*Receiver Ready*) n'active la ligne commutée de façon involontaire.

Toutefois, les homologues DLSw+ s'envoient périodiquement des messages *keepalive*, ce qui provoque l'activation de la ligne. L'option **keepalive** permet de spécifier la fréquence d'échange de ces messages. La valeur 0 indique qu'aucun message *keepalive* n'est envoyé et que, par conséquent, la ligne commutée n'est pas maintenue active. Vous devez spécifier la valeur 0 sur les *deux* homologues, c'est-à-dire que vous devez soit spécifier les routeurs distants à la fois sur le routeur local et sur le routeur Distant DLSw+, soit utiliser la commande **prom-peer-default** pour configurer **keepalive** à zéro pour toutes les connexions d'homologues transparentes (promiscuous). Cette commande possède les mêmes options que la commande **peer-on-demand-defaults** et est disponible sur les versions de maintenance les plus récentes de DLSw+.

Le mot clé **timeout** est recommandé. En l'absence des messages *keepalive* d'homologues, DLSw+ repose sur les temporisateurs TCP pour déterminer lorsque la session SNA est terminée. TCP considérera qu'il a perdu un partenaire seulement s'il ne reçoit pas d'acquittement de sa part après avoir envoyé des données. Par défaut, le protocole peut attendre jusqu'à 15 minutes la réception d'un acquittement avant de libérer la connexion. Par conséquent, lorsque le paramètre **keepalive** indique une valeur **0**, vous devez également définir le mot clé **timeout**, qui représente le temps d'attente du protocole (en secondes) avant la déconnexion. Le temporisateur devrait indiquer une valeur suffisamment longue pour permettre à l'acquittement de traverser la liaison dans les cas de congestion moyenne ou forte, mais suffisamment courte également pour limiter le temps nécessaire au protocole pour se rétablir après une interruption sur le réseau. Les connexions de contrôle de liaison de données de SNA attendent généralement 150 à 250 secondes avant d'entreprendre l'action prévue après expiration du temporisateur.

Autres considérations

Outre le fait d'empêcher le trafic des messages *keepalive* d'activer la ligne RNIS, vous devez aussi vous inquiéter des mises à jour de routage. Pour empêcher l'activation de la ligne par les mises à jour des tables de routage dans les environnements avec une configuration *hub and spoke* (en rayon autour d'un point central), utilisez des routes statiques. Sinon, vous pouvez utiliser le protocole RIP (*Routing Interface Protocol*) version 2 ou le routage IP à la demande, depuis les agences vers le site central. Le routage à la demande ou ODR (*On-Demand Routing*) est un mécanisme qui assure un routage IP à faible surcharge de service pour les sites de second niveau. Définissez le routage RIP version 2 ou le routage ODR sur l'interface RNIS du routeur central en mode passif. Redistribuez ensuite les itinéraires RIP version 2 ou ODR vers le protocole de routage principal (Enhanced IGRP ou OSPF). Cela vous permet de disposer de plusieurs routeurs sur le site central pour l'équilibrage de charge et la redondance. Ensuite, la route sera installée dynamiquement, quel que soit le routeur qui reçoit l'appel du site distant. Sur le site distant, le protocole de routage (RIP ou ODR) doit être rejeté de la liste du numéroteur.

Pour les topologies maillées, vous pouvez réduire au minimum les mises à jour de tables de routage en utilisant un protocole à vecteur de distance, comme RIP ou IGRP, en combinaison avec la fonction de routage *snapshot* de Cisco. Le routage *snapshot* empêche que les mises à jour de routage ordinaires n'activent la connexion RNIS. Les modifications dans les tables de routage sont envoyées soit lorsque le lien est ouvert par un trafic provenant de l'utilisateur final, soit en respectant un intervalle régulier configurable. Ce routage supporte non seulement les mises à jour de routage IP, mais aussi le routage Novell IPX et les mises à jour SAP.

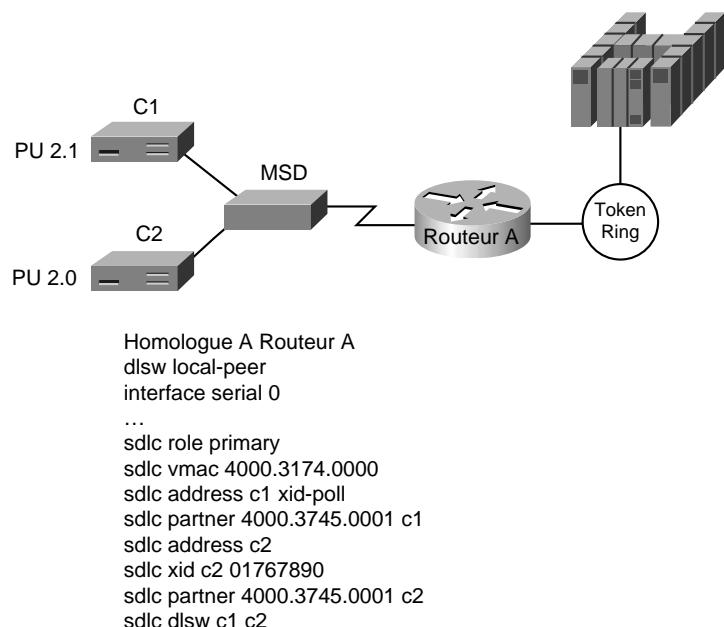
De nombreuses implémentations NetBIOS utilisent des messages *keepalive* de session (outre ceux du contrôle de liaison de données) pour maintenir les sessions. Aussi, la fonction DDR peut ne pas fonctionner avec NetBIOS (les messages garderont la ligne activée).

Commutation locale

La commutation locale (disponible avec Cisco IOS version 11.1 ou ultérieure) autorise un seul routeur à assurer la conversion de média entre SDLC et Token Ring, et entre QLLC et un LAN. Cela peut s'avérer utile dans les environnements qui nécessitent une conception de réseau SNA simplifiée et une disponibilité améliorée. Par exemple, en convertissant SDLC vers Token Ring, moins de trames FEP d'extension sont nécessaires ; les déplacements, les ajouts, les modifications sont plus facilement réalisés, et le rétablissement suite à une défaillance de FEP ou de coupleur d'interface Token Ring (TIC, *Token Ring Interface Coupler*) peut être automatique (en utilisant les adresses de TIC dupliquées). La commutation locale peut être exploitée pour connecter des dispositif SDLC directement à un routeur Cisco avec une carte CIP. Elle peut également être employée dans le cadre d'un réseau étendu sur lequel l'agence distante possède des dispositif SNA sur des réseaux locaux, mais lorsque le FEP du site central nécessite quand même la connectivité série (par exemple, lorsque le FEP est un routeur Cisco 3725). Pour utiliser la commutation locale, omettez les commandes **dlsw remote-peer**. Avec la commande **dlsw local-peer**, l'identifiant d'homologue est inutile. La Figure 8.18 illustre un exemple de réseau avec sa configuration.

Figure 8.18

Configuration de la commutation locale dans un environnement combinant des unités PU 2.0 et 2.1.



Résumé

Ce chapitre a présenté DLSw+ en fournissant des descriptions accompagnées d'exemples de configuration pour vous permettre de concevoir rapidement des réseaux DLSw+ simples. Il a passé en revue les composants essentiels des diverses fonctionnalités de la commutation de liaisons de données (DLSw+) et décrit les extensions incluses dans DLSw+ par rapport au standard DLSw. Enfin, il a présenté les fonctionnalités avancées de DLSw+, ses avantages et ses divers contextes d'utilisation.

9

Conception et configuration avec CIP

Par George Sackett et Nancy Sackett

Ce chapitre est extrait du livre (en langue anglaise) *Internetworking SNA with Cisco Solutions*, publié par Cisco Press.

Les fonctionnalités du CIP (*Channel Interface Processor*, processeur d'interface de canal) et du CPA (*Channel Port Adapter*, adaptateur de port de canal) de Cisco autorisent une connexion directe par canal à un mainframe IBM. Le CIP est disponible pour les routeurs Cisco 7000 et 7500. La carte CPA est disponible uniquement pour les routeurs Cisco 7200. Pour notre propos, nous nous référerons uniquement au CIP comme solution de connexion au mainframe. Toutes les caractéristiques, fonctions et commandes utilisées pour se connecter à des ressources de mainframe via un routeur Cisco doté du CPA sont supportées comme pour le CIP.

La connexion directe d'un routeur Cisco à un canal de mainframe permet au routeur d'exécuter les fonctions présentées ci-dessous et qui n'étaient avant assurées que par les contrôleurs FEP IBM 3745 et Interconnect Controller IBM 3172 :

- connexion d'équipements reliés par LAN aux applications TCP/IP ou SNA situées sur le mainframe ;
- fonction de décharge *TCP/IP Offload* de IBM TCP/IP pour MVS ou de Cisco IOS pour S/390 ;
- fonction MPC (*Multipath Channel*) ;
- fonction CLAW (*Common Link Access for Workstations*) pour l'accès TCP/IP à un mainframe ;
- fonction Cisco SNA (CSNA) permettant le transport de SNA et APPN ISR vers VTAM ;

- Fonction CMPC (*Cisco Multipath Channel*) pour le support des données de APPN ISR et APPN HPR ;
- connexion *via* une carte de canal parallèle PCA (*Parallel Channel Adapter*) ;
- connexion *via* une carte ECA (*ESCON [Enterprise System Connection] Channel Adapter*).

Outre ces fonctionnalités, le système Cisco IOS offre des options de connectivité avancées par l'intermédiaire des fonctions suivantes non présentes sur les contrôleurs FEP IBM 3745 et Interconnect Controller IBM 3172 :

- fonction TCP Assist pour décharger le mainframe du traitement des sommes de contrôle TCP/IP ;
- support pour héberger le serveur TN3270 sur le routeur ;
- correspondance de priorité et de type de service (ToS) IP pour les connexions TN3270 ;
- support de APPN HPR sur le routeur Cisco ;
- support pour le serveur NCIA sur le routeur Cisco ;
- support pour DLSw+ sur le routeur Cisco ;
- support pour APPN DLUR/DLUS.

Le support complet de toutes ces fonctions ainsi que de celles vues précédemment pour le transport de données SNA sur des WAN multimédias permet au routeur Cisco connecté *via* canal d'être proposé comme solution de remplacement totalement fonctionnelle pour les contrôleurs IBM 3745 ou 3172, ainsi que pour la plupart d'autres équipements de passerelle de canal.

NOTE

Bien que CIP gère concurremment la connectivité SNA, APPN et TCP/IP avec le mainframe, ce chapitre traite seulement des options de communication avec SNA et APPN.

Critères de conception

La carte processeur Cisco CIP supporte de nombreuses fonctions de connexion à un mainframe d'IBM pour SNA. Avec la possibilité d'utiliser ESCON, il est possible d'obtenir une connectivité variée avec le mainframe à partir d'un seul CIP et d'améliorer ainsi sa disponibilité pour les sessions SNA en aval. L'hôte doit utiliser EMIF pour permettre au CIP d'être relié à plusieurs partitions logiques (LPAR) avec un seul canal de connexion. Les points suivants font partie des facteurs à considérer lors de l'implémentation du CIP :

- Quelles sont, parmi les nombreuses fonctions de transport de SNA du système IOS, celles qui sont actuellement implémentées et quelles sont celles qui sont prévues ?
- Quelle est la couche de l'architecture d'interconnexion du routeur Cisco qui est la plus appropriée pour soutenir le transport de SNA vers le routeur Cisco CIP : la couche centrale, d'accès ou de distribution ?
- Combien de routeurs CIP et d'interfaces CIP sont-ils nécessaires pour gérer le trafic SNA vers le mainframe ?

- Quelle est l'influence sur les besoins, en matière de mémoire de traitement du routeur et de mémoire CIP, que peut avoir le support du trafic SNA sur la connexion CIP ? Cette question est importante lorsque des trames LLC2 doivent être transportées vers la connexion *via* une méthodologie par pont.
- Le réseau SNA est-il un mélange de routage de sous-zone SNA et de APPN ISR/HPR ou une variante de cette configuration ?
- Quel est le niveau de besoins de recourir à une procédure de reprise sans interruption ou automatique du mainframe au moyen d'une configuration offrant une haute disponibilité ?

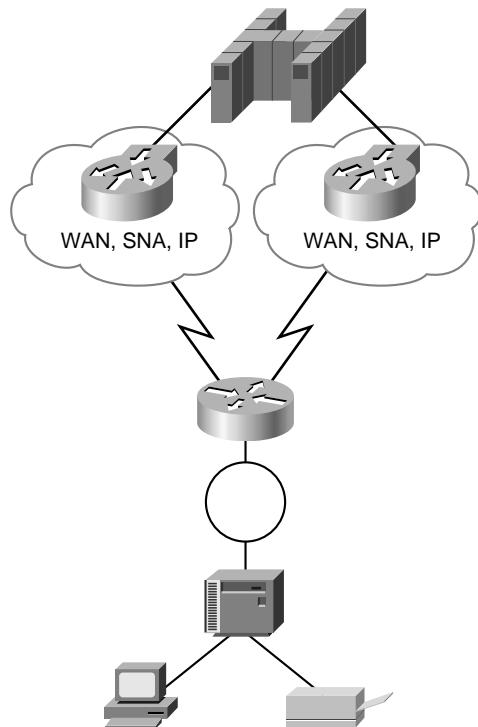
Il existe trois configurations fonctionnelles typiques permettant d'implémenter des routeurs Cisco CIP, comme vous le verrez dans les sections suivantes.

Concentration des fonctions sur un routeur CIP

Le routeur Cisco CIP fournit toutes les fonctions nécessaires à la connexion avec le mainframe. Cela peut englober tous les services de transport de SNA : DLSw+, RSRB, SDLLC, STUN, Frame Relay et APPN, en même temps que le support de TCP/IP. La Figure 9.1 illustre ce type de configuration. Si cette solution est envisagée, elle convient dans le cadre de petits réseaux comprenant au maximum 50 emplacements distants. Pour garantir la disponibilité, il faut aussi implémenter plus d'un routeur CIP afin d'offrir un soutien principal pour certains des sites distants.

Figure 9.1

Connectivité avec le mainframe IBM avec un routeur CIP réunissant toutes les fonctions.

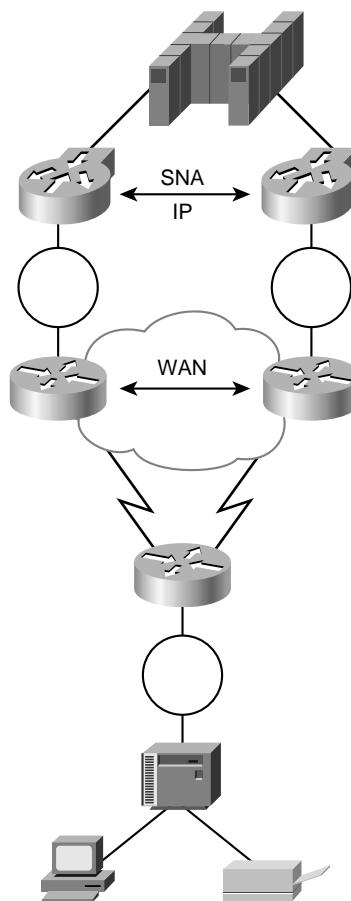


Combinaison du CIP et de SNA

Sur les réseaux où le nombre de connexions non SNA avec le mainframe *via* le CIP est minimal (c'est-à-dire FTP ou TCP), déplacer le traitement de service WAN vers les routeurs de niveau LAN permet de garantir les performances et le débit des routeurs CIP. Avec la configuration illustrée Figure 9.2, un routeur CIP peut servir des centaines d'emplacements distants. Cette conception isole la réplication des diffusions broadcast multiprotocoles du traitement SNA. Elle offre, de plus, davantage d'options de conception pour assurer la disponibilité, par la mise en œuvre d'un LAN comme épine dorsale de centre de données avec plusieurs routeurs CIP connectés à plusieurs routeurs WAN afin de relier les sites du réseau étendu. Dans cette configuration, les routeurs CIP traitent aussi bien les trames LLC2 que les paquets IP.

Figure 9.2

Connectivité CIP et SNA avec le mainframe IBM.

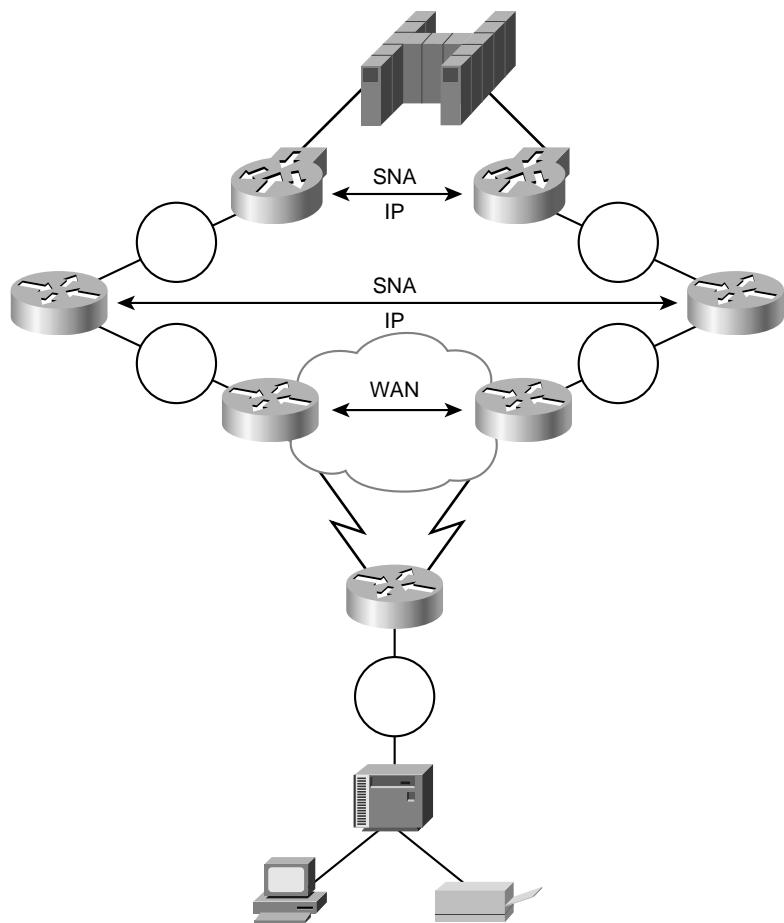


CIP en solo

Il est possible d'exploiter CIP pour traiter uniquement le trafic SRB LLC2 et IP par l'intermédiaire d'un cloisonnement supplémentaire de services. Le trafic SRB sur un routeur est commuté au lieu

d'employer DLSw+ ou APPN/DLUR, qui sont traités par le processeur principal du routeur. Dans une telle configuration (voir Figure 9.3), les routeurs ne gérant que SNA sur le LAN backbone du centre de données sont les homologues (*peer*) DLSw+ pour les sites distants. Ils transportent les trames SNA reçues vers les routeurs CIP au moyen de SRB. Quant aux routeurs WAN, ils livrent le trafic basé IP directement aux routeurs CIP. Le CIP gère 6 000 sessions PU SNA, ou même davantage, avec ce type de connexion.

Figure 9.3
Connectivité SRB et IP seul
avec le mainframe IBM.



Configurations de conception

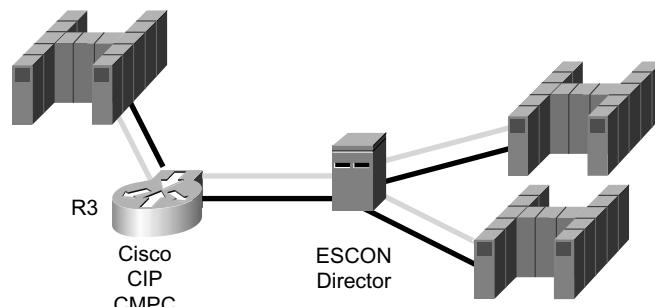
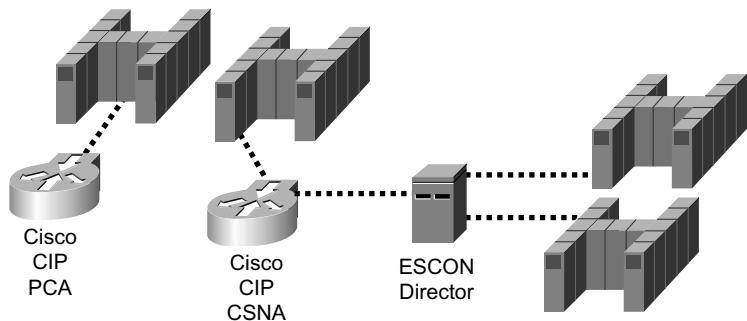
Les informations de configuration données ici concernent l'emploi d'un routeur Cisco CIP pour assurer la connectivité avec un mainframe à la place d'un FEP IBM 3745. Les exemples de configuration couvrent de nombreux mécanismes de transport SNA déjà étudiés, en illustrant l'exploitation du CIP comme solution de remplacement de l'IBM 3745 en tant qu'adresse de destination MAC pour établir une connexion SNA.

Configurations avec PCA, ESCON et MPC

La Figure 9.4 illustre les diverses options de connexion à un mainframe IBM à partir d'un routeur Cisco CIP. Le premier routeur se connecte directement à l'hôte au moyen d'une connexion *via* une carte PCA (*Parallel Channel Adapter*) *Bus-and-Tag*. Le débit offert par cette interface est d'environ 4,5 Mbit/s.

Figure 9.4

Configurations avec PCA, ESCON et MPC pour la connectivité entre CIP et mainframe.



— Canal de lecture
— Canal d'écriture
----- Canal de lecture/écriture

La Figure 9.4 illustre avec le deuxième routeur, la connectivité entre CIP et mainframe à l'aide de cartes ECA (*ESCON Channel Adapter*). Une connexion est établie directement *via* ECA et l'autre utilise *ESCON Director*. Cette technologie permet d'accéder à plusieurs partitions logiques (LPAR) ou à plusieurs mainframes au moyen d'une seule connexion ESCON à partir du routeur. Le dispositif *ESCON Director* est en quelque sorte un commutateur. Les interfaces PCA et ECA utilisent chacune un seul canal pour les opérations de lecture et d'écriture avec le mainframe.

NOTE

Le CIP fonctionne aussi avec EMIF pour autoriser des accès à plusieurs LPAR sans l'usage du commutateur ESCON Director.

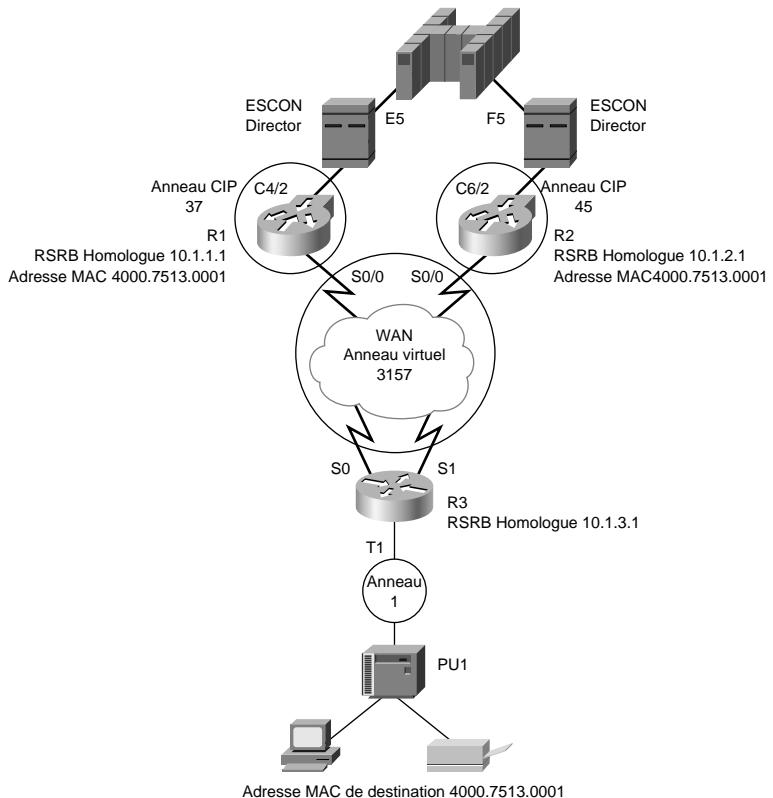
Le routeur R3 dans la Figure 9.4 emploie la fonction Cisco MPC (CMPC) pour se connecter au mainframe *via* ESCON. Elle permet l'utilisation d'une paire de canaux, l'un pour la lecture et l'autre pour l'écriture, appelée *groupe de transmission* (TG). Si vous disposez d'un CIP auquel sont connectées deux cartes d'interface de canal, l'une peut être dédiée à la lecture et l'autre à l'écriture. La fonction CMPC peut aussi utiliser une paire de sous-canaux *via* un seul canal physique.

Haute disponibilité avec RSRB et l'emploi de deux routeurs CIP

RSRB place en cache le champ RIF pour toutes les connexions avec une adresse MAC de destination établies par l'intermédiaire du routeur. La Figure 9.5 illustre l'emploi de RSRB entre un site distant servi par le routeur R3 et deux routeurs R1 et R2 de centre de données reliés par canal au mainframe au moyen de Cisco CIP. Les définitions de LAN internes sur les routeurs CIP gèrent la connectivité avec le mainframe en utilisant la même adresse MAC interne 4000.7513.0001 sur des numéros d'anneau CIP internes différents.

Figure 9.5

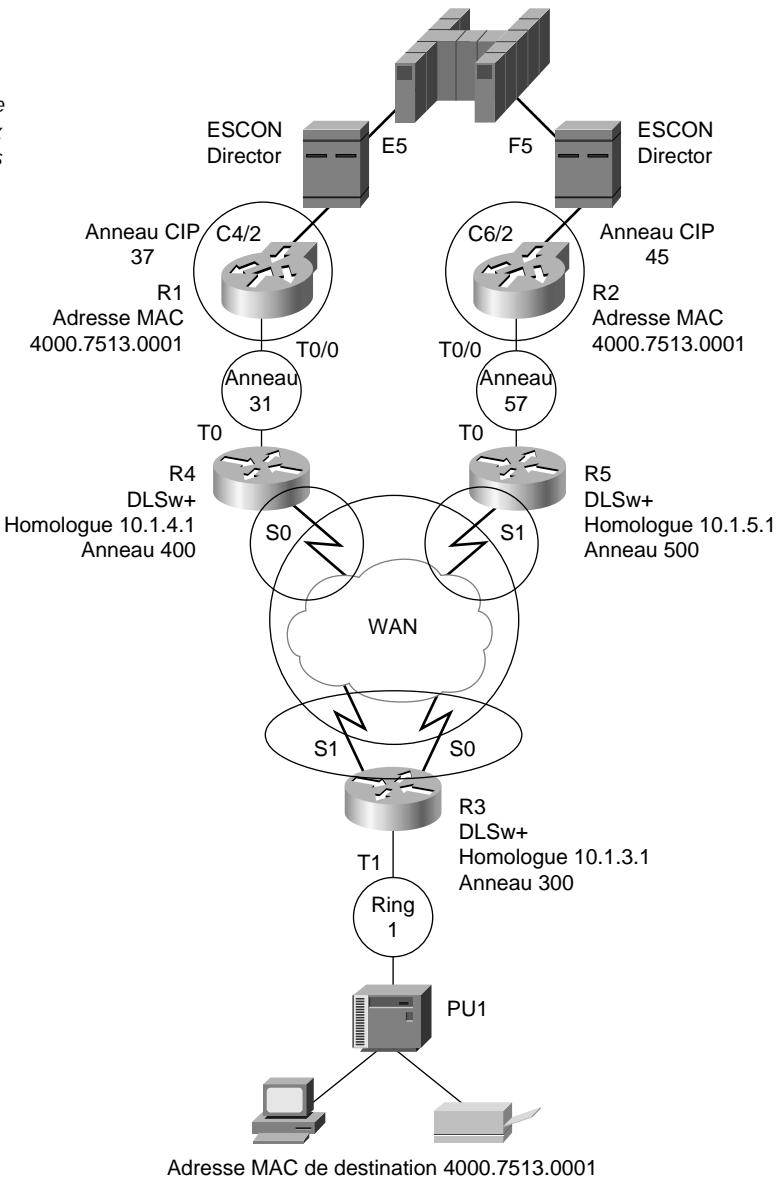
Haute disponibilité, avec l'emploi de RSRB et d'une adresse MAC dupliquée sur deux routeurs Cisco CIP connectés via des commutateurs ESCON Director.



Le cache sur R3 maintient deux entrées RIF pour l'adresse MAC de destination : l'une *via* R1 et l'autre *via* R2. La première entrée dans le cache est celle utilisée par l'emplacement distant. Si le routeur R1, ou sa connexion de canal, devenait inopérant, il expirerait et toutes les nouvelles sessions établiraient leur connectivité SNA par l'intermédiaire du routeur R2.

Figure 9.6

Haute disponibilité avec l'emploi d'une adresse MAC dupliquée, et équilibrage de charge avec DLSw+ sur deux routeurs Cisco CIP connectés via deux commutateurs ESCON Director.



Haute disponibilité et équilibrage de charge au moyen de DLSw+ et de deux routeurs CIP

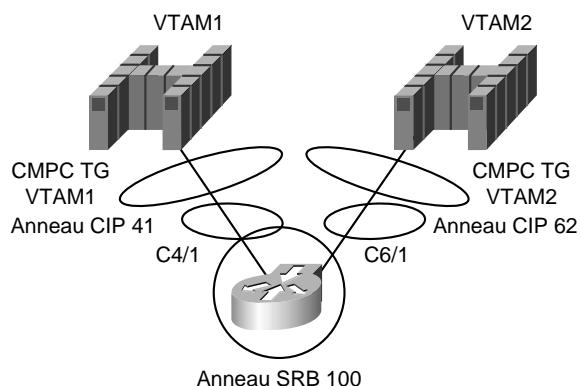
Pour apporter une solution au problème de cache RIF implémentez des routeurs DLSw+-WAN et utilisez SRB pour la connexion avec les routeurs CIP (voir Figure 9.6). Dans ce scénario, le PU1 sur l'emplacement distant se connecte à l'adresse MAC 1000.7515.0001 au moyen de DLSw+. Ce protocole prend connaissance de deux chemins à travers le réseau. Les routeurs de centre de données R4 et R5 fournissent une connectivité à tour de rôle par le biais des deux anneaux Token Ring qui les relient aux routeurs R1 et R2 connectés *via* un canal. Souvenez-vous que cette procédure ne convient que pour l'établissement de session SNA.

Communications VTAM-VTAM via un seul routeur doté de deux CIP

Les communications VTAM-VTAM sont souvent utilisées sur les réseaux où plus d'un VTAM est exécuté. La Figure 9.7 illustre l'emploi de la connectivité VTAM-VTAM à travers deux CIP sur le même routeur. Les performances sont améliorées par l'emploi du protocole CMPC. Cette configuration peut aussi être mise en place en utilisant deux routeurs CIP connectés chacun à l'un des deux VTAM. Les routeurs communiqueraient ensuite sur une épine dorsale à haute vitesse telle que Fast Ethernet, ATM ou FDDI, en utilisant le même mécanisme que celui illustré pour la configuration avec un seul routeur CIP.

Figure 9.7

Communications VTAM-VTAM via un seul routeur avec deux CIP.

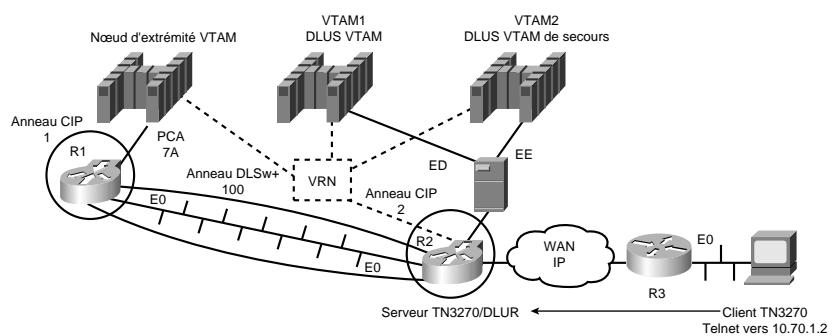


Commutation de session TN3270 avec DLUR/DLUS et redondance d'hôte VTAM

La fonction TN3270 Server du processeur Cisco CIP permet à un flux de données de l'IBM 3270 de traverser une épine dorsale IP. Cette fonction décharge la terminaison TN3270 sur le mainframe du traitement de service TCP/IP et présente au VTAM les connexions TN3270 comme des LU d'un PU connecté à un LAN.

La Figure 9.8 illustre l'emploi du serveur TN3270, plus la fonction de commutation des connexions TN3270 d'un VTAM à un autre au cas où le VTAM principal deviendrait inopérant. Les nœuds principaux commutés sur le VTAM doivent représenter les connexions PU directes pour le serveur TN3270 et posséder une définition utilisée pour la commutation de session. La configuration utilise APPN VRN (*Virtual Routing Node*, nœud de routage virtuel) pour connecter les trois nœuds APPN de mainframe. Le protocole de transport utilisé entre les deux routeurs CIP est DLSw+.

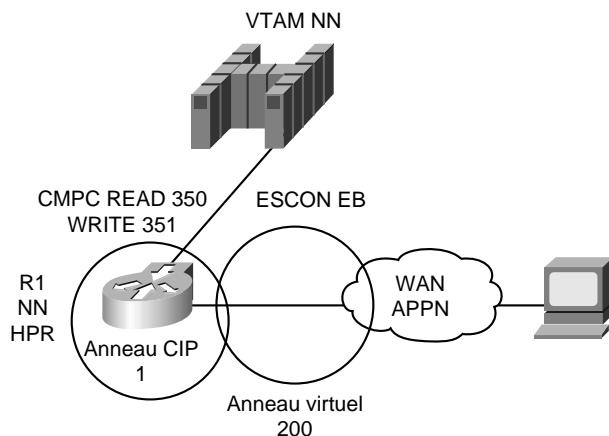
Figure 9.8
Commutation de session TN3270 en utilisant DLUR/DLUS et la redondance d'hôte.



Connexion ESCON CMPC pour APPN HPR vers VTAM

Dans la configuration de la Figure 9.9, le routeur CIP communique avec VTAM et le WAN APPN au moyen du protocole HPR. Le routeur CIP définit le canal et les ports Token-Ring comme des liaisons APPN pour établir la connexion de bout en bout. Cette même connexion peut aussi supporter le protocole APPN ISR. Le routeur CIP ne doit pas nécessairement être du type nœud de réseau (NN) APPN ; il figure ainsi juste pour illustrer le fonctionnement.

Figure 9.9
Configuration de canal CMPC
ESCON utilisant APPN HPR.



Chargement du microcode du CIP

A partir de la version 11.1 du système Cisco IOS, le microcode pour le CIP (ou *l'image CIP*) est dissocié de l'IOS. Le processeur de route (RP, *Route processor*) des routeurs Cisco 7000 ou le processeur commutateur de routeur (RSP, *Router switch processor*) des routeurs Cisco 7200/7500 doivent avoir une mémoire flash installée. Une mémoire RAM de 8 Mo au minimum est nécessaire sur le CIP lui-même pour pouvoir utiliser les fonctions de connexion par canal IBM de Cisco IOS à partir de la version 11.1.

NOTE

L'image CIP est préchargée sur les cartes flash pour tous les routeurs Cisco 7000 avec RSP7000, Cisco 7500 et Cisco 7200, commandés avec l'option CIP/CPA du système Cisco IOS, à partir de la version 11.1.

Le microcode Cisco CIP peut être trouvé sur le site Web de Cisco sous la rubrique "Support". Après avoir trouvé celui qui convient pour votre CIP ou CPA, téléchargez *via* TFTP vers un serveur TFTP valide de votre réseau. Exécutez les commandes de l'Exemple 9.1 pour transférer le microcode CIP d'un serveur TFTP vers une carte flash sur le routeur.

Exemple 9.1 : Exemple de transfert du microcode CIP vers le routeur CIP

```
Router-r1#copy tftp slot0:  
Enter source file name: cip25-8.bin  
6843800 bytes available on device slot0, proceed? [confirm]  
Address or name of remote host [tftpserver.domain.com]? 10.1.254.2  
Accessing file "cip25-8.bin" on 10.1.254.2 ...FOUND  
Loading cip25-8.bin from 10.1.254.2 (via Ethernet2/3): !  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_kernel_hw4 size = 257888  
!!!!!!!!!!!!!!CCCCCCCC  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_kernel_hw5 size = 256914  
!!!!!!!!!!!!!!CCCCCCCC  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_seg_802 size = 233792  
!!!!!!!!!!!!!!CCCCCCCC  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_seg_csna size = 85896  
!!!!!!CC  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_seg_eca size = 461408  
!!!!!!!!!!!!!!CCCCCCCCCCCC  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_seg_offload size = 64656  
!!!!!!C  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_seg_pca size = 69360  
!!!!!!CC  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_seg_push size = 13752  
!!!  
--- expanding multi-segment file ---  
slot0:cip25-8.bin_seg_tcpip size = 182032  
!!!!!!CCCC  
--- expanding multi-segment file --  
slot0:cip25-8.bin_seg_tn3270 size = 542392  
!!!!!!CCCCCCCCCCCCCCCC
```

Le fichier de configuration du routeur doit disposer d'un pointeur vers le nom et l'emplacement du microcode CIP. Cela est réalisé en entrant dans le mode de configuration sur le routeur et en tapant la commande de configuration `microcode` (voir Exemple 9.2).

Exemple 9.2 : Commande de configuration pour pointer vers le microcode CIP

```
microcode CIP flash slot0:cip25-8.bin
microcode reload
```

La commande globale `microcode` définit le processeur d'interface actuellement chargé où réside le microcode ainsi que le nom du microcode à charger. La commande globale `microcode reload` charge le CIP immédiatement.

Définition du support CSNA

La fonction Cisco SNA (CSNA) communique avec le VTAM sur le mainframe en utilisant le pilote XCA (*External Channel Adapter*) du VTAM. Pour supporter SNA, la fonction utilise une seule adresse de canal pour lire et écrire sur le mainframe. Elle utilise l'interface virtuelle CIP x/2 pour définir les LAN virtuels internes employés pour la connectivité par le biais de LLC2.

Assignation de CSNA à une adresse de dispositif d'entrée/sortie

La commande `cnsa` utilise le chemin de canal et l'adresse du dispositif. Sa syntaxe est la suivante :

```
cnsa chemin dispositif [maxpiu valeur] [time-delay valeur] [length-delay valeur]
```

Le paramètre *chemin* de la commande `cnsa` est subdivisé en trois arguments : chemin logique, adresse logique de canal et adresse d'unité de contrôle.

- Le chemin logique, composé de deux chiffres hexadécimaux, représente l'adresse de la connexion physique au niveau du mainframe. Suit un chiffre hexadécimal pour l'adresse d'unité de contrôle et un autre pour l'adresse du dispositif. Les connexions du canal PCA requièrent que les deux premiers chiffres de la valeur de chemin soient **01**. Les deux autres chiffres sont configurés dans le fichier de génération IOCP et devraient correspondre au dispositif approprié.
- L'adresse logique de canal ESCON du paramètre `cnsa chemin` doit correspondre à la valeur du port d'entrée ESCON PATH comme elle a été définie dans la génération IOCP. Dans le cas de l'emploi d'un commutateur ESCON Director, il s'agit du port servant à la connexion avec le mainframe, et dans le cas contraire (connexion ESCON directe avec le mainframe), l'argument a la valeur **01**. La définition de macro CHPID de IOCP/HCD pointe vers la partition logique au moyen d'une valeur nommée dans le paramètre PART. La macro RESOURCE de IPCP/HCD définissant la partition nommée spécifie le numéro LPAR de cette dernière. Le codage d'une valeur pour le partage pour la macro CHPID d'identification de chemin de canal nécessite l'indication du numéro de partition LPAR se connectant à la définition `cnsa` par l'intermédiaire d'un ESCON Director. Si ce commutateur n'est pas utilisé, la valeur de chemin est **01**.
- L'adresse d'unité de contrôle du paramètre `cnsa chemin` est représentée par un seul chiffre hexadécimal qui doit correspondre au paramètre IOCP/HCD CUADD de la macro CNTLUNIT. Si ce paramètre n'a pas été codé dans la macro pour ce canal, on utilise par défaut la valeur **0**.

Le paramètre *dispositif* de la commande `cnsa` représente la position de l'interface CIP comme dispositif connecté au canal. La valeur indiquée provient du paramètre UNITADD de la macro CTLUNIT dans la définition IOCP/HCD.

Par exemple, si une adresse IOCP IODEVICE est EB2, que le paramètre UNITADD de la macro CTLUNIT est spécifié avec E00 et que le paramètre IOCP UNITADD commence à 00, la commande d'interface serait définie de la façon suivante :

```
csna E220 02
```

L'adresse de port ESCON se connectant au mainframe est E2. La partition logique qui utilise cette connexion est LPAR numéro 2 et la valeur CUADD est par défaut de 0. Le CIP est connecté comme troisième dispositif sur le canal (en comptant à partir de 0), car le paramètre de dispositif indique 02.

Supposez une adresse IODEVICE de 97A, un paramètre IODEVICE ADDRESS spécifiant une adresse d'entrée/sortie débutant à 920 pour 64 adresses : IODEVICE ADDRESS=(0920,64) et un paramètre UNITADD correspondant commençant à 20 pour 64 dispositifs : UNITADD=(20,64). Le paramètre *csna dispositif* serait le résultat de la différence entre 7A et 20, ce qui donne 5A. La commande csna correspondante serait ainsi codée :

```
csna E220 5A
```

La valeur du mot clé optionnel maxpiu indique en octets la taille maximale que peut avoir un paquet placé sur le canal en cours de définition. Ce paramètre est comme un équivalent à la valeur de SNA MAXDATA ou IP MTU. Sa valeur est par défaut de 20 470 octets si elle n'est pas codée, et peut varier de 4 096 à 65 535 octets. La syntaxe pour la spécifier est la suivante :

```
maxpiu valeur
```

La valeur du mot clé optionnel time-delay est indiquée en millisecondes et fixe le délai observé avant la transmission d'un paquet reçu sur l'interface. Elle est par défaut de 10 ms et varie sinon entre 0 à 100 ms. La syntaxe pour la spécifier est la suivante :

```
time-delay valeur
```

La valeur du mot clé optionnel length-delay fixe le nombre d'octets à placer en tampon avant qu'ils soient envoyés sur l'interface de transmission. Elle est par défaut de 20 470, et les valeurs valides doivent faire partie de l'intervalle 0 à 65 535. La syntaxe du mot clé est la suivante :

```
length-delay valeur
```

Définition du LAN virtuel interne

Les communications SNA via CIP avec CSNA nécessitent la définition d'un LAN virtuel interne. Celle-ci doit être spécifiée dans le mode ENABLE au moyen de la commande de terminal CONFIG TERM. L'Exemple 9.3 en illustre un exemple.

Exemple 9.3 : Définition de LAN virtuel interne pour les services CSNA

```
source-bridge ring-group 4
!
interface Channel 4/0
no ip address
csna E220 02
!
interface Channel4/2
no ip address
no keepalive
LAN Tokenring 0
source-bridge 6 1 4
adapter 0 4000.C15C.0001
```

Avec ce listing, l'interface virtuelle CIP Channel 4/2 est utilisée pour définir le LAN virtuel interne. Comme la fonction CSNA ne requiert pas d'adresse IP pour la connexion avec le mainframe, aucune définition d'adresse n'est prévue. C'est ce qu'indique la commande `no ip address`. Comme il s'agit d'une interface virtuelle supposée n'être établie et active que lorsque l'interface physique Channel 4/0 est active, les messages `keepalive` ne sont pas nécessaires, ce qu'indique la commande `no keepalive`.

— NOTE —

Le CPA d'un routeur Cisco 7200 n'emploie pas d'interface virtuelle. Par conséquent, les commandes traitées à la section interface virtuelle du CIP seraient valables pour une interface physique sur le CPA.

L'interface LAN virtuelle interne est définie avec `LAN`. Elle peut spécifier les paramètres `FDDI`, `Ethernet` et `Tokenring`, mais ce dernier représentait le seul LAN interne supporté au moment de la rédaction de l'ouvrage. La valeur `0` qui suit le paramètre `LAN Tokenring` indique au CIP qu'il s'agit de l'interface LAN virtuelle 0. Le numéro d'interface peut varier de 0 à 31. L'interface virtuelle Channel 4/2 peut se voir assigner plusieurs interfaces LAN virtuelles.

L'instruction `source-bridge` qui suit la commande `LAN Tokenring` définit la connexion entre cet anneau virtuel LAN et l'anneau virtuel WAN. Celui-ci est la valeur indiquée dans la commande globale `source-bridge ring-group`. L'instruction de l'Exemple 9.3 associe le numéro 6 au segment de l'anneau LAN virtuel. Elle spécifie donc la connectivité entre le segment d'anneau virtuel de LAN interne (6) et le segment d'anneau virtuel de WAN (4) par l'intermédiaire du pont 1.

La dernière instruction requise pour la connectivité CSNA est `adapter`. Elle spécifie le numéro relatif d'adaptateur (`RAN`, *Relative adapter number*), ainsi que l'adresse MAC qui lui est assignée, à utiliser sur le segment de LAN virtuel interne. La valeur de RAN doit figurer dans l'intervalle 0 à 17 et correspondre au paramètre `ADAPNO` de nœud principal VTAM XCA. Le CIP autorise la définition de plusieurs adaptateurs virtuels pour le segment de LAN virtuel interne Token-Ring.

L'adresse MAC virtuelle du LAN interne (voir Exemple 9.3) est `4000.C15C.0001` sur l'adaptateur `0`. Elle sera l'adresse MAC de destination pour les équipements se connectant au mainframe au moyen de SNA.

Définition du nœud principal VTAM XCA

Le CIP2 communique avec le VTAM en utilisant un adaptateur XCA (*External Communications Adapter*). Quatre paramètres dans la définition XCA sont pertinents pour l'établissement de communications avec le CIP2. Ce sont les paramètres : `ADAPNO`, `CUADDR`, `SAPADDR` et `MEDIUM`.

L'Exemple 9.4 illustre une définition XCA pour le CIP2 CSNA défini dans l'Exemple 9.3. L'instruction `PORT` identifie le RAN en utilisant le paramètre `ADAPNO`. La valeur codée pour le paramètre XCA `ADAPNO` doit correspondre à celle définie pour la première variable de la commande CIP `adapter`. Dans les exemples donnés, la valeur est `0`.

Le paramètre XCA `CUADDR` dans l'instruction `PORT` spécifie l'adresse du dispositif d'entrée/sortie que le VTAM utilise pour communiquer avec le CIP. La valeur spécifiée dans l'Exemple 9.4 est `EB2`.

Cette valeur doit être l'adresse du dispositif d'E/S désignée par la variable device-address de l'instruction CSNA définie pour l'interface CIP Channel 4/0.

Le paramètre SAPADDR de l'instruction PORT indique le point d'accès au service (SAP) que ce noeud principal VTAM XCA utilise pour la communication avec les équipements à travers la connexion de canal. La valeur 4 de ce paramètre spécifiée sur le XCA doit correspondre avec les définitions de contrôleur PU SNA des équipements qui communiquent avec le VTAM par l'intermédiaire du CIP2.

Le dernier paramètre XCA de l'instruction PORT est MEDIUM. Il spécifie le type de LAN utilisé. Cette valeur doit refléter le type de LAN virtuel défini sur le CIP pour communiquer avec le VTAM. Dans les exemples donnés, la valeur RING sur le XCA identifie l'emploi d'un LAN Token-Ring défini par l'instruction LAN sur l'interface virtuelle CPI2 Channel 4/2.

Exemple 9.4 : Définition de nœud principal VTAM XCA pour une connexion CIP

```
XCAR1    VBUILD TYPE=XCA
CIPEB21  PORT    ADAPNO=0, CUADDR=EB2, SAPADDR=4, MEDIUM=RING, TIMER=60
*      RESSOURCES COMMUTEES PU2/PU2.1 *
GEB2101 GROUP DIAL=YES, ISTATUS=ACTIVE, AUTOGEN=(50,L,P)
```

Définition pour le support du serveur TN3270

Pour que la configuration CSNA puisse supporter les fonctions de serveur TN3270, les informations suivantes doivent être ajoutées :

- une adresse IP pour l'interface Channel 4/2 ;
- un deuxième adaptateur virtuel à utiliser sur l'interface Token-Ring virtuelle ;
- des définitions PU TN3270, pour représenter les fonctions PU pour les LU assignées par VTAM, en utilisant les DDLU (*Dynamic Definition Dependent LU*).

L'assignation d'une adresse IP à l'interface virtuelle Channel 4/2 permet l'emploi des services IP (voir Exemple 9.5). L'instruction max-llc2-sessions spécifie le nombre maximal de sessions LLC2 pouvant être actives au moyen de l'interface Channel 4/2. Le serveur TN3270 utilise un deuxième adaptateur virtuel sur le LAN virtuel. Le numéro de RAN 1 et l'adresse MAC 4000.3270.7006 définissent les adresses pour l'adaptateur du serveur TN3270.

Exemple 9.5 : Instructions requises sur l'interface CIP Channel 4/2 pour le support du serveur TN3270

```
source-bridge ring-group 4
interface channel 4/0
csna 0110 00
!
interface Channel 4/2
ip address 192.168.6.1 255.255.255.0
no keepalive
max-llc2-sessions 2000
LAN Tokenring 0
source-bridge 6 1 4
adapter 0 4000.0000.7006
adapter 1 4000.3270.7006
tn3270-server
maximum-lus 4000
pu PUEB2001 017FABC0 192.168.6.2 token-adapter 1 04 luseed LUTNS###
```

La commande `tn3270-server` permet l'emploi des fonctions du serveur TN3270. Celui-ci peut gérer au maximum 30 000 sessions LU. L'instruction `maximum-lus` limite le nombre d'unités LU pouvant être supportées par le serveur TN3270. Il est de 4000 dans l'exemple. La valeur de `max-llc2-sessions` définie précédemment limite néanmoins à 2000 le nombre d'unités logiques possibles à n'importe quel moment.

L'élément principal du serveur TN3270 est la définition de l'unité PU SNA. L'instruction `PU` définit les variables requises pour établir les sessions PU et LU avec le VTAM sur le mainframe. La syntaxe de l'instruction est la suivante :

```
PU nom-pu idblkidnum adresse-ip type-adaptateur ran saplocal luseed basenomlu
```

L'argument `nom-pu` de l'instruction `PU` pour le serveur TN3270 correspond au nom du PU commuté VTAM. La valeur `idblkidnum` doit correspondre aux valeurs `IDBLK` et `IDNUM` spécifiées dans l'instruction de définition de PU VTAM prévue pour la représentation du PU TN3270. L'argument `adresse-ip` est l'adresse IP utilisée par le client TN3270 pour se connecter au PU serveur TN3270. Elle est connue comme étant l'adresse IP d'écoute (*IP Listening Address*). La valeur de `type-adaptateur` doit correspondre au type de LAN virtuel défini pour l'interface Channel 4/2. La valeur `ran` identifie l'adaptateur utilisé pour la connectivité avec le mainframe.

La variable `saplocal` de l'instruction `PU` TN3270 indique le point d'accès au service (SAP) utilisé pour la communication *via* cette interface virtuelle pour ce PU spécifique. Si un deuxième PU était défini au niveau du serveur TN3270 en utilisant le même adaptateur virtuel, une valeur de SAP différente serait assignée à la seconde définition de PU. Généralement, la valeur SAP pour SNA commence par `04` et augmente par incrément de quatre. Par conséquent, un second PU utilisant la même adresse `mac` emploierait une valeur `saplocal` de `08`. Comme il est habituel d'utiliser une valeur de SAP de `04` pour les connexions CSNA, la valeur `08` est plus appropriée pour la connexion TN3270.

Le mot clé `luseed` indique que la fonction DDDLU VTAM est utilisée pour définir dynamiquement les noms LU et leurs caractéristiques associées. Les noms se basent sur la valeur donnée à la variable `basenomlu`. Dans l'Exemple 9.6, la variable donnée pour les noms LU dynamiques est `LUTNS###`. Les positions `###` sont remplacées par VTAM lors de la définition, par la valeur décimale de l'adresse locale du LU (LOCADDR) comme assignée par VTAM dans le nœud principal commuté. `LUSEED` génère la valeur de départ en décimale. L'utilisation de deux caractères dièse, `##`, permet de générer une valeur hexadécimale pour le nom LU. Si `LUSEED` est utilisé, il est recommandé que les valeurs de départ spécifiées dans VTAM et sur le serveur correspondent.

Exemple 9.6 : Définition de PU commuté pour supporter les DDDLU pour le serveur TN3270

```
* DEFINITION DE COMMUTATEUR CIP
SWEB200 VBUILD TYPE=SWNET,MAXGRP=4,MAXNO=80
PUEB2001 PU ADDR=01,PUTYPE=2,MAXPATH=4,ANS=CONT,LOGAPPL=NMT,
           ISTATUS=ACTIVE,MAXDATA=521,I_RETRY=YES,MAXOUT=7,
           PASSLIM=5, IDBLK=017, IDNUM=FABC0, MODETAB=SDLCTAB,
           LUSEED=LUTNS###, LUGROUP=EB2LUGRP, USSTAB=TESTUSS
PATHEB2 PATH   DIALNO=01400032707006,GRPNM=GEB2001
*LUTNS001 LU    LOCADDR=1
*LUTNS002 LU    LOCADDR=2
*LUTNS003 LU    LOCADDR=3
*LUTNS004 LU    LOCADDR=4
```

L’Exemple 9.6 illustre le nom LU résultant pour les quatre premières unités logiques LU sur le nœud principal commuté représentant le PU serveur TN3270 défini sur le routeur. L’astérisque * indique une ligne de commentaire pour VTAM. La valeur de départ de LU *luseed* du routeur doit correspondre à la valeur LUSEED spécifiée dans le nœud principal commuté VTAM. La valeur LUGROUP dans le nœud principal commuté pointe vers une liste qui identifie le type de modèle LU.

L’Exemple 9.7 liste un nœud principal LUGROUP pour VTAM.

Exemple 9.7 : Définition du nœud VTAM LUGROUP pour supporter les DDDLU pour le serveur TN3270

```
TN3270G VBUILD TYPE=LUGROUP
*
* RESSOURCES PU2/PUI.1 COMMUTEES *
*
* TEST NOEUD PRINCIPAL LUGROUP XCA POUR SESSIONS TN3270 *
* POUR CISCO CIP *
*
EB2LUGRP LUGROUP
327802 LU   DLOGMOD=D4C32782,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327803 LU   DLOGMOD=D4C32783,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327804 LU   DLOGMOD=D4C32784,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327805 LU   DLOGMOD=D4C32785,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327902 LU   DLOGMOD=D4C32782,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327903 LU   DLOGMOD=D4C32783,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327904 LU   DLOGMOD=D4C32784,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327905 LU   DLOGMOD=D4C32785,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327802E LU  DLOGMOD=SNX32702,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327803E LU  DLOGMOD=SNX32703,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327804E LU  DLOGMOD=SNX32704,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327805E LU  DLOGMOD=SNX32705,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327902E LU  DLOGMOD=SNX32702,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327903E LU  DLOGMOD=SNX32703,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327904E LU  DLOGMOD=SNX32704,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
327905E LU  DLOGMOD=SNX32705,
            MODETAB=ISTINCLM,SSCPFM=USS3270,LOGAPPL=NMT
3278S2 LU   DLOGMOD=D4C32782,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3278S3 LU   DLOGMOD=D4C32783,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3278S4 LU   DLOGMOD=D4C32784,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3278S5 LU   DLOGMOD=D4C32785,
```

Exemple 9.7 : Définition du nœud VTAM LUGROUP pour supporter les DDDLU pour le serveur TN3270 (suite)

```

3279S2    LU      MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
            DLOGMOD=D4C32782,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3279S3    LU      DLOGMOD=D4C32783,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3279S4    LU      DLOGMOD=D4C32784,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3279S5    LU      DLOGMOD=D4C32785,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3278S2E   LU      DLOGMOD=SNX32702,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3278S3E   LU      DLOGMOD=SNX32703,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3278S4E   LU      DLOGMOD=SNX32704,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3278S5E   LU      DLOGMOD=SNX32705,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3279S2E   LU      DLOGMOD=SNX32702,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3279S3E   LU      DLOGMOD=SNX32703,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3279S4E   LU      DLOGMOD=SNX32704,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
3279S5E   LU      DLOGMOD=SNX32705,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT
@        LU      DLOGMOD=D4C32782,
            MODETAB=ISTINCLM,SSCPFM=USSSCS,LOGAPPL=NMT

```

Support de TN3270 Server avec DLUR/DLUS

La fonction serveur TN3270 peut aussi être employée en utilisant les fonctionnalités DLUR/DLUS de Cisco IOS et VTAM. La fonction DLUR de TN3270 permet au PU TN3270 d'apparaître comme un nœud d'extrémité APPN. Les commandes applicables au DLUR sont les suivantes :

```

dlur nompc-qualifié nomdlus-qualifié
dlus-backup nomdlus2
preferred-nnserver nom
lsap type numéro-adaptateur [saplocal]
link nom [rmac macdist] [rsap sapdist]
vrn nom-vrn
pu nom-pu idblk-idnum adresse-ip

```

L'emploi de la commande dlur est soumis aux règles d'usage qui ont été étudiées pour les connexions APPN. L'argument *nompc-qualifié* représente le nom qualifié du point de contrôle (netid) et le nom LU utilisé pour la commutation de session. La variable *nomdlus-qualifié* indique le nom du point de contrôle fournissant les services DLUS.

La commande dlus-backup identifie le nom qualifié du point de contrôle du DLUS VTAM prévu pour assurer un secours. Il ne peut y avoir qu'une valeur dlus-backup par CIP.

L'instruction preferred-nnserver *nom* donne le nom du serveur nœud de réseau APPN auquel appartient cette définition de DLUR. Le nom est celui du point de contrôle d'un nœud de réseau (NN) adjacent. C'est un paramètre optionnel et il n'est pas requis pour que la commutation SNA puisse être réalisée.

Le paramètre `1sap type numéro-adaptateur [saplocal]` définit l'adresse locale du point d'accès au service (SAP) pour le noeud d'extrémité (EN) DLUR. Le paramètre `type` identifie le type d'adaptateur LAN interne utilisé pour le DLUR. La seule valeur valide à l'époque de la rédaction de ce livre était `token-adapter`. L'argument `numéro-adaptateur` renseigne sur l'adaptateur utilisé sur le LAN interne pour la connexion DLUR. La variable optionnelle `saplocal` représente l'adresse locale du point d'accès au service (SAP) utilisée par le DLUR, et peut prendre une valeur de l'intervalle `04` à `FC`, pouvant être incrémentée par pas de quatre (multiple de quatre). La valeur sélectionnée doit être unique pour toutes les connexions LLC2 traversant l'adaptateur. La valeur par défaut est `C0`.

La commande `link nom [rmac macdist] [rsap sapdist]` définit une liaison APPN vers l'hôte pour le noeud d'extrémité DLUR. L'argument `nom` est une chaîne alphanumérique de huit caractères qui identifie la liaison. Ce nom doit être unique pour le DLUR en cours de définition. La valeur `macdist` est optionnelle et définit l'adresse MAC distante utilisée pour connecter le noeud d'extrémité. La valeur `sapdist` représente l'adresse du SAP utilisé pour communiquer avec le DLUS à travers la liaison. La valeur par défaut est `04` et peut sinon varier de `04` à `FC` en respectant une incrémentation par multiple de quatre.

L'instruction `vrn nom-vrn` identifie le nom du noeud de routage virtuel (VRN) pour connecter le DLUR au DLUS ou éventuellement au DLUS de secours. Le DLUS principal et celui de secours doivent avoir le même nom de VRN spécifié dans le noeud commuté principal VTAM représentant le DLUR, autrement, le commutateur échouera.

L'instruction `pu nom-pu idblk-idnum adresse-ip` définit le PU DLUR TN3270 utilisé pour connecter les clients TN3270. L'argument `nom-pu` est un nom de PU unique associé à la commande `PU`. Pour faciliter l'exploitation et la documentation, le nom devrait correspondre au nom de noeud commuté principal PU VTAM défini pour supporter la définition de PU TN3270. Le paramètre `idblk-idnum` doit correspondre aux paramètres uniques IDBLK et IDNUM de la commande de définition de PU dans le VTAM qui représente cette connexion TN3270. Le paramètre `adresse-ip` est l'adresse IP utilisée par le client TN3270 pour se connecter au serveur TN3270.

Définition de la fonction CIP CMPC

Pour tirer parti de l'architecture Multipath Channel d'IBM, les tâches suivantes doivent être accomplies à la fois sur le VTAM et sur le routeur CIP :

1. Définissez le noeud principal VTAM TRL (*Transport Resource List*).
2. Définissez un noeud principal SNA local.
3. Spécifiez les sous-canaux CMPC.
4. Spécifiez les groupes de transmission (TG) CMPC.
5. Définissez le LAN virtuel interne CIP pour CMPC. Les paramètres de définition d'interface LAN sont les mêmes que ceux utilisés par CSNA.

Nœud principal VTAM TRL (Transport Resource List)

Ce noeud indique au VTAM que le contrôle de ligne MPC doit être employé sur les adresses de dispositif d'entrée/sortie `2F0` et `2F1`. L'instruction `TRLE` définit l'adresse du dispositif d'entrée/sortie pour la lecture (`READ`) et celle du dispositif utilisé pour l'écriture (`WRITE`). Ces adresses et propriétés

de dispositif doivent correspondre à celles de la définition CMPC sur le routeur CIP. L'Exemple 9.8 illustre un nœud principal TRL.

Exemple 9.8 : Nœud principal VTAM TRL pour la fonction CMPC

```
CIPTRL VBUILD TYPE=TRL
TRL2F0    TRLE LNCTL=MPC,MAXBFRU=8,REPLYTO=3.0,
           READ=(97A),                                X
           WRITE=(97B)                               X
```

NOTE

Bien qu'un couple d'adresses pair/impair ne soit pas requis, il est conseillé d'en comprendre les relations et de maintenir une continuité d'adresses de dispositifs d'E/S.

Définition du nœud principal SNA local

Comme le support CMPC ne sert que APPN, une liaison par canal MPC est définie sur l'hôte VTAM pour la connexion avec le routeur CMPC par le biais de la définition d'un nœud principal SNA local. L'instruction PU pointe vers le nœud principal TRL défini précédemment (voir Exemple 9.9). Le paramètre TRLE de l'instruction PU spécifie une instruction de définition de TRLE correspondante située sur un nœud principal TRL déjà défini. Dans cet exemple, le paramètre pointe vers l'instruction nommée TRL2F0. Notez aussi que ce nœud principal SNA local définit le PU pour XID requis avec les sessions CP-CP utilisant le routage HPR.

Exemple 9.9 : Nœud principal SNA local pour configurer la liaison par canal MPC avec le routeur CMPC à partir du VTAM

```
LAGLNA VBUILD TYPE=LOCAL
LAGPUA   PU   TRLE=TRL2F0,
           ISTATUS=ACTIVE,                                X
           XID=YES,CONNTYPE=APPN,CPCP=YES,HPR=YES          X
```

Définition des sous-canaux CMPC

La commande cmpc est spécifiée sur les interfaces physiques du CIP et pas sur l'interface x/2 logique. La raison est que CMPC couple les adresses de sous-canaux afin que chacun de ces derniers puisse être défini sur des ports d'interface CIP physique du même CIP. La syntaxe de la commande cmpc est la suivante :

```
cmpc chemin dispositif nom-tg {read | write}
```

Les paramètres *chemin* et *dispositif* sont définis exactement comme ceux qui ont été décrits pour la commande csna. L'argument *nom-tg* est un nom associé au sous-canal en cours de définition. Un sous-canal en lecture ou en écriture doit être défini pour pouvoir utiliser CMPC. La valeur de l'argument de groupe de transmission *nom-tg* lie les deux définitions cmcp pour former le CMPC TG. Voici un exemple d'emploi de la commande cmpc :

```
interface channel 4/0
!
cmpc 97A 5A R1CIP read
cmpc 97B 5B R1CIP write
```

Définition du groupe de transmission CMPC

Le groupe de transmission CMPC est défini en utilisant la commande `tg` dans la définition d'interface virtuelle de canal x/2. En voici la syntaxe :

```
tg nomtg llc type numéro-adaptateur saplocal [rmac macdist] [rsap sapdist]
```

Le paramètre `nomtg` est le nom de groupe de transmission (TG) utilisé pour une instruction `cmpc` définie précédemment. Ce nom lie le couple de sous-canaux au driver LLC2 pour le LAN interne.

Le mot clé `llc` indique la connectivité sur le CIP pour la pile LLC.

Le paramètre `type` spécifie le type de LAN interne défini pour être utilisé par le TG. La seule valeur autorisée au moment de la rédaction de l'ouvrage était `token-adapter`.

Le paramètre `numéro-adaptateur` indique la définition d'adaptateur de LAN virtuel interne à utiliser par le groupe de transmission.

Le paramètre `saplocal` spécifie l'adresse locale du point d'accès au service (SAP) utilisée pour la communication avec l'hôte. Elle doit être unique pour le routeur et l'hôte, ainsi que pour tous les clients 802.2 utilisant l'adaptateur spécifié. La valeur par défaut est `04`. Toutefois, il peut être raisonnable de spécifier la limite supérieure de l'intervalle autorisé, `FC`, et d'aller vers le bas pour toute connexion CMPC supplémentaire afin d'éviter tout conflit non connu. La valeur doit être un multiple de quatre figurant dans l'intervalle `04` à `FC`.

Le mot clé optionnel `rmac` et sa variable associée `macdist` est une adresse MAC assignée pour être utilisée par le driver CMPC pour la connectivité LLC2.

La valeur de la variable `sapdist` associée au mot clé optionnel `rsap` est par défaut de `04` et représente l'adresse distante du point d'accès au service (SAP) utilisée par le driver pour les communications.

NOTE

Avant de modifier un paramètre de la commande `tg`, la commande `no tg` doit d'abord être spécifiée. Une fois les changements apportés, la commande `new tg` doit être lancée pour qu'ils deviennent effectifs.

Exemples de configuration CIP

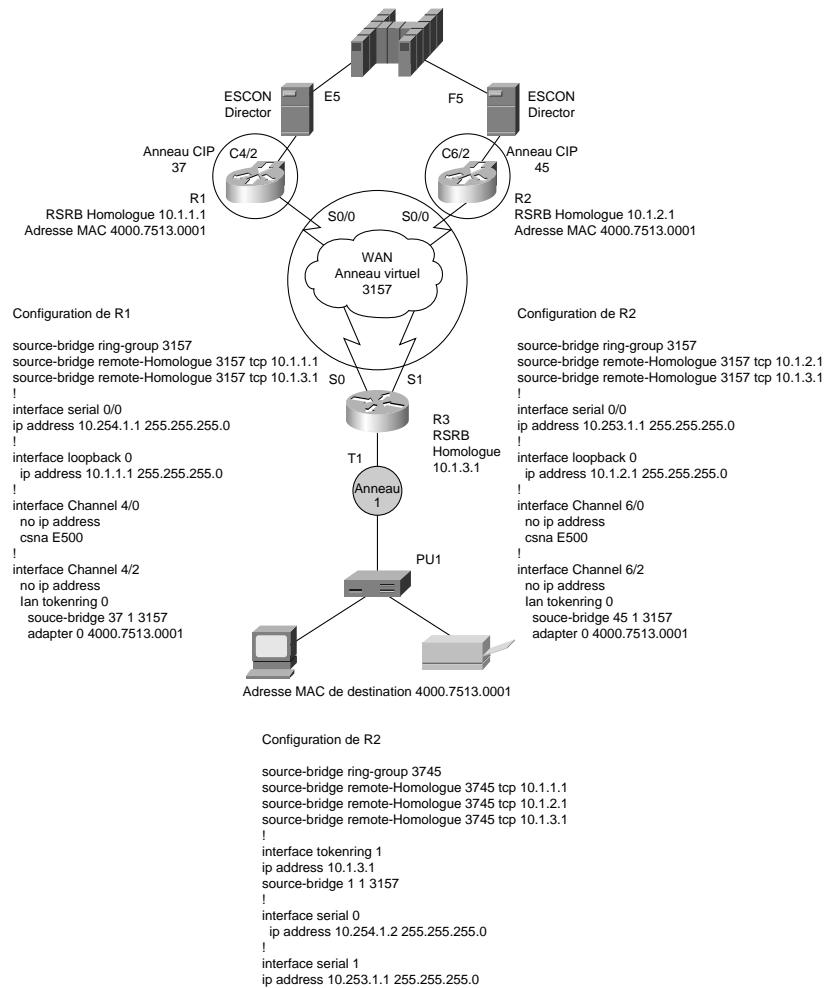
Cette section présente diverses configurations de réseau utilisant le processeur Cisco CIP comme passerelle vers le mainframe. Les configurations explorent l'emploi du CIP au moyen d'exemples de techniques d'encapsulation SNA déjà étudiées plus haut pour connecter des ressources SNA existantes à un mainframe IBM.

Haute disponibilité en utilisant RSRB et deux routeurs CIP

Dans la Figure 9.10, le routeur CIP agit comme passerelle vers le mainframe et relie aussi le WAN. RSRB est utilisé pour transporter les données des emplacements distants vers le mainframe par l'intermédiaire du CIP. Bien que RSRB et les adresses MAC dupliquées apportent une haute disponibilité, cette configuration ne fournit pas d'équilibrage de charge. DLSw+ supportera cette fonctionnalité.

Figure 9.10

Emploi de RSRB vers les routeurs WAN CIP pour fournir une haute disponibilité.

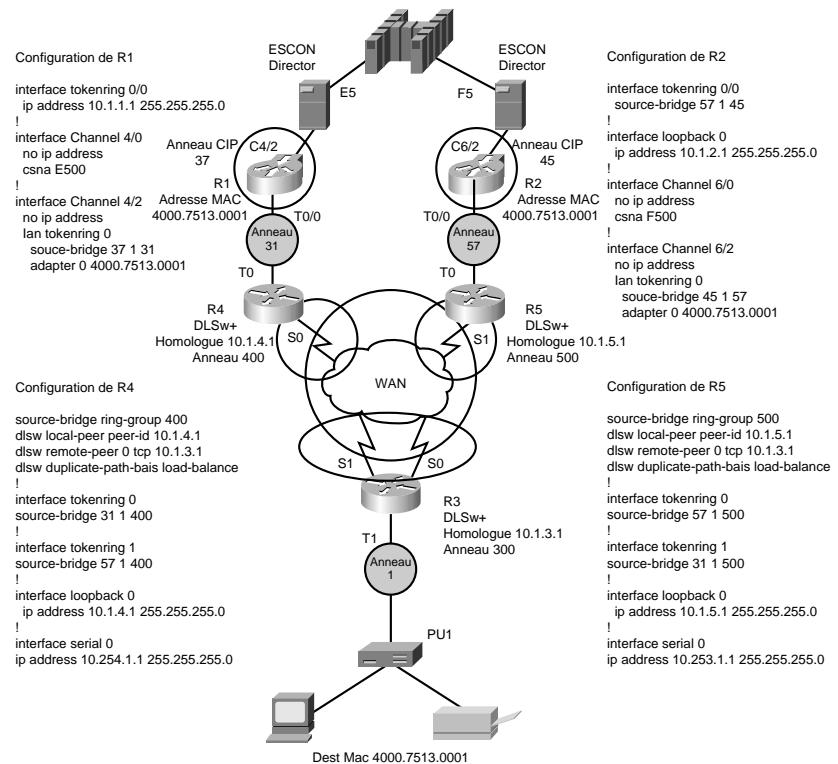


Haute disponibilité et équilibrage de charge au moyen de DLSw+ et de deux routeurs CIP

La Figure 9.11 illustre les configurations de routeur nécessaires pour fournir une haute disponibilité ainsi que l'équilibrage de charge à l'aide de DLSw+ et de deux routeurs CIP. Les routeurs WAN sur le centre de données déchargent les routeurs CIP du traitement de service, sauf pour SRB. Ce type de configuration permet l'adressage MAC dupliqué pour l'équilibrage de charge et la redondance en cas de défaillance d'un routeur CIP.

Figure 9.11

Haute disponibilité avec l'emploi d'une adresse MAC dupliquée et équilibrage de charge avec DLSw+ sur deux routeurs Cisco CIP par l'intermédiaire de deux commutateurs ESCON Director.

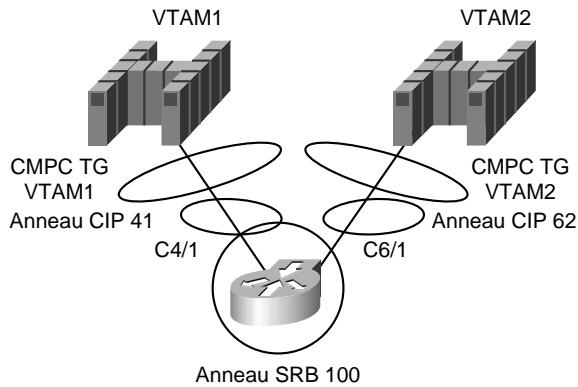


Connectivité CMPC entre deux VTAM sur un seul routeur CIP

La Figure 9.12 illustre un exemple d'emploi d'un seul routeur CIP pour des communications entre deux VTAM. Chaque VTAM est connecté à un CIP différent sur le même routeur. CMPC est utilisé ici pour supporter les communications de noeud à noeud APPN entre les VTAM. La configuration illustre l'emploi de valeurs pour l'adresse MAC distante et celle de point d'accès au service distant dans la commande tg. Le groupe de transmission nommé VTAM1 possède le point rmac de l'adresse MAC de l'adaptateur utilisé pour la connexion avec VTAM2. De la même manière, le groupe VTAM2 dispose de son point rmac vers l'adresse MAC de l'adaptateur utilisé pour la connexion avec VTAM1. Les valeurs de rsap reflètent aussi les adresses de point d'accès au service pour l'autre connexion VTAM avec le CIP.

Figure 9.12

Configuration CMPC pour la communication entre VTAM via un seul routeur doté de deux CIP.



source-bridge ring-group 100

```

interface Channel4/1
no ip address
no keepalive
cmpc C010 40 VTAM1 READ
cmpc C010 41 VTAM1 WRITE
!
interface Channel4/2
no ip address
no keepalive
lan TokenRing 0
source-bridge 41 5 100
adapter 4 4000.0000.CC42
tg VTAM1 llc token-adapter 4 34 rmac 4000.0000.CC62 rsap 30
!
interface Channel6/1
no ip address
no keepalive
cmpc C020 F4 VTAM2 READ
cmpc C010 F5 VTAM2 WRITE
!
interface Channel6/2
lan TokenRing 0
source-bridge 62 3 100
adapter 6 4000.0000.CC62
tg VTAM2 llc token-adapter 6 30 rmac 4000.0000.CC42 rsap 34

```

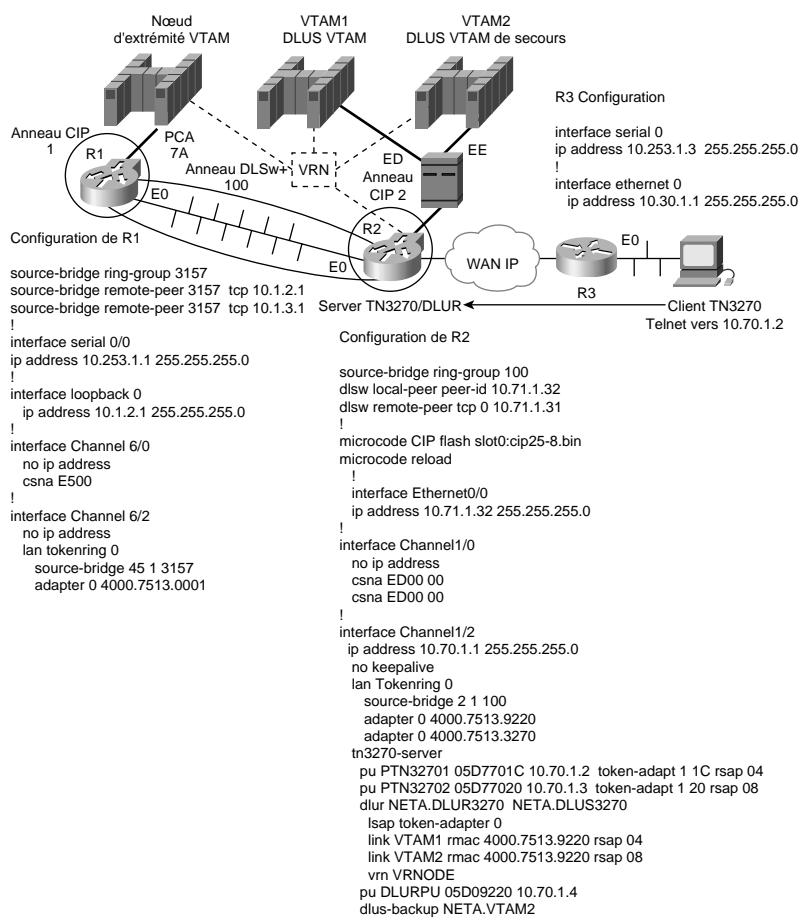
Commutation de sessions TN3270 avec DLUR/DLUS et la redondance d'hôte VTAM

La fonction TN3270 du processeur Cisco CIP permet au flux de données de l'IBM 3270 de traverser une épine dorsale IP. Cette fonction décharge la terminaison TN3270 sur le mainframe du traitement de service pour TCP/IP et présente au VTAM les connexions TN3270 comme des LU d'un PU connecté à un LAN.

La Figure 9.13 illustre l'emploi du serveur TN3270, plus la fonction de commutation des connexions TN3270 d'un VTAM à un autre au cas où le VTAM principal deviendrait inopérant. Les nœuds principaux commutés sur le VTAM doivent représenter les connexions PU directes pour le serveur TN3270 et posséder une définition utilisée pour la commutation de session. La configuration utilise APPN VRN (Virtual Routing Node, nœud de routage virtuel) pour connecter les trois nœuds APPN de mainframe. Le protocole de transport utilisé entre les deux routeurs CIP est DLSw+.

Figure 9.13

Configuration pour la commutation de session TN3270 avec DLUR/DLUS et la redondance d'hôte.

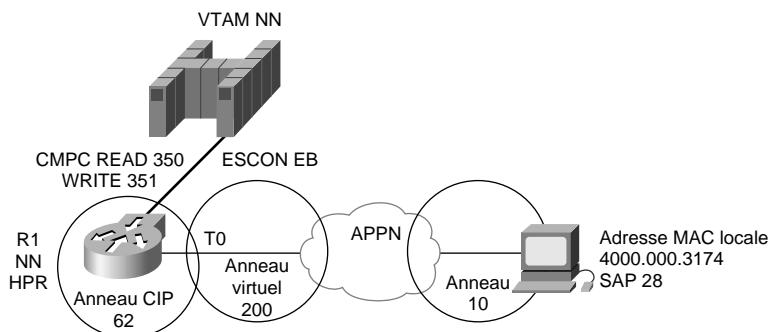


VTAM vers nœud de réseau (NN) APPN avec HPR sur CMPC

Dans la configuration illustrée Figure 9.14, le routeur CIP utilise une connexion ESCON CMPC vers le VTAM. Le routeur CIP utilise HPR pour les communications vers VTAM et le réseau APPN.

Figure 9.14

*Configuration de CMPC
ESCON pour la connexion
du WAN APPN au VTAM
avec HPR.*



R1 Configuration

```

source-bridge ring-group 200
!
interface tokenring 0
source-bridge 10 1 200
!
interface Channel6/1
no ip address
no keepalive
cmpc EB10 50 VTAM1 READ
cmpc EB10 51 VTAM1 WRITE
!
interface Channel6/2
no ip address
no keepalive
lan Tokenring 0
source-bridge 62 2 200
adapter 0 4000.7513.0061
lan Tokenring 1
tg VTAM1 llc token-adapter 0 20 rmac 4000.7513.eb10 rsap 24
!
appn control-point neta.R1
hpr
complete
!
appn port CMPC rsrb
local-sap 24
rsrb-virtual-station 4000.7513eb10 50 3 200
complete
!
appn link-station PC
port CMPC
lan-dest-address 4000.0000.3174 28
complete
!
appn routing

```

10

Conception de réseaux DDR

Par Salman Asad

La technologie DDR (*Dial-on Demand Routing*, routage par ouverture de ligne à la demande) fournit des connexions de réseau par l'intermédiaire du réseau téléphonique public commuté (RTC). Les réseaux étendus dédiés sont généralement implémentés sur des liaisons louées ou sur des technologies plus modernes proposées par des fournisseurs de services comme le Frame Relay, SMDS ou ATM. DDR assure le contrôle de session pour la connectivité étendue à travers des réseaux à commutation de circuits, ces derniers offrant à leur tour des services à la demande et une diminution des coûts d'exploitation du réseau.

DDR peut être utilisé sur des interfaces série synchrones ou asynchrones et sur RNIS (*Réseau Numérique à Intégration de Services*). Les numérotations V.25bis et DTR sont utilisées pour les CSU/DSU du service commuté 56 (*Switched 56*), les adaptateurs de terminaux (TA, *Terminal Adapter*) RNIS ou les modems synchrones. Les lignes série asynchrones sont disponibles sur le port auxiliaire des routeurs Cisco et sur les serveurs de communication Cisco pour la connexion vers des modems asynchrones. DDR est supporté sur RNIS au moyen des interfaces d'accès BRI (RNIS de base) et PRI (RNIS primaire).

Introduction au routage DDR

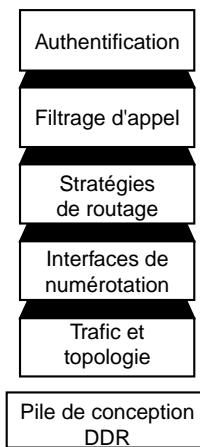
La fonctionnalité DDR du système d'exploitation Cisco IOS simule l'image d'une connectivité permanente pour les tables de routage, au moyen d'interfaces de numérotation (*dialer interfaces*). Lorsque la table de routage transmet un paquet à une interface de numérotation, DDR filtre les paquets intéressants pour établir, maintenir et libérer les connexions commutées. L'interconnexion

est mise en œuvre grâce à la connexion DDR, qui est maintenue au moyen de PPP ou d'autres techniques d'encapsulation WAN, telles HDLC, X.25 ou SLIP. Les concepteurs de réseaux peuvent utiliser le modèle présenté dans ce chapitre pour construire des réseaux DDR évolutifs, qui présentent un rapport équilibré entre les performances, la tolérance de panne et les coûts.

Pile de conception DDR

A l'instar du modèle OSI, qui permet de comprendre et de concevoir l'interconnexion de réseaux, une approche par couches (voir Figure 10.1) peut être utilisée pour concevoir des réseaux DDR.

Figure 10.1
Pile de conception DDR.



Nuage de numérotation

Le réseau formé par les équipements DDR interconnectés peut être désigné de façon générique par *média de numérotation* ou *nuage de numérotation*. L'étendue du nuage de numérotation ne comprend que les équipements interconnectés spécifiques, mais non la totalité du média commuté (la totalité du réseau RNIS s'étend sur l'ensemble du globe et va au-delà du nuage de numérotation). L'exposition à RNIS doit être prise en compte lors de la conception de stratégies de sécurité.

Les caractéristiques fondamentales du nuage de numérotation sont les suivantes :

- Le nuage de numérotation est un groupe de connexions point-à-point potentielles et actives.
- Avec des connexions actives, le nuage de numérotation forme un média NBMA (*Non-Broadcast MultiAccess*, accès multiple non broadcast) semblable au Frame Relay.
- Pour les appels sortants sur des circuits commutés (tel RNIS), la correspondance entre adresse de protocole de réseau et numéro d'annuaire doit être configurée.
- Les connexions DDR inactives font l'objet d'une simulation, de façon que les tables de routage les considèrent comme actives.

- Le trafic broadcast, ou autre trafic indésirable, qui provoque des connexions inutiles peut entraîner des coûts prohibitifs. Les frais potentiels relatifs à un média facturé à l'exploitation, tel RNIS, doivent être surveillés de près afin d'éviter de telles dépenses.

Les caractéristiques des nuages de numérotation affectent chaque étape de la conception des réseaux DDR. Une profonde compréhension de l'adressage, du routage et des stratégies de filtrage des protocoles de réseau peut aider à construire des réseaux fiables et rentables.

Trafic et topologie DDR

Pour déterminer une topologie optimale, le concepteur DDR doit effectuer une analyse préalable du trafic généré par les applications de réseau qui doivent être supportées. Cette étape implique de répondre aux questions suivantes :

- Quelle est la fréquence d'échange du trafic requise entre les sites DDR ?
- Quel est le côté de la connexion DDR qui peut établir la connexion ? Combien y a-t-il de sites distants ?
- S'agit-il d'une solution point-à-point ou multipoint ?

Topologies

Le facteur le plus important dans le choix de la topologie est le nombre de sites qui devront être supportés. Si seulement deux sites sont impliqués, la topologie point-à-point est utilisée. Si davantage de sites doivent être supportés, c'est la topologie hub-and-spoke qui est généralement implantée. Pour un environnement constitué de peu de sites, avec un faible volume de trafic, la topologie totalement maillée peut représenter la solution la plus appropriée.

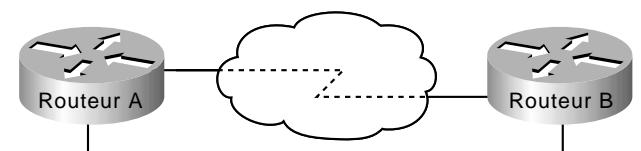
Les topologies pour DDR traitées dans cette section sont les suivantes :

- topologie point-à-point ;
- topologie totalement maillée ;
- topologie hub-and-spoke.

Topologie point-à-point

Sur une topologie point-à-point simple (voir Figure 10.2), deux sites sont connectés entre eux. Chacun d'eux possède une interface de numérotation et associe l'adresse de l'autre site à un numéro de téléphone. Si davantage de bande passante est requise, plusieurs liens peuvent être assemblés au moyen de MultiLink PPP.

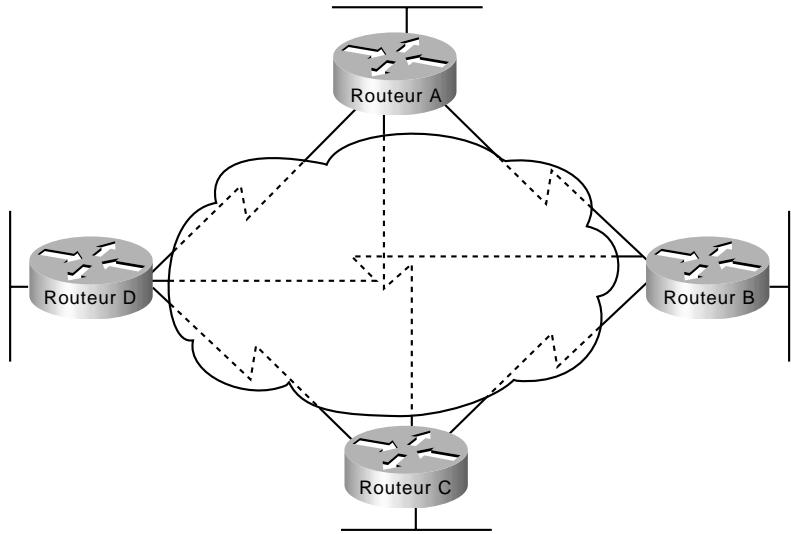
Figure 10.2
Topologie point-à-point.



Topologie totalement maillée

La configuration totalement maillée (voir Figure 10.3) est recommandée uniquement pour les réseaux DDR de très petite taille. Elle peut simplifier le processus de numérotation dans le cas d'une connectivité any-to-any, car chaque site peut appeler n'importe quel autre site directement, plutôt que devoir passer par un site central. Toutefois, la configuration sur chaque site est plus complexe, car chacun d'eux doit disposer d'informations de correspondance pour les autres sites.

Figure 10.3
Topologie totalement maillée.



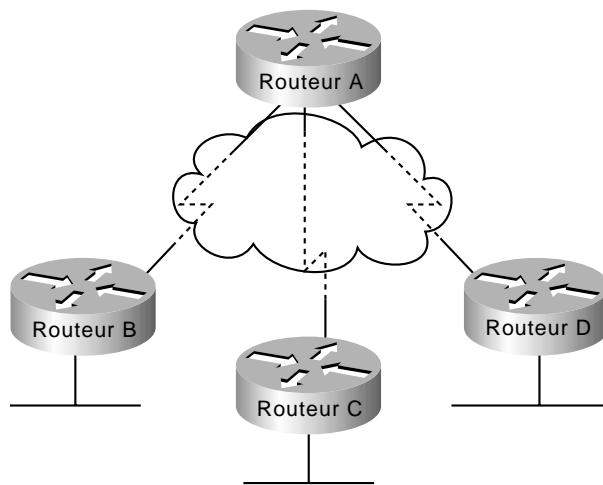
Si l'équilibrage de charge est souhaité, des interfaces peuvent être configurées afin de pouvoir supporter les fonctionnalités MultiLink PPP. En dehors de la complexité de la configuration, il faut soit prévoir un nombre d'interfaces suffisant sur chaque équipement afin de parer à l'éventualité d'un appel de la part de tous les autres équipements, soit être en mesure de pallier un problème éventuel de contention au niveau des interfaces.

Solutions DDR hub-and-spoke

Sur une topologie hub-and-spoke (voir Figure 10.4), un site central est connecté à plusieurs sites distants. Ces derniers communiquent directement avec le site central, mais ne peuvent s'appeler les uns les autres. Cette topologie convient très bien à l'évolution de solutions à grande échelle.

La topologie hub-and-spoke est plus facile à configurer qu'une topologie totalement maillée lorsqu'une connectivité multipoint est requise, car les interfaces de numérotation des sites distants doivent être mises en correspondance uniquement avec le site central. La complexité de conception (l'adressage, le routage et l'authentification) peut ainsi être gérée principalement sur le hub DDR. La configuration qui permet de supporter les sites distants peut s'en trouver grandement simplifiée (à l'instar d'une extrémité dans une topologie point-à-point).

Figure 10.4
Topologie hub-and-spoke.



Si une connectivité any-to-any est requise entre les sites distants, il est possible que le comportement du routage ait besoin d'être modifié en fonction du comportement des interfaces de numérotation, c'est-à-dire qu'il peut se révéler nécessaire de désactiver la fonctionnalité d'horizon éclaté (*split-horizon*) pour les protocoles de routage par vecteur de distance.

Plusieurs hubs peuvent être utilisés afin d'améliorer l'évolutivité des technologies hub-and-spoke. Lorsque MultiLink PPP est employé, comme c'est souvent le cas avec les solutions RNIS, les concepteurs peuvent implémenter Cisco IOS MMP (*MultiChassis MultiLink PPP*) afin d'adapter le groupe de rotation d'appels entrants à plusieurs serveurs d'accès au réseau, ou NAS (*Network Access Server*). MMP est traité en détail au Chapitre 11.

Analyse du trafic

Dans le cadre de l'analyse du trafic, créez un tableau qui permettra d'identifier quels protocoles doivent être capables de supporter la numérotation à la demande (DDR), et quels sont les équipements concernés. Le reste de la conception sera fondé sur ce tableau.

Par exemple, la société KDT a choisi une topologie hub-and-spoke (afin de garantir une certaine évolutivité) et a établi les besoins énumérés au Tableau 10.1, afin de répondre aux exigences de son nuage DDR.

Tableau 10.1 : Exigences de connectivité du protocole DDR pour la société KDT

Site distant	Protocoles d'appels entrants	Protocoles d'appels sortants
c700A	IP, IPX	Aucun
c700B	IP	Aucun
c1600A	IP, AppleTalk	IP
c2500A	IP, IPX, AppleTalk	IP, IPX, AppleTalk

Tableau 10.1 : Exigences de connectivité du protocole DDR pour la société KDT (suite)

<i>Site distant</i>	<i>Protocoles d'appels entrants</i>	<i>Protocoles d'appels sortants</i>
c2500B	IP, IPX	IP
NAS3600A	IP, IPX, AppleTalk	IP, IPX, AppleTalk

Un tel tableau permet d'identifier les sites et les protocoles qui doivent pouvoir initier des connexions DDR. Une fois la connectivité établie, chaque protocole requiert une connectivité bidirectionnelle, par l'intermédiaire de tables de routage et de correspondances d'adresses de nuage de numérotation. Les appels sont dits entrants ou sortants par rapport au hub.

Souvent, l'un des principaux objectifs d'un réseau DDR est de permettre une diminution des coûts WAN associés aux connexions dédiées. Une analyse du trafic de chaque protocole doit également être réalisée à ce stade de la conception ou lors de la définition du filtrage d'appel. Les applications de réseau exploitent l'infrastructure fournie par le réseau de façons différentes et souvent inattendues. Il est essentiel de procéder à une étude approfondie du trafic de réseau qui transitera sur le média de numérotation, de façon à déterminer si l'implémentation d'un réseau DDR peut être envisagée ou non. Les meilleurs outils dont vous disposez pour cette étude sont ceux de capture et d'analyse de paquets.

Interfaces de numérotation

L'accès au média de numérotation se fait par l'intermédiaire des interfaces de numérotation de Cisco IOS. Des canaux B RNIS, des interfaces série synchrones et des interfaces asynchrones peuvent être convertis en interfaces de numérotation à l'aide de commandes de configuration d'interface. Les éléments suivants vous permettront de mieux comprendre le concept d'interface de numérotation :

- interfaces physiques supportées ;
- groupes de rotation de numérotation ;
- profils de numérotation ;
- adressage de nuage de numérotation ;
- correspondances de numérotation.

Les interfaces de numérotation fournissent également des fonctions de simulation de table de routage et de filtrage d'appel.

Interfaces physiques supportées

Plusieurs types d'interfaces physiques peuvent être définis en tant qu'interfaces de numérotation.

Interfaces série synchrones

Des appels sur des lignes série synchrones peuvent être initiés au moyen de la numérotation V.25bis ou DTR. V.25bis est le standard UIT pour la numérotation intra-bande (*in-band*), c'est-à-dire que les informations de numérotation sont envoyées sur le même canal que celui qui transporte les

données. Ce standard est utilisé avec divers équipements, dont les modems synchrones, les adaptateurs terminaux (TA) RNIS et les CSU/DSU du service commuté 56.

Avec la numérotation DTR, le signal DTR est activé sur l'interface physique, ce qui oblige certains équipements à appeler un numéro, préalablement configuré à leur niveau. Lorsque la numérotation DTR est utilisée, l'interface ne peut pas recevoir d'appels. Néanmoins, DTR autorise l'utilisation d'équipements moins coûteux pour le cas où un seul numéro doit être appelé. Les lignes série synchrones supportent l'encapsulation de datagrammes PPP, HDLC et X.25.

Pour convertir une interface série synchrone en interface de numérotation, utilisez les commandes Cisco IOS **dialer in-band** ou **dialer dtr**.

Interfaces RNIS

Tous les équipements RNIS sont abonnés à des services assurés par un fournisseur de services RNIS, généralement une compagnie de téléphonie. Les connexions DDR RNIS sont établies sur des canaux B à 56 ou 64 Kbit/s, en fonction des capacités de transport du circuit de commutation RNIS de bout en bout. MultiLink PPP est souvent utilisé pour permettre aux équipements BRI de grouper les deux canaux B et de bénéficier ainsi d'une bande passante et d'un débit accrus. Reportez-vous au Chapitre 11 pour des recommandations sur la conception de réseaux RNIS.

Les interfaces RNIS BRI et PRI sont automatiquement configurées en tant qu'interfaces de numérotation intra-bandes. RNIS peut supporter l'encapsulation PPP, HDLC, X.25 et V.120. En général, PPP sera employé pour les solutions DDR.

Par exemple, lorsque vous examinez une interface BRI sur un routeur Cisco IOS, vous pouvez voir qu'elle se trouve en mode de simulation d'activité, afin que la table de routage puisse pointer vers elle :

```
c1600A#sh int bri 0
BRI0 is up, line protocol is up (spoofing)
```

Néanmoins, les interfaces physiques sont les canaux B individuels (BRI0:1 et BRI0:2) gérés par l'interface de numérotation (BRI0) :

```
c1600A#sh int bri 0 1
BRI0:1 is down, line protocol is down
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Closed, multilink Closed
Closed: IPCP, CDPCP
```

Connexions asynchrones par modem

Les connexions asynchrones sont utilisées par des serveurs de communication ou *via* le port auxiliaire d'un routeur. Les connexions DDR asynchrones peuvent être utilisées pour supporter plusieurs protocoles de la couche réseau. Avant d'envisager l'implémentation de solutions DDR asynchrones, les concepteurs devraient s'assurer que les applications de réseau sont capables d'accepter les délais d'établissement de connexions plus longs et le débit plus faible, induits par les modems analogiques (par rapport à RNIS). Dans certaines situations, lorsqu'il s'agit de connexions asynchrones par modem, DDR peut représenter une option très rentable.

Pour pouvoir effectuer des appels sur des connexions asynchrones, il faut configurer des scripts de dialogue (*chat script*) ou de connexion, afin que les commandes de numérotation par modem et

d'ouverture de session soient envoyées aux systèmes distants. Pour une conception plus souple, plusieurs scripts de dialogue peuvent être configurés sur les correspondances de numérotation (*dialer map*). Les scripts de modem (*modem script*) peuvent être utilisés afin de configurer les modems pour des appels sortants. Les scripts d'ouverture de session (*login script*) sont prévus afin de gérer l'ouverture de sessions sur des sites distants et préparer la liaison pour l'établissement de PPP. Les scripts de dialogue sont configurés au moyen de séquences du type attendre-envoyer et de mots clés pour modifier les paramètres, comme suit :

```
chat-script dialnum "" "atft\T" TIMEOUT 60 CONNECT \c
```

Si vous employez la technologie DDR asynchrone et appelez un système qui requiert une ouverture de session en mode caractère, utilisez le mot clé **system-script** avec la commande **dialer map**.

Les scripts de dialogue font souvent l'objet de problèmes de temporisation, car ils sont exécutés avec beaucoup plus de précision qu'ils ne le sont lorsqu'une personne physique contrôle la connexion. Par exemple, lorsqu'un modem envoie un message de connexion CONNECT, il arrive qu'il ne soit pas prêt à envoyer des données, et il peut même se déconnecter s'il reçoit des données sur le circuit TX. Pour éviter ce type d'échec, des pauses sont ajoutées en tête de certaines chaînes d'envoi.

Chaque chaîne d'envoi se termine par un retour à la ligne, même lorsqu'il s'agit d'une chaîne nulle (""). Le script de dialogue sera souvent créé sans la chaîne "send" de fin, ce qui peut entraîner des résultats inattendus. Vérifiez que tous les scripts de dialogue possèdent des séquences complètes attendre-envoyer. Si l'élément final dans la logique du script se révèle être un élément d'attente (comme dans l'exemple précédent), utilisez le caractère \c comme dernier envoi, afin de supprimer les résultats indésirables.

Utilisez la commande **debug chat** pour résoudre les problèmes de scripts de dialogue. Un débogage ligne par ligne peut fournir des détails supplémentaires lorsque la logique attendre-envoyer est défaillante. Un exemple de solution DDR asynchrone à grande échelle est décrit au Chapitre 20.

Groupes de rotation de numérotation

Sur des topologies hub-and-spoke ou totalement maillées qui supportent plusieurs connexions entre les sites, les interfaces physiques peuvent être regroupées en groupes de rotation (*rotary group*) à l'aide de la commande **dialer rotary-group**. Les interfaces physiques assignées à un groupe de rotation héritent de la configuration de l'interface de numérotation correspondante.

Si l'une des interfaces physiques dans un groupe de rotation est occupée, l'interface suivante disponible peut être utilisée pour passer ou recevoir un appel. Il n'est pas nécessaire de configurer des groupes de rotation pour les interfaces BRI et PRI puisque les canaux B RNIS sont automatiquement placés dans un groupe de rotation. Cependant, plusieurs de ces interfaces peuvent être regroupées au moyen de la commande **dialer rotary-group**.

Profils de numérotation

Les profils de numérotation, tels que le pontage multisite sur RNIS par exemple, introduits avec la version 11.2 de Cisco IOS, offrent davantage de souplesse de conception. Ces profils représentent une méthodologie alternative pour la conception de réseaux DDR et éliminent le besoin de définition logique des sites de numérotation au niveau des interfaces de numérotation physiques.

Méthodes d'encapsulation

Lorsqu'une liaison de données est clairement établie entre deux homologues DDR, les datagrammes doivent être encapsulés et délimités pour être transportés sur le média de numérotation. Les méthodes d'encapsulation disponibles dépendent de l'interface physique utilisée. Cisco supporte les encapsulations de liaison de données PPP (*Point-to-Point Protocol*), HDLC (*High-Level Data Link Control*), SLIP (*Serial Line Interface Protocol*) et X.25 pour DDR :

- **PPP.** Est la méthode d'encapsulation recommandée, car elle accepte plusieurs protocoles et est utilisée pour les connexions synchrones, asynchrones et RNIS. De plus, PPP, qui assure la négociation et l'authentification d'adresses, peut interopérer avec des solutions de différents fabricants.
- **HDLC.** Est supporté uniquement sur les lignes série synchrones et les connexions RNIS et peut accepter plusieurs protocoles. Toutefois, il n'assure pas l'authentification, fonctionnalité qui peut se révéler nécessaire pour l'utilisation de groupes de rotation.
- **SLIP.** Fonctionne uniquement sur les interfaces asynchrones et n'est supporté que par IP. Les adresses doivent être configurées manuellement. Il n'assure pas l'authentification et peut uniquement interopérer avec des solutions de fabricants qui utilisent SLIP.
- **X.25.** Est supporté sur les lignes série synchrones et sur un seul canal B RNIS.

Adressage de nuage de numérotation

Il existe deux façons de définir l'adressage sur un nuage de numérotation :

- Assigner un sous-réseau au nuage de numérotation.

Chaque site connecté au nuage de numérotation reçoit une adresse de nœud unique sur un sous-réseau pour être utilisée sur son interface de numérotation. Cette méthode ressemble à l'adressage de LAN ou de WAN multipoint et simplifie le schéma d'adressage et la création de routes statiques.

- Utiliser des interfaces sans adresse dédiée.

A l'instar des interfaces point-à-point de liaisons louées sans adresse dédiée, l'adresse d'une autre interface sur le routeur est empruntée pour être utilisée sur l'interface de numérotation. L'adressage sans adresses dédiées (*unnumbered addressing*) tire parti de l'existence de seulement deux équipements sur la liaison point-à-point. La table de routage pointe vers une interface (l'interface de numérotation) et une adresse de prochain saut (qui doit être associée à une correspondance de numérotation : statique ou dynamique).

La définition de routes statiques pour les interfaces sans adresse dédiée peut être un peu plus complexe, car le routeur doit être configuré avec l'interface qui découvre le prochain saut.

Correspondances de numérotation

A l'instar de la fonction de table ARP, les instructions **dialer map** traduisent les adresses de prochain saut en numéros de téléphone. Sans l'emploi de correspondances de numérotation configurées de façon statique, les appels DDR ne peuvent avoir lieu. Lorsque la table de routage pointe sur l'interface de numérotation et que l'adresse de prochain saut est introuvable dans une correspondance de numérotation, le paquet est supprimé.

Dans l'exemple suivant, les paquets pour un hôte sur le réseau 172.20.0.0 sont routés vers une adresse de prochain saut, 172.20.1.2, qui est associée par assignation statique au numéro de téléphone 555-1212 :

```
interface dialer 1
ip address 172.20.1.1 255.255.255.0
dialer map ip 172.20.1.2 name c700A 5551212
!
ip route 172.20.0.0 255.255.255.0 172.20.1.2
```

Les instructions **dialer map** échoueront dans le cas de diffusions broadcast, car un paquet broadcast est transmis avec une adresse de prochain saut de l'adresse broadcast. Si vous souhaitez que les paquets broadcast qui sont transmis aux sites distants soient définis par des instructions **dialer map**, utilisez le mot clé **broadcast** avec la commande **dialer map**.

Pour configurer la vitesse des appels RNIS à 56 ou 64 Kbit/s, vous pouvez utiliser l'option de vitesse avec la commande **dialer map** lors de la configuration des interfaces. Voyez le Chapitre 11 pour plus de détails sur les médias RNIS.

Lorsque vous implémentez DDR entre plus de deux sites, il faut utiliser l'authentification PPP et le mot clé **name** avec la commande **dialer map**, étant donné que les correspondances de numérotation pour les appels entrants représentent une association des adresses de protocole et des noms d'utilisateurs authentifiés.

Pour faciliter la définition de correspondances de numérotation, le concepteur de réseau doit créer une table de correspondances d'adresses qui sera utilisée pour la configuration. Dans le Tableau 10.2, le nuage de numérotation se voit assigner le sous-réseau IP 172.20.1.0/24, le réseau IPX 100 et la plage de câblage (*cable-range*) AppleTalk 20-20. Ce tableau sert de base à la définition des correspondances de numérotation pour chaque site.

Tableau 10.2 : Table de correspondances d'adresses DDR pour la société KDT

<i>Site distant</i>	<i>Protocoles d'appels entrants</i>	<i>Numéro d'annuaire</i>	<i>Notes</i>
c700A	IP: 172.20.1.2 IPX: 100.0000.0c00.0002	4085551212	
c700B	IP: 172.20.1.3	4155558888	56K
c1600A	IP: 172.20.1.4 AT: 20.4	5305551000	
c2500A	IP: 172.20.1.5 IPX: 100.0000.0c00.0005 AT: 20.5	5125558085	
c2500B	IP: 172.20.1.6 IPX: 100.0000.0c00.0006	2105552020	
NAS3600A	IP: 172.20.1.1 IPX: 100.0000.0c00.0001	8355558661	Hub

Puisque NAS3600A est le hub dans la topologie hub-and-spoke, chaque site distant est configuré avec les correspondances de numérotation qui permettent d'atteindre le site central. Par exemple, la configuration des correspondances pour c1600A serait la suivante :

```
interface dialer1
encapsulation ppp
ip address 172.20.1.4 255.255.255.0
appletalk cable-range 20-20 20.4
appletalk zone ZZ DDR
dialer in-band
dialer map ip 172.20.1.1 name nas3600A speed 56 18355558661
dialer map appletalk 20.1 name nas3600A speed 56 18355558661
dialer-group 5
ppp authentication chap callin
```

La configuration des correspondances pour NAS3600A serait la suivante :

```
interface dialer1
encapsulation ppp
ip address 172.20.1.1 255.255.255.0
appletalk cable-range 20-20 20.1
appletalk zone ZZ DDR
ipx network 100
dialer in-band
dialer map ip 172.20.1.2 name c700A
dialer map ipx 100.0000.0c00.0002 c700A
dialer map ip 172.20.1.3 name c700B
dialer map ip 172.20.1.4 name speed 56 c1600A 15305551000
dialer map appletalk 20.4 name c1600A
dialer map ip 172.20.1.5 name c2500A 15125558085
dialer map ipx 100.0000.0c00.0005 name c2500A 15125558085
dialer map appletalk 20.5 name c2500A 15125558085
dialer map ip 172.20.1.6 name c2500B 12105552020
dialer map ipx 100.0000.0c00.0006 name c2500B
dialer-group 5 ppp authentication chap callin
```

Notez que les correspondances de numérotation associent les adresses de protocole de sites distants, les noms de sites distants et les numéros d'annuaire de sites distants. Pour les sites uniquement appelants, les numéros d'annuaire ne sont pas nécessaires et peuvent être omis, ce qui évite une numérotation malencontreuse. Le tableau a servi à identifier les types de sites qui ne requièrent pas le support d'appels sortants. Pour les sites appelants, le nom d'authentification PPP est mis en correspondance avec l'adresse de protocole, afin de garantir que les paquets sortants sont placés sur la connexion PPP appropriée.

Les versions récentes de Cisco IOS permettent de créer des correspondances de numérotation dynamiques pour IP (au moyen de la négociation d'adresse IPCP) et pour IPX (au moyen de la négociation d'adresse IPXCP), éliminant ainsi le besoin de correspondances de numérotation sur les sites uniquement appelants.

Les concepteurs DDR doivent se familiariser avec l'utilisation des commandes EXEC Cisco IOS **show dialer** et **show dialer map**, afin de pouvoir vérifier l'état des sites DDR, des interfaces physiques et de la table de correspondances de numérotation. Utilisez la commande **debug dialer** pour résoudre les problèmes de connexion DDR :

```
c1600A#sh dialer
BRI0 - dialer type = ISDN
Dial String      Successes   Failures   Last called   Last status
```

```

1835558661 0      0      never
0 incoming call(s) have been screened.
BRI0:1 - dialer type = ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (5 secs)
Dialer state is idle
BRI0:2 - dialer type = ISDN
Idle timer (60 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (5 secs)
Dialer state is idle

c1600A#sh dialer map
Static dialer map ip 172.20.1.4 name nas (8355558661) on BRI0

```

Stratégies de routage

La nature des réseaux DDR implique que le routage et certaines tables de services d'annuaire soient maintenus sur les connexions inactives. Les concepteurs DDR peuvent utiliser une combinaison de techniques de routage statique, dynamique et Snapshot, afin de répondre aux besoins de conception. Le routage par défaut et les techniques de simulation de nœud distant (telles les techniques PAT de la série de routeurs Cisco 700 et EZIP de Cisco IOS) peuvent être utilisés pour simplifier considérablement la conception du routage.

L'épine dorsale au niveau du site du NAS utilisera souvent un protocole de routage à convergence rapide, tels OSPF ou EIGRP. Cependant, ces protocoles ne fonctionnent pas correctement sur le média de numérotation, en raison de leurs fonctionnalités fondées sur la diffusion broadcast et les informations d'état de lien. Généralement, les protocoles de routage statique ou de routage par vecteur de distance sont choisis pour les connexions DDR. La redistribution de route peut être nécessaire pour supporter la propagation des informations de routage entre les différents protocoles de routage.

Un examen approfondi des techniques de redistribution de routage dépasse le cadre de cet ouvrage. Toutefois, les concepteurs DDR ont besoin de développer et de vérifier leur stratégie de routage pour chaque protocole de réseau.

Routage statique

Avec le routage statique, les routes de protocole de réseau sont configurées manuellement. Le protocole de routage n'a ainsi plus besoin de diffuser en mode broadcast des mises à jour de routage sur les connexions DDR. Ce type de routage peut être efficace sur les petits réseaux qui changent peu. Les protocoles de routage peuvent parfois générer un trafic entraînant l'établissement de connexions inutiles.

Lors de la conception d'un environnement IP sans adresses dédiées, les anciennes versions de Cisco IOS requéraient plusieurs routes statiques pour chaque site : une route pour définir l'adresse du prochain saut et une autre pour définir l'interface sur laquelle trouver le prochain saut (et la correspondance de numérotation). Le code suivant :

```

interface Dialer1
  ip unnumbered Ethernet0/0
  dialer in-band
  dialer map ip 172.17.1.100 name kdt-NAS speed 56 5558660
  dialer-group 5

```

```

!
ip classless
ip route 0.0.0.0.0.0.0 172.17.1.100 200
ip route 172.17.1.100 255.255.255.255 Dialer1 200
dialer-list 5 protocol ip permit

```

crée la table de routage suivante :

```

kdt-3640#sh ip route
...<snip>...
Gateway of last resort is 172.17.1.100 to network 0.0.0.0

172.17.0.0/32 is subnetted, 1 subnets
S       172.17.1.100 is directly connected, Dialer1
      172.20.0.0/24 is subnetted, 1 subnets
S*   0.0.0.0/0 [200/0] via 172.17.1.100

```

Les versions récentes de Cisco IOS permettent de ramener la configuration à une seule route. Par exemple, la configuration suivante :

```
ip route 0.0.0.0.0.0.0 Dialer1 172.17.1.100 200 permanent
```

Résulte en une table de routage simplifiée, comme suit :

```

kdt-3640#sh ip route
...<snip>...
Gateway of last resort is 172.17.1.100 to network 0.0.0.0

172.20.0.0/24 is subnetted, 1 subnets
C       172.20.1.0 is directly connected, Ethernet0/0
S*   0.0.0.0/0 [200/0] via 172.17.1.100, Dialer1

```

Il faut généralement configurer la redistribution de routes statiques dans le protocole de routage dynamique de l'épine dorsale, afin de garantir une connectivité de bout en bout. Par exemple, pour redistribuer la route statique vers d'autres réseaux dans le système autonome IGRP 20, utilisez les commandes de configuration suivantes :

```

router igrp 20
network 172.20.0.0
redistribute static

```

Routage dynamique

Le routage dynamique peut être utilisé de différentes manières dans la conception de réseaux DDR. Il peut être employé avec le routage Snapshot (voir la section "Routage Snapshot", plus loin dans ce chapitre) pour placer en cache les routes apprises par les protocoles de routage dynamique, ce qui permet l'automatisation de la maintenance du routage statique. Le routage dynamique peut également servir de déclencheur pour la convergence de routage dans des environnements DDR étendus et complexes.

Lorsque la liaison DDR est connectée, les mises à jour de routage circulent en direction de l'homologue, autorisant les configurations redondantes à converger sur la connexion physique par la redistribution des mises à jour de routage.

Sélection d'un protocole de routage dynamique

Le protocole de routage sélectionné pour une liaison DDR est généralement un protocole de routage par vecteur de distance, tel RIP, RIP II, EIGRP, IGRP ou RTMP. Il est recommandé de choisir le protocole le plus simple, qui répond aux besoins de conception et qui est supporté par les routeurs DDR.

Interfaces passives

Les interfaces marquées comme étant passives n'enverront pas de mises à jour de routage. Pour éviter que ces mises à jour établissent des connexions sur les interfaces de numérotation qui ne s'appuient pas sur des informations de routage dynamique, configurez les interfaces avec la commande **passive-interface** ou utilisez des listes d'accès (voir les sections "Listes d'accès IP" et "Listes d'accès IPX", plus loin dans ce chapitre). L'utilisation de cette commande, ou d'une liste d'accès, empêche les mises à jour de routage de déclencher un appel. Néanmoins, si vous souhaitez qu'elles soient transmises lorsque la liaison est active, utilisez une liste d'accès au lieu de la commande **passive-interface**.

Fonctionnalité d'horizon éclaté

Les routeurs connectés à des réseaux IP de type broadcast et les routeurs qui emploient des protocoles de routage par vecteur de distance exploitent la fonctionnalité d'horizon éclaté (*split horizon*) pour limiter les risques de boucles de routage. Lorsque cette fonctionnalité est activée, les informations de routage qui arrivent sur une interface ne sont pas retransmises sur cette même interface.

NOTE

Lorsque des sites distants ont besoin de communiquer entre eux, il est préférable de désactiver la fonctionnalité d'horizon éclaté pour les topologies hub-and-spoke. Sur ces topologies, les sites en périphérie font connaissance les uns des autres par l'intermédiaire du site central auquel ils sont connectés *via* une seule interface. Pour que ces sites distants puissent échanger directement des informations, la fonctionnalité d'horizon éclaté doit être désactivée, afin que des tables de routage complètes puissent être créées sur chaque site.

Routes connectées dynamiquement

Les routes connectées dynamiquement sont les suivantes :

- **Routes AAA installées par l'utilisateur.** Des serveurs AAA peuvent installer des routes associées à des utilisateurs par le biais de l'autorisation AAA, afin de télécharger et d'installer des routes au fur et à mesure que les sites distants se connectent.
- **Routes homologues PPP.** La négociation d'adresses IPCP installe des routes hôtes (/32 masque de sous-réseau) pour l'homologue distant. Cette route hôte peut être propagée vers les routeurs d'épine dorsale, afin de fournir une convergence de routage fiable. Dans la plupart des applications, la route hôte homologue sera avantageuse (ou inoffensive) pour la conception de réseaux. Si des routes hôtes PPP interagissent mal avec les stratégies de routage existantes, elles peuvent être désactivées à l'aide de la commande de configuration d'interface **no peer neighbor-route**.

Routage Snapshot

Avec le routage Snapshot, le routeur est configuré pour le routage dynamique. Le routage Snapshot contrôle l'intervalle de mise à jour des protocoles de routage. Il fonctionne avec les protocoles de routage par vecteur de distance suivants :

- RIP (*Routing Information Protocol*) pour IP ;
- IGRP (*Interior Gateway Routing Protocol*) pour IP ;
- RIP et SAP (*Service Advertisement Protocol*) pour Novell IPX (*Internet Packet Exchange*) ;
- RTMP (*Routing Table Maintenance Protocol*) pour AppleTalk ;
- RTP (*Routing Table Protocol*) pour Banyan VINES.

Dans des circonstances normales, ces protocoles de routage diffusent en mode broadcast des mises à jour toutes les 10 à 60 secondes. Par conséquent, une liaison RNIS serait établie toutes les 10 à 60 secondes, uniquement pour échanger ces informations de routage, d'où des coûts prohibitifs. Le routage Snapshot résout ce problème.

— NOTE —

Le routage Snapshot est disponible sur le système Cisco IOS, version 10.2 ou ultérieure.

Modèle de conception du routage Snapshot

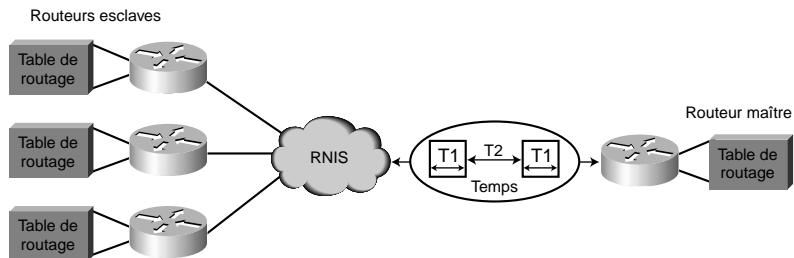
Le routage Snapshot utilise le modèle de conception client-serveur. Lorsqu'il est configuré, un routeur est désigné comme serveur Snapshot, et un ou plusieurs routeurs sont désignés comme clients Snapshot. Le serveur et les clients échangent des informations de routage durant une période active. Au début de cette période, le routeur client se connecte au routeur serveur afin d'échanger ces informations et, à l'issue de cette période, chaque routeur enregistre une capture des entrées dans sa table de routage. Celles-ci demeurent bloquées pendant une période de repos. A la fin de la période de repos, une autre période active commence, et le routeur client se connecte de nouveau au routeur serveur pour obtenir les dernières informations de routage. Le routeur client détermine la fréquence de ses appels vers le serveur. La période de repos peut durer jusqu'à 100 000 minutes (environ 69 jours).

Lorsque le routeur client passe des périodes de repos aux périodes actives, la ligne peut être impraticable ou occupée. Si cela se produit, le routeur devra attendre que s'écoule une autre période de repos avant de pouvoir mettre à jour sa table de routage, ce qui peut gravement affecter la connectivité si cette période est très longue. Pour éviter de devoir attendre la fin de la période de repos, le routage Snapshot a prévu une période de relance. Si la ligne n'est pas disponible à la fin de la période de repos, le routeur attend le temps spécifié par la période de relance, puis passe de nouveau dans une période active.

La période de relance est également utile dans des environnements qui utilisent la commutation de circuits dans lesquels il existe davantage de sites distants que de liaisons d'interface. Le site central pourrait disposer, par exemple, d'une interface PRI (avec 23 canaux B disponibles), mais appeler plus de 23 sites distants. Dans cette situation, il existe davantage de commandes de correspondances de numérotation que de lignes disponibles. Le routeur essaie les commandes **dialer map** dans

l'ordre et utilise l'intervalle de tentatives répétées pour les lignes auxquelles il ne peut immédiatement accéder (voir Figure 10.5).

Figure 10.5
Routeurs Snapshot en action.



Activation du routage Snapshot

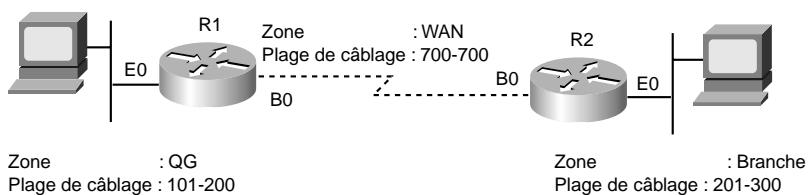
Le routage Snapshot est activé au moyen de commandes de configuration d'interface (voir Figure 10.6). Le routeur central est configuré pour le routage Snapshot, en appliquant la commande de configuration d'interface **snapshot server** sur son interface RNIS. Cette commande spécifie la longueur de la période active et indique si le routeur est autorisé à appeler les sites distants pour échanger des mises à jour de routage en l'absence d'un trafic régulier.

Les routeurs distants sont configurés pour le routage Snapshot, en appliquant la commande **snapshot client** sur chaque interface RNIS. Cette commande spécifie les variables suivantes :

- la durée de la période active (qui doit correspondre à celle spécifiée sur le routeur central) ;
- la durée de la période de repos ;
- si le routeur peut appeler le routeur central pour échanger des mises à jour de routage en l'absence d'un trafic régulier ;
- si les connexions qui sont établies pour échanger des données utilisateur peuvent être utilisées pour échanger les mises à jour de routage.

Lorsque le protocole de routage de l'épine dorsale n'est pas supporté par le routage Snapshot (par exemple OSPF ou EIGRP), les techniques standard de redistribution de routage peuvent être employées pour garantir que les mises à jour sont propagées entre les protocoles de routage, comme requis. Les précautions nécessaires devraient être prises pour assurer la redistribution de sous-réseaux, si besoin est, et éviter les boucles de routage.

Figure 10.6
Routage Snapshot AppleTalk.



- La configuration du routeur R1 de la figure est la suivante :

```
username R2 password SECRET
appletalk routing
isdn switch-type basic-5ess
!
interface BRI0
  encapsulation ppp
  appletalk cable-range 700-700 700.1
  appletalk zone WAN
  dialer map appletalk 700.2 name R2 speed 56 broadcast 5552222
dialer map snapshot 2 name R2 speed 56 broadcast 5552222
  dialer-group 1
snapshot client 5 60 dialer
  isdn spid1 5550066
  ppp authentication chap
!
dialer-list 1 protocol appletalk permit
```

- La configuration du routeur R2 est la suivante :

```
username R1 password SECRET
appletalk routing
isdn switch-type basic-5ess
interface BRI0
  encapsulation ppp
  appletalk cable-range 700-700 700.2
  appletalk zone WAN
  dialer wait-for-carrier-time 60
  dialer map appletalk 700.1 name R1 speed 56 broadcast 5550066
  dialer-group 1
snapshot server 5 dialer
  isdn spid1 5552222
  ppp authentication chap
!
dialer-list 1 protocol appletalk permit
```

Pour obtenir plus de détails sur le routage Snapshot, reportez-vous au Chapitre 21.

Secours commuté pour liaisons louées

Le secours commuté (*dial backup*) apporte une protection contre l'immobilisation d'un réseau étendu (WAN) en permettant à une connexion série dédiée de disposer d'une connexion de secours par circuits commutés. Le secours commuté peut être mis en œuvre de plusieurs façons : par le biais d'interfaces de secours (*backup interfaces*) ou au moyen de routes statiques flottantes (*floating static routes*).

Le secours commuté impose aux concepteurs d'utiliser des modèles de trafic différents de ceux des sites SOHO et ROBO qui supportent DDR. Lors de la conception des densités de port pour les lignes de secours par circuits commutés, examinez le nombre de liaisons susceptibles d'être défectiveuses simultanément en cas de panne générale, ainsi que le nombre de ports qui seraient nécessaires sur le site central dans le cas d'un scénario catastrophe. Une conception classique implique de choisir entre des modes d'appel entrant ou sortant, afin d'éviter une éventuelle contention lorsque les deux parties tentent de rétablir la connectivité.

Interfaces de secours

Une liaison série principale dédiée est configurée de façon à pouvoir disposer d'une interface de secours en cas de panne ou de dépassement des seuils de charge. En cas de défaillance de la liaison de l'interface principale ou du protocole de ligne, l'interface de secours est utilisée pour établir une connexion sur le site distant.

Une fois configurée, l'interface de secours demeure inactive, jusqu'à ce que l'une des conditions suivantes soit rencontrée :

- *Le protocole de ligne sur la liaison principale est défaillant.* La ligne de secours est alors activée, rétablissant la connexion entre les deux sites.
- *La charge de trafic sur la liaison principale dépasse une limite définie.* Cette charge est surveillée, et une valeur moyenne est calculée toutes les cinq minutes. Si cette valeur excède celle définie par l'utilisateur pour la liaison principale, la ligne de secours est activée. En fonction de la configuration de cette dernière, la totalité du trafic, ou une partie seulement, sera envoyée.

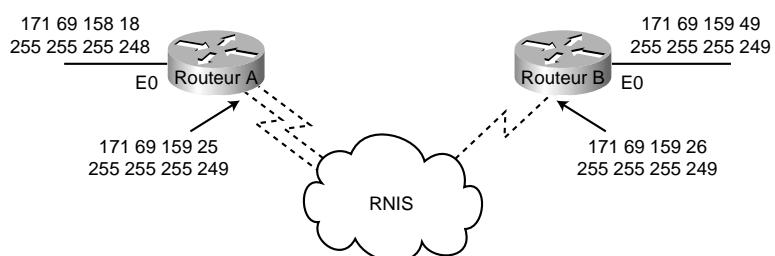
Une interface Cisco IOS est placée en mode de secours au moyen de la commande **backup interface** :

- La commande de configuration d'interface **backup interface** spécifie l'interface qui doit assurer la fonction de secours.
- La commande **backup load** spécifie le seuil de trafic en fonction duquel l'interface de secours doit être activée et désactivée.
- La commande **backup delay** spécifie le laps de temps qui doit s'écouler avant que l'interface de secours ne soit activée ou désactivée, suite à une période de transition de l'interface principale.

Les interfaces de secours sont généralement verrouillées dans état BACKUP (secours) afin de limiter leur utilisation à cette fonction. Les profils de numérotation éliminent ce verrouillage et permettent à l'interface physique d'être exploitée de plusieurs façons. La conception DDR de routes statiques flottantes élimine aussi ce verrouillage sur l'interface de numérotation.

Dans la Figure 10.7, une liaison louée relie le routeur A au routeur B, et l'interface BRI 0/2 sur le routeur B est utilisée en tant que ligne de secours.

Figure 10.7
Exemple de secours
commuté sur RNIS.



Avec la configuration suivante, l'interface BRI 2/0 (ligne de secours) est activée uniquement en cas de défaillance de l'interface série 1/0 (liaison principale). La commande **backup delay** configure la

connexion de secours afin qu'elle soit activée trente secondes après la défaillance de l'interface série 1/0 et qu'elle demeure active pendant soixante secondes après son rétablissement :

```
interface serial 1/0
    ip address 172.20.1.4 255.255.255.255.0
    backup interface bri 2/0
    backup delay 30 60
```

Avec la configuration suivante, l'interface BRI 2/0 est activée uniquement lorsque la charge sur l'interface série 1/0 dépasse 75 % de sa bande passante. La ligne de secours est désactivée lorsque la charge globale de la liaison principale et de la ligne de secours est inférieure à 5 % de la bande passante de la liaison principale :

```
interface serial 1/0
    ip address 172.20.1.4 255.255.255.255.0
    backup interface bri 2/0
    backup delay 75 5
```

Avec la configuration suivante, l'interface BRI 2/0 est activée uniquement en cas de défaillance de l'interface série 1/0 ou lorsque le trafic sur cette interface dépasse 25 % de sa bande passante. Si l'interface 1/0 est défaillante, dix secondes s'écouleront avant que l'interface BRI 2/0 ne devienne active. Une fois l'interface 1/0 rétablie, BRI 2/0 demeurera active pendant soixante secondes. Si cette interface a été activée suite à un dépassement de seuil de charge sur l'interface 1/0, elle sera désactivée lorsque la charge globale de la liaison principale et de la ligne de secours retombera en dessous de 5 % de la bande passante de l'interface 1/0 :

```
interface serial 1/0
    ip address 172.20.1.4 255.255.255.255.0
    backup interface bri 2/0
    backup load 25 5
    backup delay 10 60
```

Routes statiques flottantes

Le fonctionnement d'une interface de secours est déterminé par l'état de la liaison et du protocole de ligne sur la connexion principale. Il peut arriver que la connectivité de bout en bout soit perdue, mais, dans ce cas, le protocole de ligne demeure actif. Par exemple, l'état du protocole de ligne sur une liaison Frame Relay est déterminé par les messages ILMI en provenance du DCE (*Data Communication Equipment*, équipement de communication de données) ou commutateur Frame Relay. La connectivité vers le DCE Frame Relay ne garantit pas une connectivité de bout en bout.

La conception du secours commuté au moyen de routes statiques flottantes utilise les protocoles de maintenance de table de routage et de routage dynamique de Cisco IOS. Voyez le Chapitre 19 et ses exemples d'utilisation des routes statiques flottantes afin d'assurer le secours de liaisons louées.

Routes et mises à jour SAP statiques IPX

Avec DDR, vous devez configurer des routes statiques, car les mises à jour de routage ne peuvent être transmises sur des connexions DDR inactives. Pour créer des routes statiques vers des destinations spécifiques, utilisez la commande **ipx route**. Vous pouvez également configurer des mises à jour SAP statiques à l'aide de la commande **ipx sap** afin que les clients puissent toujours joindre un serveur particulier. De cette façon, vous pouvez déterminer les zones de votre réseau où les mises à jour SAP établiront des connexions à la demande.

Dans l'exemple suivant, le trafic pour le réseau 50 sera toujours envoyé à l'adresse 45.0000.0c07.00d3, et le trafic pour le réseau 75 sera toujours envoyé à l'adresse 45.0000.0c07.00de. Le routeur répondra aux requêtes GNS avec le serveur WALT si aucune connexion SAP dynamique n'est possible :

```
ipx route 50 45.0000.0c07.00d3
ipx route 75 45.0000.0c07.00de
ipx sap 4 WALT 451 75.0000.0000.0001.5
```

Configuration de zones statiques AppleTalk

Les routes et les zones AppleTalk statiques sont créées au moyen de la commande **appletalk static**, comme dans l'exemple suivant :

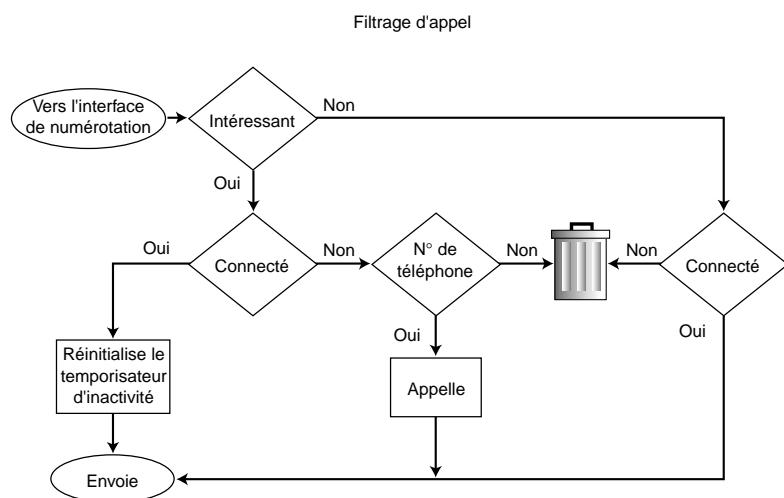
```
appletalk static cable-range 110-110 to 45.2 zone Marketing
```

Dans de nombreuses situations, la configuration manuelle de plages de câblage (*cable-range*) et de zones AppleTalk statiques se révélera coûteuse. L'utilisation du routage Snapshot devrait être envisagée pour assurer la mise en cache automatique.

Filtrage d'appel

Le filtrage d'appel (*dialer filtering*) est utilisé pour identifier tous les paquets qui traversent des connexions DDR comme *intéressants* ou *inintéressants*, à l'aide de listes de contrôle d'accès (ACL, *Access Control List*) [voir Figure 10.8]. Seuls les paquets jugés intéressants peuvent établir et maintenir une connexion DDR. C'est au concepteur DDR que revient la tâche de déterminer quels types de paquets sont inintéressants, et de créer des listes ACL afin d'empêcher que ces paquets ne provoquent des connexions inutiles.

Figure 10.8
Filtrage d'appel.



Lorsqu'un paquet est jugé inintéressant et qu'aucune connexion n'est établie, il est supprimé. En revanche, si une connexion a déjà été établie vers la destination spécifiée, le paquet jugé inintéressant

est envoyé sur la liaison, et le temporisateur d'inactivité n'est pas réinitialisé. Si le paquet est jugé intéressant et qu'il n'y a pas de connexion sur l'interface disponible, le routeur tente d'établir une connexion.

Chaque paquet qui arrive sur une interface de numérotation est filtré et identifié comme intéressant ou inintéressant, en fonction des commandes de configuration **dialer-group** (groupe de numérotation) et **dialer-list** (liste de numérotation). La configuration Cisco IOS de l'interface Dialer1 suivante utilise le groupe de numérotation 5 afin de déterminer quels paquets sont intéressants, selon les instructions de la liste de numérotation 5. Ces dernières définissent le groupe de numérotation 5 et déterminent que tous les paquets IP, IPX et AppleTalk sont intéressants :

```
interface Dialer1
dialer-group 5
!
dialer-list 5 protocol ip permit
dialer-list 5 protocol ipx permit
dialer-list 5 protocol appletalk permit
!
```

Le système Cisco IOS supporte à présent de nombreux protocoles de filtrage d'appel, comme le montre la rubrique dialer-list de l'aide en ligne :

```
kdt-3640(config)#dialer-list 5 protocol ?
    appletalk AppleTalk
    bridge Bridging
    clns OSI Connectionless Network Service
    clns_es CLNS End System
    clns_is CLNS Intermediate System
    decnet DECnet
    decnet_node DECnet node
    decnet_router-L1 DECnet router L1
    decnet_router-L2 DECnet router L2
    ip IP
    ipx Novell IPX
    llc2 LLC2
    vines Banyan Vines
    xns XNS
```

Filtrage par listes ACL

Il est possible de mettre en œuvre un filtrage d'appels plus granulaire pour chaque protocole en définissant des listes de contrôle d'accès (ACL) Cisco IOS. Par exemple, la configuration suivante définit le trafic SNMP comme inintéressant, au moyen de la liste de numérotation 3 et de listes ACL étendues :

```
dialer-list protocol ip 3 list 101
!
access-list 101 deny udp any any eq snmp
access-list 101 permit ip any any
```

Les effets des mises à jour de routage et des services d'annuaire sur les interfaces de numérotation peuvent être gérés à l'aide de plusieurs techniques, telles que le routage statique et, par défaut, les interfaces passives et les correspondances de numérotation non broadcast. En ce qui concerne les solutions qui nécessitent le routage dynamique et ne peuvent utiliser Snapshot, les informations

de routage peuvent néanmoins être supportées sur la liaison RNIS, puis jugées inintéressantes par le processus de filtrage d'appels.

Par exemple, si la conception du réseau requiert des paquets de mises à jour de routage IGRP, ceux-ci peuvent être filtrés par l'intermédiaire de listes d'accès, afin d'éviter l'établissement de connexions DDR inutiles, comme suit :

```
access-list 101 deny igrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Vous pouvez utiliser l'une des deux listes d'accès suivantes pour identifier le trafic EIGRP comme inintéressant :

```
access-list 101 deny eigrp any any
access-list 101 deny ip any 224.0.0.10.0.0.0.0
```

La première liste d'accès rejette tout le trafic EIGRP ; la seconde rejette l'adresse multicast (224.0.0.10) utilisée par EIGRP pour ses mises à jour. Lorsque vous employez des listes d'accès pour contrôler le trafic EIGRP, vous devez configurer des routes statiques sur la liaison RNIS. Une fois la connexion DDR établie, les mises à jour de routage peuvent circuler sur la ligne. Lors de la conception du filtrage d'appel, il est important de comprendre à quel niveau les requêtes de mise à jour et de service sont utiles et à quel niveau ces types de paquets peuvent être filtrés en toute sécurité.

Il faut examiner attentivement les protocoles de services d'annuaire et les applications de réseau qui doivent être supportés sur chaque site. Bon nombre de protocoles et d'applications peuvent provoquer l'établissement et la maintenance de connexions DDR, d'où parfois des charges WAN invraisemblables s'ils ne sont pas correctement surveillés et filtrés. N'attendez pas de recevoir votre facture téléphonique pour procéder à une analyse approfondie du trafic et des coûts de votre réseau. Si vous êtes concerné par les coûts WAN, implémentez des outils de surveillance afin d'obtenir un retour d'informations rapide sur la fréquence et la durée des connexions. (Les problèmes de réduction des coûts sont traités au Chapitre 11.)

SNMP

Bien que le protocole SNMP puisse fournir des informations utiles sur les connexions RNIS et la façon dont elles sont exploitées, son utilisation peut provoquer un accroissement excessif des temps d'activité sur les liaisons RNIS. Par exemple, HP Open View collecte des informations en interrogeant régulièrement le réseau à la recherche d'événements SNMP. Ces interrogations entraînent un établissement plus fréquent de connexions RNIS pour vérifier que les routeurs distants sont toujours opérationnels, ce qui augmente les frais d'utilisation de RNIS. Pour contrôler ces frais, le site central doit filtrer les paquets SNMP à destination des sites distants *via* RNIS. Les paquets SNMP en provenance de sites distants peuvent toujours être autorisés, ce qui permet aux interceptions SNMP de circuler vers la plate-forme de gestion SNMP. De cette manière, si un dispositif SNMP est défaillant sur un site distant, l'alerte atteindra la plate-forme de gestion SNMP sur le site central.

Pour contrôler le trafic SNMP, créez une liste d'accès qui refuse les paquets SNMP. Voici un exemple de filtrage de paquets SNMP :

```
access-list 101 deny tcp any any eq 161
access-list 101 deny udp any any eq snmp
access-list 101 permit ip any any
!
dialer-list 1 list 101
```

Paquets IPX

Sur les réseaux Novell IPX, il faut envisager le filtrage des mises à jour de routage au niveau des interfaces DDR pour les protocoles répertoriés dans le Tableau 10.3.

Tableau 10.3 : Cycles des paquets de mises à jour Novell IPX

Type de paquet	Cycle de mise à jour périodique
RIP	60 secondes
SAP	60 secondes
Sérialisation	66 secondes

Vous pouvez utiliser des listes d'accès pour déclarer intérressants les paquets à destination du socket de sérialisation Novell (numéro de protocole 0, numéro de socket 457), les paquets RIP (numéro de protocole 1, numéro de socket 453), les paquets SAP (numéro de protocole 4, numéro de socket 452) et les paquets de diagnostic générés par la fonctionnalité de découverte automatique (numéro de protocole 4, numéro de socket 456). Les paquets intérressants sont supprimés et ne provoquent pas l'initialisation de connexions. (Un exemple de liste d'accès IPX est présenté au Chapitre 21.)

IPX envoie plusieurs types de paquets (paquets *watchdog* IPX et paquets *keepalive* SPX) qui peuvent provoquer des connexions inutiles lorsqu'ils ne sont pas contrôlés. De plus, NetWare inclut un protocole de synchronisation horaire qui entraîne lui aussi l'établissement de connexions inutiles s'il n'est pas contrôlé.

Les réseaux Novell IPX utilisent plusieurs types de paquets de mises à jour qu'il faut parfois filtrer au moyen de listes d'accès. Les hôtes Novell diffusent en mode broadcast des paquets de sérialisation à des fins de protection contre la copie. Les mises à jour des tables de routage RIP et les annonces de service SAP sont diffusées en broadcast toutes les 60 secondes. Les paquets de sérialisation sont envoyés environ toutes les 66 secondes.

Dans l'exemple suivant, la liste d'accès 901 identifie les paquets SAP (452), RIP (453) et de sérialisation (457) comme intérressants, et les types de paquets IPX inconnu/tous (0), tous ou RIP (1), tous ou SAP (4), SPX (5), NCP(7) et NetBIOS (20) comme intéressants :

```
access-list 901 deny 0 FFFFFFFF 452
access-list 901 deny 4 FFFFFFFF 452
access-list 901 deny 0 FFFFFFFF 453
access-list 901 deny 1 FFFFFFFF 453
access-list 901 deny 0 FFFFFFFF 457
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 452
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 453
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 457
access-list 901 permit 0
access-list 901 permit 1
access-list 901 permit 2
access-list 901 permit 4
access-list 901 permit 5
access-list 901 permit 17
```

Vous pouvez autoriser n'importe quel autre type de paquet IPX, si besoin est. Depuis la version 10.2 du système Cisco IOS, la configuration des listes d'accès Novell IPX a été améliorée grâce au support du caractère générique (**-1**). Voici ce que donnerait l'exemple précédent :

```
access-list 901 deny -1 FFFFFFFF 452
access-list 901 deny -1 FFFFFFFF 453
access-list 901 deny -1 FFFFFFFF 457
access-list 901 deny -1 FFFFFFFF 0 FFFFFFFF 452
access-list 901 deny -1 FFFFFFFF 0 FFFFFFFF 453
access-list 901 deny -1 FFFFFFFF 0 FFFFFFFF 457
access-list 901 permit -1
```

Contrôle des paquets *watchdog IPX*

Les serveurs NetWare envoient des paquets *watchdog* aux clients et déconnectent ceux qui ne répondent pas. Lorsque la simulation *watchdog IPX* est activée, le routeur local au serveur NetWare répond aux paquets *watchdog* à la place des clients du serveur. La simulation *watchdog IPX* permet aux clients de rester connectés aux serveurs sans avoir besoin d'envoyer constamment des paquets sur la liaison RNIS. Cette fonctionnalité est particulièrement importante pour contrôler les temps d'activité des liaisons RNIS. La commande de configuration d'interface qui permet d'activer cette fonctionnalité est **ipx watchdog-spoof**.

Contrôle des paquets *keepalive SPX*

Certains services fondés sur SPX (*Sequenced Packet Exchange*) dans les environnements Novell utilisent des paquets *keepalive*. Ces paquets servent à vérifier l'intégrité des communications de bout en bout lorsque des transmissions avec garantie de livraison et séquencement des paquets sont nécessaires. La fréquence de génération de ces paquets peut être ajustée par l'utilisateur ; elle est de cinq secondes par défaut, mais peut accepter une fréquence minimale de quinze minutes. La simulation SPX, telle qu'elle est implémentée dans le système Cisco IOS, reçoit, reconnaît et acquitte avec succès les paquets *keepalive* à la fois sur l'extrémité serveur et sur l'extrémité client.

Serveurs de temps et paquets de répliques NDS

NetWare 4.x inclut un protocole de synchronisation horaire qui provoque l'envoi de mises à jour toutes les dix minutes de la part des serveurs de temps NetWare 4.x. Pour éviter que ces serveurs ne génèrent des paquets de mises à jour qui déclenchaient l'établissement de connexions inutiles, vous devez charger un module NetWare (NLM, *NetWare-loadable Module*) appelé TIME-SYNC.NLM, qui permet d'augmenter l'intervalle de synchronisation jusqu'à plusieurs jours.

Un problème analogue est causé par les tentatives de synchronisation de répliques (*replica*) NDS. NetWare 4.1 inclut deux modules NLM, DSFILTER.NLM et PINGFILT.NLM, qui fonctionnent de concert pour contrôler les mises à jour de synchronisation NDS. Utilisez-les pour garantir que le trafic de synchronisation NDS sera envoyé aux serveurs spécifiés uniquement à des horaires précis.

Filtrage AppleTalk

Les services d'annuaire conviviaux d'AppleTalk se fondent sur des noms de zones et sur le protocole NBP (*Name Binding Protocol*). Des applications, tel le Sélecteur MacOs (*Chooser*), utilisent des recherches NBP (*lookup*) pour rechercher des services, tels que AppleShare, par noms de zone.

Certaines applications utilisent ces services de façon excessive et émettent des diffusions broadcast sur toutes les zones, sans tenir compte des réseaux DDR. Cela provoque en retour le déclenchement de demandes d'ouverture de ligne. Des applications comme QuarkXpress et 4D utilisent des diffusions broadcast sur toutes les zones pour examiner périodiquement le réseau à des fins de contrôle de licence, ou pour fournir des liens vers d'autres ressources du réseau. La commande **test appletalk:nbp lookup** combinée avec la commande **debug dialer** surveille le trafic NBP et peut vous aider à déterminer les types de paquets qui déclenchent l'établissement de connexions.

Depuis la version 11.0 de Cisco IOS, vous pouvez filtrer les paquets NBP en fonction du nom, du type et de la zone du dispositif émetteur. Le filtrage NBP AppleTalk permet aux routeurs Cisco de créer des pare-feu, des déclencheurs de demandes d'ouverture de ligne et des options de gestion de file d'attente, en se fondant sur n'importe quel type ou objet NBP. (Voyez le Chapitre 21 pour obtenir un exemple de configuration.) Enfin, si les applications qui utilisent NBP ont été isolées, consultez leurs fabricants et demandez-leur comment contrôler ou éliminer le trafic NBP.

Certaines applications Macintosh envoient périodiquement des recherches NBP vers toutes les zones pour de nombreuses raisons : contrôle des numéros de série identiques à des fins de protection contre la copie, recherche automatique d'autres serveurs, etc. Il en résulte que les liaisons RNIS sont activées fréquemment, d'où un gaspillage. Dans les versions 11.0 (2.1) ou ultérieures de Cisco IOS, les routeurs Cisco autorisent l'utilisateur à configurer le filtrage NBP sur les listes de numérotation en vue d'éviter ce problème. Pour cela, vous devez remplacer la ligne suivante sur les deux routeurs :

```
dialer-list 1 protocol appletalk permit
```

par ces lignes :

```
dialer-list 1 list 600  
  
access-list 600 permit nbp 1 type AFPServer  
access-list 600 permit nbp 2 type LaserWriter  
access-list 600 deny other-nbps  
access-list 600 permit other-access broadcast-deny
```

Cet exemple indique que les recherches NBP déclencheront l'établissement d'une connexion RNIS pour deux services uniquement. Si vous voulez autoriser d'autres types de services, ajoutez-les dans l'exemple avant l'instruction **deny other-nbps**. Vérifiez que les numéros de séquences sont différents, sinon ils remplaceront les précédents. Par exemple, si vous souhaitez aussi permettre que les recherches NBP déclenchent l'établissement d'une connexion pour le service DeskWriter, la liste ressemblera à ce qui suit :

```
dialer-list 1 list 600  
  
access-list 600 permit nbp 1 type AFPServer  
access-list 600 permit nbp 2 type LaserWriter  
access-list 600 permit nbp 3 type DeskWriter  
access-list 600 deny other-nbps  
access-list 600 permit other-access broadcast-deny
```

NOTE

Les serveurs AppleShare utilisent le protocole AFP (*Apple Filing Protocol*) pour envoyer des *ticks* environ toutes les trente secondes aux clients AppleShare connectés. Ces *ticks* permettent aux connexions DDR de rester actives. Pour éviter les connexions DDR inutiles, vous devez annuler manuellement le montage des serveurs AppleTalk ou y installer un logiciel qui déconnecte automatiquement les utilisateurs après une période d'inactivité.

Paquets Banyan VINES, DECnet et OSI

Cisco IOS 10.3 a introduit les listes d'accès pour les protocoles Banyan VINES, DECnet IV et OSI. Lorsque des correspondances de numérotation sont configurées pour ces protocoles, des listes d'accès peuvent être utilisées afin de déterminer les paquets intéressants (c'est-à-dire les paquets qui déclencheront l'ouverture d'une ligne à la demande).

Routage à la demande et PPP

Plusieurs aspects du routage à la demande sont utilisés pour fournir des fonctionnalités DDR entre les routeurs locaux et distants. Les principales fonctionnalités sont les correspondances de numérotation (*dialer map*), l'encapsulation PPP, l'authentification CHAP, les groupes de rotation de numérotation, et la commande **pulse-time**. Les lignes de commentaires dans l'exemple suivant expliquent l'utilisation de ces fonctionnalités :

```
interface dialer 1
ip address 130.100.120.10 255.255.255.0
!
!Le type d'encapsulation sur l'interface dialer 1 est PPP.
encapsulation ppp
!
!Le type d'authentification pour PPP sur l'interface dialer 1 est CHAP.
ppp authentication chap
!
!Cette commande fait de l'interface une interface DDR.
dialer in-band
!
!Cette commande associe l'interface au groupe de numérotation d'accès,
!qui est défini avec la commande dialer-list
dialer group 1
!
! Cette commande autorise le site distant sanjose et le site central
! à s'appeler. La chaîne de numérotation 5555555 est le numéro de
! téléphone du site distant qui est utilisé pour l'appeler. Le nom
! sanjose est utilisé lorsque le site distant appelle le site central.
dialer map ip 130.100.120.15 name sanjose 5555555
!
! Cette commande n'utilise aucune chaîne définie ce qui permet au
! site distant sanjose d'appeler le site central, mais n'autorise
! pas ce dernier à appeler le site distant.
dialer map ip 130.120.100.15 name sanjose
!
! Cette commande définit un intervalle de cinq secondes pour les
! signaux DTR sur les interfaces DDR du groupe de numérotation 1.
! Cet intervalle long permet au modem de déterminer lorsque des
! signaux ont été supprimés.
```

```
pulse-time 5
!
! Ces commandes placent les interfaces série asynchrones 1 et 2
! dans le groupe de rotation de numérotation 1. Les sous-commandes
! d'interface appliquées au groupe 1 (par exemple, encapsulation PPP
! et CHAP) s'appliquent à ces interfaces.
interface async 1
dialer rotary-group 1
interface async 2
dialer rotary-group 1
! Les mots de passe CHAP sont spécifiés pour les serveurs distants.
username sanjose password cisco
username rtp password cisco
```

Authentification

L'authentification apporte deux fonctions dans la conception de réseaux DDR : la sécurité et le suivi des connexions. Comme la majorité des réseaux DDR se connectent au réseau téléphonique public commuté, il est impératif d'implémenter un modèle de sécurité fiable pour empêcher des accès non autorisés aux ressources sensibles. L'authentification permet également à DDR d'effectuer un suivi des sites qui sont actuellement connectés et autorise la création de faisceaux MultiLink PPP. Les sujets suivants sont traités dans cette section :

- l'authentification PPP ;
- le protocole CHAP (*Challenge Handshake Authentication Protocol*) ;
- le protocole PAP (*Password Authentication Protocol*) ;
- la sécurité RNIS ;
- la fonction de rappel DDR ;
- les listes d'accès IPX.

Authentification PPP

L'authentification PPP *via* CHAP ou PAP (comme décrit dans le RFC 1334) devrait être utilisée pour fournir une sécurité sur les connexions DDR. L'authentification PPP a lieu après que LCP (*Link Control Protocol*) a été négocié sur la connexion DDR, mais avant que les protocoles de réseau n'aient été autorisés à circuler. Elle est négociée en tant qu'option LCP et est bidirectionnelle, ce qui signifie que chaque partie peut authentifier l'autre. Dans certains environnements, il peut être nécessaire d'activer l'authentification PPP du côté appelé uniquement (ce qui signifie que le côté appelant n'authentifie pas le côté appelé).

Protocole CHAP

Avec CHAP, un équipement distant qui tente de se connecter sur le routeur local se voit présenter un défi (*challenge*), CHAP contenant le nom d'hôte et une valeur de départ (*seed*) pour le défi. Lorsque le routeur distant reçoit le défi, il examine le nom d'hôte qui y est contenu et le renvoie avec une réponse CHAP dérivée de la valeur de départ et du mot de passe pour ce nom d'hôte. Les mots de passe doivent être identiques sur l'équipement distant et sur le routeur local. Les noms et mots de passe sont

configurés au moyen de la commande **username**. Dans l'exemple suivant, le routeur nas3600A autorisera le routeur c1600A à l'appeler en utilisant le mot de passe "bubble" :

```
hostname nas3600A
username c1600A password bubble
!
interface dialer 1
ppp authentication chap callin
```

Dans l'exemple suivant, le routeur Macduff autorisera le routeur Macbeth à l'appeler en utilisant le mot de passe "bubble" :

```
hostname nas3600A
username c1600A password bubble
!
interface dialer 1
encapsulation ppp
dialer in-band
dialer-groupe 5
dialer map ip 172.20.1.1 name nas3600A 18355558661
ppp authentication chap callin
```

Les étapes décrites ci-dessous illustrent le fonctionnement de CHAP :

1. c1600A appelle nas3600A, puis LCP est négocié.
2. nas3600A met c1600A au défi avec : <nas3600A/chaîne_de_défi>.
3. c1600A recherche le mot de passe pour le nom d'utilisateur nas3600A, puis génère la chaîne de réponse (chaîne_de_réponse).
4. c1600A envoie une réponse à nas3600A : <c1600A/chaîne_de_réponse>.
5. nas3600A examine le mot de passe pour le nom d'utilisateur c1600A, puis génère la chaîne de réponse (chaîne_de_réponse) prévue. Si la chaîne de réponse reçue correspond à celle prévue, l'authentification PPP est réussie, et PPP peut négocier les protocoles de contrôle de réseau (tel IPCP). Si l'authentification PPP échoue, le site distant est déconnecté.

Protocole PAP

A l'instar de CHAP, PAP est un protocole d'authentification utilisé par PPP. Néanmoins, PAP est moins sûr que CHAP, car ce dernier transmet une version cryptée du mot de passe sur la ligne physique, alors que PAP communique le mot de passe en clair, ce qui l'expose aux attaques par *sniffer* (outil de surveillance de réseau).

Lorsque l'accès est authentifié avec PAP, le routeur examine le nom d'utilisateur qui correspond à la ligne de correspondance de numérotation utilisée pour initier l'appel. Lorsqu'il est authentifié avec PAP lors d'un appel entrant, PAP recherche le nom d'utilisateur associé à son nom d'hôte (car aucune correspondance de numérotation n'a été utilisée pour initier la connexion).

Dans l'exemple de configuration suivant, le routeur NAS authentifiera l'homologue avec PAP lorsqu'il répondra à l'appel DDR, puis comparera le résultat à la base de données locale :

```
hostname nas3600A
aaa new-model
aaa authentication ppp default local
username c2500A password freedom
username nas3600A password texas
```

```
!
interface Dialer1
encapsulation ppp
ppp authentication pap
```

Sécurité RNIS

DDR RNIS peut utiliser l'identifiant d'appelant (*caller-ID*) afin d'améliorer la sécurité en configurant l'appelant RNIS sur les interfaces RNIS entrantes. Les appels entrants sont filtrés pour vérifier que l'identifiant de la ligne appelante provient d'une origine connue. Toutefois, ce filtrage nécessite une connexion RNIS de bout en bout qui permet de fournir l'identifiant de l'appelant au routeur.

Fonction de rappel DDR

Les environnements DDR peuvent être configurés afin d'exploiter la fonction de rappel (*callback*). Lorsqu'un site distant appelle un site central (ou inversement), ce dernier peut être configuré pour déconnecter le site distant, puis initier une connexion sortante vers ce site.

Cette fonction permet d'accroître la sécurité en garantissant que le site distant ne peut se connecter qu'à partir d'un seul emplacement, comme défini par le numéro de rappel. Cette fonction améliore également l'administration en centralisant la facturation des connexions distantes.

Listes d'accès IPX

Les liste d'accès déterminent si les paquets sont intéressants ou inintéressants. Les paquets jugés intéressants provoquent l'activation automatique des connexions DDR ; les paquets jugés inintéressants ne déclenchent pas leur établissement. Néanmoins, si une connexion DDR est active, les paquets jugés inintéressants seront quand même transmis à travers cette liaison.

Résumé

Lors de la conception de réseaux DDR, examinez le type de la topologie : point-à-point, hub-and-spoke ou totalement maillée. Etudiez également le type de schéma d'adressage utilisé et les problèmes de sécurité. Gardez à l'esprit que le choix du média influence la façon dont les paquets sont envoyés. Définissez la destination des paquets en configurant des routes statiques, des zones et des services. Déterminez de quelle manière les paquets atteignent leur destination, en configurant des interfaces de numérotation et en associant les adresses et les numéros de téléphone. Enfin, déterminez à quel moment le routeur devra établir la connexion, en définissant des paquets intéressants et inintéressants, ce qui élimine les diffusions broadcast AppleTalk inutiles et les paquets de simulation *watchdog* IPX. Ces recommandations vous aideront à implémenter des réseaux évolutifs, présentant un rapport équilibré entre les performances, la tolérance aux pannes et le coût.

Pour obtenir davantage d'informations sur la création de réseaux DDR, avec des exemples de protocoles, voyez les Chapitres 11, 20 et 21.

Conception de réseaux RNIS

Par Salman Asad

Le réseau RTC (*Réseau Téléphonique Commuté*) a été transformé en un réseau numérique à intégration de services, appelé RNIS (en anglais ISDN, *Integrated Systems Digital Network*). Le respect des normes internationales du système de signalisation SS7 (*Signalling System 7*) permet de mettre en œuvre des communications internationales numériques à 64 Kbit/s, sans restriction. RNIS a facilité l'intégration de divers services de téléphonie, tels que l'identification de l'appelant, le rappel automatique sur occupation, la conférence à trois, etc., ainsi que des services de transmission de données qui incluent l'audioconférence, la visioconférence, l'Internet, le transfert de fichiers, l'interconnexion de réseaux, etc. Grâce aux services de l'accès RNIS de base avec l'interface BRI (*Basic Rate Interface*) et de l'accès RNIS primaire avec l'interface PRI (*Primary Rate Interface*), la commutation d'appels RNIS peut être étendue jusqu'aux équipements de télécommunication du client (CPE, *Customer Premises Equipment*) et fournir ainsi des chemins numériques de bout en bout.

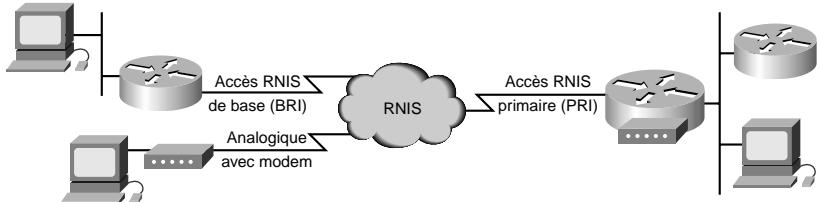
Avant la disponibilité de RNIS, la connectivité sur le réseau RTC était simplement assurée au moyen du service téléphonique classique, avec un modem analogique. La connectivité sur RNIS offre aux concepteurs de réseaux une bande passante accrue, une réduction du temps nécessaire à l'établissement des connexions, une latence réduite et des rapports signal/bruit inférieurs.

RNIS est maintenant déployé rapidement dans de nombreuses applications, telles que le routage par ouverture de ligne à la demande ou DDR (*Dial-on-Demand Routing*), le secours par ligne communiquée, la connectivité SOHO (*Small Office/Home Office*, petit bureau/bureau à domicile) et ROBO (*Remote Office/Branch Office*, bureau distant/bureau d'agence), ainsi que l'agrégation de pools de

modems. Ce chapitre étudie la conception de ces applications. Son principal objectif est d'examiner les problèmes de conception associés à la création de réseaux RNIS. Pour étudier des exemples spécifiques, reportez-vous aux chapitres qui présentent des études de cas sur le sujet.

A la Figure 11.1, RNIS est utilisé pour assurer simultanément des accès numériques et des accès par modems pour des sites distants qui emploient une solution de connexion hybride.

Figure 11.1
RNIS peut supporter des solutions de numérotation hybrides (analogique et numérique).



Applications de RNIS

RNIS a plusieurs applications dans la mise en œuvre de réseaux. Le système d'exploitation Cisco IOS est depuis longtemps utilisé pour élaborer des solutions qui implémentent DDR et le secours par ligne commutée pour la connectivité ROBO. Plus récemment, RNIS a fait l'objet d'implémentations croissantes pour gérer la connectivité SOHO. Dans le cadre de ce livre, le côté appelant de RNIS sera désigné par le terme SOHO; le côté répondant par NAS (*Network Access Server*, serveur d'accès au réseau), sauf spécification particulière. Cette section traite des sujets suivants :

- le routage DDR ;
- le secours par ligne commutée ;
- la connectivité SOHO ;
- l'agrégation de modems.

Routage DDR

La connectivité permanente par l'intermédiaire de RNIS est simulée par des routeurs Cisco IOS, au moyen de DDR. Lorsque des paquets qualifiés arrivent sur une interface de numérotation, la connectivité est établie sur RNIS. Après une certaine période d'inactivité (préconfigurée), la connexion RNIS est libérée. Des canaux B RNIS peuvent être ajoutés et supprimés du faisceau MultiLink PPP, par le biais de seuils configurables. La Figure 11.2 illustre l'emploi de DDR pour la connexion de sites distants avec RNIS.

Figure 11.2
DDR crée la connexion entre des sites RNIS.

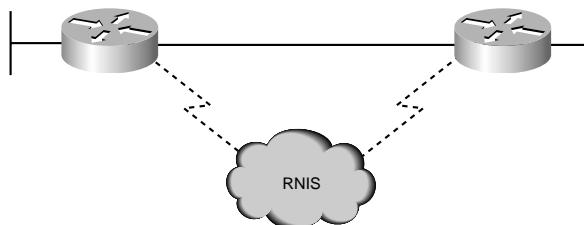


Liaison de secours par ligne commutée

RNIS peut être utilisé en tant que service de secours pour une ligne louée entre un bureau distant et un site central. Si le lien principal est défaillant, une connexion par circuit commuté RNIS est établie, et le trafic est rerouté *via* RNIS. Lorsque le lien principal est rétabli, le trafic y est de nouveau redirigé, et la ligne RNIS est désactivée.

Le secours par ligne commutée peut être réalisé au moyen de routes statiques (*floating static routes*) et de DDR, ou à l'aide des commandes d'interface backup. Cette fonction peut également être configurée sur la base de seuils de trafic du lien principal. Si la charge sur le lien principal excède une valeur définie par l'utilisateur, la ligne RNIS de secours est activée, afin d'augmenter la bande passante disponible entre les deux sites (voir Figure 11.3).

Figure 11.3
RNIS peut fournir une solution de secours pour un lien principal entre des sites.

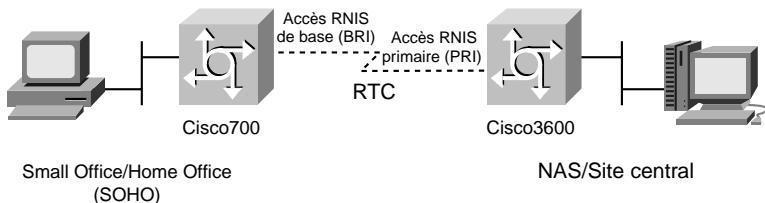


Connectivité SOHO

Les sites SOHO (*Small Office/Home Office*) peuvent maintenant être supportés de façon rentable, grâce aux services de l'interface BRI de l'accès RNIS de base. Les sites SOHO occasionnels ou permanents ont ainsi la possibilité de se connecter aux sites de leur entreprise, ou à l'Internet, en bénéficiant de vitesses beaucoup plus élevées que celles permises par la téléphonie classique, avec l'emploi de modems.

La connectivité SOHO implique en général l'emploi exclusif de la ligne commutée (connexions initiées par SOHO). Elle peut tirer profit des technologies émergeantes de traduction d'adresses, telles que PAT (*Port and Address Translation*, traduction d'adresses et de ports) — supportée par la série Cisco 700 — et EZIP — du système Cisco IOS —, pour simplifier la conception et l'exploitation. A l'aide de ces fonctions, le site SOHO peut supporter plusieurs équipements, mais apparaît, pour le serveur NAS Cisco IOS, comme étant une seule adresse IP (voir Figure 11.4).

Figure 11.4
Un site SOHO peut apparaître, pour le NAS Cisco IOS, comme étant un nœud IP unique.



Agrégation de modems

L'exploitation de modems en racks ainsi que du câblage associé a été éliminée, et remplacée par l'intégration de cartes modem numériques, sur les serveurs NAS Cisco IOS. Cette intégration rend possible l'emploi de technologies de modems à 56 Kbit/s. Des solutions de numérotation hybrides peuvent être élaborées au moyen d'un seul numéro de téléphone, afin de fournir une connectivité par modem analogique et RNIS (voir Figure 11.1).

Elaboration de solutions RNIS

RNIS ne résout pas à lui seul les problèmes d'interconnexion. A l'aide de DDR ou de sessions initiées par l'utilisateur, RNIS peut fournir au concepteur un chemin de données sur lequel des liens PPP peuvent être négociés. Pour pouvoir exploiter le réseau RTC, en vue d'apporter une connectivité de réseau, il faut examiner attentivement les questions liées à la sécurité et à la limitation des coûts.

Cette section présente les problèmes de conception associés à RNIS, qui seront ensuite traités plus en détail dans les prochaines sections :

- connectivité RNIS ;
- encapsulation de datagrammes ;
- routage DDR ;
- problèmes de sécurité ;
- limitation des coûts.

Connectivité RNIS

La connectivité RNIS est assurée au moyen d'interfaces physiques : PRI pour l'accès RNIS primaire, et BRI pour l'accès RNIS de base. Une seule interface fournit un faisceau multiplexé de canaux B et D. Le canal B (*Bearer*) fournit des services de transport de données ou de la voix sur une bande passante élevée (jusqu'à 64 Kbit/s par canal B). Le canal D (*Delta*) sert à la signalisation et au contrôle, et peut également être utilisé pour les applications de données qui réclament peu de bande passante.

Le service d'accès RNIS de base est assuré sur une boucle locale, exploitée traditionnellement pour la commutation vers un service téléphonique analogique. L'accès RNIS de base met à la disposition de l'abonné deux canaux B à 64 Kbit/s et un canal D à 16 Kbit/s (2B + D).

Le service d'accès RNIS primaire est assuré sur des lignes louées T1 ou E1 traditionnelles, qui relient l'équipement du client (CPE) et le commutateur RNIS :

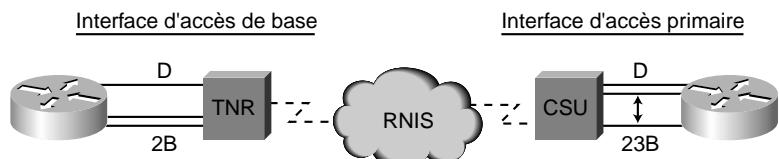
- l'accès RNIS primaire sur une ligne T1 fournit 23 canaux B à 64 Kbit/s et un canal D à 64 Kbit/s (23B + D) ;
- l'accès RNIS primaire sur une ligne E1 fournit 30 canaux B à 64 Kbit/s et un canal D à 64 Kbit/s (30B + D).

L'exploitation des services de l'accès RNIS primaire et de l'accès RNIS de base impose des exigences strictes en matière d'équipements physiques, ainsi que de câblage sur la portion entre le commutateur RNIS et l'équipement RNIS du client. Les installations classiques peuvent impliquer

des délais supplémentaires, ainsi que l'obligation de travailler avec des groupes de support dédiés au sein de l'environnement de votre fournisseur de services RNIS (voir Figure 11.5).

Figure 11.5

Connectivité RNIS avec les interfaces BRI et PRI.



Encapsulation de datagrammes

Lorsque DDR (ou un utilisateur) établit un lien de bout en bout à travers RNIS, on recourt à une méthode d'encapsulation de datagrammes afin d'assurer le transport des données. Les techniques d'encapsulation disponibles pour la conception avec RNIS sont PPP, HDLC, X.25 et V120. La technologie X.25 peut également être utilisée pour la livraison de datagrammes sur le canal D.

La plupart des réseaux utilisent le protocole PPP comme méthode d'encapsulation. Ce protocole est un mécanisme point-à-point puissant et modulaire, qui permet d'établir des liaisons de données, d'apporter une sécurité et d'encapsuler le trafic. Il est négocié entre les homologues qui communiquent chaque fois qu'une connexion est établie. Les liens PPP peuvent ensuite être utilisés par les protocoles de réseau tels IP et IPX. Les solutions PPP peuvent supporter l'agrégation de bandes passantes au moyen de MultiLink PPP, en vue d'améliorer le débit, ce qui offre davantage de bande passante aux applications de réseau.

Routage DDR

Les concepteurs d'applications de réseau doivent déterminer de quelle façon les connexions RNIS seront initiées, maintenues et libérées. DDR est constitué d'un ensemble de fonctions sophistiquées du système d'exploitation Cisco IOS, qui établit et libère de façon intelligente les connexions de circuits commutés, selon les besoins du trafic transporté sur le réseau. DDR peut simuler le routage et les services d'annuaire de différentes manières, afin de donner l'illusion d'une connectivité permanente à travers des connexions de circuits commutés. Reportez-vous au Chapitre 10 pour plus de renseignements sur la conception DDR.

Problèmes de sécurité

Les équipements de réseau peuvent aujourd'hui être connectés via le réseau RTC, il est donc impératif de concevoir un modèle de sécurité robuste, afin de protéger votre réseau. Le système d'exploitation Cisco IOS utilise le modèle AAA pour mettre en œuvre une sécurité. RNIS propose l'utilisation des informations d'identification de l'appelant et du numéro appelé (DNIS, *Dialed Number Information Service*) afin d'apporter davantage de souplesse dans la conception de la sécurité.

Limitation des coûts

L'objectif principal de l'exploitation de RNIS sur un réseau est d'éviter les coûts associés aux services de connexion permanente, tels que les lignes louées ou le Frame Relay. A cet effet, il est très

important d'évaluer les profils de trafic de données et de surveiller ceux d'utilisation des services RNIS, afin de vous assurer que les coûts WAN sont bien contrôlés. La fonction de rappel de l'appelant peut également être utilisée pour centraliser la facturation.

Problèmes de connectivité avec RNIS

En fonction des besoins applicatifs et de l'ingénierie de trafic (*traffic engineering*), les services d'accès RNIS de base ou d'accès RNIS primaire sont sélectionnés sur chaque site afin d'établir une connectivité RNIS. Sur certains sites, l'ingénierie de trafic peut nécessiter plusieurs services d'accès de base ou primaires. Une fois la connexion RNIS établie par l'intermédiaire de ces interfaces, les services RNIS de bout en bout doivent être implémentés. Cette section couvre les sujets suivants, liés à la connectivité RNIS :

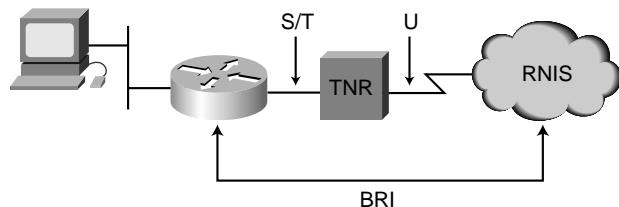
- connectivité BRI ;
- connectivité PRI ;
- RNIS de bout en bout ;
- encapsulation de datagrammes.

Implémentation d'une interface d'accès de base BRI

La boucle locale BRI est reliée à une terminaison numérique de réseau TNR, ou NT1 (*Network Termination-1*), installée chez le client. L'interface de la boucle locale située sur la terminaison numérique de réseau est appelée *point de référence U*. Du côté de la terminaison client, on trouve le point de référence S/T. Ce point de référence peut supporter un bus multipoint d'équipements RNIS, tels des adaptateurs de terminaux AT (ou TA, *Terminal Adapter*). La Figure 11.6 illustre une installation BRI type.

Figure 11.6

La boucle locale BRI connectée à RNIS.



Equipements pour l'interface BRI

Deux types courants d'équipements de télécommunication RNIS sont disponibles, côté client, pour les services BRI : routeurs RNIS et adaptateurs de terminaux (TA) pour PC. Certains équipements BRI proposent des terminaisons numériques de réseau ainsi que des adaptateurs de terminaux intégrés pour les téléphones analogiques.

Routeurs LAN

Les routeurs RNIS assurent le routage entre l'interface BRI et le LAN, au moyen de DDR.

DDR établit et libère automatiquement les liaisons par circuits commutés, qui fournissent ainsi une connectivité transparente pour les sites distants, en se fondant sur le trafic du réseau. DDR contrôle également l'établissement et la libération des canaux B secondaires, en se fondant sur des seuils de charge. MultiLink PPP est utilisé pour assurer l'agrégation de bandes passantes, lorsque plusieurs canaux B sont utilisés. Pour plus d'informations sur DDR, voyez le Chapitre 10.

Certaines applications RNIS peuvent nécessiter que l'utilisateur contrôle directement les appels RNIS. Les fonctions émergeantes du système exploitation Cisco IOS peuvent autoriser ce contrôle au niveau de l'ordinateur de bureau. Les nouveaux modèles Cisco 700 permettent un contrôle direct, au moyen d'un bouton d'appel situé sur la face avant du routeur.

La série de routeurs Cisco 700, ainsi que les séries de routeurs Cisco 1000, 1600 et 2500, basés sur Cisco IOS, fournissent une interface BRI. Plusieurs interfaces BRI sont disponibles sur les séries Cisco 3600 et 4x00.

Adaptateurs de terminaux pour PC (AT-PC)

Ces équipements se connectent aux stations de travail PC, soit par l'intermédiaire du bus PC, soit de façon externe, *via* des ports de communication (tels que RS-232), et peuvent être utilisés de la même manière que les modems analogiques (tels que V.34) internes et externes.

Les adaptateurs de terminaux pour PC peuvent apporter à l'utilisateur un contrôle direct sur l'initiation et la libération de sessions RNIS, comme s'il utilisait un modem analogique. Des mécanismes automatisés doivent être assurés afin de permettre l'ajout et le retrait d'un second canal B. Les cartes PC des séries Cisco 200 fournissent des services RNIS pour PC.

Configuration BRI

La configuration BRI implique de configurer les types de commutateurs RNIS ainsi que les identifiants SPID (*Service Profile Identifier*, identifiant de profil de service) de la manière suivante.

Types de commutateurs RNIS

Les commutateurs de centre de raccordement RNIS (également appelés *équipements d'échange local*) assurent deux fonctions sur le plan local : la terminaison locale et la terminaison d'échange. La fonction de terminaison locale gère la transmission et la terminaison au niveau de la boucle locale. La fonction de terminaison d'échange gère la portion de commutation de l'échange local. Tout d'abord, cette fonction démultiplexe les bits sur les canaux B et D. Ensuite, les informations du canal B sont routées vers la première section du commutateur de circuit, et les paquets du canal D sont routés vers le circuit de séparation de paquets du canal D.

Pour un fonctionnement correct de RNIS, il est impératif que les types de commutateurs corrects soient configurés sur l'équipement RNIS. Jusqu'à la version 11.2 de Cisco IOS, le type de commutateur RNIS était configuré par le biais d'une commande globale (notez que cela signifie également que vous ne pouvez pas utiliser les cartes BRI et PRI sur un même châssis Cisco IOS). Avec la version Cisco IOS 11.3T, ou ultérieure, plusieurs types de commutateurs peuvent être supportés sur un même châssis.

- **Types de commutateurs Cisco IOS.** La commande Cisco IOS suivante illustre les types de commutateurs BRI supportés :

```
kdt-3640(config)#isdn switch-type ?
  basic-1tr6      1TR6 switch type for Germany
  basic-5ess      AT&T 5ESS switch type for the U.S.
  basic-dms100    Northern DMS-100 switch type
  basic-net3      NET3 switch type for UK and Europe
  basic-ni1       National ISDN-1 switch type
  basic-nwnet3    NET3 switch type for Norway
  basic-nznet3    NET3 switch type for New Zealand
  basic-ts013     TS013 switch type for Australia
  ntt            NTT switch type for Japan
  vn2            VN2 switch type for France
  vn3            VN3 and VN4 switch types for France
```

- **Types de commutateur Cisco 700.** Sur la série de routeurs Cisco 700, utilisez la commande `set switch`, qui accepte les options suivantes, lorsque vous utilisez l'image logicielle US :

```
SEt SWitch 5ESS | DMS | NI-1 |PERM64 | PERM128
```

SPID (Service Profile Identifier)

Un identifiant de profil de service SPID est un numéro fourni par l'opérateur RNIS qui identifie la configuration de ligne du service BRI. Ces identifiants permettent à plusieurs équipements RNIS, tels ceux destinés au transfert de la voix et des données, de partager la boucle locale. Ils sont requis par les commutateurs DMS-100 et National ISDN-1. Selon la version logicielle exploitée, les commutateurs AT&T 5ESS peuvent également nécessiter l'emploi d'identifiants SPID.

Chaque identifiant SPID pointe vers des informations d'établissement et de configuration de ligne. Lorsqu'un équipement tente de se connecter au réseau RNIS, il exécute un processus d'initialisation de niveau 2 sur le canal D, qui provoque l'assignation d'un identifiant TEI (*Terminal Endpoint Identifier*) à cet équipement. Ce dernier tente ensuite une initialisation de niveau 3 sur le canal D. Si des identifiants SPID sont nécessaires, mais n'ont pas été configurés ou l'ont été incorrectement, l'initialisation de niveau 3 échoue, et les services RNIS ne peuvent pas être utilisés.

Le commutateur AT&T 5ESS supporte jusqu'à huit identifiants SPID par interface BRI. Puisque plusieurs SPID peuvent être appliqués à un seul canal B, plusieurs services peuvent être supportés simultanément. Par exemple, le premier canal B peut être configuré pour des données, et le second à la fois pour la voix (au moyen d'un téléphone RNIS) et pour des données.

Les commutateurs DMS-100 et National ISDN-1 ne supportent que deux identifiants SPID par interface BRI : un SPID pour chaque canal B. Si les deux canaux B sont destinés à n'être utilisés que pour des données, configurez les routeurs pour les deux SPID (un pour chaque canal B). Vous ne pouvez pas traiter en même temps des données et de la voix sur le même canal B. L'absence ou la présence de l'identifiant SPID d'un canal dans la configuration du routeur indique si le second canal B peut être utilisé pour les données ou pour la voix.

NOTE

Il n'existe aucun format standard pour les identifiants SPID. Par conséquent, les numéros varient en fonction du fabricant du commutateur, et de l'opérateur.

Voici un exemple de configuration type de SPID pour Cisco IOS :

```
interface BRI0
isdn spid1 0835866201 8358662
isdn spid2 0835866401 8358664
```

Ces commandes spécifient également le numéro d'annuaire local (LDN, *Local Directory Number*), qui est le nombre à sept chiffres assigné par le fournisseur de services et utilisé pour le routage d'appel. Le LDN n'est pas indispensable pour établir des connexions RNIS, mais il doit être spécifié si vous voulez recevoir des appels entrants sur le canal B 2. Cet identifiant est nécessaire uniquement lorsque deux identifiants SPID sont configurés (par exemple, lors de la connexion à un commutateur DMS ou NI1). Chaque SPID est associé à un LDN. La configuration du LDN permet aux appels entrants qui arrivent sur le canal B 2 d'être correctement traités. Si le LDN n'est pas configuré, il est possible que les appels entrants qui arrivent sur le canal B 2 échouent.

Voici un exemple de configuration type de SPID pour la série Cisco 700 :

```
SET 1 SPID 51255500660101
SET 1 DIRECTORYNUMBER 5550066
SET PHONE1 = 5550066
SET 2 SPID 51255500670101
```

Contrôle du fonctionnement de l'interface BRI

Pour vérifier l'état des interfaces BRI avec le système Cisco IOS, utilisez la commande `show isdn status`. Dans l'exemple suivant, les TEI ont été négociés avec succès, et le niveau 3 de RNIS (bout en bout) est prêt à effectuer ou à recevoir des appels :

```
kdt-1600#sh isdn status
The current ISDN Switchtype = basic-ni1
ISDN BRI0 interface
  Layer 1 Status:
    ACTIVE
  Layer 2 Status:
    TEI = 109, State = MULTIPLE_FRAME_ESTABLISHED
    TEI = 110, State = MULTIPLE_FRAME_ESTABLISHED
  Spid Status:
    TEI 109, ces = 1, state = 8(established)
      spid1 configured, spid1 sent, spid1 valid
      Endpoint ID Info: epsf = 0, usid = 1, tid = 1
    TEI 110, ces = 2, state = 8(established)
      spid2 configured, spid2 sent, spid2 valid
      Endpoint ID Info: epsf = 0, usid = 3, tid = 1
  Layer 3 Status:
    0 Active Layer 3 Call(s)
  Activated dsl 0 CCBs = 0
  Total Allocated ISDN CCBs = 0
```

La résolution de problèmes liés à la configuration de SPID est réalisé avec la commande `debug isdn q921`. Dans l'exemple suivant, vous pouvez constater que l'identifiant `isdn spid1` a été rejeté par le commutateur RNIS :

```
kdt-1600#debug isdn q921
ISDN Q921 packets debugging is on
kdt-1600#clear int bri 0
kdt-1600#
*Mar 1 00:09:03.728: ISDN BR0: TX -> SABMEp sapi = 0 tei = 113
*Mar 1 00:09:04.014: ISDN BR0: RX <- IDREM ri = 0 ai = 127
```

```

*Mar 1 00:09:04.018: %ISDN-6-LAYER2DOWN:
    Layer 2 for Interface BRI0, TEI 113 changed to down
*Mar 1 00:09:04.022: %ISDN-6-LAYER2DOWN:
    Layer 2 for Interface BR0, TEI 113 changed to down
*Mar 1 00:09:04.046: ISDN BR0: TX -> IDREQ ri = 44602 ai = 127
*Mar 1 00:09:04.049: ISDN BR0: RX <- IDCKRQ ri = 0 ai = 113
*Mar 1 00:09:05.038: ISDN BR0: RX <- IDCKRQ ri = 0 ai = 113
*Mar 1 00:09:06.030: ISDN BR0: TX -> IDREQ ri = 37339 ai = 127
*Mar 1 00:09:06.149: ISDN BR0: RX <- IDREM ri = 0 ai = 113
*Mar 1 00:09:06.156: ISDN BR0: RX <- IDASSN ri = 37339 ai = 114
*Mar 1 00:09:06.164: ISDN BR0: TX -> SABMEp sapi = 0 tei = 114
*Mar 1 00:09:06.188: ISDN BR0: RX <- UAf sapi = 0 tei = 114
*Mar 1 00:09:06.188: %ISDN-6-LAYER2UP:
    Layer 2 for Interface BR0, TEI 114 changed to up
*Mar 1 00:09:06.200: ISDN BR0: TX ->
    INFOc sapi = 0 tei = 114 ns = 0 nr = 0 i = 0x08007B3A06383932393833
*Mar 1 00:09:06.276: ISDN BR0: RX <-
    INFOc sapi = 0 tei = 114 ns = 0 nr = 1 i = 0x08007B080382E43A
*Mar 1 00:09:06.283: ISDN BR0: TX -> RRr sapi = 0 tei = 114 nr = 1
*Mar 1 00:09:06.287: %ISDN-4-INVALID_SPIID: Interface BR0, Spid1 was rejected

```

Vérifiez l'état de la ligne RNIS de la série Cisco 700, à l'aide de la commande `show status`, de la manière suivante :

```

kdt-776> sh status
Status 01/04/1995 18:15:15
Line Status
  Line Activated
  Terminal Identifier Assigned SPID Accepted
  Terminal Identifier Assigned SPID Accepted
Port Status                               Interface Connection Link
  Ch: 1 Waiting for Call
  Ch: 2 Waiting for Call

```

Remarques sur BRI

Les problèmes suivants, relatifs à la configuration BRI, doivent être examinés :

- **Négociation TEI.** Certains commutateurs désactivent le niveau 2 du canal D si aucun appel n'est actif. Ainsi, le routeur doit être configuré afin d'effectuer la négociation TEI au premier appel, à la place du démarrage (choix par défaut). Pour cela, utilisez la commande de configuration globale suivante :

```
isdn tei-negotiation first-call
```

- **Sous-adressage RNIS.** Le bus S/T est un bus point-multipoint. Plusieurs équipements de télécommunication RNIS du client peuvent partager le même bus S/T. Le routage d'appels vers des équipements individuels sur un bus S/T est activé au moyen du sous-adressage RNIS.

- **Routage de la voix.** Les routeurs de la série Cisco 700 peuvent fournir des prises jacks pour la connexion de postes téléphoniques analogiques classiques. Les sites SOHO peuvent tirer parti de la possibilité de router simultanément les appels données et voix sur la même interface BRI. Les numéros de téléphone de port vocal ainsi que la priorité de voix doivent être configurés pour les besoins du site SOHO. L'exemple suivant illustre une configuration de routage type pour la voix, sur un routeur Cisco 700 :

```
SET SWITCH NI-1
SET 1 SPID 51255500660101
```

```

SET 1 DIRECTORYNUMBER 5550066
SET PHONE1 = 5550066
SET 2 SPID 51255500670101
SET 2 DIRECTORYNUMBER 5550067
SET PHONE2 = 5550067
SET VOICEPRIORITY INCOMING INTERFACE PHONE1 NEVER
SET VOICEPRIORITY OUTGOING INTERFACE PHONE1 NEVER
SET CALLWAITING INTERFACE PHONE1 OFF
SET VOICEPRIORITY INCOMING INTERFACE PHONE2 ALWAYS
SET VOICEPRIORITY OUTGOING INTERFACE PHONE2 ALWAYS
SET CALLWAITING INTERFACE PHONE2 ON
kdt-776> sh voicerouting
Interface   VoicePriority   VoicePriority   Call   Directory   Ring
              In             Out            Waiting Number     Cadence
PHONE1      NEVER          NEVER          OFF    6720066
PHONE2      ALWAYS         ALWAYS         ON     6720067
DOV          N/A            N/A            N/A
UNSPECIFIED N/A            N/A            N/A

```

Implémentation d'une interface d'accès primaire PRI

Les routeurs Cisco IOS supportent les interfaces PRI au moyen de cartes MIP (*MultiChannel Interface Processor*, processeur d'interface multicanal). Les cartes MIP peuvent gérer des lignes T1/E1 fractionnées ou des tranches de temps PRI. Ces cartes sont disponibles sur les routeurs des séries Cisco 4x00, 36x0, 5x00 et 7x00.

Pour spécifier que la carte MIP doit être utilisée en tant qu'interface PRI, utilisez la commande de configuration de contrôleur `pri-group timeslots`.

Les routeurs Cisco IOS qui supportent les interfaces PRI deviennent des serveurs NAS. Les routeurs des séries Cisco 5x00 et 36x0 acceptent des solutions de numérotation hybrides (téléphonie classique et RNIS) en autorisant la connexion de modems analogiques par l'intermédiaire de la plaque de connexion arrière du NAS.

Configuration PRI

La configuration des types de commutateurs RNIS pour l'interface BRI se fait au moyen de la commande `isdn switch-type` :

```

AS5200-2(config)#isdn switch-type ?
primary-4ess      AT&T 4ESS switch type for the U.S.
primary-5ess      AT&T 5ESS switch type for the U.S.
primary-dms100    Northern Telecom switch type for the U.S.
primary-nets5     European switch type for NET5
primary-ntt       Japan switch type
primary-ts014     Australia switch type

```

En général, il s'agit d'une commande de configuration globale. La version 11.3T (ou ultérieure) de Cisco IOS assure la gestion de plusieurs types de commutateurs sur un seul châssis Cisco IOS. Les services PRI sont activés sur le serveur NAS en configurant les contrôleurs T1 (ou E1). Voici un exemple de configuration T1 type, sur un Cisco 5200 :

```

controller T1 0
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24

```

```
!
controller T1 1
framing esf
clock source line secondary
linecode b8zs
pri-group timeslots 1-24
!
```

Notez que les canaux PRI 0-23 sont mis en correspondance avec les tranches de temps PRI 1-24. La même assignation +1 est utilisée sur l'interface PRI basée sur la ligne E1.

Pour configurer une interface PRI basée sur T1, appliquez les commandes de configuration au canal D PRI, c'est-à-dire à l'interface Serial0:23. Tous les canaux situés sur une interface PRI (ou BRI) sont automatiquement regroupés en une interface de numérotation. Lorsque les appels sont effectués ou reçus sur les canaux B, la configuration est clonée à partir de l'interface de numérotation (Serial0:23). Si un NAS contient plusieurs interfaces PRI, elles peuvent être regroupées en une interface de numérotation, à l'aide de la commande d'interface dialer rotary-group, comme illustré dans l'exemple suivant :

```
interface Serial0:23
dialer rotary-group 1
!
interface Serial1:23
dialer rotary-group 1
!
interface Dialer1
ip unnumbered Ethernet0
encapsulation ppp
peer default ip address pool default
dialer in-band
dialer idle-timeout 120
dialer-group 1
no fair-queue
no cdp enable
ppp authentication pap chap
ppp multilink
```

Avec cette configuration, chaque configuration de canal B ou de faisceau MultiLink PPP est clonée à partir de l'interface Dialer1.

Contrôle du fonctionnement de l'interface PRI

L'état du contrôleur T1 est vérifié au moyen de la commande EXEC Cisco IOS show controller t1, de la manière suivante :

```
AS5200-1#sh contr t1
T1 0 is up.
No alarms detected.
Version info of slot 0: HW: 2, Firmware: 14, NEAT PLD: 14, NR Bus PLD: 22
Framing is ESF, Line Code is B8ZS, Clock Source is Line Primary.
Data in current interval (685 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
Total Data (last 24 hours)
  0 Line Code Violations, 0 Path Code Violations,
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 8 Degraded Mins,
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

```
T1 1 is up.  
No alarms detected.  
Version info of slot 0: HW: 2, Firmware: 14, NEAT PLD: 14, NR Bus PLD: 22  
Framing is ESF, Line Code is B8ZS, Clock Source is Line Secondary.  
Data in current interval (197 seconds elapsed):  
    0 Line Code Violations, 0 Path Code Violations  
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins  
    0 Errorred Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs  
Total Data (last 24 hours)  
    0 Line Code Violations, 0 Path Code Violations,  
    0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 4 Degraded Mins,  
    0 Errorred Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Des violations de code de ligne excessives, ou d'autres erreurs, provoquent une dégradation importante des performances. Vérifiez auprès de votre fournisseur de services PRI que ces compteurs fonctionnent correctement. Utilisez la commande EXEC Cisco IOS show isdn status, de la manière suivante, pour savoir si RNIS est opérationnel :

```
AS5200-1#sh isdn status
The current ISDN Switchtype = primary-dms100
ISDN Serial0:23 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
ISDN Serial1:23 interface
    Layer 1 Status:
        ACTIVE
    Layer 2 Status:
        TEI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Layer 3 Status:
        0 Active Layer 3 Call(s)
    Activated dsl 1 CCBs = 0

Total Allocated ISDN CCBs = 0
```

Vérifiez l'état du canal B de la manière suivante, à l'aide de la commande EXEC show isdn service :

RNIS de bout en bout

Cette section traite des sujets suivants, en rapport avec l'implémentation de RNIS de bout en bout :

- système de signalisation 7, ou SS7 (*Signaling System 7*) ;
- vitesse du chemin de données.

Système de signalisation 7 (SS7)

La signalisation SS7 met en œuvre des commutateurs avec des fonctionnalités de signalisation hors bande pour les tronçons du réseau téléphonique (connexions DS0 de commutateur-commutateur). La gestion d'appels de bout en bout (tels l'établissement et la libération de connexions) suit la spécification Q.931, et est étendue aux équipements de connexion PRI/BRI sur le canal D.

La signalisation hors bande *via* SS7 présente de nombreux avantages pour la connexion de réseaux, parmi lesquels un temps d'établissement de connexion réduit, un indicateur de capacité du canal porteur et d'autres indicateurs de progression, des chemins de données de 64 Kbit/s, l'identification de l'appelant, et les informations de numéro appelé (DNIS, *Dialed Number Information Service*). La sortie produite par la commande du système Cisco IOS debug isdn q931 montre des messages d'établissement de connexion (SETUP) RNIS Q.931 types, reçus par un serveur NAS.

Le message SETUP inclut un élément d'information (IE, *Information Element*) de capacité du canal porteur, qui indique à l'équipement RNIS ainsi qu'au côté destinataire le type d'application transportée sur le canal B. RNIS doit fournir un canal de bout en bout, capable de transporter le service porteur, et de donner une indication de progression au côté récepteur afin de l'aider à mieux exploiter la connexion RNIS.

La sortie de la commande Cisco IOS debug isdn q931 affiche différentes possibilités de transport pour chaque type d'appel entrant, comme le montrent les exemples suivants :

- Appel entrant à 64 Kbit/s pour des données :

```
ISDN Se0:23: RX <- SETUP pd = 8 callref = 0x0470
    Bearer Capability i = 0x8890
    Channel ID i = 0xA98382
    Calling Party Number i = '!', 0x83, '5125558084'
    Called Party Number i = 0xC9, '52000'
```

- Appel entrant à 56 Kbit/s pour des données :

```
ISDN Se0:23: RX <- SETUP pd = 8 callref = 0x05DC
    Bearer Capability i = 0x8890218F
    Channel ID i = 0xA98382
    Calling Party Number i = '!', 0x83, '5125558084'
    Called Party Number i = 0xC9, '52000'
```

- Appel entrant pour la voix :

```
ISDN Se0:23: RX <- SETUP pd = 8 callref = 0x015C
    Bearer Capability i = 0x8090A2
    Channel ID i = 0xA98383
    Progress Ind i = 0x8283 - Origination address is non-ISDN
    Called Party Number i = 0xC1, '5552000'
```

Pour pouvoir router les communications téléphoniques vers des cartes modems intégrées, utilisez la commande de configuration d'interface Cisco IOS isdn incoming-voice modem. Sur certains réseaux, les connexions pour le transport de données peuvent être effectuées à l'aide d'un message

SETUP Q.931, qui indique qu'il s'agit de connexions pour la voix. Dans certaines régions ou pays, les structures tarifaires pour RNIS rendent ce type de connexion plus rentable. Cette conception de réseau est généralement appelée *réseau RNIS données sur voix*. Néanmoins, le fait d'indiquer au dispositif de commutation RNIS que le canal porteur est réservé à la voix autorise la connexion à emprunter des tronçons non numériques. Les concepteurs doivent par conséquent examiner avec précaution les risques potentiels d'une telle conception. Pour configurer les appels entrants de type données sur voix avec Cisco IOS, utilisez la commande de configuration `isdn incoming-voice data` de la manière suivante :

```
NAS-522(config)#int serial 0:23
NAS-522(config-if)#isdn incoming ?
  data    Incoming voice calls will be handled as data.
  modem   Incoming voice calls will be handled as modems.
```

Vitesse du chemin de données

Avant l'implémentation de SS7, la signalisation de la gestion des connexions de bout en bout était transmise en intrabande, en rognant des bits sur les tronçons DS0 (fonction RBT, *Robbed Bit Trunking*). L'utilisation occasionnelle du huitième bit (le moins significatif) de chaque octet d'information vocale n'était pas préjudiciable à la qualité de la livraison, et assurait une signalisation commutateur-commutateur. La signalisation hors bande de bout en bout, *via* SS7 et les canaux D BRI ou PRI, permet aux connexions pour les données d'être établies par l'intermédiaire de réseaux RNIS, en utilisant le tronçon DS0 complet (64 Kbit/s). Certains tronçons du réseau RTC ne supportent toujours pas la signalisation hors bande et autorisent uniquement la fonction RBT (ligne T1/E1 fractionnée), ce qui limite le canal porteur à 56 Kbit/s.

Le dispositif de commutation RNIS est responsable de la fourniture d'un chemin de bout en bout qui correspond à la capacité du canal porteur. Si une connexion est établie à 64 Kbit/s alors qu'il n'existe pas de chemin à 64 Kbit/s pour cette connexion, un signal d'occupation doit être reçu. Les concepteurs de réseaux doivent considérer la possibilité d'un blocage occasionnel d'appels RNIS à 64 Kbit/s. Une conception robuste peut nécessiter que certains sites soient supportés avec des connexions de données à 56 Kbit/s. Le Tableau 11.1 présente les vitesses d'appels sortants.

Tableau 11.1 : Vitesses d'appels sortants avec correspondances et profils de numérotation Cisco IOS

<i>Vitesse en sortie</i>	<i>Correspondances de numérotation</i>	<i>Profil de numérotation</i>	<i>Cisco 700</i>
64 Kbit/s	dialer map ... speed 64 (par défaut)	??	set speed 64
56 Kbit/s	dialer map ... speed 56	??	set speed 56
Auto	multiple dialer maps	??	set speed auto (par défaut)

Lorsque des appels sont effectués initialement à 64 Kbit/s, mais qu'ils sont livrés incorrectement à leur destination par le réseau RNIS, *via* un chemin à 56 Kbit/s, les données ainsi transmises sont altérées. Le dépannage, à l'aide de la commande `debug isdn q931`, signalera que l'appel a abouti, mais la commande `debug ppp negotiation` n'indiquera aucune réception. Les paquets endommagés sont

ignorés. Si les appels aboutissent et que PPP ne négocie pas LCP (*Link Control Protocol*), il est recommandé de toujours tester les connexions sortantes à 56 Kbit/s :

■ Vitesse d'appels sortants.

- **Configuration de la vitesse avec Cisco IOS.** Utilisez le paramètre speed sur la ligne de la commande dialer map, afin d'effectuer des appels à 56 Kbit/s, comme dans l'exemple suivant :

```
int dialer 1
dialer map ip 172.20.1.1 name nas speed 56 5558084
```

- **Configuration de la vitesse des profils de numérotation Cisco IOS.** L'exemple suivant illustre comment configurer un profil de numérotation, afin d'effectuer des appels à 56 Kbit/s :

```
interface dialer 1
dialer remote-name nas
dialer string 5558084 class unameit
!
map-class dialer unameit
dialer isdn speed 56
```

- **Configuration de la vitesse sur un routeur Cisco 700.** Utilisez la commande de configuration set speed, afin de contrôler la vitesse des appels sortants.

■ Vitesse d'appels entrants.

La capacité de transport RNIS Q.931, ainsi que d'autres éléments d'informations (IE), sont utilisés pour déterminer la vitesse de l'appel entrant, ce qui donne de bons résultats dans la plupart des cas. Toutefois, pour certains types d'applications pays-pays, le message SETUP entrant sera livré avec une capacité de transport qui ne correspond pas à la demande initiale. Si un élément d'information isdn not end-to-end est également reçu, il peut être utilisé pour remplacer la capacité de transport reçue, au moyen de la commande de configuration Cisco IOS isdn not end-to-end.

Problèmes d'encapsulation de datagrammes

RNIS peut utiliser PPP, HDLC ou X.25 pour l'encapsulation. PPP est celui utilisé le plus souvent, car il fournit un excellent mécanisme d'authentification et de négociation de liens compatibles, et de configuration de protocole.

Protocole PPP

PPP (*Point-to-Point Protocol*) fournit une méthode standard pour le transport de paquets multiprotocoles sur des liaisons point-à-point. Ce protocole est défini dans le RFC 1661. Il comprend plusieurs composantes, auxquelles le concepteur de réseaux est confronté.

Délimitation des trames PPP

Le RFC 1662 traite de l'implémentation de PPP pour la délimitation de trames de type HDLC. En fait, PPP n'est pas implémenté de la même manière selon qu'il s'agit de lignes asynchrones ou synchrones.

Lorsqu'une extrémité de la liaison utilise PPP synchrone (par exemple un routeur RNIS), et que l'autre extrémité emploie PPP asynchrone (par exemple un adaptateur terminal RNIS connecté à un

port série de PC), deux techniques peuvent être employées pour assurer la compatibilité des trames. La méthode recommandée est l'activation de la conversion des trames PPP synchrones en trames PPP asynchrones sur l'adaptateur de terminal RNIS. Si cela n'est pas possible, V.120 peut alors être utilisé pour encapsuler les trames PPP asynchrones, afin qu'elles puissent être transportées sur RNIS.

Protocole LCP (Link Control Protocol)

Le protocole LCP de PPP permet d'établir, de configurer, de maintenir, et de terminer une connexion point-à-point. Avant de pouvoir échanger des datagrammes de couche réseau (tel IP), LCP doit d'abord établir la connexion et négocier des paramètres de configuration. Cette phase se termine avec l'envoi, puis la réception d'une trame d'acquittement de configuration.

Authentification PPP

Les protocoles d'authentification de PPP, PAP (*Password Authentication Protocol*) et CHAP (*Challenge Handshake Authentication Protocol*), sont définis dans le RFC 1334. Après l'établissement de la connexion PPP par LCP, un protocole d'authentification optionnel peut être implémenté avant de procéder à la négociation et à l'établissement des protocoles de contrôle de réseau (NCP, *Network Control Protocols*). Si l'authentification est souhaitée, elle doit être négociée en tant qu'option, durant la phase d'établissement de LCP. Elle peut être bidirectionnelle (chaque côté authentifie l'autre) ou unidirectionnelle (un seul côté, généralement l'appelant, authentifie l'autre).

La plupart des conceptions RNIS nécessitent que l'équipement appelé authentifie le dispositif appelant. Outre les avantages sur le plan de la sécurité, l'authentification fournit également une indication sur l'état de DDR et des faisceaux MultiLink PPP.

Protocoles NCP (Network Control Protocols)

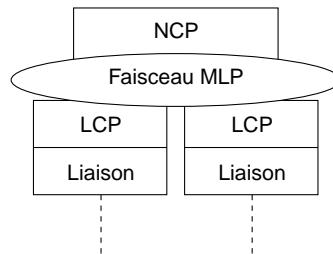
Il s'agit d'une famille de protocoles de contrôle qui permettent d'établir et de configurer différents protocoles de la couche réseau. PPP est conçu pour permettre l'emploi simultané de plusieurs protocoles de ce niveau.

Après l'établissement de LCP et la réussite de l'authentification, les noeuds PPP envoient des trames NCP afin de négocier et d'établir la connectivité pour un ou plusieurs protocoles de la couche réseau. Par exemple, afin de supporter IP sur une connexion PPP, le protocole IPCP est négocié, et établi selon les directives du RFC 1332. Une fois l'établissement de IPCP réussi, les datagrammes IP peuvent être transmis sur la connexion PPP.

MultiLink PPP (MLP)

MultiLink PPP est un standard qui permet de grouper plusieurs liaisons PPP, et qui autorise une interopérabilité multifabricant. Il est décrit dans le RFC 1717. MLP définit une méthode pour ordonner et transmettre des paquets sur plusieurs interfaces physiques. Afin de réduire les risques de problèmes de latence, MLP définit également une méthode de fragmentation et de réassemblage des paquets de grande taille. La Figure 11.7 illustre une vue conceptuelle de ce protocole en action.

Figure 11.7
MultiLink PPP en action.



Lorsqu'un paquet NCP d'une taille supérieure à 30 octets arrive sur une interface maître MLP pour être transmis, il est fragmenté, puis envoyé sur chaque liaison physique du faisceau MLP. Lorsque les fragments de paquet MLP arrivent sur la destination PPP, MLP réassemble les paquets originaux, puis les réordonne correctement dans le flux de données.

Avec MLP, les équipements BRI peuvent doubler leur bande passante de connexion sur la liaison, en passant de 56/64 Kbit/s à 112/128 Kbit/s. MLP est supporté tant que les équipements font partie du même groupe de rotation de numérotation ou du même pool.

Les fonctionnalités avancées de Cisco IOS et de Cisco 700 sont utilisées pour déterminer à quel moment ajouter des liaisons à l'interface maître MLP, ou en supprimer. La fonction DDR de Cisco IOS autorise une configuration, selon un certain seuil de charge. Le facteur de charge peut être calculé sur le trafic entrant, sur le trafic sortant, ou sur le trafic bidirectionnel.

La configuration partielle suivante pour un serveur NAS place deux interfaces BRI dans un groupe de rotation de numérotation, active le support de MLP, puis définit un seuil de charge, afin de déterminer à quel moment des canaux B supplémentaires doivent être activés :

```

interface BRI2/0
encapsulation ppp
dialer rotary-group 1
isdn spid1 0835866201
isdn spid2 0835866401
!
interface BRI2/1
encapsulation ppp
dialer rotary-group 1
isdn spid1 0835867201
isdn spid2 0835967401
!
interface Dialer1
ip unnumbered Ethernet0/0
encapsulation ppp
dialer in-band
dialer map ip 172.20.2.1 name kdt-nas 8358661
dialer load-threshold 100 either
dialer-group 1
ppp authentication chap callin

ppp multilink

```

L'état du protocole MLP, ainsi que celui des sessions, peut être contrôlé au moyen des commandes `show user` et `show ppp multilink`.

```

KDT-5200#sh user
Line      User      Host(s)          Idle Location
* 51 vty 1    admin    idle           00:00:00
      Vi1      jack-isdn Virtual PPP (Bundle) 00:00:46
      Vi9      cisco776  Virtual PPP (Bundle) 00:00:46
      Se0:18   jack-isd Sync PPP           00:09:06
      Se0:21   cisco776 Sync PPP           00:18:59
      Se0:22   jack-isdn Sync PPP          00:08:49

KDT-AS5200#sh ppp multi
Bundle cisco776, 1 member, Master link is Virtual-Access9
Dialer Interface is Dialer1
  0 lost fragments, 3 reordered, 0 unassigned, sequence 0x2068/0x1A7C rcvd/sent
  0 discarded, 0 lost received, 1/255 load

Member Link: 1
Serial0:21

Bundle jack-isdn, 2 members, Master link is Virtual-Access1
Dialer Interface is Dialer1
  0 lost fragments, 8 reordered, 0 unassigned, sequence 0x5DEB/0x1D7E4 rcvd/sent
  0 discarded, 0 lost received, 1/255 load

Member Links: 2
Serial0:18
Serial0:22

```

Comme nous l'avons vu précédemment, MLP utilise le nom d'authentification PPP pour construire et maintenir les faisceaux MLP. Pour activer MLP sur un routeur Cisco 700, appliquez la commande de configuration suivante :

```
set ppp multilink on
```

Protocole CCP (Compression Control Protocol)

Le protocole CCP de PPP est un avant-projet RFC de l'IETF (*Internet Engineering Task Force*), qui définit une méthode pour négocier la compression de données sur des liaisons PPP. Ces dernières peuvent être des lignes louées ou des liaisons WAN par circuits commutés, ou encore RNIS. La compression permet d'augmenter le débit et de réduire le temps de transfert des fichiers.

Pour activer la compression, utilisez la commande de configuration d'interface compress sur les deux extrémités de la liaison. Utilisez le mot clé stac pour activer l'algorithme de compression de Stacker (LZS) ou le mot clé predictor pour activer l'algorithme RAND (un algorithme de prévision). L'algorithme Stacker convient pour l'encapsulation LAPB et PPP, l'algorithme RAND pour l'encapsulation HDLC et PPP. L'algorithme Stacker est recommandé pour l'encapsulation PPP.

Pour déterminer, sur un système Cisco IOS, quels composants ont été négociés (LCP, IPCP, CCP, etc.), utilisez la commande show interface sur l'interface maître. Pour résoudre les problèmes de négociation PPP, employez les commandes debug ppp negotiation et debug ppp authentication.

Sécurité RNIS

A l'aide de SS7, RNIS peut livrer des éléments d'informations de bout en bout, par exemple l'identifiant d'appelant ou le numéro appelé (DNIS). Ces informations peuvent être utilisées dans le but

d'apporter un niveau de sécurité supplémentaire lors de la conception de solutions RNIS. Il est recommandé de toujours implémenter l'authentification PPP.

- **Authentification PPP.** L'authentification PPP est utilisée dans le but d'apporter une sécurité minimale sur un réseau RNIS ainsi que sur d'autres liaisons d'encapsulation PPP. Le nom d'utilisateur authentifié est également employé par MultiLink PPP pour maintenir les faisceaux, et par DDR afin de déterminer quels sites de numérotation sont actuellement connectés.

L'authentification PPP est activée au moyen de la commande d'interface `ppp authentication`. PAP et/ou CHAP peuvent être utilisés pour authentifier la connexion distante. CHAP est considéré comme étant plus efficace, car il utilise la méthode de négociation en trois temps (*three-way handshake*), ce qui évite l'envoi du mot de passe en texte clair sur la liaison PPP. Il est souvent nécessaire d'authentifier le côté distant, uniquement dans le cas d'appels entrants (et non d'appels sortants).

- **Filtrage de l'identifiant d'appelant.** La commande de configuration d'interface `isdn caller` configure le filtrage de l'identifiant d'appelant. Par exemple, la commande suivante configure un réseau RNIS afin qu'il accepte les appels qui présentent un identifiant d'appelant commençant par 41555512, sans exigence particulière pour les deux derniers chiffres :

```
isdn caller 41555512xx
```

Plusieurs commandes `isdn caller` peuvent être employées, si nécessaire. Si un appel est reçu sans indication de l'identifiant d'appelant, ou qu'il présente un identifiant non conforme, l'appel est rejeté.

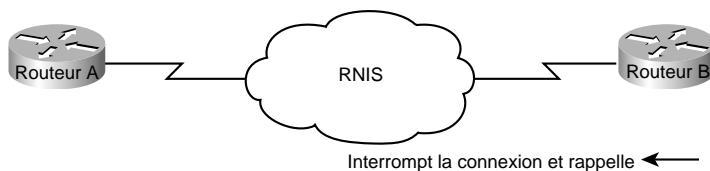
- **Rappel de l'appelant.** La fonction de rappel (*callback*) permet à un routeur (en général, un routeur distant) d'initier une liaison WAN par circuit commuté vers un autre équipement, et de demander à celui-ci de le rappeler. L'équipement (par exemple, un routeur de site central) répond à la requête en appelant le dispositif à l'origine de la demande de connexion. La fonction de rappel utilise le protocole PPP et les spécifications du RFC 1570. La Figure 11.8 illustre un processus de négociation type.

Figure 11.8

Rappel RNIS.

→ Requête de rappel avec LCP

→ Authentification



Le processus de rappel représenté à la Figure 11.8 comprend les étapes suivantes :

1. Le routeur A établit une connexion par circuit commuté vers le routeur B.
2. Les routeurs A et B négocient le protocole de contrôle de liaison LCP de PPP. Le routeur A, ou le routeur B, peut demander un rappel.

3. Le routeur A s'authentifie auprès du routeur B à l'aide des protocoles PAP ou CHAP de PPP. Le routeur B peut optionnellement s'authentifier auprès du routeur A.
4. Les deux routeurs interrompent la connexion sur le circuit commuté.
5. Le routeur B établit une connexion par circuit commuté vers le routeur A.

La fonction de rappel permet de centraliser la facturation pour les services de connexions synchrones par commutation. Elle permet également de tirer profit des différences de tarification entre les communications nationales et internationales. Toutefois, le rappel nécessite l'établissement d'une connexion par circuit commuté avant que la requête de rappel ne puisse être transmise. Cela induit toujours un coût minimum (selon la tarification locale) pour le routeur qui demande le rappel.

Reportez-vous au Chapitre 10 pour plus de détails sur le rappel DDR. Le Chapitre 21 fournit un exemple de configuration de rappel.

- **Vérification du numéro appelé.** Lorsque plusieurs équipements et un routeur partagent la même boucle locale RNIS, vous pouvez vérifier que c'est bien le dispositif approprié qui répond à l'appel entrant. Pour cela, il faut configurer l'équipement afin qu'il compare le numéro appelé et la sous-adresse donnée par le commutateur dans le message SETUP avec le numéro et la sous-adresse qui ont été définis.

Pour configurer la fonction de vérification du numéro appelé sur le routeur, utilisez les commandes de configuration d'interface `isdn answer1` ou `isdn answer2` sur l'interface BRI. Elles permettent de spécifier soit le numéro appelé, soit la numérotation de sous-adresse, ou les deux. Si vous n'utilisez aucune de ces commandes, le routeur traite et accepte tous les appels entrants.

Evolutivité des réseaux RNIS

Cette section traite des fonctionnalités qui permettent aux réseaux RNIS d'être évolutifs :

- nœuds distants virtuels ;
- profils virtuels ;
- MultiLink PPP multichâssis (MMP, *Multichassis MultiLink PPP*).

Nœuds distants virtuels

A l'aide des fonctions de traduction d'adresse de réseau NAT (*Network Address Translation*), telles que les fonctionnalités PAT des routeurs Cisco 700 ou EZIP de Cisco IOS, les sites distants peuvent apparaître au serveur NAS comme étant un nœud unique, avec une seule adresse IP. Cela réduit les problèmes de consommation d'adresses IP ainsi que la complexité de conception, souvent liée au déploiement de grands réseaux RNIS avec DDR, tout en supportant la connectivité LAN et DDR sur le site distant.

Les fonctions NAT utilisent l'adresse IP reçue de la part du serveur NAS durant la négociation IPCP. Les adresses IP de tous les paquets routés entre le LAN et la liaison PPP sont traduites en une seule adresse IP. Différents numéros de ports UDP/TCP sont utilisés avec cette adresse IP unique, afin de déterminer les paquets qui doivent être renvoyés vers les adresses IP appropriées sur le

LAN. Toutes les commandes de configuration de routeurs Cisco 700 suivantes activent la traduction NAT pour la fonction PAT.

PAT et DHCP sur Cisco 700

La configuration suivante définit un routeur Cisco 700 pour les services PAT et DHCP :

```
cd internal
set ip address 172.24.4.254
set ip netmask 255.255.255.0
set ip routing on
set ip rip update off
cd
set user access-gw1
set ip routing on
set ip framing none
set number 18005552626
set ip rip update off
set encaps ppp
set ip route destination 0.0.0.0 gateway 0.0.0.0
set ip pat on
cd lan
set bridging on
set encaps ppp
set ip routing on
cd
set ip pat porthandler default 172.24.4.1
set ip pat porthandler http 172.24.4.1
set bridging on
set dhcp server
set dhcp domain cisco.com
set dhcp address 172.24.1.1 10
set dhcp netmask 255.255.255.0
set dhcp gateway primary 172.24.4.254
set dhcp dns primary 172.30.1.100
set dhcp dns secondary 172.30.2.100
set dhcp wins primary 172.30.1.101
set dhcp wins secondary 172.30.2.101
set ppp authentication incoming chap
set ppp authentication outgoing chap
set ppp secret client
<insert_secret>
<insert_secret>
set ppp secret host
<insert_secret>
<insert_secret>
```

Si le support des connexions de réseau en sortie vers le site distant est requis, la configuration d'un gestionnaire de port peut être ajoutée, afin que le routeur SOHO sache vers quelle adresse IP transmettre les paquets pour les différents types de connexions :

```
kdt-776> sh ip pat
Dropped - icmp 0, udp 0, tcp 0, map 0, frag 0
Timeout - udp 5 minutes, tcp 30 minutes
Port handlers [default 172.24.4.1]:
  Port    Handler      Service
  -----  -----
  0       172.24.4.1   DEFAULT
  23      Router       TELNET
```

```

67      Router      DHCP Server
68      Router      DHCP Client
69      Router      TFTP
80      172.24.4.1   HTTP
161     Router      SNMP
162     Router      SNMP-TRAP
520     Router      RIP

```

Translation Table - 11 Entries.

Inside	Outside	Orig. Port/ID	Trans. Port/ID	Timeout
172.24.4.1	172.17.190.5	0x414	0xff7d	1
172.24.4.1	172.17.190.5	0x415	0xff7c	30
172.24.4.1	172.17.190.26	0x40d	0xff88	27
172.24.4.1	172.17.114.11	0x416	0xff7b	4
172.24.4.1	172.17.114.11	0x417	0xff7a	4
172.24.4.1	172.17.114.11	0x40f	0xff82	4
172.24.4.1	172.17.190.19	0x418	0xff79	1
172.24.4.1	172.17.190.5	0x410	0xff81	1
172.24.4.1	172.17.114.11	0x411	0xff80	4
172.24.4.1	172.17.114.11	0x412	0xff7f	4
172.24.4.1	172.17.190.5	0x413	0xff7e	1

Profils virtuels

Les profils virtuels (introduits avec Cisco IOS 11.3) sont des applications PPP, qui créent des interfaces d'accès virtuel pour chaque utilisateur connecté. Ils apportent une souplesse de conception supplémentaire lors de l'élaboration de réseaux RNIS pour le support de SOHO. Leur emploi pour les connexions entrantes par circuits commutés peut simplifier l'adressage de nœud et la mise en correspondance d'adresses, ces fonctions étant autrement fournies par l'utilisation de DDR sur les interfaces RNIS. Les appels sortants fondés sur des profils virtuels ne sont plus supportés à partir de la version Cisco IOS 11.3.

La configuration d'interface d'accès virtuel peut être clonée à partir d'un modèle virtuel d'interface. Pour en apprendre davantage sur les interfaces d'accès virtuel, visitez le site <http://cio.cisco.com/warp/customer/131/4.html>. Les profils virtuels se fondent sur des modèles virtuels, et peuvent utiliser AAA fondé sur une configuration par utilisateur pour créer des interfaces d'accès virtuel. La configuration par utilisateur peut être ajoutée afin de répondre aux besoins spécifiques du protocole, pour des utilisateurs individuels ou des groupes.

Les interfaces d'accès virtuel Cisco IOS peuvent simplifier le support des nœuds distants pour IPX et AppleTalk, en utilisant la même configuration que celle employée sur les interfaces de groupe asynchrones traditionnelles. La configuration suivante fournit l'adressage d'homologue pour IP, IPX et AppleTalk, au moyen de l'interface Virtual-Template1 :

```

interface Virtual-Template1
ip unnumbered Ethernet0/0
appletalk client-mode
ipx ppp-client Loopback0
peer default ip address pool default

```

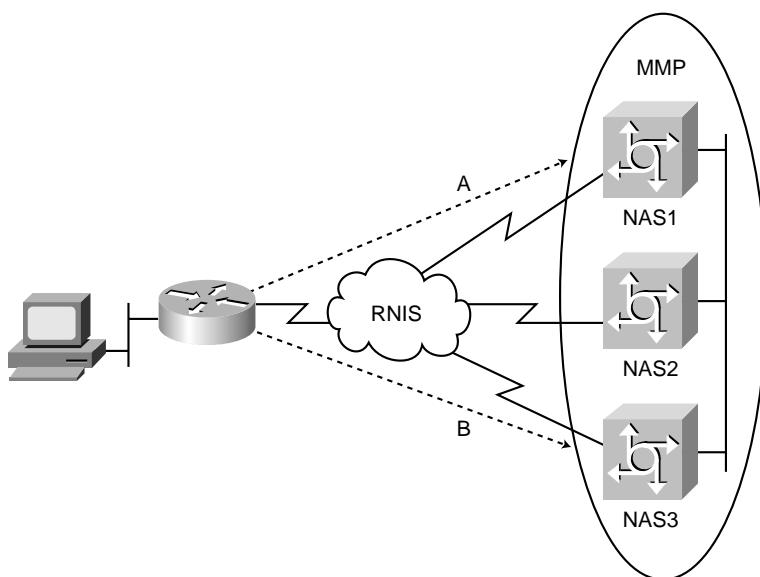
MultiLink PPP multichâssis (MMP)

Dans une conception avec MultiLink PPP sans support multichâssis, les groupes de voies fournis par l'opérateur téléphonique (*hunt-groups*) ne peuvent pas s'étendre sur plus d'un serveur NAS

Cisco IOS, sinon plusieurs canaux B risqueraient de ne pas être réassemblés. Par exemple, un AS5300 peut supporter jusqu'à quatre interfaces PRI, en fournissant un maximum de 120 canaux B (basés E1) dans un seul groupe de voies pour appel entrant. Une plus grande capacité de NAS devrait être fournie par la configuration d'un nouveau groupe (avec un nouveau numéro d'annuaire pilote) pour chaque serveur d'accès de réseau (voir Figure 11.9). Cela a pour effet négatif de fragmenter le pool d'appel.

Figure 11.9

MMP permet à un groupe de voies de l'opérateur téléphonique de s'étendre sur plusieurs serveurs NAS.



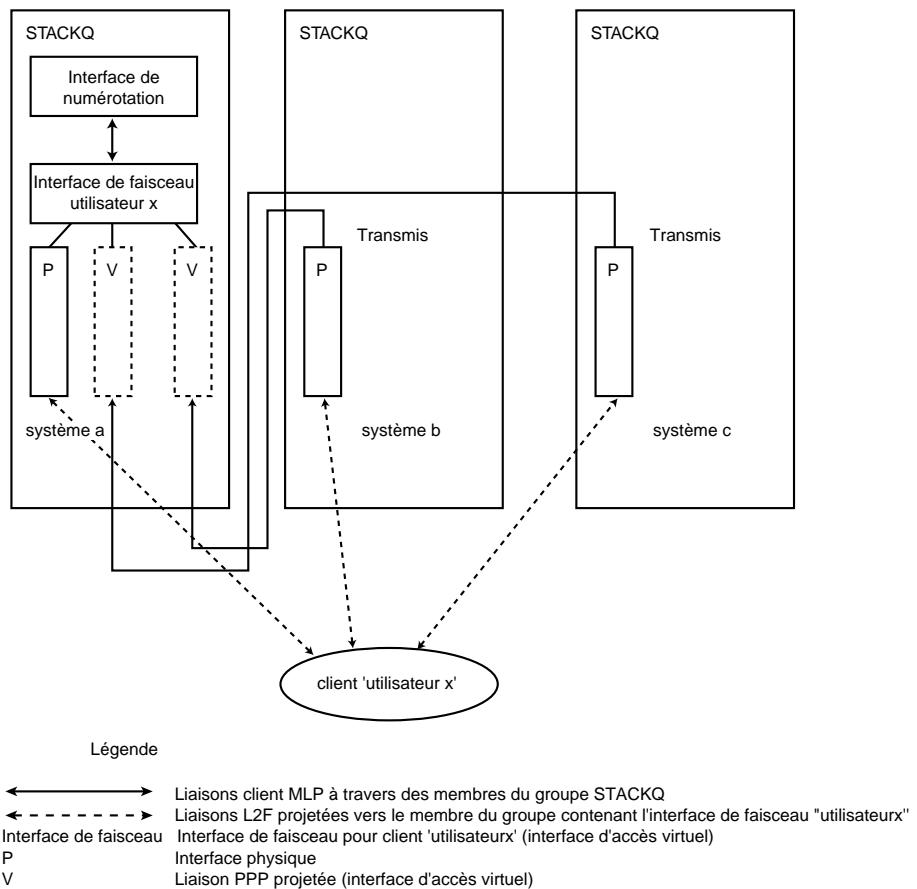
Cisco affirme que, quelle que soit la taille de NAS développée, il subsistera toujours des clients qui auront besoin de pools de ports d'accès plus grands. Ainsi, la version Cisco IOS 11.2 a introduit le protocole MMP (*MultiChassis MultiLink Point-to-Point Protocol*), qui étend le protocole MLP (*MultiLink PPP*) en fournissant un mécanisme qui permet de regrouper de façon transparente les canaux B sur plusieurs serveurs NAS.

MMP inclut deux composantes principales, qui viennent compléter MLP :

- **Le groupe de numérotation Stack Group.** Il englobe les serveurs NAS, qui opèrent en groupe lors de la réception d'appels MLP. Chaque session MLP reçue par un NAS est transmise sous forme d'offre, au moyen du protocole SGBP (*Stack Group Bidding Protocol*). Cela permet principalement à des liaisons MLP secondaires d'être regroupées vers l'interface MLP maître. Différentes stratégies d'offre, telles que hors charge (*off-load*) ou avec équilibrage de charge (*load-sharing*) peuvent être employées afin de déterminer qui doit remporter l'offre d'interface maître.
- **Le protocole L2F (*Level 2 Forwarding*, transmission de niveau 2).** Avant-projet de standard de l'IETF, le protocole L2F permet l'encapsulation de fragments MLP dans un tunnel entre l'interface physique MLP et l'interface maître MLP.

A l'aide de MMP, le potentiel MLP peut être aisément augmenté ou réduit, dans les grands pools de numérotation, selon les besoins. Des ressources processeur peuvent être ajoutées aux pools de numérotation, par l'intermédiaire de serveurs hors charge. Des tâches, telles que la fragmentation et le réassemblage MLP, la compression PPP et le cryptage, peuvent être gourmandes en ressources processeur ; leur exécution sur des serveurs hors charge peut se révéler avantageuse (voir Figure 11.10).

Figure 11.10
Sessions MMP actives.



Pour configurer MMP sur un serveur NAS Cisco IOS, utilisez la commande `sgbp`, comme suit :

```
kdt-3640(config)#sgbp ?
  group      SGBP group name
  member    SGBP group member configuration
  ppp-forward  SGBP participation for non-MultiLink PPP also
  seed-bid   mastership query seed bid
  source-ip  SGBP source ip address
```

Pour surveiller et dépanner MMP, utilisez à la fois `sgbpet vpdn` (pour L2F) :

```
sh sgbp  
sh vpdn  
debug sgbp  
debug vpdn
```

MMP représente une solution qui peut interopérer avec des matériels qui proviennent de différents fabricants, car il ne nécessite pas de fonctionnalités logicielles particulières sur les sites distants. La seule exigence est le support du standard de l'industrie MLP (RFC 1717).

Limitation des frais d'utilisation de RNIS

RNIS étant un système de connexion par circuits commutés, la facturation est fonction de la consommation. Dans ces conditions, l'objectif de la configuration sera de minimiser la durée d'activité des liaisons, en contrôlant les types de paquets qui déclenchent l'établissement de connexions. La réduction du temps d'activité devient difficile lorsque des protocoles de routage sont utilisés, car ils ont besoin d'envoyer des messages broadcast réguliers pour transmettre les informations de routage.

Sur certaines installations, les frais d'utilisation de RNIS peuvent facilement excéder les 20 000 francs par mois pour un seul site, si la conception et la gestion sont médiocres. Cisco recommande vivement la mise en place d'une administration de réseau appropriée, afin de soutenir une conception prudente, ce qui limite les frais. Selon les protocoles utilisés par le réseau, il est parfois nécessaire de recourir à une combinaison des techniques suivantes :

- analyse de trafic ;
- structure de tarification ;
- formation des utilisateurs ;
- exploitation de SNMP ;
- emploi de l'application CEA (*Cisco Enterprise Accounting*) pour RNIS ;
- comptabilité AAA.

Analyse de trafic

La plupart des solutions RNIS peuvent demeurer rentables tant que les canaux B RNIS restent inactifs la majeure partie de la journée. L'expérience montre que le Frame Relay peut représenter une solution plus rentable à partir d'un certain nombre d'heures par jour, selon l'application utilisée. Le point à partir duquel une ligne louée devient plus rentable dépend des structures de coût de chaque application point-à-point.

Chaque application et chaque protocole de réseau possède son lot de difficultés. Les clients de courrier électronique peuvent être configurés pour interroger régulièrement les serveurs POP. En vue d'une synchronisation, l'emploi du protocole NTP (*Network Time Protocol*) peut être souhaitable. Pour pouvoir contrôler exactement à quel moment les connexions DDR sont établies, le concepteur du réseau doit étudier de près les points suivants :

- Quels sont les sites qui peuvent initier des connexions en fonction du trafic ?

- Est-ce que les appels sortants sont requis vers des sites SOHO ? Si oui, le sont-ils pour l'administration réseau ou l'administration des stations de travail ?
- Quels sont les sites qui peuvent libérer les connexions en se fondant sur l'inactivité de liaison ?
- Comment les services d'annuaires et les tables de routage sont-ils supportés à travers une connexion inactive ?
- Quelles sont les applications qui doivent être gérées sur des connexions DDR ? Pour combien d'utilisateurs ?
- Quels sont les protocoles qui peuvent provoquer des connexions DDR de manière inattendue ? Peuvent-ils être filtrés ?
- Les filtres de numérotation fonctionnent-ils comme prévu ?

Des directives devraient être données aux utilisateurs sur la manière de limiter et/ou d'éliminer les frais RNIS excessifs. Ces directives résulteront en premier lieu de l'identification des applications requises sur ces connexions. Les outils de suivi de paquets peuvent être utilisés avec beaucoup d'efficacité afin de déterminer comment réduire ou éliminer les connexions DDR inutiles. Par exemple :

- L'envoi et la réception de courrier électronique devront, si possible, être manuels.
- Un réseau Windows peut nécessiter un échange de trafic de services d'annuaires périodique.
- Les serveurs AppleShare devront être déconnectés pour éviter les paquets tickle.
- Les applications d'accès aux bases de données, telles que les logiciels de planification, peuvent avoir besoin d'être déconnectées lorsqu'elles ne sont pas utilisées.

Structure de tarification

Certains fournisseurs de services RNIS procèdent à une facturation à la connexion et à la minute, même pour les appels locaux. Il est important d'examiner la question des frais de communications locales et longue distance lors du choix de la conception et des paramètres DDR. La fonction de rappel RNIS peut être utilisée dans le but de centraliser les frais de communication longue distance, ce qui peut réduire considérablement la surcharge liée aux tâches administratives, et offrir l'opportunité de réviser le cadre de facturation. La fonction de rappel RNIS peut également permettre d'améliorer la sécurité.

Formation des utilisateurs

Les utilisateurs finaux devraient être formés à surveiller leurs routeurs RNIS, ainsi que l'état des voyants de leurs canaux B sur leurs équipements BRI. Si les canaux B sont actifs alors que les utilisateurs ne travaillent sur aucune application de réseau, ils alerteront les administrateurs du réseau. La formation des utilisateurs peut se révéler très efficace dans le cadre d'une politique de réduction des frais RNIS.

Exploitation de SNMP

Le protocole SNMP (*Simple Network Management Protocol*) s'appuie sur des bases d'informations d'administration, les MIB (*Management Information Base*), afin de stocker des données sur les

événements de réseau. Actuellement, aucun standard n'existe pour les MIB RNIS mais, depuis l'introduction de Cisco IOS version 10.3(3), deux MIB RNIS Cisco sont disponibles. Grâce à ces MIB, les plates-formes d'administration compatibles SNMP (par exemple, HP OpenView ou SunNet Manager) peuvent interroger les routeurs Cisco afin d'obtenir des statistiques sur RNIS.

Les MIB RNIS Cisco se concentrent principalement sur l'interface RNIS et les informations de voisinage. Deux groupes MIB sont définis : demandNbrTable et demandNbrEntry. Le Tableau 11.2 répertorie certaines des variables MIB disponibles dans les MIB RNIS. L'application CEA pour RNIS peut permettre l'accès aux données de la MIB d'historique d'appels (*Call History*).

Tableau 11.2 : Variables MIB RNIS Cisco

<i>Objet MIB</i>	<i>Description</i>
demandNbrPhysIf	Valeur d'index de l'interface physique sur laquelle le voisin sera appelé ; sur une interface RNIS, c'est la valeur ifIndex du canal D.
demandNbrMaxduration	Durée maximale d'appel, en secondes.
demandNbrLastduration	Durée du dernier appel, en secondes.
demandNbrAcceptCalls	Nombre d'appels en provenance du voisin acceptés.
demandNbrRefuseCalls	Nombre d'appels en provenance du voisin refusés.

La MIB Cisco d'historique d'appels conserve les informations d'appel à des fins de comptabilité. L'objectif est de fournir l'historique d'une interface RNIS, ce qui inclut le nombre d'appels effectués et leur durée. La plupart des variables MIB d'historique d'appels font partie du groupe MIB ciscoCallHistory. Le Tableau 11.3 répertorie certaines de ces variables MIB.

Tableau 11.3 : Variables MIB Cisco d'historique d'appels

<i>Objet MIB</i>	<i>Description</i>
ciscoCallHistoryStartTime	La valeur de sysUpTime, lorsque cette entrée d'historique d'appel a été créée. Cette variable peut être utilisée afin d'extraire tous les appels intervenus après une heure spécifique.
ciscoCallHistoryCalledNumber	Le numéro qui a été utilisé pour effectuer cet appel.
ciscoCallHistoryCallConnectionTime	La valeur de sysUpTime, lorsque la connexion a été établie.
ciscoCallHistoryCallDisconnectTime	La valeur de sysUpTime, lorsque la connexion a été libérée.

Les MIB RNIS de Cisco impliquent le support de SNMP sur le réseau. Si une plate-forme compatible SNMP est présente, les MIB peuvent fournir des informations précieuses sur les liaisons RNIS. La MIB d'historique d'appels apporte en particulier des renseignements essentiels sur les durées d'activité RNIS, ce qui est utile pour contrôler les frais.

Cisco propose une large gamme de produits RNIS afin de répondre à la variété des besoins en matière de connexion. Le système Cisco IOS fournit un certain nombre de fonctionnalités qui optimisent les

performances du réseau RNIS et en minimisent les frais d'exploitation, telles le routage Snapshot, les listes d'accès, le filtrage NBP (pour AppleTalk), ainsi que le contrôle de paquets *watchdog* et *keepalive* (pour IPX).

Emploi de l'application CEA (Cisco Enterprise Accounting) pour RNIS

CEA pour RNIS est une application qui s'exécute sous Windows NT. Elle peut être utilisée pour superviser la MIB d'historique d'appels et fournir aux gestionnaires de réseau des enregistrements détaillés d'appels, avec une estimation des coûts.

Comptabilité AAA

La comptabilité AAA peut être implémentée pour fournir un retour d'informations sur la durée de connexion des sessions PPP. Les informations de comptabilité sont transportées vers des serveurs TACACS+ ou RADIUS, où elles peuvent en général être consultées au moyen d'outils SQL standards, afin de générer ou de planifier des rapports. La commande suivante active les enregistrements de la comptabilité AAA pour les sessions PPP :

```
aaa accounting network stop-only
```

Dépannage de RNIS

Lors du dépannage de RNIS, il est important de garder à l'esprit l'architecture de protocoles RNIS, ainsi que sa relation avec le modèle de référence OSI. RNIS opère au niveau des trois couches OSI inférieures, c'est-à-dire physique, liaison de données et réseau. Au niveau de la couche réseau, des protocoles tels I.430 pour BRI et I.431 pour PRI sont répartis sur les canaux B et D. Au niveau liaison de données, PPP est utilisé en tant que protocole de canal B. HDLC pourrait l'être également, mais il présente moins d'avantages que PPP. LAPD (Q.921) est employé en tant que protocole de canal D sur cette couche. Au niveau de la couche réseau, des protocoles tels que IP, IPX, etc. sont employés sur des canaux B ; Q.931 est utilisé sur le canal D.

Il faut donc tenir compte de cette structure lors du dépannage, et procéder de façon systématique et progressive. Commencez par résoudre les problèmes de la couche physique, avant de vous attaquer à ceux des couches supérieures. Examinez toujours les deux extrémités d'une connexion RNIS ; cela vous permettra de cerner de nombreux problèmes, qui seront traités en détail plus loin dans ce chapitre.

Avant de dépanner un lien RNIS, il est conseillé d'exécuter un ping de l'interface RNIS distante. Si vous y parvenez, cela signifie que la connexion fonctionne correctement. Dans le cas contraire, inutile de mettre en cause le routage. N'oubliez pas qu'une interface RNIS est une interface DDR ; avec Cisco IOS, elle devient active uniquement lorsque des paquets intéressants déclenchent l'établissement de la connexion. Pour vérifier la configuration du routeur et surveiller le trafic intéressant, vous pouvez utiliser sur le routeur les commandes suivantes : `debug dialer events` et `debug dialer packets`.

L'exemple suivant illustre la présence de paquets intéressants qui déclenchent la liaison RNIS. Vous pouvez voir leurs adresses IP source et de destination :

```
Router # debug dialer events
Dialing cause: BRI0: ip (s=20.20.20.20 d=20.20.22.22)
Router # debug dialer packets
BRI0: ip (s=20.20.20.20, d=20.20.22.22), 100 bytes, interesting (ip PERMIT)
```

Dépannage de la couche physique

Vous devriez toujours commencer par résoudre les problèmes de cette couche. Une commande IOS très pratique, `show isdn status`, signale l'état des trois couches pour PRI ou BRI (BRI, dans notre exemple). En l'exécutant, vous pouvez donc avoir une idée de la source du problème. Le résultat suivant indique que la couche 1 (physique) se trouve dans un état désactivé, ce qui dénote une situation anormale. En effet, lorsqu'une couche n'est pas active, aucune des couches supérieures ne peut l'être.

```
Router # show isdn status
ISDN BRI0 interface
  Layer 1 Status:
    DEACTIVATED
  Layer 2 Status:
    Layer 2 NOT Activated
  Layer 3 Status:
    No Active Layer 3 Call(s)
  Activated dsl 0 CCBs are 0, Allocated = 0
```

Cette situation peut provenir soit d'un problème externe, soit d'un problème interne au routeur. Dans le premier cas, il peut s'agir d'une défaillance de câblage, de l'opérateur téléphonique, d'une terminaison numérique de réseau (TNR). On peut encore envisager que le réseau n'a pas répondu à la requête d'activation de l'interface RNIS du routeur. Un problème interne au routeur signifie simplement que celui-ci n'a pas émis de requête d'activation de l'interface RNIS.

Commande `debug bri`

Une commande IOS très pratique, `debug bri`, permet de savoir si le problème est interne au routeur ou non. Cette commande met en œuvre une communication entre le système IOS et le chipset RNIS de l'interface RNIS. Les commandes `write_sid` sont envoyées au chipset RNIS. En fonction du type de routeur Cisco, vous obtenez différentes valeurs `wrote` (`wrote = E`, `wrote = 1B`, etc.). Plus précisément, l'exécution d'une commande `write_sid` signifie que le routeur tente d'activer la liaison et demande au chipset RNIS de générer des indicateurs HDLC. Par exemple, `wrote = 1B` signifie que le chipset RNIS envoie ces indicateurs. Si tout se passe bien, ces commandes `write_sid` sont suivies d'interruptions SID (*SID interrupt*), avec un état `reg = C`. Ces interruptions sont ensuite envoyées par le chipset RNIS au système IOS, et indiquent que le bit d'activation (A) vient d'être activé, ce que le réseau prend en compte. Avec les nouvelles versions de Cisco IOS, cette même information est fournie par une indication d'activation de message reçu. Les résultats suivants indiquent que le réseau ainsi que le routeur effectuent chacun correctement leur tâche :

```
BRI: write_sid: scp = 0, wrote = 1B
BRI: write_sid: scp = 0, wrote = 20
BRI: write_sid: scp = 0, wrote = 3
SID interrupt. status reg = C
BRI: Received activation indication...
BRI: write_sid: scp = 0, wrote = E
BRI: write_sid: scp = 0, wrote = E
```

Lorsque tout ne se passe pas comme prévu, la commande `debug bri` produit la sortie suivante :

```
BRI: Starting Power Up timer for unit = 2
BRI: write_sid: wrote 3 for subunit 2, slot 1
BRI: Starting T3 timer after expiry of Power
Up timeout for unit = 2, current state is F4 ...
BRI: write_sid: wrote 92 for subunit 2, slot 1
```

```
BRI: write_sid: wrote 93 for subunit 2, slot 1
BRI: T3 timer expired for unit = 2, current state is F2
BRI: write_sid: wrote 1 for subunit 2, slot 1
BRI: write_sid: wrote 0 for subunit 2, slot 1
BRI: Forced interrupt for subunit 2, slot 1 is F
BRI: write_sid: wrote FF for subunit 2, slot 1
BRI: write_sid: wrote 1 for subunit 2, slot 1
BRI: write_sid: wrote 0 for subunit 2, slot 1
BRI: Deactivation for unit = 2, current state is F2
```

Où T3 représente le bloc descripteur dans IOS. Notez que le routeur envoie des commandes `write_sid`, ce qui signifie qu'il tente d'activer la ligne et demande au chipset RNIS de générer des indicateurs HDLC. `wrote = 3` indique que le chipset génère effectivement ces indicateurs. Mais, lorsque ces derniers demeurent sans réponse, le routeur déclenche le temporisateur T3 et tente d'envoyer quelques indicateurs HDLC supplémentaires. A l'expiration du temporisateur, le routeur place l'interface BRI dans un état de désactivation. Les résultats de l'exemple précédent indiquent que le routeur remplit son rôle, à l'inverse réseau, qui ne répond pas en activant le bit d'activation. Le problème est donc externe au routeur. Dans la plupart des cas, le câblage ou l'opérateur téléphonique sont la source du problème.

Lorsque la couche physique ne présente aucun problème et qu'elle est activée, vous devriez obtenir les résultats suivants, à l'aide, respectivement, des commandes `show isdn status` et `show controller bri`:

```
Layer 1 Status: ACTIVATED
```

ou

```
Layer 1 is ACTIVATED
```

Dépannage d'une interface PRI

Tenter de résoudre des problèmes PRI de couche 1 revient à essayer de dépanner une connexion T1. Lorsque tout fonctionne correctement, aucune alarme n'est détectée sur la connexion T1. Vérifiez que vous obtenez bien le résultat suivant, à l'aide de la commande `show controller t1`:

```
Router # show controller t1
T1 2/0 is up
Description: Primary Rate Interface to DMS-100
No alarms detected
Framing is ESF, Line Code is B8ZS, Clock Source is Line
Data in current interval (165 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 1 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errorred Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 12 Unavail Secs
```

En revanche, en cas de problème, vous devriez voir que le transmetteur envoie des alarmes distantes, ce qui est mauvais signe. Les principales informations à surveiller sont l'état de la ligne, les alarmes, ainsi que les violations de code et de chemin (*code/path violations*). L'état de la ligne indique si elle est active, inactive ou administrativement inactive. La section relative aux alarmes est particulièrement importante, car elle permet de connaître le type de problème qui intervient sur la ligne. La présence d'une alarme signifie un problème majeur. Par conséquent, si une connexion T1 est en état d'alarme, vous devriez vérifier la configuration de la délimitation de trames et des paramètres de codage de ligne. Le résultat suivant reflète une situation problématique au niveau de la couche physique, dans un environnement PRI.

```
Router # show controller t1
T1 2/1 is down
Transmitter is sending remote alarm
Receiver has loss of signal
Framing is ESF, Line Code is B8ZS, Clock Source is Line
Data in current interval (160 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs,
  0 Errorred Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 160 Unavail Secs
```

Dépannage de la couche liaison de données

Nous avons fait le tour des problèmes qui peuvent survenir au niveau de la couche physique, et avons vu comment les résoudre. Nous allons à présent aborder ceux de la couche 2 (liaison de données). Si la commande `show isdn status` produit le résultat suivant, cela signifie que la couche 1 est active, mais non la couche 2 :

```
Router # show isdn status
The current ISDN Switchtype = basic-net3
ISDN BRI0 interface
Layer 1 Status:
Activated
Layer 2 Status:
Layer 2 NOT Activated
Layer 3 Status:
No Active Layer 3 Call(s)
Activated dsl 0 CCBs are 0, Allocated = 0
```

Comme nous l'avons mentionné, deux types de protocoles opèrent au niveau de cette couche : PPP (canal B) et LAPD (canal D). Vous devriez régler les problèmes de liaison de données pour les canaux B et D séparément. Le standard RNIS ne définit pas de protocole particulier de couche 2 pour le canal B. Dans la plupart des cas, PPP est utilisé, car il est souple d'utilisation. Sur le canal D, LAPD (*Link Access Procedure* sur canal D) devrait être employé afin d'être en conformité avec le standard. Ce protocole est également appelé Q.921. La signalisation Q.921 est mise en œuvre entre le routeur local et le commutateur RNIS local, mais ne fonctionne pas de bout en bout.

Dépannage du processus TEI

Dans un environnement BRI, le processus TEI (*Terminal Endpoint Identifier*) a lieu au niveau de la couche 2. La raison d'une assignation d'identifiant TEI dans un tel environnement est qu'une connexion S/T sur une seule interface BRI peut supporter jusqu'à huit équipements, chacun d'eux possédant un numéro TEI unique assigné par le commutateur RNIS local. Grâce à ces identifiants, le commutateur peut distinguer les différents équipements connectés au bus S/T sur l'interface BRI. Si tout fonctionne normalement, lorsque le routeur envoie une requête d'identification (IDREQ) au commutateur, ce dernier accuse réception au moyen d'un paquet d'identification assignée (IDASSN).

Les paquets IDREQ et IDASSN contiennent deux valeurs importantes : l'indicateur d'action (AI, *Action Indicator*) et l'indicateur de référence (RI, *Reference Indicator*). Chaque fois que le routeur envoie une requête IDREQ au commutateur, l'indicateur AI possède toujours la valeur 127. Ce caractère générique signifie que le routeur demande au commutateur d'assigner n'importe quelle valeur TEI valide. La plage de valeurs TEI valides est comprise entre 64 et 126. Les valeurs TEI situées entre 0 et 63 sont réservées pour des identifiants TEI fixes. Aux débuts de RNIS, les valeurs

TEI étaient configurées manuellement. A l'heure actuelle, tout le processus de négociation et d'assignation TEI est dynamique. Gardez à l'esprit que, dans un environnement PRI, un seul équipement est connecté à l'interface RNIS. Par conséquent, l'utilisation de ces identifiants n'est pas nécessaire, d'où une valeur TEI de 0.

L'indicateur RI dans le paquet IDREQ contient toujours un numéro aléatoire, qui devrait être le même dans le paquet IDASSN de réponse du commutateur. L'exécution de la commande `debug isdn q921` sur le routeur révèle le processus d'assignation. Le résultat suivant montre que le routeur envoie un message IDREQ avec RI = 15454 (qui est une valeur aléatoire) et AI = 127 (qui est un caractère générique). Le paquet IDASSN du commutateur utilise la même valeur RI, mais une valeur AI = 64, c'est-à-dire l'identifiant TEI 64 valide :

```
Router # debug isdn q921
TX -> IDREQ ri = 15454 ai = 127
RX <- IDASSN ri = 15454 ai = 64
```

Lorsqu'un problème survient, le paquet IDREQ est retransmis avec des valeurs RI différentes et une valeur AI de 127, sans que le commutateur n'envoie de paquet IDASSN. Dans ce cas, le routeur fonctionne correctement, à l'inverse du commutateur, qui n'acquitte pas le message du routeur. Il arrive parfois que le commutateur réponde, mais en assignant un identifiant TEI invalide, ce qui est également révélateur d'un dysfonctionnement du commutateur :

```
Router # debug isdn q921
TX -> IDREQ ri = 89898 ai = 127
TX -> IDREQ ri = 90976 ai = 127
TX -> IDREQ ri = 23434 ai = 127
```

Après que le commutateur local a assigné au routeur un identifiant TEI valide, le routeur tente d'établir une connexion HDLC traditionnelle avec le commutateur. Le routeur envoie un message SABME (*Set Asynchronous Balance Mode Extended*) avec l'identifiant TEI 64 qui vient d'être assigné par le commutateur local. L'identifiant de point d'accès au service (SAPI, *Service Access Point Identifier*) se comporte comme étant un champ de type sur Ethernet, et identifie le protocole de couche supérieure. Dans le résultat de la commande `debug isdn q921`, vous pouvez voir que la valeur de SAPI est égale à 0, ce qui veut dire que le protocole de canal D de couche 3 utilisé est Q.931. Le commutateur répond au message SABME par un message UA, ce qui signifie qu'il accepte l'identifiant

```
Router # debug isdn q921
TX -> SABMEp sapi = 0 tei = 64
RX <- UAf sapi = 0 tei = 64
```

Une fois la connexion de liaison de données établie, des trames d'information INFO sont échangées entre le routeur et le commutateur local. Ces trames sont acquittées au moyen d'autres trames INFO ou de trames RR (*Receive Ready*). N'oubliez pas que ces trames INFO contiennent les messages de signalisation Q.931, c'est-à-dire qu'elles contiennent un champ NS (envoi de numéro de séquence) et un champ NR (numéro de séquence suivant attendu) :

```
Router # debug isdn q921
RX <- INFOc sapi = 0 tei = 64 ns = 0 nr = 0
TX -> RRr sapi = 0 tei = 64 nr = 1
TX -> INFOc sapi = 0 tei = 64 ns = 0 nr = 1
```

Lorsqu'aucune trame INFO n'est échangée entre le routeur et le commutateur local, vous devriez remarquer un échange périodique de trames RR. Cet échange fait office de mécanisme *keepalive*,

c'est-à-dire qu'il permet de contrôler l'activité de la connexion de niveau 2, même si aucun trame INFO ne circule. Dans ce cas, la commande `debug isdn q921` produirait une sortie analogue à ce qui suit :

```
Router # debug isdn q921
RX <- RRp sapi = 0 tei = 80 nr = 5
TX -> RRF sapi = 0 tei = 80 nr = 4
RX <- RRp sapi = 0 tei = 80 nr = 5
TX -> RRF sapi = 0 tei = 80 nr = 4
RX <- RRp sapi = 0 tei = 80 nr = 5
TX -> RRF sapi = 0 tei = 80 nr = 4
RX <- RRp sapi = 0 tei = 80 nr = 5
TX -> RRF sapi = 0 tei = 80 nr = 4
```

Lorsque la communication au niveau de la couche 2 est opérationnelle, vous devriez obtenir le résultat suivant, avec la commande `debug isdn q921` (tous les champs affichés ont été décrits précédemment) :

```
Router # debug isdn q921
TX -> IDREQ ri = 15454 ai = 127
RX <- IDASSN ri = 15454 ai = 64
TX -> SABMEp sapi = 0 tei = 64
RX <- UAf sapi = 0 tei = 64
RX <- INFOc sapi = 0 tei = 64 ns = 0 nr = 0
TX -> RRr sapi = 0 tei = 64 nr = 1
TX -> INFOc sapi = 0 tei = 64 ns = 0 nr = 1
```

A présent, la commande `show isdn status` devrait révéler la valeur TEI et l'état de la couche 2 :

```
Router # show isdn status
Layer 1 Status:
    ACTIVE
Layer 2 Status:
    TEI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
Layer 3 Status:
    0 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 0
```

Vous pouvez donc voir que la valeur TEI est égale à 0, ce qui signifie qu'il s'agit d'une liaison PRI. S'il s'était agi d'une interface BRI, la valeur TEI aurait été valide (c'est-à-dire qu'elle serait située dans une plage de 64 à 126). L'état de la couche 2 indiqué (**MULTIPLE_FRAME_ESTABLISHED**) signifie qu'elle est opérationnelle, à l'inverse de la couche 3, qui n'est pas active.

Dépannage de la couche réseau

Nous allons maintenant aborder les problèmes de la couche 3. Rappelez-vous que deux types de protocoles opèrent à ce niveau : les protocoles IP, IPX, etc. (canal B) et les protocoles Q.931 (canal D). Le standard RNIS ne définit pas de protocole particulier de couche 2 pour le canal B. Des protocoles de niveau 3, tels que IP, IPX et autres, pourraient donc être utilisés, en fonction du protocole de canal B de niveau 2. Sur le canal D, Q.931 devrait être utilisé, afin de respecter le standard RNIS. La signalisation Q.931 est mise en œuvre entre le routeur local et le commutateur RNIS local, et permet d'indiquer au commutateur que vous souhaitez appeler un numéro. Lorsque le commutateur tente d'établir l'appel, il traduit les signaux Q.931 en signaux SS7 correspondants (car la signalisation SS7 est exploitée au sein d'un réseau RNIS). Lorsque le commutateur RNIS distant reçoit les signaux SS7, il les traduit de nouveau en signaux Q.931 correspondants. La signalisation Q.931 ne fonctionne pas de bout en bout.

Q.931

Q.931 est un protocole de signalisation de couche 3 pour les canaux D, dans un environnement RNIS. Etant donné qu'il n'a pas été normalisé dès les débuts de RNIS, il existe plusieurs moutures de ce protocole, dont plusieurs ont été développées par les principaux opérateurs téléphoniques. Bien que ces versions soient semblables, vous devez veiller à configurer le même type de commutation au niveau du routeur et du commutateur RNIS local. Si le commutateur est configuré pour la commutation RNIS de type basic-ni1, le routeur doit être configuré pour supporter ce même type de commutation, dont il existe également plusieurs versions. Des efforts sont mis en œuvre en vue de définir basic-net3 en tant que standard européen, et basic-ni1 en tant que standard américain.

Q.931 supporte 37 méthodes d'établissement de connexion différentes. Il s'agit d'un protocole très souple et très étendu. La signalisation SVC Frame Relay ainsi que la signalisation UNI ATM se fondent sur la signalisation Q.931. La commande `debug isdn q931` peut être activée sur le routeur pour surveiller les signaux Q.931 et détecter une éventuelle défaillance. Pour obtenir une vision d'ensemble, vous devez l'exécuter des deux côtés de la connexion. Tous les signaux Q.931 de niveau 3 sont transmis dans des trames INFO de niveau 2 :

```
Router # debug isdn q931
TX -> INFOc sapi = 0 tei = 80 ns = 6 nr = 6
      SETUP pd = 8 callref = 0x02
          Bearer Capability i = 0x8890
          Channel ID i = 0x83
          Called Party Number i = 0x80, '555555'
RX <- INFOc sapi = 0 tei = 80 ns = 6 nr = 7
      CALL_PROC pd = 8 callref = 0x82
          Channel ID i = 0x89
RX <- INFOc sapi = 0 tei = 80 ns = 7 nr = 7
      CONNECT pd = 8 callref = 0x82
```

Chaque fois que le routeur établit un appel, il doit envoyer un paquet SETUP contenant toujours un descripteur de protocole `pd = 8` (`pd, protocol descriptor`). Une valeur hexadécimale aléatoire est générée pour le numéro de référence `callref`, qui est utilisé pour garder trace de l'appel. Si deux appels sont établis, la valeur de `callref` permet de déterminer à quel appel appartient le message RX (reçu). 0x8890 signifie qu'il s'agit d'un appel de type données à 64 Kbit/s ; 0x8890218F d'un appel de type données à 56 Kbit/s ; et 0x8090A2 d'un appel de type voix. L'identifiant de canal 0x83 signifie que le routeur demande au commutateur de lui assigner un canal D. Le numéro de la partie appelée est 555555.

Le message CALL_PROC indique que l'appel est en cours. Le premier chiffre du numéro de référence est différent, afin de distinguer un appel TX d'un appel RX. Le second chiffre est identique à celui contenu dans le message SETUP. L'identifiant de canal 0x89 désigne le premier canal B, et 0x8A désigne le second. Cette séquence d'événements est la même pour chaque établissement d'appel. Le routeur est totalement dépendant de la société de téléphonie en ce qui concerne l'assignation d'un canal B. Si le commutateur n'assigne pas de canal au routeur, l'appel ne peut être établi. Dans ce cas, un message CONNECT, avec le même numéro de référence que celui reçu pour CALL_PROC (0x82), est reçu de la part du commutateur.

SPID

Une fois que les couches 1 et 2 sont actives, le routeur doit en premier lieu envoyer l'identifiant SPID au commutateur, avant tout message SETUP. Les identifiants SPID sont assignés par le fournisseur de services et devraient être configurés sur le routeur tels qu'ils ont été fournis. Il s'agit habituellement de nombres de 12 à 14 chiffres constitués du numéro de téléphone et de chiffres supplémentaires. Ils sont utilisés uniquement en Amérique du Nord, et seuls certains types de commutateurs requièrent leur emploi (par exemple, dms-100 et ni-1). De plus, ils sont mis en œuvre uniquement dans des environnements BRI.

Ces identifiants permettent d'associer un terminal particulier à un profil de service spécifique. Ils sont validés par le commutateur RNIS local lors d'un échange avec le routeur. Un identifiant SPID valide est acquitté par un identifiant de point terminal (*endpoint ID*). Si le SPID est rejeté par le commutateur, il renvoie un message de contenu d'élément d'information invalide (*Invalid IE Contents*). Cette négociation peut être visualisée au moyen de la commande `debug isdn q931`. Dans le résultat suivant, vous pouvez voir que le routeur envoie au commutateur deux identifiants SPID, l'un après l'autre. Les deux sont acquittés par le commutateur, ce qui est signifié par l'envoi d'un identifiant de point terminal pour chaque SPID transmis. Ces SPID sont codés au format Ascii, c'est-à-dire que 36 signifie 3, 31 signifie 1, etc. Dans certains cas, vous devez configurer le numéro LDN après les SPID. Ce numéro est configuré afin de pouvoir recevoir des appels entrants sur le second canal B.

```
Router # debug isdn q931
TX -> INFORMATION pd = 8 callref = (null)
SPID Information i = 0x363133373835323631323030
RX <- INFORMATION pd = 8 callref = (null)
ENDPOINT IDent i = 0xF180
TX -> INFORMATION pd = 8 callref = (null)
SPID Information i = 0x363133373835323631333030
RX <- INFORMATION pd = 8 callref = (null)
ENDPOINT IDent i = 0xF080
```

Dans le résultat suivant, vous pouvez voir que le SPID envoyé au commutateur est rejeté au moyen d'un message de contenu d'élément d'information invalide ("Invalid IE contents"). En effet, le SPID est invalide. Dans ce cas, il faut déterminer si le routeur et le commutateur sont configuré avec le SPID correct :

```
TX -> INFORMATION pd = 8 callref = (null)
SPID Information i = 0x31323334353536373736
RX <- INFORMATION pd = 8 callref = (null)
Cause i = 0x82E43A-Invalid IE contents
```

A ce stade, la commande `sh isdn status` renseignera sur l'état des SPID. Dans la sortie suivante, les deux SPID sont rejettés, car ils sont invalides :

```
Router # show isdn status
Layer 1 Status:
ACTIVE
Layer 2 Status:
TEI = 88, State = MULTIPLE_FRAME_ESTABLISHED
Spid Status:
TEI 88, ces = 1, state = 6(not initialized)
spid1 configured, no LDN, spid1 sent, spid1 NOT valid
TEI Not Assigned, ces = 2, state = 1(terminal down)
spid2 configured, no LDN, spid2 NOT sent, spid2 NOT valid
```

```
Layer 3 Status:  
0 Active Layer 3 Call(s)  
Activated dsl 1 CCBs = 0
```

Messages RELEASE_COMP

Une fois que le commutateur a validé les SPID, l'appel peut être établi. Il existe plusieurs raisons pour lesquelles un appel peut être refusé. Si l'autre extrémité est configurée pour le filtrage d'appel et n'autorise par conséquent que certains numéros — dont vous ne faites pas partie —, l'appel peut échouer. Il est possible également que le réseau soit défaillant. Le résultat suivant, produit par la commande `debug isdn q931`, montre que la connexion RNIS n'a pas été établie. L'envoi d'un message SETUP résulte en un message RELEASE_COMP en retour, qui contient un identifiant de cause relatif au rejet de l'appel. On peut voir qu'il s'agit ici d'un problème de niveau Q.931. Il est important de faire la différence entre une connexion qui n'a jamais établie (problème Q.931) et une connexion qui l'a été pendant quelques secondes avant d'être interrompue (Q.931 fonctionne normalement, mais non PPP) :

```
Router # debug isdn q931  
TX -> SETUP pd = 8 callref = 0x01  
Bearer Capability i = 0x8890  
Channel ID i = 0x83  
Called Party Number i = 0x80, '4839625'  
RX <- RELEASE_COMP pd = 8 callref = 0x81  
Cause i = 0x8295 - Call rejected
```

L'identifiant de cause relatif au rejet d'appel est une valeur hexadécimale. Pour déterminer la cause d'une défaillance, décodez-la, puis consultez votre fournisseur. Si l'appel s'établit puis s'interrompt après quelques secondes, Q.931 fonctionne normalement, mais non PPP. Ce protocole s'exécute sur le canal B de RNIS et est transparent pour l'opérateur. Il se fonde sur le RFC 1548, entre autres. Les trois principaux composants de PPP sont l'encapsulation multiprotocole, LCP et les protocoles NCP. LCP est utilisé afin d'établir et de maintenir la liaison de données, ainsi que pour assurer la négociation d'options (telle l'utilisation de CHAP). Les protocoles NCP sont employés afin d'établir et de configurer les protocoles de niveau 3, dont la négociation d'options spécifiques aux protocoles (adresses) ainsi que différents protocoles de niveau 3 (IPCP, IPXCP, ATCP, etc.). Lors de la négociation PPP, les options LCP sont négociées en premier et suivies des options NCP.

LCP

Lors de la négociation LCP, une requête de configuration (CONFREQ) propose plusieurs options. Lorsque ces dernières sont toutes acceptables, la station distante retourne un acquittement de configuration (CONFACK). Toutes les négociations PPP sont bidirectionnelles. Vous pouvez observer ce processus en exécutant des commandes `debug` sur certains routeurs Cisco. Le résultat de la commande `debug` suivante montre une requête CONFREQ entrante (I, *incoming*) et un message CONFACK sortant (O, *outgoing*) :

```
Router # debug ppp packet  
PPP BRI: B-Channel 1: I LCP CONFREQ(1) id 2 (4)  
PPP BRI: B-Channel 1: O LCP CONFACK(2) id 2 (4)
```

Le résultat de la commande `debug` suivante montre la négociation pour le type d'authentification PAP (value = C023) et le nombre magique (MAGICNUMBER) qui évite la formation de boucle sur la connexion.

S'il s'agissait d'une authentification CHAP, vous verriez la valeur hexadécimale C223 :

```
Router # debug ppp negotiation
ppp: sending CONFREQ, type = 3 (CI_AUTHTYPE), value = C023/0
ppp: sending CONFREQ, type = 5 (CI_MAGICNUMBER), value = 8C01B4
ppp: config ACK received, type = 3 (CI_AUTHTYPE), value = C023
ppp: config ACK received, type = 5 (CI_MAGICNUMBER), value = 8C01B4
```

La commande `show interface bri 0 1` indique si l'état de LCP est ouvert (OPEN) ou fermé (CLOSED). Si les options sont négociées, l'état devrait être ouvert. Le résultat suivant indique un état LCP ouvert, mais les options NCP n'ont pas encore été négociées :

```
Router # show interface bri 0 1
BRI0: B-Channel 1 is up, line protocol is up
    Hardware is BRI
    MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
    Encapsulation PPP, loopback not set, keepalive set (10 sec)
    lcp state = OPEN
    ncp ipcp state = REQSENT    ncp osicp state = NOT NEGOTIATED
    ncp ipxcp state = NOT NEGOTIATED    ncp xnscp state = NOT NEGOTIATED
    ncp vinescp state = NOT NEGOTIATED    ncp deccp state = NOT NEGOTIATED
    ncp bridgecp state = NOT NEGOTIATED    ncp atalkcp state = NOT NEGOTIATED
    Last input 0:00:00, output 0:00:00, output hang never
    Last clearing of "show interface" counters never
    Output queue 0/40, 0 drops; input queue 0/75, 0 drops
    Five minute input rate 0 bits/sec, 0 packets/sec
    Five minute output rate 0 bits/sec, 1 packets/sec
    9099 packets input, 855915 bytes, 0 no buffer
```

Si l'état LCP est fermé, les options PPP ne correspondent pas sur les deux équipements (à moins qu'il ne s'agisse d'une liaison à 56 Kbit/s). La majorité des connexions longue distance en Amérique du Nord, ainsi que les connexion internationales avec cette partie du monde, sont limitées à 56 Kbit/s. Pour ces connexions, il arrive parfois que le bit de poids de plus fort des données envoyées soit remplacé par les informations de signalisation, ce qui modifie les données ou génère des erreurs CRC visibles pour l'équipement situé à l'autre extrémité. Dans ce cas, utilisez la spécification V.110 à 56 Kbit/s. Avec cette spécification, sur les huit positions binaires pour chaque canal B, seuls sept bits sont utilisés pour le transfert des données, le huitième contenant des données quelconques, de façon à éviter une altération de la charge utile.

Dans plusieurs situations, les connexions intercommutateurs peuvent ramener la vitesse à 56 Kbit/s. Il existe plusieurs capacités de canal porteur (*bearer capability*) qui spécifient si l'appel est établi à 56 Kbit/s et s'il exploite l'adaptation de débit de la spécification V.110. Si le protocole de signalisation international sur le réseau RNIS est adapté à RNIS, cette indication de 56 Kbit/s sera transmise jusqu'à l'abonné distant, qui traitera l'appel à cette vitesse. Parfois, sur les liaisons internationales, cette indication est éliminée, car l'opérateur met en œuvre une ancienne version de SS7. Dans ce cas, la partie réceptrice pense que l'appel s'effectue à 64 Kbit/s. L'instruction `dialer map` sur un routeur Cisco permet de spécifier la vitesse de l'appel sortant, la valeur par défaut étant de 64 Kbit/s. Le résultat de la commande `debug isdn q931` fait parfois apparaître un message qui indique que l'appel n'est pas un appel RNIS de bout en bout ("Call not end-to-end RNIS"). Si vous obtenez ce message, vous pouvez configurer `isdn not-en-to-end 56` sur le routeur, afin qu'il traite l'appel à une vitesse de 56 Kbit/s :

```
Router # debug isdn q931
TX -> SETUP pd = 8 callref = 0x02
      Bearer Capability i = 0x8890
      Channel ID i = 0x83
```

```

Called Party Number i = 0x80, '5555555'
RX <- CALL_PROC pd = 8
    callref = 0x82
    Channel ID i = 0x89
    Locking Shift to Codeset 5
    Codeset 5 IE 0x2A i = 0x808E0C, 'OUTSIDE CALL'
RX <- PROGRESS pd = 8 callref = 0x82
    Progress Ind i = 0x8A81 -
Call not end-to-end ISDN
RX <- CONNECT pd = 8 callref = 0x82
    Progress Ind i = 0x8482 - Destination address is non-ISDN

```

Type d'authentification PPP

Une fois que les problèmes relatifs à LCP et au débit à 56 Kbit/s sont résolus, l'étape suivante consiste à vérifier l'authentification PPP. HDLC pourrait être utilisé en tant que protocole de canal B de niveau 2, mais il ne supporte aucun type d'authentification. Certains implémentent ce protocole dans le seul objectif de voir RNIS fonctionner, sans se soucier de l'authentification. Une telle approche est à éviter, car l'utilisation de PAP ou de CHAP permet de résoudre les problèmes de préfixes. CHAP est souvent préféré à PAP, car il utilise une fonction de hachage MD5. Si vous exécutez la commande debug ppp chap sur le routeur, vous pouvez observer le processus de négociation :

```

Router # debug ppp chap
ISDN Event: Connected to 5555555 on B1 at 64 kbps
BRI0: B-Channel 1: PPP AUTH CHAP input code = 1 id = 10 len = 14
BRI0: B-Channel 1: PPP AUTH CHAP input code = 2 id = 16 len = 26
BRI0: B-Channel 1: remote passed CHAP authentication
BRI0: B-Channel 1: PPP AUTH CHAP input code = 3 id = 10 len = 4
BRI0: B-Channel 1: Passed CHAP authentication with remote...

```

Vous pouvez également exécuter la commande show dialer des deux côtés de la connexion, afin de vérifier que le nom du routeur distant est contenu dans le résultat. Si le nom apparaît des deux côtés, l'authentification CHAP ou PAP a réussi, car ce nom est communiqué au cours de ce processus. Dans le cas contraire, assurez-vous que le mot de passe pour l'authentification est bien le même des deux côtés, sachant qu'il est sensible à la casse. Dans l'exemple suivant, vous savez que l'authentification CHAP ou PAP a réussi, car le nom est affiché (SANJOSE) :

```

Router # show dialer
BRI0 - dialer type = ISDN
Dial String      Successes   Failures   Last called   Last status
4085555555      0           0           never
0 incoming call(s) have been screened
BRI0: B-Channel 1 - dialer type = ISDN
Rotary group 0, priority = 0
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Time until disconnect 85 secs
Connected to 4085555555 (SANJOSE)

```

PAP et CHAP permettent d'identifier le site connecté. Sans ces protocoles, cette information serait déterminée au moyen du numéro d'appelant RNIS, ce qui pose souvent problème, car ce numéro peut ne pas avoir été présenté, ou présenté avec ou sans préfixe. Il arrive que les opérateurs modifient les numéros en ajoutant ou en supprimant un préfixe, mais ils peuvent également ajouter ou supprimer des numéros. Il est donc délicat de s'appuyer sur le préfixe d'une connexion RNIS. Lorsque vous introduisez CHAP ou PAP, ce problème est résolu puisque ces protocoles s'appuient sur le nom d'hôte du routeur distant.

Protocoles NCP

Il faut ensuite se concentrer sur les problèmes liés aux protocoles NCP, qui négocient et vérifient les paramètres de niveau réseau. Un protocole NCP différent est associé à chaque protocole de réseau (IPCP pour IP, IPXCP pour IPX, etc.). Une requête de configuration NCP est envoyée à un protocole NCP, à l'autre extrémité de la connexion. Si cette dernière supporte le protocole NCP, elle acquitte la requête au moyen d'un message d'acquittement. Sinon, elle renvoie un message de configuration NCP non acquittée ("NCP configure-not-acknowledge"). Les deux parties échangent ces messages afin de s'accorder sur les NCP supportés par chacune. Le résultat de la commande debug suivante illustre la négociation du protocole IPCP :

```
Router # debug ppp negotiation
BRI0: B-Channel 1: O IPCP CONFREQ id D (10) Type3 (6) 147 211 117 40
BRI0: B-Channel 1: I IPCP CONFREQ id C (10) Type3 (6) 147 211 117 1
BRI0: B-Channel 1: O IPCP CONFACK id C (10) Type3 (6) 147 211 117 1
BRI0: B-Channel 1: I IPCP CONFACK id D (10) Type3 (6) 147 211 117 40
```

La commande `show interface bri 0 1` permet de connaître l'état du protocole NCP. Le résultat suivant indique que l'état de IPCP est ouvert. OSICP et XNSCP ne sont pas négociés, car aucune tentative n'a été entreprise. IPXCP se trouve dans un état de requête, c'est-à-dire qu'une négociation a été initiée sans succès, probablement parce que le numéro de réseau IPX de l'interface RNIS distante n'a pas été configuré.

```
Router # show interface bri 0 1
BRI0: B-Channel 1 is up, line protocol is up
Hardware is BRI
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
lcp state = OPEN
ncp ipcp state = OPEN
ncp osicp state = NOT NEGOTIATED
ncp ipxcp state = REQSENT
ncp xnscp state = NOT NEGOTIATED
```

A présent que les trois couches sont actives et fonctionnent normalement, vous devriez pouvoir exécuter un ping de l'adresse IP distante de l'interface RNIS. A ce stade, vous pouvez vous préoccuper des problèmes de routage. Si vous ne parvenez pas à réaliser un ping d'une adresse IP située au-delà de l'interface RNIS distante, le problème ne relève pas de la connectivité RNIS. Vérifiez que le trafic intéressant ainsi que le filtrage d'appel ont été définis correctement. N'attendez pas de recevoir votre première facture RNIS ! Utilisez les commandes IOS `show dialer`, `debug dialer`, et `show isdn history` afin de surveiller le trafic intéressant.

Résumé

La disponibilité croissante ainsi que la baisse des coûts font de RNIS une solution de choix pour de nombreuses applications de réseau. Les fonctions de Cisco IOS permettent l'élaboration de solutions RNIS étendues et souples. Le routage DDR est utilisé pour initier et terminer les connexions. Les profils virtuels peuvent être utilisés pour faciliter l'évolution en masse des solutions de réseau RNIS par commutation de circuits. Certaines précautions doivent toutefois être prises afin de garantir la maîtrise des coûts.

12

Conception de réseaux LAN commutés

Par Christophe Paggen

Ce chapitre décrit les trois technologies qui peuvent être utilisées par les concepteurs de réseaux dans la conception de réseaux LAN commutés :

- commutation LAN (Ethernet, Fast Ethernet et Gigabit Ethernet) ;
- réseaux LAN virtuels (VLAN) ;
- commutation ATM (LANE, MPOA).

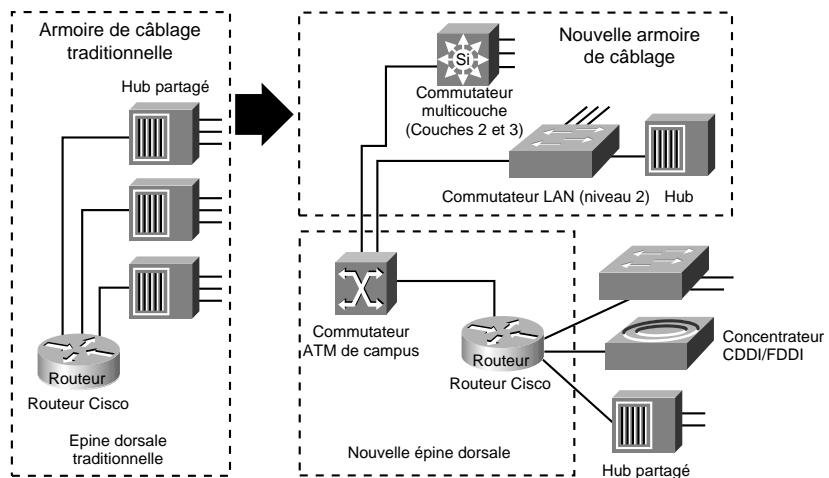
Les aspects pratiques de la conception de réseaux de campus évolutifs seront également abordés.

Evolution des réseaux partagés vers des réseaux commutés

Les technologies LAN sont en constante évolution, poussées par le besoin toujours grandissant de l'ordinateur de bureau en bande passante. On remarque aujourd'hui que les personnes qui travaillent dans ce domaine depuis à peine plus de deux années se réfèrent déjà au passé proche comme s'il s'agissait d'histoire ancienne. Il y a quelques années, l'objectif des réseaux LAN à forte capacité était de fournir un niveau de puissance globale élevé capable d'être partagée entre plusieurs équipements, supposition faite que toutes les stations n'aient pas besoin de cette puissance de façon continue. Toutefois, la bande passante totale était disponible selon un modèle de temps partagé pour quiconque devait communiquer. Les LAN partagés étaient très efficaces pour fournir des topologies logiques totalement maillées, sans avoir à supporter le coût de plusieurs centaines de connexions point-à-point. Un LAN partagé correctement conçu optimisait les chances de disponibilité

des canaux, c'est-à-dire que la capacité totale de transport devait être supérieure à l'ensemble des besoins des stations, en matière de communication. L'incroyable montée en puissance de l'ordinateur de bureau, dès la fin des années 80, a rendu obsolète un débit de 10 Mbit/s qui risquait de provoquer un goulet d'étranglement au niveau des transmissions. De plus, le nombre toujours croissant des équipements par segment a contribué à la généralisation de l'utilisation de la bande passante. Afin d'améliorer les performances de l'utilisateur, les administrateurs de réseaux commencèrent à segmenter les LAN partagés au moyen de ponts. Les ponts de réseaux locaux ont été disponibles à partir de 1984, mais leur capacité interne de pontage demeurait un frein, et il était rare qu'ils puissent exploiter la capacité totale du câblage sous-jacent. Avec les progrès accomplis dans le domaine des semi-conducteurs, courant 1990, on a assisté à l'émergence de circuits intégrés conçus sur mesure afin d'intégrer des fonctions spécifiques à certaines applications (ASIC, *Application-Specific Integrated Circuits*), ce qui a permis la fabrication de ponts LAN multiports capables de transmettre les trames à la vitesse du câble. Ces ponts ont été lancés sur le marché en tant que *commutateurs*. Les concepteurs de réseaux se sont ensuite empressés de remplacer, dans les armoires de câblage, les hubs existants par ces commutateurs (voir Figure 12.1).

Figure 12.1
Evolution des réseaux à médias partagés vers des réseaux commutés.



Cette stratégie a permis aux administrateurs de réseau de sauvegarder les investissements existants en matière de câblage, et d'accroître ainsi les performances de leur réseau, grâce à une bande passante dédiée pour chaque utilisateur. L'évolution des armoires de câblage coïncide avec une évolution analogue, au niveau de l'épine dorsale du réseau. Aujourd'hui, le rôle de Fast Ethernet, d'ATM (*Asynchronous Transfer Mode*) et, plus récemment, de Gigabit Ethernet, est en augmentation constante. Plusieurs protocoles ont été standardisés, tels que LANE (*LAN Emulation*), 802.1q/p, ainsi que 802.3z et 802.3ab (1000BaseTX). Les concepteurs de réseaux concentrent leurs réseaux fédérateurs de routeurs au moyen de commutateurs multicouches hautement performants, de routeurs de commutation et de commutateurs ATM, afin de fournir la bande passante supplémentaire requise par les services de données à fort débit.

Technologies de conception de réseaux LAN commutés

Avec l'avènement de technologies telles que la commutation de niveau 2, la commutation de niveaux 3 et 4 et les réseaux VLAN, la construction de réseaux locaux de campus devient plus complexe. Aujourd'hui, les quatre technologies suivantes sont nécessaires pour élaborer avec succès des réseaux de campus :

- Technologies de commutation LAN.

La commutation Ethernet, Fast Ethernet et Gigabit Ethernet est une commutation de niveau 2 qui assure la segmentation du réseau en domaines de broadcast, au moyen de réseaux VLAN. Elle représente la structure de base du réseau. La commutation Token Ring offre les mêmes fonctionnalités que la commutation Ethernet, mais utilise une technologie d'accès par anneau à jeton à 16 Mbit/s. Vous pouvez utiliser un commutateur Token Ring en tant que pont transparent ou pont à routage à l'aide de la source (SRB, *Source Routing Bridge*). Le média Ethernet est aujourd'hui plus connu que Token Ring, et est plus volontiers mis en œuvre que la technologie de bus.

- Agrégation de liens pour une bande passante accrue.

L'agrégation de liens Fast Ethernet individuels rend possible la création de canaux à 800 Mbit/s. Les interfaces Gigabit Ethernet peuvent également être regroupées pour offrir des canaux multi-gigabits qui concurrencent, voire surpassent, les vitesses le plus élevées fournies actuellement par les solutions ATM. Ces canaux sont traités par le commutateur comme étant un lien logique unique, ce qui autorise une intégration transparente avec le protocole d'arbre recouvrant (*Spanning Tree*).

- Technologies de commutation ATM.

La commutation ATM est une technologie de commutation ultrarapide pour la voix, la vidéo et les données. Des agrégats de bandes passantes atteignant des vitesses OC-48 (environ 2480 Mbit/s) émergent aujourd'hui, alors que les interfaces OC-12 (environ 620 Mbit/s) sont encore exploitées sur de nombreux réseaux. Le fonctionnement d'ATM est comparable aux technologies de commutation LAN en ce qui concerne le traitement des données.

- Technologies de routage.

Le routage est une technologie essentielle pour connecter des réseaux LAN dans un environnement de campus. Bon nombre de routeurs actuels sont capables d'assurer un routage à la vitesse du câble, c'est pourquoi on les appelle souvent "routeurs de commutation de niveaux 3 et 4". La commutation de niveau 3 (ou 4) n'est rien de plus qu'un routage classique à vitesse hautement optimisée.

NOTE

Les réseaux LAN commutés sont fréquemment appelés réseaux LAN de campus.

Rôle de la commutation LAN sur les réseaux de campus

La plupart des concepteurs de réseaux ont intégré des équipements de commutation sur leurs réseaux existants de médias partagés afin d'atteindre les objectifs suivants :

- Augmenter la bande passante disponible pour chaque utilisateur, et réduire ainsi la congestion sur les réseaux de médias partagés. Des liaisons à 10-100 Mbit/s vers l'ordinateur de bureau sont aujourd'hui courantes. Certains constructeurs ont déjà commencé à fabriquer des cartes réseau (NIC, *Network Interface Card*) Gigabit Ethernet.
- Exploiter la facilité de gestion des réseaux VLAN en même temps que les caractéristiques de souplesse et d'évolutivité du routage. Ce qui, combiné avec l'utilisation de serveurs DHRP (*Dynamic Host Resolution Protocol*), permet de réduire le coût des déplacements, ajouts et modifications.
- Déployer des applications multimédias émergeantes sur différentes plates-formes et technologies de commutation, afin de les rendre disponibles pour une variété d'utilisateurs. Ce type d'applications fait une utilisation intensive du multicast IP. Le programme IP/TV en est un exemple.
- Assurer une évolution progressive vers des solutions de commutation hautement performantes, telles que Gigabit Ethernet et ATM à haute vitesse.

La *segmentation* de réseaux LAN à média partagé divise les utilisateurs en deux segments séparés ou plus, ce qui réduit le nombre de ceux qui se partagent la bande passante. La commutation LAN qui repose sur cette tendance emploie la *microsegmentation*, qui fractionne encore davantage le LAN pour former des groupes d'utilisateurs encore plus réduits, jusqu'à finalement offrir un segment de LAN dédié par utilisateur. Chaque port de commutateur fournit un segment Ethernet dédié à 10-100-1000 Mbit/s ou un segment Token Ring dédié à 4-16 Mbit/s dans les environnements existants.

Les segments (ou VLAN) sont interconnectés au moyen d'équipements, en général des routeurs, qui rendent possible la communication entre des LAN, tout en bloquant les autres types de trafic. Les commutateurs possèdent l'intelligence nécessaire pour surveiller le trafic et élaborer des tables d'adressage basées sur les adresses MAC, ce qui leur permet de transmettre les paquets directement vers des ports spécifiques. La plupart du temps, les commutateurs offrent également un service non bloquant, qui permet plusieurs conversations (un trafic entre deux ports) simultanées. L'architecture d'un commutateur est dite non bloquante lorsque la bande passante de son circuit de commutation excède la bande passante totale de tous ses ports (c'est-à-dire un panneau arrière à 12 Gbit/s pour 96 ports à 10-100 Mbit/s).

La commutation est rapidement devenue la solution pour l'amélioration de la circulation du trafic LAN par excellence, pour les raisons suivantes :

- À la différence des hubs et des répéteurs, les commutateurs permettent à plusieurs flux de données de circuler simultanément (un commutateur est équivalent à plusieurs ponts à deux ports indépendants) et indépendamment.
- Grâce à la microsegmentation, les commutateurs ont la possibilité de supporter les exigences croissantes des technologies émergeantes en termes de vitesse et de bande passante (un VLAN est un domaine de broadcast).

- Les commutateurs fournissent une bande passante dédiée aux utilisateurs, au moyen de technologies commutées et de groupes commutés à haute densité Ethernet 10-100 Mbit/s sur fibre ou cuivre, Fast EtherChannel, Gigabit Ethernet, Gigabit EtherChannel et LANE ATM, ou MPOA (*Multiprotocol over ATM*).

Solutions de réseaux commutés

Pour être efficace, une solution de réseau commuté doit présenter les caractéristiques suivantes :

- Optimisation des investissements stratégiques dans l'infrastructure de communication existante, avec augmentation de la bande passante disponible (par exemple, réutilisation du plan de câblage existant).
- Réduction des coûts d'exploitation du réseau.
- Options pour le support d'applications multimédias, ainsi que d'autres types de trafic exigeants sur une variété de plates-formes (par exemple, surveillance IGMP). Cela implique le support des fonctionnalités de qualité de service (QoS) pour assurer le traitement préférentiel de certains modèles de trafic (par exemple, différenciation fondée sur la priorité IP ou la priorité 802.1q).
- Evolutivité, contrôle de trafic et sécurité à un niveau au moins équivalent, voire supérieur, à celui des réseaux actuels basés sur des routeurs (par exemple, filtrage de protocoles et sécurité de ports).
- Support de l'agent RMON (*Remote Monitoring*) imbriqué.

Pour atteindre ces objectifs, il faut comprendre le rôle de l'infrastructure logicielle de connexion au sein des réseaux commutés. Sur les réseaux actuels, les routeurs permettent l'interconnexion de technologies LAN et WAN disparates, tout en implémentant également des filtres de sécurité et des pare-feu logiciels. Ce sont ces capacités qui ont permis aux réseaux actuels d'évoluer de façon globale, tout en demeurant stables et robustes. Les routeurs limitent également la portée du trafic broadcast en le bloquant, sauf spécification contraire.

A mesure que les réseaux évoluent vers des réseaux commutés, des fonctionnalités analogues de connexion logique sont requises pour assurer la stabilité et l'évolutivité. Bien que les commutateurs LAN et ATM améliorent grandement les performances, ils représentent également de nouveaux défis de connexion pour les concepteurs. Les réseaux commutés doivent s'intégrer avec les réseaux LAN et WAN existants, mais aussi avec les futurs réseaux multiservices capables de transporter simultanément la voix et les données.

Par conséquent, un véritable réseau commuté n'est pas seulement un ensemble d'ordinateurs reliés, mais représente un système composé d'équipements intégrés, supportés par une infrastructure logicielle de connexion intelligente. Ce qui était auparavant centralisé au niveau des routeurs est maintenant devenu disponible au niveau des commutateurs LAN multicouches haut de gamme. Avec l'avènement des réseaux commutés, les fonctionnalités sont souvent distribuées à travers le réseau, reflétant ainsi la nature décentralisée des systèmes de commutation. Disposer d'une infrastructure de connexion demeure cependant une nécessité.

Composants du modèle de réseau commuté

Un réseau commuté englobe les trois composants de base suivants :

- des plates-formes de commutation physiques ;
- une infrastructure logicielle commune ;
- des outils et des applications d'administration de réseau.

Cisco apporte aux concepteurs une solution complète pour implémenter et gérer des réseaux commutés évolutifs et fiables.

Plates-formes de commutation évolutives

Le premier composant du modèle de réseau commuté est la plate-forme de commutation physique. Il peut s'agir d'un commutateur ATM, d'un commutateur LAN multicouche ou d'un routeur de commutation.

Commutateurs ATM

La famille de commutateurs ATM multiservices d'entreprise de Cisco Systems inclut des commutateurs ATM de moyenne gamme pour les groupes de travail et les épines dorsales de campus, les réseaux MAN, et les épines dorsales d'autres fournisseurs de services. Les performances de cette série de commutateurs s'étendent entre 5 et 40 Gbit/s. Ils fournissent des services optimisés pour les applications basées sur la commutation de cellules et de paquets, ce qui inclut le support de toutes les classes de trafic ATM, jusqu'aux fonctionnalités de commutation OC-48. A mesure que cette famille s'agrandit, les nouveaux produits peuvent tirer parti de l'ensemble des modules existants, à savoir les modules CAM (*Carrier Adapter Modules*) et PAM (*Port Adapter Modules*), des logiciels de commutation, ou encore utiliser des modules CAM et PAM spécialement conçus pour ces produits. Cette compatibilité en aval protège les investissements existants en équipement et logiciels, tout en facilitant l'évolution du réseau.

Pour les réseaux de campus, cette famille de produits inclut actuellement les commutateurs suivants :

- **LightStream 1010 (LS1010).** Commutateur ATM non bloquant, totalement modulaire à 5 Gbit/s, qui supporte une grande variété d'interfaces allant des vitesses T1/E1 jusqu'à OC-12c, à 622 Mbit/s.
- **Catalyst 8510 (Cat8510).** Commutateur L2/L3/ATM non bloquant, modulaire à 10 Gbit/s, qui atteint actuellement une vitesse OC-12c, ce qui assure un routage adapté au câble. Il supporte Fast Ethernet et Gigabit Ethernet.
- **Catalyst 8540 (Cat8540).** Commutateur L2/L3/ATM, modulaire à 40 Gbit/s, qui atteint actuellement une vitesse OC-12. Il supporte Fast Ethernet et Gigabit Ethernet, avec une redondance optionnelle du circuit de commutation et du processeur.

De la même manière qu'il existe des routeurs et des commutateurs LAN qui présentent des différences en termes de prix, de performances et de fonctionnalités, les commutateurs ATM peuvent être répartis dans les quatre catégories distinctes suivantes, qui reflètent les besoins d'applications et de marchés spécifiques :

- commutateurs ATM de groupe de travail ;
- commutateurs ATM de campus ;

- commutateurs ATM d'entreprise ;
- commutateurs ATM d'accès multiservices.

Commutateurs ATM de groupe de travail et de campus

Les *commutateurs ATM de groupe de travail* sont optimisés pour déployer ATM au niveau des ordinateurs de bureau, par l'intermédiaire d'interfaces ATM de faible coût, avec une interopérabilité de signalisation ATM pour les adaptateurs ATM, ainsi que le support de la qualité de service pour les applications multimédias.

Les *commutateurs ATM de campus* sont généralement utilisés sur les épines dorsales ATM à petite échelle (par exemple, pour relier des routeurs ATM ou des commutateurs LAN). Cet emploi des commutateurs ATM permet d'éviter la congestion sur les épines dorsales actuelles, tout en autorisant le déploiement de nouveaux services, tels que les réseaux VLAN. Les commutateurs de campus doivent supporter une grande variété de types d'épines dorsales locales et de réseaux étendus, mais doivent également être optimisés afin de représenter un bon rapport prix/performances en ce qui concerne la fonction d'épine dorsale locale. Dans cette catégorie de commutateurs, les capacités de routage ATM — qui permettent à plusieurs commutateurs d'être reliés —, ainsi que les mécanismes de contrôle de congestion — qui visent l'optimisation des performances d'épines dorsales — jouent un rôle très important.

Commutateurs ATM d'entreprise

Les commutateurs ATM d'entreprise sont des équipements multiservices sophistiqués, conçus pour former les épines dorsales centrales des grands réseaux d'entreprises. Ils viennent compléter le rôle que jouent les routeurs multiprotocoles haut de gamme actuels. Leur emploi est proche de celui des commutateurs ATM de campus, dans ce sens qu'ils sont utilisés pour interconnecter des commutateurs ATM de groupes de travail, ainsi que d'autres équipements reliés à ATM, tels les commutateurs LAN. Ils offrent des services de cellules et de trames, ainsi que des fonctionnalités avancées de qualité de service (QoS) et de routage dynamique. Ils peuvent non seulement agir en tant qu'épine dorsale ATM, mais également servir de points uniques d'intégration de tous les services et technologies disparates que l'on peut actuellement trouver sur les épines dorsales d'entreprises (voix, vidéo et données). La possibilité d'intégrer tous ces services sur une plate-forme et une infrastructure de transport ATM communes procure aux concepteurs de réseaux une plus grande souplesse d'administration, tout en éliminant le besoin de recourir à plusieurs réseaux superposés.

Commutateurs LAN

Un commutateur LAN est un équipement généralement doté de nombreux ports qui permettent de connecter des segments LAN (habituellement Ethernet 10-100 Mbit/s), ainsi que de plusieurs ports à haute vitesse (tels Fast Ethernet 100 Mbit/s, ATM OC-12/48 ou Gigabit Ethernet). Ces ports ultrarapides peuvent à leur tour relier le commutateur LAN à d'autres équipements du réseau. Il existe trois catégories principales de commutateurs LAN :

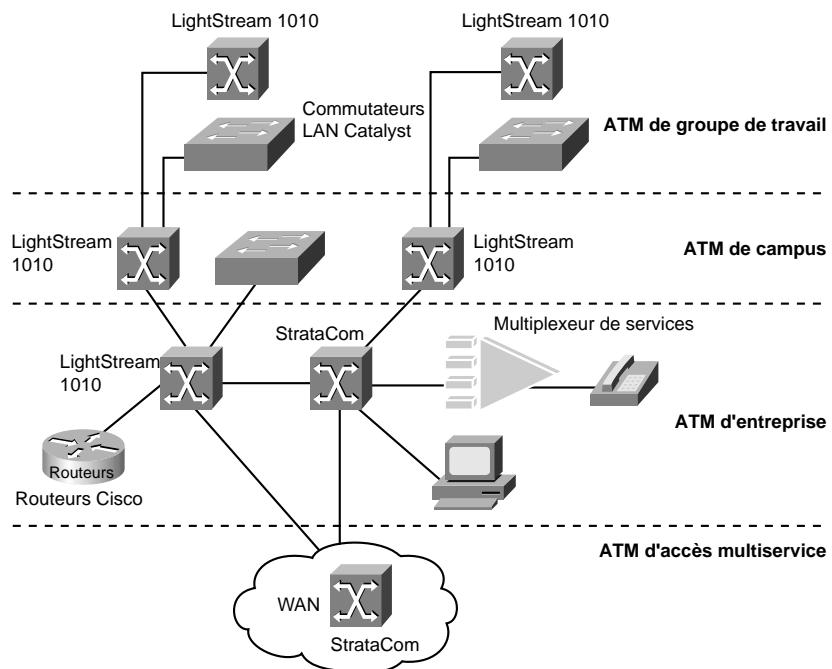
- **Commutateur d'armoire de câblage.** Equipment qui assure un accès pour les hôtes à la frontière du réseau (par exemple, les séries Catalyst 2900XL, Catalyst 4000, voire Catalyst 5x00).

- **Commutateur multicouche.** Equipement de niveaux 2, 3 ou 4 qui fournit différentes interfaces, de hautes densités de ports, ainsi qu'une grande variété de fonctions, qui le rendent adapté à la distribution des principales couches du réseau (par exemple, les séries Catalyst 5500 et 6000).
- **Routeur de commutation.** Equipement de niveaux 2, 3, ou 4 qui opère principalement au niveau de la couche centrale du réseau, ce qui assure une commutation multiservice à la vitesse du câble sur toutes ses interfaces (par exemple, la série Catalyst 8500).

Un commutateur LAN possède une bande passante dédiée par port, et chaque port représente un segment différent. Pour obtenir les meilleures performances possibles, les concepteurs assignent souvent un seul hôte par port, lui attribuant ainsi une bande passante dédiée de 10 Mbit/s, 100 Mbit/s, voire 1 Gbit/s (voir Figure 12.2), ou de 16 Mbit/s pour les réseaux Token Ring existants.

Figure 12.2

Exemple de configuration avec un commutateur LAN.



Lorsqu'un commutateur LAN démarre initialement, et à mesure que les différents équipements qui lui sont connectés demandent des services à d'autres équipements, il construit une table qui associe l'adresse MAC source de chaque équipement local au numéro de port sur lequel il s'est signalé. Ainsi, pour reprendre l'exemple de la Figure 12.2, lorsque l'hôte A situé sur le port 1 a besoin de communiquer avec l'hôte B situé sur le port 2, le commutateur transmet directement les trames du port 1 vers le port 2, ce qui épargne aux autres hôtes situés sur le port 3 de répondre aux trames qui ne leur sont pas destinées. Si l'hôte C a besoin d'envoyer des données vers l'hôte D, alors que l'hôte A envoie des données vers l'hôte B, cela reste possible, car le commutateur LAN peut transmettre des trames du port 3 vers le port 4 en même temps qu'il transmet les trames du port 1 vers le port 2.

Chaque fois qu'un équipement connecté au commutateur LAN envoie un paquet vers une adresse qui ne se trouve pas dans la table d'adressage du commutateur, ou un paquet broadcast ou multicast, le commutateur envoie le paquet sur tous ses ports, à l'exception de celui sur lequel il est arrivé. Cette technique est appelée *inondation (flooding)*. Plusieurs techniques existent qui permettent de restreindre l'inondation du trafic multicast à certains ports seulement, tels que le protocole CGMP (*Cisco Group Management Protocol*) et la surveillance IGMP (*Internet Group Management Protocol*) pour les commutateurs qui supportent des fonctions de commutation de niveau 3. Ces protocoles agissent sur les paquets multicast uniquement, non sur les paquets broadcast. Une autre fonctionnalité, appelée *suppression broadcast*, peut permettre de limiter les effets négatifs des tempêtes de broadcast.

Etant donné que les commutateurs LAN fonctionnent comme des ponts transparents traditionnels, ils éliminent les limites de groupes de travail ou de départements déjà définis. Un réseau construit et conçu uniquement avec des commutateurs LAN présente une topologie de réseau *linéaire*, qui ne comporte qu'un seul domaine de broadcast. Par conséquent, un tel réseau est susceptible de rencontrer les problèmes propres aux réseaux linéaires (ou *pontés*), c'est-à-dire qu'ils sont peu évolutifs. Notez cependant que les commutateurs LAN qui supportent des réseaux VLAN sont plus évolutifs que les ponts traditionnels. Le problème d'évolutivité dépend principalement d'un protocole très utile, rencontré sur la plupart des réseaux de niveau 2 redondants, à savoir le protocole d'arbre recouvrant (*Spanning Tree IEEE 802.1d*).

Commutateurs d'accès multiservices

Au-delà des réseaux privés, les plates-formes ATM sont également largement déployées par les fournisseurs de services, à la fois au niveau des équipements de télécommunication de clients et au sein de réseaux publics. Ce type d'implémentation est utilisée pour supporter plusieurs services MAN et WAN sur une infrastructure ATM commune, telle que la commutation Frame Relay, l'interconnexion de LAN ou les services publics ATM. Les commutateurs ATM d'entreprise sont souvent employés dans ces applications de réseaux publics en raison à la fois de leur haut degré de disponibilité et de redondance, et du nombre d'interfaces qu'ils peuvent gérer.

Plates-formes de routage

Outre les commutateurs LAN et ATM, les concepteurs emploient également des routeurs en tant que composants essentiels d'une infrastructure de réseau commuté. Alors que les commutateurs LAN sont ajoutés dans les armoires de câblage afin d'augmenter la bande passante et de réduire les niveaux de congestion sur les hubs de médias partagés existants, les technologies d'artère, telles que Gigabit Ethernet ou la commutation ATM, sont déployées sur les épines dorsales. Sur un réseau commuté, les plates-formes de routage permettent l'interconnexion de technologies LAN et WAN disparates, tout en implémentant également des filtres de broadcast et des systèmes de pare-feu logiques. De manière générale, si vous avez besoin de services de réseau avancés, tels que la protection par pare-feu contre les diffusions broadcast ou la communication entre des réseaux LAN dissemblables, les routeurs sont nécessaires. De plus, les routeurs de commutation jouent un rôle important sur les réseaux de campus actuels. Ils limitent l'étendue des VLAN et, plus particulièrement, l'étendue des domaines à arbre recouvrant. Avec la création de fermes de serveurs centralisées, les modèles de trafic requièrent maintenant l'utilisation de routeurs de commutation, qui opèrent à la vitesse du câble. Plusieurs techniques sont disponibles pour répondre à cette

demande, tels MLS (*Multilayer LAN Switching*), CEF (*Cisco Express Forwarding*) et MPOA (*Multiprotocol over ATM*). Les routeurs (ou routeurs de commutation, ou encore commutateurs multicouches) sont aujourd’hui essentiels pour assurer l’évolutivité des réseaux de campus. Les réseaux linéaires implémentés au moyen de VLAN de campus disparaissent avec l’affirmation de cette tendance.

Infrastructure logicielle commune

Le deuxième niveau du modèle de réseau commuté est une infrastructure logicielle commune. Sa fonction est d’unifier la diversité des plates-formes de commutation physique : commutateurs LAN multicouches, commutateurs ATM et routeurs multiprotocoles. Plus spécifiquement, l’infrastructure logicielle devrait permettre de réaliser les tâches suivantes :

- surveillance de la topologie logique du réseau ;
- routage et rerouting logique du trafic ;
- gestion et contrôle du trafic sensible ;
- fourniture de systèmes pare-feu, de passerelles, du filtrage et de la traduction de protocoles.

Cisco met à la disposition des concepteurs de réseaux le logiciel de commutation de Cisco IOS (*Internetwork Operating System*, système d’exploitation d’interréseau). Ce sous-ensemble du système Cisco IOS est optimisé pour la commutation, et représente l’élément unificateur pour la ligne de produits de commutation Cisco sur un réseau commuté. Le système Cisco IOS est exécuté sur des routeurs autonomes, des modules de routeurs pour hubs de médias partagés, des commutateurs multicouches, des commutateurs d’accès multiservices WAN, des commutateurs LAN, des commutateurs ATM et des autocommutateurs (PBX, *Private Branch eXchange*) compatibles ATM. Outre des niveaux optionnels de routage et de commutation sur un réseau commuté, il fournit de nouvelles fonctionnalités, telles que les tronçons VLAN, des services de gestion de réseaux ATM, la commutation multicouche à la vitesse du câble, des extensions pour supporter de nouvelles applications multimédias en réseau (multicast IP, etc.), des outils de gestion et d’analyse du trafic, ainsi que de nombreuses autres fonctionnalités.

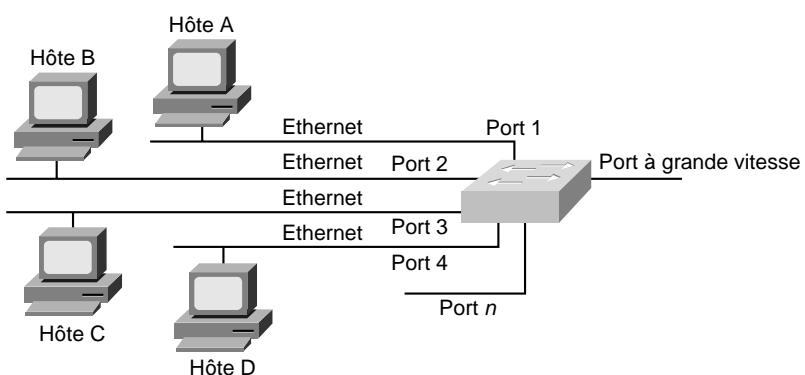
Réseaux VLAN

Un VLAN se compose généralement de plusieurs systèmes terminaux, des hôtes ou des équipements de réseau (tels que des commutateurs et des routeurs), qui sont tous membres d’un seul domaine logique de broadcast. Un VLAN n’est pas soumis à des contraintes de proximité physique pour le domaine de broadcast. Ce type de réseau est supporté sur divers équipements (par exemple des commutateurs LAN) capables de gérer des protocoles de tronçons VLAN entre eux. Chaque VLAN gère un arbre recouvrant distinct au moyen du protocole Spanning Tree (IEEE 802.1d), ce qui autorise diverses topologies logiques sur un seul réseau physique (c'est-à-dire, l'équilibrage de charge VLAN sur des tronçons de même coût, etc.). Il est fréquent d’implémenter des VLAN fondés sur un sous-réseau de protocole de niveau 3.

La première génération de VLAN s’appuie sur divers mécanismes de multiplexage, au niveau de la couche 2 du modèle OSI — tels que IEEE 802.10 pour les interfaces FDDI, LANE (*LAN Emulation*) sur les liaisons ATM, ISL (*Inter-Switch Link*, liaison intercommutateur), ou IEEE 802.1q sur Ethernet —, qui permettent la formation de groupes broadcast multiples, disjoints, et superposés sur

une seule infrastructure de réseau. Cela signifie qu'il est possible de supporter de nombreux VLAN sur une même interface physique, également appelée *tronçon* (*trunk*). La Figure 12.3 illustre un exemple de réseau LAN commuté, qui utilise des VLAN de campus (un concept qui a commencé à émerger en 1996). La couche 2 du modèle de référence OSI assure la transmission fiable de données à travers un lien physique. Elle est liée à l'adressage physique, à la topologie du réseau, à la gestion de l'accès au média, à la notification d'erreur, à la livraison ordonnée des trames et au contrôle de flux. L'IEEE a divisé cette couche en deux sous-couches, MAC et LLC, cette dernière étant parfois simplement appelée *couche de liaison*.

Figure 12.3
Topologie VLAN type.



A la Figure 12.3, un réseau Ethernet à 10-100 Mbit/s connecte les hôtes de chaque étage aux commutateurs A, B, C et D. Un réseau Fast Ethernet, ou Gigabit Ethernet, à 100 Mbit/s connecte ces commutateurs au commutateur E. Le VLAN 10 se compose des hôtes situés sur les ports 6 et 8 du commutateur A, et sur le port 2 du commutateur B. Le VLAN 20 se compose des hôtes qui se trouvent sur le port 1 du commutateur A, et sur les ports 1 et 3 du commutateur B.

Les VLAN peuvent servir à regrouper des utilisateurs qui présentent une caractéristique commune, indépendamment de leur connectivité physique. Ils peuvent être répartis sur un environnement de campus, ou même dispersés géographiquement.

Problèmes inhérents au protocole d'arbre recouvrant Spanning Tree

Bien que le déploiement de VLAN de campus était une pratique courante il y a quelques années, ce modèle de conception est rapidement devenu obsolète, principalement en raison de son manque d'évolutivité. Le problème d'évolutivité est en partie inhérent au protocole d'arbre recouvrant STP (*Spanning Tree Protocol*) utilisé pour éliminer les boucles logiques au niveau 2 du modèle OSI. Etant donné que l'en-tête de niveau 2 ne contient pas de champ de durée de vie (TTL, *Time To Live*), les paquets peuvent boucler indéfiniment sur le réseau. Contrairement à la croyance générale, les paquets broadcast ne sont pas les seuls à créer des boucles infinies ; une tempête unicast peut tout aussi bien se produire sur un réseau de couche 2. Même si STP permet d'éviter ces boucles, il impose une surcharge supplémentaire au niveau des ressources processeur des commutateurs. Lorsque les performances de ce protocole se dégradent, pour une raison quelconque (manque de

ressources CPU, par exemple), le réseau peut connaître des défaillances. Voici les caractéristiques d'un domaine de broadcast STP :

- Les liens redondants sont placés dans un état bloquant, et ne transportent aucun trafic.
- Des chemins non optimaux existent entre différents points.
- La convergence du protocole STP requiert en général 50 secondes ($2 \times \text{Forward Delay} + \text{Max Age} = (2 \times 15) + 20 = 50$; Forward Delay et Max Age sont deux temporiseurs utilisés par STP). Bien que les valeurs IEEE minimales autorisent une convergence aussi rapide que 14 secondes [$(2 \times 4) + 6$], il est tout à fait déconseillé d'appliquer ces valeurs sur la plupart des réseaux.
- Le trafic broadcast au sein du domaine de couche 2 déconnecte tous les hôtes.
- Les tempêtes de broadcast ou d'unicast au sein du domaine de couche 2 affectent le domaine dans son intégralité. Un problème local peut rapidement devenir général.
- L'identification des problèmes est une tâche laborieuse et longue.
- La sécurité de réseau assurée au niveau 2 du modèle OSI est limitée.

A l'aide d'un routeur, les hôtes d'un VLAN peuvent communiquer avec ceux d'un autre VLAN. Comparés à STP, les protocoles de routage présentent les caractéristiques suivantes :

- équilibrage de charge sur de nombreux chemins à coût identique (jusqu'à six chemins sur certaines plates-formes Cisco) ;
- chemins à coût optimal ou réduit entre les réseaux ;
- convergence plus rapide qu'avec STP, avec des protocoles intelligents (EIGRP, IS-IS et OSPF) ;
- informations d'accessibilité résumées (et donc évolutives) ;
- identification des problèmes de niveau 3 plus aisée.

Outils et applications d'administration de réseau

La troisième et dernière composante du modèle de réseau commuté est l'ensemble des outils et des applications utilisés pour l'administration du réseau. Etant donné que la commutation est intégrée à travers l'ensemble du réseau, l'administration joue un rôle essentiel, à la fois au niveau du groupe de travail et au niveau de l'épine dorsale. La gestion d'un réseau basé sur des commutateurs nécessite une approche radicalement différente de celle utilisée pour un réseau local traditionnel fondé sur des hubs et des routeurs.

Lors de la conception d'un réseau commuté, les concepteurs doivent s'assurer qu'ils prennent bien en compte les applications d'administration nécessaires à la surveillance, à la configuration, à la planification et à l'analyse des équipements et des services. Cisco propose ce genre d'outils pour les réseaux commutés émergeants.

Conception de réseaux LAN commutés

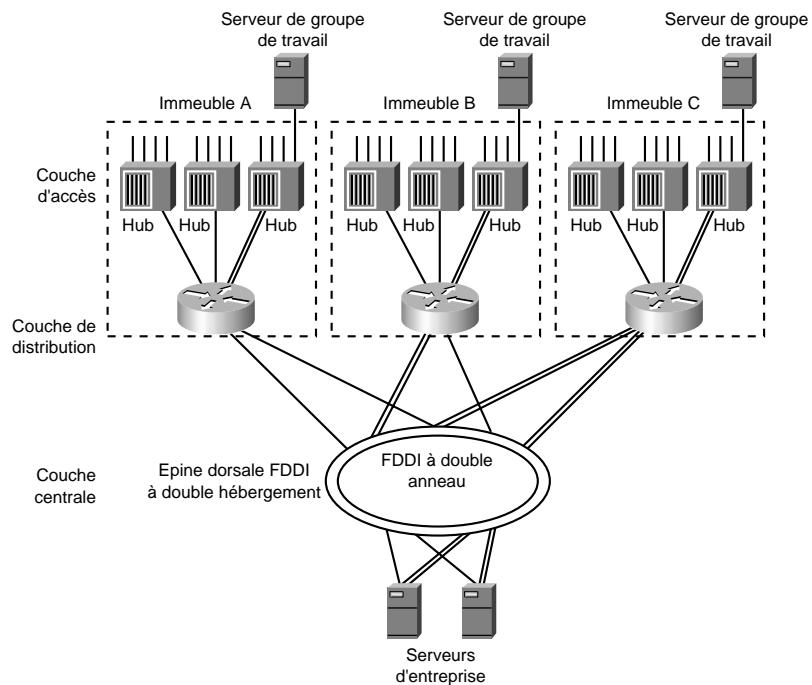
A présent que les différents composants des réseaux de campus commutés ont été introduits, nous allons examiner plusieurs approches de conception de ces réseaux. Les facteurs liés à l'évolutivité, ainsi qu'à la migration d'environnements existants vers des réseaux commutés hautement efficaces seront également abordés.

Modèle hub et routeur

La Figure 12.4 illustre un réseau de campus fondé sur une conception traditionnelle, avec hubs et routeurs. Les équipements de la couche d'accès sont des hubs qui agissent comme répéteurs de niveau 1. La couche de distribution est formée de routeurs. La couche centrale comprend des concentrateurs FDDI ainsi que d'autres hubs, qui agissent comme répéteurs de niveau 1. Les routeurs de la couche de distribution assurent un contrôle du trafic broadcast ainsi que la segmentation. Chaque hub d'armoire de câblage correspond à un réseau ou sous-réseau logique, et est connecté à un port de routeur. En tant qu'alternative, plusieurs hubs pourraient être implémentés en cascade, ou regroupés au moyen de ponts, afin de former un seul réseau ou sous-réseau logique.

Figure 12.4

Réseau de campus traditionnel, avec hubs et routeurs.



Le modèle avec hubs et routeurs est évolutif, grâce aux fonctionnalités de protocoles de routage intelligent, tels OSPF et EIGRP. La couche de distribution représente la ligne de démarcation entre la couche d'accès et la couche centrale.

Les routeurs de la couche de distribution assurent la segmentation, ainsi que la terminaison de domaines de collision et de domaines de broadcast. Le modèle est cohérent et déterministe, ce qui simplifie les tâches de dépannage et d'administration. Il s'adapte efficacement à tous les protocoles de réseau, tels que Novell IPX, AppleTalk, DECnet et TCP/IP.

Ce modèle est simple à configurer et à maintenir, en raison de sa modularité. Les routeurs de la couche de distribution sont tous configurés avec les mêmes fonctionnalités, et les éléments de configuration

courants peuvent simplement être copiés. Le comportement des routeurs est donc prévisible, ce qui facilite l'identification des problèmes.

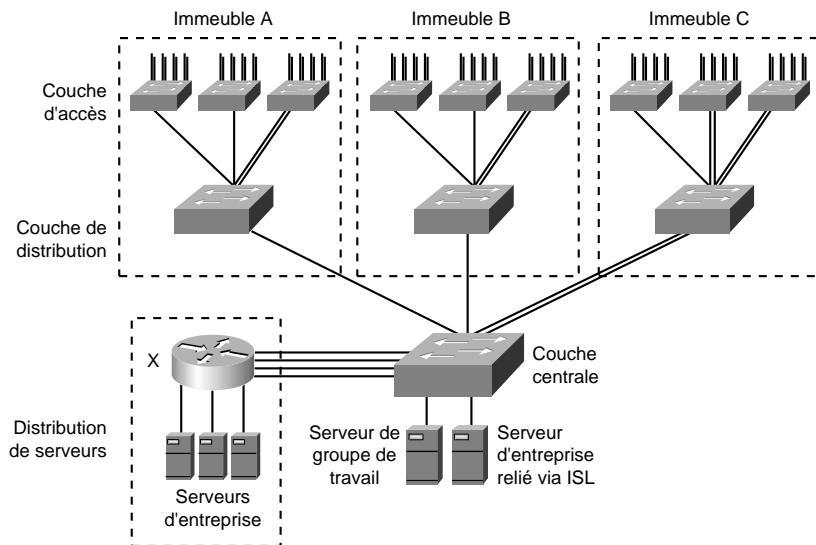
La charge de la commutation de paquets de niveau 3 et des services intermédiaires est répartie entre tous les routeurs.

La puissance de traitement d'un réseau fondé sur ce modèle peut évoluer, au fur et à mesure qu'augmentent les exigences en matière de performances. Le média partagé au niveau de la couche d'accès et de la couche centrale peut évoluer vers la commutation de niveau 2, et la couche de distribution peut évoluer vers la commutation de niveau 3, au moyen de commutateurs multicouches. La montée en puissance du média partagé (niveau 1) n'affecte pas la structure d'adressage du réseau, la conception logique ou la configuration des routeurs.

Modèle de VLAN de campus

La Figure 12.5 illustre une conception traditionnelle de VLAN de campus existant. La commutation de niveau 2 est mise en œuvre sur les couches centrale, de distribution et d'accès. Quatre groupes de travail sont distribués à travers plusieurs commutateurs de couche d'accès. La connectivité entre ces groupes de travail est réalisée au moyen du routeur X, qui est relié aux quatre VLAN. La commutation et les services de niveau 3 sont concentrés sur ce routeur. Les serveurs d'entreprise sont placés derrière le routeur sur différents réseaux logiques représentés par les lignes.

Figure 12.5
Conception de réseau
VLAN de campus.

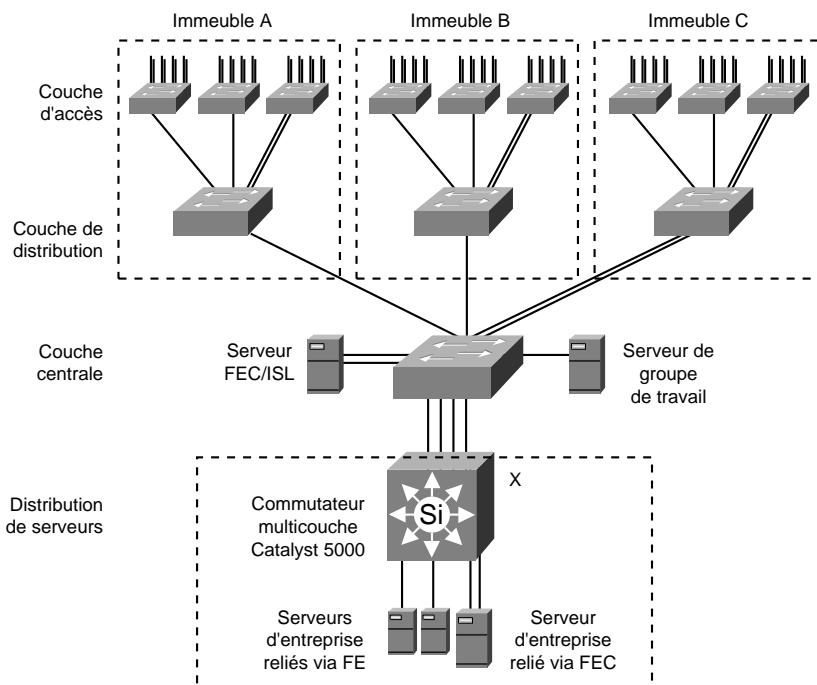


Les connexions de VLAN au routeur X pourraient être remplacées par un seul tronçon ISL. Dans les deux cas, le routeur X est désigné par le terme *routeur manchot* (*one-armed router*), du fait qu'il reçoit et transmet tout le trafic sur le même port. Davantage de routeurs pourraient être employés pour répartir la charge, auquel cas chacun d'eux serait relié à plusieurs, voire à tous les VLAN. Le

trafic entre les groupes de travail doit traverser le réseau à partir du VLAN source, vers un port du routeur passerelle, afin d'être redirigé vers le VLAN de destination.

La Figure 12.6 illustre une variante du modèle de VLAN de campus qui tire parti de la commutation multicouche. Le commutateur X fait partie de la série de commutateurs multicouches Catalyst 5000. Le routeur manchot est remplacé par un module RSM (*Route Switch Module*) et par la fonction de commutation matérielle de niveau 3 de la carte NetFlow Feature Card (NFFC). Les serveurs d'entreprise situés dans la ferme de serveurs pourraient être rattachés au moyen de Fast Ethernet (FE) à 100 Mbit/s, ou Fast EtherChannel (FEC), afin d'obtenir une bande passante duplex (FDX, *Full Duplex*) qui atteigne les 200 Mbit/s ou 400 Mbit/s.

Figure 12.6
Réseau VLAN de campus avec une commutation multicouche.



Le modèle de VLAN de campus est très dépendant de la règle des 80/20. Lorsque 80 % du trafic demeurent dans les limites d'un groupe de travail, 80 % des paquets sont commutés au niveau 2, entre le client et le serveur. Toutefois, si 90 % du trafic sont transmis aux serveurs d'entreprise dans la ferme de serveurs, 90 % des paquets sont commutés par le routeur manchot. L'adaptabilité des performances du modèle VLAN est limitée par les caractéristiques du protocole STP. Chaque VLAN équivaut à un réseau ponté linéaire.

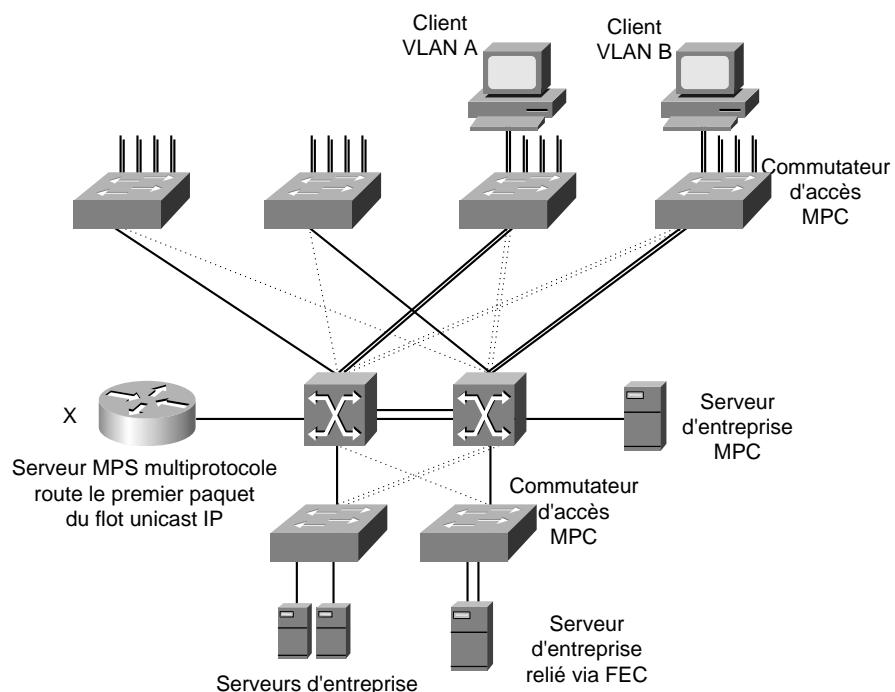
La souplesse de ce modèle autorise le déplacement de stations terminales configurées de façon statique vers un autre étage ou immeuble au sein du même campus, grâce au serveur VMPS (*VLAN Membership Policy Server*) de Cisco et au protocole VTP (*VLAN Trunking Protocol*). Par exemple,

un utilisateur mobile peut connecter un PC portatif à un port LAN situé dans un autre immeuble. Le commutateur local envoie une requête au serveur VMPS, afin de connaître les règles d'accès pour l'utilisateur, et de savoir à quel VLAN il appartient, puis ajoute le port de l'utilisateur au VLAN approprié.

MPOA (Mutliprotocol over ATM)

MPOA ajoute des fonctionnalités de commutation de niveau 3 sur un réseau LANE ATM. L'infrastructure ATM est identique à celle d'un réseau LANE ATM. Les LECS et LES/BUS de chaque ELAN sont configurés de la même manière. La Figure 12.7 présente les éléments d'une conception de petit réseau de campus avec MPOA.

Figure 12.7
Conception
de réseau de
campus avec
MPOA.



MPOA ajoute les éléments matériels et logiciels MPC (*MultiProtocol Client*, client multiprotocole) sur les commutateurs d'accès, ainsi que sur le serveur multiprotocole (MPS, *MultiProtocol Server*) qui est implémenté au niveau logiciel sur le routeur X. Lorsque le client du VLAN B communique avec un serveur d'entreprise situé dans la ferme de serveurs, le premier paquet est transmis par le client MPC sur le commutateur d'accès au serveur MPS, au moyen de LANE. Le serveur fait suivre le paquet vers le client MPC de destination, toujours en utilisant LANE, puis demande aux deux MPC d'établir une connexion SVC (*Switched Virtual Circuit*, circuit virtuel commuté) directe entre le sous-réseau A et le sous-réseau de la ferme de serveurs.

Avec MPOA, les paquets unicast IP empruntent le circuit virtuel commuté, tel que spécifié. En revanche, les paquets multicast sont envoyés au BUS, afin d'inonder le réseau ELAN d'origine. Ensuite, le routeur X reproduit le trafic multicast vers le BUS de chaque ELAN ayant besoin de le recevoir, tel que défini par le routage multicast. Puis, les BUS en question inondent chaque ELAN de destination avec le paquet.

Les paquets de protocoles autres que IP suivent toujours une logique d'itinéraire LANE-routeur-LANE, sans établir de circuit virtuel commuté. La conception de MPOA doit tenir compte de la quantité de trafic broadcast, multicast, et non IP, en rapport avec les performances du routeur. L'implémentation de MPOA devrait être envisagée sur les réseaux qui transportent principalement un trafic unicast IP, ainsi que sur les tronçons ATM reliés au commutateur d'armoire de câblage.

Modèle multicouche

Pour concevoir des réseaux de campus efficaces et évolutifs, il faut se représenter le réseau comme étant un grand puzzle modulaire, dans lequel de nouvelles pièces peuvent facilement être ajoutées (une pièce peut être un nouvel immeuble, un nouveau groupe d'utilisateurs ou une ferme de serveurs, par exemple). L'objectif du modèle multicouche est d'introduire les différentes couches dans cette représentation modulaire.

Nouvelle règle 80/20

La règle 80/20 traditionnelle est sous-jacente aux modèles de conception vus dans la section précédente. Avec le modèle de VLAN de campus, le groupe de travail logique est réparti à travers le réseau, mais demeure organisé de façon que 80 % du trafic soient maintenus dans les limites du VLAN. Les 20 % de trafic restants quittent le réseau ou sous-réseau par l'intermédiaire d'un routeur.

Cette règle est apparue, car chaque département ou groupe de travail disposait d'un serveur local sur le LAN. Ce serveur était exploité comme serveur de fichiers, d'ouverture de sessions et d'applications. La règle 80/20 a rapidement évolué, avec l'émergence des intranets et des applications d'entreprise qui s'appuient sur les services IP distribués. De nombreuses applications, nouvelles ou existantes, s'orientent vers le Web distribué pour le stockage et l'extraction de données. En conséquence, le modèle de trafic évolue maintenant vers une règle 20/80, c'est-à-dire que 20 % seulement du trafic sont réservés au groupe de travail LAN et que les 80 % restants quittent le réseau.

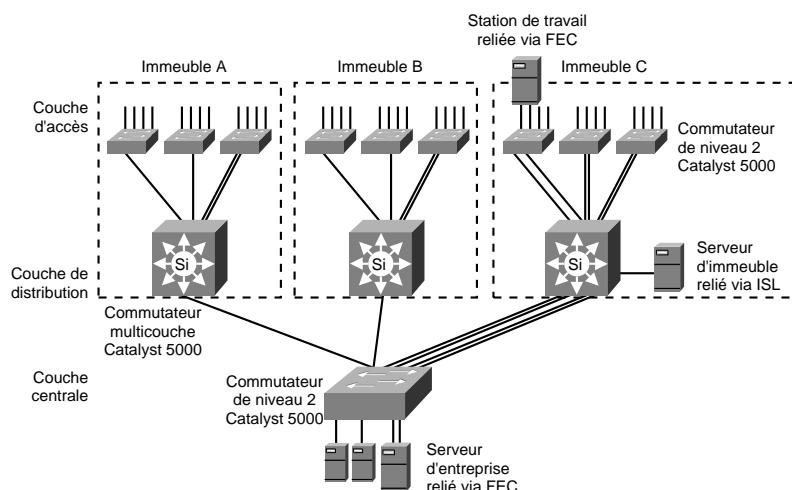
Composants du modèle multicouche

Les performances de la commutation multicouche répondent aux exigences de cette nouvelle règle de trafic 20/80. Les deux composants de la commutation multicouche sur la série Catalyst 5000 sont le module RSM et la carte NetFlow Feature Card. Le module RSM (*Route Switch Module*) est un routeur multiprotocole sur carte, fondé sur le système IOS de Cisco, qui présente des performances et des fonctionnalités semblables à celles du routeur Cisco 7500 RSP2. La carte NetFlow Feature Card (NFFC/NFFC-2) est une carte fille pour le moteur superviseur (*Supervisor Engine*), de la famille de commutateurs Catalyst 5000. Elle assure à la fois la commutation de niveau 3 pour IP, multicast IP ou IPX, et la commutation de niveau 2 au niveau matériel, grâce à des circuits intégrés spécialisés (ASIC). Il est important de noter que les performances qu'elle affiche pour la commutation de niveau 3 ne sont pas inférieures à celles obtenues pour la commutation de niveau 2.

Une alternative est la série 6000, plus puissante, ainsi que son module de commutation multicouche MSM (*Multilayer Switching Module*), qui se fonde sur le module SRP (*Switch Route Processor*) du Catalyst 8510, avec des performances qui atteignent les 6 millions de paquets par seconde pour IP et IPX. Pour encore plus de puissance, la carte MSFC (*Multiprotocol Switching Feature Card*), de la famille de Catalyst 6000, peut être utilisée afin d'obtenir des performances qui atteignent les 15 millions de paquets par seconde pour IP et IPX.

La Figure 12.8 illustre une conception de réseau de campus multicouche simple. Le réseau consiste en trois immeubles, A, B et C, reliés au moyen d'une épine dorsale (couche centrale). La couche de distribution est formée de commutateurs multicouches de la famille Catalyst 5000 ou 6000. Le modèle multicouche tire parti des performances et des fonctionnalités de commutation de niveau 2 offertes par cette série de commutateurs. Il permet également de préserver la conception ainsi que l'adressage logique du réseau existant, comme dans le modèle traditionnel avec hubs et routeurs. Les sous-réseaux de la couche d'accès se terminent au niveau de la couche de distribution, de même que les sous-réseaux d'épine dorsale. Par conséquent, le modèle multicouche ne consiste pas en des réseaux VLAN de campus, mais tire parti des tronçons VLAN, comme mentionné précédemment.

Figure 12.8
Conception de réseau de campus multicouche avec commutation multicouche.



La commutation de niveau 3 est employée au niveau de la couche de distribution du modèle multicouche ; c'est de là que proviennent bon nombre des avantages propres au routage. Cette couche représente une frontière qui empêche le trafic broadcast de circuler entre un immeuble et l'épine dorsale. Les fonctionnalités à valeur ajoutée du système Cisco IOS sont exploitées à ce niveau. La couche de distribution commute, par exemple, les informations en cache relatives aux serveurs Novell, et répond aux requêtes GNS (*Get Nearest Server*) de clients Novell, dans un immeuble. Les messages du protocole DHCP (*Dynamic Host Configuration Protocol*) envoyés par des stations IP mobiles à un serveur DHCP en sont un autre exemple.

Au niveau des commutateurs multicouches de la couche de distribution, le système Cisco IOS implémente une autre fonctionnalité, appelée LAM (*Local-Area Mobility*, mobilité locale). La

LAM est utile sur les intranets de campus qui n'ont pas déployé de services DHCP ; elle autorise des stations de travail configurées avec des passerelles et des adresses IP statiques à être déplacées sur tout le réseau. LAM fonctionne en propageant l'adresse des hôtes mobiles (route d'hôte ou 32 bits) vers la table de routage de niveau 3.

Il existe en fait des centaines de fonctionnalités Cisco IOS intéressantes qui permettent d'améliorer la stabilité, l'évolutivité et la gestion des réseaux d'entreprise. Elles s'appliquent à tous les protocoles que l'on peut rencontrer sur un réseau de campus, tels que DECnet, AppleTalk, IBM SNA, Novell IPX, TCP/IP, etc. Un facteur commun à ces fonctionnalités est qu'elles influent toutes sur l'ensemble du réseau, c'est-à-dire qu'elles sont globales. Elles s'opposent en cela à des caractéristiques telles que la densité de ports ou les performances de ports, qui concernent un seul équipement. Ces caractéristiques individuelles n'ont pas grand-chose à voir avec la stabilité, l'évolutivité et la facilité de gestion des réseaux d'entreprise.

Le principal atout du modèle multicouche vient de sa nature hiérarchique et modulaire. Il est hiérarchique, car les couches sont clairement définies et spécialisées. Il est modulaire, car tous les éléments d'une même couche exécutent les mêmes fonctions logiques. Le grand avantage d'une conception modulaire est qu'elle autorise le déploiement de différentes technologies, sans répercussion sur la structure logique du modèle. Par exemple, Token Ring peut être remplacé par Ethernet, FDDI par Fast Ethernet commuté, des hubs par des commutateurs de niveau 2, Fast Ethernet par LANE ATM, LANE ATM par Gigabit Ethernet, etc. Une telle modularité facilite la migration et l'intégration avec les technologies existantes.

Un autre avantage important de la conception modulaire est que tous les équipements d'une couche sont programmés de la même manière et exécutent les mêmes tâches, ce qui facilite grandement la configuration. Le dépannage en est également simplifié, car la conception d'ensemble est hautement déterministe en termes de performances, de détermination de chemin et de rétablissement à la suite de défaillances.

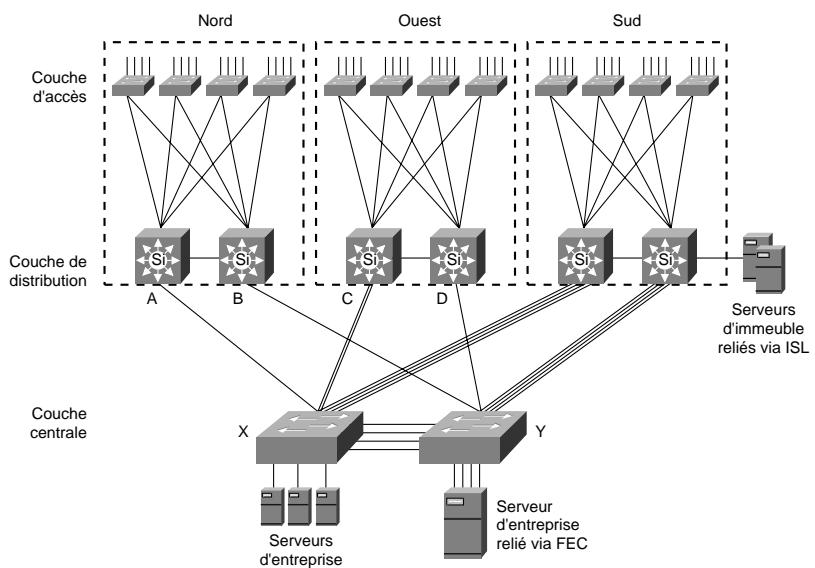
Au niveau de la couche d'accès, un sous-réseau correspond à un VLAN. Un VLAN peut être associé à un ou plusieurs commutateurs de niveau 2. Inversement, un ou plusieurs VLAN peuvent être configurés au niveau d'un seul commutateur de niveau 2. Si des commutateurs des séries Catalyst 4000, 5000 ou 6000 sont utilisés sur cette couche, les tronçons VLAN (ISL ou 802.1q) autorisent l'assignation souple de réseaux et de sous-réseaux sur plusieurs commutateurs. Plus loin dans ce chapitre, des exemples de configuration avec deux VLAN par commutateur illustrent l'utilisation de tronçons VLAN, afin d'implémenter l'équilibrage de charge et la récupération rapide après panne entre la couche de distribution et la couche d'accès.

Dans sa forme la plus simple, la couche centrale est un seul réseau logique, ou VLAN. Les exemples de ce chapitre présentent cette couche comme étant une simple infrastructure commutée de niveau 2, exempte de boucles. Il est préférable d'éviter les boucles d'arbre recouvrant au niveau de cette couche. La section suivante se concentre sur l'exploitation de l'équilibrage de charge et de la convergence rapide des protocoles de routage de niveau 3, tels que OSPF et EIGRP, pour gérer la détermination de chemin et le rétablissement après panne, sur l'épine dorsale. Par conséquent, ces fonctions sont gérées au niveau de la couche de distribution du modèle multicouche.

Redondance et équilibrage de charge

A la Figure 12.8, un commutateur de la couche de distribution représente un point de panne potentiel pour un immeuble. Un millier d'utilisateurs dans l'immeuble A, par exemple, pourraient perdre leur connexion avec l'épine dorsale dans le cas d'une panne de courant, ou dans le cas d'un lien défaillant entre un commutateur d'armoire de câblage et un commutateur de couche de distribution. La Figure 12.9 illustre une conception multicouche qui traite ce problème.

Figure 12.9
Conception de réseau de campus multicouche redondante.



La connectivité redondante des domaines nord, ouest et sud est assurée par des commutateurs de la couche de distribution. La redondance de l'épine dorsale est mise en œuvre avec l'installation de deux commutateurs Catalyst, ou plus, au niveau de la couche centrale. Les liens redondants qui partent de la couche de distribution vers la couche centrale assurent la reprise de fonction (*failover*), ainsi que l'équilibrage de charge sur plusieurs chemins, à travers l'épine dorsale.

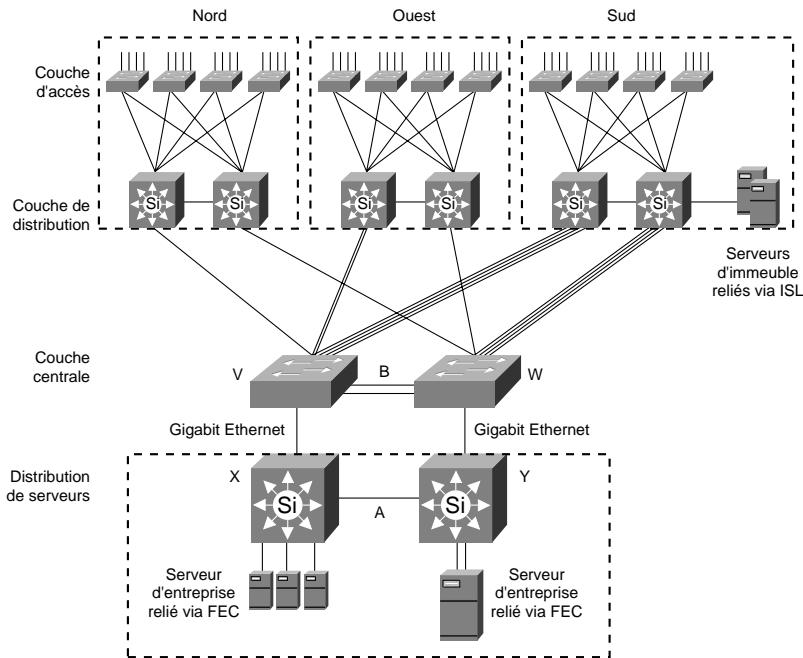
Des liens redondants connectent donc chaque commutateur de la couche d'accès à un couple de commutateurs Catalyst de la couche de distribution. Une reprise de fonction rapide au niveau 3 est possible grâce au protocole HSRP (*Hot Standby Router Protocol*) de Cisco. Les deux commutateurs de couche de distribution d'un domaine donné coopèrent pour fournir des fonctions de routeur-passeur HSRP pour tous les hôtes IP de l'immeuble. Au niveau 2, c'est l'algorithme de convergence UplinkFast de Cisco qui assure la reprise de fonction de la liaison principale vers la liaison de secours, et ce en trois secondes environ.

L'équilibrage de charge à travers la couche centrale est gérée par des protocoles de routage intelligent de niveau 3, implémentés par le système Cisco IOS. Dans notre exemple, il existe quatre chemins de même coût entre tous les immeubles, pris deux par deux. Comme le montre la Figure 12.9, les quatre chemins entre le domaine nord et le domaine ouest sont AXC, AXYD, BYC et BYD.

et BYXC. Ces chemins de niveau 2 sont considérés comme étant de coût égal par les protocoles de routage de niveau 3. Notez que tous les chemins des domaines nord, ouest et sud vers l'épine dorsale comprennent un seul saut (*hop*). Le système Cisco IOS supporte l'équilibrage de charge sur un maximum de six chemins de coût identique pour IP (ce que ne permet actuellement pas la série de routeurs de commutation Catalyst 8500, qui supporte seulement deux chemins de même coût), et sur davantage de chemins pour d'autres protocoles.

La Figure 12.10 présente le modèle multicouche avec une ferme de serveurs d'entreprise. Cette ferme de serveurs est implémentée en tant que bloc de conception modulaire, au moyen de la commutation multicouche. Le tronçon Gigabit Ethernet A transporte le trafic entre les serveurs. Le tronçon Fast EtherChannel B transporte le trafic de l'épine dorsale. Tout le trafic interserveur est maintenu à l'extérieur de l'épine dorsale, ce qui présente des avantages à la fois en termes de sécurité et de performances. Les serveurs d'entreprise bénéficient d'une redondance HSRP rapide entre les commutateurs multicouches X et Y. La stratégie d'accès à la ferme de serveurs peut être contrôlée par des listes d'accès configurées sur ces commutateurs. Dans cette figure, les commutateurs de niveau 2 de couche centrale V et W sont séparés des commutateurs de distribution de serveurs, par souci de clarté. Normalement, sur un réseau de cette taille, V et W seraient regroupés avec X et Y.

Figure 12.10
Modèle multicouche,
avec une ferme de serveurs.

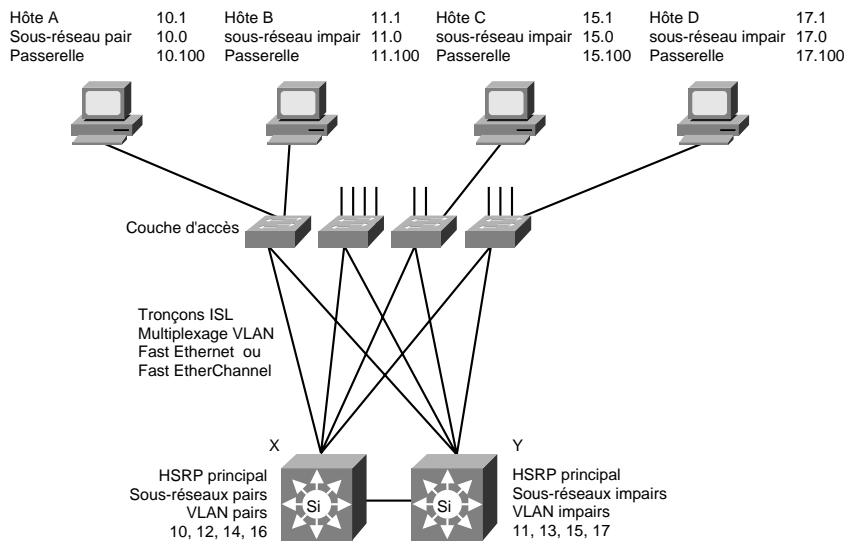


Le fait de regrouper des serveurs dans une ferme permet également d'éviter les problèmes liés à la redirection IP et de sélectionner le meilleur routeur-passerelle, lorsque les serveurs sont directement rattachés au sous-réseau d'épine dorsale (voir Figure 12.9). En effet, HSRP ne serait pas utilisé pour les serveurs d'entreprise illustrés dans cette figure. Ils emploieraient plutôt Proxy ARP

(Address Resolution Protocol), IRDP (Internet Router Discovery Protocol), GDP (Gateway Discovery Protocol) ou la surveillance RIP (Routing Information Protocol) afin de constituer leurs tables de routage.

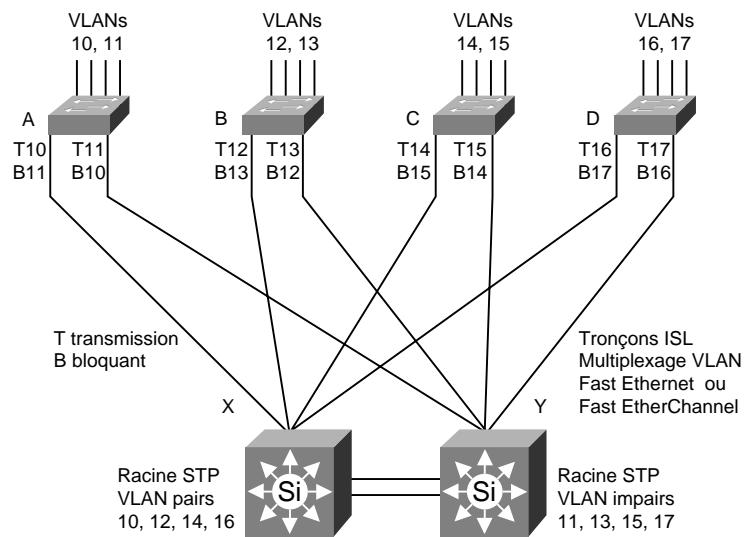
La Figure 12.11 illustre le fonctionnement de HSRP entre deux commutateurs de la couche de distribution. Les systèmes hôtes se connectent à un port de commutateur de couche d'accès. Les sous-réseaux à numéros pairs sont associés aux VLAN à numéros pairs, et les sous-réseaux à numéros impairs aux VLAN à numéros impairs. Le rôle de routeur-passerelle HSRP principal est assuré par le commutateur X pour les sous-réseaux pairs, et par le commutateur Y pour les sous-réseaux impairs. Le rôle de routeur-passerelle HSRP de secours est assuré par le commutateur Y pour les sous-réseaux pairs, et par le commutateur X pour les sous-réseaux impairs. La convention suivie ici est la suivante : chaque routeur-passerelle HSRP possède toujours une adresse d'hôte 100, c'est-à-dire que la passerelle HSRP pour le sous-réseau 15.0 est 15.100. Si la passerelle 15.100 n'est plus alimentée ou est déconnectée, le commutateur X endosse l'adresse 15.100, ainsi que l'adresse MAC HSRP, en deux secondes environ.

Figure 12.11
Redondance avec HSRP.



La Figure 12.12 illustre l'équilibrage de charge entre la couche d'accès et la couche de distribution, au moyen du protocole de tronçons VLAN ISL (ou IEEE 802.1q) de Cisco. Dans cet exemple, les VLAN 10 et 11 sont associés au commutateur A de la couche d'accès, et les VLAN 12 et 13 au commutateur B. Chaque commutateur de couche d'accès possède ainsi deux tronçons vers la couche de distribution. Le protocole d'arbre recouvrant STP place les liens redondants dans un état bloquant, tel qu'illusttré. La répartition de la charge est mise en œuvre en désignant un tronçon comme étant le chemin de transmission actif pour les VLAN pairs, et l'autre tronçon comme étant un chemin de transmission actif pour les VLAN impairs.

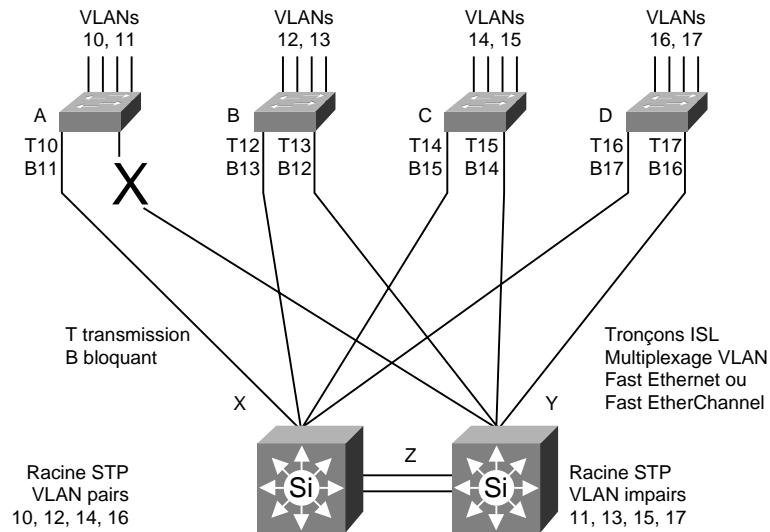
Figure 12.12
Tronçons VLAN pour l'équilibrage de charge.



Sur le commutateur A, le tronçon T10 est le chemin de transmission du VLAN 10, et le tronçon T11 celui du VLAN 11. Le tronçon B11 est le chemin bloquant du VLAN 11, et le tronçon B10 celui du VLAN 10. Pour accomplir cela, le commutateur X est configuré comme racine des VLAN pairs, et le commutateur Y comme racine des VLAN impairs.

La Figure 12.13 illustre la configuration de la Figure 12.12, après une défaillance de liaison, signifiée par la grande croix. L'algorithme UplinkFast fait en sorte que le tronçon T10 du commutateur A devienne le chemin de transmission actif du VLAN 11.

Figure 12.13
Tronçons VLAN avec reprise de fonction UplinkFast.



Le trafic est commuté sur le tronçon Fast EtherChannel Z, si nécessaire. Le tronçon Z est le chemin de secours de niveau 2 de tous les VLAN du domaine, mais transporte également le trafic en retour, qui est réparti entre les commutateurs X et Y. Avec STP, la convergence se ferait en 40 à 50 secondes. Avec UplinkFas, la reprise de fonction prend environ trois secondes.

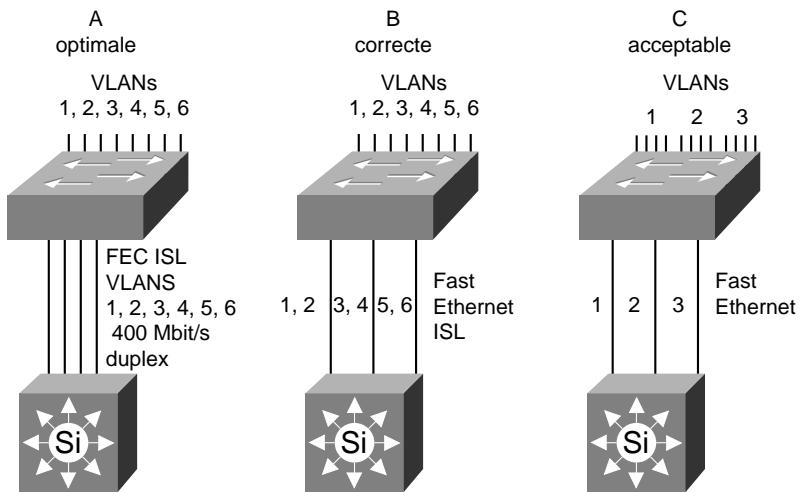
Augmentation de la bande passante

Dans le modèle multicouche, la capacité des tronçons Ethernet peut être accrue de différentes manières. Ethernet peut migrer vers Fast Ethernet, qui, à son tour, peut migrer vers Fast EtherChannel, Gigabit Ethernet ou Gigabit EtherChannel. Les commutateurs de couche d'accès peuvent gérer de nombreux VLAN qui comprennent de nombreux tronçons. Le multiplexage VLAN avec ISL (ou 802.1q) peut ainsi être mis en œuvre sur les différents tronçons.

Fast EtherChannel regroupe jusqu'à huit liaisons Fast Ethernet en un seul tronçon de haute capacité. Cette technologie est supportée par les familles de routeurs Cisco 7500 et 8500, et sur les séries de commutateurs Catalyst 4000, 5000 et 6000. Son support a été annoncé par plusieurs partenaires, parmi lesquels Adaptec, Auspex, Compaq, Hewlett-Packard, Intel, Sun Microsystems et Znyx. Grâce aux tronçons Fast EtherChannel, un serveur hautement performant peut être connecté à l'épine dorsale avec une bande passante de 400 Mbit/s, pour un débit total de 800 Mbit/s. Les routeurs Cisco haut de gamme supportent également Gigabit EtherChannel, et plusieurs fabricants ont annoncé des cartes réseau Gigabit.

La Figure 12.14 présente les trois méthodes qui permettent d'augmenter la bande passante entre un commutateur de couche d'accès et un commutateur de couche de distribution. Dans la configuration "A optimale", tous les VLAN sont regroupés sur Fast EtherChannel au moyen de ISL. La configuration "B correcte" combine la segmentation et des tronçons ISL. Enfin, la configuration "C acceptable" illustre une segmentation simple.

Figure 12.14
Augmentation de la bande passante de tronçons Ethernet.



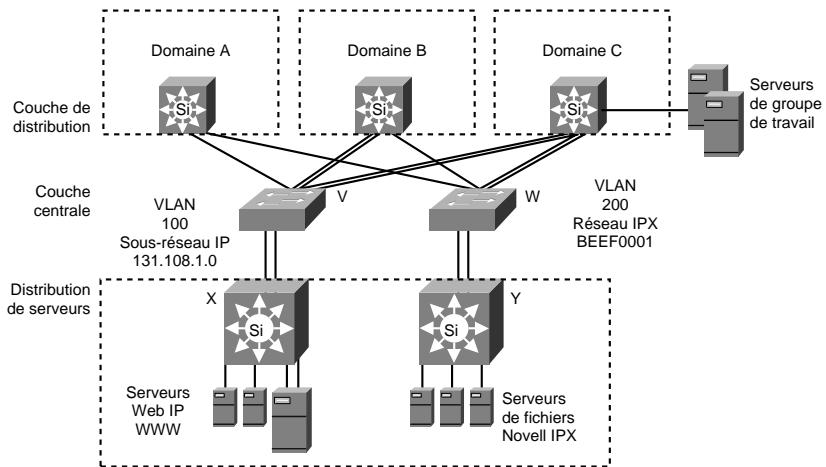
Il est conseillé d'implémenter la configuration A lorsque cela est possible, car Fast EtherChannel permet une exploitation plus efficace de la bande passante, en multiplexant le trafic de plusieurs VLAN sur un seul tronçon. Si vous ne disposez pas d'une carte de ligne Fast EtherChannel, choisissez la configuration B. Si ni Fast EtherChannel, ni les tronçons ISL ne sont envisageables, utilisez la configuration C. Dans le cas d'une segmentation simple, chaque VLAN utilise un seul tronçon, ce qui signifie qu'un tronçon peut être congestionné alors qu'un autre reste inexploité. De plus, davantage de ports sont nécessaires pour obtenir des performances équivalentes aux deux premières configurations. L'augmentation de la bande passante des épines dorsales ATM se fait par l'ajout de tronçons OC-3, OC-12 ou OC-48. Le routage intelligent fourni par le protocole PNNI (*Private Network-to-Network Interface*) gère l'équilibrage de charge et la reprise rapide de fonction.

Organisation de la couche centrale

Grâce à la commutation de niveau 3 sur la couche de distribution, il est possible d'implémenter l'épine dorsale en tant qu'unique ou que multiples réseaux logiques, selon les besoins. La technologie VLAN peut permettre de créer des réseaux logiques séparés, qui peuvent être exploités à des fins différentes. Un VLAN de couche centrale pourrait être créé pour le trafic de gestion, et un autre pour les serveurs d'entreprise. Une stratégie différente pourrait être appliquée à chaque VLAN, au moyen de listes d'accès au niveau de la couche de distribution. De cette manière, l'accès au trafic de gestion et aux ports des équipements de réseau est strictement contrôlé.

Il existe un autre moyen de partitionner logiquement la couche centrale. Il s'agit de se fonder sur des protocoles. Vous pouvez, par exemple, créer un VLAN pour les serveurs d'entreprise IP, et un autre pour les serveurs d'entreprise IPX ou DECnet. Ce partitionnement logique peut être étendu jusqu'à devenir une séparation physique, réalisée au moyen de commutateurs de couche centrale, lorsque les stratégies de sécurité l'imposent. Dans la Figure 12.15, le VLAN 100 situé sur le commutateur V correspond au sous-réseau IP 131.108.1.0, auquel est relié la ferme de serveurs Web. Le VLAN 200 situé sur le commutateur W correspond au réseau IPX BEEF0001, auquel est rattaché la ferme de serveurs Novell.

Figure 12.15
Partitionnement physique de la couche centrale.



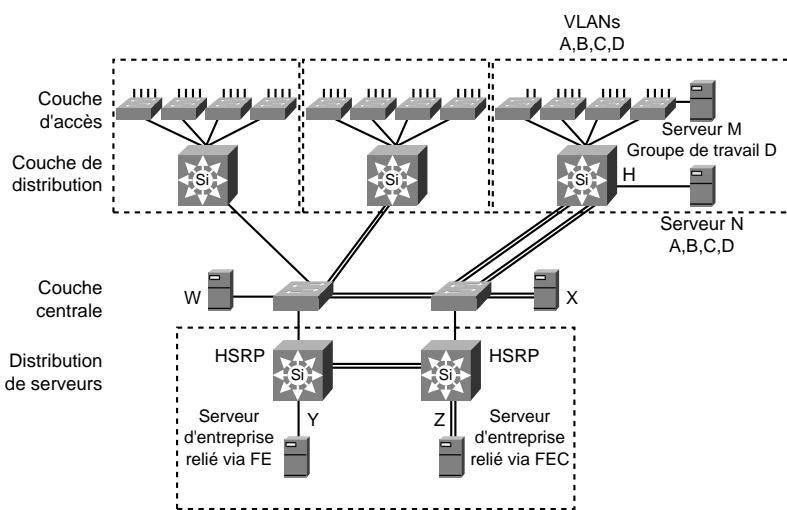
Bien entendu, il est préférable que la topologie de l'épine dorsale soit la plus simple possible. Un nombre limité de VLAN ou ELAN est conseillé. Les problèmes d'évolutivité relatifs à un grand nombre de commutateurs de niveau 3, reliés deux par deux à travers plusieurs réseaux, seront traités plus loin, à la section "Problèmes d'évolutivité".

Positionnement des serveurs

Les entreprises centralisent souvent leurs serveurs. Dans certaines situations, les services sont regroupés sur un seul serveur. Dans d'autres, les serveurs sont regroupés dans un centre de données, pour des raisons de sécurité physique ou de facilité d'administration. Dans un même temps, il est de plus en plus fréquent que des groupes de travail ou des individus publient en local leur page sur le Web et la rendent accessible pour l'entreprise tout entière.

Dans le cas de serveurs centralisés reliés directement à l'épine dorsale, tout le trafic client-serveur passe d'un sous-réseau de la couche d'accès à un sous-réseau de la couche centrale. Le contrôle stratégique de l'accès aux serveurs d'entreprise est implémenté au moyen de listes d'accès, qui sont appliquées au niveau de la couche de distribution. Dans la Figure 12.16, le serveur W est rattaché au sous-réseau central *via* Fast Ethernet, et le serveur X *via* Fast EtherChannel. Comme mentionné précédemment, les serveurs reliés directement à l'épine dorsale doivent utiliser Proxy ARP, IRDP, GDP ou la surveillance RIP pour élaborer leurs tables de routage. HSRP ne serait pas utilisé sur les sous-réseaux de couche centrale, car les commutateurs de la couche de distribution sont tous reliés à différentes parties du réseau de campus.

Figure 12.16
Connexion de serveurs
dans le modèle
multicouche.



Les serveurs d'entreprise Y et Z sont placés dans une ferme, en implantant la commutation multicouche sur les commutateurs de distribution de serveurs. Le serveur Y est relié par Fast Ethernet, et le serveur Z par Fast EtherChannel. Le moyen de contrôler l'accès à ces serveurs est implanté au moyen de listes d'accès situées sur les commutateurs de couche centrale. Un autre

avantage important de la distribution de serveurs est qu'elle permet l'utilisation de HSRP afin d'assurer la redondance avec reprise rapide de fonction. Elle permet également de maintenir le trafic interserveur en dehors de l'épine dorsale.

Le serveur M se trouve dans le groupe de travail D, qui correspond à un VLAN. Il est relié par l'intermédiaire de Fast Ethernet au port d'un commutateur de couche centrale, puisque la majorité du trafic vers ce serveur est interne au groupe de travail (règle 80/20). Ce serveur pourrait être dissimulé à l'entreprise, grâce à la configuration d'une liste d'accès au niveau du commutateur H de couche de distribution, si nécessaire.

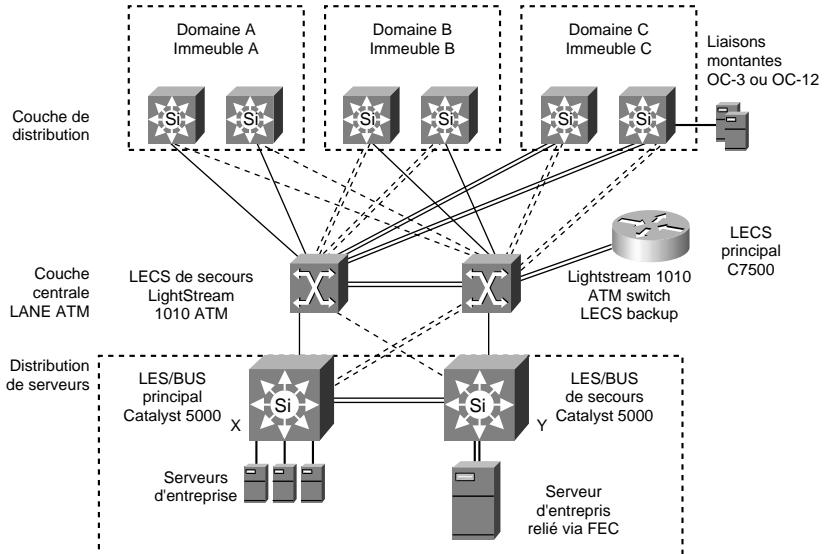
Le serveur N est relié au commutateur H. Il s'agit d'un serveur d'immeuble, qui communique avec les clients des VLAN A, B, C et D. Un chemin commuté direct de niveau 2 entre le serveur N et les clients des VLAN A, B, C et D peut être implanté de deux façons. A l'aide de quatre cartes réseau, le serveur peut être directement rattaché à chaque VLAN. A l'aide d'une carte réseau ISL, il peut communiquer directement avec les quatre VLAN, par l'intermédiaire d'un tronçon VLAN. A l'instar du serveur M, le serveur N peut également être dissimulé à l'entreprise, grâce à la configuration d'une liste d'accès au niveau du commutateur H, si nécessaire.

Epine dorsale LANE ATM

La Figure 12.17 illustre le modèle de campus multicouche avec une épine dorsale LANE ATM. Pour les clients qui requièrent une qualité de service (QoS) garantie, ATM est une solution efficace. Les applications relatives au transfert de la voix et de la vidéo en temps réel peuvent nécessiter des fonctionnalités ATM, telles que la gestion de files d'attente par flux, qui assure un contrôle granulaire du délai et de la gigue (*jitter*).

Figure 12.17

Modèle multicouche, avec couche centrale LANE ATM.



Tous les commutateurs multicouches Catalyst 5000 de la couche de distribution sont équipés d'une carte LANE, qui agit comme un client LEC, ce qui leur permet de communiquer à travers l'épine dorsale. Cette carte est dotée d'une interface physique ATM OC-3 ou OC-12 redondante, appelée Dual-PHY. Dans la Figure 12.17, les lignes pleines représentent des lignes actives ; celles en pointillés des lignes de secours dynamique (*hot standby*). Deux commutateurs LightStream 1010 forment la couche centrale ATM. Les routeurs et serveurs dotés d'interfaces ATM natives sont directement rattachés aux ports ATM de l'épine dorsale. Les serveurs d'entreprise situés dans la ferme de serveurs sont reliés par Fast Ethernet ou Fast EtherChannel aux commutateurs multicouches Catalyst 5000 X et Y. Ces derniers sont également équipés de cartes LANE, et agissent comme LECS pour connecter les serveurs d'entreprise basés Ethernet au réseau ELAN ATM de couche centrale.

Les commutateurs de couche centrale LightStream 1010 peuvent être reliés par des tronçons OC-3, OC-12 ou OC-48, selon les besoins. Lorsque davantage de puissance est nécessaire, ces commutateurs peuvent être remplacés par des routeurs multiservices Catalyst 8500. Le protocole PNNI gère l'équilibrage de charge ainsi que le routage intelligent entre les commutateurs ATM. Le routage intelligent est d'une importance capitale, au fur et à mesure que le nombre de commutateurs de couche centrale devient supérieur à deux. Le protocole STP n'est pas utilisé sur l'épine dorsale. Les protocoles de routage intelligent, tels OSPF et EIGRP, assurent la détermination de chemin ainsi que la répartition de la charge entre les commutateurs de la couche de distribution.

Cisco a implémenté le protocole SSRP (*Simple Server Redundancy Protocol*) afin d'assurer la redondance des LECS et LES/BUS. Ce protocole est disponible sur les routeurs Cisco 7500, sur la série de commutateurs Catalyst 5000, et sur les commutateurs ATM LightStream 1010. Il est compatible avec tous les LECS qui se conforment au standard LANE 1.0.

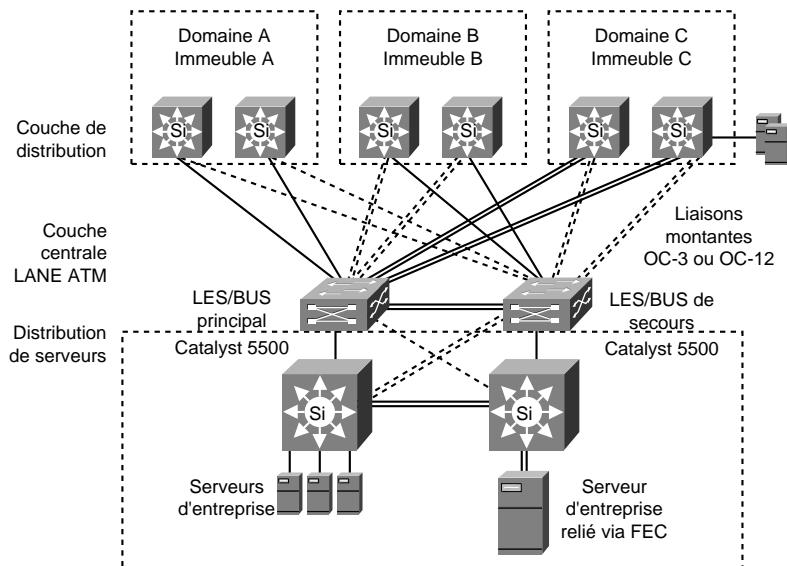
La carte LANE pour les commutateurs de la série Catalyst 5000 est un BUS efficace qui affiche des performances broadcast de 120 Kbit/s. Cette capacité suffit même aux réseaux de campus les plus grands. La Figure 12.17 présente le couple LES/BUS principal sur le commutateur X et celui de secours sur le commutateur Y. Sur un petit réseau de campus SSRP, la reprise de fonction LES/BUS requiert seulement quelques secondes, mais peut atteindre plusieurs minutes sur un très grand réseau. Pour cette raison, des épingles dorsales ELAN doubles sont souvent exploitées sur les grands réseaux de campus, afin d'offrir une convergence rapide en cas de défaillance LES/BUS.

Imaginez que deux ELAN, Rouge et Bleu, soient créés sur l'épine dorsale. Si le couple LES/BUS de l'ELAN Rouge est déconnecté, le trafic est rapidement rerouté vers l'ELAN Bleu, jusqu'au rétablissement de l'ELAN Rouge. Une fois ce dernier rétabli, les commutateurs multicouches de la couche de distribution y rétablissent la communication et réinitialisent l'équilibrage de charge sur les deux ELAN. Ce processus s'applique aux protocoles routés, mais non aux protocoles pontés.

La base de données des LECS principal et de secours est configurée sur les commutateurs ATM LightStream 1010, en raison de leur position centrale. Lorsque l'état du ELAN est stable, le LECS ne subit aucune surcharge processeur, puisqu'il est contacté uniquement lorsqu'un nouveau LEC rejoint l'ELAN. Par conséquent, les performances ne rentrent pas vraiment en ligne de compte lors du choix de l'emplacement des LECS principal et de secours. Une option intéressante pour un LECS principal serait de le placer sur un routeur Cisco 7500, avec une connexion ATM directe à l'épine dorsale, car il ne serait pas affecté par le trafic de signalisation ATM dans le cas d'une panne LES/BUS.

La Figure 12.18 présente une autre option d'implémentation de la couche centrale LANE qui utilise des commutateurs Catalyst 5500. Ici, le Catalyst 5500 agit en tant que commutateur ATM, suite à l'ajout d'une carte processeur ATM (ASP, *ATM Switch Processor Card*). De plus, il est configuré en tant que LEC au moyen d'une carte LANE/MPOA OC-12, et en tant que commutateur de trames Ethernet grâce à l'ajout de cartes de ligne Ethernet ou Fast Ethernet appropriées. La ferme de serveurs est implémentée au moyen de la commutation multicouche. Le Catalyst 5500 combine les fonctionnalités d'un LightStream 1010 et d'un Catalyst 5000 en un seul châssis. Grâce au module ATM FIM (*Fabric Integration Module*), il est également possible de combiner en un seul châssis les fonctionnalités du Catalyst 8510 SRP et celles du Catalyst 5500.

Figure 12.18
Couche centrale
LANE ATM, avec
des commutateurs
Catalyst 5500.



Multicast IP

Les applications fondées sur le multicast IP occupent une place de plus en plus importante sur les intranets d'entreprise. Des applications telles IPTV, Microsoft NetShow et NetMeeting sont en cours de déploiement. Plusieurs facteurs doivent être pris en compte afin de pouvoir gérer efficacement le trafic multicast :

- routage multicast : modes PIM (*Protocol-Indépendant Multicast*) dense, clairsemé ou clairsemé-dense ;
- les clients et les serveurs rejoignent des groupes multicast au moyen du protocole IGMP (*Internet Group Management Protocol*) ;
- élagage d'arbres multicast avec CGMP (*Cisco Group Multicast Protocol*) et surveillance IGMP ;
- performances multicast de routeurs et de commutateurs ;
- stratégie multicast.

Le protocole de routage multicast le plus utilisé est PIM (*Protocol-Independant Multicast*). Il est largement déployé sur l'Internet et sur les réseaux d'entreprise, et opère en collaboration avec de nombreux protocoles de routage, tels que OSPF et EIGRP. Les routeurs PIM sont parfois nécessaires pour pouvoir interagir avec DVMRP (*Distance Vector Multicast Routing Protocol*), qui est un protocole de routage multicast existant déployé sur les épines dorsales multicast d'Internet (MBONE, *Multicast backbone*). Actuellement, 50 % des épines dorsales multicast l'utilisent, et l'on s'attend à ce qu'il remplace un jour DVMRP.

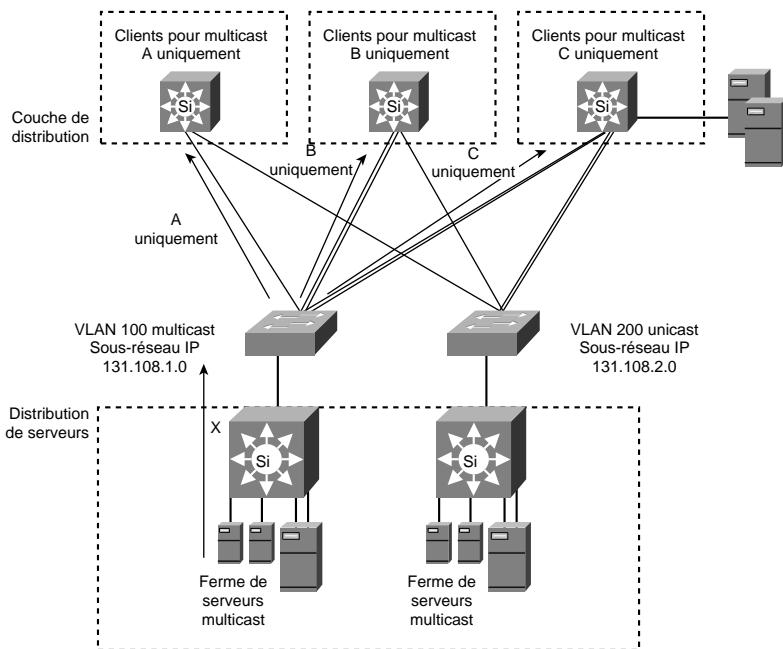
PIM peut être configuré en mode dense (*dense*), clairsemé (*sparse*), ou clairsemé-dense (*sparse-dense*). Le mode dense est utilisé par des applications comme IPTV, c'est-à-dire lorsque le réseau de campus comprend un seul serveur multicast et de nombreux clients. Le mode clairsemé est utilisé par les applications de groupe de travail, telles que NetMeeting. Dans les deux cas, PIM élabore des arbres multicast, afin de réduire la quantité de trafic qui circule sur le réseau, ce qui est particulièrement important pour les applications consommatrices en bande passante, comme la vidéo en temps réel. Mais, dans la plupart des environnements, PIM est configuré en mode clairsemé-dense, de façon que le choix du mode se fasse automatiquement, selon les besoins. C'est-à-dire que le choix du mode — dense ou clairsemé — est déterminé en fonction du mode utilisé par le groupe multicast.

IGMP est exploité par les clients et serveurs multicast afin de joindre ou d'annoncer des groupes multicast. Le routeur passerelle local transmet les diffusions multicast sur les sous-réseaux qui comprennent des écouteurs (*listener*) actifs, mais bloque le trafic dans le cas contraire. CGMP étend l'élagage (*prune*) multicast jusqu'au commutateur Catalyst. Un routeur Cisco envoie un message CGMP afin de fournir l'adresse MAC de tous les hôtes qui appartiennent à un groupe multicast. Lorsque les commutateurs Catalyst reçoivent le message CGMP, ils le transmettent uniquement aux ports dont l'adresse MAC se trouve dans leur table de transmission. Ce processus permet de bloquer les paquets multicast en provenance de ports de commutateurs auxquels ne correspond aucun membre de groupe en aval. En ce qui concerne les commutateurs de niveau 3, la surveillance IGMP représente une solution plus efficace que CGMP, car elle leur fournit suffisamment de fonctionnalités pour pouvoir analyser les paquets IGMP en provenance de clients et créer les entrées de table de transmission appropriées.

L'architecture des commutateurs Catalyst leur permet de transmettre les flux multicast sur un port, plusieurs ports ou tous les ports, sans que les performances en soient affectées. Ils peuvent gérer un ou plusieurs groupes multicast simultanément, à la vitesse du câble.

Comme illustré à la Figure 12.19, une façon d'implémenter une stratégie multicast est de regrouper les serveurs multicast dans une ferme placée derrière le commutateur Catalyst X. Ce dernier agit en tant que pare-feu multicast. Il veille au respect des limitations de débit et contrôle l'accès des sessions multicast. Pour isoler davantage le trafic multicast, vous pouvez créer un VLAN/sous-réseau multicast séparé, au niveau de la couche centrale. Le VLAN multicast peut être une partition logique des commutateurs de couche centrale existants, ou un commutateur dédié, si le trafic est très dense. Un point de rendez-vous (RP, *Rendezvous Point*), c'est-à-dire la racine d'un arbre multicast, peut être implémenté sur le commutateur X.

Figure 12.19
Pare-feu multicast et épine dorsale.



Problèmes d'évolutivité

Le modèle de conception multicouche est évolutif en soi. Les performances de la commutation de niveau 3 peuvent augmenter, car il s'agit d'une commutation distribuée. Les performances d'épine dorsale peuvent être optimisées par l'ajout de plusieurs liens entre les commutateurs. Les domaines de commutation ou immeubles individuels peuvent supporter jusqu'à 1 000 équipements clients avec deux commutateurs de couche de distribution, dans une configuration redondante classique. Davantage de groupes d'immeubles ou de serveurs peuvent être ajoutés sans qu'il soit nécessaire de modifier la conception. Etant donné que ce modèle est très structuré et déterministe, il est également évolutif en termes de gestion et d'administration.

Dans toutes les conceptions multicouches qui ont été présentées, les boucles ont été évitées sur l'épine dorsale, grâce à STP. Ce protocole requiert environ 40 à 50 secondes pour converger, et ne supporte pas l'équilibrage de charge sur plusieurs chemins. Sur les épingles dorsales Ethernet, aucune boucle n'est configurée ; sur les épingles dorsales ATM, PNNI gère la répartition de la charge. Dans tous les cas, les protocoles de routage intelligent de niveau 3, tels OSPF et EIGRP, assurent la détermination de chemin ainsi que l'équilibrage de charge sur de multiples liens au niveau de l'épine dorsale.

La surcharge associée à OSPF sur l'épine dorsale augmente avec le nombre de commutateurs de couche de distribution. Cela est dû au fait que ce protocole élit un routeur désigné et un routeur désigné de secours, chargés de gérer la plupart des tâches OSPF pour les autres commutateurs de niveau 3 de couche de distribution. Si deux VLAN ou ELAN sont créés sur l'épine dorsale, un routeur désigné et un routeur désigné de secours sont définis pour chacun. Par conséquent, le trafic

de routage OSPF et la surcharge processeur augmentent en même temps que le nombre de VLAN ou ELAN. C'est pourquoi, il vaut mieux limiter le nombre de ces réseaux sur une épine dorsale. En ce qui concerne les grandes épines dorsales LANE ATM, il est recommandé de créer deux ELAN (voir la section "Epine dorsale LANE ATM", plus haut dans ce chapitre).

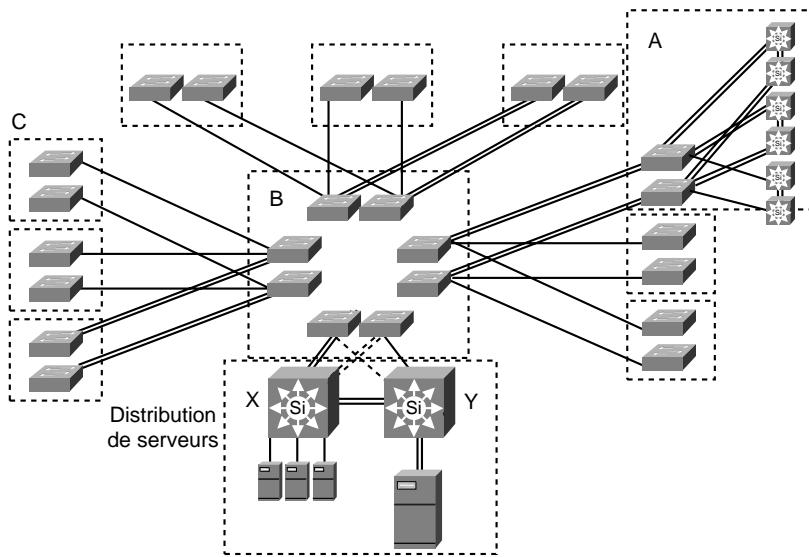
Une autre considération importante relative à l'évolutivité de OSPF est la synthèse de routage. Sur un grand réseau de campus, il est recommandé de configurer une zone OSPF par immeuble, et de configurer les commutateurs de la couche de distribution en tant que routeurs interzones (ABR, *Area Border Router*). La synthèse de routage est mise en œuvre en regroupant un bloc d'adresses de sous-réseaux contigus en une seule annonce au niveau du routeur interzones. Cela permet de réduire la quantité d'informations de routage qui circulent sur le réseau, et d'améliorer la stabilité de la table de routage. EIGRP peut être configuré de la même manière pour cette fonctionnalité.

La surcharge de certains protocoles, tels que AppleTalk RTMP (*Routing Table Maintenance Protocol*), Novell SAP et Novell RIP, augmente en même temps que le nombre d'homologues. Supposez que douze commutateurs de couche de distribution soient reliés à l'épine dorsale et exécutent Novell SAP. Si 100 services SAP sont annoncés sur le réseau de campus, chaque commutateur de cette couche injecte $100 : 7 = 15$ paquets SAP sur l'épine dorsale toutes les 60 secondes. Tous ces commutateurs reçoivent et traitent donc $12 \times 15 = 180$ paquets SAP à ce rythme. Le système Cisco IOS fournit des fonctionnalités comme le filtrage SAP, qui permet de bloquer les annonces SAP en provenance de serveurs locaux lorsque cela est nécessaire. Néanmoins, 180 paquets est un nombre raisonnable. Mais que dire de 100 commutateurs de couche de distribution qui annoncent 1 000 services SAP ?

La Figure 12.20 illustre la conception d'une grande épine dorsale ATM redondante et hiérarchique de campus. Le couche centrale ATM, désignée par la lettre B, consiste en huit commutateurs LightStream 1010, avec un maillage partiel de tronçons OC-12.

Figure 12.20

Epine dorsale ATM de campus redondante et hiérarchique.



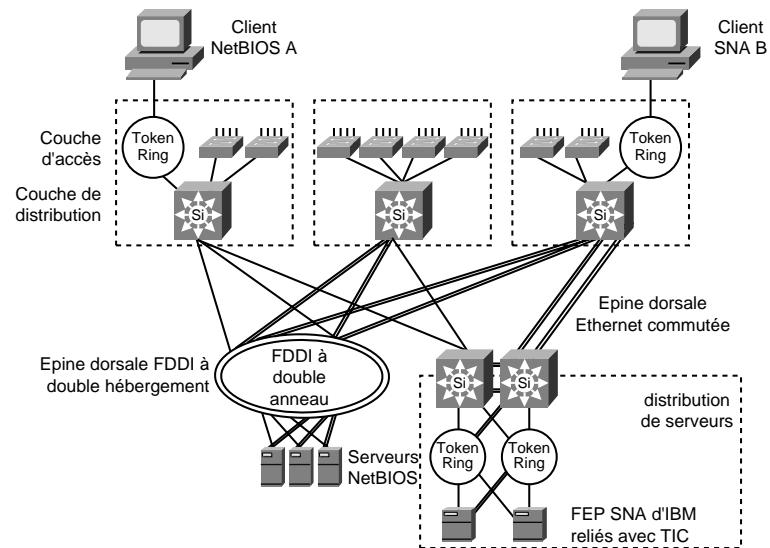
Le domaine C est formé de trois couples de commutateurs LightStream 1010, et peut être configuré avec un préfixe d'adresse ATM, résumé au niveau de sa connexion avec la couche centrale. Sur un réseau de cette échelle, la configuration manuelle de la synthèse de routage ne présente pas vraiment d'avantage. La synthèse par défaut implique un maximum de 26 entrées de routage, correspondant aux 26 commutateurs de la figure. Dans le domaine A, des couples de commutateurs de couche de distribution sont rattachés au circuit de commutation ATM avec LANE OC-3. Une ferme de serveurs située derrière les commutateurs Catalyst X et Y est directement reliée à la couche centrale, au moyen de cartes LANE/MPOA OC-12.

Stratégies de migration

Le modèle de conception multicouche décrit la structure logique du réseau de campus. L'adressage et la conception de niveau 3 sont indépendants du média. Les principes de conception logique sont les mêmes, qu'ils soient implantés à l'aide d'Ethernet, de Token Ring, de FDDI ou d'ATM. Ce qui n'est pas toujours le cas avec des protocoles pontés, tels que NetBIOS et SNA (*Systems Network Architecture*), qui dépendent du média. Par exemple, les applications Token Ring qui traitent des trames dont la taille dépasse les 1 500 octets autorisés par Ethernet méritent une attention particulière.

La Figure 12.21 présente un réseau de campus multicouche, avec une épine dorsale FDDI parallèle. Celle-ci pourrait être raccordée à l'épine dorsale Fast Ethernet commutée, grâce à la mise en œuvre d'un pontage avec traduction des trames (*translational bridging*) au niveau de la couche de distribution. Une autre solution serait de configurer l'épine dorsale FDDI en tant que réseau logique séparé. Plusieurs raisons justifient de conserver une épine dorsale FDDI existante. FDDI supporte des trames de 4 500 octets, alors que les trames Ethernet ne peuvent pas dépasser 1 500 octets. Cet aspect a son importance pour le trafic de protocoles pontés en provenance de systèmes terminaux Token Ring qui génèrent des trames de 4 500 octets. Il est également important pour les serveurs d'entreprise dotés de cartes d'interface FDDI.

Figure 12.21
Migration FDDI et
Token Ring.



DLSw+ (*Data Link Switching Plus*) est l'implémentation de Cisco du standard DLSw. Les trames SNA en provenance du client SNA B natif sont encapsulées dans TCP/IP par un routeur, ou un commutateur de couche de distribution dans le modèle multicouche. Un commutateur de couche de distribution désencapsule le trafic SNA vers un FEP (*Front-End Processor*, processeur frontal) relié à Token Ring dans le centre de données. Les commutateurs multicouches peuvent être rattachés à Token Ring au moyen d'une carte VIP (*Versatile Interface Processor*) et d'un adaptateur de port (*Port Adapter*) Token Ring.

Sécurité dans le modèle multicouche

Les listes de contrôle d'accès sont supportées par la commutation multicouche, sans entraîner de dégradation des performances. Etant donné que tout le trafic transite par la couche de distribution, c'est l'endroit idéal pour implémenter une stratégie de sécurité fondée sur des listes de contrôle d'accès. Celles-ci peuvent également être utilisées dans le cadre de la sécurité globale du réseau afin de limiter l'accès aux commutateurs eux-mêmes. De plus, les protocoles TACACS+ et RADIUS assurent un contrôle centralisé de l'accès aux commutateurs. Le système Cisco IOS fournit également plusieurs niveaux d'autorisation avec cryptage des mots de passe. Les responsables de réseaux peuvent se voir assigner un niveau de permissions particulier qui leur donne accès à des ensembles de commandes spécifiques.

L'implémentation de la commutation de niveau 2 sur la couche d'accès et sur la ferme de serveurs présente des avantages immédiats en matière de sécurité. Sur un média partagé, tous les paquets sont visibles par tous les utilisateurs du réseau logique. Un utilisateur a ainsi la possibilité de visualiser des mots de passe ou des fichiers en clair. Sur un réseau commuté, les conversations sont accessibles uniquement à l'émetteur et au récepteur ; avec une ferme de serveurs, tout le trafic inter-serviteur est maintenu en dehors de l'épine dorsale.

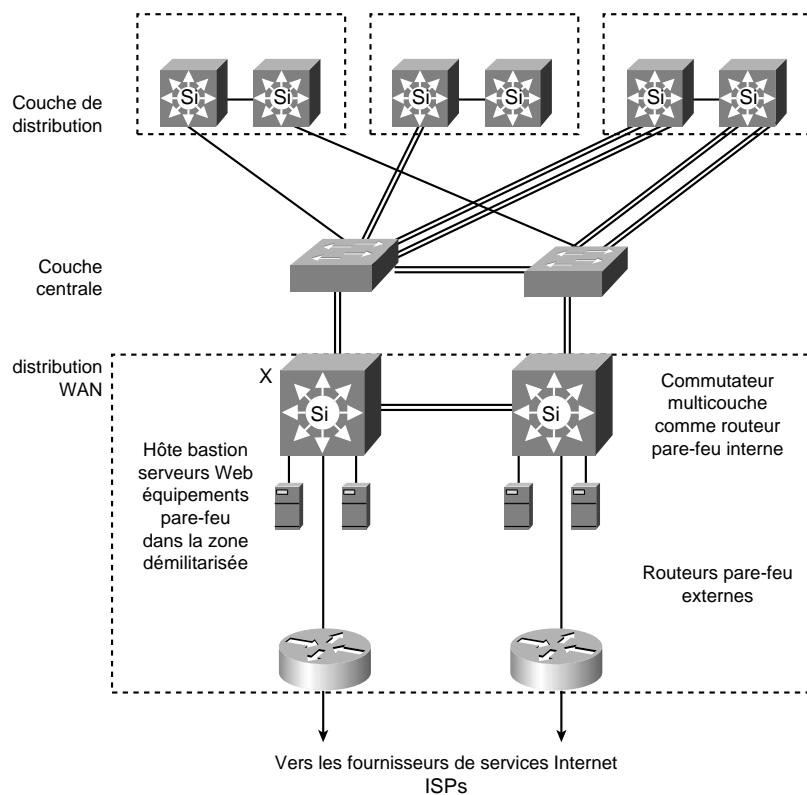
La sécurité WAN est implémentée au moyen de systèmes pare-feu. Un pare-feu est constitué d'un ou de plusieurs routeurs et de systèmes hôtes bastion placés sur un réseau spécial, appelé zone démilitarisée (DMZ, *Demilitarized Zone*). Des serveurs de caches Web ainsi que d'autres équipements pare-feu peuvent être reliés à la zone démilitarisée. Les routeurs pare-feu internes sont rattachés à l'épine dorsale de campus au niveau de ce que l'on pourrait appeler une couche de distribution WAN.

La Figure 12.22 illustre une conception avec couche de distribution WAN et des composants pare-feu.

Pontage dans le modèle multicouche

En ce qui concerne les protocoles non routés, le pontage est configuré. Le pontage entre les VLAN de la couche d'accès et l'épine dorsale est géré par le module RSM (*Route Switch Module*), le Catalyst 6000 MSM/MSFC ou le routeur de commutation 8500. Etant donné que tous les VLAN de couche d'accès utilisent le protocole d'arbre recouvrant STP IEEE, le module RSM ne devrait pas être configuré avec un groupe de pont (*bridge group*) IEEE. Le pontage IEEE a pour effet de regrouper tous les arbres recouvrants de tous les VLAN en un seul arbre, avec un seul pont racine. Configurez le module RSM avec un groupe de pont STP DEC afin de maintenir séparés tous les arbres recouvrants. Souvenez-vous que les commutateurs LAN exécutent uniquement le protocole STP IEEE. Il est recommandé d'utiliser une version récente du système IOS sur le module RSM (ou MSM, ou encore SRP) afin de permettre aux unités de données du protocole de pontage par arbre recouvrant (BPDU, *Bridge Protocol Data Units*) DEC de circuler entre les modules RSM jusqu'aux commutateurs Catalyst de couche 2, de façon transparente.

Figure 12.22
Distribution WAN vers l'Internet.



Avantages du modèle multicouche

Ce chapitre a présenté plusieurs variantes du modèle de conception multicouche. Qu'il soit implémenté avec des épines dorsales Ethernet à commutation de trames ou avec des épines dorsales ATM à commutation de cellules, il présente les mêmes avantages de base. Le modèle est hautement déterministe, ce qui facilite sa maintenance, au fur et à mesure qu'il évolue. L'approche modulaire facilite l'ajout de nouveaux immeubles ou de fermes de serveurs. Des protocoles de routage intelligent de niveau 3 gèrent l'équilibrage de charge et la convergence rapide sur l'épine dorsale. La structure et l'adressage logiques du modèle hubs et routeurs sont préservés, ce qui rend la migration plus aisée. De nombreux services à valeur ajoutée du système Cisco IOS, tels que les serveurs proxy, la mise en œuvre de tunnel et la synthèse de routage, sont implementés au moyen de listes d'accès, au niveau de la couche de distribution ou des commutateurs de distribution de serveurs.

La redondance et la convergence rapide sont assurées par des fonctionnalités, telles que UplinkFast et HSRP. La bande passante peut évoluer depuis Fast Ethernet vers Fast EtherChannel ou Gigabit Ethernet, sans qu'il soit nécessaire de modifier l'adressage ou les stratégies en place. Grâce aux fonctionnalités du système Cisco IOS, le modèle multicouche supporte tous les protocoles de campus courants, tels que TCP/IP, AppleTalk, Novell IPX, DECnet, IBM SNA, NetBIOS, etc. La plupart des intranets les plus étendus et les plus réussis s'appuient sur ce modèle. Il épargne tous les

problèmes d'évolutivité rencontrés avec des conceptions pontées ou commutées linéaires. Enfin, grâce à la commutation multicouche, il peut gérer la commutation de niveau 3 au niveau matériel, sans provoquer de dégradation de performances, à l'inverse de la commutation de niveau 2.

Résumé

Les conceptions de réseaux locaux de campus utilisent des commutateurs en remplacement des hubs traditionnels, et emploient une combinaison appropriée de routeurs afin de réduire la propagation des messages broadcast. Grâce aux composants logiciels et matériels appropriés en place et à une conception efficace, il est possible de construire des topologies semblables aux exemples décrits dans ce chapitre.

13

Protocole PIM Sparse Mode

Par Beau Williamson

Ce chapitre est extrait de l'ouvrage *Developing IP Multicast Networks, Volume I* paru (en langue anglaise) chez Cisco Press (ISBN : 1-57870-077-9).

Pour revoir les notions élémentaires du multicast IP, reportez-vous à l'Annexe I.

A l'instar du protocole PIM-DM (*Protocol Independent Multicast Dense Mode*), le protocole PIM-SM (*Protocol Independent Multicast Sparse Mode*) utilise la table de routage unicast pour exécuter la fonction de contrôle RPF (*Reverse Path Forwarding*, transmission sur chemin inverse) au lieu de maintenir une table de routage multicast séparée. Par conséquent, quels que soient les protocoles de routage unicast utilisés pour remplir la table de routage unicast (incluant les routes statiques), PIM-SM utilise ces informations pour assurer la transmission multicast. Il est donc indépendant du protocole.

Certaines des caractéristiques essentielles de PIM-SM sont les suivantes :

- indépendant du protocole (utilise la table de routage unicast pour le contrôle RPF) ;
- pas de protocole de routage multicast séparé — du type protocole de routage multicast par vecteur de distance (DVMRP, *Distance Vector Multicast Routing Protocol*) ;
- comportement d'adhésion explicite ;
- sans classe (à condition que le routage unicast sans classe soit mis en œuvre).

Ce chapitre présente les mécanismes fondamentaux utilisés par PIM-SM, qui sont les suivants :

- modèle d'adhésion explicite ;

- arbres partagés ;
- arbres de plus court chemin (SPT, *Shortest Path Tree*) ;
- enregistrement de source ;
- routeur désigné (DR, *Designated Router*) ;
- basculement SPT ;
- actualisation d'état (*State-Refresh*) ;
- découverte de point de rendez-vous (RP, *Rendez-vous Point*).

De plus, certains des mécanismes utilisés dans PIM-DM sont également exploités par PIM-SM, parmi lesquels :

- découverte de voisin PIM ;
- évaluations PIM.

Etant donné que ces mécanismes ne sont pas abordés ici, étudiez-les avant de procéder à la lecture de ce chapitre. Pour finir, ce chapitre se limite à la présentation du protocole PIM-SM, et donc à ses aspects élémentaires.

Modèle d'adhésion explicite

Comme son nom l'indique, PIM-SM se conforme au modèle de mode *sparse*, c'est-à-dire *clair-semé*, dans lequel le trafic multicast est envoyé uniquement vers les points du réseau qui en ont explicitement fait la demande. PIM-SM utilise pour cela des messages d'adhésion PIM (*Join*), qui sont transmis de saut en saut vers le nœud racine de l'arbre, c'est-à-dire vers le point de rendez-vous (RP) dans le cas d'un arbre partagé, ou bien vers le routeur de premier saut directement rattaché à la source multicast dans le cas d'un arbre de plus court chemin (SPT, *Shortest Path Tree*). A mesure qu'un message Join traverse l'arbre en remontant vers la racine, les routeurs qui se trouvent sur le chemin se placent dans un état de transmission de façon que le trafic multicast requis puisse être transmis vers le bas de l'arbre.

De la même manière, lorsque le trafic multicast n'est plus nécessaire, un routeur envoie un message d'élagage PIM (*Prune*) vers la racine de l'arbre pour stopper ce trafic. A mesure que ce message Prune traverse l'arbre de saut en saut, chaque routeur modifie son état de façon appropriée. Cette actualisation résulte souvent en une annulation de l'état de transmission associé à un groupe ou une source multicast.

Retenez que, dans le modèle d'adhésion explicite, les routeurs se placent dans un état de transmission en réponse aux messages Join. Cela diffère considérablement des protocoles par inondation et élagage (*flood-and-prune*) tels que PIM-DM, où l'activation de l'état de transmission est déclenchée par l'arrivée de données multicast.

Arbres partagés PIM-SM

PIM-SM se fonde sur un arbre partagé unique et unidirectionnel dont le nœud racine est appelé point de rendez-vous ou RP (*Rendez-vous Point*). Pour cette raison, ces arbres partagés sont parfois désignés par le terme arbres RP, ou encore RPT (*RP Tree*).

Les routeurs de dernier saut (c'est-à-dire ceux auxquels sont directement connectés des destinataires pour un groupe multicast) qui doivent recevoir le trafic de la part d'un groupe multicast spécifique se joignent à l'arbre partagé. Lorsqu'un routeur de dernier saut n'a plus besoin de recevoir le trafic d'un groupe multicast spécifique (c'est-à-dire lorsque plus aucun destinataire pour le groupe multicast n'est directement connecté au routeur), il s'exclut lui-même de l'arbre partagé.

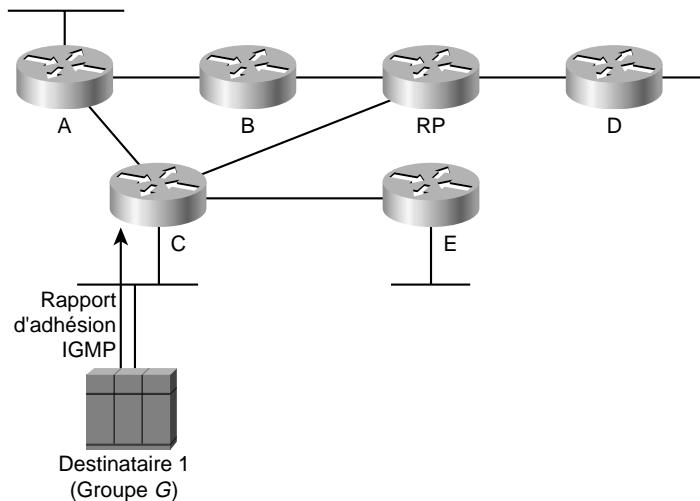
Etant donné que PIM-SM utilise un arbre partagé unidirectionnel sur lequel le trafic peut seulement circuler vers le bas de l'arbre, les sources multicast doivent s'enregistrer auprès du RP pour que leur trafic multicast puisse être transmis sur l'arbre (*via* le RP). Ce processus d'enregistrement déclenche l'envoi d'un message Join SPT par le RP vers la source lorsqu'il existe sur le réseau des destinataires actifs pour le groupe multicast. Ces messages Join SPT sont décrits plus en détail à la section "Arbres de plus court chemin PIM-SM" et le processus d'enregistrement est décrit à la section "Enregistrement de source multicast".

Adhésion à un arbre partagé

La Figure 13.1 illustre la première étape d'adhésion à un arbre partagé dans le cas d'une implémentation simple de PIM-SM. Dans cette étape, un seul hôte (Destinataire 1) rejoint le groupe multicast G *via* un rapport d'adhésion IGMP (*Internet Group Membership Protocol*).

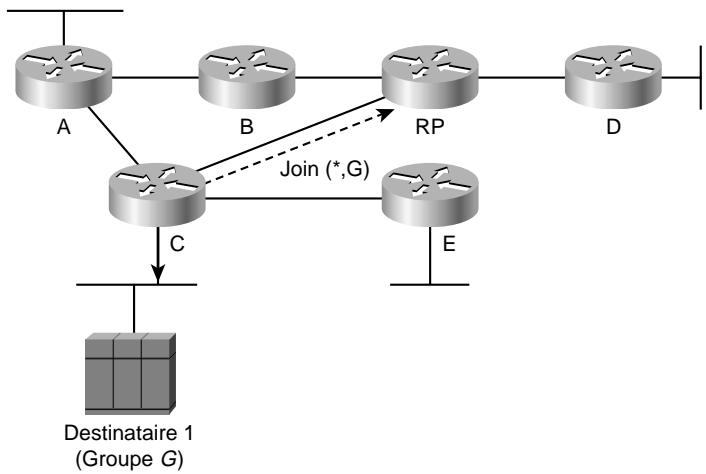
Figure 13.1

Adhésion à un arbre partagé PIM — Etape 1.



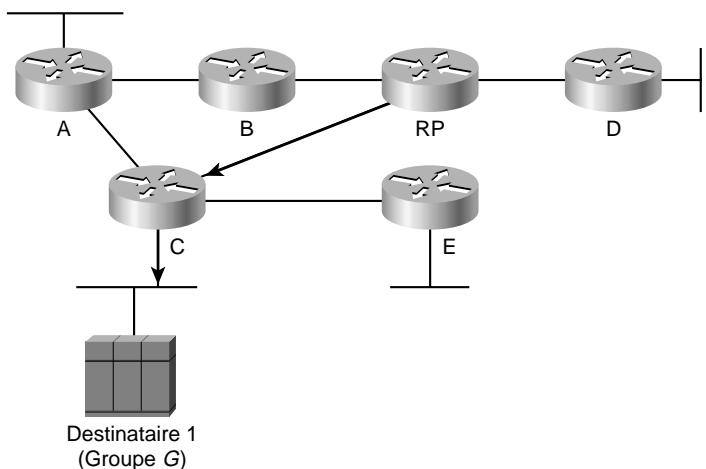
Comme le destinataire 1 est le premier hôte à rejoindre le groupe multicast dans l'exemple, le routeur C doit créer une entrée d'état $(*,G)$ dans sa table de routage multicast pour ce groupe multicast. Il place ensuite l'interface Ethernet dans la liste des interfaces sortantes de l'entrée $(*,G)$ (voir la flèche, Figure 13.1). Etant donné que le routeur C a dû créer une nouvelle entrée d'état $(*,G)$, il doit également envoyer au RP un message Join PIM $(*,G)$ (voir la flèche en pointillés, Figure 13.2), afin de rejoindre l'arbre partagé. Le routeur C s'appuie sur sa table de routage multicast pour déterminer l'interface à utiliser en direction du RP.

Figure 13.2
Adhésion à un arbre partagé PIM — Etape 2.



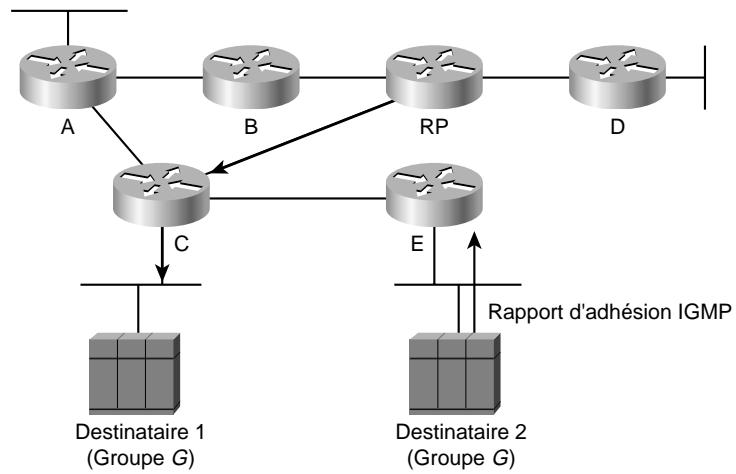
Le RP reçoit le message Join $(*,G)$, et comme il n'avait pas non plus d'entrée d'état pour le groupe multicast G , il crée une entrée d'état $(*,G)$ dans sa table de routage multicast et ajoute la route vers le routeur C dans sa liste d'interfaces sortantes. A ce stade, un arbre partagé pour le groupe multicast G a été construit entre le RP, le routeur C et le destinataire 1 (voir les flèches en gras, Figure 13.3). A présent, tout le trafic adressé au groupe multicast G qui atteint le RP peut circuler vers le bas de l'arbre partagé en direction du destinataire 1.

Figure 13.3
Adhésion à un arbre partagé — Etape 3.



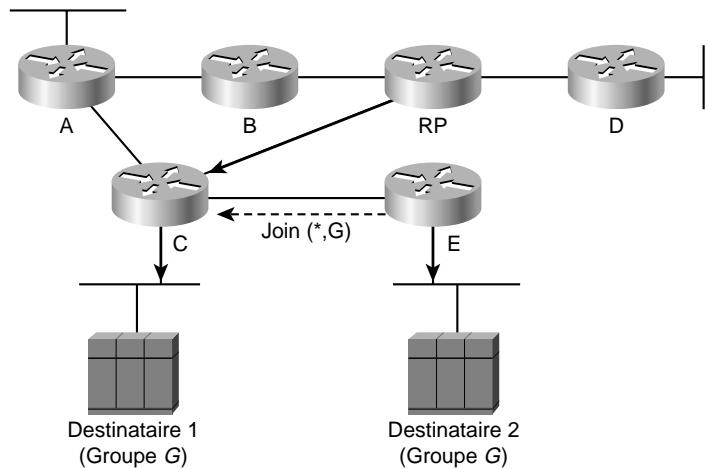
Poursuivons avec notre exemple en supposant qu'un autre hôte (Destinataire 2) rejoigne le groupe multicast G (voir Figure 13.4). A nouveau, cet hôte fait part de son désir de joindre le groupe multicast en envoyant un rapport d'adhésion IGMP au routeur E .

Figure 13.4
Adhésion à un arbre partagé — Etape 4.



Comme le routeur E n'avait pas d'entrée d'état pour le groupe multicast G, il crée une entrée d'état $(*,G)$ dans sa table de routage multicast et ajoute l'interface Ethernet dans sa liste d'interfaces sortantes (voir la flèche en gras au niveau du routeur E, Figure 13.5). De plus, puisqu'il a dû créer une entrée d'état $(*,G)$, il envoie au RP un message Join $(*,G)$, (voir la flèche en pointillés, Figure 13.5), afin de rejoindre l'arbre partagé pour le groupe G.

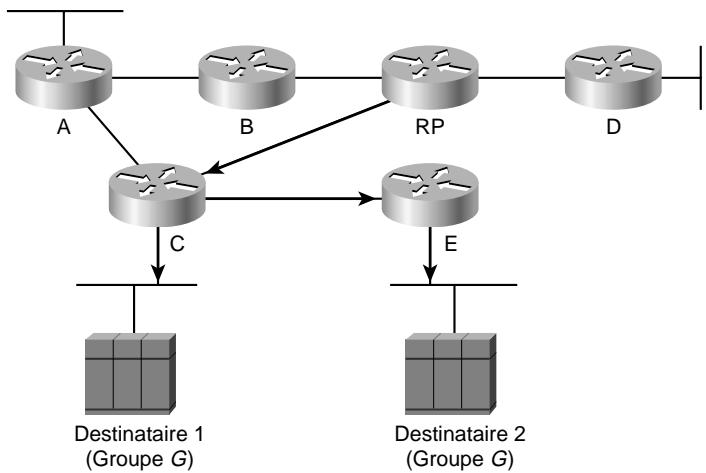
Figure 13.5
Adhésion à un arbre partagé — Etape 5.



Lorsque le routeur C reçoit le message Join $(*,G)$ du routeur E, il découvre qu'il possède déjà une entrée d'état $(*,G)$ pour le groupe G, c'est-à-dire qu'il participe déjà à l'arbre partagé pour ce groupe. Par conséquent, il ajoute simplement le lien vers le routeur E dans la liste d'interfaces sortantes de son entrée $(*,G)$.

La Figure 13.6 présente l'arbre partagé résultant (signifié par les flèches en gras), qui inclut les routeurs C et E ainsi que leurs hôtes directement connectés, c'est-à-dire les destinataires 1 et 2.

Figure 13.6
Adhésion à un arbre partagé — Etape 6.

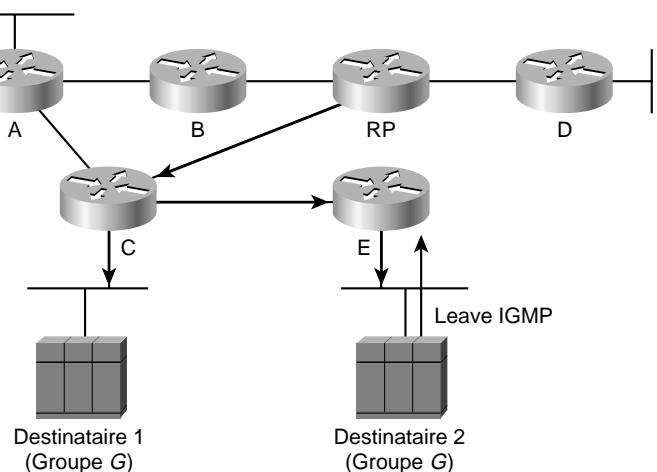


Elagage d'un arbre partagé

Etant donné que PIM-SM utilise le modèle d'adhésion explicite pour construire des arbres de distribution lorsque nécessaire, il emploie également des messages d'élagage (*Prune*) pour exclure des branches lorsque celles-ci n'ont plus besoin de recevoir le trafic multicast. On pourrait tout aussi bien stopper l'envoi périodique de messages Join servant à l'actualisation de l'arbre et autoriser les branches à le quitter. Toutefois, il en résulterait une exploitation peu efficace des ressources de réseau.

A titre d'exemple, supposez que le destinataire 2 quitte le groupe multicast G en envoyant un message Leave IGMP (de départ) au routeur E (voir Figure 13.7).

Figure 13.7
Elagage d'arbre partagé — Etape 1.



Comme le destinataire 2 était le seul hôte ayant rejoint le groupe multicast G sur l’interface Ethernet du routeur E, cette interface est supprimée de la liste d’interfaces sortantes de son entrée $(*,G)$ (voir l’absence de flèche entre le routeur E et le destinataire 2, Figure 13.8). Une fois l’interface supprimée, la liste d’interfaces sortantes pour cette entrée se retrouve vide (nulle), ce qui veut dire que le routeur E n’a plus besoin de recevoir de trafic pour ce groupe. Il envoie donc au RP un message Prune $(*,G)$ (voir Figure 13.8), pour s’exclure de l’arbre partagé.

Lorsque le routeur C reçoit le message Prune, il supprime son lien vers le routeur E de sa liste d’interfaces sortantes pour l’entrée $(*,G)$ (voir l’absence de flèche entre ces deux routeurs, Figure 13.9). Toutefois, comme le routeur C comprend toujours un hôte directement connecté pour le groupe multicast (Destinataire 1), sa liste d’interfaces sortantes pour l’entrée $(*,G)$ ne se retrouve pas vide (non nulle). Par conséquent, il demeure dans l’arbre partagé et n’envoie pas de message Prune au RP.

Figure 13.8
Elagage d’arbre partagé — Etape 2.

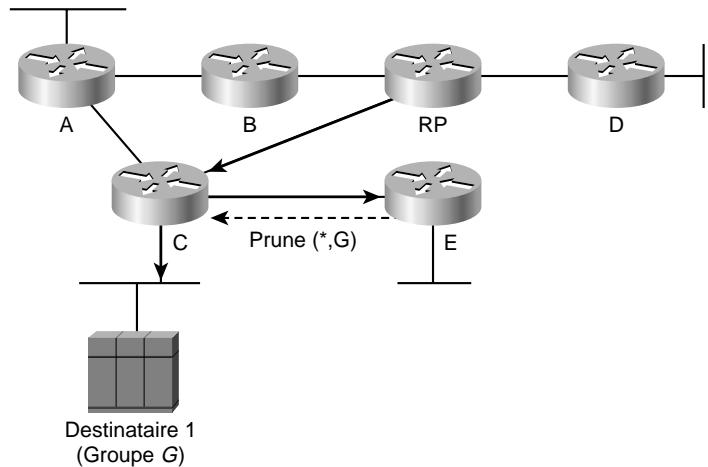
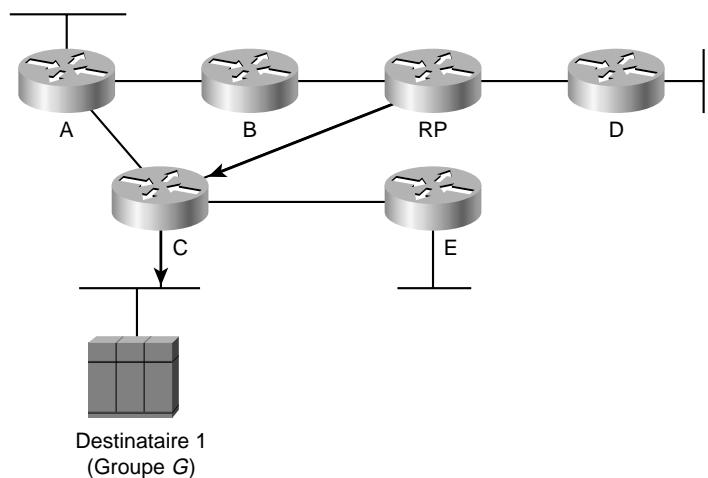


Figure 13.9
Elagage d’arbre partagé — Etape 3.



NOTE

L'exemple d'élagage d'arbre partagé présenté dans cette section n'aborde pas la situation dans laquelle un message Prune (*,G) est envoyé sur un réseau multiaccès (tel qu'un segment Ethernet) sur lequel plusieurs routeurs PIM-SM continuent à faire partie du même arbre partagé.

Arbres de plus court chemin PIM-SM

Contrairement à d'autres protocoles opérant en mode *sparse*, l'un des principaux avantages de PIM-SM est qu'il ne limite pas la réception du trafic multicast à l'arbre partagé. En effet, le mécanisme d'adhésion explicite utilisé pour rejoindre un arbre partagé peut également servir à joindre un arbre SPT (*Shortest Path Tree*) dont la racine est une source particulière. L'avantage que cela présente est évident. En rejoignant un arbre SPT, le trafic multicast est directement routé vers les destinataires et ne traverse donc pas le RP, réduisant de ce fait la latence sur le réseau et les risques de congestion au niveau du RP. D'un autre côté, les routeurs participant à l'arbre SPT (S, G) doivent créer et maintenir des entrées d'état (S, G) dans leurs tables de routage multicast, ce qui bien entendu consomme davantage de ressources de routeur.

Toujours est-il que la somme des informations (S, G) maintenues par les routeurs sur un réseau PIM-SM qui utilise des arbres SPT est généralement inférieure à celle requise pour des protocoles opérant en mode *dense*. La raison est que le mécanisme d'inondation et d'élagage (*flood-and-prune*) mis en œuvre par ces protocoles oblige tous les routeurs sur le réseau à maintenir des entrées d'état (S, G) dans leurs tables de routage multicast pour toutes les sources actives. Il en est ainsi même lorsqu'il n'existe aucun destinataire actif pour le groupe vers lequel les sources envoient du trafic. Le fait de rejoindre un arbre SPT PIM-SM permet de tirer parti d'un arbre de distribution optimal tout en évitant la surcharge et l'inefficacité associées aux autres protocoles en mode dense, tels que PIM-DM, DVRMP et MOSPF (*Multicast Open Shortest Path First*). Vous comprenez donc mieux pourquoi l'utilisation de PIM-SM est généralement plus souvent recommandée que celle de ces protocoles.

Cela nous amène à une question évidente : si l'utilisation des arbres SPT est si efficace, pourquoi joindre en premier lieu un arbre partagé ? Le problème est qu'en l'absence d'un arbre partagé pour transmettre les paquets multicast initiaux provenant d'une source, les routeurs ne disposent daucun autre moyen pour savoir qu'elle est active.

NOTE

Plusieurs méthodes, incluant l'utilisation d'entrées DNS (*Domain Name System*) dynamiques, ont été proposées pour indiquer aux routeurs quelles sources sont actuellement actives pour quels groupes. A l'aide de ces informations, un routeur pourrait immédiatement et directement joindre l'arbre SPT de toutes les sources actives dans un groupe, éliminant ainsi le besoin d'un arbre partagé et d'un RP. Malheureusement, aucune des méthodes envisagées jusqu'à présent n'a permis de recueillir le consensus de la communauté Internet.

La prochaine section présente le processus de construction d'un arbre SPT au moyen de messages Join et Prune (S, G). Ne perdez pas de vue que l'objectif est ici de comprendre les concepts élémentaires de

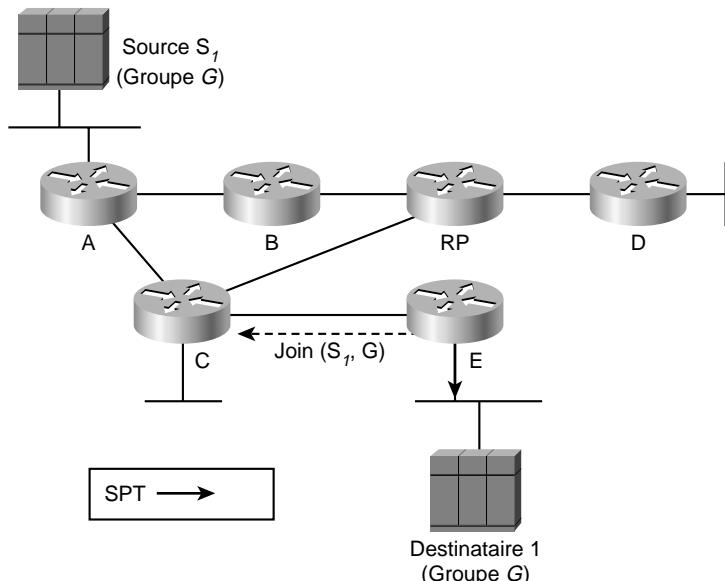
l'adhésion. Les situations et conditions dans lesquelles des routeurs PIM-SM rejoignent habituellement un arbre SPT seront traitées plus loin dans ce chapitre.

Adhésion à un arbre SPT

Dans la section "Adhésion à un arbre partagé" plus haut dans ce chapitre, nous avons vu qu'un routeur envoie au RP un message Join (*,G) pour se joindre à l'arbre partagé et recevoir ainsi le trafic multicast pour un groupe multicast, le groupe G. Toutefois, nous allons voir ici qu'en envoyant un message Join (S, G) vers une source S, un routeur peut tout aussi facilement joindre l'arbre SPT pour cette source et recevoir directement le trafic multicast envoyé par S au groupe G.

La Figure 3.10 illustre l'envoi d'un message Join (S, G) vers une source active pour participer à l'arbre SPT. Ici, le destinataire 1 a déjà rejoint le groupe G, comme illustré par la flèche en gras au niveau du routeur E.

Figure 13.10
Adhésion SPT — Etape 1.



Pour notre exemple, nous allons supposer que le routeur E sait (par magie) que la source S_1 est active pour le groupe G.

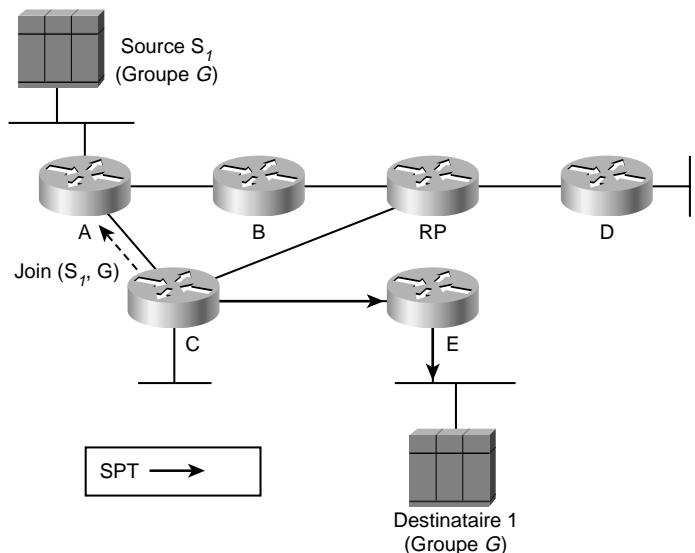
NOTE

En réalité, le routeur E aurait appris que la source S_1 est active suite à la réception d'un paquet provenant de la source via l'arbre partagé. Toutefois, pour mettre en évidence le fait que les arbres SPT sont indépendants des arbres partagés (et pour simplifier l'exemple), ignorons ce détail et concentrons-nous sur la possibilité qu'un routeur de joindre explicitement un arbre SPT, de la même manière qu'il peut joindre un arbre partagé.

Comme le routeur E souhaite joindre l'arbre SPT pour la source S_1 , il envoie un message Join (S_1, G) vers la source. Il détermine l'interface appropriée pour envoyer ce message en calculant l'interface RPF en direction de la source S_1 . Le processus de calcul RPF s'appuie sur la table de routage unicast qui indique que le routeur de premier saut vers la source est le routeur C.

Lorsque le routeur C reçoit le message Join (S_1, G) du routeur E, il crée une entrée (S_1, G) dans sa table de transmission multicast et ajoute l'interface de réception du message dans la liste d'interfaces sortantes de l'entrée (voir la flèche en gras entre les routeurs C et E, Figure 13.11). Etant donné que le routeur C a dû créer une entrée d'état pour (S_1, G), il envoie également vers la source un message Join (S_1, G) (voir la flèche en pointillés, Figure 13.11).

Figure 13.11
Adhésion SPT — Etape 2.



Lorsque le routeur A reçoit le message Join (S_1, G), il ajoute le lien vers le routeur C dans la liste d'interfaces sortantes de son entrée (S_1, G) existante (voir la flèche en gras entre ces deux routeurs, Figure 13.12). Le routeur A, aussi appelé routeur de premier saut pour la source S_1 , a déjà créé une entrée (S_1, G) lorsqu'il a reçu le premier paquet multicast en provenance de la source.

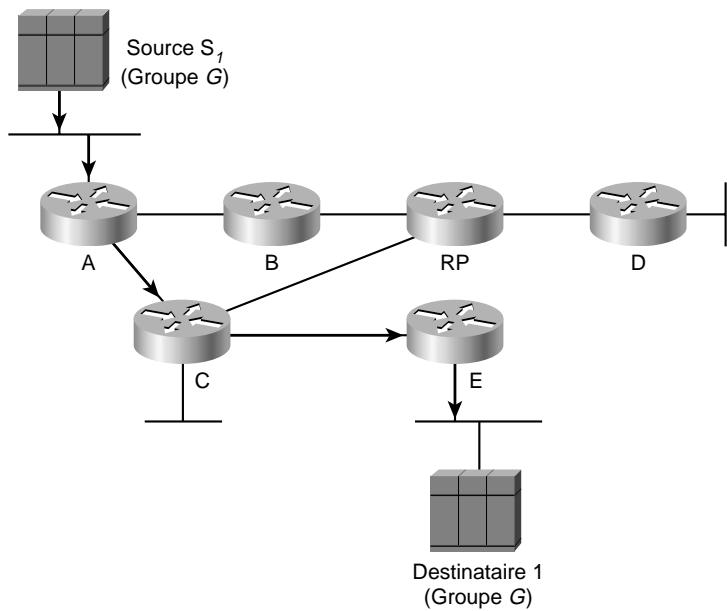
Elagage d'un arbre SPT

Un arbre SPT peut être élagué au moyen de messages Prune (S_1, G), de la même manière qu'un arbre partagé peut l'être à l'aide de messages Prune ($*, G$).

NOTE

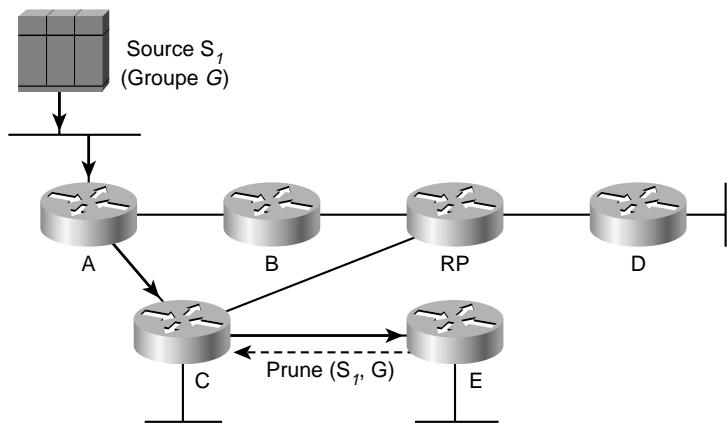
A nouveau, l'exemple d'élagage d'arbre SPT présenté dans cette section n'aborde pas la situation dans laquelle un message Prune (S, G) est envoyé sur un réseau multiaccès (tel qu'un segment Ethernet) sur lequel plusieurs routeurs PIM-SM continuent à faire partie du même arbre SPT.

Figure 13.12
Adhésion SPT — Etape 3.



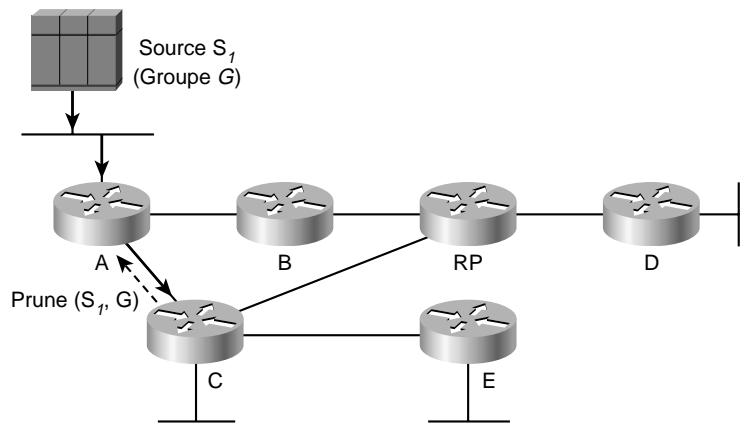
Supposez maintenant que le routeur E ne possède plus de destinataire directement connecté pour le groupe G et qu'il n'a donc plus besoin de recevoir de trafic (S_1, G). Il envoie donc vers la source S_1 un message Prune (S_1, G) (voir la flèche en pointillés, Figure 13.13).

Figure 13.13
Elagage SPT — Etape 1.



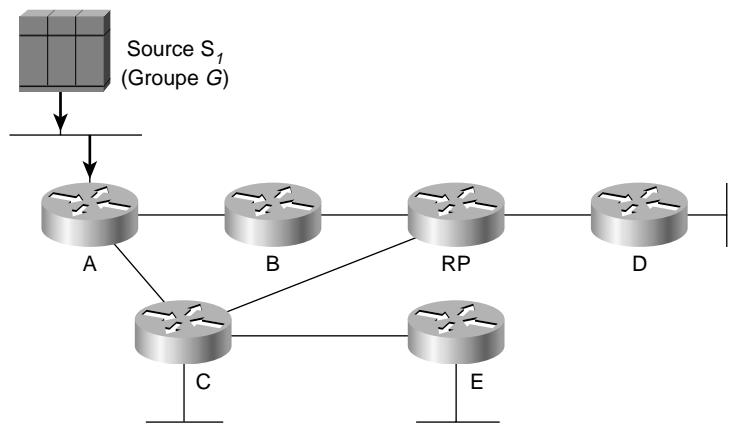
Lorsque le routeur C reçoit le message Prune (S_1, G) du routeur E, il supprime l'interface de réception du message de la liste des interfaces sortantes de son entrée (S_1, G) (voir l'absence de flèche entre ces deux routeurs, Figure 13.14). Comme le routeur C se retrouve avec une liste d'interfaces sortantes vide, il doit envoyer vers la source S_1 un message Prune (S_1, G) (voir la flèche en pointillés, Figure 13.14).

Figure 13.14
Elagage SPT — Etape 2.



Lorsque le routeur A reçoit le message Prune (S_1, G) du routeur C, il supprime l'interface de réception du message de la liste des interfaces sortantes de son entrée (S_1, G) (voir l'absence de flèche entre ces deux routeurs, Figure 13.15). Toutefois, comme le routeur A est le routeur de premier saut pour la source S_1 , c'est-à-dire qu'il y est directement connecté à la source, plus aucune action n'a lieu et il continue simplement à supprimer les paquets provenant de la source S_1 , car la liste des interfaces sortantes pour l'entrée (S_1, G) est vide.

Figure 13.15
Elagage SPT — Etape 3.



NOTE

Les exemples d'arbres SPT utilisés ici ont été radicalement simplifiés afin de faciliter la compréhension du concept SPT dans PIM-SM. A nouveau, l'objectif était de démontrer que le mécanisme explicite d'adhésion/élagage PIM-SM peut aussi bien être mis en œuvre avec des arbres SPT qu'avec des arbres partagés. Cette possibilité prend toute son importance dans les prochaines sections relatives à l'enregistrement de source et au basculement SPT.

Messages Join/Prune PIM

Bien que nous nous soyons référés aux messages Join (adhésion) et Prune (élagage) du protocole PIM comme à deux types de messages distincts, il n'existe en réalité qu'un seul type de message Join/Prune PIM. En effet, chaque message contient à la fois une liste d'adhésion et une liste d'élagage, chacune d'elle pouvant être vide, en fonction des informations transmises vers le sommet de l'arbre de distribution. En incluant plusieurs entrées dans une liste d'adhésion et/ou d'élagage, un routeur a la possibilité de rejoindre et/ou de quitter plusieurs sources et/ou groupes en utilisant un seul message Join/Prune PIM. L'efficacité du processus d'actualisation périodique s'en trouve considérablement améliorée puisqu'un seul message est généralement nécessaire pour actualiser l'état d'un routeur en amont.

Les entrées contenues dans les listes d'adhésion et d'élagage de ces messages partagent un format commun, incluant entre autres les informations suivantes :

- **Adresse source multicast.** Adresse IP de la source multicast. Si le bit WC est activé, il s'agit de l'adresse du RP.
- **Adresse de groupe multicast.** Adresse de groupe multicast de classe D.
- **Bit WC (Wildcard flag, indicateur générique).** Signifie que les destinataires en aval du RP s'attendent à recevoir des paquets de toutes les sources *via* cet arbre partagé (*,G).
- **Bit RP (RP Tree flag, indicateur RPT).** Cette information d'adhésion/élagage s'applique à l'arbre partagé et doit être transmise vers son sommet.

En combinant ces informations dans chaque entrée de liste d'adhésion/élagage, différentes requêtes peuvent être formulées vers un routeur en amont.

Par exemple, un message Join/Prune PIM comprenant l'entrée suivante dans la liste d'adhésion :

Adresse source = 192.16.10.1

Adresse de groupe = 224.1.1.1

Indicateurs = WC, RP

indique qu'il s'agit d'une requête Join (*, G) (signifié par les bits WC et RP activés) pour le groupe 224.1.1.1 dont le RP est 192.16.10.1.

Un message Join/Prune PIM comprenant l'entrée suivante dans la liste d'élagage :

Adresse source = 191.1.2.1

Adresse de groupe = 239.255.1.1

Indicateurs = Aucun

indique qu'il s'agit d'une requête Prune (S, G) (signifié par la non activation des bits WC et RP) pour la source 191.1.2.1, groupe 239.255.1.1.

NOTE

Les informations relatives au contenu des messages Join/Prune sont présentées ici, car elles sont particulièrement importantes pour comprendre le processus d'élagage de flux de trafic provenant d'une source spécifique sur un arbre partagé, décrit plus loin dans la section "Basculement SPT".

Actualisation d'état PIM-SM (State-Refresh)

Pour éviter qu'un routeur PIM-SM ne demeure dans un état de transmission alors qu'il ne le devrait pas, l'information qui détermine cet état est définie avec une durée de vie de trois minutes, à expiration de laquelle elle est supprimée. Par exemple, si un routeur en amont perd un message Prune en raison d'une congestion, il pourrait rester dans un état de transmission pendant un laps de temps trop long. La durée de vie est configurée en associant un temporisateur de trois minutes à chaque entrée d'état $(*,G)$ et (S, G) dans la table de routage multicast. Lorsqu'un temporisateur expire, l'entrée d'état correspondante est supprimée. Par conséquent, les routeurs situés en aval de l'arbre doivent régulièrement actualiser cet état de transmission pour empêcher qu'il n'expire et ne soit ainsi supprimé. Pour cela, ils envoient des messages Join vers le routeur voisin en amont approprié toutes les minutes. Lorsque ce dernier reçoit le message, il actualise son état de transmission multicast existant et réinitialise ses temporisateurs.

Les routeurs actualisent les arbres partagés périodiquement (toutes les minutes) en envoyant des messages Join $(*,G)$ vers leur voisin en amont en direction du RP. Pour actualiser les arbres SPT, ils envoient toutes les minutes des messages Join (S, G) vers leur voisin en amont en direction de la source.

Les routeurs envoient ces messages Join $(*,G)$ et (S, G) périodiques tant que la liste des interfaces sortantes des entrées $(*,G)$ et (S, G) correspondantes n'est pas vide, ou tant qu'ils possèdent un hôte directement connecté pour le groupe multicast G. En l'absence de ces messages, l'état de transmission multicast pour le groupe G finirait par expirer (au bout de trois minutes) et les arbres de distribution associés aux entrées de routage $(*,G)$ et/ou (S, G) seraient éliminés.

NOTE

Le processus d'actualisation périodique est vraisemblablement l'un des aspects de PIM-SM le plus souvent ignoré lorsque des étudiants s'initient aux notions élémentaires de ce protocole. Il en résulte une certaine confusion concernant la maintenance de certains temporisateurs dans la table de transmission multicast, mais aussi lorsque ce trafic de messages Join est observé durant des sessions de débogage.

Enregistrement de source multicast

Dans la section "Arbres partagés PIM-SM", vous avez appris de quelle manière les routeurs utilisent des messages Join $(*,G)$ pour rejoindre l'arbre partagé d'un groupe multicast (groupe G). Comme PIM-SM utilise un arbre partagé unidirectionnel, le trafic multicast peut uniquement circuler vers le bas de l'arbre. Par conséquent, une source multicast doit d'une manière ou d'une autre transmettre son trafic au RP pour, qu'à partir de là, il puisse circuler sur l'arbre. Pour cela, PIM-SM fait en sorte que le RP joigne l'arbre SPT en direction de la source de façon à pouvoir recevoir le trafic provenant de celle-ci. Mais auparavant, comme le RP doit être informé de l'existence de la source, PIM-SM implémente un processus d'enregistrement de source au moyen de messages d'enregistrement (*Register*) et de fin d'enregistrement (*Register – Stop*).

NOTE

On s'Imagine souvent, à tort, qu'une source doit s'enregistrer avant qu'un destinataire ne puisse participer à un arbre partagé. En réalité, des destinataires peuvent joindre un arbre partagé même s'il n'existe aucune source active. Ainsi, lorsqu'une source devient active, le RP joint alors l'arbre SPT vers la source et commence à transmettre le trafic vers le bas de l'arbre partagé. De la même manière, une source peut s'enregistrer en l'absence de destinataires actifs sur le réseau. Ensuite, lorsqu'un destinataire rejoint le groupe, le RP joint l'arbre SPT vers toutes les sources du groupe et commence à transmettre le trafic sur l'arbre partagé.

La section suivante décrit le processus d'enregistrement d'une source au moyen de messages PIM Register et Register-Stop. Ce processus opère en signalant à un RP une source active sur le réseau et en transmettant les paquets multicast initiaux au RP pour qu'il les envoie vers le bas de l'arbre partagé. En fin de section, un exemple détaillé illustre ce processus.

Messages Register PIM

Les messages Register PIM sont envoyés au RP par les routeurs DR (*Designated Router*) de premier saut, c'est-à-dire ceux qui sont directement connectés à une source multicast. Ces messages remplissent deux objectifs :

1. Notifier le RP que la source S est active pour le groupe G.
2. Transmettre au RP les paquets multicast initiaux envoyés par la source S_1 (chacun encapsulé dans un seul message Register) pour qu'il les achemine sur son arbre partagé.

Par conséquent, lorsqu'une source multicast commence à émettre, le DR qui lui est directement connecté reçoit les paquets multicast qu'elle envoie et crée une entrée d'état (S, G) dans sa table de routage multicast. De plus, comme le DR est directement relié à la source, il encapsule chaque paquet multicast dans un message Register séparé et les envoie au RP en mode unicast. La manière dont le DR découvre l'adresse du RP sera décrite à la section "Découverte de RP", plus loin dans ce chapitre.

NOTE

Contrairement aux autres messages PIM qui sont envoyés en mode multicast sur un segment local et qui circulent de saut en saut à travers le réseau, les messages PIM Register et Register-Stop sont transmis en mode unicast entre le routeur de premier saut et le RP.

Lorsqu'un RP reçoit un message Register, il commence par le désencapsuler de façon à examiner le paquet multicast qu'il contient. Si le paquet est destiné à un groupe multicast actif (c'est-à-dire que des requêtes Join d'arbre partagé ont été reçues pour le groupe), le RP transmet le paquet vers le bas de l'arbre. Il joint ensuite l'arbre SPT pour la source S afin de pouvoir recevoir le trafic (S, G) d'origine plutôt qu'il ne soit encapsulé dans des messages Register. Par contre, s'il n'existe pas d'arbre partagé actif pour le groupe, le RP supprime simplement le paquet multicast et n'envoie pas de requête Join vers la source.

Messages Register-Stop PIM

Les messages Register-Stop PIM sont envoyés par le RP au routeur DR de premier saut pour lui demander de stopper l'envoi de messages Register (S, G) dans l'une des situations suivantes :

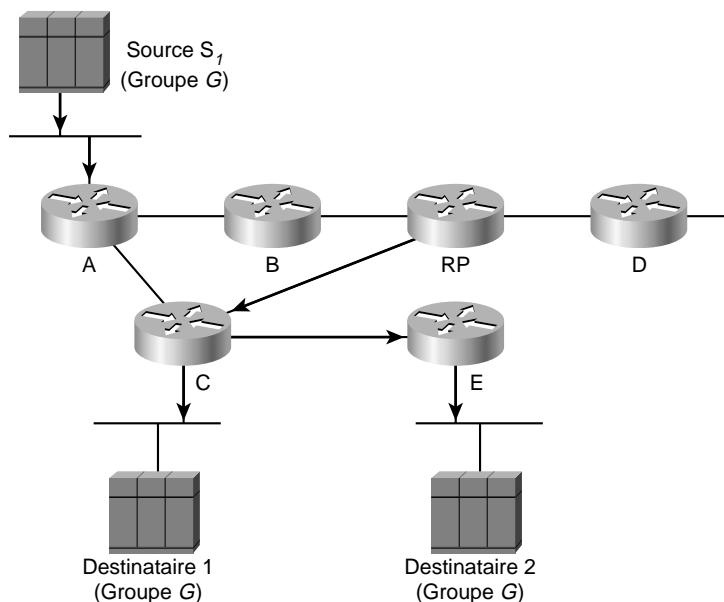
- Lorsque le RP commence à recevoir du trafic multicast provenant de la source S via l'arbre SPT (S, G).
- Lorsque le RP n'a plus besoin de recevoir ce trafic, car il n'existe aucun arbre partagé pour le groupe.

Lorsqu'un DR de premier saut reçoit un message Register-Stop, il sait que le RP a reçu le message Register et qu'il a rencontré l'une des deux conditions précitées. Dans tous les cas, il met fin au processus d'enregistrement et arrête d'encapsuler les paquets (S, G) dans des messages Register.

Exemple d'enregistrement de source

Reprenons l'exemple de réseau de la Figure 13.6, au point où deux routeurs (Routeur C et Routeur E) ont rejoint le groupe multicast G après avoir reçu des rapports d'adhésion IGMP de la part de leurs hôtes directement connectés. A ce stade, les deux routeurs ont donc réussi à rejoindre l'arbre partagé. Supposons maintenant que la source multicast S₁ commence à envoyer du trafic multicast vers le groupe G (voir Figure 13.16).

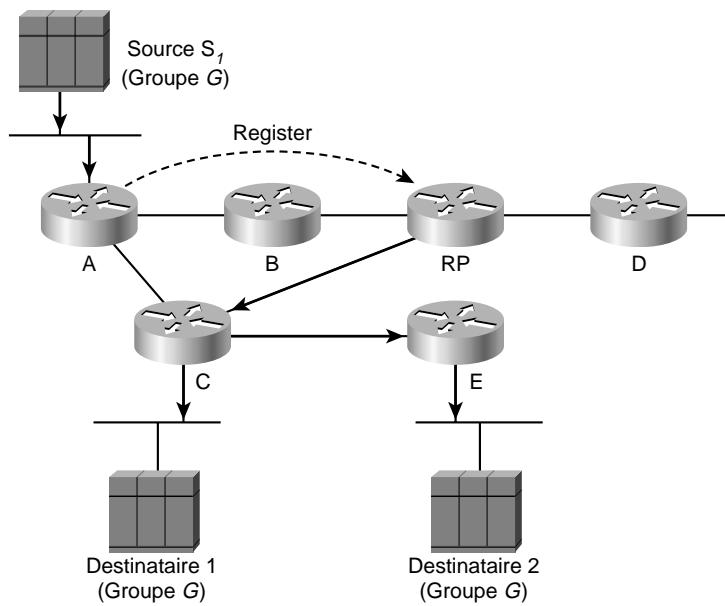
Figure 13.16
Enregistrement de source — Etape 1.



Etant donné que le routeur A est le DR de premier saut, il répond au trafic multicast provenant de la source S₁ en encapsulant les paquets multicast dans des messages Register et en les envoyant au RP en mode unicast (voir la flèche en pointillés, Figure 13.17). Notez que les messages Register ne sont

pas transmis saut par saut comme les autres messages PIM, mais sont envoyés directement au RP à l'instar d'un paquet unicast normal.

Figure 13.17
Enregistrement de source — Etape 2.



Lorsque le RP reçoit le message Register, il le désencapsule et découvre que le paquet est adressé au groupe multicast G. Comme il constate qu'il existe un arbre partagé avec une liste d'interfaces sortantes non vide, il envoie le paquet ainsi désencapsulé vers le bas de l'arbre (voir les flèches en gras, Figure 13.17). De plus, il envoie une requête Join (S_1, G) vers la source S_1 pour joindre l'arbre SPT afin de recevoir le trafic (S_1, G) et le transmettre sur l'arbre partagé. La requête Join (S_1, G) circule de saut en saut jusqu'au DR de premier saut, le routeur A (voir Figure 13.18).

Une fois que la requête Join (S_1, G) a atteint le routeur A, cela signifie qu'un arbre SPT (S_1, G) a été construit entre ce routeur et le RP (voir les flèches en gras, Figure 13.19). Dès lors, le trafic (S_1, G) peut commencer à circuler vers le RP via le nouvel arbre SPT (S_1, G).

Mais étant donné que le RP n'a plus besoin de continuer à recevoir le trafic (S_1, G) encapsulé dans des messages Register, il envoie un message Register–Stop unicast vers le DR de premier saut (Router A) (voir Figure 13.19).

Poursuivons avec notre exemple et imaginons qu'une autre source multicast (Source S_2) connectée au routeur D commence à émettre vers le groupe G. Le même processus d'enregistrement a lieu, avec pour résultat l'adhésion du RP à l'arbre SPT (S_2, G) afin qu'il puisse recevoir le trafic (S_2, G) et l'envoyer sur l'arbre partagé pour le groupe G.

Figure 13.18
Enregistrement de source — Etape 3.

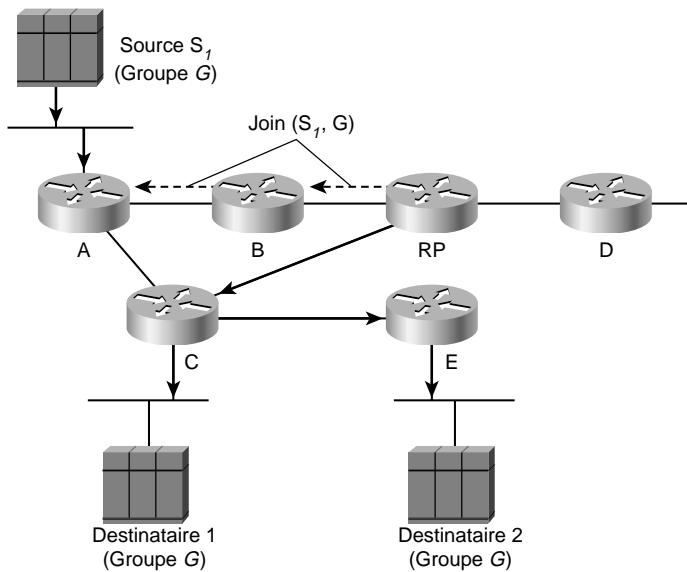
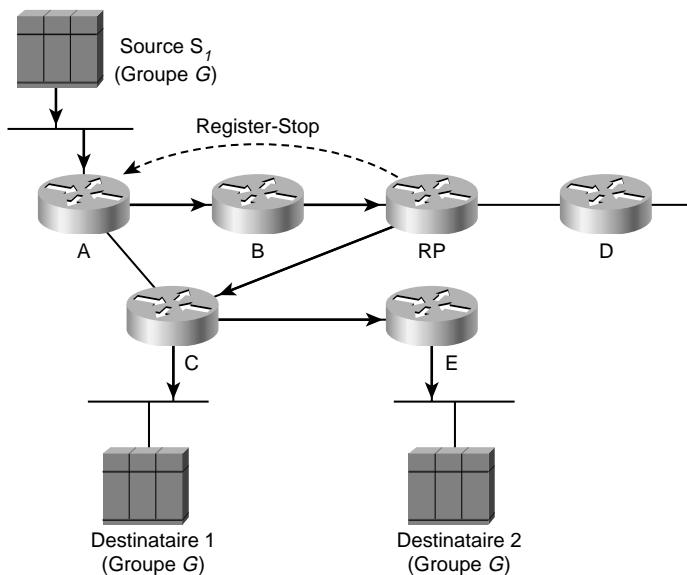
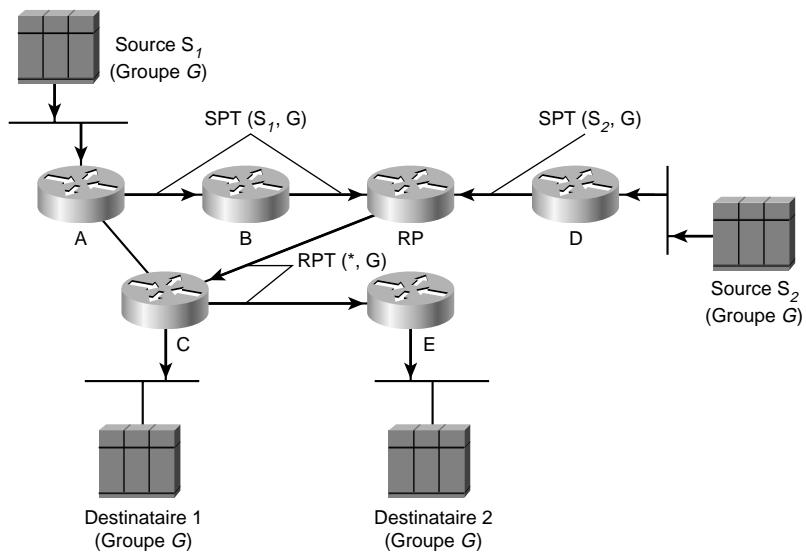


Figure 13.19
Enregistrement de source — Etape 4.



Le RP participe donc aux arbres SPT (S_1, G) et (S_2, G) pour les deux sources actives du groupe G (voir Figure 13.20). Ce trafic est transmis vers le bas de l'arbre partagé ($*, G$) en direction des destinataires 1 et 2. Les chemins sont à présent complets entre les sources et les destinataires et le trafic multicast circule correctement.

Figure 13.20
Enregistrement de source — Etape 5.



Basculement SPT

PIM-SM autorise un routeur DR de dernier saut (c'est-à-dire un DR avec des hôtes directement connectés qui ont joint un groupe multicast) à basculer de l'arbre partagé vers l'arbre SPT pour une source spécifique. Ce processus est habituellement mis en œuvre en spécifiant un seuil SPT relatif à la bande passante. Lorsque ce seuil est dépassé, le DR de dernier saut joint le SPT. Sur les routeurs Cisco, ce seuil est défini par défaut avec la valeur zéro, ce qui signifie que le SPT est rejoint dès que le premier paquet multicast envoyé par une source a été reçu via l'arbre partagé.

Exemple de basculement SPT

Revenons à notre exemple au point où nous l'avons laissé (voir Figure 13.20). Comme le routeur C est un DR de dernier saut, il a la possibilité de basculer vers l'arbre SPT des sources S₁ et S₂. Nous nous concentrerons sur la source S₁, car elle représente un cas plus intéressant pour notre exemple. Pour accomplir ce basculement, le routeur C doit envoyer une requête Join (S₁, G) vers la source S₁ (voir la flèche en pointillés, Figure 13.21).

Lorsque le routeur A reçoit cette requête Join, il ajoute l'interface sur laquelle elle a été reçue dans la liste d'interfaces sortantes de l'entrée (S₁, G) dans sa table de transmission multicast, ajoutant ainsi le lien entre lui et le routeur C à l'arbre SPT (S₁, G) (voir Figure 13.22). A ce stade, le trafic multicast (S₁, G) peut circuler directement vers le routeur C via le SPT (S₁, G).

Figure 13.21
Basculement SPT
— Etape 1.

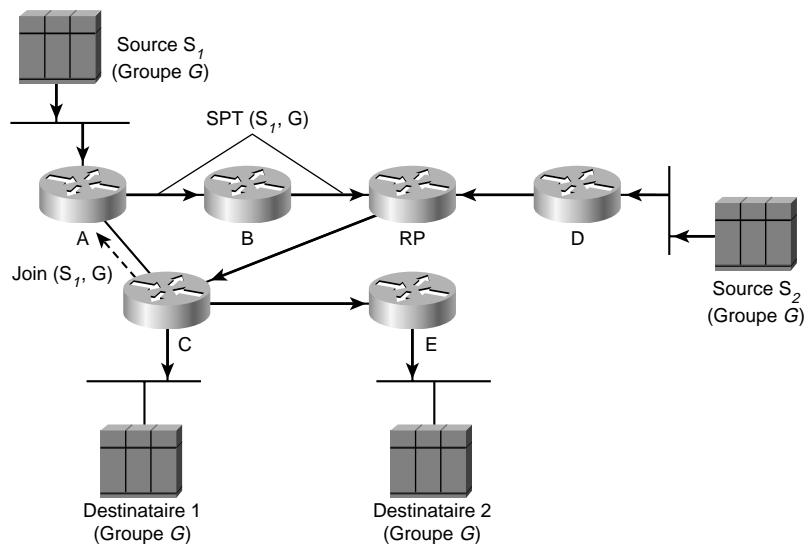
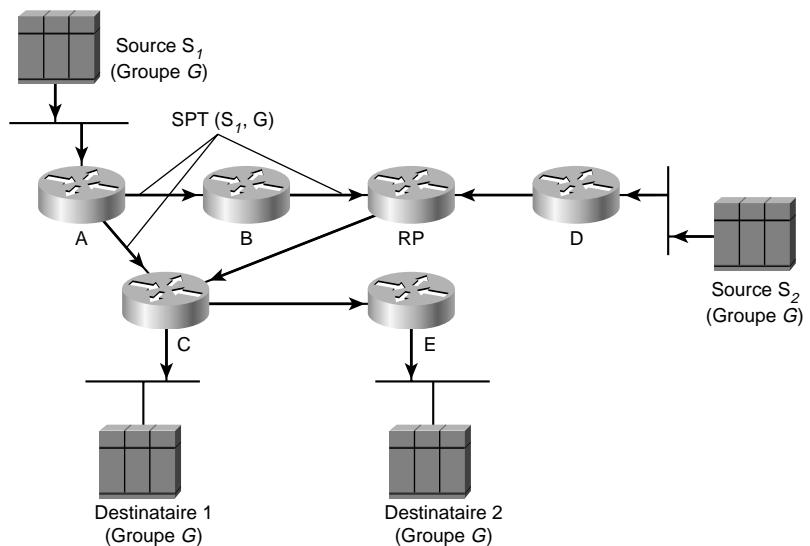


Figure 13.22
Basculement SPT
— Etape 2.



NOTE

Normalement, les seuils SPT sont configurés de façon cohérente sur tous les routeurs du réseau. Dans une situation comme celle illustrée ici, le routeur E initierait aussi un basculement vers le SPT en envoyant une requête Join (S, G) au routeur en amont, vers la source, qui dans ce cas serait le routeur C. Toutefois, pour que cet exemple reste simple, nous examinerons uniquement le cas du routeur C. Pour finir, n'oubliez pas que ce sont les routeurs, et non les destinataires, qui initient ce basculement vers le SPT.

Vous avez probablement remarqué que le trafic multicast (S_I , G) peut maintenant emprunter deux chemins pour atteindre le routeur C, à savoir l'arbre partagé et l'arbre SPT. Comme l'utilisation de ces deux chemins provoquerait la livraison de paquets dupliqués au routeur C et consommerait inutilement la bande passante du réseau, il faut indiquer au RP d'élaguer le trafic multicast (S_I , G) sur l'arbre partagé.

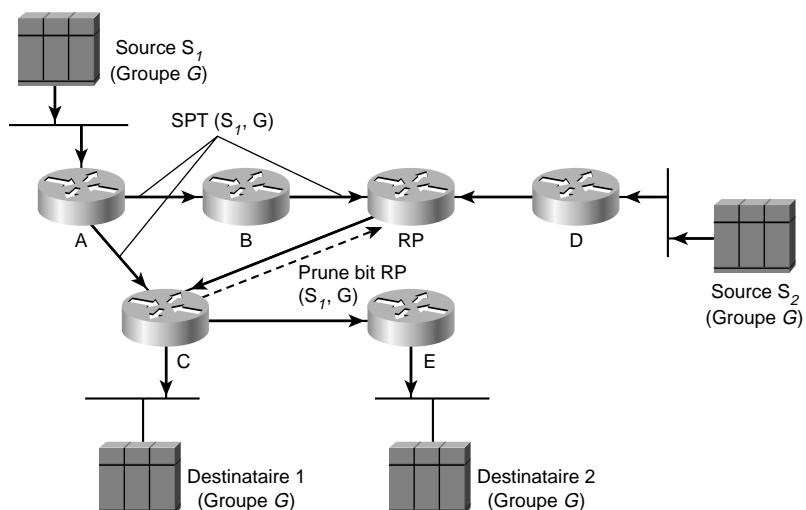
Elagage de source sur l'arbre partagé

Dans une situation comme celle illustrée Figure 13.22, dans laquelle le trafic source circule vers le bas de l'arbre partagé, mais est également reçu *via* le SPT, un type spécial de message Prune est utilisé pour indiquer au RP d'élaguer la source de ce trafic sur l'arbre partagé. Ce message spécial est appelé *Prune bit RP* (S, G), car le bit RP est activé dans l'entrée de la liste d'élagage. Comme mentionné à la section "Messages Join/Prune PIM", l'indicateur RP (ou bit RP) signale que le message en question s'applique à l'arbre partagé et doit être transmis vers le RP. Le fait d'activer ce bit dans un message Prune (S_I, G) puis d'envoyer ce dernier vers le sommet de l'arbre partagé indique aux routeurs traversés d'élaguer le trafic multicast de la source S_I sur l'arbre partagé.

Dans la Figure 13.23, le routeur C envoie un message Prune bit RP (S_1, G) vers le RP de l'arbre partagé afin de supprimer le trafic multicast S_1 sur cet arbre. À réception de ce message, le RP actualise son état de transmission multicast de façon que le trafic (S_1, G) ne soit plus transmis sur le lien vers le routeur C. Toutefois, comme ce lien représentait la seule interface de l'arbre partagé sur laquelle le trafic (S_1, G) circulait, le RP n'a lui aussi plus besoin de recevoir ce trafic.

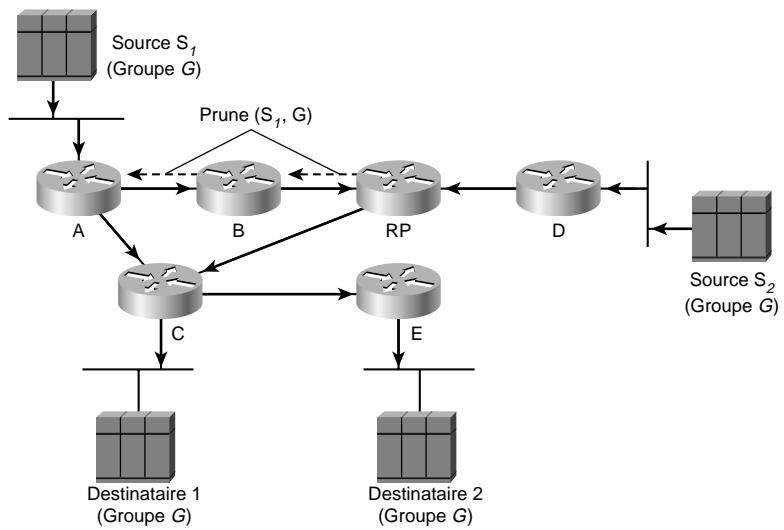
Figure 13.23

*Elagage de source
sur l'arbre partagé
— Etape 1.*



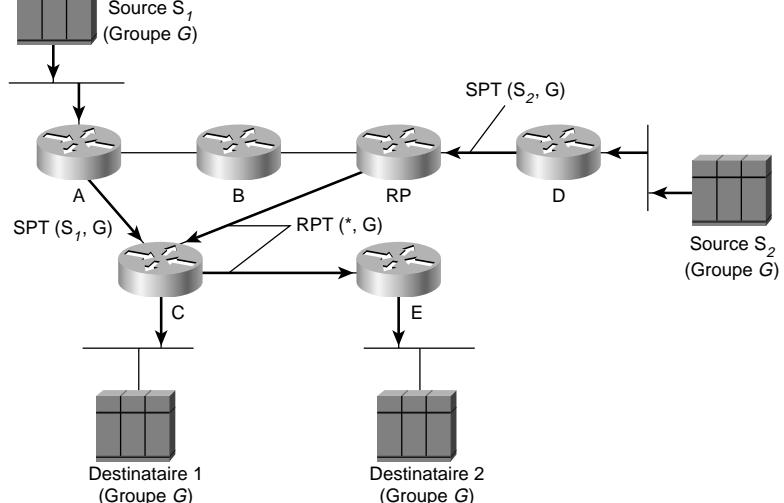
Pour stopper le flux de trafic (S_1 , G) devenu inutile, le RP envoie un message Prune (S_1 , G) vers la source S_1 . Ce message, représenté par les flèches en pointillés dans la Figure 13.24, passe par le routeur B avant d'atteindre le routeur de premier saut, c'est-à-dire le routeur A.

Figure 13.24
Elagage de source
sur l'arbre partagé
— Etape 2.



La Figure 13.25 présente le résultat. L'arbre SPT (S_1, G) a été élagué, laissant uniquement le lien entre le routeur A et le routeur C. Le routeur E reçoit toujours le trafic (S_1, G) de la part du routeur C (comme indiqué par la flèche en gras entre ces deux routeurs) bien que le routeur E ignore que son voisin en amont (Routeur C) a basculé vers le SPT pour la source S_1 .

Figure 13.25
Elagage de source
sur l'arbre partagé
— Etape 3.



Dans la Figure 13.25, le trafic (S_2, G) continue de circuler vers le RP et vers le bas de l'arbre partagé en direction des destinataires 1 et 2.

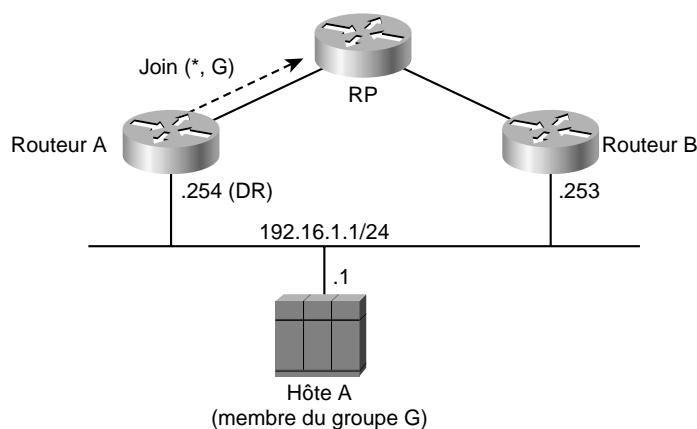
Routeur DR PIM-SM

PIM élit un routeur désigné ou DR (*Designated Router*) sur chaque réseau multiaccès (un segment Ethernet, par exemple) en utilisant des messages Hello PIM. Dans le cas du protocole PIM-DM, le rôle de DR n'a de sens que si la version 1 de IGMP est utilisée sur le réseau multiaccès, car elle ne met pas en œuvre de mécanisme IGMP d'élection d'interrogateur (*Querier Election*). Si c'était le cas, le routeur DR élu assurerait aussi la fonction d'interrogateur IGMP. Toutefois, comme nous allons le voir, le rôle d'un DR est beaucoup plus important dans le cas du protocole PIM-SM.

Rôle du routeur DR

Examinez l'exemple de réseau illustré Figure 13.26, dans lequel deux routeurs PIM-SM sont connectés à un réseau multiaccès commun comportant un destinataire actif pour le groupe G. Comme le modèle d'adhésion explicite est mis en œuvre, seul le DR (ici le routeur A) devrait envoyer des requêtes Join au RP pour construire l'arbre partagé pour le groupe G. Si les deux routeurs étaient autorisés à envoyer des requêtes Join $(*, G)$ au RP, des chemins parallèles seraient créés et l'hôte A recevrait un trafic multicast dupliqué.

Figure 13.26
Routeur DR PIM-SM.



De la même manière, si l'hôte A commençait à émettre du trafic multicast pour le groupe, c'est le DR qui serait chargé d'envoyer des messages Register au RP. A nouveau, si les deux routeurs étaient autorisés à envoyer des messages Register, le RP recevrait des paquets dupliqués.

Reprise de fonction du routeur DR

Lorsque plusieurs routeurs sont connectés à un segment LAN, PIM-SM ne fournit pas seulement une méthode permettant d'élire le DR, mais offre également le moyen de détecter une défaillance au niveau du DR existant. Par exemple, si le DR de la Figure 13.26 (Routeur A) tombait en panne, le routeur B détecterait cette situation à expiration de ses informations de voisinage pour le routeur A. Une nouvelle élection de DR aurait ensuite lieu et le routeur B deviendrait le nouveau DR actif pour ce réseau.

Dans une telle situation, le routeur B sait déjà qu'il existe un destinataire actif (Hôte A) sur le réseau, car il a reçu le rapport d'adhésion IGMP de ce dernier. Il dispose donc d'une entrée d'état IGMP pour le groupe G sur cette interface, ce qui l'amènerait à envoyer une requête Join vers le RP aussitôt qu'il serait élu comme nouveau DR. La circulation du trafic serait alors établie sur une nouvelle branche de l'arbre partagé *via* le routeur B. De plus, si l'hôte A émettait du trafic, le routeur B initierait un nouveau processus Register immédiatement après avoir reçu le paquet multi-cast de la part de l'hôte A, déclenchant ainsi l'adhésion du RP au SPT pour l'hôte A *via* la nouvelle branche passant par le routeur B.

Découverte de RP

Pour garantir un fonctionnement efficace de PIM-SM, tous les routeurs dans un domaine PIM-SM doivent connaître l'adresse du RP. Sur les réseaux de petite taille qui utilisent un seul RP pour tous les groupes multicast, il serait possible de spécifier manuellement l'adresse IP du RP dans la configuration de chaque routeur. Toutefois, sur un réseau en extension ou sur lequel le RP change souvent, la configuration manuelle de chaque routeur peut rapidement devenir un cauchemar. De plus, ce problème peut encore se compliquer lorsque plusieurs RP situés dans différents endroits du domaine sont utilisés pour gérer les groupes multicast, soit pour optimiser l'arbre partagé ou pour répartir la charge de travail du RP entre plusieurs routeurs.

La version 2 de PIM définit un mécanisme appelé Bootstrap qui permet à tous les routeurs PIM-SM dans un domaine de découvrir dynamiquement toutes les correspondances groupe-RP, évitant ainsi le problème de configuration manuelle. L'implémentation Cisco de PIM fournit un autre mécanisme appelé Auto-RP qui assure la même fonction. Il a été développé avant que ne soit publiée la spécification de PIMv2 pour permettre aux routeurs des réseaux PIM-SM existants de connaître dynamiquement ces correspondances groupe-RP.

Evolutivité de PIM-SM

Etant donné que PIM-SM utilise le modèle d'adhésion explicite, le trafic multicast est limité aux portions du réseau sur lesquelles il est souhaité. Par conséquent, et comme mentionné précédemment, PIM-SM est plus efficace que les protocoles par inondation et élagage (*flood-and-prune*) tels que DVRMP et PIM-DM et convient donc mieux pour les réseaux multicast pouvant compter des hôtes de l'autre côté de liaisons WAN.

Outre les avantages évidents du modèle d'adhésion explicite, PIM-SM permet aux ingénieurs de réseaux de mettre en œuvre des arbres SPT afin de réduire la latence généralement associée à l'utilisation d'arbres partagés. Quant au choix d'utiliser ou non ces arbres SPT, il peut être effectué individuellement pour chaque groupe. Par exemple, dans le cas d'une application multicast coopérative et interactive (*many-to-many*) à faible débit, comme SDR, s'exécutant sur un réseau avec une topologie en étoile, l'utilisation d'arbres SPT n'est pas forcément justifiée. Dans ce cas, la définition d'un seuil SPT infini pourrait obliger tout le trafic de groupe à demeurer sur l'arbre partagé. Cette possibilité de contrôler l'utilisation des arbres SPT offre aux ingénieurs de réseaux une meilleure maîtrise de la quantité des états créés sur les routeurs du réseau, sachant que le nombre de ces états représente l'un des principaux facteurs affectant l'évolutivité de n'importe quel protocole de routage multicast.

Pour la plupart des réseaux multicast généraux, PIM-SM s'avère être le protocole de routage multicast intradomaine de choix. Il existe bien sûr des exceptions, comme pour les réseaux à usage plus spécifique conçus pour supporter des applications de réseau spécialisées s'exécutant sous le contrôle total des administrateurs de réseau. Dans ce genre de situation, PIM-SM pourrait toujours représenter la solution la plus appropriée, mais d'autres protocoles pourraient également être développés pour opérer efficacement dans le cadre d'un contrôle strict du réseau et des applications.

Résumé

Ce chapitre a présenté les notions élémentaires du protocole PIM-SM. Il se caractérise par l'utilisation d'un modèle d'adhésion explicite pour construire des arbres partagés et des arbres SPT. De plus, comme le trafic circule uniquement vers le bas d'un arbre partagé dans le cas d'une implémentation traditionnelle de PIM-SM, le RP est autorisé à rejoindre l'arbre SPT en direction de la source pour recevoir le trafic provenant de celle-ci. Toutefois, comme le RP doit auparavant connaître l'existence de la source, un processus d'enregistrement de source (*Register*) est mis en œuvre. Le dernier point, et peut-être le plus ignoré des aspects de PIM-SM, est que les routeurs comportant des destinataires directement connectés rejoignent le plus souvent immédiatement le SPT vers une source nouvellement détectée pour contourner le RP.

II

Etudes de cas

- | | |
|-----------|---|
| 14 | <i>Gestion de réseau commuté</i> |
| 15 | <i>Architecture de commutation de paquets</i> |
| 16 | <i>Redistribution EIGRP et OSPF</i> |
| 17 | <i>Configuration de EIGRP sur des réseaux Novell et AppleTalk</i> |
| 18 | <i>Conception, configuration, et dépannage de MPOA</i> |
| 19 | <i>Routage DDR</i> |
| 20 | <i>Evolutivité du routage DDR</i> |
| 21 | <i>Emploi efficace de RNIS en milieu multiprotocole</i> |
| 22 | <i>Amélioration de la sécurité sur les réseaux IP</i> |
| 23 | <i>HSRP pour un routage IP avec tolérance aux pannes</i> |

14

Gestion de réseau commuté

Par Paul Della Maggiora et al.

Ce chapitre fait partie de l'ouvrage *Performance and Fault Management*, à paraître chez Cisco Press (en langue anglaise).

Il réunit un ensemble de directives concernant la surveillance des pannes et la corrélation d'événements, telles qu'elles s'appliquent aux commutateurs et routeurs Cisco, dans le but d'aider les administrateurs à mieux gérer leur réseau d'équipements Cisco. Il débute par une présentation des options de gestion de commutateurs et de routeurs, et se poursuit avec la définition plus spécifique des objets MIB, des interceptions SNMP, et des messages Syslog associés aux problèmes typiques de fonctionnement ou de performances. Ces scénarios peuvent être utilisés pour spécifier des éléments particuliers à surveiller et implémenter des règles de corrélation d'événements. Ce chapitre inclut une base de connaissances Cisco relative à ses commutateurs et routeurs.

Il aborde aussi les erreurs et la corrélation d'événements pour les commutateurs et routeurs Cisco en s'appuyant sur les objets MIB et les messages Syslog. Comme les bases MIB privées de Cisco évoluent constamment, certains des scénarios décrits dans ce chapitre peuvent ne pas s'appliquer à votre installation si les objets MIB et/ou les messages Syslog ne sont pas supportés ou applicables dans votre environnement. Le site Web www.cisco.com contient un listing croisé de toutes les bases MIB et messages Syslog, de façon à présenter les objets ou messages supportés par certaines plates-formes et versions de IOS.

Ce chapitre était à l'origine un livre blanc écrit par un groupe d'ingénieurs réseau de chez Cisco pour s'attaquer aux préoccupations des clients lors de la migration de leurs réseaux de routeurs ou de hub partagés vers des réseaux de routeurs ou commutés. Ils constatèrent que la stratégie de

gestion de réseau qui était opérationnelle pour les réseaux partagés n'était pas suffisamment évolutive pour supporter et surveiller efficacement les réseaux commutés.

Ce chapitre se termine par un ensemble d'études de cas qui vous aideront dans la gestion de réseaux commutés.

Présentation

Ce chapitre est un condensé d'une grande quantité d'informations sur la gestion d'équipements Cisco prévu pour aider les utilisateurs finaux à mieux gérer leurs réseaux, mais aussi pour permettre aux fournisseurs d'applications de gestion de réseaux d'améliorer leur offre de produits. Les directives présentées ici, visant à améliorer le suivi du réseau et à mieux comprendre les interdépendances d'événements, correspondent aux conditions que l'auteur juge essentiel de surveiller.

Outre la description des événements de commutateur et de routeur les plus importants à analyser sur un seul équipement, ce chapitre présente une série de scénarios de mise en relation d'événements pour examiner un VLAN ou un sous-réseau, ou même la totalité du réseau, à travers plusieurs dispositifs. Il introduit le modèle événementiel de Cisco ainsi qu'une description de tous les moyens disponibles pour collecter des informations à partir d'un commutateur ou d'un routeur.

Lectorat de ce chapitre

Ce chapitre s'adresse aux ingénieurs en gestion de réseau qui doivent mettre en place une administration de réseau pour les commutateurs et routeurs Cisco. Il suppose que le lecteur détient les connaissances de base sur les théories de commutation et de routage, sur le protocole SNMP (*Simple Network Management Protocol*), et sur les commutateurs et routeurs Cisco. Il s'adresse aussi aux fournisseurs de plates-formes et d'applications de gestion de réseau afin qu'ils améliorent leurs produits en intégrant des règles spécifiques de surveillance et de corrélation d'événements pour les équipements Cisco.

Termes et acronymes employés dans ce chapitre

Le Tableau 14.1 liste et explique les termes importants que vous rencontrerez dans ce chapitre.

Tableau 14.1 : Terminologie employée dans le domaine de la gestion de réseaux

Terme	Description
802.10	Le protocole 802.10 intègre un mécanisme permettant au trafic LAN de transporter un identificateur VLAN, autorisant ainsi une commutation sélective des paquets. Il est issu de la spécification IEEE 802.10 SITS (<i>Standards for Interoperable LAN/MAN Security</i>), adoptée fin 1992. Il a été développé à l'origine pour répondre aux problèmes de sécurité dans des environnements LAN/MAN (<i>Metropolitan Area Network</i>) partagés.
ARP	<i>Address Resolution Protocol</i> (protocole de résolution d'adresses).
ASIC	<i>Application-Specific Integrated Circuit</i> (circuit intégré pour applications spécifiques).
ATM	<i>Asynchronous Transfer Mode</i> (mode de transfert asynchrone).

Tableau 14.1 : Terminologie employée dans le domaine de la gestion de réseaux (suite)

Terme	Description
BPDU	<i>Bridge Protocol Data Unit</i> (unité de données de protocole de pont).
BRI	<i>Basic Rate Interface</i> (interface primaire).
CAM	<i>Content-Addressable Memory</i> (mémoire accessible par son contenu).
CDP	<i>Cisco Discovery Protocol</i> (protocole de découverte Cisco).
CLI	<i>Command-Line Interface</i> (interface en ligne de commande).
CPU	<i>Central Processing Unit</i> (unité de traitement centrale).
CRC	<i>Cyclic Redundancy Check</i> (contrôle de redondance cyclique).
CRM	<i>Cisco Resource Manager</i> (gestionnaire de ressource Cisco).
CWSI	<i>CiscoWorks for Switched Internetworks</i> (CiscoWorks pour interréseaux commutés).
DBMS	<i>Database Management System</i> (système de gestion de bases de données).
EARL	<i>Enhanced Address Recognition Logic</i> (circuit de reconnaissance d'adresse avancée).
ECS	<i>Event-Correlation System</i> (système de corrélation d'événements).
E-SPAN	<i>Enhanced Switched Port Analyzer</i> (analyseur avancé de port commuté).
event (événement)	Généralement, un message d'information ou d'erreur généré par un équipement Cisco.
FDDI	<i>Fiber Distributed Data Interface</i> (interface de données distribuée sur fibre optique).
GUI	<i>Graphical User Interface</i> (interface graphique utilisateur).
ISL	<i>Inter-Switch Link</i> (liaison inter-commutateurs).
LANE	<i>LAN Emulation</i> (émulation LAN).
LLC	<i>Logical Link Control</i> (contrôle de liaison logique).
MAC	<i>Media Access Control</i> (contrôle d'accès au média).
MAU	<i>Media Attachment Unit</i> (unité de connexion au média).
MIB	<i>Management Information Base</i> (base d'informations de gestion).
NIC	<i>Network Interface Card</i> (carte d'interface de réseau).
NMP	<i>Network Management Processor</i> (processeur de gestion de réseau).
NMS	<i>Network Management System</i> (système de gestion de réseau).
OID	<i>Object Identifier</i> (identificateur d'objet).
OSI	<i>Open System Interconnection</i> (interconnexion de systèmes ouverts).
PDU	<i>Protocol Data Unit</i> (unité de données de protocole).
PVID	<i>Port VLAN ID</i> (identifiant de port VLAN).

Tableau 14.1 : Terminologie employée dans le domaine de la gestion de réseaux (suite)

Terme	Description
RADIUS	<i>Remote Access Dial-In User Service</i> (service utilisateur d'accès distant par liaison commutée).
RMON	<i>Remote Monitoring</i> (suivi à distance).
RNIS	Réseau numérique à intégration de services (ISDN dans le cas de caractéristiques techniques ou applications d'origines anglo-saxonnes, <i>Integrated Services Digital Network</i>).
severity	Niveau de gravité d'un événement.
SLA	<i>Service-Level Agreement</i> (accord de niveau service).
SNAP	<i>Subnetwork Access Protocol</i> (protocole d'accès au sous-réseau).
SNMP	<i>Simple Network Management Protocol</i> (protocole d'administration de réseau simplifiée).
SPAN	<i>Switched Port Analyzer</i> (analyseur de port commuté).
SRAM	<i>Static Random-Access Memory</i> (mémoire statique à accès sélectif). Type de mémoire RAM qui conserve son contenu tant qu'elle est sous tension. Elle ne requiert pas de rafraîchissement constant.
STP	<i>Spanning-Tree Protocol</i> (protocole par arbre recouvrant).
syslog	Un service de journalisation d'erreurs supporté par les commutateurs et routeurs fonctionnant sous IOS.
syslogd	Le démon <i>syslogd</i> consigne des messages système dans un ensemble de fichiers définis par le fichier de configuration <i>/etc/syslog.conf</i> .
TACACS	<i>Terminal Access Controller Access Control System</i> (Système de contrôle d'accès de contrôleur d'accès de terminal).
trap	Interception. Il s'agit d'un événement SNMP.
VLAN	LAN virtuel.
VMPS	<i>VLAN Membership Policy Server</i> (serveur de stratégie d'adhésion VLAN).
VTP	<i>VLAN Trunk Protocol</i> (protocole de tronçon VLAN). Un protocole de messagerie de niveau 2 qui maintient la cohérence de la configuration VLAN à travers le réseau.

D'autres acronymes concernant la famille de Catalyst 5000 peuvent être trouvés sur le site Web de Cisco.

Introduction à l'administration de réseau

L'*administration de réseau* est la mise en application de techniques de gestion des équipements dédiés à la communication en réseau, tels que les commutateurs, les routeurs, les hubs, et d'autres dispositifs de connexion formant l'infrastructure de réseau.

L'organisme de normalisation ISO a aidé à simplifier la séparation des activités de gestion de réseaux en identifiant cinq domaines principaux :

- gestion des erreurs ;
- gestion de la configuration ;
- gestion de la comptabilité ;
- gestion des performances ;
- gestion de la sécurité.

Le site Web de Cisco donne un aperçu de ces domaines fonctionnels ainsi qu'une introduction à la conception de réseaux.

Etant donné qu'il existe déjà plusieurs ouvrages consacrés à la gestion des réseaux, ce chapitre est uniquement consacré aux domaines de gestion des erreurs et des performances tels qu'ils s'appliquent aux commutateurs et routeurs Cisco.

Présentation technique des équipements Cisco

Cette section couvre les notions de base sur l'implémentation Cisco de certains protocoles et fonctions. Elle pose les fondations pour le reste de ce chapitre.

Introduction aux commutateurs

Un commutateur Catalyst est un équipement de pontage multiport. L'architecture de commutation de Cisco repose sur le concept de commutation multicouche, qui combine la simplicité d'emploi de la commutation de niveau 2 (pontage) entre stations d'un groupe de travail, avec la stabilité et la sécurité de la commutation de niveau 3 (routage) entre différents groupes de travail.

La commutation multicouche joue un rôle important dans les environnements commutés étendus affichant une croissance continue, pour les raisons suivantes :

- Elle offre un excellent débit car elle permet de fournir une bande passante dédiée aux utilisateurs individuels.
- Elle prévient les goulets d'étranglement provoqués par la commutation simple de niveau 2 lorsque plusieurs segments à 10 Mbit/s convergent vers des connexions individuelles à 10 Mbit/s en direction de serveurs et de routeurs.

Comme un commutateur est un pont multiport, chaque port représente un segment ou un anneau distinct avec une bande passante théorique de 10 Mo, à la différence du hub qui partage une capacité de 10 Mo entre tous ses divers ports.

Comme tous les ports communiquant sont pontés, chacun d'eux ne voit que le trafic broadcast, multicast, ou unicast qu'il reçoit ou envoie. Par conséquent, lorsqu'un équipement connecté au port 2 de commutateur communique avec un autre équipement connecté au port 3, aucun autre port ne verra le trafic échangé. Même un analyseur de réseau connecté au port 4 ne verrait pas les trames traversant ces ports.

Cette section décrit les différents composants et protocoles qui constituent un commutateur.

Le site Web Cisco fournit une introduction détaillée aux bases de la commutation.

Processeur et circuit ASIC (*Application-Specific Integrated Circuit*)

A l'instar des routeurs, les commutateurs sont dotés d'un processeur, et à l'inverse des routeurs, ils assurent la transmission de la majorité des paquets sans solliciter le processeur. Les décisions de commutation sont réalisées au niveau du circuit ASIC, et selon le type de commutateur, la table de pontage peut aussi être stockée sur ce circuit.

Certaines des opérations réalisées par le processeur du commutateur incluent la gestion de l'arbre recouvrant (*Spanning-Tree*), des services Telnet, du protocole CDP, de la sécurité (comme avec TACACS), de la surveillance à distance (RMON), du protocole VTP (*VLAN Trunk Protocol*), de l'agrégation de ports, des VLAN dynamiques, et de SNMP.

Par conséquent, mesurer la capacité du processeur d'un commutateur importe peu pour déterminer les performances de ce dernier en matière de transmission de paquets.

Table CAM (*Content-Addressable Memory*)

Certains ponts/commutateurs gardent trace des ports sur lesquels ils ont reçu certaines adresses MAC (*Media Access Control*) afin d'isoler les conversations unicast sur les ports impliqués. Dans d'autres situations, tout le trafic unicast et broadcast est transmis vers tous les ports commutés, ce qui s'avère excessif. Cette fonction de suivi est traditionnellement mise en œuvre en utilisant une base de données de transmission (parfois appelé une table de pontage) et des tables CAM.

La base de données de transmission est habituellement une simple table ou base de données centralisée dans laquelle le pont place toutes les adresses MAC (et leurs ports) qu'il découvre pour pouvoir ensuite pour transmettre les paquets sur les ports appropriés.

La table CAM est une mémoire accessible par son contenu (par opposition à un accès par adresse). Chaque port physique dispose de sa propre table CAM. Dans le mode non transparent (*non-promiscuous mode*), c'est-à-dire en l'absence de pontage, la CAM contient l'adresse MAC gravée à l'origine sur la carte réseau (NIC, *Network Interface Card*) ainsi que d'autres adresses programmées (multicast, broadcast) qu'elle doit écouter. Tout paquet ne faisant pas l'objet d'une recherche CAM concluante est supprimé.

Les ponts opèrent en mode transparent ou sans distinction (*promiscuous mode*), ce qui signifie que la CAM sur chaque port est initialement nettoyée pour que toutes les adresses soient acceptées. A mesure que la table de transmission se construit, la CAM d'un port se remplit avec les adresses MAC des stations qui génèrent du trafic sur ce port. Dans ce mode, les paquets reçus sur un port et comportant une adresse de destination pour laquelle une entrée existe dans la CAM du port, sont rejettés, c'est-à-dire qu'ils ne traversent pas le pont. Lorsque la CAM contient des adresses MAC, la lecture d'une entrée peut être réalisée de façon sélective. Cette procédure est plus rapide qu'une recherche séquentielle dans la base de transmission. De nombreuses cartes réseau possèdent une CAM, mais le commutateur Catalyst 5000 n'en possède pas sur ses ports Ethernet.

Sur le Catalyst 5000, le terme "CAM" est utilisé pour des raisons historiques, car en réalité il n'existe pas de CAM. En effet, il utilise un circuit de reconnaissance d'adresses avancée central, appelé EARL (*Enhanced Address Recognition Logic*), qui permet d'améliorer les performances et d'apporter des fonctionnalités additionnelles en combinant l'identifiant VLAN avec l'adresse MAC lors de l'exécution des fonctions de découverte et de recherche. Ce circuit regroupe les fonctions de la base de transmission (liste complète centralisée de toutes les adresses MAC, des identifiants

VLAN, et des ports) et celles de la CAM (consultation rapide par contenu au lieu d'une recherche séquentielle). Les adresses MAC sont stockées sur une puce SRAM située sur le moteur superviseur et leur usage n'affecte pas l'utilisation de la mémoire ou du processeur sur le NMP (*Network Management Processeur*, processeur de gestion de réseau). La puce est dotée de suffisamment de SRAM pour pouvoir stocker 16 000 adresses MAC.

Chemin d'un paquet

Généralement, le chemin parcouru par un paquet à travers le commutateur ressemble à ce qui suit :

1. Le commutateur reçoit un paquet sur un port donné.
2. Il recherche l'adresse MAC de destination et la compare aux entrées contenues dans la base de transmission. Il enregistre dans la table CAM (de pontage) l'adresse MAC source ainsi que le port sur lequel il a reçu le paquet.
3. Si l'adresse de destination est une adresse unicast qui a été enregistrée dans la table CAM, le commutateur transmet le paquet en sortie sur le port de destination associé s'il s'agit d'un port différent.
4. Si l'adresse de destination ne se trouve pas dans la table ou s'il s'agit d'une adresse broadcast ou multicast, le commutateur transmet le paquet sur tous ses ports à l'exception de celui sur lequel il a été reçu.

Toutes ces opérations sont réalisées sans affecter le processeur principal du commutateur.

Pont transparent et pont traducteur

Lorsque le pontage est mis en œuvre, les commutateurs Catalyst peuvent réaliser à la fois un pontage transparent et un pontage traducteur.

Le premier type de pontage désigne la transmission du trafic provenant d'un port d'un type de réseau donné, comme Ethernet, vers un autre port de même média. Un paquet ainsi acheminé d'un port d'entrée vers un port de sortie pour un même média n'est pas modifié.

Le deuxième type de pontage va plus loin en permettant de transmettre le trafic d'un média donné vers un média de destination différent, comme de Ethernet vers FDDI. Cette fonction nécessite une étape de traduction du paquet, qui comprend au minimum le remplacement d'une partie des informations du paquet relatives à une certaine topologie par celles relatives à une autre topologie. Un temps supplémentaire de traitement est donc nécessaire pour recevoir le paquet, l'analyser, et le traduire avant de le transmettre vers la destination.

Réseaux et services VLAN

Un VLAN est un domaine de broadcast défini administrativement qui peut englober plusieurs commutateurs. Les stations d'un VLAN reçoivent uniquement les paquets qui sont envoyés en mode unicast, broadcast, ou multicast (inondés) sur ce VLAN. Un tel réseau virtuel améliore les performances en limitant l'échange de trafic aux stations qui en font partie et en bloquant le trafic des autres VLAN. Cette technologie peut permettre la mise en place d'une barrière de sécurité (*firewall*) entre les stations finales de différents VLAN sur un même commutateur.

Les commutateurs Catalyst incluent les composants de VLAN suivants :

- **Tronçons VLAN.** Permettent d'étendre des réseaux VLAN à partir d'un commutateur Catalyst à un ou plusieurs routeurs ou autres commutateurs Catalyst au moyen d'interfaces à haute vitesse, telles que Fast Ethernet, FDDI, et ATM. Deux protocoles de tronçons de VLAN sont supportés actuellement (du moins à l'époque de la conception de l'ouvrage) : ISL (*Inter-Switch Link*) pour Ethernet et Fast Ethernet, et 802.10 pour FDDI.
- **FastEtherChannel.** Permet la répartition du trafic sur plusieurs tronçons ISL Fast Ethernet parallèles. En configurant des paramètres d'arbre recouvrant basés sur une organisation par VLAN, vous pouvez définir les VLAN qui sont actifs sur un tronçon et ceux qui devraient emprunter le tronçon comme solution de secours en cas de défaillance.
- **VTP (*VLAN Trunk Protocol*).** Permet de maintenir une désignation cohérente et une connectivité entre tous les équipements d'un domaine administratif. Lorsque de nouveaux VLAN sont ajoutés à un commutateur Catalyst 5000 dans un domaine, le VTP distribue automatiquement ces informations à tous les équipements qui en font partie. Le VTP est transmis sur toutes les connexions de tronçons, incluant ISL, 802.10, et ATM LANE (*LAN Emulation*). En utilisant plusieurs serveurs VTP pour assurer la modification et la maintenance des informations de VLAN, vous pouvez implémenter une redondance dans un domaine de réseau. Seuls quelques serveurs VTP sont nécessaires sur un grand réseau. Sur un petit réseau, tous les équipements sont généralement des serveurs VTP. La version 3.1 de Software Release pour la série de Catalyst 5000 supporte la version 2 de VTP, qui est une extension de la version 1.

Protocole STP (*Spanning-Tree Protocol*)

Lors de la création d'un réseau implémentant la tolérance aux pannes, un chemin exempt de boucles doit exister entre tous ses nœuds. Un algorithme par arbre recouvrant (Spanning-Tree) est utilisé pour calculer le meilleur chemin sans boucle à travers un réseau commuté au moyen de commutateurs Catalyst. Les paquets STP sont envoyés et reçus régulièrement par les commutateurs du réseau. Ceux qui participent à l'arbre ne transmettent pas les paquets, mais les traitent pour déterminer l'arbre lui-même. Le protocole de pont IEEE 802.1D, ou STP, assure cette fonction pour les commutateurs Catalyst.

La famille de commutateurs Catalyst peut utiliser STP sur tous les VLAN. Ce protocole détecte et interrompt les boucles en plaçant certaines connexions en mode de veille, qui sont activées en cas de défaillance. Un arbre recouvrant séparé est mis en œuvre sur chaque VLAN configuré afin de garantir la validité des topologies de niveau 2 sur le réseau.

Ce protocole supporte plusieurs états de port :

- désactivé ;
- en transmission ;
- en apprentissage ;
- en écoute ;
- bloquant.

L'état de chaque port est défini initialement lors de la configuration puis modifié ultérieurement par le processus STP. Après configuration de l'état du port, la spécification 802.1D (RFC 1493) détermine si le port transmet ou bloque les paquets.

Analyseur de port commuté SPAN

La fonction SPAN (*Switched Port Analyzer*) permet de surveiller le trafic sur n'importe quel port au moyen d'un dispositif d'analyse ou de sondage RMON. La fonction E-SPAN (*Enhanced SPAN*) permet d'analyser le trafic de plusieurs ports d'un même VLAN.

SPAN redirige le trafic d'un port Ethernet, Fast Ethernet, FDDI, ou VLAN vers un port Ethernet ou Fast Ethernet à des fins d'analyse ou de dépannage. Vous pouvez effectuer le suivi d'un seul port ou VLAN à l'aide d'un analyseur dédié tel qu'un *sniffer général de réseau*, ou d'une sonde RMON comme Cisco SwitchProbe.

Introduction aux routeurs

Les routeurs sont des équipements de commutation de niveau 3. Le routage inclut deux activités : la détermination d'itinéraires de routage optimaux à travers un réseau et le transport (ou la commutation) de groupes d'informations (généralement appelés paquets) à travers un réseau. La commutation est un processus relativement simple, contrairement au routage qui peut être très complexe. Les algorithmes de routage peuvent être différenciés grâce à plusieurs caractéristiques essentielles. Tout d'abord, les objectifs particuliers du concepteur de l'algorithme influent sur le comportement du protocole de routage résultant. Deuxièmement, chaque algorithme a un impact différent sur le réseau et les ressources du routeur. Pour finir, ils utilisent des métriques variées qui affectent le calcul des routes optimales.

Vous trouverez une présentation détaillée des fondements du routage sur le site Web Cisco.

Introduction aux commutateurs de niveau 3

Les commutateurs de niveau 3 combinent les technologies de routage et de commutation pour assurer une commutation de niveaux 2 et 3.

Technologies communes aux commutateurs et aux routeurs

Cette section décrit deux protocoles communs aux commutateurs et aux routeurs et qui permettent d'élaborer une représentation complète des équipements de niveaux 2 et 3 sur le réseau.

Protocole CDP (*Cisco Discovery Protocol*)

Le protocole CDP est indépendant du média et du protocole et peut fonctionner sur tous les équipements Cisco, dont les routeurs, les ponts, les serveurs d'accès et de communication, et les commutateurs. Avec CDP, les applications d'administration de réseau peuvent obtenir le type d'équipement et l'adresse de l'agent SNMP des équipements voisins, ce qui leur permet d'envoyer des requêtes SNMP à ces derniers.

CDP a été conçu pour répondre à un besoin né de l'existence de protocoles transparents virtuels de niveau inférieur. Il permet aux applications d'administration de réseau de découvrir des équipements Cisco qui sont adjacents à d'autres équipements déjà connus, en particulier ceux exécutant

des protocoles transparents de niveau inférieur. Il fonctionne sur tous les médias qui supportent le protocole SNAP (*Subnetwork Access Protocol*), y compris sur les réseaux LAN et Frame Relay. Il opère uniquement au niveau de la couche liaison de données, pas au niveau réseau. Avec CDP, deux systèmes supportant des protocoles de niveau réseau différents peuvent se découvrir l'un et l'autre.

Les informations CDP placées en cache sont disponibles pour les applications d'administration de réseau. Les équipements Cisco ne transmettent jamais un paquet CDP. Lorsque de nouvelles informations sont reçues, les anciennes sont alors ignorées. Les outils CiscoWorks pour interréseaux commutés (CSWI, *CiscoWorks for Switched Internetworks*) exploitent ces renseignements lors de la découverte du réseau.

Le protocole CDP est également très utile pour le dépannage. Sur un réseau composé seulement de routeurs, les tables ARP (*Address Resolution Protocol*), les tables de routage, ainsi que d'autres informations, sont utilisées pour découvrir la topologie ou pour confirmer la connectivité de celle qui est déjà connue. Sur un réseau de ponts, ces tables ne sont pas utilisées et l'on utilise à la place une base de données de transmission (qui n'est pas utile pour découvrir les ponts car elle sert pour les stations finales) et des informations d'arbre recouvrant (qui peuvent être désactivées, et sont communiquées uniquement en amont vers la racine). CDP est capable de découvrir tous les équipements Cisco voisins et peut fournir des informations telles que le nom d'hôte, la version du système Cisco IOS, et l'adresse IP de gestion.

Visitez le site Web Cisco pour obtenir des informations sur la configuration de CDP sur un commutateur Catalyst 5000.

Fonction RMON imbriquée

Le RFC 1757 définit une partie de la base d'informations d'administration MIB (*Management Information Base*) pour le suivi des informations de couche liaison de données de segments distants, et plus particulièrement des caractéristiques de trafic et des taux d'erreurs.

Les équipements de surveillance de réseaux à distance, souvent appelés *moniteurs* ou *sondes*, sont des instruments qui existent uniquement dans le but d'administrer un réseau. Il s'agit souvent d'équipements autonomes qui consacrent une quantité significative de leurs ressources internes à la gestion de réseau. Une entreprise peut déployer un grand nombre de ces dispositifs, un par segment de réseau, pour administrer son interréseau. De plus, ils peuvent permettre à un fournisseur de services d'administration de réseau d'accéder aux réseaux de clients souvent éloignés géographiquement.

Les objets définis dans le RFC 1757 sont prévus pour servir d'interface entre un agent RMON et une application d'administration RMON et n'ont pas été conçus pour être manipulés directement par des utilisateurs. Bien que certains puissent tolérer l'affichage direct de certains de ces objets, peu accepteront la complexité liée à la manipulation directe des objets pour créer des lignes. Ces fonctions devraient être gérées par l'application d'administration. Cisco propose des applications pour assurer ces fonctions.

La fonction RMON, comme décrite dans le RFC 1757, est implémentée sur les produits Catalyst et les routeurs Cisco de la façon suivante :

- sous la forme de statistiques, d'historiques, d'alarmes, et d'événements (des neuf groupes RMON) sur des segments Ethernet des commutateurs de groupe de travail Catalyst 5000 ou

- 5500 avec la version 2.1 ou ultérieure de Software Release, et sur tous les commutateurs de groupe de travail Catalyst 2900 ;
- sous la forme de statistiques, d'historiques, d'alarmes, et d'événements (des neuf groupes RMON) sur des segments Ethernet des commutateurs Catalyst 1900 et 2820 avec la version 5.33 ou ultérieure de Software Release ;
 - sous la forme de statistiques, d'historiques, d'alarmes, et d'événements (des neuf groupes RMON) sur des segments Ethernet des commutateurs de groupe de travail Catalyst 3000 (3000, 3100, et 3200) ;
 - tous les neufs groupes RMON sur des segments Ethernet des commutateurs de groupe de travail Catalyst 1200 avec Software Release supportant DMP et NMP version 3.1 ou ultérieure ;
 - le système IOS version 11.1 ou ultérieure supporte les fonctions EtherStats, EtherHistory, d'alarmes, ainsi que de groupes MIB d'événements.

Protocole d'administration de réseau

Cette section aborde l'utilisation des protocoles d'administration de réseau reconnus comme standards de l'industrie pour gérer des réseaux Cisco.

Protocoles de base

Quatre types de protocoles sont disponibles pour administrer des équipements Cisco :

- Telnet ;
- SNMP ;
- RMON ;
- Syslog.

Telnet

Telnet (également connu sous le nom de CLI) permet de se connecter directement à un commutateur ou à un routeur pour accéder aux commandes de configuration et de surveillance.

SNMP

Comme défini dans le RFC 1157, le protocole SNMP s'appuie sur un concept de gestionnaire SNMP communiquant avec un ou plusieurs agents SNMP. Les opérations Get, Get-Next, et Set de SNMP sont réalisées par le gestionnaire vers un agent pour recueillir ou définir des variables d'administration supportées par ce dernier. Les informations d'administration disponibles via SNMP et Telnet sont généralement identiques. Les agents SNMP peuvent avertir le gestionnaire au moyen d'interceptions (*traps*), pouvant contenir n'importe quelle quantité d'informations d'administration afin de mieux qualifier leur objectif.

RMON

Fondées sur la technologie SNMP, les fonctions de suivi de réseaux à distance sont assurées par un ensemble de données RMON dédiées et un moteur de suivi situé sur un équipement. La communication

— par exemple, la définition de règles de collecte et la réception de notifications de la part du moteur — est mise en œuvre via SNMP. RMON opère au niveau des couches ISO 1 et 2, et RMON2 opère au niveau de la couche ISO 4 et des couches supérieures.

Syslog

Le protocole Syslog est utilisé par les équipements Cisco pour émettre des notifications non sollicitées vers une station d'administration. Bien que semblable aux interceptions SNMP, il sert uniquement à la notification d'événements. L'objet CISCO-SYSLOG-MIB est implémenté sur les équipements Cisco comme solution alternative à l'émission de messages Syslog pour autoriser n'importe quel gestionnaire SNMP à recevoir tous les événements via SNMP.

Présentation du modèle d'événements

Cette section présente le modèle d'événements conceptuel de Cisco tel qu'il est appliqué sur ses équipements. Nous commencerons par une introduction des types d'événements disponibles sur ses commutateurs et ses routeurs.

Types d'événements

Tous les équipements Cisco génèrent des interceptions SNMP pour avertir les applications NMS de certaines conditions d'activité et d'erreurs. De plus, les équipements utilisant le système IOS génèrent des messages Syslog.

Messages Syslog

La fonction de journalisation Syslog du système IOS est identique à celle d'Unix. Il s'agit d'un mécanisme de journalisation basé sur UDP permettant aux applications et aux systèmes d'exploitation de rapporter des conditions d'activité ou d'erreurs. Tous les routeurs et la plupart des commutateurs génèrent des messages Syslog. Ceci signifie que n'importe quelle station d'administration Unix (de préférence la station d'administration du réseau Unix) peut servir de serveur Syslog pour n'importe quel équipement Cisco. Lors de la journalisation, chaque message Syslog est accompagné d'informations de temps, de service, de niveau de gravité, et d'une description.

Interceptions SNMP

Visitez le site Web Cisco pour obtenir une liste de toutes les interceptions SNMP supportées par Cisco. Celles-ci peuvent également être obtenues dans les fichiers MIB de Cisco.

Interceptions SNMP publiques et privées. Tous les équipements Cisco génèrent des interceptions SNMP. De plus, comme la plupart d'entre eux gèrent la fonction d'alarme standard RMON et les groupes d'événements MIB, une fonction supplémentaire d'interrogation locale de n'importe quelle variable MIB peut être configurée sur un équipement pour assurer le suivi des seuils et générer des interceptions SNMP selon les besoins.

Interceptions SNMP Syslog. De plus en plus de routeurs Cisco implémentent la fonction MIB Syslog de Cisco pour générer des interceptions SNMP, à la place ou en plus des messages Syslog. Elle optimise l'administration des équipements Cisco par l'intermédiaire de SNMP en ajoutant un

plus grand nombre de messages non sollicités pouvant être reçus par un processeur NMP, améliorant ainsi l'administration des routeurs.

Pour activer les interceptions Syslog sur un routeur, exécutez la commande suivante :

```
snmp-server enable traps syslog
```

La commande suivante spécifie le niveau de messages à envoyer :

```
logging history niveau
```

Événements de plate-forme

Les plates-formes SNMP peuvent générer leurs propres événements ou interceptions suite à l'interrogation distante d'objets MIB spécifiques et de l'application de seuils à ces objets. De plus, des moteurs de corrélation d'événements et des applications de reporting sur les performances de réseau peuvent aussi générer leurs propres événements à destination du NMP.

Traitement des événements

Le traitement des événements est caractérisé par les quatre activités décrites ci-après.

Collecte d'événements

L'essentiel pour pouvoir tirer parti d'un moteur de corrélation d'événements complet, est de l'alimenter avec autant d'événements que possible afin d'obtenir le niveau maximal de filtrage et de corrélation désiré.

Un moteur affichant de hautes performances est nécessaire pour pouvoir accepter tous les événements reçus. Il doit pouvoir traiter les interceptions SNMP et les messages Syslog.

Compréhension des événements

Le traitement et le reporting d'événements doivent être accompagnés d'une explication détaillée pour chaque événement et de sa relation avec le fonctionnement de l'équipement, et éventuellement du réseau.

Filtrage des événements

Les événements excessifs et répétés finissent généralement par encombrer le système d'administration du réseau à un tel point que les opérateurs préfèrent désactiver la fonction et s'appuyer sur leur intuition et les plaintes des utilisateurs. Par conséquent, il est important de fournir un moyen efficace de réduction du nombre des événements rapportés aux opérateurs en supprimant les messages répétitifs (par exemple, les messages identiques qui se répètent dans un intervalle de temps donné) et en éliminant les événements de basse priorité (par exemple, ceux dont la transmission est jugée inutile par l'opérateur).

Corrélation d'événements

Après avoir filtré les événements, il est important de toujours évaluer la nature et le niveau de gravité de chaque événement par rapport à un équipement ou à d'autres événements. Un événement signalant qu'un routeur est inopérant peut être temporairement ignoré si, par exemple, vous savez qu'il est en train de redémarrer suite à une erreur logicielle. S'il n'est pas de nouveau en ligne après cinq minutes, l'opérateur doit toutefois être immédiatement averti.

Modèle d'événements Cisco

Cette section introduit un modèle permettant de gérer un volume élevé d'interceptions et de messages Syslog et de les corrélérer avec votre réseau, faisant de ces informations un outil et non plus une gêne.

Modèle d'événements théoriques

Le modèle d'événements proposé ici est un modèle conceptuel permettant la corrélation des événements Cisco. Il suppose que les interceptions SNMP et les messages Syslog sont générés directement par l'équipement ou bien en résultat de la gestion de seuils SNMP via l'alarme RMON et les groupes d'événements. Tous ces types d'événements servent à alimenter le modèle d'événements.

Tous les événements sont d'abord filtrés pour éliminer le plus grand nombre possible d'événements jugés sans intérêt par rapport à une base de connaissances. Cette opération réduit le traitement qui sera nécessaire dans des phases suivantes du modèle de gestion d'événements.

Les événements jugés intéressants sont ensuite normalisés selon une forme commune pour faciliter le traitement dans le moteur de corrélation d'événements. La normalisation peut également nécessiter la modification du niveau de gravité d'un événement pour qu'il reflète une priorité plus précise par rapport à un site spécifique.

Le moteur de corrélation inclut plusieurs conditions de corrélation pouvant éliminer les événements, les transmettre directement systématiquement, les transmettre directement uniquement si une ou plusieurs conditions se produisent dans un intervalle de temps spécifique, les modifier, ou en créer de nouveaux. Chaque condition est spécifique à un équipement, un type d'équipement, ou à tous les équipements selon la portée des règles de corrélation. Celles-ci peuvent utiliser des informations externes, comme celles qui renseignent sur une topologie physique ou logique, afin de mieux isoler un équipement fautif. Les règles peuvent également provoquer l'émission de requêtes supplémentaires vers un ou plusieurs équipements si davantage d'informations sont requises à n'importe quel stade de leur application.

La Figure 14.1 illustre le modèle conceptuel.

Bien qu'elle présente des commandes CLI utilisées pour communiquer avec un équipement, cette option n'est généralement pas nécessaire car les messages Syslog et les objets MIB SNMP fournissent toutes les informations requises pour gérer ces équipements.

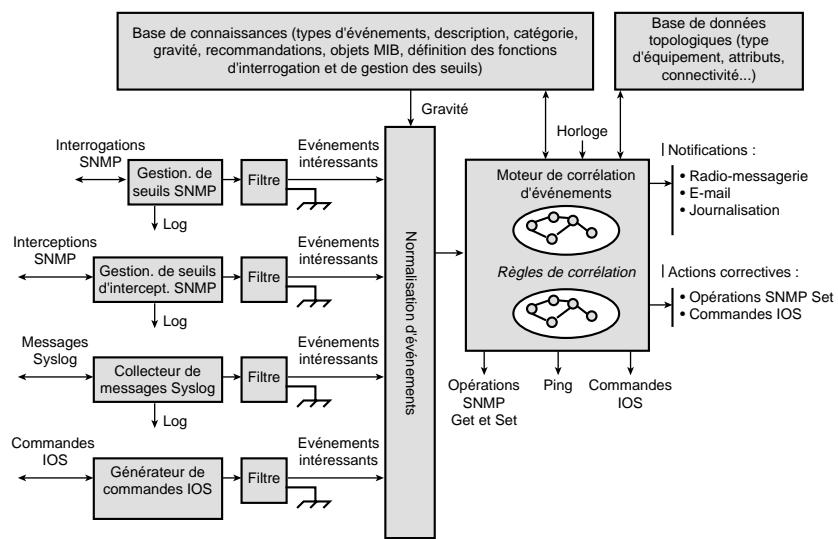
Systèmes de corrélations d'événements tiers

Chaque système de corrélation d'événements ou ECS (*Event Correlation System*) dispose de sa propre méthode de mise en correspondance du modèle conceptuel de Cisco avec son implémentation propriétaire. L'implémentation du modèle dans un moteur de corrélation tiers peut nécessiter une programmation supplémentaire ou l'écriture de scripts selon les capacités du moteur.

Le Tableau 14.2 identifie les composants du modèle Cisco décrits précédemment qui peuvent exister dans un moteur de corrélation tiers.

Figure 14.1

Modèle d'événements conceptuel de Cisco.

**Tableau 14.2 : Composants du modèle d'événements Cisco**

<i>Composant</i>	<i>Correspondance dans le moteur de corrélation</i>
Base de connaissances	Il s'agit d'une base de données relationnelle contenant tous les messages Syslog et les recommandations du système IOS de Cisco, ainsi que les interceptions SNMP de Cisco. Elle devrait être constituée à partir de la base de connaissances de messages Syslog existante de Cisco et d'autres programmes ou tables de correspondances de niveaux de gravité.
Base de données topologiques	Cette topologie est généralement disponible à partir de la plate-forme NMS par l'intermédiaire d'API publiées ou d'une fonction d'exportation.
Gestionnaire de seuils SNMP	Cette fonction est supportée soit au moyen de la plate-forme ou du moteur d'interrogation, soit par l'intermédiaire de la fonction d'alarme RMON intégrée et des groupes d'événements MIB.
Collecteur d'interceptions SNMP	Cette fonction est supportée soit par l'intermédiaire de la plate-forme existante, soit au moyen du collecteur d'interceptions du moteur de corrélation.
Collecteur de messages Syslog	Un module personnalisé prévu pour recevoir et analyser de façon appropriée les messages Syslog.
Générateur de commandes IOS	Il s'agit généralement d'un client Telnet. Il peut être fourni sous forme de scripts ou être intégré au moteur de corrélation.

Tableau 14.2 : Composants du modèle d'événements Cisco (suite)

Composant	Correspondance dans le moteur de corrélation
Normalisation d'événements	Chaque plate-forme ou moteur possède ses propres méthodes pour normaliser un événement.
Opérations SNMP Get et Set	Elles peuvent apparaître sous forme de scripts ou être intégrées à la plate-forme NMS ou au moteur de corrélation.
Requêtes ping (ICMP)	Elles peuvent être fournies sous forme de scripts ou être intégrées à la plate-forme NMS ou au moteur de corrélation.
Commandes IOS	Il s'agit généralement d'un client Telnet. Elles peuvent apparaître sous forme de scripts ou être intégrées au moteur de corrélation.
Objets MIB	Les objets MIB Cisco peuvent être téléchargés vers la plate-forme NMS ou dans le moteur de corrélation et servir de fondements pour la base de connaissances.
Notifications par radio-messagerie	Le courrier électronique est généralement supporté par la plate-forme NMS ou par le moteur de corrélation. Les systèmes de radio-messagerie sont généralement proposés par des fournisseurs tiers.
Actions correctives	Elles peuvent être invoquées à partir de la plate-forme NMS ou du moteur de corrélation lorsqu'une règle de corrélation est évaluée comme vraie dans le cadre d'une tentative de correction de la condition fautive.

Etant donné que la plupart des procédures de gestion d'erreurs impliquent leur détection et l'analyse des causes originelles, ce chapitre attache moins d'importance aux actions de correction automatiques.

Directives d'administration de réseau

Cette section présente une série d'étapes visant à implémenter une gestion efficace du réseau.

Conception efficace et armoires de câblage sécurisées

L'administration efficace d'un réseau commence par une conception efficace. Cette approche implique les étapes suivantes :

- Sécuriser les armoires de câblage et contrôler les accès. Une armoire non verrouillée est une source de problèmes.
- Documenter le réseau physique, en incluant les équipements et le câblage. Vous devez connaître les équipements connectés aux différents ports de chaque commutateur et routeur et être capable d'identifier les câbles connectés à ces équipements.

- Définir et appliquer des stratégies de déplacement, d'ajout, et de changement de matériel, dans lesquelles les modifications du réseau doivent être consignées et planifiées par avance chaque fois que cela est possible. Des cartes physiques et des inventaires devraient toujours refléter les changements.

Identification des ports jugés "critiques"

Comme le prix des commutateurs est de plus en plus abordable, ils tendent à remplacer les hubs et les MAU (*Media Attachment Unit*) dans les armoires de câblage. Généralement, les clients opèrent une migration de leurs réseaux basés sur des hubs en remplaçant les ports de ces derniers par des ports de commutateurs. Les utilisateurs et les serveurs subissent une migration progressive par le transfert de chaque connexion d'un port de hub vers un port de commutateur.

Le domaine de broadcast ou le segment Ethernet qui était traditionnellement utilisé pour la surveillance n'existe plus. Il s'agissait d'un média partagé sur lequel n'importe quel port pouvait permettre à un utilisateur muni d'un analyseur d'obtenir une vue complète de ce qui se produisait au niveau du trafic. Dans un environnement commuté, le domaine de broadcast (VLAN) peut s'étendre sur plusieurs commutateurs, armoires de câblage, et immeubles. Le trafic unicast et parfois multicast est limité aux ports auxquels il se destine.

Habituellement, un analyseur de trafic peut être utilisé pour observer tout le trafic sur un segment et déterminer les équipements qui sont les plus utilisés, surchargés, sous-exploités, etc. Dans un environnement commuté, une telle vue d'ensemble n'est possible nulle part sur le réseau. Le trafic sur chaque port d'un VLAN est différent à l'exception des ports qui ne possèdent qu'un équipement actif, le commutateur. Même si un port SPAN était utilisé, il indiquerait ce qui se passe sur un seul commutateur, ce qui ne représente qu'une partie d'un VLAN implémenté sur plusieurs commutateurs.

Bien que le taux des diffusions broadcast limite toujours la croissance d'un VLAN, comme c'était déjà le cas sur un média partagé, il ne représente qu'un aspect parmi d'autres. Comme il n'est pas pratique d'analyser chaque port commuté pour obtenir une vue complète, nous devons identifier, documenter, et maintenir uniquement les ports commutés jugés critiques.

Un port commuté critique est un port dont le fonctionnement est vital pour l'exploitation du réseau. Par exemple, les connexions de ports suivantes sont d'une importance capitale :

- ports de serveur de fichiers et d'applications ;
- ports de routeur ;
- ports de tronçon ;
- ports de ligne vitale (pour ces employés dont les ports ne devraient jamais tomber en panne).

Les ports de clients (à l'exception de ceux de ligne vitale) ne devraient jamais être considérés comme critiques. Tenter de maintenir des données d'administration pour tous ces ports peut se révéler une tâche laborieuse pouvant surcharger les ressources du commutateur. De plus, obtenir une alerte à chaque fois qu'un utilisateur éteint son PC n'est d'aucune utilité comparé à un avertissement signalant qu'un port de tronçon ou de routeur a été désactivé de façon imprévue.

Une fois les ports critiques identifiés, ils doivent être documentés, marqués physiquement, et maintenus par l'intermédiaire d'une stratégie administrant les déplacements, les ajouts, et les changements.

Sinon, les opérateurs risquent de réagir à des conditions de ports qui étaient auparavant critiques mais qui ne le sont plus suite à un changement n'ayant pas été documenté.

Les sections suivantes traitent des stratégies d'administration pour les ports critiques. L'établissement de rapports sur la disponibilité du réseau par équipement ou par port critique de commutateur peut fournir à la direction de l'entreprise une référence importante à partir de laquelle effectuer des décisions.

Mise en place du suivi d'erreurs

Le suivi d'erreurs consiste à surveiller la disponibilité du réseau, journaliser et traiter les interceptions SNMP ainsi que les messages Syslog. Si ce n'est pas déjà le cas, vos équipements devraient être configurés pour pouvoir gérer les accès SNMP, la génération des interceptions SNMP, et la génération des messages Syslog avec des informations de temps. Synchronisez les horloges sur vos équipements et votre station d'administration NMS (*Network Management Station*) avec NTP pour améliorer les capacités de corrélation d'événements.

Surveillance de la disponibilité

La méthode la plus simple pour contrôler la disponibilité des équipements est de vérifier les réponses renvoyées après une requête **ping** (ICMP) ou **get** de SNMP. Les produits NMS standards peuvent assurer le suivi de tous les objets qu'ils gèrent par l'intermédiaire de ces mécanismes simples. Bien qu'une réponse **ping** ne garantit pas qu'un commutateur fonctionne correctement, l'absence d'une telle réponse révèle manifestement un problème. L'utilisation d'un dispositif NMS avec contrôle de disponibilité lié à la couleur d'équipement sur une carte topologique est l'exemple le plus courant d'un système de contrôle d'erreurs.

Mise en place de la journalisation Syslog

Configurez les routeurs et les commutateurs pour qu'ils envoient leurs messages de console vers un serveur Syslog, généralement la station NMS. Un commutateur Catalyst 5000 peut placer dans un tampon de 1 Ko les *n* derniers messages Syslog de console qu'il génère. Bien qu'ils soient utiles pour une référence rapide à partir de l'interface en ligne de commande (CLI), il est recommandé de consigner ces messages sur un serveur Syslog pour disposer d'informations permanentes et pouvoir les corrélérer ultérieurement.

Les messages de journaux sont des messages système qui seraient normalement envoyés sur le port de console, par exemple : *11/4/1996, 13:52:54:SYS-5: Module 3 failed configuration* (échec de configuration du module 3). Les routeurs et les commutateurs Cisco génèrent de nombreux types de messages système différents.

Les messages Syslog de commutateur sont formatés avec deux paramètres : le service et la gravité. Vous devez choisir parmi huit services (*local0* à *local7*), en vous fondant sur ceux que le serveur Syslog consigne déjà. Il est préférable de choisir un service qui sera dédié à vos équipements de réseau. Les routeurs Cisco choisissent par défaut *local7*, qui est un choix approprié, sauf en cas de conflit.

Vous pouvez configurer le niveau de gravité de chaque type de message que vous voulez que le commutateur envoie. Vous devriez consigner un niveau de gravité "avertissement" inférieur à celui

de chaque type de messages système afin de ne pas encombrer les journaux avec des messages superflus qui n'apporteraient pas d'informations utiles.

Bien que la fonction d'information Syslog puisse être utilisée pour la gestion des erreurs, elle ne représente pas un mécanisme d'alerte en temps réel, contrairement à une interception SNMP (à moins que vous n'effectuez un travail supplémentaire pour qu'elle le devienne). Les informations Syslog sont toutefois utiles pour la corrélation d'événements. L'analyse des fichiers Syslog à la recherche de messages se rapportant à un événement donné peut fournir des renseignements utiles sur la cause d'un problème. Vous pouvez configurer le serveur Syslog pour que les messages de différents niveaux de gravité soient consignés dans des fichiers différents ou dans un seul fichier volumineux. Vous pouvez ensuite utiliser des outils comme Perl pour y rechercher les informations souhaitées. Des outils comme le gestionnaire de ressources CRM (*Cisco Resource Manager*) peuvent collecter des informations Syslog et créer des rapports basés sur les niveaux de gravité et les dates. Ces outils peuvent également synthétiser les messages pour en faciliter l'interprétation.

Mise en œuvre des interceptions SNMP

Les interceptions SNMP représentent un mécanisme permettant à un équipement de signaler à un opérateur de réseau en temps réel et unilatéralement qu'une certaine condition est survenue. Il s'agit de notifications non sollicitées, indépendantes de toute activité d'interrogation SNMP. Les interceptions générées par les commutateurs et les routeurs Cisco fournissent des informations utiles sur les conditions d'environnement potentiellement nuisibles, l'état des processeurs, et celui des ports. Chaque équipement émet aussi des interceptions en se basant sur les fonctions qu'ils supporte. Par exemple, un commutateur Cisco déclenchera des interceptions SNMP de changement de topologie d'arbre recouvrant lorsqu'une configuration sera modifiée par l'ajout ou la suppression d'un tronçon ou d'un commutateur sur le réseau.

Au départ, il est recommandé d'autoriser les interceptions de module, de châssis, de pont, d'authentification, et d'activation et de désactivation de ports. Les interceptions au niveau port nécessitent l'activation des interceptions sur les ports jugés critiques avec la commande suivante :

```
set port trap module|port enable|disable
```

De nombreux produits NMS disposent de récepteurs d'interceptions qui les consignent et qui peuvent être configurés pour y réagir de façon relativement sophistiquée. Vous pouvez demander à être informé des interceptions au moyen d'une fenêtre surgissante, d'une alarme sonore, ou d'un signal électronique de pager.

Collecte de données de référence

Après avoir documenté le réseau, identifié les ports commutés critiques pour la bonne marche de l'organisation, et activé le suivi de l'état des commutateurs et des routeurs, il est temps d'étudier la vraie nature du réseau en surveillant régulièrement les données et en étudiant les flux du trafic.

En recueillant des informations de référence sur le réseau, vous obtiendrez une vue précise du trafic et disposerez de données pour évaluer la croissance du réseau dans le temps et les goulets d'étranglements. Avec le temps, cet ensemble d'informations pourra servir de référence pour fixer les seuils utiles à l'étape suivante (traitée dans la section "Définition de seuils"). Une base de valeurs de référence représente également un instrument précieux lorsque vous tentez de déterminer les causes de problèmes de performances.

La collecte de données de référence sur le réseau est également une étape essentielle en raison de l'importance croissante de la planification des ressources. Selon Optimal (www.optimal.com), 85 % des nouveaux déploiements d'applications échouent aux tests de conformité de niveau service. Voici quelques-unes des nombreuses raisons de cet échec :

- la complexité croissante des réseaux ;
- l'utilisation d'applications multimédias à forte bande passante et l'augmentation des applications produisant un trafic en rafales ;
- l'exploitation croissante du réseau pour des applications non dédiées à l'entreprise (trafic Internet et Web) ;
- l'augmentation du nombre d'entreprises mettant à jour leurs réseaux et applications existants au lieu d'en concevoir de nouveaux.

La constitution d'une base de référence est donc essentielle pour la planification des ressources. Elle permet aux administrateurs de réseau de comprendre le niveau actuel des performances, ce qui est crucial pour pouvoir envisager de nouvelles extensions du réseau ou des applications. Les valeurs de référence doivent être mises à jour au moins tous les trimestres pour identifier les ressources et les tendances.

Déterminez en premier lieu les informations que vous souhaitez observer dans la durée. Par exemple :

- l'utilisation des ressources processeurs ;
- la consommation de la mémoire ;
- l'utilisation des interfaces ;
- les taux d'erreurs, particulièrement les erreurs CRC ;
- le trafic multicast ;
- le trafic broadcast.

Ces informations doivent être collectées pendant une certaine période, et au minimum pendant deux semaines. Des mesures pouvant s'étaler jusqu'à deux mois peuvent renseigner sur les fluctuations normales qui doivent être prises en compte. Cette durée minimale permet d'enregistrer le "rythme" normal du trafic du réseau. Plus l'étude sera longue, puis il sera possible de voir apparaître les modèles réels de comportement du trafic sur le réseau. Les échantillons devraient être recueillis assez fréquemment pour pouvoir capturer précisément les fluctuations, mais pas trop non plus, pour éviter que ces variations ne faussent les résultats.

Après la collecte des données, vous pouvez écrire des scripts ou acquérir des programmes pour collationner les données et établir des rapports comparatifs permettant d'identifier les zones de problèmes ou celles de forte activité.

Vous pourriez par exemple collecter les informations de performances et d'erreurs pour les ports critiques de commutateurs et de routeurs toutes les quinze minutes pendant deux semaines. A l'issue de cette période de collecte, une analyse devrait mettre en évidence le trafic de référence et les taux d'erreurs pour chaque port important. Ces moyennes seront nécessaires pour les étapes suivantes.

Les données de référence peuvent être collectées de différentes façons :

- Utilisez l'interrogation (*polling*) SNMP pour collecter les données nécessaires. Employez les outils NMS pour déterminer des pourcentages de référence du trafic local et de celui traversant le campus, et allouez ensuite la bande passante selon les résultats obtenus. Il existe trois types de modèles de trafic qui devraient être analysés :
 - **Trafic local.** Le trafic qui est confiné à une petite portion du réseau.
 - **Trafic de niveau campus.** Le trafic qui traverse l'épine dorsale du réseau, ou un routeur, ou les deux.
 - **Trafic campus/Internet.** Le trafic échangé en sortie ou en entrée entre le campus et l'Internet.
- Utilisez des outils tels que TrafficDirector avec des fonctions RMON intégrées ou des sondes RMON externes telles que SwitchProbes pour collecter des informations statistiques et historiques Ethernet, Token Ring, FDDI, et ATM à partir des commutateurs et des routeurs. Bien que RMON 1 puisse surveiller le trafic jusqu'au niveau 3, les sondes RMON 2 peuvent être utilisées pour déterminer des valeurs de référence des couches supérieures du modèle OSI (*Open System Interconnection*). La base de référence recueillie dans un environnement de commutateurs ne s'applique généralement qu'au niveau physique et au niveau liaison de données de la pile OSI.
- Utilisez l'interface en ligne de commande (CLI) *via Telnet* pour collecter des statistiques. Ceci devrait être réalisé au moyen de scripts, comme ceux de Expect ou de Perl. NMS ou d'autres applications commerciales de collecte d'informations peuvent aussi être employées pour recueillir ces données par l'intermédiaire de SNMP.

Valeurs de seuils

Après avoir réuni une base de valeurs de référence, vous devriez maintenant avoir une idée de ce qui devrait être considéré comme un "comportement normal" pour différents segments de réseau, et en particulier pour les ports critiques. L'étape suivante consiste à configurer les seuils RMON. L'alarme et les groupes d'événements RMON vous permettent de définir des seuils provoquant l'envoi d'une interception SNMP par le commutateur lorsqu'ils sont franchis.

Pour contrôler la génération des alarmes, deux types différents de valeurs de seuils doivent être définis :

- **Valeurs de seuils en augmentation.** Elles provoquent la génération d'une alarme lorsque la valeur de l'objet MIB augmente jusqu'à dépasser le seuil.
- **Valeurs de seuils en diminution.** Elles provoquent la génération d'une alarme lorsque la valeur de l'objet MIB diminue et passe en-dessous du seuil.

Ces alarmes ne sont pas émises à chaque fois qu'un seuil est franchi. Il existe un mécanisme d'hystérésis permettant de limiter le nombre d'alarmes générées. Chaque seuil agit comme un mécanisme de réarmement pour autoriser le seuil opposé à générer une alarme. Par exemple, supposez que pour un port le seuil en augmentation soit configuré pour 40 %, et que le seuil en diminution soit défini à 25 %. L'utilisation du port est normalement proche de 20 %. Si elle augmente soudain pour atteindre 50 % puis redescend pour fluctuer entre 35 % et 50 %, une alarme sera envoyée uniquement la première fois que le seuil en augmentation sera franchi. Lors des fluctuations consécutives de 35 à 50 %, aucune alarme ne sera émise. Lorsque l'activité du port retombe aux alentours

de 20 %, le seuil en diminution est alors franchi. Une alarme est générée et le seuil en augmentation est réarmé. On peut ainsi en déduire que la situation à l'origine de la première alarme est passée. Ce mécanisme empêche la réception d'informations redondantes sur une condition déjà connue et permet aussi d'être renseigné sur la fin d'un incident.

Configuration de seuils

Pour générer des alarmes utiles, vous devez définir des seuils sensibles. Ceci n'est malheureusement pas toujours facile à réaliser. En règle générale, vous devriez vous appuyer sur les données de référence que vous avez recueillies. Définissez un seuil qui puisse vous alerter lorsqu'une condition problématique se produit et un seuil opposé qui vous avertit lorsque la situation est redevenue normale.

Voici une liste de directives permettant de déterminer les seuils appropriés :

- Pour l'utilisation des ports, c'est-à-dire les niveaux de trafic multicast et broadcast, exploitez les valeurs de référence que vous avez collectées.
- Les seuils concernant les erreurs CRC devraient être très bas, c'est-à-dire ne dépassant pas une erreur par heure. Vous ne devriez pas établir d'informations de référence pour les erreurs CRC car le taux d'erreur pour Ethernet est très bas d'après les spécifications. Les collisions étant normales, elles devraient être référencées et les seuils devraient être configurés de façon appropriée.
- Si vous définissez des valeurs de seuil trop faibles, de nombreuses alarmes seront générées. Bien que vous souhaitiez que les opérateurs soient avertis des événements se produisant sur le réseau, vous ne devez pas non plus les inonder de messages. Une trop grande quantité d'alarmes risque de provoquer l'indifférence des opérateurs qui finiront par les ignorer.
- Si au contraire vous définissez des seuils trop élevés, les opérateurs risquent de ne pas être avertis suffisamment tôt de certains événements, ou de prendre connaissance d'une situation critique longtemps après la génération de l'interception SNMP. Par exemple, il n'est pas logique de générer une interception lorsque l'utilisation d'une liaison atteint 98 % car les utilisateurs finaux auront déjà souffert d'une sérieuse dégradation des performances, avant que le seuil de soit franchi.

Adaptation des seuils

Au cours des semaines suivantes, continuez à observer les données collectées. En les analysant et en surveillant le taux d'alarmes, vous pourrez déterminer l'efficacité des seuils que vous avez configurés et les ajuster au besoin.

L'adaptation des valeurs de seuils est un processus qui se poursuit à mesure que le réseau se développe, que le trafic augmente, et que ses comportements changent.

Réduction des données de la base de référence

Avec l'introduction des alarmes et des événements, il n'est plus nécessaire de procéder à une interrogation intensive pour obtenir des statistiques de trafic car l'équipement peut assurer lui-même son suivi par l'intermédiaire des événements et des alarmes RMON. En revanche, une interrogation visant à connaître les erreurs, comme avec ICMP ou SNMP, reste toujours nécessaire car un équipement ne sera pas en état d'annoncer ses défaillances s'il devient inopérant.

D'une façon générale, vous pouvez désactiver la collection des données historiques RMON lorsque vous entrez dans la phase de collecte régulière des données de référence. Ceci permet de réduire la consommation de ressources processeur et mémoire sur le commutateur. Vous devriez toutefois continuer à surveiller les ports critiques de tronçons de commutateur.

Analyse et collecte régulières des données de référence

Après avoir défini les ports critiques et les seuils d'alarmes, il se peut que vous souhaitiez collecter davantage de données de référence. Ces données sont pratiques pour analyser la croissance du réseau dans le temps et mesurer les performances du réseau commuté. L'analyse des tendances de comportement et la planification des ressources s'impose lorsque vous collectez activement les données de référence et sondez souvent votre réseau commuté.

Réfléchissez attentivement à la fréquence avec laquelle vous souhaitez interroger votre réseau. Une interrogation toutes les cinq minutes pour de nombreux ports commutés serait excessive. La section suivante donne des informations spécifiques sur les éléments à sonder et à surveiller activement sur un commutateur ou un routeur, et sur la façon de recueillir de façon continue des données utiles. L'interrogation SNMP, les alarmes et les événements RMON, et/ou les commandes CLI, font partie de la panoplie des moyens dont vous pouvez disposer pour mener à bien ces tâches.

Recommandations sur les commutateurs Cisco Catalyst

Jusqu'à présent, ce chapitre a présenté les données utiles que vous avez besoin de connaître et le processus que vous devriez enclencher pour administrer les commutateurs sur votre réseau. Cette section expose les détails d'implémentation de cette stratégie sur des commutateurs Catalyst. L'administration d'un réseau commuté exige davantage qu'une simple surveillance, et une collecte des informations SNMP et MIB. Elle doit débuter avec les premières étapes de conception de la commutation et se poursuivre jusqu'aux phases ultimes de déploiement du réseau commuté. Plusieurs aspects sont à considérer dans le cadre de l'administration d'un tel réseau : les recommandations de conception et de configuration, l'interrogation SNMP, les interceptions SNMP, la journalisation Syslog, et les fonctions RMON. Visitez le site Web Cisco pour obtenir des informations sur la configuration de la gestion de réseaux sur un Catalyst 5000.

Recommandations de conception et de configuration

Avant de déployer des commutateurs sur le réseau, tenez compte des recommandations de conception et de configuration suivantes.

Conception du réseau

Les ponts racines devraient être définis statiquement sur les commutateurs de distribution lorsque la fonctionnalité d'arbre recouvrant (STP) est utilisée. Elle devrait être activée sur tous les ports de tronçon. Vous pouvez aussi éventuellement l'activer sur les ports d'utilisateurs finaux au cas où une boucle viendrait à se former par erreur sur le réseau. Cette simple précaution peut permettre d'éviter l'immobilisation de votre réseau en cas de boucle.

Acquisition de données

Vous pouvez obtenir les mêmes données de différentes façons à partir d'un commutateur. La méthode que vous utilisez dépend de nombreux facteurs :

- la taille de votre réseau ;
- les besoins en matière d'administration de réseau ;
- les outils dont vous disposez pour collecter et traiter ces données.

Pour de très petits réseaux, la simple interface CLI peut suffire. Pour des réseaux plus grands et plus complexes, il peut s'avérer utile de mettre en place une station NMS avec des interrogateurs SNMP, des gestionnaires d'interceptions SNMP, et une base de données relationnelle. Dans la plupart des situations, on rencontre une combinaison de ces outils avec, en plus, l'emploi de quelques scripts Perl et Expect pour combler les manques. Les sections suivantes décrivent les données à collecter, comment les obtenir, et comment les transformer en informations utiles. Elles présentent les données que vous pouvez obtenir à partir des commandes CLI et des objets MIB de SNMP.

Cette section aborde également la gestion de base des erreurs au moyen des interceptions SNMP et des messages Syslog.

Telnet et l'interface CLI

Vous pouvez collecter toutes les données de performances qui vous sont utiles pour interroger et surveiller le réseau en ouvrant une session Telnet sur le commutateur et émettant diverses commandes CLI. L'interface en ligne de commande vous permet d'obtenir des statistiques de trafic et d'erreurs ainsi que des informations essentielles sur le fonctionnement général du commutateur. Il est évident que cette méthode ne convient pas dans le cas d'un grand nombre de commutateurs ou pour réaliser un suivi continu d'un certain nombre d'entre eux. Elle n'en demeure pas moins efficace pour obtenir des données en temps réel lors du dépannage d'un problème. C'est aussi un instrument nécessaire pour collecter des renseignements qui ne sont pas disponibles via SNMP. Vous pouvez recourir à des langages d'écriture de scripts tels que Expect et Perl pour recueillir ce genre de données de façon régulière ou en réponse à la détection de certaines conditions d'erreurs. Les commandes CLI permettant l'obtention de données spécifiques sont traitées plus loin dans cette section.

Interrogation SNMP

La méthode la plus couramment adoptée pour recueillir des données de performances est SNMP. Par l'intermédiaire de l'interrogation SNMP, vous pouvez collecter des informations MIB RMON, MIB-2, et d'autres données spécifiques de l'entreprise. Ces informations incluent des statistiques de trafic concernant les ports critiques et peuvent aussi comprendre des données spécifiques sur l'ensemble des performances du commutateur, telles que l'utilisation de la plaque de connexion arrière.

Les plates-formes NMS commerciales comptent parmi les méthodes de gestion de réseau s'appuyant sur SNMP habituellement utilisées. Vous pouvez également utiliser les services d'interrogation de ce genre d'ensembles logiciels pour recueillir périodiquement des informations spécifiques sur vos commutateurs et les conserver dans une base de données quelconque. Celle-ci peut être aussi simple qu'un ensemble de fichiers linéaires ou aussi complexe qu'un système de gestion de

base de données relationnelle (SGBDR). Des rapports peuvent ensuite être générés à partir de ces données par importation des fichiers linéaires dans un tableur ou avec l'utilitaire de reporting du SGBDR. Vous pouvez également opter pour la création de vos propres outils SNMP en utilisant un langage de scripts tel que Perl. Celui-ci est également utile pour créer des rapports à partir de fichiers linéaires.

Cisco TrafficDirector est un exemple d'ensemble de programmes spécialisés dans la gestion de réseaux. Ils sont semblables aux produits NMS généraux mentionnés précédemment, mais sont spécifiques à certains types de données, tels que les statistiques de trafic RMON ou MIB-2. Ces ensembles proposent généralement un certain nombre de rapports de base avec des options permettant de les adapter à vos besoins.

Une fois que vous disposez de moyens pour collecter les données, vous devez décider de celles à interroger. Plusieurs objets MIB peuvent contenir les mêmes données. Par exemple, *etherStatsTable* de RMON, *ifTable* de MIB-2, et la MIB dot3, sont tous des objets qui fournissent des statistiques semblables sur le trafic et les erreurs des ports Ethernet. Toutefois, nous vous recommandons d'utiliser *etherStatsTable* pour la plupart des interrogations. De nombreuses applications commerciales s'appuient déjà sur cet objet pour recueillir des données et disposent d'outils tout prêts pour les traiter et générer des rapports. Il est également facile de tirer parti des fonctions RMON de collecte de données historiques afin de réduire la charge de service des procédures d'interrogation. Notez que certaines versions du système Cisco IOS pour commutateur Catalyst autorisent la définition de seuils RMON uniquement dans l'objet *etherStatsTable*. Comme nous voulons établir des objets de référence sur lesquels définir des seuils RMON, l'objet *etherStatsTable* convient bien au départ. Certains objets de statistiques utiles à l'élaboration d'une base de référence sont *etherStatsOctets* pour le trafic total, *etherStatsMulticastPkts* pour le trafic multicast, et *etherStatsBroadcastPkts* pour le trafic broadcast.

Les objets de statistiques d'erreurs à surveiller sont ceux qui concernent les trames en erreur, comme *etherStatsCRCAlignErrors*, et peut-être aussi ceux qui concernent les fragments et les perturbations (*jabber*) Ethernet, comme *etherStatsFragments* et *etherStatsJabber*. La surveillance des collisions Ethernet sur un réseau commuté n'est généralement utile que sur les segments partagés.

Pour obtenir une définition détaillée des objets MIB que vous interrogez, il n'existe pas de meilleure source que le document MIB lui-même. Tous les documents sur les objets MIB supportés par les équipements Cisco sont disponibles au public dans la zone MIB du site Web de Cisco. Les répertoires "v1" et "v2" contiennent les objets MIB ASN.1 complets avec les définitions dans la syntaxe SNMP v1 ou SNMP v2. La plupart des stations NMS peuvent compiler ces fichiers directement dans une base MIB sans aucune modification. Les répertoires "oid" et "schema" sont fournis pour d'autres stations NMS qui requièrent des données MIB dans ce format. Le répertoire "oid" est également commode pour rechercher l'identificateur d'objet complet (OID) d'un objet donné si vous écrivez vos propres scripts pour collecter ces données. Le répertoire "support_list" est une directive un peu vague permettant de déterminer les objets supportés à certains niveaux des équipements et du système Cisco IOS.

Après avoir installé et configuré votre réseau commuté, vous devez mettre en place la station NMS qui se chargera du processus d'interrogation SNMP. L'interrogation des commutateurs ressemble à celle des routeurs, la seule différence étant la quantité et le type des variables MIB sollicitées. Un grand nombre de variables MIB pour les interfaces et les ports ne seront pas interrogées avec SNMP

en raison de la densité de ports sur les commutateurs et l'état inconnu des ports directement connectés aux stations de travail ou PC pouvant être éteints à tout moment. SNMP est très utile pour vérifier le bon fonctionnement des commutateurs et des ports de tronçons. Les ports utilisateurs peuvent être gérés uniquement en s'appuyant sur les interceptions d'événements d'états de ligne, établie ou relâchée, ou en utilisant les fonctionnalités intégrées de RMON. Les variables MIB de commutateur étudiées dans cette section proviennent directement des objets MIB suivants : RFC1213, CISCO-STACK-MIB, ETHERLIKE-MIB, et BRIDGE-MIB.

Les trois sections suivantes sur les procédures d'interrogation de variables MIB sont tirées des directives contenues dans le guide *Guidelines for Polling MIB Variables*, telles qu'elles s'appliquent aux routeurs. Les mêmes principes peuvent être appliqués dans le cas d'un environnement commuté, mais avec des variables MIB différentes.

Avant d'étudier les éléments qui doivent être interrogés, nous devons déterminer l'objectif des interrogations. On peut dire qu'il existe trois objectifs principaux aux interrogations : déterminer la disponibilité d'un équipement (interrogation de surveillance), déterminer si une condition d'erreur s'est produite ou est en passe de se produire (interrogation de seuils), ou analyser les données et mesurer des tendances ou des performances (interrogation de performances).

Interrogation de surveillance

L'objectif de l'interrogation de surveillance est de détecter les changements de comportement sur le réseau et de générer immédiatement une alarme. Elle vise la détection d'erreurs dites "dures", tel qu'un équipement ne répondant pas ou le changement d'état d'une interface. Une alarme de cette catégorie doit immédiatement être suivie d'une action appropriée. Si votre système fait l'objet d'un suivi permanent (24/24 heures et 7/7 jours), une alarme d'interrogation de surveillance devrait générer un signal visible et sonore sur le système de façon que l'opérateur puisse réagir immédiatement. Si le suivi n'est pas continu, il est recommandé de diriger n'importe quelle alarme d'interrogation de surveillance vers la personne appropriée, si possible par pager ou par e-mail.

Des applications d'interrogation de surveillance sont incluses dans la plupart des plates-formes SNMP commerciales et applications de gestion de réseau basées sur SNMP. Leur but est d'analyser les points de données et de générer une alarme lorsque cela est nécessaire.

Interrogation de seuils

L'objectif de l'interrogation de seuils est de déterminer les conditions d'erreurs qui s'aggravent afin d'entreprendre les actions qui s'imposent avant que les performances ne soient réellement affectées. Une grande variété de problèmes apparaît sous la forme de conditions d'erreurs aggravées. Elles peuvent se transformer en erreurs "dures", ou se présenter par intermittence. L'interrogation de seuils est un outil qui permet de détecter ces problèmes.

Pour l'implémenter, il faut en premier lieu décider des variables MIB à interroger (les variables MIB pour les commutateurs suivent dans cette section). Les utilisateurs qui débutent avec cette forme d'interrogation peuvent commencer avec les variables qui sont suggérées ci-après puis ajouter toute autre variable MIB qui serait appropriée pour leur réseau.

Après avoir choisi les variables MIB à interroger, vous devez leur définir des valeurs de références. Pour cela, vous pouvez démarrer une procédure d'interrogation de ces variables pendant une

certaine période (une semaine par exemple) et analyser ensuite les données produites. La détermination des valeurs de référence doit être réalisée lors de périodes de pointe de trafic pour qu'elles soient les plus représentatives possibles de conditions inhabituelles. Plus votre réseau est statique (changements annuels) et moins vous aurez à renouveler les valeurs de référence, et plus il est dynamique (changements mensuels), plus vous devrez mettre à jour votre base de référence. A l'aide de ces données étalons, déterminez ensuite les valeurs situées en dehors des limites. Une règle générale est de définir des seuils dépassant de 10 à 20 % les valeurs maximales relevées.

Les valeurs seuils pour n'importe quelle variable MIB peuvent être appliquées uniformément sur tous les commutateurs, ou être adaptées par groupes de commutateurs ayant des caractéristiques similaires (par exemple, commutateur central ou de distribution).

Une autre décision devant être prise concerne le choix des types de notification appropriés à émettre lorsque les seuils sont franchis. Les dépassements de seuils ne sont pas indicateurs d'erreurs "dures" et ne demandent généralement pas une réaction immédiate. La journalisation des valeurs seuils et leur examen journalier est le meilleur moyen de rester informé. Il est très important d'analyser les causes de dépassements répétés. Vous pouvez ainsi déterminer si un problème qui s'est produit peut être corrigé, ou si les valeurs hors limites sont simplement dues à des seuils trop faibles étant donné la situation.

Interrogation de performances

L'objectif de l'interrogation de performances est de collecter des données pouvant être analysées dans le temps pour déterminer les tendances et faciliter la planification des ressources. A l'instar de l'interrogation de seuils, il faut commencer par déterminer les variables MIB à interroger. Des suggestions sont données plus loin dans cette section pour choisir les variables MIB qui seraient les plus utiles à l'interrogation de performances des commutateurs.

Dans le cadre de ce processus, des points de données individuels (données brutes) sont stockés par intermittence sur la machine assurant l'interrogation. Selon le mécanisme d'interrogation utilisé, les données peuvent être conservées dans un format brut ou dans une base de données relationnelle.

Afin d'améliorer la gestion des données, les informations brutes devraient être périodiquement comparées et faire l'objet de calculs dont les résultats seraient enregistrés dans une autre base de données ou un autre fichier afin de générer des rapports ultérieurs. Les données brutes peuvent être conservées pendant un certain temps à des fins de sauvegarde, mais il faut au final les supprimer et ne conserver que les agrégats de performances. La dernière étape de ce processus est la production de rapports à partir des résultats, qui seront examinés périodiquement pour identifier les tendances ou à des fins de prévisions des ressources.

Pour mieux illustrer ce processus, voici un exemple de système d'interrogation de performances d'une entreprise :

- Les variables MIB individuelles sont assemblées pour former des groupes d'interrogations. Chaque groupe est interrogé toutes les cinq minutes et les données sont stockées dans une base de données Sybase en fonction du nom du groupe. Chaque matin à 12h01, les données brutes de la base sont traitées afin de calculer les valeurs minimales, maximales, et moyennes pour chaque heure, et les résultats sont ensuite enregistrés dans une autre base de données Sybase (au moyen de programmes SQL écrits spécifiquement pour cette opération).

- Chaque samedi matin à 1h00, les points de données brutes individuels de la semaine passée sont supprimés de la base de données. Le premier jour du mois, les valeurs de minimum, maximum, et de moyenne par heure sont traitées avec d'autres calculs pour dégager des valeurs de minimum, maximum et de moyenne journalière. Ces résultats sont à nouveau stockés dans une autre base de données. Le premier mardi du mois, une série de rapports sont générés à partir des résultats horaires et journaliers pour être examinés lors de la réunion de planification des ressources. Après la génération des états, les données de résultats par heure sont archivées sur bande.

Pour obtenir davantage d'informations sur la surveillance des performances, reportez-vous au manuel de référence IBM (*IBM Red Books*) intitulé *Monitoring Performance In Router Networks*, Document GG24-4157-RMON.

RMON

Comme mentionné précédemment, la plupart des commutateurs Catalyst supportent une version "allégée" de RMON qui se compose de quatre groupes de base RMON-1 : statistiques, historiques, alarmes, et événements. Pour l'élaboration des valeurs de référence, le groupe *etherStats* propose un éventail de statistiques utiles sur le trafic de niveau 2. Vous pouvez utiliser les objets du Tableau 14.3 pour recueillir des statistiques sur le trafic unicast, multicast, et broadcast, ainsi que sur une variété d'erreurs de niveau 2. L'agent RMON sur le commutateur peut être configuré pour stocker ces échantillons dans le groupe historiques. Ce mécanisme permet de réduire le volume d'interrogations sans réduire le nombre d'échantillons. L'emploi des historiques RMON permet d'obtenir des valeurs de référence plus précises sans entraîner trop de surcharge de service due aux interrogations. Plus vous collectez d'historiques, plus les ressources du commutateur sont sollicitées.

La fonction la plus puissante de RMON-1 est le mécanisme de gestion des seuils fourni par les groupes alarmes et événements. Il permet de configurer le commutateur de façon qu'il envoie une interception SNMP lorsqu'une condition anormale se présente. Après avoir identifié tous les ports jugés critiques et recueilli des données de référence reflétant l'activité normale sur ces ports à l'aide des interrogations SNMP (et peut-être aussi des historiques RMON), vous êtes prêt à définir les seuils RMON. Définissez-les pour qu'ils génèrent une alarme lorsque des écarts importants sont constatés par rapport aux valeurs de référence sur un de ces ports. Prévoyez aussi des seuils inférieurs afin d'être averti lorsque le trafic revient à un niveau normal toujours par rapport aux valeurs de référence.

Pour configurer ces seuils, la meilleure solution est d'utiliser des ensembles logiciels d'administration RMON. La création des lignes dans les tables d'alarmes et d'événements est une tâche laborieuse et complexe. Les ensembles logiciels RMON NMS, tels que TrafficDirector, proposent des interfaces graphiques qui facilitent cette configuration.

Bien que les commutateurs fournissent seulement quatre groupes de base RMON-1, il est important de ne pas oublier le reste des objets RMON-1 et RMON-2. Vous pouvez obtenir des informations de niveau 3 et supérieur sur vos commutateurs à l'aide de la fonction de port SPAN et d'une sonde RMON externe, comme SwitchProbe de Cisco. Cette sonde supporte RMON-2 et peut être alimentée à partir d'un port SPAN pour assurer le suivi complet des données RMON sur n'importe quel port ou la totalité d'un VLAN sur un commutateur donné. Vous pouvez utiliser cette combinaison SwitchProbe et port SPAN pour capturer un flot de paquets sur un port spécifique (en utilisant le

groupe de capture de paquets de RMON-1) puis les télécharger vers un logiciel d'administration RMON à des fins d'analyse. La combinaison SwitchProbe et port SPAN peut également servir à recueillir des statistiques de niveau couche réseau et couche application sur un port donné ou sur un VLAN. Le port SPAN est contrôlable via SNMP avec le groupe SPAN de l'objet CISCO-STACK-MIB. Ce processus est donc facile à automatiser. TrafficDirector utilise ces fonctions avec sa fonctionnalité d'agent "errant" (*roving*).

Il y a certains risques à sonder tout un VLAN. Même si vous utilisez une sonde à 100 Mbit/s, la totalité du flux de paquets d'un VLAN, ou même d'un port duplex à 100 Mbit/s, peut excéder la bande passante d'un port SPAN. Prenez donc soin de ne pas le surcharger. S'il fonctionne continuellement à pleine charge, il est possible que des données soient perdues.

Contraintes de mémoire RMON

Il est important de se souvenir que la fonction principale d'un commutateur est de commuter des trames et non d'agir comme une sonde RMON multiport. Lorsque vous prévoyez des historiques et des seuils sur plusieurs ports pour toutes les conditions possibles, gardez à l'esprit que des ressources du commutateur seront monopolisées pour l'administration et ne seront pas disponibles pour sa fonction principale. N'oubliez pas non plus la règle préconisant d'interroger et de définir des seuils uniquement pour les ports qui auront été identifiés comme étant critiques.

En ce qui concerne les statistiques, les historiques, les alarmes, et les événements RMON, la consommation de la mémoire est constante sur toutes les plates-formes de commutateur. RMON utilise un *seau* pour stocker les historiques et les statistiques sur l'agent RMON (en l'occurrence le commutateur). La taille du seau est d'abord définie sur la sonde RMON (SwitchProbe) ou sur l'application RMON (TrafficDirector), et le seau est ensuite envoyé vers le commutateur pour y être configuré.

Famille de commutateurs Catalyst 5000

Environ 450 Ko d'espace de code seront ajoutés à l'image NMP pour supporter la version réduite de RMON (quatre groupes RMON : statistiques, historiques, alarmes, et événements). Les besoins en mémoire dynamique pour les fonctions RMON varient car ils dépendent de la configuration d'exécution. Le Tableau 14.3 explique l'utilisation de la mémoire RMON pour chaque groupe du RMON réduit.

Tableau 14.3 : Utilisation de la mémoire RMON d'exécution

<i>Définition de groupe</i>	<i>Espace DRAM utilisé</i>	<i>Remarques</i>
Statistiques	140 octets par port Ethernet/Fast Ethernet commuté	Par port.
Historiques	3,6 Ko pour 50 seaux.	Chaque seau supplémentaire utilise 56 octets.
Alarmes et événements	2,6 Ko par alarme avec ses entrées d'événements correspondantes	Par alarme par port.

Un seul pool de DRAM est dédié à l'allocation dynamique et chaque fonction/processus l'utilise. Sur le Catalyst 5000, version 3.1 ou ultérieure, utilisez la commande **show version** pour visualiser la quantité de mémoire DRAM utilisée et libre. En vous fondant sur les données précédentes, déterminez les exigences de mémoire RMON. La sauvegarde de la configuration relative à RMON occupe approximativement les quantités de mémoire suivantes :

- 10 Ko d'espace NVRAM si la taille totale de la NVRAM du système est de 128 Ko.
- 20 Ko d'espace NVRAM si la taille totale de la NVRAM du système est de 256 Ko ou plus.
- L'impact au niveau des ressources processeur de l'utilisation des fonctions RMON de collecte d'informations et d'alarme sur un commutateur Cisco, peut être décrit de la façon suivante :
 - **Groupe statistiques** : Il utilise des cycles processeur uniquement lorsqu'il traite une requête SNMP **Get** recueillant des statistiques RMON de port. Son impact est donc minimal car les informations *etherStats* sont collectées au niveau matériel.
 - **Groupes historiques et alarmes/événements** : Ces groupes utilisent peu de cycles processeur pour chaque période d'interrogation par port (c'est-à-dire, pour chaque cliché d'historique et chaque seuil d'alarme à évaluer). L'impact dépend de l'intervalle entre les interrogations et du nombre de ports. La surcharge de processeur devrait être minimale avec un module superviseur 2 ou 3 (en supposant un nombre de ports inférieur à 150 et des intervalles d'interrogation de 30 secondes ou davantage).

Contraintes de mémoire Syslog

La configuration de Syslog sur les commutateurs Catalyst 5000 consomme 1 Ko de mémoire (pour les versions 2.2 et ultérieures) pour enregistrer les derniers messages Syslog générés.

Indexation de chaînes de communauté et VLAN

Certaines bases MIB standard supposent qu'une entité SNMP particulière ne contient qu'une instance de la base MIB. Par conséquent, la base standard ne dispose d'aucun index permettant aux utilisateurs d'accéder directement à une instance particulière de la MIB. Pour palier ce manque, Cisco autorise l'indexation de chaîne de communauté. La syntaxe utilisée est *chaîne_communauté @numéro_instance*.

Par exemple, le commutateur Catalyst gère une instance de la base standard BRIDGE-MIB pour chaque VLAN sur le commutateur. Si la chaîne de communauté en lecture seule est "public" et que la chaîne de communauté en lecture-écriture est "private", vous pourriez utiliser **public@25** pour lire la base BRIDGE-MIB pour le VLAN 25, et **private@33** pour lire et écrire dans la base BRIDGE-MIB pour le VLAN 33. Si les chaînes **public** ou **private** sont utilisées seules sans précision de l'instance, la base du VLAN 1 sera lue par défaut.

Les interceptions envoyées à partir d'une base MIB indexée par une chaîne de communauté indiquent également l'instance de la base à laquelle elles correspondent en utilisant l'indexation. Par exemple, une interception STP *newRoot* à partir de BRIDGE-MIB pour le VLAN 25 utiliserait une chaîne de communauté **public@25** dans le champ de communauté de l'interception, en supposant que la chaîne de communauté en lecture seule soit "public".

Notez également que l'indexation de chaîne de communauté n'affecte pas l'accès aux bases MIB ne comportant qu'une instance. Par conséquent, **public@25** peut être utilisé pour accéder à RFC1213-MIB pendant qu'un accès à BRIDGE-MIB pour le VLAN 25 se produit.

Un autre exemple pour le commutateur Catalyst est la base SNMP-REPEATER-MIB. Pour accéder à cette MIB pour un répéteur donné sur le commutateur Catalyst, utilisez la syntaxe *chaîne _communauté@numéro_module/numéro_port*. Si la chaîne de communauté en lecture seule est par exemple, "public", vous pouvez utiliser **public@3/1** pour lire SNMP-REPEATER-MIB pour le répéteur attaché au port 1 sur le module 3.

Pour déterminer les VLAN disponibles sur un commutateur Catalyst donné, vous devez interroger le groupe MIB *vlanTable* de la base CISCO-STACK-MIB en utilisant l'identifiant de VLAN comme index.

Depuis Cat5xxx version 4.1(1), l'identifiant *vlanIndex* a été ajouté à la liste *varBind* des interceptions *newRoot* et *topologyChange* définies dans la base BRIDGE-MIB. Ainsi, les plates-formes et les applications SNMP n'ont pas besoin de décoder la chaîne de communauté dans l'interception. Voici deux exemples des nouvelles interceptions supportées :

```
Received SNMPv1 Trap:
Community: public@2
Enterprise: dot1dBridge
Agent-addr: 172.10.17.31
Enterprise Specific trap.
Enterprise Specific trap: 2      (interception topologyChange)
Time Ticks: 27654316
vtpVlanIndex.1.2 = 2            (numéro de VLAN)
ifName.97 = 4/2                (index de l'interface)

Received SNMPv1 Trap:
Community: public@3
Enterprise: dot1dBridge
Agent-addr: 172.10.17.31
Enterprise Specific trap.
Enterprise Specific trap: 1      (interception newRoot)
Time Ticks: 27651818
vtpVlanIndex.1.3 = 3            (numéro de VLAN)
```

Indexation d'interface SNMP à partir de *ifIndex* et *ifName*

L'identification du port ayant généré une interception d'événement donnée peut s'avérer difficile. Savoir qu'une interception provient de l'objet *ifIndex 100* n'aide pas à identifier sa source. Mais savoir qu'elle provient du port 1/1 est très utile. Nous utilisons la base IF-MIB pour affecter l'objet *ifIndex* à un numéro de port. Si vous interrogez l'objet *ifXTable* pour connaître *ifName*, vous pouvez obtenir une correspondance entre *ifIndex* et le port en question. Si vous avez reçu une interception, par exemple pour *ifIndex 17*, vous pourriez interroger *ifName* afin de connaître le port, comme illustré dans l'exemple suivant :

```
$ snmpwalk robotron ifName
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.1 : DISPLAY STRING- (ascii): sc0
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.2 : DISPLAY STRING- (ascii): s10
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.3 : DISPLAY STRING- (ascii): 1/1
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.4 : DISPLAY STRING- (ascii): 1/2
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.5 : DISPLAY STRING- (ascii): 2/1
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.6 : DISPLAY STRING- (ascii): 2/2
```

```

ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.7 : DISPLAY STRING- (ascii): 2/3
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.8 : DISPLAY STRING- (ascii): 2/4
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.9 : DISPLAY STRING- (ascii): 2/5
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.10 : DISPLAY STRING- (ascii): 2/6
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.11 : DISPLAY STRING- (ascii): 2/7
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.12 : DISPLAY STRING- (ascii): 2/8
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.13 : DISPLAY STRING- (ascii): 2/9
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.14 : DISPLAY STRING- (ascii): 2/10
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.15 : DISPLAY STRING- (ascii): 2/11
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.16 : DISPLAY STRING- (ascii): 2/12
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.17 : DISPLAY STRING- (ascii): 2/13
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.18 : DISPLAY STRING- (ascii): 2/14
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.19 : DISPLAY STRING- (ascii): 2/15
ifMIB.ifMIBObjects.ifXTable.ifXEntry.ifName.20 : DISPLAY STRING- (ascii): 2/16

```

Le résultat de la commande indique que le port 2/13 a généré l'interception.

Configuration de SNMP, SPAN, Syslog et des interceptions SNMP

Utilisez les commandes **set snmp** pour définir tous les paramètres SNMP : chaînes de communauté, RMON, et autres interceptions SNMP. Le Tableau 14.4 décrit ces commandes.

Tableau 14.4 : Commandes de configuration IOS pour SNMP

<i>Commande</i>	<i>Description</i>
set snmp ?	Affiche la syntaxe à utiliser pour définir différents paramètres.
set snmp trap	Active les différentes interceptions SNMP sur le commutateur.
set port trap	Active ou désactive les interceptions de liaison sur la base de chaque port. Si des stations finales sont connectées au commutateur, vous devriez prévoir des interceptions de liaison uniquement pour les port jugés critiques.
show snmp	Vérifie la configuration actuelle de SNMP sur le commutateur.
set span	Définit la source et la destination de la fonction SPAN. Celle-ci peut également être configurée via SNMP en utilisant les objets du groupe <i>monitorGrp</i> dans la base <i>CISCO-STACK-MIB</i> .
set logging	Configure le commutateur pour qu'il envoie ses messages de console vers un serveur Syslog. Nous vous recommandons d'utiliser la commande set logging level pour définir un niveau de gravité de 4 pour tous les services, ou le niveau avertissement (<i>warning</i>).

Vous trouverez des informations détaillées sur toutes les commandes **set** pour la version 4.2 sur le site Web de Cisco.

Les méthodes habituelles de gestion d'erreur impliquent la journalisation des interceptions SNMP (ce qui comprend des interceptions de seuils RMON) et des messages Syslog, puis le traitement des données suivis des réactions appropriées. La plupart des suites logicielles NMS fournissent un démon d'interception qui reçoit et journalise les interceptions SNMP, ainsi que des mécanismes permettant d'y réagir. Parmi ces mécanismes, on trouve généralement l'affichage de messages, l'émission d'alarmes sonores sur la station NMS, ou l'exécution d'un script de pager. Des actions plus complexes peuvent comprendre l'exécution d'un script Expect qui collecte des données sensibles

au temps afin de déterminer l'état du commutateur immédiatement après l'apparition d'une erreur, ou le déclenchement d'une procédure de capture de paquets à partir du port approprié en utilisant une sonde RMON externe. Plusieurs scénarios du genre sont décrits plus loin dans ce chapitre.

En ce qui concerne les messages Syslog, la plupart des systèmes Unix (si ce n'est pas tous) fournissent un démon Syslog. D'autres démons du domaine commercial ou public sont également disponibles pour les systèmes Win95 ou WinNT. Ces démons journalisent généralement tous les messages de commutateur dans un fichier particulier. Un script ou un outil quelconque de reporting peut ensuite être utilisé pour analyser le fichier afin de produire des informations utiles. L'utilitaire Cisco Resource Manager possède un utilitaire Syslog Analyzer qui crée des rapports à partir des messages Syslog en se basant sur les niveaux de gravité ou les équipements qui les ont générés.

La plupart des produits NMS commerciaux gèrent les interceptions SNMP standard de base (telles que *linkUp* et *linkDown*) ainsi que les seuils RMON. En ce qui concerne les interceptions spécifiques à Cisco, vous devez configurer NMS pour les formater afin qu'elles puissent être lues et reconnues. Le site Web Cisco fournit dans le fichier *trapd.conf* des informations sur le formatage des interceptions pour HP OpenView Network Node Manager et Tivoli NetView.

Les bases MIB spécifiques à Cisco peuvent être trouvées dans les documents MIB, tels que ceux listés dans le Tableau 14.5.

Tableau 14.5 : Liste des interceptions SNMP pour les commutateurs Cisco

Document MIB	Interceptions spécifiques
CISCO-STACK-MIB	Interceptions de module : <ul style="list-style-type: none"> • lerAlarmOn • lerAlarmOff • moduleUp • moduleDown Interceptions de châssis : <ul style="list-style-type: none"> • chassisAlarmOn • chassisAlarmOff Interceptions de permission IP : <ul style="list-style-type: none"> • IpPermitDeniedTrap
BRIDGE-MIB (RFC 1493)	Interceptions STP
RFC 1157	Interception d'authentification
CISCO-VTP-MIB	Interceptions VTP : <ul style="list-style-type: none"> • vtpConfigRevNumberError • vtpConfigDigestError • vtpServerDisabled • vtpMtuTooBig • vtpVlanRingNumberConfigConflict • vtpVersionOneDeviceDetected
CISCO-VLAN-MEMBERSHIP-MIB	Interceptions VMPS (<i>VLAN Membership Policy Server</i>)

Tableau 14.5 : Liste des interceptions SNMP pour les commutateurs Cisco (suite)

<i>Document MIB</i>	<i>Interceptions spécifiques</i>
SNMP-REPEATER-MIB (RFC 1516)	Interceptions de répéteur
IF-MIB (RFC 1573)	Interceptions de ligne établie/libérée pour chaque port (<i>LinkUp</i> et <i>LinkDown</i>)

Etat des ressources de commutateur

Il est important de connaître l'état des ressources d'un commutateur pour pouvoir juger de son bon fonctionnement en matière de trafic, de système, de processeur, et d'utilisation de la mémoire.

Bases MIB SNMP

Les variables suivantes sont utiles pour déterminer l'utilisation de la plaque de connexion arrière du commutateur. Les mêmes compteurs sont utilisés lors de l'affichage des indicateurs de niveau de trafic rouges sur l'avant de la carte superviseur. Ces variables ne devraient toutefois pas être confondues avec l'utilisation des ressources processeur ou mémoire.

Les informations suivantes sont disponibles sur le site Web Cisco :

- **SysTraffic.** Valeur de mesure du trafic, comme le pourcentage d'utilisation de la bande passante pour l'intervalle d'interrogation précédent.
- **SysTrafficPeak.** Valeur de mesure de pointe de trafic depuis la dernière fois que les compteurs du port ont été réinitialisés ou que le système a démarré (voir *sysClearPortTime*).
- **SysTrafficPeakTime.** Le temps (en centièmes de seconde) écoulé depuis que la valeur de mesure de pointe de trafic a été trouvée.
- **SysTrafficMeterTable.** Trafic dans le processeur système et sur les bus système internes. S'applique uniquement aux modules superviseurs III du Catalyst 5000.

Interface CLI

Utilisez les commandes décrites dans cette section comme méthodes additionnelles de collecte de données sur les ressources de commutateur.

Commande show biga — Erreurs de ressources de commutateur (RsrcErrors)

Cette commande indique les pertes en file d'attente de superviseur, semblables aux pertes en files d'entrées sur les routeurs, et révèle le trafic destiné aux superviseurs, comme les unités BPDU (*Bridge Protocol Data Unit*). Cette commande s'applique aux moteurs superviseurs 1 et 2. L'élément d'intérêt principal du résultat de cette commande est *RsrcErrors* :

```
switch 5000 (enable) show biga
BIGA Registers:
  cstat:      00  upad :      FFFF  pctrl :      0000  nist :      0000
  sist :     0018  hica :      0000  hicb :      0000  hicc :       00
  dctrl:     F5FF  dstat:     0000  dctrl2:      80  npim :      00F8
  thead: 101F196C  ttail: 101F196C  ttmph : 101F196C  tptr : 104347E2
  tdsc : 00000500  tlen :      0000  tqsel :       05
  rhead: 101F1220  rtail: 101F1204  rtmpf : 101F123C  rptr : 10586C80
```

```

rdsc : 804D0000 rplen: 101F1234 rtlen : 00000000 rlen : 1600
fltr : 00FF fc : 00 Rev : 04 CFG : 02020202
BIGA Driver:
    Initialzd: TRUE SpurusIntr: 00000000 NPIMShadow: 00F8

BIGA Receive:
    RxDone : FALSE
    First RBD : 101EF894 Last RBD : 101F1478
    SoftRHead : 101F1210 SoftRTail : 101F11F4
    FramesRcvd: 04572393 BytesRcvd : 589914384
    QueuedRBDs: 00000256 RsrcErrors: 00000000

BIGA Transmit:
    First TBD : 101F1494 Last TBD : 101F1B78
    SoftTHead : 101F19D4 SoftTTail : 101F19D4
    Free TBDs : 00000064 No TBDs : 00000000
    AcknowErrs: 00000000 HardErrors: 00000000
    QueuedPkts: 00000000 XmittedPkt: 11353833
    XmittedByt: 909016542 Panic : 00000000
    Frag<=4Byt: 00000306

```

Commande show inband — Erreurs de ressources de commutateur (RsrcErrors)

Cette commande indique les pertes en file d'attente de superviseur, semblables aux pertes en files d'entrées sur les routeurs, et révèle le trafic destiné aux superviseurs, comme les BPDU. Cette commande s'applique au moteur superviseur 3. L'élément d'intérêt principal du résultat de cette commande est *RsrcErrors* :

```

switch 5000 (enable) show inband
Inband Driver:
DriverPtr: A0559F20 Initialzd: TRUE SpurusIntr: 00000000
    RxDone: FALSE TxDMAWorking: FALSE RxRecovPtr: 00000000(-1)
    FPGACntl: 004F Characteristics:0000 LastISRCause: 04

Transmit:
    First TBD : A055E7A4(0 ) Last TBD : A055F784(0 )
    TxHead : A055F5A4(112) TxTail : A055F5A4(112)
    AvailTBDs : 00000128 QueuedPkts: 00000000
    XmittedPkt: 07626990 XmittedByt: 581073462
    PanicEnd : 00000000 PanicNullP: 00000000
    BuflenErrs: 00000000 Len0Errs : 00000000
    Frag<=4Byt: 00000162 SpursTxInt: 00000000
    No TBDs : 00000000 NullMbuf : 00000000

Receive:
    First RBD : A0559FA4(0 ) Last RBD : A055E780(511)
    RxHead : A055AE44(104) RxTail : A055AE20(103)
    AvailRBD : 00000512 RsrcErrors: 0000824
    PanicNullP: 00000000 PanicFakeI: 00000000
    FramesRcvd: 18507368 BytesRcvd : 1676456769
    RuntsRcvd : 00000000 HugeRcvd : 00000000

GT64010 IntMask: F00F0000 IntCause: 0330E083
GT64010 TX DMA (CH 1):
    Count: 0000 Src : 0134B062 Dst : 4ff10056 NRP : 0
00000000
    Cntl : 15C0
GT64010 RX DMA (CH 2):
    Count: 0680 Src : 4FF20000 Dst : 01c3e580 NRP : 0

```

```

0558590
Cntl :      55C0

PSI (PCI SAGE/PHOENIX Interface) FPGA:
Control : 004F TxCount : 0056
RxDMACmd: 35C0 RxBufSiz: 0680 MaxPkt : 0680
IntCause: 0002 IntMask : 0003

```

Commande show mbuf

Le résultat de cette commande affiche la mémoire utilisée sur le NMP. Ces données devraient être collectées une fois que les valeurs de références ont été définies. Vous pouvez mesurer la tendance de consommation de la mémoire sur le commutateur. Les champs "clusters" et "mbufs" représentent deux zones de la mémoire de travail. La deuxième ligne de ce listing indique l'espace total disponible pour ces zones sur le système. La troisième ligne affiche la quantité de mémoire disponible au moment de l'affichage de ce résultat. La quatrième ligne révèle la limite inférieure depuis le dernier démarrage du commutateur :

```

switch 5000 (enable) show mbuf
MBSTATS:
    mbufs          10224  clusters        3932
    free mbufs     9946   clfree       3675
    lowest free mbufs  9935   lowest clfree  3665

MALLOC STATS :
Block Size      Free Blocks
    16            1
    48            2
    112           1
    144           1
    208           1
    240           1
    400           1
    496           4

Largest block available : 7510096
Total Memory available  : 7546400
Total Memory used       : 563952

```

Commande ps-c

Cette commande permet d'afficher des données d'utilisation processeur du NMP. La dernière ligne du listing représente le temps d'inactivité. Dans cet exemple, le processeur du commutateur est actif à 59 % (41 % d'inactivité). Sur cette même ligne, les champs "high" et "low" représentent les limites supérieures et inférieures depuis le dernier démarrage du commutateur. Le champ "Average" indique la durée moyenne d'inactivité depuis le dernier démarrage. La colonne d'utilisation du processeur "CPU-Usage" totalise 100 % (avec plus ou moins d'erreurs d'arrondi) et indique la durée d'occupation du processeur par ce processus. Dans cet exemple, le noyau (*kernel*) utilise 93 % de 59 %, ce qui représente environ 49 % des capacités du processeur :

```

switch 5000 (enable) ps -c
CPU usage information:
Name          CPU-Usage      Invokations
----- -----
Kernel        93%           1
SynDiags      0%            1

```

```

SynConfig      0%          1
Earl          1%          1
THREAD        0%          1
Console       0%          1
telnetd       0%          1
cdpd          0%          1
cdpdtimer     0%          1
SptTimer      0%          1
SptBpduRx    0%          1
VtpTimer      0%          1
VtpRx         0%          1
DISL_Rx       0%          1
DISL_Timer    0%          1
sptHelper     0%          1
..etc
..etc
System Idle - Current: 41% High: 51% Low: 8% Average: 47%

```

Commande show log

Cette commande affiche l'état de l'activité ainsi que les exceptions. Dans cet exemple, les informations résultant d'un plantage de commutateur en plus des données de journalisation standard sont fournies. Les plantages peuvent être provoqués par des problèmes matériels ou logiciels. La mention "Vector: 007C" représente une expiration de délai du bus du commutateur et provient très probablement d'un problème matériel. Assurez-vous que les cartes sont correctement connectées. Si le plantage continue de se produire, vous pouvez retirer les modules un par un jusqu'à ce que le problème disparaisse.appelez le centre d'assistance technique (TAC) pour faire remplacer le module défaillant. Pour les problèmes logiciels (Vector: 007C), contactez également le TAC.

```

switch 5000 show log
Network Management Processor (ACTIVE NMP) Log:
  Reset count: 100
  Re-boot History: Mar 19 1998 16:06:10 3, Mar 11 1998 12:03:03 3
                    Mar 10 1998 04:34:52 3, Mar 08 1998 08:38:30 3
                    Mar 08 1998 08:09:51 3, Mar 08 1998 06:28:31 3
                    Mar 08 1998 05:33:23 3, Mar 02 1998 09:02:13 3
                    Feb 20 1998 05:02:35 3, Feb 20 1998 04:55:45 3
  Bootrom Checksum Failures: 0   UART Failures: 0
  Flash Checksum Failures: 0   Flash Program Failures: 0
  Power Supply 1 Failures: 39  Power Supply 2 Failures: 1
  DRAM Failures: 0

  Exceptions: 9
  Last Exception occurred on Feb 18 1998 17:14:18 ...
  Software version = 2.3(1)
  Error Msg:
  PID = 0 Co_-_?
  PC: 1015A3AC, Status: 2009, Vector: 007C
  sp+00: 20091015 A3AC007C 00000000 00000001
  sp+10: 00400000 AAAA0000 107F0008 1025EEC0
  sp+20: 107FFFA0 1017563E 00000000 107FFE8
  sp+30: 10175EA0 00000000 000006C7 00000000
  sp+40: 00000000 00000000 00000000 00000000
  sp+50: 00000000 00000000 50000200 00000007
  sp+60: 68000000 00000000 00000000 00000000
  sp+70: 00000000 00000000 00000000 00000000
  sp+80: 00000000 00000000 00000000 00000000
  sp+90: 00000000 00000000 00000000 00000000

```

```

sp+A0: 00000000 00000000 00000000 00000000
sp+B0: 00000000 00000000 00000000 00000000
sp+C0: 00000000 00000000 00000000 00000000
sp+D0: 00000000 00000000 00000000 00000000
sp+E0: 00000000 00000000 00000000 00000000
sp+F0: 00000000 4937F8E7 00000000 00000000
D0: 00000003, D1: 00000010, D2: 00000000, D3: 00000001
D4: 0040B5C1, D5: AAAAF0E7, D6: 00000003, D7: 10800000
A0: 68000000, A1: 00000079, A2: 50000200, A3: 50000200
A4: 103FFFFC, A5: 64000000, A6: 107FFFA0, sp: 107FFF80

```

NVRAM log:

```

01. 12/29/97,07:05:17:convert_post_SAC_CiscoMIB:Nvram block 0 unconvertable: 2(1)
02. 12/29/97,07:05:17:convert_post_SAC_CiscoMIB:Nvram block 1 unconvertable: 1(0)
03. 12/29/97,07:05:17:convert_post_SAC_CiscoMIB:Nvram block 5 unconvertable: 1(0)
04. 12/29/97,07:05:17: check_block_and_log:Block 59 has been deallocated: (0x500
191D8)
05. 12/29/97,07:05:17: convert_post_SAC_CiscoMIB:Nvram block 61 unconvertable:
1(0)

```

Module 2 Log:

```

Reset Count: 2
Reset History: Thu Mar 19 1998, 16:09:04
               Wed Mar 11 1998, 12:05:57

```

FCP Flash Checksum Failures:	0	DMP Flash Checksum Failures:	0
FCP Flash Program Failures:	0	DMP Flash Program Failures:	0
FCP DRAM Failures:	0	DMP DRAM Failures:	0
FCP SRAM Failures:	0	DMP SRAM Failures:	0
FCP Exceptions:	0	DMP Exceptions:	0
Path Test Failures:	0		

Module 3 Log:

```

Reset Count: 2
Reset History: Thu Mar 19 1998, 16:08:18
               Wed Mar 11 1998, 12:05:11

```

Module 4 Log:

```

Reset Count: 1
Reset History: Mon Mar 23 1998, 10:50:06

```

Module 5 Log:

```

Reset Count: 2
Reset History: Thu Mar 19 1998, 16:08:18
               Wed Mar 11 1998, 12:05:11

```

Etat de châssis et d'environnement

Les informations d'état de châssis et d'environnement sont utiles pour déterminer l'état fonctionnel du châssis du commutateur et des sources d'alimentation.

Bases MIB SNMP

Les objets MIB SNMP de cette liste devraient être interrogés si l'interception *chassisAlarmOn* se produit.

Les informations suivantes sont disponibles sur le site Web Cisco :

- **chassisPs1Status.** Etat de la source d'alimentation numéro 1. Si elle n'est pas opérationnelle, la valeur de *chassisPs1TestResult* donne davantage d'informations sur les conditions de panne qui se sont produites.
- **chassisPs2Status.** Etat de la source d'alimentation numéro 2. Si elle n'est pas opérationnelle, la valeur de *chassisPs2TestResult* donne davantage d'informations sur les conditions de panne qui se sont produites.
- **chassisFanStatus.** Etat du ventilateur du châssis. S'il n'est pas opérationnel, la valeur de *chassisFanTestResult* donne davantage d'informations sur les conditions de panne qui se sont produites.
- **chassisMinorAlarm.** Etat de l'alarme mineure relative au châssis.
- **chassisMajorAlarm.** Etat de l'alarme majeure du châssis.
- **chassisTempAlarm.** Etat de l'alarme de température de châssis.

Lorsque le voyant système passe au rouge, une alarme *chassisMajorAlarm* est générée et lorsqu'il passe à l'orange, une alarme *chassisMinorAlarm* est générée. L'interception générée sera *chassisAlarmOn*. Les informations d'interception sont accompagnées de variables qui indiquent si l'interception provient d'une alarme *chassisTempAlarm*, *chassisMinorAlarm*, ou *chassisMajorAlarm*. Déchiffrer l'interception permet de connaître l'alarme qui l'a déclenchée.

Les conditions suivantes provoquent une alarme majeure :

- n'importe quelle panne de tension ;
- pannes simultanées de température et de ventilateur ;
- panne totale de l'alimentation (2 sources sur 2 ou 1 source sur 1) ;
- échec EEPROM ;
- échec NVRAM ;
- échec de communication MCP ;
- état NMP inconnu.

Les conditions suivantes provoquent une alarme mineure :

- alarme de température ;
- panne de ventilateur ;
- panne partielle de l'alimentation (1 source sur 2) ;
- deux sources d'alimentation de types incompatibles.

Dans le cas d'une alarme mineure ou majeure, le voyant d'état du système sur le panneau avant devient rouge. Ces informations s'appliquent aux commutateurs de la famille Catalyst 5000. D'autres produits qui utilisent la base CISCO-STACK-MIB s'appuient sur des définitions différentes des alarmes majeures et mineures.

Interface CLI

Cette section contient des exemples de résultats provenant de commandes de l'interface CLI qui renseignent sur l'état du châssis et de l'environnement.

Commande show system

Les informations affichées par cette commande peuvent aussi être obtenues au moyen de SNMP :

```
switch 5000 (enable) show system
PS1-Status PS2-Status Fan-Status Temp-Alarm Sys-Status Uptime d,h:m:s Logout
-----
ok       none      ok        off      ok      14,21:20:38   20 min

PS1-Type  PS2-Type  Modem   Baud  Traffic Peak Peak-Time
-----
WS-C5008A  none      disable  9600   0%     0%   Wed Oct 22 1997, 14:17:56

System Name          System Location          System Contact
-----
switch 5000
```

Commande show test

Cette commande affiche l'état matériel des composants du commutateur. Vous devez spécifier le module pour lequel vous souhaitez obtenir des résultats de test :

```
switch 5000 show test 1
Environmental Status (. = Pass, F = Fail, U = Unknown)
PS (3.3V): .    PS (12V): .    PS (24V): .    PS1: .    PS2: .
Temperature: .    Fan: .

Module 1 : 2-port 100BaseFX MM Supervisor
Network Management Processor (NMP) Status: (. = Pass, F = Fail, U = Unknown)
ROM: .    Flash-EEPROM: .    Ser-EEPROM: .    NVRAM: .    MCP Comm: .

EARL Status :
    NewLearnTest: .
    IndexLearnTest: .
    DontForwardTest: .
    MonitorTest: .
    DontLearn: .
    FlushPacket: .
    ConditionalLearn: .
    EarlLearnDiscard: .
    EarlTrapTest: .

LCP Diag Status for Module 1 (. = Pass, F = Fail, N = N/A)
CPU       : .    Sprom     : .    Bootcsum : .    Archsum : N
RAM       : .    LTL       : .    CBL       : .    DPRAM     : .    SAMBA : N
Saints    : .    Pkt Bufs : .    Repeater : N    FLASH     : N

MII Status:
Ports 1 2
-----
N  N

SAINT/SAGE Status :
Ports 1 2 3
```

```
-----  
.  
.  
.  
Packet Buffer Status :  
Ports 1 2 3  
-----  
.  
.  
Loopback Status [Reported by Module 1] :  
Ports 1 2 3  
-----  
.  
.
```

Etat de modules de commutateur

L'état de modules représente l'état fonctionnel des modules de commutateur et de leurs composants.

Bases MIB SNMP

Les bases MIB SNMP de cette liste devraient être interrogées si l'interception *moduleUp* ou *moduleDown* est générée.

Les informations suivantes sont disponibles sur le site Web Cisco :

- **moduleStatus.** L'état fonctionnel du module. S'il n'indique pas que le module est opérationnel, la valeur de *moduleTestResult* donnera davantage d'informations sur les conditions de la panne du module.
- **moduleAction.** Lorsque cet objet est interrogé, il renvoie les informations suivantes :
 - other(1) — Module activé en permanence.
 - enable(3) — Module actuellement activé.
 - disable(4) — Module actuellement désactivé.

La définition de cet objet avec l'une des valeurs acceptables peut donner les résultats suivants :

- other(1) — Produit une erreur.
- reset(2) — Réinitialise le circuit de contrôle du module.
- enable(3) — Si l'état du module est configurable, active le module ou produit une erreur.
- disable(4) — Si l'état du module est configurable, désactive le module ou produit une erreur.

La définition de cet objet avec n'importe quelle autre valeur produit une erreur.

- **moduleStandbyStatus.** Etat d'un module redondant.

Interface CLI

Cette section contient des exemples de résultats de commandes CLI qui renseignent sur l'état des modules.

Commande show module

Ces résultats peuvent aussi être obtenus par l'intermédiaire de SNMP :

switch 5000 (enable) show module						
Mod	Module-Name	Ports	Module-Type	Model	Serial-Num	Status
1		2	100BaseFX MM Supervis	WS-X5006	003292389	ok
3		12	10BaseFL Ethernet	WS-X5011	003140385	ok
4		12	10BaseFL Ethernet	WS-X5011	003418318	ok
5		12	100BaseTX Ethernet	WS-X5113	002203857	ok
Mod	MAC-Address(es)			Hw	Fw	Sw
1	00-60-47-96-f2-00	thru	00-60-47-96-f5-ff	1.4	2.1	2.1(9)
3	00-60-3e-d1-86-e4	thru	00-60-3e-d1-86-ef	1.3	1.2	2.1(9)
4	00-60-3e-c9-90-54	thru	00-60-3e-c9-90-5f	1.1	1.2	2.1(9)
5	00-40-0b-d5-0e-10	thru	00-40-0b-d5-0e-1b	1.4	1.2	2.1(9)

Commande show test

Ce listing affiche l'état des auto-tests matériels sur chaque module :

```
switch 5000 (enable) show test 4

Module 4 : 12-port 10/100BaseTX Ethernet

LCP Diag Status for Module 4  (. = Pass, F = Fail, N = N/A)
CPU          : .     Sprom      : .     Bootcsum : .     Archsum   : N
RAM          : .     LTL       : .     CBL       : .     DPRAM     : N     SAMBA   : .
Saints       : .     Pkt Bufs  : .     Repeater : N     FLASH    : N

SAINT/SAGE Status :
Ports 1 2 3 4 5 6 7 8 9 10 11 12
-----
. . . . . . . . . . . .

Packet Buffer Status :
Ports 1 2 3 4 5 6 7 8 9 10 11 12
-----
. . . . . . . . . . . .

Loopback Status [Reported by Module 1] :
Ports 1 2 3 4 5 6 7 8 9 10 11 12
-----
. . . . . . . . . . . .

Channel Status :
Ports 1 2 3 4 5 6 7 8 9 10 11 12
-----
```

Topologie STP

Ces commandes **show** et variables MIB permettent d'obtenir l'état de la topologie d'arbre recouvrant STP (*Spanning-Tree*) sur le commutateur. Reportez-vous aux précédentes sections relatives au protocole STP et à l'indexation basée sur les communautés SNMP.

Bases MIB SNMP

NOTE

Reportez-vous à la section "Indexation de chaînes de communauté et VLAN" plus haut dans ce chapitre pour obtenir des informations d'utilisation.

Les bases MIB SNMP de cette liste devraient être interrogées si l'interception *newRoot* ou *topologyChange* se produit.

Les informations suivantes sont disponibles sur le site Web Cisco :

- **dot1dStpTimeSinceTopologyChange.** La durée écoulée (en centièmes de seconde) depuis le dernier changement de topologie détecté par l'entité.
- **dot1dStpTopChanges.** Le nombre total de changements de topologie détectés par ce pont depuis la dernière réinitialisation ou initialisation de l'entité d'administration.
- **dot1dStpDesignatedRoot.** L'identificateur de pont de la racine de l'arbre recouvrant comme déterminé par le protocole STP exécuté sur ce nœud. Cette valeur est utilisée comme paramètre *Root Identifier* dans toutes les unités BPDU (*Bridge Protocol Data Unit*) de configuration initiés par ce nœud.
- **dot1dStpRootCost.** Le coût du chemin vers la racine à partir de ce pont.
- **dot1dStpRootPort.** Le numéro du port qui offre le chemin de plus faible coût vers le pont racine à partir de ce pont.

Interface CLI

Commande show spantree

Les données affichées dans ce listing peuvent également être obtenues au moyen de SNMP :

```
switch 5000 (enable) show spantree1
VLAN 1
Spanning tree enabled

Designated Root          00-60-47-96-f2-00
Designated Root Priority 32768
Designated Root Cost     0
Designated Root Port      1/0
Root Max Age 20 sec     Hello Time 2 sec   Forward Delay 15 sec

Bridge ID MAC ADDR       00-60-47-96-f2-00
Bridge ID Priority        32768
Bridge Max Age 20 sec    Hello Time 2 sec   Forward Delay 15 sec

Port      Vlan  Port-State      Cost  Priority  Fast-Start
-----  -----  -----
1/1       1     not-connected  10    32        disabled
1/2       1     not-connected  10    32        disabled
5/8       1     disabled       10    32        disabled
5/9       1     disabled       10    32        disabled
5/10      1     not-connected  10    32        disabled
```

Informations de base de données de transmission de pont

Les informations MIB et de la commande **show** suivantes renseignent sur le contenu et l'état de la base de transmission du commutateur. Reportez-vous à la section "Table CAM (*Content-Addressable Memory*)", plus haut dans ce chapitre pour obtenir davantage d'informations à ce sujet.

Pour déterminer le port sur lequel une adresse MAC donnée est reliée à un commutateur Catalyst, vous devez rechercher l'adresse MAC dans la table *dot1dTpFdbTable* (1.3.6.1.2.1.17.4.3) et déterminer le port de pont associé en utilisant l'objet *dot1dTpFdbPort* (1.3.6.1..1.17.4.3.1.2). Il se peut que vous ayez à utiliser l'indexation de chaîne de communauté si plusieurs VLAN sont associés à ce commutateur.

Convertissez ensuite cet index de pont en un *ifIndex* en utilisant l'objet *dot1dBasePortIfIndex* (1.3.6.1.2.1.17.1.4.1.2). Vous pouvez ensuite utiliser l'objet *ifName* (1.3.6.1.2.1.31.1.1.1.1) de la base IF-MIB (RFC 1573) pour obtenir le numéro de connecteur/port auquel l'adresse MAC est associée.

NOTE

Le pont transparent Ethernet est le seul équipement traité ici.

Bases MIB SNMP

NOTE

Reportez-vous à la section "Indexation de chaînes de communauté et VLAN" pour obtenir des informations d'utilisation.

La base de données de transmission de pont est utilisée par le circuit EARL et est disponible via l'objet MIB suivant :

- **dot1dTpFdbTable.** Une table qui contient des informations sur les entrées unicast pour lesquelles le pont transmet et/ou filtre des données. Ces données sont utilisées par la fonction de pont transparent pour déterminer la façon de propager une trame reçue.

Interface CLI

Les exemples suivants présentent les informations affichées par les commandes CLI, et qui renseignent sur la table CAM.

Commande show cam count dynamic

Cette commande affiche le nombre total d'entrées de la CAM découvertes par le commutateur. Ces données devraient être collectées lorsque les valeurs de référence initiales ont été définies pour suivre la croissance des adresses MAC sur un commutateur.

```
switch 5000> show cam count dynamic
Total Matching CAM Entries = 200
```

Erreurs de port

Les variables MIB et les résultats Telnet qui suivent rapportent des erreurs survenues sur les interfaces de commutateur.

Bases MIB SNMP

Les informations suivantes sont disponibles sur le site Web Cisco :

- **dot3StatsAlignmentErrors.** Un compte des trames reçues sur une interface, dont la longueur en octets n'est pas intégrale et pour lesquelles le contrôle FCS (*Frame Check Sequence*) a échoué.
Le total indiqué par une instance de cet objet est incrémenté lorsque l'état *alignmentError* est renvoyé par le service MAC vers la couche LLC (*Logical Link Control*) (ou un autre utilisateur du service MAC). Les trames reçues avec plusieurs conditions d'erreurs sont, selon les conventions IEEE 802.3 Layer Management, comptées exclusivement en fonction du statut d'erreur présenté à la sous-couche LLC.
- **dot3StatsFCSErrors.** Un compte des trames reçues sur une interface, dont la longueur en octets est intégrale et pour lesquelles le contrôle FCS (*Frame Check Sequence*) a échoué.
Le total indiqué par une instance de cet objet est incrémenté lorsque l'état *frameCheckError* est renvoyé par le service MAC vers la couche LLC (ou un autre utilisateur du service MAC). Les trames reçues avec plusieurs conditions d'erreurs sont, selon les conventions IEEE 802.3 Layer Management, comptées exclusivement en fonction du statut d'erreur présenté à la sous-couche LLC.
- **dot3StatsSingleCollisionFrames.** Un compte des trames transmises avec succès sur une interface donnée pour laquelle la transmission est bloquée si une seule collision se produit.
Une trame qui est comptée par une instance de cet objet est aussi comptée par l'instance correspondante de l'un des objets *ifOutUcastPkts*, *ifOutMulticastPkts*, ou *ifOutBroadcastPkts*, mais pas par celle de l'objet *dot3StatsMultipleCollisionFrames*.
- **dot3StatsMultipleCollisionFrames.** Un compte de trames transmises avec succès sur une interface donnée pour laquelle la transmission est bloquée s'il y a plus d'une collision.
Une trame qui est comptée par une instance de cet objet est aussi comptée par l'instance correspondante de l'un des objets *ifOutUcastPkts*, *ifOutMulticastPkts*, ou *ifOutBroadcastPkts*, mais pas par celle l'objet *dot3StatsSingleCollisionFrames*.
- **dot3StatsLateCollisions.** Le nombre de fois qu'une collision est détectée sur une interface particulière, après un délai de 512 bits-temps dans la transmission du paquet.
512 bits-temps correspondent à 51,2 microsecondes sur un système à 10 Mbit/s. Une collision (tardive) incluse dans un compte représenté par une instance de cet objet est considérée comme étant une collision (générique) en vue d'autres statistiques relatives aux collisions.
- **dot3StatsExcessiveCollisions.** Un compte des trames dont la transmission a échoué sur une interface donnée en raison de collisions excessives.

- **dot3StatsCarrierSenseErrors.** Le nombre de fois qu'une condition d'écoute de porteuse a été perdue ou jamais maintenue lors de la tentative de transmission d'une trame sur une interface donnée.

Le compte représenté par une instance de cet objet est incrémenté (au plus) une fois par tentative de transmission, même si la condition d'écoute de porteuse varie durant une tentative.

- **dot3StatsInternalMacReceiveErrors.** Un compte des trames dont la réception sur une interface donnée a échoué en raison d'une erreur de réception interne de la sous-couche MAC. Une trame n'est comptée par une instance de cet objet que si elle est aussi comptée par l'instance correspondante de l'objet *dot3StatsFrameTooLongs*, *dot3StatsAlignmentErrors*, ou *dot3StatsFCSErrors*.

La signification précise du compte représenté par une instance de cet objet est liée à l'implémentation. En particulier, une instance de cet objet peut représenter un compte des erreurs de réception sur une interface donnée qui ne sont autrement pas comptées.

- **dot3StatsInternalMacTransmitErrors.** Un compte des trames dont la transmission sur une interface donnée échoue en raison d'une erreur de transmission interne de la sous-couche MAC. Une trame n'est comptée que par une instance de cet objet que si elle n'est pas comptée par l'instance correspondante de l'objet *dot3StatsLateCollisions*, *dot3StatsExcessiveCollisions* ou *dot3StatsCarrierSenseErrors*.

La signification précise du compte représenté par une instance de cet objet est liée à l'implémentation. En particulier, une instance de cet objet peut représenter un compte des erreurs de transmission sur une interface donnée qui ne sont autrement pas comptées.

- **dot3StatsFrameTooLongs.** Un compte des trames reçues sur une interface donnée, dont la taille excède le maximum autorisé.

Le compte représenté par une instance de cet objet est incrémenté lorsque l'état *frameTooLong* est renvoyé par le service MAC à la sous-couche LLC (ou un autre utilisateur MAC). Les trames reçues avec plusieurs conditions d'erreurs sont, selon les conventions IEEE 802.3 Layer Management, comptées exclusivement en fonction du statut d'erreur présenté à la sous-couche LLC.

Interface CLI

Voici un exemple des résultats renvoyés par la commande CLI qui renseigne sur les comptes d'erreurs par port.

Commande show port counters

Cette commande affiche les compteurs d'erreurs de ports tels que ceux d'erreurs d'alignement, d'erreurs FCS, de statistiques de collisions, etc. :

```
switch 5000 (enable) show port counters
Port Align-Err FCS-Err Xmit-Err Rcv-Err UnderSize
----- -----
1/1      0        0        0        0        0
1/2      0        0        0        0        0
2/7      0        0        0        0        0
2/8     428      159      0        0       718
2/9      0        0        0        0        0

Port Single-Col Multi-Coll Late-Coll Excess-Col Carri-Sen Runts Giants
```

1/1	0	0	0	0	0	0	0
1/2	0	0	0	0	0	0	0
2/1	4855	479	0	0	0	0	0
2/2	775	94	0	0	0	0	0
2/3	65	6	0	0	0	0	0
2/4	69	9	0	0	0	0	0
2/5	354	36	0	0	0	0	0
2/6	0	0	0	0	0	0	0
2/7	104	14	0	0	0	0	0
2/8	0	0	0	0	621	-	

Taux d'utilisation des ports, broadcast, multicast, et unicast

Les administrateurs de réseau sont confrontés au problème de taux de trafic broadcast sur les ports commutés. Comme ce trafic est transmis vers tous les ports d'un VLAN, vous pouvez configurer un port "fictif" participant au VLAN, et ne capturer que le trafic broadcast. Vous pouvez ensuite comparer ce taux au taux maximal théorique de la ligne.

Bases MIB SNMP

Voici les objets MIB SNMP utilisés dans ce contexte. Les informations peuvent être trouvées sur le site Web Cisco :

- **dot1dTpPortInFrames.** Le nombre de trames qui ont été reçues sur ce port sur son segment. Notez qu'une trame reçue sur une interface correspondant à ce port n'est comptée par cet objet que s'il s'agit d'un protocole en cours de traitement par la fonction locale, y compris pour les trames de gestion de pont.
- **dot1dTpPortOutFrames.** Le nombre de trames qui ont été transmises par ce port sur son segment. Notez qu'une trame transmise sur l'interface correspondant à ce port n'est comptée par cet objet que s'il s'agit d'un protocole en cours de traitement par la fonction locale de pontage, y compris pour les trames de gestion de pont.
- **ifInMulticastPkts.** Le nombre de paquets délivrés par cette sous-couche à une (sous-)couche supérieure, qui ont été adressés à une adresse multicast au niveau de cette sous-couche. Pour un protocole de la couche MAC, cela comprend les adresses de groupes et les adresses fonctionnelles.
- **ifInBroadcastPkts.** Le nombre de paquets délivrés par cette sous-couche à une (sous-)couche supérieure, qui ont été adressés à une adresse broadcast au niveau de cette sous-couche.
- **ifOutMulticastPkts.** Le nombre total de paquets dont la transmission a été demandée par des protocoles de couche supérieure, et qui ont été expédiés à une adresse multicast au niveau de cette sous-couche (incluant ceux qui ont été ignorés ou non envoyés). Pour un protocole de la couche MAC, cela comprend les adresses de groupes et des adresses fonctionnelles.
- **ifOutBroadcastPkts.** Le nombre total de paquets dont la transmission a été demandée par des protocoles de couche supérieure, et qui ont été expédiés à une adresse broadcast au niveau de cette sous-couche (incluant ceux qui ont été ignorés ou non envoyés).

- **etherStatsBroadcastPkts.** Le nombre total de paquets corrects reçus qui ont été dirigés vers l'adresse de broadcast. Notez qu'il n'inclut pas les paquets multicast.
- **etherStatsMulticastPkts.** Le nombre total de paquets corrects reçus qui ont été dirigés vers une adresse multicast. Notez qu'il n'inclut pas les paquets envoyés vers l'adresse broadcast.

Interface CLI

Voici un exemple de résultats renvoyés par la commande CLI fournissant des statistiques de niveau MAC.

Commande show mac

Cette commande affiche des statistiques de niveau MAC, telles que le nombre de trames reçues/transmises, le nombre de paquets multicast reçus/transmis, et le nombre de paquets broadcast reçus/transmis :

```
switch 5000 (enable) show mac
```

MAC	Rcv-Frms	Xmit-Frms	Rcv-Multi	Xmit-Multi	Rcv-Broad	Xmit-Broad
1/1	0	0	0	0	0	0
1/2	0	0	0	0	0	0
2/1	7564831	3159859	93795	2982015	7375010	47356
2/2	839319	11317193	97413	2991019	1560	7417591
2/3	40744	10516768	5631	3096045	6	7419192
2/4	40989	10523185	6222	3102759	0	7419195
2/5	87858	10577397	6179	3114275	920	7418557
2/6	0	0	0	0	0	0
2/7	53448	10557561	5632	3124050	0	7419181
2/8	1646786	31124783	1645159	31124783	0	0
2/9	45666	10610469	4980	3150899	543	7418652
2/10	44872	10582388	5723	3158925	118	7417517
2/11	24269744	8525203	24269742	1104787	0	7420184

Utilisation client

Certains clients s'appuient sur leurs commutateurs pour obtenir des informations d'utilisation relatives aux utilisateurs et aux applications, afin de déterminer le niveau de respect de l'accord SLA (*Service-Level Agreement*, accord de niveau de service), et aussi à des fins de facturation par utilisateur ou par groupe. Pour cela, il est recommandé d'examiner les couches situées au-dessus du niveau 2 OSI. Dans cette situation, les commutateurs devraient être traités comme des hubs ou des MAU, et vous devriez exploiter les protocoles de niveaux supérieurs (qui voyageront "au-dessus" du commutateur) pour collecter ces informations.

Si vous voulez connaître le niveau de disponibilité d'un serveur pour ses utilisateurs, vous devriez périodiquement exécuter un **ping** du serveur (mais pas trop fréquemment pour ne pas le congestionner) et mesurer le temps de réponse. Partez du principe que la commutation est réalisée à la vitesse de la ligne, à moins que des données n'indiquent que le commutateur représente un goulet d'étranglement.

Ce chapitre de traite pas de la commutation Cisco Netflow ou multicouche.

Reporting de temps de réponse

Le reporting de temps de réponse est la mesure du temps de réponse entre deux points de réseau pour déterminer les délais d'acheminement. Bien que la plupart des NMS soient capables de réaliser des ping à partir d'une station centrale, vous pouvez également utiliser la base CISCO-PING-MIB pour demander aux routeurs Cisco et à certains commutateurs d'effectuer un ping d'équipements spécifiques et de renvoyer le temps aller-retour. Vous pouvez également découvrir tous les équipements Cisco voisins de routeurs et de commutateurs Cisco en interrogeant la base CISCO-CDP-MIB.

Variables MIB pour les environnements commutés

Cette section identifie, au moyen des Tableaux 14.6 et 14.7, les variables MIB qui sont généralement intéressantes pour l'administration des erreurs et des performances, et explique les erreurs les plus couramment rencontrées.

Tableau 14.6 : Performances d'ensemble de commutateur

<i>Fichier MIB</i>	<i>Objets MIB</i>
CISCO-STACK-MIB	SysTraffic SysTrafficPeak SysTrafficPeaktme SysConfigChangeTime ChassisPs1Status ChassisPs2Status ChassisFanStatus ChassisMinorAlarm ChassisMajorAlarm ChassisTempAlarm ModuleStatus ModulePortStatus ModuleStandbyStatus

Tableau 14.7 : Ports de tronçons et ports de serveur critiques

<i>Fichier MIB</i>	<i>Objets MIB</i>
A partir de CISCO-STACK-MIB basé sur l'objet <i>portIndex</i> (référence croisée avec <i>ifIndex</i> par l'intermédiaire du champ <i>portIfIndex</i> correspondant pour l'instance de table correspondante).	PortOperStatus VlanPortIslOperStatus (trunk ports only) PortAdminSpeed PortDuplex PortSpanTreeFastStart

Tableau 14.7 : Ports de tronçons et ports de serveur critiques (suite)

<i>Fichier MIB</i>	<i>Objets MIB</i>
A partir de ETHERLIKE-MIB basé sur <i>ifIndex</i> .	Dot3StatsAlignmentErrors Dot3StatsFCSErrors dot3StatsSingleCollisionFrames dot3StatsMultipleCollisionFrames dot3StatsLateCollisions dot3StatsExcessiveCollisions dot3StatsInternalMacTransmitErrors dot3StatsInternalMacReceiveErrors dot3StatsDeferredTransmissions
A partir de BRIDGE-MIB basé sur <i>ifIndex</i> .	dot1dStpPortStatus dot1dStpPortForwardTransitions dot1dTlpLearnedEntryDiscards
A partir de RFC1213 basé sur <i>ifIndex</i> . Il est recommandé de surveiller les débits plutôt que les valeurs absolues avec ces compteurs.	if.ifInDiscards if.ifInErrors if.ifOutDiscards if.ifOutErrors if.ifInOctets if.ifOutOctets if.ifInUcastPkts if.ifInNUcastPkts if.ifOutUcastPkts if.fOutNUcastPkts ip.ipInRequests ip.ipInDelivers ip.ipForwDatagrams

Erreurs d'alignement

Les erreurs d'alignement représentent un compte des trames reçues qui ne se terminent pas par un nombre pair d'octets et qui affichent un CRC incorrect.

A réception de paquets d'une taille inférieure à 64 octets et ne se terminant pas sur une limite d'octet (par exemple, un fragment provenant d'une collision), le commutateur Catalyst incrémentera les compteurs *runt counter* et *align-err counter*.

Une erreur d'alignement est révélatrice d'un problème de câble ou d'un transmetteur défaillant sur l'équipement de réseau connecté à l'autre extrémité. La valeur de ce compteur devrait être égale à zéro ou en tout cas très faible. Des erreurs de ce type peuvent se produire lorsque le câble est connecté la première fois. De plus, si un hub est connecté, des collisions entre d'autres équipements qui y sont connectés peuvent aussi provoquer ce genre d'erreurs.

Erreurs FCS

Le compte d'erreurs FCS représente le nombre des trames qui ont été transmises et reçues avec une somme de contrôle incorrecte (valeur CRC) dans la trame Ethernet. Elles sont ignorées et ne sont pas propagées sur les autres ports. Un faible nombre d'erreurs de ce genre est acceptable mais il pourrait aussi indiquer la présence de câbles, de cartes, ou d'autres composants défectueux.

Runts

Les trames *runts* (*nains*) sont trop petites pour un segment Ethernet.

Le comportement de ces trames se caractérise comme suit :

- Avec les paquets d'une taille inférieure à 64 octets (par exemple, des fragments provenant d'une collision) et un CRS incorrect, le commutateur Catalyst incrémentera le compteur *runts counter*.
- Avec les paquets d'une taille inférieure à 64 octets et ne se terminant pas sur une limite d'octet (par exemple, des fragments provenant d'une collision), le commutateur Catalyst incrémentera les compteurs *runts counter* et *align-err counter*.
- Aucune erreur FCS-err n'est journalisée avec des paquets d'une taille inférieure à 64 octets.
- Une erreur FCS-err est journalisée lorsqu'un paquet de 63 octets est reçu et que 4 bits sont ajoutés pour l'erreur *align* et l'erreur *dribble*, provoquant un paquet incorrect de 64 octets (voir Tableau 14.8).

Un faible nombre d'erreurs de ce genre est acceptable mais il pourrait aussi indiquer la présence de câbles, de cartes, ou d'autres composants défectueux. Dans un environnement Ethernet partagée, les trames *runts* sont presque toujours provoquées par des collisions. Si ces trames apparaissent et que le niveau de collisions n'est pas élevé ou s'il s'agit d'un environnement Ethernet, elles peuvent résulter de livraisons incomplètes (*underruns*) ou d'un programme défaillant sur une carte réseau. Connectez un analyseur de protocole pour tenter d'identifier la carte défectueuse en déterminant l'adresse source de ces trames.

Le Tableau 14.8 décrit les compteurs qui sont incrémentés dans certaines situations d'erreurs.

Tableau 14.8 : Conditions d'erreurs associées à des compteurs d'erreurs

<i>Taille de paquets (octets)</i>	<i>Erreur</i>	<i>Compteur de port incrémenté</i>
66-1500		
63		Undersize
63	CRC	Runts
63	align	align-err et runts
63	dribble	Undersize
63	symbol	Runts
63	CRC/align	align-err et runts
63	CRC/align/dribble	FCS-err

Tableau 14.8 : Conditions d'erreurs associées à des compteurs d'erreurs (suite)

<i>Taille de paquets (octets)</i>	<i>Erreur</i>	<i>Compteur de port incrémenté</i>
63	CRC/align/dribble/symbol	FCS-err
63	align/dribble	FCS-err
62	align/dribble	Runts
54	align/dribble	Runts
44	align/dribble	Runts

Les types d'erreurs sont définis de la façon suivante :

- **align.** Quatre bits supplémentaires insérés avant le CRC.
- **CRC.** CRC incorrect généré.
- **symbol.** Sur le premier octet précédent le CRC, le premier groupe de quatre bits générera un symbole invalide.
- **dribble.** Quatre bits supplémentaires ajoutés après le CRC.

Autres objets à surveiller

En règle générale, un réseau doit être surveillé après qu'il ait atteint un état stable. Lorsqu'un sous-système (que ce soit une configuration de modules, de ports, de VLAN, ou d'une autre entité) atteint un niveau stable de fonctionnement, des seuils et des scénarios de corrélation supplémentaires doivent être activés pour le sous-système.

Objets MIB simples

Cette section liste les objets MIB qui devraient être interrogés ainsi que les informations qu'ils fournissent.

MIB-II

Les objets MIB-II listés dans le Tableau 14.9 doivent être surveillés dans le cadre de l'administration de ports.

Tableau 14.9 : Objets MIB-II

<i>Objet MIB</i>	<i>Description</i>	<i>Raison du suivi</i>
ifEntry.ifOperStatus	Etat de fonctionnement de base de port.	Déetecte une transition de port d'un état actif vers un autre état. Il est recommandé de contrôler cette condition uniquement pour les ports de tronçons.
ifEntry.ifLastChange	Surveille les changements de configuration de port inattendus.	Déetecte si des administrateurs effectuent des changements de configuration de ports. Les modifications normales devraient être ignorées.

Tableau 14.9 : Objets MIB-II (suite)

<i>Objet MIB</i>	<i>Description</i>	<i>Raison du suivi</i>
ifEntry.ifInDiscards ifInErrors IfUnknownProtos ifOutDiscards ifOutErrors	Surveille les erreurs d'interface. Surveille les erreurs de trafic IP.	Déetecte les taux élevés d'erreurs de ce genre. <i>ipOutDiscards</i> peut indiquer des échecs de routage de paquets valides de la part du routeur, révélant une insuffisance de tampons ou d'autres conditions spécifiques à cet équipement. <i>ipOutNoRoutes</i> révèle des applications malveillantes ou des attaques de la sécurité génèrent des paquets qui ne peuvent pas être routés. Signale <i>ifOutQLen</i> lorsqu'une telle erreur se produit.
IpInHdrErrors ipInAddrErrors ipInUnknownProtos ipInDiscards ipOutDiscards ipOutNoRoutes ipReasmReqds ipReasmFails ipFragFails ipFragCreates	Surveilles les erreurs de trafic IP.	Déetecte les taux élevés d'erreurs de ce genre.
TcpInErrs tcpOutRsts	Surveille les erreurs de trafic TCP.	Déetecte les taux élevés d'erreurs de ce genre.
udpInErrors	Surveille les erreurs de trafic UDP.	Déetecte les taux élevés d'erreurs de ce genre.
SnmpInBadCommunityNames	Surveille les attaques contre la sécurité visant l'agent SNMP.	Déetecte une augmentation notable du taux de cet objet.
snmpInBadVersions snmpInASNParseErrs snmpInTooBigs snmpInNoSuchNames snmpInBadValues snmpOutTooBigs	Surveille les requêtes NMS.	Déetecte si un NMS génère trop de requêtes invalides, ou de requêtes valides qui conduisent à un nombre excessif de réponses invalides.
snmpInGenErrs	Surveille le comportement des agents SNMP.	Déetecte si un agent SNMP rapporte trop d'erreurs.
snmpEnableAuthenTraps	Surveille que les interceptions sont émises comme configurées.	Déetecte les changements dans cet objet.

CISCO-STACK-MIB

Plusieurs objets MIB de la base CISCO-STACK MIB doivent être surveillés pour garantir une certaine exactitude.

Groupes système et châssis

Le Tableau 14.10 liste les objets MIB des groupes système et châssis qui devraient être surveillés.

Tableau 14.10 : Objets MIB système et châssis

Objet MIB	Description	Raison du suivi
sysIpVlan	VLAN associé à l'adresse IP du commutateur.	Déetecte si le commutateur se trouve dans un VLAN différent de celui prévu. Cela permet de savoir si le trafic administratif entre en collision avec le trafic utilisateur alors qu'ils sont supposés circuler dans des VLAN différents.
sysClearPortTime	Temps (en centièmes de seconde) écoulé depuis que les compteurs de ports ont été réinitialisés. Ecrire un zéro dans cet objet efface toutes les valeurs de compteurs de ports.	Toute interruption (sauf <i>rollover</i>) de ce compteur indique une réinitialisation. Celle-ci doit être détectée car elle affecte les autres activités de collecte de valeurs de référence ou de surveillance.
sysEnableChassisTraps	Permet la génération des interceptions <i>chassisAlarmOn</i> et <i>chassisAlarmOff</i> .	Evite que les interceptions de <i>châssis</i> soient désactivées par inadvertance.
sysEnableModuleTraps	Permet la génération des interceptions <i>moduleUp</i> et <i>moduleDown</i> .	Evite que les interceptions de <i>châssis</i> soient désactivées par inadvertance.
sysEnableBridgeTraps	Permet la génération des interceptions <i>newRoot</i> et <i>topologyChange</i> .	Evite que les interceptions STP soient désactivées par inadvertance.
sysEnableRepeaterTraps	Permet la génération des interceptions RFC1516 <i>rptrHealth</i> , <i>rptrGroupChange</i> et <i>rptrResetEvent</i> .	Evite que les interceptions de répéteurs soient désactivées par inadvertance.
sysEnableIpPermitTraps	Permet la génération des interceptions <i>ipPermitDeniedTrap</i> .	Evite que les interceptions de permissions IP soient désactivées par inadvertance.
sysEnableConfigTraps	Permet la génération des interceptions <i>sysConfigChangeTrap</i> .	Déetecte si la configuration du commutateur est modifiée. Sert le même objectif que les messages Syslog SYS-5-CONFIG#. Collecte la valeur <i>sysConfigChangeTime</i> pour la joindre dans la notification.
sysConfigChangeTime	Durée écoulée depuis le dernier changement de configuration du commutateur.	Déetecte si cet objet présente une interruption (sauf <i>rollover</i>) pour surveiller les changements de configuration.

Tableau 14.10 : Objets MIB système et châssis (suite)

<i>Objet MIB</i>	<i>Description</i>	<i>Raison du suivi</i>
sysEnableEntityTrap	Permet la génération des interceptions <i>entConfigChange</i> .	Déetecte un changement matériel ou logiciel. Cette interception peut aussi être utilisée pour déclencher un nouvel inventaire de l'équipement (<i>moduleTable</i>) pour déterminer une différence dans la configuration.
sysEnableStpxTrap	Permet la génération des interceptions <i>stpxInconsistencyUpdate</i> (de la base CISCO-STP-EXTENSIONS-MIB).	Déetecte une transition UplinkFast d'un état bloquant vers un état de transmission. Garantit que l'indicateur <i>stpxUplinkFastEnabled</i> (de la base CISCO-STP-EXTENSIONS-MIB) est activé lors du test de cette condition.
chassisPs1Status	Etat de la source d'alimentation 1.	Déetecte un problème au niveau de la source d'alimentation 1. Lorsqu'une erreur est détectée, collecte <i>chassisPs1TestResult</i> pour continuer à informer l'opérateur.
chassisPs2Status	Etat de la source d'alimentation 2.	Déetecte un problème au niveau de la source d'alimentation 2. Lorsqu'une erreur est détectée, collecte <i>chassisPs2TestResult</i> pour continuer à informer l'opérateur.
chassisFanStatus	Etat du ventilateur de châssis.	Déetecte un problème avec le ventilateur de châssis. Lorsqu'une erreur est détectée, collecte <i>chassisFanTestResult</i> pour continuer à informer l'opérateur.
chassisMinorAlarm	Etat d'alarme mineure de châssis.	Déetecte les alarmes mineures lorsque l'état de cet objet varie entre désactivé (<i>off</i>) et activé (<i>on</i>). Inclus dans l'interception <i>chassisAlarmOn</i> .
chassisMajorAlarm	Etat d'alarme majeure de châssis.	Déetecte les alarmes majeures lorsque l'état de cet objet varie entre désactivé (<i>off</i>) et activé (<i>on</i>). Inclus dans l'interception <i>chassisAlarmOn</i> .
chassisTempAlarm	Alarme de température de châssis.	Déetecte les alarmes majeures lorsque l'état de cet objet varie entre désactivé (<i>off</i>), activé (<i>on</i>), et critique (<i>critical</i>). Inclus dans l'interception <i>chassisAlarmOn</i> .

Conditions de modules

Le Tableau 14.11 liste les objets MIB de modules (cartes de lignes) qui devraient être surveillés.

Tableau 14.11 : Objets MIB de modules

Objet MIB	Description	Raison du suivi
moduleEntry.moduleSerialNumber moduleEntry.moduleSwVersion	Identifie de façon unique un module par son numéro de série et sa version de logiciel.	Déetecte lorsqu'un de ces objets change.
moduleEntry.moduleStatus	Etat de contrôle du module.	Déetecte si cet objet n'est pas opérationnel, en supposant que <i>moduleEntry.moduleStandbyStatus est active(2)</i> .
moduleEntry.moduleStandbyStatus	Surveille si un module superviseur est en mode actif ou en mode veille.	Déetecte lorsqu'un changement de superviseur se produit. Un module superviseur est identifié par son <i>moduleEntry.moduleType</i> d'un des types valides (voir MIB pour plus d'informations).

Conditions de ports

Le Tableau 14.12 liste les objets MIB de ports qui devraient être surveillés.

Tableau 14.12 : Objets MIB de ports

Objet MIB	Description	Raison du suivi
portEntry.portDuplex	Indique si un port opère en mode semi-duplex ou duplex.	Déetecte un changement duplex. Déetecte si sa valeur est <i>disagree(3)</i> , ce qui indique une non concordance duplex. La notification peut être ignorée si le changement fait partie du fonctionnement normal.
portEntry.portSpanTreeFastStart	Indique si le port passe immédiatement dans un état de transmission.	Déetecte si cet objet passe de l'état activé à l'état désactivé. La notification peut être ignorée si le changement fait partie du fonctionnement normal.
portEntry.portLinkFaultStatus	Surveille les ports Gigabit Ethernet.	Déetecte un changement d'état de l'objet à partir de l'état <i>noFault</i> .
moduleEntry.modulePortStatus	Surveille l'état de modules et de ports (cet objet offre la possibilité de vérifier tous les ports du module avec une seule requête SNMP.)	Déetecte un changement de cet objet. Lorsque c'est le cas, il détermine s'il s'agit d'un changement d'état de module ou de port. Si c'est un port, il indique celui qui est concerné. Rapporte <i>ifOperStatus</i> et <i>ifAdminStatus</i> en utilisant son objet <i>portEntry.portIfIndex</i> correspondant pour lire via index dans <i>ifTable</i> .

Tableau 14.12 : Objets MIB de ports (suite)

<i>Objet MIB</i>	<i>Description</i>	<i>Raison du suivi</i>
portEntry.portOperStatus	Surveille les échecs de port. Cette fonction serait exécutée si la condition précédente ne s'appliquait pas à tous les ports mais seulement à certains ports spécifiques.	Déetecte si cet objet n'est pas opérationnel, en supposant qu'il ne se trouve pas sur un module superviseur en mode veille. Rapporte <i>ifOperStatus</i> et <i>ifAdminStatus</i> en utilisant son objet <i>portEntry.portIfIndex</i> correspondant pour lire via index dans <i>ifTable</i> .
portEntry.portLinkFaultStatus	Surveille les liaisons Gigabit.	Déetecte si cet objet ne présente pas l'état <i>noFault(1)</i> ou passe vers un autre état.

Conditions de tronçons

Le Tableau 14.13 liste les objets MIB de tronçons qui devraient être surveillés.

Tableau 14.13 : Objets MIB de tronçons

<i>Objet MIB</i>	<i>Description</i>	<i>Raison du suivi</i>
vlanPortEntry.vlanPortIsAdminStatus	Surveille les tronçons qui sont configurés en tant que tel.	Déetecte un échec de fonctionnement de tronçon. Pour que des ports connus (en supposant une configuration avec ports prédéfinis) puisse être des ports de tronçons entre des commutateurs, comme défini par <i>portEntry.portModuleIndex</i> et <i>portEntry.portIndex</i> , lit leur objet <i>portEntry.portIfIndex</i> correspondant et utilise cette valeur pour lire via index dans la table <i>ifTable</i> leur objet <i>ifEntry.ifAdminStatus = up</i> et <i>ifEntry.ifOperStatus = up</i> . Pour ces mêmes ports, utilise <i>portModuleIndex</i> et <i>portIndex</i> pour lire via index dans la table <i>vlanPortEntry</i> et vérifier que leur objet <i>vlanPortIsAdminStatus = trunking</i> .

Conditions de VLAN

Le Tableau 14.14 liste les objets MIB de VLAN qui devraient être surveillés.

Tableau 14.14 : Objets MIB de VLAN

<i>Objet MIB</i>	<i>Description</i>	<i>Raison du suivi</i>
vlanEntry.vlanSpanningTreeEnable	Surveille l'activation de STP par VLAN.	Déetecte tout changement dans la configuration STP de VLAN.
vlanEntry.vlanPortVlan	Surveille lorsqu'un port est déplacé vers un VLAN différent, pour des raisons de sécurité et d'ingénierie de trafic.	Surveille l'appartenance VLAN de chaque port. Rapporte <i>vlanPortModule</i> et <i>vlanPort</i> dans la notification.

Tableau 14.14 : Objets MIB de VLAN (suite)

Objet MIB	Description	Raison du suivi
vlanEntry.vlanPortIslOperStatus	Surveille les ports de tronçons.	Pour chaque port dans le mode de tronçons, détecte un changement de l'objet vers le mode <i>notTrunking</i> , et vice versa. Rapporte <i>vlanPortModule</i> et <i>vlanPort</i> dans la notification.
vlanEntry.vlanPortOperStatus	Surveille l'état du VLAN sur les ports.	En supposant que cette condition s'applique à tous les ports en mode actif, détecte un changement d'état de l'objet. Rapporte les objets <i>vlanPortModule</i> et <i>vlanPort</i> correspondants dans la notification.

Conditions EtherChannel

Le Tableau 14.15 liste les objets MIB pour EtherChannel qui devraient être surveillés.

Tableau 14.15 : Objets MIB pour EtherChannel

Objet MIB	Description	Raison du suivi
portChannelEntry.portChanelPorts	Surveille les ports assignés à un seul canal EtherChannel.	Déetecte l'ajout ou la suppression de ports d'un EtherChannel. Rapporte <i>portChannelModuleIndex</i> , <i>portChannelPortIndex</i> , et <i>portChannelIfIndex</i> dans la notification à l'opérateur.
portChannelOperStatus	Surveille l'état des ports EtherChannel.	Déetecte les changements d'état. Rapporte <i>portChannelModuleIndex</i> , <i>portChannelPortIndex</i> , et <i>portChannelIfIndex</i> dans la notification à l'opérateur.
PortChannelNeighbourDeviceId portChannelNeighbourPortId	Surveille si l'autre extrémité de l'EtherChannel est modifiée.	Déetecte le changement de valeur de ces objets. Rapporte <i>portChannelModuleIndex</i> , <i>portChannelPortIndex</i> , et <i>portChannelIfIndex</i> dans la notification à l'opérateur.

Conditions RSM

Le Tableau 14.16 liste les objets MIB pour le module RSM qui devraient être surveillés.

Tableau 14.16 : Objets MIB pour module RSM

Objet MIB	Description	Raison du suivi
moduleIpAddress	Surveille les routes RSM.	Pour les modules wsx5302 et wsx5304, lit leur objet <i>moduleIPAddress</i> . Utilise ensuite l'adresse IP découverte pour lire les informations MIB-II. Applique les règles définies plus haut pour MIB-II.

Conditions diverses

Le Tableau 14.17 liste les objets MIB génériques qui devraient être surveillés.

Tableau 14.17 : Objets MIB divers

Objet MIB	Description	Raison du suivi
tftpHost tftpFile tftpModule	Surveille lorsque de nouvelles images peuvent être chargées.	Pour chaque <i>tftpModule</i> qui est configuré sur le commutateur, vérifie que la combinaison de ces trois objets est correcte (c'est-à-dire, comme prévue). Notifie l'opérateur si une incohérence est détectée.
tftpResult	Surveille les transferts tftp.	Déetecte un échec de cet objet. Informe l'opérateur si cet objet est dans un état <i>inProgress</i> . Alerte l'opérateur pour toutes les autres valeurs de cet objet.
Objets scalaires de pont-routeur dans le groupe <i>brouter</i>	Surveille la configuration du pont-routeur (<i>brouter</i>). Ce groupe s'applique à FDDI.	Déetecte un changement dans la configuration du pont-routeur. Applicable seulement aux interfaces FDDI.
brouterPortEntry.brouterPortBridgeVlan	Surveille l'appartenance VLAN du port de pont-routeur.	Déetecte le placement d'un port dans un VLAN différent. Applicable aux interfaces FDDI seulement.
mcastRouterEntry.mcastRouterOperStatus mcastEnableCgmp mcastEnableIgmp	Surveille si le multicast est activé sur le routeur.	Déetecte un changement d'état de port ou si des caractéristiques sont activées.
dnsGrp.dnsenable	Surveille la configuration DNS.	Déetecte un changement d'état DNS. Transmet <i>dnsServerTable</i> avec la notification.
dnsServerEntry.dnsServerType	Surveille les entrées de serveur DNS.	Déetecte un changement de type d'une entrée DNS. Génère une alerte critique si une entrée est supprimée.
syslogServerEntry.syslogHostEnable	Surveille la configuration Syslog du commutateur.	Déetecte si des messages Syslog ne sont plus envoyés aux hôtes corrects.
syslogServerEntry	Surveille la configuration Syslog du commutateur.	Déetecte une suppression d'entrée.

Tableau 14.17 : Objets MIB divers (suite)

Objet MIB	Description	Raison du suivi
syslogMessageControlEntry.syslog-MessageFacility syslogMessageSeverity	Surveille la configuration Syslog du commutateur.	Déetecte si un service est journalisé avec une gravité inférieure (signifiant davantage de messages Syslog) ou supérieure (signifiant moins de messages Syslog).
tacacsGrp.tacacsLoginAuthentication tacacsEnableAuthentication tacacsLocalLoginAuthentication tacacsLocalEnableAuthentication tacacsDirectedRequest	Surveille la configuration TACACS. Seulement applicable si TACACS est utilisé sur le commutateur.	Déetecte un changement de ces objets, indiquant l'activation ou la désactivation de fonctions TACACS.
ipPermitEnable	Surveille si une session Telnet à distance avec le commutateur est autorisée.	Déetecte un changement d'état, indiquant une perte d'accès Telnet distant ou une faille de sécurité, s'il ne s'agit pas d'un changement de configuration autorisé.
ipPermitListEntry	Surveille les sessions Telnet autorisées avec le commutateur.	Déetecte l'ajout ou la suppression d'entrées. Rapporte <i>ipPermitAddress</i> à l'opérateur.
ipPermitDeniedListEntry	Surveille les accès refusés sur le commutateur.	Déetecte l'ajout d'entrées dans cette table. Rapporte <i>ipPermitDeniedAddress</i> , <i>ipPermitDeniedAccess</i> , et <i>ipPermitDeniedTime</i> à l'opérateur.

Autres corrélations

Les scénarios de corrélation d'événements de cette section peuvent être développés pour un commutateur Catalyst 5000.

Scénario 1. Déteсter que tous les modules ont été activés comme prévu. Ce scénario demande de connaître le nombre de modules existants sur le commutateur. Il peut être extrait de *chassis-Grp.chassisNumSlots*.

Après le redémarrage d'un commutateur (SYS-5: *system reset*) ou la réception d'une interception *coldStart*, vérifiez que tous les modules voulus sont à nouveau en ligne, par l'intermédiaire du message *Syslog SYS-5: Module x is online*, où x est l'indice de module. Un autre méthode permettant de détecter cette situation est de traiter l'interception *sysConfigChangeTrap* (avec *varBind* contenant l'indice de module). Corrélez l'interrogation et l'interception pour éviter l'envoi de notifications dupliquées à l'opérateur. Incluez dans la notification, la valeur de l'objet *moduleEntry* correspondant en fonction de l'indice de module donné.

Sinon, vous pouvez surveiller la valeur de *chassisSlotConfig* pour voir si la valeur n'a pas changé.

Scénario 2. Distinguer les erreurs mineures de source d'alimentation des erreurs majeures.

Générez une notification mineure ou majeure à l'opérateur selon le niveau d'erreur de la source d'alimentation (selon la valeur des objets *chassisPs1Status* ou *statusPs2Status*).

Scénario 3. Effectuer la corrélation des interceptions d'alarmes de châssis avec l'interrogation d'objet MIB pour rechercher un changement d'état.

Associez tout changement d'état de *chassisTempAlarm*, *chassisMinorAlarm*, ou *chassisMajorAlarm* avec une interception *chassisAlarmOn* pour vous assurer qu'une seule notification est envoyée à l'opérateur pour le même problème, selon la nouvelle valeur de l'un de ces objets. Emettez, intensifiez, ou supprimez l'alarme en conséquence.

Assurez-vous que l'objet *sysEnableChassisTraps* est activé pour que ce scénario puisse fonctionner.

Scénario 4. Surveiller les modules superviseurs.

Pour tous les modules dont le type (*moduleType*) correspond à un module superviseur (valeur = 23, 38 à 42, 57, 78, ou 300), effectuez les contrôles périodiques suivants. Dans les notifications à l'opérateur, incluez *moduleName*, *moduleModel*, *moduleHwVersion*, *moduleFwVersion*, et *moduleSwVersion*.

Surveillez leur état avec *moduleStatus* et générez une alarme correspondant au niveau de gravité du champ d'état. Ajoutez l'objet *moduleTestResult* dans la notification à l'opérateur.

Vérifiez que la version de microprogramme est correcte en contrôlant que les champs *moduleHwVersion*, *moduleFwVersion*, et *moduleSwVersion* contiennent les valeurs attendues. Si le moteur de corrélation ne peut pas comparer les chaînes, les objets MIB *moduleHwHiVersion*, *moduleHwLoVersion*, *moduleFwHiVersion*, *moduleFwLoVersion*, *moduleSwHiVersion*, et *moduleSwLoVersion* sont conformes à ce qu'ils sont supposés être.

Déetectez lorsqu'une carte superviseur passe de l'état actif en mode veille, ou vice versa, en surveillant l'objet *moduleStandbyStatus*. Déetectez aussi lorsque cet objet n'est ni actif ni en veille.

A partir de tous les modules superviseurs installés (comme défini par *moduleType*), assurez-vous que l'un d'entre eux est actif (*moduleStandbyStatus* est actif) et que tous les autres sont en mode veille.

Scénario 5. Surveiller les ports de cartes superviseurs.

Pour tous les modules dont le type (*moduleType*) correspond à un module superviseur (valeur = 23, 38 à 42, 57, 78, ou 300), effectuez les contrôles périodiques suivants sur les ports dont les objets *portModuleIndex* (dans la table *portTable*) se vérifient avec l'indice d'un module superviseur (dans la table *moduleTable*). Dans les notifications envoyées à l'opérateur, incluez *moduleName* et *moduleModel*, et *moduleHwVersion*, *moduleFwVersion*, et *moduleSwVersion*.

Surveillez *modulePortStatus* (décoder la chaîne d'octet comme spécifié dans la MIB). Rapportez tout changement d'état.

Vérifiez que lorsqu'un objet *moduleStandbyStatus* de module est *active(2)*, les ports sur ce module présentent un état correct s'ils sont utilisés, en contrôlant le champ *portOperStatus* dans la table *portTable*. Notez qu'une prochaine version de Catalyst 5000 rendra actifs les ports même sur les cartes superviseurs en mode veille, ce qui affectera ce scénario.

Scénario 6. Surveiller le contrôle de flux des ports.

Pour chaque port dans la table *portTable*, détectez les divergences entre les objets suivants :

- portAdminRxFlowControl et portOperRxFlowControl
- portAdminTxFlowControl et portOperTxFlowControl

Scénario 7. Vérifier que les liens sont connectés aux ports appropriés sur les autres commutateurs.

En utilisant la base CDP MIB de Cisco, vérifier que chaque port connu comme étant un tronçon (étant donné les valeurs prédéfinies de *portEntry.portModuleIndex* et *portEntry.portIndex*) sur un commutateur est configuré avec CDP. Par exemple, *cdpInterfaceEntry.cdpInterfaceEnable* = true lorsque *cdpInterface.cdpInterfaceIfIndex* correspond à *portEntry.portIfIndex*.

Pour les mêmes ports identifiés dans l'étape précédente, vérifiez les entrées de *cdpCacheEntry* avec les expressions suivantes :

- *cdpCacheEntry.cdpCacheIfIndex* = *portEntry.portIfIndex* (étant donné les objets *portEntry.portModuleIndex* et *portEntry.portIndex* prédéfinis)
- et
- *cdpCacheEntry.cdpCacheDeviceIndex* = 1..N

Les objets *cdpCacheEntry.cdpCacheDeviceId* et *cdpCacheEntry.cdpCacheDevicePort* correspondants ont la valeur attendue.

Scénario 8. Pour chaque VLAN sur ce commutateur, réaliser les étapes suivantes :

- Vérifiez que les ports de tronçons prévus pour être configurés dans ce VLAN existent. Si un port existe :
 - Vérifiez qu'ils sont configurés comme ISL.
 - Vérifiez que le port est configuré pour un VLAN statique (supposition adoptée dans ce scénario).
 - Vérifiez que STP est activé sur le port.
 - Recueillez son état STP et rapportez les différences avec un état précédent connu.
- Vérifiez que les ports avec *vlanPortEntry.vlanPortIslOperStatus* configurés avec la valeur *trunking(1)* ont leur objet *vlanPortEntry.vlanPortIslAdminStatus* correspondant configuré sur *on(1)* ou *noNegotiate(5)*.

Pour chaque port dans l'étape précédente, procédez comme suit :

- Vérifiez que son *vlanPortEntry.vlanPortAdminStatus* est défini avec la valeur *static*.
- Recherchez dans la table *vlanTable* des entrées pour lesquelles *vlanEntry.vlanIfIndex* correspond au module/port prédéfini par tronçons, et vérifiez que son *vlanEntry.vlanSpanTreeEnable* = *enabled(1)*.
- Utilisez l'objet *portEntry.portCrossIndex* correspondant pour lire *via index* dans *RFC1493.dot1dStpPortEntry* (ou *portEntry.portCrossIndex* = *RFC1493.dot1dStpPortEntry.dot1dStpPort*) afin de recueillir *RFC1493.dot1dStpPortEntry.dot1dStpPortState* et rapporter tout changement d'état.

Recommandations sur les routeur Cisco

Cette section fournit des informations sur la gestion de réseau pour les routeurs Cisco. Visitez le site Web Cisco pour obtenir davantage d'informations sur la surveillance du routeur et du réseau et de leurs performances.

Gestion des erreurs

L'objectif principal de la gestion des erreurs est de détecter les problèmes et d'en informer les utilisateurs le plus tôt possible pour que des mesures soient adoptées avant que les performances ne se dégradent. Cette section débute par un examen des fonctions de la gestion d'erreurs puis se concentre sur les différentes options disponibles pour l'implémentation.

Voici la liste des principales fonctions :

- surveillance de l'état du réseau ;
- détection et notification des problèmes ;
- analyse des problèmes et rétablissement des services.

Surveillance de l'état du réseau

La capacité de détecter rapidement les problèmes survenant sur le réseau est primordial. Le personnel d'exploitation du réseau peut s'appuyer sur une carte graphique du réseau pour afficher les états opérationnels des éléments vitaux tels que les routeurs et les commutateurs. La plupart des logiciels commerciaux de gestion de réseau peuvent assurer la découverte des différents équipements. Chacun d'eux est représenté par un élément graphique sur la console d'administration de la plate-forme. Différentes couleurs sur les éléments graphiques représentent l'état opérationnel actuel des équipements. Ces produits peuvent aussi recevoir et afficher des événements générés à partir des équipements de réseau.

Les équipements de réseau peuvent être configurés pour envoyer des notifications aux plates-formes d'administration du réseau. A réception des notifications, les éléments graphiques figurant les équipements changent de couleur selon le niveau de gravité de la notification reçue.

Détection et notification des problèmes

Il existe des méthodes permettant de détecter les erreurs survenant sur un réseau composé de routeurs et de commutateurs Cisco. Les plus courantes font usage des messages Syslog, des interceptions SNMP, et de RMON. Les équipements Cisco sont capables d'envoyer des messages Syslog à un serveur Syslog. Il s'agit de messages système émanant de routeurs/commutateurs et décrivant différentes conditions de l'équipement. Les interceptions SNMP transmises par les équipements sont utiles pour signaler les conditions d'erreurs.

Tous les messages Syslog et les interceptions n'indiquent pas forcément une condition d'erreur sur un équipement. Certains messages sont informatifs et ne nécessitent pas d'actions de la part de l'utilisateur. Le volume des messages Syslog et des interceptions envoyés par un équipement peut être limité par l'application de commandes spécifiques dans le fichier de configuration.

Messages Syslog

Les messages Syslog envoyés par les routeurs et les commutateurs peuvent être dirigés vers un ou plusieurs serveurs Syslog. Les équipements peuvent être configurés pour n'envoyer que certains messages. En limitant leur nombre, un utilisateur peut se concentrer sur certains aspects spécifiques de fonctionnement du réseau. Par exemple, le message Syslog suivant apparaît lorsqu'une interface sur un routeur tombe en panne :

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1, changed state to down
```

Les messages Syslog envoyés par les équipements peuvent être collectés par n'importe quel démon Syslog de type Unix à des fins d'analyse mais aussi de création de rapports et d'adoption de mesures appropriées.

SNMP

Les équipements Cisco configurés avec SNMP peuvent être interrogés en vue d'obtenir diverses informations. De plus, ils peuvent envoyer des interceptions vers une station d'administration lorsque des conditions spécifiques se produisent. En configurant ces équipements pour la gestion des interceptions SNMP, des conditions révélatrices peuvent être détectées rapidement. Un utilisateur peut rapidement déterminer l'état fonctionnel de toutes les interfaces sur un routeur, *via* SNMP par exemple, sans avoir à entrer les commandes CLI ordinaires. Le Tableau 14.18 présente un échantillon des informations retournées *via* SNMP.

Tableau 14.18 : Etat des interfaces de réseau obtenu *via* SNMP

<i>Index</i>	<i>Description</i>	<i>AdminStatus</i>	<i>OperStatus</i>
1	Ethernet0	Up	Up
2	Ethernet1	Up	Up
3	FastEthernet0	Up	Up
4	Fddi0	Up	Up
5	Tunnel0	Up	Down

La commande CLI permettant d'afficher l'état de l'interface est la suivante :

```
gateway> show interface ethernet 0

Ethernet0 is up, line protocol is up (OperStatus)
Hardware is Lance, address is 0000.0c38.1669 (bia 0000.0c38.1669)
Internet address is 172.16.97.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:00, output hang never
```

Outre les bases MIB standards, les routeurs et les commutateurs Cisco supportent une variété de bases MIB spécifiques aux équipements Cisco. Elles vous permettent de collecter des données de fonctionnement sur chaque dispositif. En voici une liste partielle :

- **Bases spécifiques aux technologies.** RNIS (ISDN), LANE, CIP, DLSW+, Frame Relay, ATM, etc.
- **Bases spécifiques aux routeurs.** Pool de mémoire, châssis, processeur, mémoire flash, etc.
- **Bases spécifiques aux commutateurs.** VLAN, STACK, VTP, VMPS, CDP, etc.

La plupart des fichiers MIB définissent aussi des interceptions SNMP. Chaque définition d'interception liste les objets MIB inclus dans la PDU d'interception et les conditions l'ayant générée. Le Tableau 14.19 liste par catégories les interceptions SNMP définies dans les fichiers MIB de routeur.

Tableau 14.19 : Liste des interceptions SNMP pour les routeurs Cisco

<i>Fichier MIB</i>	<i>Interceptions supportées</i>
Mécanismes internes de routeur	
CISCO-FLASH	ciscoFlashCopyCompletionTrap ciscoFlashPartitioningCompletionTrap ciscoFlashMiscOpCompletionTrap ciscoFlashDeviceChangeTrap
CISCO-ACCESS-ENVMON	caemTemperatureNotification
CISCO-ENVMON	ciscoEnvMonShutdownNotification ciscoEnvMonVoltageNotification ciscoEnvMonTemperatureNotification ciscoEnvMonFanNotification ciscoEnvMonRedundantSupplyNotification
CISCO-CONFIG-MAN	ciscoConfigManEvent
SNA	
CISCO-RSRB	rsrbPeerStateChangeNotification
CISCO-DLSW	ciscoDlswTrapTConnPartnerReject ciscoDlswTrapTConnProtViolation ciscoDlswTrapTConnUp ciscoDlswTrapTConnDown ciscoDlswTrapCircuitUp ciscoDlswTrapCircuitDown
CISCO-CHANNEL	cipCardLinkFailure cipCardDtrBrdLinkFailure
CISCO-DSPU	newdspuPuStateChangeTrap newdspuPuActivationFailureTrap newdspuLuStateChangeTrap dspuLuActivationFailureTrap dspuSapStateChangeTrap

Tableau 14.19 : Liste des interceptions SNMP pour les routeurs Cisco (suite)

<i>Fichier MIB</i>	<i>Interceptions supportées</i>
CISCO-CIPCSNA	cipCsnaOpenDuplicateSapFailure cipCsnaLlc2ConnectionLimitExceeded
CISCO-BSTUN	bstunPeerStateChangeNotification
CISCO-STUN	stunPeerStateChangeNotification
CISCO-SNA-LLC	llcCcStatusChange
CISCO-SDLLC	convSdllcPeerStateChangeNotification
RNIS	
CISCO-ISDN	demandNbrCallInformation demandNbrCallDetails
FRAME RELAY	
RFC 1315 (Frame Relay)	frDLCIStatusChange
X.25	
RFC 1382 (X.25)	x25Restart x25Reset

RMON

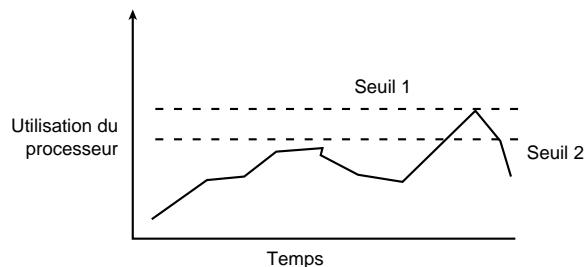
La section précédente a montré comment les interceptions SNMP pouvaient envoyer des alertes à une station d'administration. Cette approche réactive est utile pour informer les opérateurs de réseau d'un problème. Une approche encore plus proactive serait d'informer les opérateurs avant qu'un problème potentiel n'affecte l'équipement. Par exemple, les performances deviendraient problématique si le pourcentage d'utilisation du processeur sur un routeur atteignait une valeur élevée. L'approche ordinaire qui consiste à interroger le routeur avec SNMP pour connaître son taux d'utilisation pourrait manquer l'événement en raison de l'intervalle d'interrogation choisi. En utilisant le support RMON sur les équipements Cisco, ceux-ci peuvent être configurés pour surveiller l'utilisation du processeur et envoyer une alerte seulement lorsqu'un seuil est atteint (c'est-à-dire lorsque le taux d'utilisation atteint 90).

La Figure 14.2 montre comment RMON peut être exploité pour contrôler l'usage du processeur. L'équipement prélève la valeur d'utilisation du processeur à intervalles prédéfinis. Si elle atteint le Seuil 1, un événement peut être généré pour en informer l'utilisateur ou une entrée peut être consignée dans la table RMON consultable. Le Seuil 2 est défini pour réactiver la surveillance lorsque l'utilisation du processeur atteint cette valeur. RMON élimine le besoin d'interrogation régulière à partir d'une console d'administration et réduit le volume du trafic SNMP sur le réseau.

D'autres statistiques pouvant être surveillées au moyen de RMON incluent les pertes en entrée/sortie, les échecs de tampon, les températures internes, le nombre de paquets BECN/FECN Frame Relay, etc.

Figure 14.2

Définition des seuils pour l'utilisation du processeur au moyen de RMON.



Analyse des problèmes et rétablissement des services

Les événements observés sur la console d'administration doivent être diagnostiqués pour déterminer le niveau de gravité d'un problème et l'action corrective à entreprendre. Avec les messages Syslog, la gravité et la description du problème peuvent être déterminés rapidement grâce au texte qu'ils contiennent. Les mesures correctives peuvent être adoptées après avoir déterminé la nature du problème.

Mécanismes internes du système

Les messages Syslog du Tableau 14.20 ont été identifiés comme étant des conditions que vous pourriez vouloir surveiller. La liste n'est pas exhaustive et ne traite que les messages liés au système. Elle ne tient pas compte de ceux concernant les protocoles de routage et les interfaces de réseau spécifiques comme X.25, RNIS, Frame Relay, etc.

Tableau 14.20 : Messages Syslog à surveiller

Message Syslog	Description	Raison du suivi
%SYS-4-SNMP_HOSTCONFIGSET: SNMP hostConfigSet request. Loading configuration from...	Ces messages indiquent que le routeur est en train de charger une nouvelle configuration.	Ces messages peuvent indiquer une condition légitime initiée par un opérateur de réseau ou un problème logiciel/matériel du routeur ayant provoqué ce chargement de configuration.
%SYS-4-SNMP_NETCONFIGSET: SNMP netConfigSet request. Loading configuration from...		
%IP-4-DUPADDR	Ce message indique que le routeur a détecté une adresse IP dupliquée.	Cette condition peut sérieusement affecter le réseau si l'adresse IP dupliquée se rapporte à un routeur ou un serveur.
%IPRT-3-NOMEMORY	Ce message rapporte une insuffisance de mémoire sur le routeur.	Les conditions de mémoire insuffisantes doivent absolument être surveillées car elles peuvent considérablement affecter le fonctionnement du routeur.
%SYS-...	Ces messages système concernent les mécanismes internes du routeur.	Sélectionnez les messages intéressant pour votre environnement.

Surveillance de l'environnement

Certains modèles de routeurs Cisco peuvent réaliser un suivi des dispositifs environnementaux pour surveiller les conditions d'alimentation et de température. Des capteurs sur la carte obtiennent périodiquement des mesures concernant le châssis et vérifient qu'ils se situent dans les limites voulues. Des messages d'avertissement sont affichés sur la console pour les valeurs hors limites.

L'état de l'environnement est accessibles *via* SNMP à partir des routeurs supportant les bases MIB OLD-CISCO-ENV-MIB, CISCO-ENVMON-MIB, ou CISCO-ACCESS-ENVMON-MIB. Les objets définis dans les fichiers MIB peuvent renvoyer des informations similaires à celles fournies par les commandes CLI.

Dans le Tableau 14.21, les valeurs de tension sont obtenues à partir d'objets définis dans la base CISCO-ENVMON-MIB. Les valeurs renvoyées correspondent à celles obtenues avec la commande CLI de l'IOS **show environmental**. En plus de fournir des objets SNMP pour surveiller la température et la tension, les bases CISCO-ENVMON-MIB et CISCO-ACCESS-ENVMON-MIB disposent aussi d'interceptions prédéfinies. Elles sont envoyées vers une console d'administration lorsque les mesures sortent des limites normales. Reportez-vous à la section "Gestion des erreurs" plus haut dans ce chapitre pour obtenir davantage d'informations concernant les interceptions supportées.

Tableau 14.21 : Table d'état de la tension

Description	Valeur	Limite inf.	Limite sup.	LastShutdown	Etat
Tension +12	12308	10904	13384	12308	Normal
Tension +5	5171	4606	5698	5171	Normal
Tension -12	-12073	-10146	-13859	-12073	Normal
Tension +24	24247	20377	27646	24247	Normal
Référence 2.5	2490	1250	3714	0	Normal

Le Tableau 14.22 liste les messages Syslog concernant l'environnement.

Tableau 14.22 : Messages Syslog concernant l'environnement

Message Syslog	Description	Raison du suivi
%ENV- <i>x</i> , %ENVM- <i>x</i> , %CI-3-BLOWER, %CI-1-BLOWSHUT, %CI-2-ENVCRIT, %CI-4-ENVWARN, %SYS-1-OVERTEMP	Ces messages signalent des problèmes liés au ventilateur et à la température à l'intérieur du routeur.	N'importe lequel de ces messages peut être révélateur d'une panne imminente du routeur.
%CI-3-PSFAIL	Ces messages signalent un problème système comme une panne de la source d'alimentation.	Tous ces messages devraient être considérés comme critiques.

Gestion des performances

Il s'agit d'un domaine fonctionnel qui traite de divers aspects des performances du réseau. On peut évaluer les performances d'un réseau en mesurant les temps de réponse, l'utilisation de la ligne, le débit, etc. Une base de référence peut être élaborée et servir à comparer les mesures prélevées périodiquement. Il est ainsi possible de déterminer si les performances réelles sont alignées par rapport aux métriques définies dans l'accord de niveau de service. Cette section étudie brièvement plusieurs aspects de la gestion des performances en général. L'objectif principal est de démontrer la façon dont les valeurs de performances d'un routeur peuvent être prélevées et examinées en utilisant SNMP.

Les tâches impliquées dans cette gestion sont les suivantes :

1. Définition des valeurs de référence pour les performances du réseau.
2. Définition d'un accord de niveau de service et de métriques.
3. Suivi et mesure des performances.
4. Définition du reporting des seuils et des exceptions.
5. Analyse et mise au point.

Définition des valeurs de référence pour les performances du réseau

Pour définir des valeurs de référence, il faut prélever de façon continue pendant une certaine période des échantillons de statistiques sur les performances du réseau. Ces informations peuvent être collectées au moyen d'une sonde autonome reliée à un segment de LAN ou à une liaison WAN. Les données sont ensuite utilisées pour déterminer un modèle de comportement du trafic qui est jugé comme normal pour le réseau. Les mesures qui seront prises dans le futur pourront ainsi être comparées avec ces résultats de référence afin de pouvoir juger de la qualité des performances.

Définition d'un accord de niveau de service et de métriques

L'accord de niveau de service ou SLA (*Service Level Agreement*) implique la définition de caractéristiques spécifiques de performances du réseau. L'accord prévoit certaines métriques de performances qui sont utilisées pour mesurer le niveau de service réel offert par rapport à celui qui aura été prévu. C'est un accord qui est couramment conclu entre un fournisseur de services et un utilisateur. Parmi les métriques de performances du réseau, on peut citer les temps de réponse, la disponibilité, etc.

Suivi et évaluation des performances

Les performances d'un réseau sont directement liées à l'état fonctionnel de ses équipements. Les composants matériels et logiciels d'un équipement de réseau peuvent aussi influer sur les performances, et un seul composant défectueux peut même provoquer une interruption totale des services. Il est vital de surveiller aussi l'environnement du réseau, et tout particulièrement des éléments comme l'alimentation, la température, la ventilation, et s'assurer que ceux-ci fonctionnent conformément aux spécifications données. Des composants logiciels tels que les tampons, la mémoire, etc., peuvent également avoir un impact significatif sur les protocoles exécutés sur l'équipement.

Utilisation du processeur et allocation des tampons ou autres zones de mémoire

Le taux d'utilisation du processeur est un indicateur utile pour évaluer le niveau de performances d'un routeur. En mesurant l'emploi des ressources processeur sur une durée prolongée, il est possible d'identifier une tendance et de déterminer un modèle de comportement du trafic. Les routeurs s'exécutant constamment avec de forts pourcentages d'utilisation peuvent affecter les performances globales des services de transmission et de traitement des paquets. Il existe des commandes CLI de routeur qui permettent d'afficher des informations sur le niveau d'utilisation des ressources processeur et sur les processus actifs. Ces données peuvent être lues au moyen d'objets définis dans le fichier OLD-CISCO-CPU-MIB. Voici un exemple d'informations sur l'utilisation des ressources processeur renvoyées par la commande CLI **show processes** :

```
Router# show processes
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%

  PID QTy      PC Runtime (ms)    Invoked   uSecs     Stacks TTY Process
    1 Mwe 6039CCC8      2203448    9944378    221 7392/9000    0 IP-EIGRP Router
    2 Lst 60133594      329612     34288    9613 5760/6000    0 Check heaps
    3 Cwe 6011D820        0          1      0 5648/6000    0 Pool Manager
    4 Mst 6015FAA8        0          2      0 5608/6000    0 Timers
```

L'utilisation des ressources processeur peut être découverte au moyen des objets MIB du Tableau 14.23.

Tableau 14.23 : Objets MIB de la base OLD-CISCO-CPU-MIB pour surveiller les ressources processeur

Objets	Description	OID
busyPer	Pourcentage d'occupation CPU durant les 5 dernières secondes.	1.3.6.1.4.1.9.2.1.56
avgBusy1	Moyenne variable sur une minute du pourcentage d'occupation CPU.	1.3.6.1.4.1.9.2.1.57
AvgBusy5	Moyenne variable sur cinq minutes du pourcentage d'occupation CPU.	1.3.6.1.4.1.9.2.1.58

La quantité de mémoire principale restante qu'un processeur peut utiliser a une influence prépondérante sur les performances. Les tampons sont alloués à partir de la mémoire dans différents pools utilisés par un protocole. Les paquets IPX SAP, par exemple, utilisent les tampons de "taille moyenne" (*middle buffer*) lors de l'envoi de paquets. Les commandes CLI suivantes sont habituellement utilisées pour assurer un suivi des statistiques de mémoire et de tampon sur un routeur :

- **show memory ;**
- **show buffers ;**
- **show interface.**

Les valeurs collectées au moyen des commandes CLI sont accessibles *via* SNMP. A cet effet, Cisco fournit les fichiers MIB suivants qui permettent d'obtenir des informations équivalentes à celles renvoyées par les commandes : CISCO-MEMORY-POOL-MIB, OLD-CISCO-INTERFACES-MIB, et OLD-CISCO-MEMORY-MIB.

La commande **show memory** affiche la mémoire allouée :

```
Router# show memory
```

	Head	Total(b)	Used(b)	Free(b)	Lowest(b)	Largest(b)
Processor	60DB19C0	119858752	1948928	117909824	117765180	117903232
Fast	60D919C0	131072	69560	61512	61512	61468

L'allocation mémoire peut être découverte au moyen des objets MIB du Tableau 14.24.

Tableau 14.24 : Objets MIB de la base CISCO-MEMORY-POOL-MIB pour surveiller les ressources mémoires

Objets	Description	OID
CiscoMemoryPoolName	Un nom assigné au pool de mémoire.	1.3.6.1.4.1.9.9.48.1.1.1.2
CiscoMemoryPoolUsed	Le nombre d'octets utilisés actuellement dans le pool de mémoire.	1.3.6.1.4.1.9.9.48.1.1.1.5
CiscoMemoryPoolFree	Le nombre d'octets libres du pool mémoire sur l'équipement administré.	1.3.6.1.4.1.9.9.48.1.1.1.6
CiscoMemoryPoolLargestFree	Le nombre le plus élevé d'octets contigus libres dans le pool de mémoire.	1.3.6.1.4.1.9.9.48.1.1.1.7

NOTE

Vous pouvez utiliser les objets MIB *freemem* de la base CISCO-MEMORY-MIB pour les versions de IOS antérieures à la version 11.1.

La commande **show buffers** affiche l'espace alloué en tampon :

```
Router# show buffers
Buffer elements:
 499 in free list (500 max allowed)
 124485689 hits, 0 misses, 0 created

Public buffer pools:
Small buffers, 104 bytes (total 120, permanent 120):
 112 in free list (20 min, 250 max allowed)
 35868550 hits, 0 misses, 0 trims, 0 created
 0 failures (0 no memory)
Middle buffers, 600 bytes (total 90, permanent 90):
 88 in free list (10 min, 200 max allowed)
 37894226 hits, 0 misses, 0 trims, 0 created
 0 failures (0 no memory)
Big buffers, 1524 bytes (total 90, permanent 90):
 90 in free list (5 min, 300 max allowed)
 1161634 hits, 0 misses, 0 trims, 0 created
 0 failures (0 no memory)
Large buffers, 5024 bytes (total 10, permanent 10):
 10 in free list (0 min, 30 max allowed)
 0 hits, 0 misses, 0 trims, 0 created
 0 failures (0 no memory)
Huge buffers, 18024 bytes (total 0, permanent 0):
```

```

0 in free list (0 min, 13 max allowed)
0 hits, 0 misses, 0 trims, 0 created
0 failures (0 no memory)

```

L'espace alloué dans les tampons de mémoire peut être découvert au moyen des objets MIB du Tableau 14.25.

Tableau 14.25 : Objets MIB de la base OLD-CISCO-MEMORY-MIB pour surveiller les tampons de mémoire

<i>Objets</i>	<i>Description</i>	<i>OID</i>
Eléments de tampon (<i>Buffer Elements</i>)		
bufferElFree	Nombre d'éléments de tampon libres.	1.3.6.1.4.1.9.2.1.9
bufferElMax	Nombre maximal d'éléments de tampon.	1.3.6.1.4.1.9.2.1.10
bufferElHit	Nombre d'éléments de tampon trouvés.	1.3.6.1.4.1.9.2.1.11
bufferElMiss	Nombre d'éléments de tampon non trouvés.	1.3.6.1.4.1.9.2.1.12
bufferElCreate	Nombre de créations d'éléments de tampon.	1.3.6.1.4.1.9.2.1.13
Petits tampons (<i>Small Buffers</i>)		
bufferSmSize	Taille des petits tampons.	1.3.6.1.4.1.9.2.1.14
bufferSmTotal	Nombre total de petits tampons.	1.3.6.1.4.1.9.2.1.15
bufferSmFree	Nombre de petits tampons libres.	1.3.6.1.4.1.9.2.1.16
bufferSmMax	Nombre maximal de petits tampons.	1.3.6.1.4.1.9.2.1.17
bufferSmHit	Nombre d'entrées trouvées en petits tampons.	1.3.6.1.4.1.9.2.1.18
bufferSmMiss	Nombre d'entrées non trouvées en petits tampons.	1.3.6.1.4.1.9.2.1.19
bufferSmTrim	Nombre de suppressions en petits tampons.	1.3.6.1.4.1.9.2.1.20
bufferSmCreate	Nombre de créations en petits tampons.	1.3.6.1.4.1.9.2.1.21
Tampons moyens (<i>Medium Buffers</i>)		
bufferMdSize	Taille des tampons moyens.	1.3.6.1.4.1.9.2.1.22
bufferMdTotal	Nombre total de tampons moyens.	1.3.6.1.4.1.9.2.1.23
bufferMdFree	Nombre de tampons moyens libres.	1.3.6.1.4.1.9.2.1.24
bufferMdMax	Nombre maximal de tampons moyens.	1.3.6.1.4.1.9.2.1.25
bufferMdHit	Nombre d'entrées trouvées en tampons moyens.	1.3.6.1.4.1.9.2.1.26
bufferMdMiss	Nombre d'entrées non trouvées en tampons moyens.	1.3.6.1.4.1.9.2.1.27
bufferMdTrim	Nombre de suppressions en tampons moyens.	1.3.6.1.4.1.9.2.1.28
bufferMdCreate	Nombre de créations en tampons moyens.	1.3.6.1.4.1.9.2.1.29

Tableau 14.25 : Objets MIB de la base OLD-CISCO-MEMORY-MIB pour surveiller les tampons de mémoire (suite)

Objets	Description	OID
Grands tampons (Big Buffers)		
bufferBgSize	Taille des grands tampons.	1.3.6.1.4.1.9.2.1.30
bufferBgTotal	Nombre total de grands tampons.	1.3.6.1.4.1.9.2.1.31
bufferBgFree	Nombre de grands tampons libres.	1.3.6.1.4.1.9.2.1.32
bufferBgMax	Nombre maximal de grands tampons.	1.3.6.1.4.1.9.2.1.33
bufferBgHit	Nombre d'entrées trouvées en grands tampons.	1.3.6.1.4.1.9.2.1.34
bufferBgMiss	Nombre d'entrées non trouvées en grands tampons.	1.3.6.1.4.1.9.2.1.35
bufferBgTrim	Nombre de suppressions en grands tampons.	1.3.6.1.4.1.9.2.1.36
bufferBgCreate	Nombre de créations en grands tampons.	1.3.6.1.4.1.9.2.1.37
Tampons volumineux (Large Buffers)		
bufferLgSize	Taille des tampons volumineux.	1.3.6.1.4.1.9.2.1.38
bufferLgTotal	Nombre total de tampons volumineux.	1.3.6.1.4.1.9.2.1.39
bufferLgFree	Nombre de tampons volumineux libres.	1.3.6.1.4.1.9.2.1.40
bufferLgMax	Nombre maximal de tampons volumineux.	1.3.6.1.4.1.9.2.1.41
bufferLgHit	Nombre d'entrées trouvées en tampons volumineux.	1.3.6.1.4.1.9.2.1.42
bufferLgMiss	Nombre d'entrées non trouvées en tampons volumineux.	1.3.6.1.4.1.9.2.1.43
bufferLgTrim	Nombre de suppressions en tampons volumineux.	1.3.6.1.4.1.9.2.1.44
bufferLgCreate	Nombre de créations en tampons volumineux.	1.3.6.1.4.1.9.2.1.45
Tampons énormes (Huge Buffers)		
bufferHgSize	Taille des tampons énormes.	1.3.6.1.4.1.9.2.1.62
bufferHgTotal	Nombre total de tampons énormes.	1.3.6.1.4.1.9.2.1.63
bufferHgFree	Nombre de tampons énormes libres.	1.3.6.1.4.1.9.2.1.64
bufferHgMax	Nombre maximal de tampons énormes.	1.3.6.1.4.1.9.2.1.65
bufferHgHit	Nombre d'entrées trouvées en tampons énormes.	1.3.6.1.4.1.9.2.1.66
bufferHgMiss	Nombre d'entrées non trouvées en tampons énormes.	1.3.6.1.4.1.9.2.1.67
bufferHgTrim	Nombre de suppressions en tampons énormes.	1.3.6.1.4.1.9.2.1.68
bufferHgCreate	Nombre de créations en tampons énormes.	1.3.6.1.4.1.9.2.1.69
Echecs en tampons (Buffer Failures)		
bufferFail	Nombre d'échecs d'allocation en tampon.	1.3.6.1.4.1.9.2.1.46
bufferNoMem	Nombre d'échecs de création en tampon faute de mémoire libre.	1.3.6.1.4.1.9.2.1.47

La commande **show interface** affiche les statistiques d'interface :

```
Router# show interface
Ethernet0/0 is up, line protocol is up
  Hardware is cxBus Ethernet, address is 0010.f65f.7000 (bia 0010.f65f.7000)
  Internet address is 172.16.97.1/24
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    12072853 packets input, 1379751443 bytes, 0 no buffer
    Received 1824605 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 input packets with dribble condition detected
    11283674 packets output, 1218604416 bytes, 0 underruns
    0 output errors, 24888 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

Les informations d'interfaces peuvent être obtenues au moyen des objets MIB du Tableau 14.26.

Tableau 14.26 : Objets MIB de la base OLD-CISCO-INTERFACES-MIB pour surveiller les interfaces

<i>Objets</i>	<i>Description</i>	<i>OID</i>
Statistiques des entrées		
cisco.local.lifTable.locIfInBitsSec	Moyenne variable sur cinq minutes de bits par seconde en entrée.	1.3.6.1.4.1.9.2.2.1.1.6
locIfInPktsSec	Moyenne variable sur cinq minutes de paquets par seconde en entrée.	1.3.6.1.4.1.9.2.2.1.1.7
interfaces.ifTable.ifInErrors	Nombre de paquets entrants comportant des erreurs et non transmis à un protocole de niveau supérieur.	1.3.6.1.2.1.2.2.1.14
interfaces.ifTable.ifOutError	Nombre de paquets sortants comportant des erreurs et non transmis à un protocole de niveau supérieur.	1.3.6.1.2.1.2.2.1.20
ifInNUcastPkts	Nombre de paquets non unicast transmis à un protocole de niveau supérieur.	1.3.6.1.2.1.2.2.1.12
locIfInRunts	Nombre de paquets en entrée d'une taille inférieure à celle autorisée par le média.	1.3.6.1.4.1.9.2.2.1.1.10
locIfInGiants	Nombre de paquets en entrée d'une taille supérieure à celle autorisée par le média.	1.3.6.1.4.1.9.2.2.1.1.11
locIfInCRC	Nombre de paquets en entrée ayant des erreurs de CRC.	1.3.6.1.4.1.9.2.2.1.1.12

Tableau 14.26 : Objets MIB de la base OLD-CISCO-INTERFACES-MIB pour surveiller les interfaces (suite)

Objets	Description	OID
locIfInOverrun	Compte d'entrées arrivées trop rapidement pour être reçues par le matériel.	1.3.6.1.4.1.9.2.2.1.1.14
locIfInIgnored	Nombre de paquets en entrée ignorés par cette interface.	1.3.6.1.4.1.9.2.2.1.1.15
locIfInAbort	Nombre de paquets en entrée abandonnés.	1.3.6.1.4.1.9.2.2.1.1.16
locIfInputQueueDrops	Nombre de paquets abandonnés faute de place en file d'attente d'entrée.	1.3.6.1.4.1.9.2.2.1.1.26
Statistiques des sorties		
locIfOutBitsSec	Moyenne variable sur cinq minutes de bits par seconde en sortie.	1.3.6.1.4.1.9.2.2.1.1.8
locIfOutPktsSec	Moyenne variable sur cinq minutes de paquets par seconde en sortie.	1.3.6.1.4.1.9.2.2.1.1.9
ifOutErrors	Nombre de paquets en sortie non transmis pour cause d'erreurs.	1.3.6.1.2.1.2.2.1.20
locIfCollisions	Nombre de collisions en sortie détectées sur cette interface.	1.3.6.1.4.1.9.2.2.1.1.25
locIfResets	Nombre de réinitialisations internes de l'interface.	1.3.6.1.4.1.9.2.2.1.1.17
locIfRestarts	Nombre de redémarrages complets de l'interface.	1.3.6.1.4.1.9.2.2.1.1.18
locIfCarTrans	Nombre de transitions du signal porteur de l'interface.	1.3.6.1.4.1.9.2.2.1.1.21
locIfOutputQueueDrops	Nombre de paquets abandonnés faute de place en file d'attente de sortie.	1.3.6.1.4.1.9.2.2.1.1.27

Une autre façon d'aborder les objets MIB est de les trier par types d'interfaces, comme présenté dans le Tableau 14.27.

Tableau 14.27 : Objets MIB relatifs aux interfaces

Objets	Description
Pour toutes les interfaces	cisco.local.lifTable.locIfInbitsSec cisco.local.lifTable.locIfOutbitsSec mib-2.interfaces.ifTable.ifInErrors mib-2.interfaces.ifTable.ifOutErrors cisco.local.lifTable.locIfInputQueueDrops cisco.local.lifTable.locIfOutputQueueDrops cisco.local.lifTable.locIfInIgnored cisco.local.lifTable.locIfResets cisco.local.lifTable.locIfRestarts

Tableau 14.27 : Objets MIB relatifs aux interfaces (suite)

<i>Objets</i>	<i>Description</i>
Pour les interfaces série	cisco.local.lifTable.locIfCRC cisco.local.lifTable.locIfAbort cisco.local.lifTable.locIfFrame cisco.local.lifTable.locIfCarTrans cisco.local.lifTable.locIfOverrun
Pour les interfaces Ethernet	cisco.local.lifTable.locIfCollisions cisco.local.lifTable.locIfRunts cisco.local.lifTable.locIfGiants cisco.local.lifTable.locIfFrame
Pour les interfaces Token Ring (du RFC 1231)	dot5StatsLineErrors dot5StatsBurstErrors dot5StatsACErrors dot5StatsAbortTransErrors dot5StatsInternalErrors dot5StatsFrameCopiedErrors dot5StatsTokenErrors dot5StatsSoftErrors dot5StatsSignalLoss dot5StatsFreqErrors
Pour les interfaces FDDI (du RFC 1512)	snmpFddiMACLostCts snmpFddiMACErrorCts

Les tâches finales liées à la gestion des performances sont la définition de seuils, la génération de rapports d'exceptions, l'analyse, et l'application de mesures d'optimisation.

Scénarios de corrélation d'événements de réseau

Cette section conclut le chapitre par la présentation d'un certain nombre de scénarios de corrélation d'événements de réseau.

Test d'accessibilité périodique

Nous supposerons ici que tous les équipement de réseau sont interrogés soit par l'intermédiaire de ICMP (ping) ou de SNMP (ou bien les deux) pour déterminer leur accessibilité à partir de la plate-forme NMS. Chaque fois qu'un équipement n'est pas accessible, un événement DEVICE_DOWN est généré par NMS vers le moteur de corrélation d'événements.

La plupart des NMS supportent cette fonctionnalité.

Base de données de topologie logique

Nous supposerons que la topologie logique (c'est-à-dire de niveau 3) du réseau est disponible de façon que le moteur de corrélation puisse comprendre la connectivité de sous-réseau logique et déterminer si un équipement donné est "logiquement" positionné avant ou après un autre équipement selon le point de vue de NMS.

La plupart des NMS supportent cette fonctionnalité.

Base de données de topologie physique

Certaines règles de corrélation requièrent des connaissances de la topologie physique (c'est-à-dire de niveau 2) du réseau pour comprendre la façon dont les commutateurs et les routeurs sont interconnectés sur un sous-réseau.

Très peu de NMS supportent cette fonctionnalité.

Elaboration de la base de référence

Certains scénarios de corrélation d'événements impliquent l'évaluation des différences d'état des objets gérés avant et après la survenance d'un événement. Le moteur de corrélation d'événements doit maintenir de telles variables ou y avoir accès et être en mesure de collecter le nouvel état lorsque c'est nécessaire.

Le mécanisme de gestion de seuils requiert également que les seuils soient définis à des niveaux représentatifs du réseau du client. Comme chaque réseau est différent et affiche des modèles de trafic différents, ce chapitre ne peut pas indiquer des valeurs de seuil fixes. A la place, les objets MIB et les événements les plus représentatifs pour l'approche la plus proactive possible seront traités.

Personnalisation

Le moteur de corrélation d'événements doit autoriser une certaine forme de personnalisation des règles de corrélation pour chaque client. Des règles par défaut devraient être fournies pour refléter les situations les plus courantes.

Scénarios de situations à problèmes

Pour illustrer le modèle d'événements de la Figure 14.1, les conditions décrites dans les sections suivantes ont été identifiées comme étant les plus critiques dans le cadre d'un réseau typique de commutateurs et de routeurs. Cette étude a porté essentiellement sur la famille de commutateurs Catalyst 5000 et sur le routeur Cisco 7500.

Les règles de gestion de seuils impliquant des situations simples de cause à effet (comme un commuteur qui excède une certaine valeur, provoquant de ce fait une notification de l'opérateur) ont été volontairement ignorées dans ce chapitre car elles ne requièrent aucune forme de corrélation.

Certains scénarios présentent des définitions pour une règle de *corrélation simple* et une règle de *corrélation avancée* permettant des implémentations progressives. La règle simple représente l'ensemble minimal de fonctionnalités fournies pour résoudre une situation problématique, et la règle avancée assure une résolution plus étendue.

Certains indications relatives aux intervalles d'interrogation sont fournies. Toutefois, chaque site devrait réévaluer ces intervalles en fonction de ses modèles de trafic et de la capacité de ses équipements.

Fonctions de filtrage de base

Un petit nombre de messages Syslog essentiels doivent être filtrés pour réduire le nombre de notifications des opérateurs de réseau. Ces filtres doivent pouvoir supprimer des messages identiques répétés toutes les n minutes.

Ces messages Syslog s'appliquent aux routeurs Cisco 7500 et sont présentés dans le Tableau 14.28.

Tableau 14.28 : Messages Syslog filtrés

Type de message/Description	Codage du message
Configuration Changes Report (Rapport de changements de configuration)	SYS-5-CONFIG SYS-5-CONFIG_I SYS-5-CONFIG_L SYS-5-CONFIG_M SYS-5-CONFIG_NV SYS-5-CONFIG_NV_M
CPU Hog Report (Rapport d'occupation du processeur)	Ces messages s'appliquent aux routeurs Cisco 7500 et à d'autres routeurs utilisant IOS. L'identifiant situé après le mot CONFIG spécifie l'origine du changement de configuration. Tous ces messages sont considérés comme étant identiques pour la corrélation d'événements car les opérateurs sont concernés par tous les changements de configuration, quelle que soit la manière dont ils ont été mis en œuvre. Le filtrage doit être appliqué si plusieurs messages sont envoyés en n minutes par le même équipement. Recommandation : $n = 5$ minutes
snmpAuthenticationFailure	Ce message s'applique aux routeurs Cisco 7500 et à d'autres routeurs utilisant IOS. Ces derniers génèrent un message Syslog SYS-3-CPUHOG. Ce message se répète lorsque le processeur est occupé pendant un long moment. Le filtrage doit être appliqué pour éliminer les messages dupliqués envoyés en n minutes par le même routeur. Recommandation : $n = 5$ minutes
	Cette interception est définie dans le RFC 1213, MIB. Cette interception indique une tentative d'accès à un agent SNMP avec une chaîne de communauté invalide. Si plus de trois interceptions de ce type sont reçues en 5 minutes de la part du même équipement, elles devraient être ignorées. Sinon, une notification d'avertissement devrait être envoyée à l'opérateur de réseau pour l'alerter d'une attaque possible pouvant mettre en péril la sécurité.

Conditions de redémarrage d'équipement n° 1

Plate-forme : Routeur Cisco 7500.

Objectif : Déetecter lorsqu'un équipement signale son arrêt (par opposition à son inaccessibilité qui est traitée dans le scénario "Problème de défaillance de routeur/commutateur").

Indications : Le système Cisco IOS consigne le message Syslog avant (SYS-5-RELOAD) et après (SYS-5-RESTART) le redémarrage d'un équipement.

Logique de corrélation : Lorsque le message SYS-5-RELOAD est reçu, le moteur de corrélation d'événements doit attendre de recevoir un message SYS-5-RESTART dans un intervalle de n minutes et annuler le message d'origine. S'il ne reçoit pas de message SYS-5-RESTART pendant cet intervalle, une alerte critique devrait être notifiée à l'opérateur. Si le routeur rapporte la réception de ce message dans l'intervalle spécifié, la condition est simplement consignée à titre informatif, avec la valeur de l'objet MIB *whyReload* MIB.

Si le routeur est détecté comme étant inopérant, cette information alimentera la règle de corrélation pour le problème d'activité/inactivité de routeur, de façon que le contrôle d'accessibilité de base ne le signale pas à nouveau comme étant inactif.

Cause probable : Erreur logicielle ou intervention de l'opérateur.

Actions/Résolution : Notifier l'opérateur si le routeur n'a pas émis de message SYS-5-RESTART dans un intervalle de n minutes (où n est le temps nécessaire au routeur pour se recharger + 1 minute).

Conditions de redémarrage d'équipement n° 2

Plate-forme : Commutateur Catalyst 5000.

Objectif : Déetecter lorsqu'un équipement signale qu'il est réinitialisé à partir de la console (par opposition à son inaccessibilité qui est traitée dans le scénario "Problème de défaillance de routeur/commutateur").

Indications : Le système Cisco IOS consigne le message Syslog avant que le commutateur ne soit réinitialisé (SYS-5:System reset) et une interception SNMP de démarrage à froid et/ou un message IOS (SNMP-5:Cold Start Trap) après que l'équipement ait redémarré.

Logique de corrélation : Lorsque le message SYS-5:System reset est reçu, le moteur de corrélation d'événements doit attendre de recevoir un message IOS SNMP-5:Cold Start Trap ou une interception SNMP de démarrage à froid (*cold start trap*) dans un intervalle de n minutes et annuler le message d'origine. S'il ne reçoit pas de message SNMP-5:Cold Start Trap pendant cet intervalle, une alerte critique devrait être notifiée à l'opérateur. Si le routeur rapporte la réception de ce message ou de l'interception SNMP dans l'intervalle spécifié, la condition est simplement consignée à titre informatif.

Si le commutateur est détecté comme étant inopérant, cette information alimentera la règle de corrélation pour le problème d'activité/inactivité de commutateur, de façon que le contrôle d'accessibilité de base ne le signale pas à nouveau comme étant inactif.

Cause probable : Erreur logicielle ou intervention de l'opérateur.

Actions/Résolution : Notifier l'opérateur si le commutateur n'a pas émis de message *SNMP-5: Cold Start Trap* dans un intervalle de n minutes (où n est le temps nécessaire au commutateur pour se recharger + 1 minute).

Détection de conditions de lien actif/inactif

Plate-forme : Routeur Cisco 7500 et autres routeurs dotés d'interfaces BRI.

Objectif : La détection d'un lien actif ou inactif est perçue par les clients comme étant l'exigence la plus importante. Une corrélation supplémentaire permettra la détection de transitions normales d'état actif/inactif sur des liaisons commutées mais aussi de transitions plus douteuses sur d'autres liaisons.

Une interface inactive peut représenter une situation d'alerte critique sur un routeur ou un commutateur. Les routeurs d'accès comportant des liens RNIS et ASCII voient leurs interfaces passer d'un état à l'autre plusieurs fois dans une même journée au rythme des établissements et libérations d'appels qui sont initiés dans le cadre de l'activité normale. Une règle de corrélation devrait être appliquée pour distinguer les conditions de liaisons inactives anormales de celles habituelles.

Indications : Des messages Syslog *LINK_3_UPDOWN* sont consignés.

Logique de corrélation : Deux niveaux de corrélation ont été identifiés :

- corrélation simple ;
- corrélation avancée.

Pour une corrélation simple, si la chaîne BRI est contenue dans le message, il devrait être supprimé.

Pour une corrélation avancée, si le message ne contient pas la chaîne BRI, la base de données de topologie physique devrait être interrogée pour déterminer le type du lien, c'est-à-dire s'il connecte deux routeurs, un routeur et un commutateur, ou un routeur et un port d'utilisateur.

Le message Syslog devrait être traité uniquement s'il s'agit d'un lien entre deux équipements Cisco.

Cause probable : Le lien a été déconnecté ou rompu.

Actions/Résolution : Notifier l'opérateur de réseau, sauf si l'interface est celle d'un utilisateur final, ou une interface ASCII ou BRI.

Changements de topologie STP

Plate-forme : Catalyst 5000 uniquement.

Objectif : La reconfiguration d'un arbre STP peut avoir des effets désastreux, allant jusqu'à rendre certaines portions du réseau inaccessibles. Lorsqu'une reconfiguration STP est détectée, le moteur de corrélation d'événements devrait vérifier que le réseau est encore opérationnel.

Indications : Les messages Syslog suivants sont reçus :

- SPANTREE-6: "port [dec]/[dec] state in vlan [dec] changed to blocking".
- SPANTREE-6: "port [dec]/[dec] state in vlan [dec] changed to forwarding".

Ou une des interceptions SNMP du RFC 1493 (Bridge MIB) est reçue :

- topologyChange
- newRoot

Ces interceptions contiennent la chaîne de communauté au format *communauté@ID_vlan*, où *ID_vlan* est l'identifiant du VLAN sur lequel l'arbre recouvrant STP a changé. Pour le commutateur Catalyst 5000 version 4.1 et ultérieure, ces interceptions contiendront *vtpVlanIndex* et *ifName* dans la liste *varBinds* pour fournir des informations supplémentaires à l'application traitant ces interceptions.

Logique de corrélation : Trois types de corrélation sont possibles, en fonction de la portée d'interrogation du système ECS sur le réseau :

- corrélation simple ;
- corrélation intermédiaire ;
- corrélation avancée.

La corrélation *simple* consiste à faire en sorte que chaque équipement qui signale un changement STP en utilisant les moyens décrits précédemment soit surveillé afin de s'assurer qu'il est rétabli dans état valide. Pour cela, le processus décrit ci-après est accompli, en se basant sur la MIB du Catalyst 5000.

Tout d'abord, il faut vérifier que l'objet *sysEnableBridgeTraps* de la base CISCO-STACK-MIB a été configuré pour être activé(1). Si ce n'est pas le cas, une alerte devrait être déclenchée.

Le champ de communauté dans l'interception *topologyChange* ou *newRoot* doit être lu et utilisé pour continuer à interroger le commutateur émetteur. Vous pouvez ainsi interroger le VLAN sur lequel le changement de topologie a eu lieu.

Il faut également identifier les ports qui étaient des tronçons avant le changement STP. Pour cela, une liste de tous les tronçons par VLAN doit être maintenue. Vous devez donc comparer la liste précédant le changement avec celle lui succédant. Un port de tronçon est défini comme ayant son objet MIB *vlanPortIslOperStatus* dans la table *vlanPortTable* de la base CISCO-STACK-MIB avec une valeur *trunking(1)*.

Ensuite, il faut identifier les ports de tronçons de ce VLAN qui ont connu un changement d'état en recherchant dans la table *vlanPortTable* les entrées pour lesquelles la valeur de *vlanPortVlan* a été définie avec l'identifiant de VLAN spécifié dans l'interception.

Pour chacun des ports sélectionné, identifiez l'objet MIB *vlanPortIslOperStatus* avec une valeur *trunking(1)*. Vous devez surveiller l'état de chaque tronçon comme spécifié dans le RFC 1493. Vous pouvez procéder de la manière suivante.

Consultez l'objet *vlanPortIslAdminStatus* dans la table *vlanPortTable* et assurez-vous qu'il ne soit pas défini avec la valeur *off(2)*. Sinon, générez une alerte indiquant que le port a été désactivé.

Pour chaque port de tronçon dans le VLAN sélectionné, consultez les objets *vlanPortModule* et *vlanPort* correspondants à partir de la table *vlanPortTable*. Utilisez ces deux valeurs pour lire *via index* dans la table *portTable* de la base CISCO-STACK-MIB afin d'extraire la valeur *portIfIndex* correspondante. Utilisez cette valeur pour lire l'état MIB-II *ifOperStatus* et déterminer si l'interface est toujours active. Si ce n'est pas le cas, générez une alerte.

Lisez la valeur *portCrossIndex* dans la table *the portTable* de la base CISCO-STACK-MIB pour l'entrée sélectionnée et utilisez cette valeur pour lire *via index* dans la table RFC 1493 *dot1dStpPortTable* afin de vérifier que *dot1dStpPortEnable* est défini avec la valeur *enabled(1)*.

Ensuite, utilisez la même valeur *portCrossIndex* dans la table *portTable* de la base CISCO-STACK-MIB pour localiser l'entrée correspondante dans la table RFC 1493 *dot1dStpPortTable* et vérifier que *dot1dStpPortState* est défini pour le mode *blocking(2)* ou *forwarding(5)*, 2 minutes après que l'interception ait été reçue. Autrement, envoyez une alerte.

Vérifiez également que les ports identifiés comme tronçons avant que l'interception n'ait eu lieu soient ensuite toujours opérationnels en tant que tels. Sinon, il faut générer une alerte. De la même manière, une situation dans laquelle un port qui n'était pas un tronçon avant le changement STP est identifié au cours du traitement de l'interception comme étant devenu un tronçon, devrait être rapportée.

Les alertes devraient aussi inclure un message e-mail résumant les contradictions mises en évidence lors de cette corrélation. Le fait qu'un e-mail séparé soit généré pour chaque non concordance de port ou bien que toutes les non concordances de port associées au changement STP soient regroupées dans un seul e-mail dépend de l'implémentation.

NOTE

Une alternative au traitement des interceptions consisterait à interroger l'objet MIB RFC 1493 *dot1dStpTopChanges* afin de déterminer s'il a été au minimum incrémenté de 1 ou décrémenté (indiquant une réinitialisation d'agent) depuis la dernière interrogation.

Le deuxième type de corrélation est appelé *intermédiaire*. Une reconfiguration STP est toujours limitée au sous-réseau. En supposant que le moteur de corrélation d'événements connaisse tous les équipements sur le sous-réseau avant la reconfiguration, une corrélation simple pourrait garantir qu'ils sont toujours actifs et opérationnels (en réalisant un test d'accessibilité) et qu'ils n'ont pas changé (en comparant la chaîne RFC1213-MIB *sysDescr* précédente avec celle existante pour chaque équipement). Une découverte de topologie logicielle sera également initiée pour détecter si de nouveaux équipements ont été ajoutés au réseau. Une alternative est de s'appuyer sur les commutateurs nouvellement ajoutés au réseau pour générer des interceptions, afin que le système ECS puisse les détecter.

Bien qu'imparfaite, cette règle de corrélation peut aider un opérateur de réseau à cerner l'étendue du problème plus rapidement.

Le dernier type de corrélation est appelé *avancé*. Un moyen de connaître les raisons d'une reconfiguration STP est d'obtenir la liste des équipements impliqués dans chaque arbre recouvrant sur le réseau. Une topologie STP peut être connue en interrogeant le groupe MIB *dot1stp* de la base MIB RFC 1493. CWSI version 1.2 et ultérieure peut aussi être utilisé pour afficher une représentation graphique de l'arbre STP sur la topologie physique découverte via CDP. Notez que Cisco supporte un seul arbre recouvrant par VLAN. L'identifiant de VLAN est fourni soit dans le message Syslog, soit dans la chaîne de communauté contenue dans l'interception SNMP. Si aucun VLAN n'est configuré sur le réseau, on suppose alors l'existence d'un seul VLAN avec un identifiant de VLAN

de 1. Par conséquent, le terme VLAN est utilisé dans cette section pour représenter le sous-réseau lorsqu'aucun VLAN n'est configuré.

Lorsque l'arbre recouvrant d'un VLAN est reconfiguré, le moteur de corrélation d'événements peut alors identifier le VLAN concerné et déterminer les changements qui ont eu lieu dans l'arbre.

La logique de corrélation d'événements écoute les interceptions SNMP *newRoot* ou *topology-Change* du RFC 1493 (Bridge MIB) afin de détecter le moment où la reconfiguration STP se produit. Ces interceptions sont toujours envoyées par un équipement dont le port a changé d'état, comme défini dans le RFC.

Si une interception *topologyChange* est reçue, le moteur de corrélation d'événements peut facilement compiler la liste des équipements impliqués dans la reconfiguration STP.

Si le système ECS ne parvient pas à extraire la chaîne de communauté de l'interception et ne traite pas les messages Syslog, la règle de corrélation d'événement doit associer l'interception à un VLAN en détectant celui dont le compteur de changements de topologie a été incrémenté de 1. Pour cela, le groupe *vlanTable* CISCO-STACK-MIB peut être interrogé pour établir une liste des VLAN configurés sur le commutateur. En utilisant la chaîne de communauté SNMP pour adresser des VLAN individuels (avec *communauté@ID_vlan*), le système NMS pourrait aussi interroger l'objet MIB RFC 1493 *dot1dStpTopChanges*, qui indique le nombre de changements de topologie depuis le redémarrage ou la réinitialisation de l'équipement. Cette méthode peut vous permettre d'isoler le VLAN concerné par le changement de façon que les vérifications suivantes portent uniquement sur lui.

Etant donné que la reconfiguration STP est automatique, la logique de corrélation d'événements doit déterminer les éléments suivants :

- la cause du changement de topologie ;
- l'exactitude de la nouvelle topologie STP.

Le moteur de corrélation d'événements doit déterminer si un nœud a été détecté comme inopérant avant que le changement de topologie STP n'ait été découvert. La règle de corrélation d'événements calculera la différence entre la topologie STP précédent la reconfiguration et la nouvelle, avec pour objectifs :

- Si une nouvelle racine a été définie, déterminer si l'équipement racine précédent est inactif, et si la nouvelle racine est un nouvel équipement ajouté au réseau.
- Si un seul changement topologique a eu lieu, déterminer si un autre nœud a été ajouté dans l'arbre STP (par exemple, redémarré) ou supprimé (par exemple, est en cours de redémarrage ou complètement inaccessible) en redécouvrant tous les équipements impliqués dans le VLAN.
- Si aucun équipement n'a été ajouté ou supprimé, cela signifie qu'un lien redondant a été supprimé (par exemple, un câble a été débranché) ou ajouté.

Dans n'importe laquelle de ces situations, le moteur de corrélation d'événements doit identifier les ports participants à un arbre recouvrant qui sont passés d'un état de transmission à un état bloquant, ou bien d'un état d'apprentissage à un état de transmission. Il doit également contrôler si l'objet MIB RFC1213-MIB *operStatus* de l'un de ces ports n'est pas passé d'un état activé (*up*) à un état désactivé (*down*), lors d'une tentative visant à identifier une défaillance ou une déconnexion de port.

L'opérateur sera ensuite informé de l'équipement et du port qui ont provoqué le changement. Il se peut que la règle de corrélation d'événements identifie plusieurs causes de défaillance possibles ou équipements responsables, auquel cas il faudrait en informer l'opérateur.

La notion d'exactitude peut être très complexe, selon les caractéristiques du réseau.

La méthode la plus simple permettant de déterminer l'exactitude d'une configuration STP est de s'assurer que tous les équipements de l'arbre recouvrant du VLAN sont joignables. Par conséquent, la règle de corrélation déclenchera un test d'accessibilité vers tous les équipements connus comme ayant été membres de l'arbre recouvrant avant la reconfiguration. Elle initiera également une découverte du nouvel arbre STP afin de détecter si de nouveaux équipements ont été ajoutés.

Le moteur de corrélation d'événements de l'équipement (ou des équipements) impliqué dans la reconfiguration STP informera l'opérateur de réseau et spécifiera la cause la plus vraisemblable, à savoir :

- Un équipement a été ajouté ou supprimé sur le sous-réseau.
- Un lien a été ajouté ou supprimé entre deux équipements.

Le plus difficile est de déterminer les interfaces qui ont été activées ou désactivées, et qui ont donc pu provoquer la reconfiguration, sans indiquer celles qui étaient connues comme étant inactives *avant* le changement de topologie STP. Cette règle de corrélation peut être appliquée par l'intermédiaire des mêmes mécanismes que ceux décrits précédemment. La découverte STP doit inclure les ports participant à un arbre STP avec leurs objets *operStatus* et *adminStatus* tels qu'il sont définis dans la table *ifTable* de la MIB RFC1213, et comparer les valeurs des ces objets MIB avant et après la reconfiguration STP. Une autre méthode permettant de savoir si la reconfiguration a été provoquée par une interface inactive est de la mettre en corrélation avec une interception SNMP *linkDown* ou un message Syslog reçu quelques secondes après une interception SNMP *topology-Change* ou *newRoot* ou un message Syslog de changement de topologie sur un VLAN.

Une alternative serait de surveiller l'objet MIB *dot1dStpPortForwardTransitions* afin de détecter à quel moment il est incrémenté de 1.

Cause probable : Un équipement impliqué dans l'arbre recouvrant a été éteint, est tombé en panne, ou a été ajouté au réseau. Ou bien un lien a été ajouté ou supprimé entre deux équipements.

Actions/Résolution : Notifier l'opérateur comme mentionné précédemment. Aucune action automatique n'est prévue.

Problème de défaillance de routeur/commutateur

Plate-forme : Catalyst 5000 et routeur Cisco 7500.

Objectif : Déetecter la défaillance d'un commutateur ou d'un routeur, sans indiquer les équipements inaccessibles derrière lui.

En se basant sur la connaissance de la structure topologique, un moteur de corrélation doit identifier la défaillance la plus vraisemblable dans un groupe de noeuds inaccessibles. En supposant que Cisco gère uniquement les équipements Cisco, l'état des équipements d'utilisateurs finaux, tels que des PC et des serveurs, ne sera pas surveillé.

Indications : Plusieurs équipements ne sont pas accessibles au même moment.

Logique de corrélation : Une base de données de topologie logique (couche 3) peut servir à détecter un routeur défaillant dans un groupe de routeurs inaccessibles. Toutefois, une base de données de topologie logique (couche 2) est nécessaire pour détecter un commutateur défaillant dans un groupe de commutateurs injoignables.

Pour chaque équipement signalé comme inaccessible au bout de n minutes, une interrogation de son objet RFC1213-MIB *sysObjectID* sera initiée et utilisera la table de correspondances de Cisco.

Ensuite, le moteur de corrélation d'événements exécutera une corrélation simple ou avancée. La recommandation est $n = 5$ minutes.

La corrélation simple implique l'utilisation de la base de données de topologie NMS existante.

Cette méthode convient tout à fait pour identifier un routeur défaillant parmi d'autres routeurs, mais ne permet pas d'effectuer cette différenciation pour les commutateurs (car la plupart des NMS ne supportent pas la topologie de niveau 2).

La corrélation avancée autorise l'identification d'un commutateur défaillant à partir d'un groupe de commutateurs sur un sous-réseau en utilisant la base de données de connectivité physique qui décrit la façon dont les commutateurs sont interconnectés. Le système ECS devrait commencer par utiliser la topologie de niveau 3 pour repérer le sous-réseau concerné, puis une base de données de topologie de niveau 2 afin d'identifier le commutateur faisant l'objet de la défaillance.

NOTE

Il est préférable de connecter la station NMS directement à un réseau commuté car le système NMS n'est pas capable d'isoler un commutateur pouvant se trouver "derrière" d'autres commutateurs, à moins que le moteur de corrélation d'événements ne détermine sur quel commutateur la station NMS est connectée. Cette solution peut être mise en œuvre en interrogeant les tables MAC sur chaque commutateur et en associant les adresses MAC à la station NMS. Ce processus peut être très long car il se peut que des milliers d'adresses doivent être collectées.

Cause probable : Un routeur ou un commutateur est défaillant.

Actions/Résolution : Notifier l'opérateur de réseau au moyen d'une seule notification identifiant l'équipement responsable.

Problème de performances d'équipement

Plate-forme : Routeur Cisco 7500.

Objectif : Déetecter à quel moment un trafic excessif impose une charge trop importante sur le processeur.

Les responsables de réseaux n'ont qu'une compréhension limitée de la circulation du trafic entre leurs commutateurs et routeurs Cisco. Il est essentiel de pouvoir déterminer les conditions de trafic intensif sur un réseau. Les conditions de surcharge du processeur signalées par des messages Syslog SYS-3-CPUHOG seront surveillées et une alerte sera générée si des conditions excessives sont rencontrées — c'est-à-dire des conditions ne concernant pas le trafic temporaire, comme signalé par NetFlow, et pouvant représenter une situation de surcharge temporaire.

Indications : Le message Syslog SYS-3-CPUHOG est consigné, indiquant une condition de surcharge du processeur.

Logique de corrélation : Deux niveaux de corrélation ont été identifiés.

Le premier type de corrélation est simple. Le moteur de corrélation d'événements déclenchera un processus de collecte de statistiques de trafic toutes les 20 secondes pendant n minutes pour les objets *ifInOctets* et *ifOutOctets* de la table RFC1213 MIB *ifTable*. Si le trafic sur une interface dépasse 40 % de la capacité du lien (*ifSpeed*) pendant plus de 50 % du temps de collecte, l'opérateur en sera informé avec une référence vers l'interface (ou les interfaces) subissant une charge de trafic excessive.

Si l'interface concernée est la même que celle utilisée pour effectuer le ping et le test d'accessibilité SNMP, la condition résultera probablement en une inaccessibilité temporaire de l'équipement, le signalant comme inopérant. La condition de faibles performances de l'équipement alimentera la règle de corrélation d'accessibilité de façon que l'opérateur ne soit pas informé à deux reprises d'un même problème, ou que d'autres équipements ne soient pas considérés comme inopérants/inaccessibles en raison de la surcharge de cette interface (voir la section "Problème de défaillance de routeur/commutateur").

La condition de faibles performances sera considérée comme étant une alarme mineure pendant n minutes et ne sera pas signalée à l'opérateur de réseau si à l'issue de cet intervalle elle n'est plus vraie. La recommandation est $n = 15$ minutes.

S'il n'existe aucune condition de performances, le manque d'accessibilité sera jugé comme étant une alarme critique car l'équipement est probablement complètement immobilisé.

Le second type de corrélation est avancé. NetFlow peut être utilisé pour réaliser une corrélation plus approfondie et pour éviter de rapporter les surcharges temporaires en vérifiant quels protocoles sont responsables de cet impact au niveau des performances. Le processus se déroule comme suit.

La commande IOS **show ip cache flow** affichera une table des adresses IP indiquant sur quels ports et interfaces elles sont configurées. Les intitulés des colonnes de la table sont *SrcIPaddress*, *DstIPaddress*, *SrcP*, *DstP*, *SrcIf*, et *DstIf*. A partir des informations qu'elle fournit, vous pouvez déterminer si la charge du processeur est causée par un trafic excessif sur une interface donnée, et si le trafic est passager (FTP sur le port 21, par exemple). S'il est identifié comme temporaire, le moteur de corrélation d'événements ignorera le message Syslog CPUHOP pendant 5 minutes pour cette session spécifique. Si ce message est répété dans le cadre de la même session NetFlow au-delà d'une période de 30 minutes, l'opérateur recevra un avertissement lui indiquant qu'une session NetFlow inhabituelle est en cours. La commande IOS **export ip flow** peut également être utilisée.

Si le message Syslog CPUHOP se produit de façon répétée pour différentes sessions (par exemple, 10 fois par heure), l'opérateur sera averti que l'équipement est continuellement soumis à une surcharge et devrait être examiné de plus près.

Cause probable : Le problème peut provenir d'une session temporaire (telle que FTP) ou d'un routeur dont la puissance est insuffisante pour pouvoir gérer le trafic qu'il reçoit.

Actions/Résolution : Notifier l'opérateur si le problème de performances persiste, comme décrit plus haut.

Problème environnemental n° 1

Plate-forme : Catalyst 5000 avec module superviseur redondant.

Objectif : Détecter des hausses de températures pouvant conduire à une panne du commutateur.

Indications : Le commutateur Catalyst 5000 doté d'un module superviseur redondant émet un message Syslog SYS-0: "Temp high Failure" ou une interception SNMP CISCO-STACK MIB *chassisAlarmOn* avec la liste *varBind* contenant *chassisTempAlarm* = on(2), *chassisMinorAlarm* = on(2) ou off(1), et *chassisMajorAlarm* = on(2), chaque fois que la température dépasse 50° Celsius.

Logique de corrélation : Au bout de 5 minutes, s'il y a réception d'un autre message Syslog SYS-0: "Temp Critical Recovered" ou SYS-2: "Temp high Okay", ou de l'interception SNMP CISCO-STACK MIB *chassisAlarmOff*, l'alerte devrait être effacée du moteur de corrélation d'événements.

Si aucun de ces messages ou interception SNMP n'est reçu, l'alerte devrait alimenter la règle d'activité/inactivité de commutateur indiquant qu'il est inopérant.

Cause probable : Le système d'air conditionné dans la pièce ou le ventilateur est tombé en panne.

Actions/Résolution : Le problème devrait être immédiatement signalé à l'opérateur sous forme d'une notification de pager. S'il se résout de lui-même, l'opérateur devrait à nouveau en être averti.

Problème environnemental n°2

Plate-forme : Routeur Cisco 7000.

Objectif : Détecter des hausses de températures pouvant conduire à une panne du routeur.

Indications : Un des messages Syslog suivants est reçu :

- ENV-2-TEMP
- ENV-1-SHUTDOWN
- ENVM-2-TEMP
- ENVM-1-SHUTDOWN

Les messages -TEMP généreront une alarme majeure, et les messages SHUTDOWN une alarme critique.

Une plus grande granularité peut être mise en œuvre si le système ECS peut décoder la température indiquée dans le message Syslog et appliquer ses propres seuils et niveaux d'alarme.

L'alarme devra éventuellement être effacée manuellement par l'opérateur.

Cause probable : Le système d'air conditionné dans la pièce ou le ventilateur est tombé en panne.

Actions/Résolution : Notifier l'opérateur.

Résumé

L'objectif de ce chapitre est de servir de référence sur les composants de routeurs et commutateurs Cisco pouvant être gérés par des clients Cisco. Il vous a appris à identifier et à gérer les éléments essentiels d'un commutateur Catalyst, et a mis en évidence les différences de gestion qui existent entre un commutateur et un routeur.

Les aspects suivants ont été abordés :

- introduction à la gestion de réseau ;
- théorie et implémentation du pontage sur des commutateurs et des routeurs Cisco et technologies communes à ces deux types d'équipements ;
- introduction aux protocoles de gestion de réseau et au modèle d'événements de Cisco, et description des événements Cisco : messages Syslog et interceptions SNMP ;
- composants essentiels d'une stratégie de gestion de réseau réussie ;
- éléments de commutateurs nécessitant une gestion, et techniques de gestion de ressources appropriées ;
- scénarios de surveillance et de corrélation avancés incluant un ou plusieurs équipements ;
- détails des messages Syslog et fonctions de reporting ;
- exemples de définition de seuils RMON.

15

Architecture de commutation de paquets

Par Russ White

Ce chapitre figurera dans l'ouvrage *Inside Cisco IOS*, à paraître chez Cisco Press (en langue anglaise).

L'objectif principal d'un routeur multiprotocole est bien sûr de commuter les paquets d'un segment de réseau vers un autre. Si le planificateur (*scheduler*) et le gestionnaire de mémoire constituent l'infrastructure logicielle du routeur, l'architecture de commutation du système IOS représente ses fondements. Les méthodes et structures de commutation mises en œuvre par ce système déterminent essentiellement la façon dont le routeur assure sa fonction principale. Aussi, des efforts considérables ont été déployés pour concevoir et optimiser cet aspect primordial du système IOS.

Néanmoins, le processus de commutation de paquets demeure assez simple. Lorsqu'un paquet est reçu, son adresse de destination est examinée et comparée avec les entrées d'une liste de destinations connues. Si une correspondance est trouvée, le paquet est transmis vers l'interface appropriée, sinon il est supprimé. Par conséquent, le problème n'est pas de savoir *comment* commuter les paquets, mais plutôt comment les commuter *rapidement*. La commutation de paquets est une opération consommatrice de données, par opposition aux opérations consommatrices de calculs. Aussi, pour accélérer son exécution, il ne suffit pas d'utiliser un processeur plus rapide. D'autres facteurs, tels que les performances de bus en E/S et la vitesse de la mémoire de données, peuvent avoir un impact considérable sur le fonctionnement de ce processus. Pour les développeurs du système IOS,

le défi consistait à obtenir les meilleures performances de commutation possibles en fonction des limites des ressources disponibles (CPU, bus E/S et mémoire).

Au fur et à mesure que la taille et le nombre des réseaux routés augmentaient, les développeurs IOS ont dû travailler sans relâche à la résolution de ce problème de performances. Il en a résulté une révision et un perfectionnement continuels des méthodes de commutation du système IOS. Lorsque ce système a été initialement développé, il n'existait qu'une seule méthode de commutation, appelée aujourd'hui *commutation par processus*. Les versions suivantes ont introduit de nouvelles méthodes de commutation, certaines s'appuyant sur des optimisations matérielles spécifiques, d'autres exploitant des techniques logicielles et supportant de nombreuses plates-formes. Aujourd'hui, le système IOS fournit des méthodes de commutation qui permettent de commuter plusieurs centaines de milliers de paquets par seconde, au moyen de tables de routage qui contiennent des centaines de milliers de routes, et qui peuvent être implémentées au niveau de l'épine dorsale de l'Internet.

La liste suivante résume les méthodes de commutation développées depuis la version 12.0 du système Cisco IOS :

- commutation par processus ;
- commutation rapide ;
- commutation autonome ;
- commutation SSE (*Silicon Switching Engine*, moteur de commutation en silicium) ;
- commutation optimale ;
- commutation rapide distribuée ;
- transmission expresse Cisco (CEF, *Cisco Express Forwarding*) ;
- transmission expresse Cisco distribuée (dCEF, *Distributed Cisco Express Forwarding*).

Quatre de ces méthodes (commutation par processus, commutation rapide, commutation optimale et transmission CEF) sont traitées en détail dans ce chapitre.

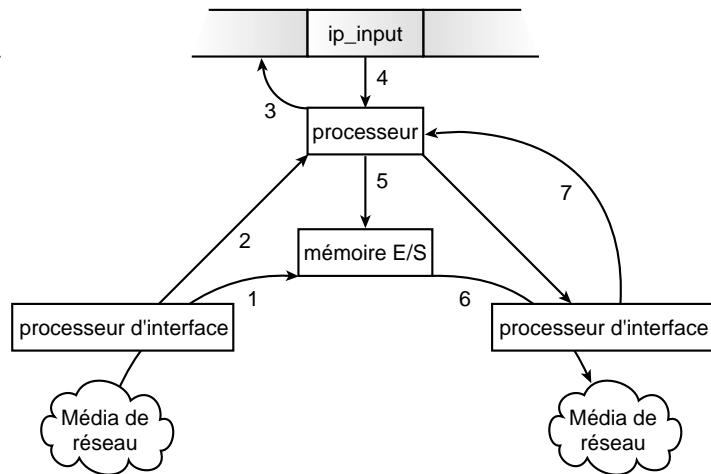
Bien que ce chapitre utilise des exemples de routage IP pour illustrer les différentes méthodes de commutation, bon nombre d'entre elles fonctionnent également avec d'autres protocoles de réseau, tel IPX, ainsi qu'avec la technique de pontage. Même si les structures employées sont souvent indépendantes pour chaque protocole — par exemple, IP et IPX exploitent un cache rapide (*Fast Cache*) différent —, leur contenu est semblable, et les méthodes fonctionnent pratiquement de la même manière pour tous les protocoles.

Commutation par processus

La commutation par processus a été la première méthode de commutation implémentée dans le système IOS. Elle présente très peu d'optimisations. Elle applique une technique de commutation de paquets "en force", qui peut consommer énormément de temps processeur. Cependant, elle possède l'avantage d'être indépendante de la plate-forme, ce qui la rend universellement disponible pour tous les produits fondés sur le système Cisco IOS. A l'inverse de la plupart des autres méthodes de commutation, elle fournit également certaines fonctions d'équilibrage de charge, qui seront traitées en détail plus loin dans ce chapitre.

Pour comprendre le fonctionnement de la commutation par processus, nous allons examiner les étapes nécessaires afin de commuter un paquet au moyen de cette méthode. La Figure 15.1 illustre le chemin commuté par processus d'un paquet IP.

Figure 15.1
Le chemin commuté par processus.



Tout d'abord, l'interface de réseau du routeur détecte sur le câble un paquet à traiter. Elle reçoit donc ce paquet, puis le transfère en mémoire d'entrée/sortie (étape 1 de la Figure 15.1).

L'interface de réseau interrompt le processeur central, pour lui signaler qu'un paquet a été placé en mémoire d'entrée/sortie, en attente de traitement. Le programme d'interruption du système IOS examine les informations contenues dans l'en-tête du paquet (type d'encapsulation, en-tête de couche réseau, etc.), détermine qu'il s'agit d'un paquet IP, puis le place dans la file d'entrée du processus de commutation approprié (étape 2 de la Figure 15.1). Pour les paquets IP, le processus de commutation est appelé **ip_input**.

La présence d'un seul paquet dans la file d'entrée du processus **ip_input** suffit pour que ce dernier soit autorisé à s'exécuter (étape 3 de la Figure 15.1).

Lorsque l'exécution du processus **ip_input** (étape 4 de la Figure 15.1) est engagée, l'opération de transmission du paquet peut commencer. Toutes les décisions relatives à la direction dans laquelle il sera envoyé sont prises à cette étape. Dans cet exemple, le processus **ip_input** consulte la table de routage, afin de déterminer s'il existe une route vers l'adresse IP de destination. Si c'est le cas, il extrait l'adresse de prochain saut (c'est-à-dire le prochain routeur sur le chemin ou la destination finale) dans l'entrée de la table de routage, et consulte ensuite le cache ARP, afin d'obtenir les informations nécessaires à la création d'un nouvel en-tête MAC (*Media Access Control*, contrôle de l'accès au média) pour le prochain saut. Le processus crée ensuite l'en-tête MAC, qui remplace les données de l'en-tête existant dans le paquet reçu. Enfin, le paquet est placé dans la file d'attente de l'interface de réseau en sortie pour être transmis (étape 5 de la Figure 15.1).

Lorsque l'interface de réseau en sortie détecte la présence d'un paquet en attente d'être envoyé, elle le retire de la mémoire d'entrée/sortie, puis le transmet sur le réseau (étape 6 de la Figure 15.1). Une fois que l'interface a terminé l'envoi du paquet, elle interrompt le processeur central, afin de le lui signaler. Le système IOS met ensuite à jour ses compteurs de paquets envoyés, puis libère l'espace occupé précédemment par le paquet en mémoire d'entrée/sortie (étape 7 de la Figure 15.1).

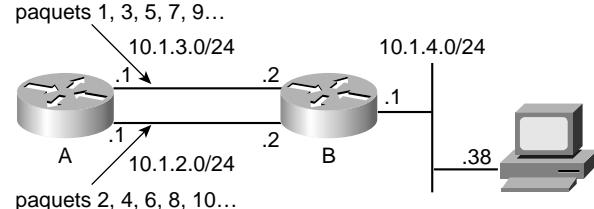
Equilibrage de charge avec la commutation par processus

L'un des avantages de la commutation par processus est qu'elle supporte l'équilibrage de charge par paquets, ce qui représente un moyen relativement simple d'optimiser l'utilisation du média lorsqu'il existe plusieurs routes (chemins) vers une destination. Dans ce cas, les paquets commutés par processus sont automatiquement distribués sur les chemins disponibles, en fonction de la métrique de routage (ou coût) assignée à chaque chemin.

Le coût de chaque chemin dans la table de routage est utilisé afin de calculer un compte de *parts de trafic* (*traffic share count*), qui permet de déterminer le chemin à emprunter. Pour mieux comprendre comment fonctionne cette répartition, examinons la Figure 15.2.

Figure 15.2

Equilibrage de charge sur plusieurs chemins de même coût.



Dans cet exemple, le routeur A dispose de deux chemins de même coût vers le réseau 10.1.4.0/24. Sa table de routage devrait donc ressembler à ce qui suit :

```
RouterA#show ip route 10.1.4.0 255.255.255.0
Routing entry for 10.1.4.0/24
Known via "static", distance 1, metric 0
Routing Descriptor Blocks:
  10.1.2.1
    Route metric is 0, traffic share count is 1
  * 10.1.3.1
    Route metric is 0, traffic share count is 1
```

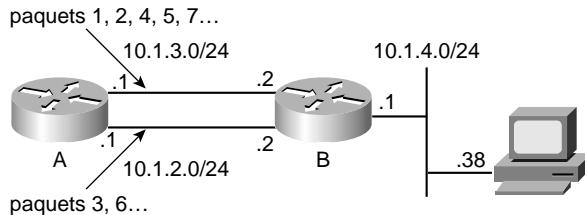
L'astérisque (*) en regard de l'un des chemins signifie que le chemin en question sera utilisé afin de transmettre le prochain paquet commuté vers le réseau 10.1.4.0/24. Le compte de parts de trafic est égal à 1 pour les deux chemins, ce qui signifie qu'ils seront exploités à tour de rôle pour envoyer les paquets.

Dans cet exemple, le prochain paquet reçu pour ce réseau sera routé vers le prochain saut, 10.1.3.0/24, le deuxième paquet sera envoyé vers le prochain saut, 10.1.2.0/24, le troisième vers 10.1.3.0/24, et ainsi de suite (voir la numérotation des paquets à la Figure 15.2).

Certains protocoles de routage pour IP, en particulier IGRP (*Interior Gateway Routing Protocol*) et EIGRP (*Enhanced IGRP*), peuvent inclure des chemins de coûts inégaux dans leur table de routage.

Dans ce cas, l'algorithme de partage du trafic fonctionne un peu différemment. Si un des liens de l'exemple précédent changeait de telle sorte que la quantité de bande passante doublait sur un des deux chemins, la répartition de charge serait modifiée (voir Figure 15.3).

Figure 15.3
Equilibrage de charge sur des chemins de coûts différents.



La table de routage du routeur A ressemblerait à ce qui suit :

```

RouterA#show ip route 10.1.4.0 255.255.255.0
Routing entry for 10.1.4.0/24
Known via "EIGRP", distance 90, metric 284600
Routing Descriptor Blocks:
  10.1.2.1
    Route metric is 569200, traffic share count is 1
  * 10.1.3.1
    Route metric is 284600, traffic share count is 2
  
```

Examinez les comptes de parts de trafic dans cette sortie de la commande `show ip route`. Le chemin de coût le plus faible qui passe par 10.1.3.1 possède un compte de 1 ; celui de coût le plus élevé qui passe par 10.1.2.1 présente un compte de 2. A présent, pour chaque paquet commuté sur le chemin de coût le plus élevé, deux paquets seront commutés sur celui de coût le plus faible, tel que signifié par la numérotation des paquets à la Figure 15.3.

NOTE

Bien que le partage de charge par paquet soit très efficace pour équilibrer la charge sur plusieurs liaisons, il présente un inconvénient de taille, à savoir que les paquets peuvent arriver dans le désordre sur leur destination. Le traitement des paquets désordonnés peut considérablement dégrader les performances des stations finales. Ce risque est d'autant plus important dans le cas d'une grande variation de latence entre les routes disponibles.

Inconvénients de la commutation par processus

Comme mentionné précédemment, un inconvénient majeur de la commutation par processus est sa lenteur. Cette méthode effectue une recherche dans la table de routage pour chaque paquet traité. Au fur et à mesure que la taille de la table augmente, le temps nécessaire pour exécuter une recherche croît également (de même que le temps de commutation total). Des temps de recherche plus longs intensifient l'utilisation du processeur, effet qui est multiplié par le taux de paquets entrants. Bien que cet effet puisse demeurer imperceptible sur des réseaux de très petite taille, qui comprennent seulement quelques routes, en ce qui concerne les réseaux plus étendus qui disposent de centaines ou de milliers de routes, la taille de la table de routage peut avoir un impact significatif sur l'utilisation

du processeur, ainsi que sur la latence de routage (c'est-à-dire le délai écoulé entre l'arrivée d'un paquet sur le routeur et son départ).

Un autre facteur important qui affecte les performances de la commutation par processus est le temps de transfert des données en mémoire. Sur certaines plates-formes, les paquets reçus doivent être copiés depuis la mémoire d'entrée/sortie vers une autre mémoire, avant de pouvoir être commutés. Une fois le processus de routage terminé, ils doivent être recopier en mémoire d'entrée/sortie, en vue de leur transmission. Ces opérations de copie de données en mémoire sont coûteuses en ressources processeur, et peuvent par conséquent affecter les performances de cette méthode de commutation sur les plates-formes concernées.

Pour que le système IOS prenne sa place dans le monde des réseaux routés en constante évolution, une méthode de commutation globalement plus efficace était nécessaire. Les premiers développeurs IOS l'ont rapidement mise en œuvre. Pour mieux comprendre la solution proposée, examinons les aspects de la commutation par processus qui doivent faire l'objet d'une optimisation.

Pour reprendre l'exemple précédent de commutation par processus IP, le processus **ip_input** requiert trois éléments d'information essentiels pour commuter un paquet :

- **Accessibilité.** Cette destination est-elle accessible ? Si oui, quelle est l'adresse de réseau IP du prochain saut vers la destination ? Cette information se trouve dans la table de routage, également appelée *table de transmission*.
- **Interface.** Sur quelle interface ce paquet devrait-il être transmis afin d'atteindre cette destination ? Cette information est contenue dans la table de routage.
- **En-tête de couche MAC.** Quel en-tête MAC doit être placé dans ce paquet pour adresser correctement le prochain saut ? Les données d'en-tête MAC proviennent de la table ARP pour IP, ou d'autres tables de correspondances, telle la table Frame Relay.

Etant donné que chaque paquet entrant peut être différent, le processus **ip_input** doit examiner ces éléments d'information essentiels chaque fois qu'il commute un paquet. Il doit rechercher dans une table de routage parfois très volumineuse les données d'accessibilité et d'interface, puis examiner une autre table, qui peut elle aussi être très volumineuse, afin d'y trouver les données d'en-tête MAC. Une amélioration conséquente serait de permettre au processus **ip_input** de "mémoriser" le résultat des recherches qu'il effectue pour certaines destinations. Par exemple, il pourrait maintenir une table plus réduite de combinaisons accessibilité/interface/MAC pour les destinations les plus fréquentes, ce qui réduirait considérablement le temps de recherche pour la plupart des paquets entrants. De plus, étant donné que la recherche est la tâche la plus intensive, une table plus petite accélérerait suffisamment son exécution, de façon que l'opération de commutation complète puisse être réalisée par le programme d'interruption qui reçoit le paquet (éliminant ainsi le besoin de copier les données en mémoire, d'où une économie supplémentaire de temps). Par conséquent, pour permettre au système IOS de maintenir une table de recherche réduite, et obtenir ainsi une amélioration des performances, la solution proposée a été l'utilisation d'un cache rapide (*Fast Cache*).

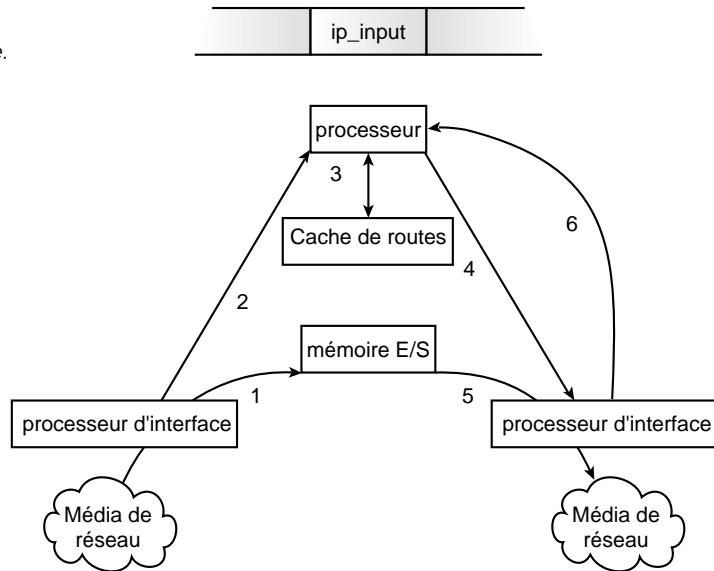
Mise en cache avec la commutation rapide

En informatique, le terme *cache* désigne en général une zone de stockage locale d'accès très rapide, qui sert à stocker certains sous-ensembles de données fréquemment utilisés. Par exemple, un ordinateur pourrait conserver en mémoire RAM une copie locale de certaines portions d'un fichier enregistré sur disque dur, qui fait l'objet d'accès fréquents. Ou bien, un processeur pourrait placer dans une zone de mémoire associative très rapide des instructions préalablement extraites, afin d'accroître les performances. Les deux caractéristiques essentielles d'un tel cache sont une taille relativement réduite — comparée à l'espace total de données —, et un accès très rapide à n'importe quel membre adressable de son contenu.

Les développeurs du système IOS se sont appuyés sur ces concepts pour créer le cache rapide. Ce dernier est simplement une structure de données dans le système IOS, utilisée pour conserver une copie des combinaisons accessibilité/interface/MAC obtenues lors de la commutation par processus des paquets.

Pour illustrer l'utilité du cache rapide, nous allons reprendre notre exemple de commutation par processus, et lui ajouter une étape supplémentaire (voir Figure 15.4). Après que le processus **ip_input** a extrait les informations de prochain saut, d'interface de sortie et d'en-tête MAC, il les enregistre dans une structure de données spéciale, le cache rapide, qui autorise un accès très rapide à n'importe lequel de ses membres, en fonction de l'adresse IP de destination. Au fil du temps, le processus **ip_input** consignera dans ce cache un grand nombre des destinations IP fréquemment utilisées.

Figure 15.4
Le chemin de commutation rapide.



Examinons de nouveau la méthode de commutation par processus, avec cette fois l'introduction du cache rapide. L'interface physique commence donc par détecter la présence d'un paquet sur le média. Elle le reçoit, puis le transfère en mémoire d'entrée/sortie (étape 1 de la Figure 15.4).

A l'étape 2, l'interface physique interrompt le processeur central afin de lui signaler qu'un paquet reçu se trouve en mémoire d'entrée/sortie, en attente de traitement. Le programme d'interruption du système IOS examine les informations d'en-tête du paquet, et détermine qu'il s'agit d'un paquet IP. A présent, au lieu de placer le paquet dans la file d'entrée du processus **ip_input**, comme précédemment, le programme d'interruption consulte directement le cache rapide, afin de vérifier si des informations d'interface sortante et d'en-tête MAC relatives à cette destination y ont été consignées. S'il trouve dans le cache une entrée correspondante, il lit les informations d'en-tête MAC qu'elle contient, puis les écrit dans le paquet. Cette entrée lui indique également un pointeur vers l'interface de sortie appropriée. L'étape 3 de la Figure 15.4 représente la lecture en cache et l'opération d'écriture des données MAC.

Le processeur central (toujours dans le cadre de la même interruption) signale à l'interface physique de sortie qu'un paquet placé en mémoire d'entrée/sortie est prêt à être envoyé. Il met fin à l'interruption, afin de permettre à d'autres processus de poursuivre leur exécution (étape 4 de la Figure 15.4).

A l'étape 5, l'interface retire le paquet de la mémoire d'entrée/sortie, puis le transmet. Elle interrompt ensuite le processeur central pour mettre à jour ses compteurs, et libérer l'espace mémoire occupé précédemment par le paquet (étape 6 de la Figure 15.4).

L'exemple décrit ici illustre le fonctionnement de la commutation rapide. Notez que le processus **ip_input** n'est jamais impliqué dans la commutation d'un paquet. En fait, aucun processus planifié n'est impliqué dans la commutation rapide d'un paquet, dès lors qu'il existe en cache une entrée correspondante. Grâce à cette fonctionnalité de cache rapide, le système IOS peut maintenant exécuter une opération complète de commutation de paquets dans le laps de temps très court d'une interruption. La mise en cache a permis au système IOS de séparer la tâche consommatrice en ressources — qui consiste à prendre une décision de routage — de la tâche moins coûteuse qui consiste à transmettre un paquet. La commutation rapide a donc introduit le concept "router une fois, transmettre plusieurs fois".

Une remarque importante doit être faite ici. Comme vous avez pu le constater, les entrées du cache rapide sont générées au fur et à mesure que les paquets sont commutés par processus. Par conséquent, étant donné que c'est l'opération de commutation par processus qui crée les entrées en cache, le premier paquet envoyé vers une destination donnée est toujours commuté par processus, même lorsque la commutation rapide est activée. Une fois l'entrée enregistrée dans le cache, les paquets ultérieurs vers cette même destination peuvent être traités par commutation rapide.

De plus, certaines conditions sont nécessaires pour permettre un remplissage efficace du cache rapide, au moyen de la commutation par processus. Notamment, le réseau doit être globalement stable, avec peu de changements de routes, et le trafic doit plutôt circuler en direction d'un sous-ensemble particulier de destinations. Dans certains environnements de réseau, telle l'épine dorsale de l'Internet, ces conditions ne sont pas présentes. Les conditions de réseau existantes peuvent alors induire un très faible taux de correspondance des entrées en cache, ce qui entraîne un grand nombre de paquets commutés par processus. Dans d'autres cas, par exemple lorsque le cache n'est pas assez grand pour contenir toutes les entrées nécessaires, les conditions de réseau peuvent provoquer le remplacement systématique des entrées les plus anciennes par celles nouvellement créées. De tels environnements seront traités plus loin dans ce chapitre.

Structure du cache rapide

Pour comprendre le fonctionnement du cache rapide et sa capacité à fournir rapidement les informations de transmission, nous allons étudier sa structure.

Tout d'abord, pour avoir une idée précise de son contenu, examinons le résultat de la commande `show ip cache verbose` :

```
router#show ip cache verbose
IP routing cache 1 entry, 172 bytes
 124 adds, 123 invalidates, 0 refcounts
 Minimum invalidation interval 2 seconds, maximum interval 5 seconds,
   quiet interval 3 seconds, threshold 0 requests
 Invalidation rate 0 in last second, 0 in last 3 seconds

 Prefix/Length    Age      Interface    Next Hop
 10.1.1.16/32-24 1w4d    Ethernet0    10.1.1.16
                 14 00403337E5350060474FB47B0800
```

D'après ce résultat, on peut voir que le routeur conserve des informations sur le préfixe de destination, la longueur du préfixe, l'interface de sortie, l'adresse IP de prochain saut et l'en-tête MAC. Toutes les données nécessaires à la commutation d'un paquet vers une destination spécifique sont contenues dans cette entrée.

Le cache rapide possède une autre caractéristique, qui n'apparaît pas de façon évidente dans cette sortie. A l'inverse des tables principales, à partir desquelles les entrées du cache sont générées, et qui ne sont finalement rien de plus que de longues listes, le cache est implémenté au moyen d'une structure de données spéciale, qui autorise l'extraction rapide de n'importe quel membre. Avec les tables principales, le temps de recherche augmente proportionnellement à leur taille. Grâce à sa structure, le cache rapide autorise un temps de recherche minimal qui, de plus, demeure relativement constant, indépendamment du nombre total d'entrées.

Table de hachage

Le cache rapide IP a été initialement implémenté sous forme d'une structure de données, appelée *table de hachage* (voir Figure 15.5).

Figure 15.5
Structure du cache rapide.

10.1.11.0	172.16.188.0	192.168.104.0	10.89.83.0			
172.16.216.0	10.1.111.0	10.84.55.0	172.147.9.1.0	10.254.144	192.168.12.0	
10.89.54.0						
10.1.109.0	192.168.14.0	172.16.218.0	10.89.53.0			
192.168.15.0	10.89.52.0	10.1.108.0				
10.254.156.0	172.16.212.0	172.147.87.0	10.89.59.0	192.168.0.0	10.1.99.0	
10.1.244.0	172.16.67					

Dans la table de hachage, chaque préfixe IP pointe vers un emplacement particulier de la table. Une entrée particulière peut être trouvée en exécutant des opérations booléennes (avec OU exclusif sur les 16 bits de poids le plus faible et les 16 bits de poids le plus fort de l'adresse IP de 32 bits recherchée). Le résultat de ce calcul pointe vers l'emplacement de la table de hachage souhaité, appelé *compartiment de hachage (hash bucket)*. Chaque compartiment de hachage contient une entrée de cache, dont un en-tête MAC précalculé pour le prochain saut.

Une opération de hachage ne produit pas toujours un hachage unique pour chaque adresse IP. Une situation dans laquelle plusieurs adresses IP pointent vers le même compartiment de hachage est appelée *collision*. Lorsqu'une collision survient, le système IOS regroupe les entrées de cache qui font l'objet d'une collision en une liste placée dans le compartiment de hachage, avec un maximum de six entrées. De cette manière, aucune recherche portant sur plus de six entrées dans le cache n'est nécessaire pour trouver une correspondance particulière.

Dans la version 10.2 de Cisco IOS, la table de hachage a été remplacée par une structure de données, appelée arbre binaire (*radix tree*), c'est-à-dire à deux voies. Dans cette implémentation, les en-têtes MAC sont toujours stockés dans un cache.

Arbre binaire

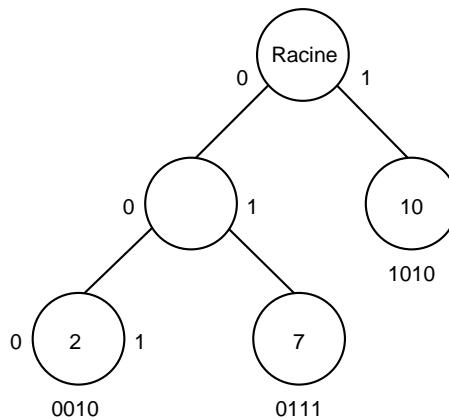
A l'instar de la table de hachage, l'arbre binaire est une structure de données spéciale, utilisée pour améliorer le temps d'extraction de données membres.

L'arbre binaire tire son nom de la façon dont les données sont stockées, c'est-à-dire en fonction de leur valeur binaire. Dans la pratique, cela signifie que les informations sont stockées dans une structure arborescente fondée sur la représentation binaire de la clé (champ unique, qui identifie de façon unique chaque ensemble de données). Par exemple, examinez les chiffres suivants :

- 10 (est égal à 1010 en notation binaire) ;
- 7 (est égal à 0111 en notation binaire) ;
- 2 (est égal à 0010 en notation binaire).

Vous pourriez stocker ces chiffres dans une structure d'arbre binaire (voir Figure 15.6).

Figure 15.6
Un arbre binaire.



Les branches de l'arbre sont basées sur la représentation binaire de chaque chiffre, à n'importe quel niveau. Par exemple, pour stocker ou trouver le chiffre 10, vous commencez votre recherche par la racine, en examinant le premier bit contenu dans 1010, qui est 1. Le nombre 1 signifie que vous devez choisir la branche de droite, ce qui vous conduit à un nœud de l'arbre. Etant donné que ce nœud ne possède pas d'enfants, vous comparez le nombre qu'il contient avec celui que vous recherchez, en vue de trouver une correspondance. Dans ce cas, il y a correspondance.

Autre exemple. Pour trouver ou stocker le nombre 7, vous débutez également par la racine. Etant donné que le premier bit de la représentation binaire de ce nombre est 0, vous devez choisir la branche gauche, qui conduit à un nœud avec enfants. Vous devez donc de nouveau choisir quelle branche emprunter. Pour cela, vous examinez le second bit du nombre 7 qui est 1, ce qui vous conduit vers la branche droite. Comme précédemment, puisque ce nœud ne possède pas d'enfants, vous comparez le nombre qu'il contient avec celui que vous recherchez, en vue de trouver une correspondance.

Limitations du cache rapide pour le routage IP

Le cache rapide présente une limitation importante relative au stockage des préfixes IP, à savoir qu'il n'autorise pas le chevauchement des entrées. Par exemple, imaginez que des entrées en cache soient créées pour les préfixes IP suivants :

- 172.31.46.0/24 ;
- 172.31.46.128/25 ;
- 172.31.46.129/32.

Etant donné que le cache rapide ne tient pas compte du masque de sous-réseau (ou longueur de préfixe), il n'existe aucun moyen, lors d'une opération de recherche, de savoir que l'entrée 172.31.46.129 utilise un préfixe de 32 bits et que l'entrée 172.31.46.128 utilise un préfixe de 25 bits.

Pour contourner cette limitation, une solution simple consiste à créer une entrée de cache pour chaque hôte de destination. Mais, en raison du grand nombre d'entrées qui seraient ainsi créées, cette solution imposerait une charge de traitement trop importante, et consommerait une trop grande quantité d'espace mémoire.

Par conséquent, une autre solution, fondée sur l'ensemble de règles suivant, a été adoptée :

- Si la destination est directement connectée, mettre en cache avec une longueur de préfixe de 32 bits.
- Si plusieurs chemins de même coût existent vers cette destination, mettre en cache avec une longueur de préfixe de 32 bits.
- S'il s'agit d'un superréseau, mettre en cache, en utilisant la longueur de préfixe du superréseau.
- S'il s'agit d'un réseau principal sans sous-réseau, mettre en cache, en utilisant la longueur de préfixe du réseau principal.
- S'il s'agit d'un réseau principal avec sous-réseaux, mettre en cache, en utilisant le préfixe de plus grande longueur sur le réseau principal.

Par conséquent, en s'appuyant sur l'extrait de table de routage IP suivant, qui provient d'un routeur Cisco, on pourrait déterminer les longueurs de préfixe qu'il utilise pour différentes destinations :

```
router#show ip route
...
O 172.31.0.0 [110/11] via 172.25.10.210, 2d01h, Ethernet0
    [110/11] via 172.25.10.215, 2d01h, Ethernet0
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D EX 172.16.180.0/25 [170/281600] via 172.25.10.210, 3d20h, Ethernet0
D EX 172.16.180.24/32 [170/281600] via 172.25.10.210, 3d20h, Ethernet0
O 10.0.0.0 [110/11] via 172.25.10.210, 2d01h, Ethernet0
O 192.168.0.0/16 [110/11] via 172.25.10.210, 2d18h, Ethernet0
    172.25.0.0/24 is subnetted, 1 subnet
C 172.25.10.0 [0/0] via connected, Ethernet0
```

Voici quelques exemples :

- Chaque destination sur le réseau 172.31.0.0/16 sera placée en cache, avec une longueur de préfixe de 32 bits, car il existe deux chemins de même coût vers ce réseau, présent dans la table de routage.
- Chaque destination sur le réseau 172.16.0.0/16 sera placée en cache, avec une longueur de préfixe de 32 bits, car il existe une route d'hôte dans cette plage.
- Le réseau 10.0.0.0/8 recevra une entrée en cache, car il s'agit d'une route vers un réseau principal qui ne comprend pas de sous-réseau, de route d'hôte, de chemins de même coût, etc.
- Le réseau 192.168.0.0/16 recevra une entrée en cache, car il s'agit d'une route de superréseau sans sous-réseau.
- Toutes les destinations sur le réseau 172.25.10.0/24 seront placées en cache, avec une longueur de préfixe de 32 bits, car ce réseau est directement connecté au routeur.

Maintenance du cache rapide

Il est important d'assurer la maintenance des données placées en cache, pour éviter qu'elles ne soient périmées et qu'elles ne perdent leur synchronisation avec les informations maîtres qui ont servi à l'élaboration initiale du cache. Pour cela, deux méthodes sont mises en œuvre, à savoir l'invalidation d'entrées spécifiques et l'invalidation aléatoire d'entrées.

Dans le cas de la commutation rapide, la difficulté consiste à garantir la mise à jour du cache rapide, afin que son contenu corresponde à celui de la table de routage et du cache ARP (ou d'autres tables à partir desquelles les en-têtes MAC sont constitués).

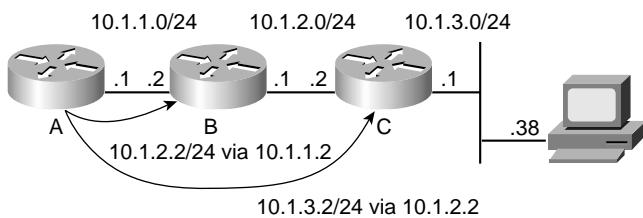
Invalidation d'entrées spécifiques

La difficulté de maintenir le cache de routes synchronisé avec la table de routage croît avec l'utilisation de la commutation de paquets IP, en raison d'un phénomène appelé *récursivité*, qui est expliqué plus bas.

Routage récursif

Etant donné que le routage récursif est un aspect très important, lié au fonctionnement d'un cache de routes, il peut être utile d'en examiner un exemple. La Figure 15.7 illustre le phénomène de récursivité sur un réseau.

Figure 15.7
Une route récursive.



A la Figure 15.7, le routeur A doit rechercher une route vers l'hôte 10.1.3.38, et déterminer quels prochains saut et en-tête MAC utiliser. Lorsqu'il examine sa table de routage, il découvre que cette destination est accessible *via* 10.1.2.2.

Etant donné que cette destination n'est pas directement connectée au routeur A, il doit de nouveau consulter sa table de routage afin de déterminer comment atteindre le prochain saut. Il recherche donc une route vers 10.1.2.2, et constate qu'il est accessible *via* 10.1.1.2, qui lui est directement connecté.

Le routeur A envoie donc à 10.1.1.2 tout le trafic destiné à 10.1.3.38, afin qu'il continue de l'acheminer.

Lorsque la commutation rapide est utilisée, le problème de récursivité est résolu au moment de la création d'une entrée en cache plutôt que lors de la commutation d'un paquet. C'est-à-dire que le cache de routes contient l'en-tête MAC et l'interface de sortie qui correspondent au prochain saut pour chaque destination. Les entrées en cache rapide sont donc indépendantes de celles de la table de routage et du cache ARP.

Puisque la récursivité est résolue lors de la création d'une entrée en cache, il n'existe aucune corrélation directe entre le cache rapide, d'une part, et la table de routage et le cache ARP, de l'autre. Par conséquent, il faut trouver un moyen de maintenir la synchronisation du cache avec les données des tables originales. La meilleure solution consiste à invalider, ou supprimer, les entrées de cache qui correspondent à des données modifiées dans les tables principales.

Des entrées peuvent être supprimées du cache rapide pour les raisons suivantes :

- L'entrée de cache ARP pour le prochain saut est modifiée, supprimée ou périmée.
- L'entrée de table de routage pour le préfixe est modifiée ou supprimée.
- L'entrée de table de routage pour le prochain saut vers cette destination est modifiée.

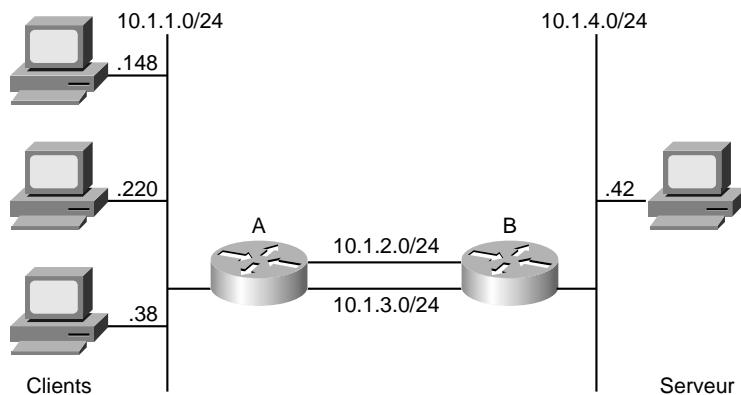
Invalidation aléatoire d'entrées

Le système IOS invalide de petites portions du cache rapide toutes les minutes, afin d'éviter que sa taille n'augmente excessivement, et également de resynchroniser régulièrement les entrées avec la table de routage et le cache ARP. Lorsque la quantité de mémoire disponible dépasse 200 Ko, le processus d'invalidation des entrées de cache supprime 1/20^e du total des entrées de cache de façon aléatoire. Lorsque l'espace disponible est inférieur à 200 Ko, le processus s'intensifie, invalidant 1/5^e du total des entrées par minute.

Equilibrage de charge avec la commutation rapide

A l'inverse de la commutation par processus, la commutation rapide ne supporte pas la répartition de charge par paquet. Cette limitation peut conduire à une exploitation inefficace du média lorsque plusieurs chemins existent vers une même destination. Elle s'explique par la séparation des tâches de routage et de transmission, mentionnée précédemment. Pour mieux comprendre ce problème, et les inconvénients qui l'accompagnent, examinons l'exemple illustré à la Figure 15.8.

Figure 15.8
Equilibrage de charge
avec le cache rapide.



A la Figure 15.8, plusieurs stations de travail sont connectées à un segment de réseau relié au routeur A. Chacune d'elles communique avec le même serveur, situé sur un autre segment de réseau, relié au routeur B. Le routeur A dispose de deux chemins parallèles vers le routeur B. En supposant qu'ils soient de même coût, il serait souhaitable de pouvoir les exploiter tous les deux, pour y équilibrer le trafic. Voyons donc ce qui se produirait.

En partant d'un cache rapide vide, le routeur A reçoit un paquet de la part du client 10.1.1.220, destiné au serveur 10.1.4.42. Comme nous l'avons vu plus haut, ce premier paquet est commuté par processus, et le routeur A crée une entrée dans le cache rapide pour la destination 10.1.4.42. Etant donné qu'il existe deux chemins de même coût vers cette destination (*via* le routeur B), le routeur A doit choisir l'un des deux chemins lorsqu'il crée l'entrée dans le cache. Il utilise pour cela l'algorithme de répartition de charge par paquet, décrit précédemment, afin de prendre une décision.

Lorsque le routeur A reçoit un autre paquet destiné au serveur 10.1.4.42, il est traité par commutation rapide, car il existe déjà une entrée dans le cache rapide pour cette destination. Etant donné que le pointeur vers l'interface de transmission est intégré au cache, le routeur A commute ce paquet sur le même chemin que le premier. Il continuera ainsi à envoyer tous les paquets destinés au serveur 10.1.4.42 sur ce chemin, jusqu'à ce que l'entrée en cache soit périme ou invalidée. Si cette entrée est supprimée, l'autre chemin pourra ensuite être choisi, mais les paquets seront de nouveau envoyés vers le serveur 10.1.4.42 uniquement sur ce chemin.

S'il existait plusieurs serveurs sur le réseau 10.1.4.0/24, le même processus se reproduirait pour chacun d'eux. C'est-à-dire que, même si le chemin placé en cache était différent pour chaque

serveur, les paquets de clients adressés à l'un d'entre eux seraient néanmoins acheminés uniquement sur le chemin qui lui est associé.

Imaginons maintenant que le trafic circule dans l'autre sens. Le routeur B place en cache les destinations sur le réseau de clients de la même manière que le routeur A. Dans ce cas, le routeur B crée trois entrées, les deux premières associées à un des deux chemins, et la troisième associée à l'autre chemin. Il se peut que le routeur B décide d'envoyer du trafic pour deux clients sur le chemin qui n'a pas été utilisé par le routeur A, ce qui entraînerait une distribution efficace de la charge de trafic sur les chemins parallèles. Mais, le routeur B peut également associer deux entrées de cache au même chemin que celui choisi par le routeur A pour envoyer le trafic vers le serveur, ce qui entraîne cette fois une utilisation non équilibrée des chemins.

Cette absence de stratégie d'équilibrage de charge déterministe représente une source de difficultés pour de nombreux concepteurs de réseaux. C'est pourquoi de nouvelles méthodes de commutation ont été développées, en vue de supporter des stratégies déterministes qui résolvent ce problème, parmi lesquelles on trouve la transmission expresse Cisco ou CEF (*Cisco Express Forwarding*), décrite plus loin dans ce chapitre.

Commutation optimale

La commutation optimale met en œuvre une commutation rapide, avec des optimisations relatives à la gestion de cache. A l'instar de la commutation rapide, elle commute un paquet au cours d'une seule interruption. La principale différence réside au niveau de l'accès au cache de routes. De plus, le programme de commutation optimale a été conçu de façon à tirer parti d'architectures de processeur spécifiques, tandis que le code pour la commutation rapide est générique, et n'a pas été optimisé pour un processeur particulier. A noter également que la commutation optimale est disponible uniquement pour le protocole IP.

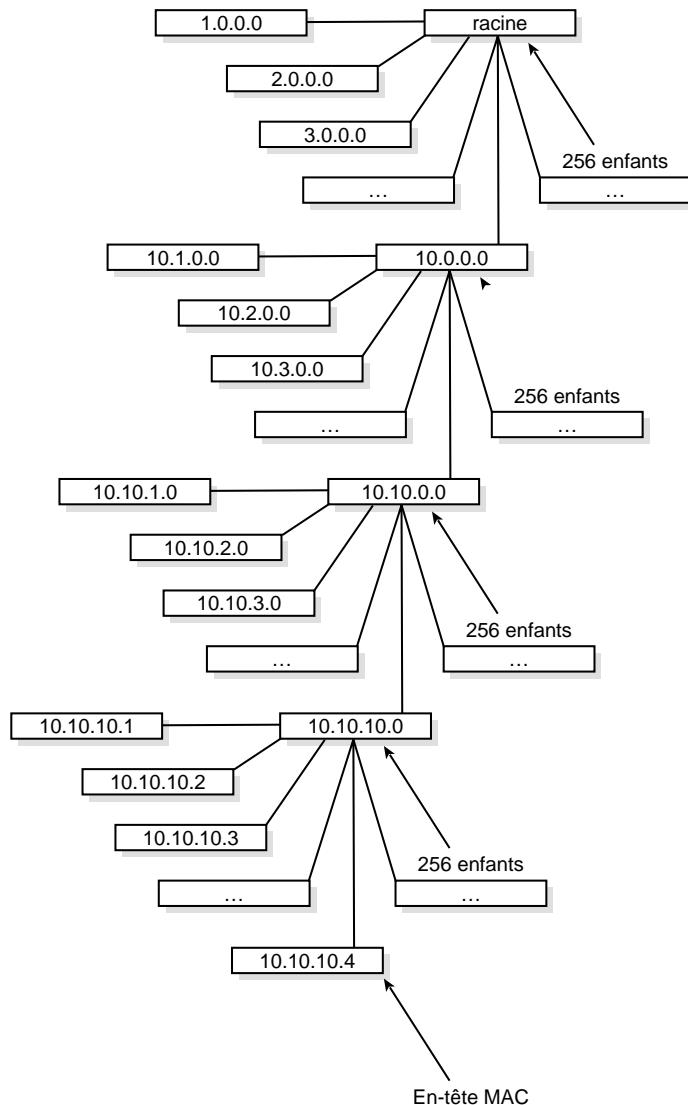
Plus haut dans ce chapitre, vous avez appris que l'accès au cache rapide se faisait par l'intermédiaire d'une table de hachage, avec les premières versions du système Cisco IOS, puis *via* un arbre binaire, à partir de la version 10.2. Lorsque la commutation optimale est utilisée, l'accès au cache se fait *via* un arbre multivoie (256 voies), appelé *mtrie* (*multiway trie*). La Figure 15.9 illustre un arbre *mtrie*.

Les informations d'accessibilité sont stockées sous forme d'un ensemble de noeuds qui comprennent chacun 256 enfants. Les en-têtes MAC précalculés sont stockés au niveau des noeuds. Bien que cette structure autorise des recherches plus rapides que l'arbre binaire, elle souffre néanmoins des limitations du cache rapide.

La commutation optimale partage les caractéristiques suivantes avec la commutation rapide :

- Les entrées de cache sont créées lorsque le premier paquet est commuté par processus vers une destination.
- Les entrées de cache sont invalidées au fur et à mesure que la table de routage ou d'autres informations en cache sont modifiées.
- L'équilibrage de charge est déterminé en fonction de l'adresse de destination.
- Les mêmes règles sont appliquées afin de déterminer quelle entrée sera créée pour une destination donnée.

Figure 15.9
Le cache optimal.



Le résultat de la commande `show ip cache optimum` ressemble beaucoup à celui de la commande `show ip cache`. Les en-têtes diffèrent en raison de la structure de données *mtrie* :

```

router#show ip cache optimum
Optimum Route Cache
 1 prefixes, 1 nodes, 0 leaf refcount, 8K bytes
 0 nodes pending, 0 node alloc failures
 8 prefix updates, 4 prefix invalidations
Prefix/Length  Age   Interface  Next Hop
10.1.1.16/32-24  1w4d  Ethernet0  10.1.1.16
  
```

Transmission expresse Cisco (CEF)

La fonctionnalité CEF (*Cisco Express Forwarding*, transmission expresse Cisco) est la méthode de commutation la plus récente et la plus rapide, disponible dans le système Cisco IOS. Elle a été développée afin d'éliminer les faiblesses majeures de la commutation rapide, parmi lesquelles :

- Absence de support pour le chevauchement des entrées en cache.
- Tout changement dans la table de routage ou dans le cache ARP entraîne l'invalidation de grandes sections du cache de routes, en raison d'une absence de corrélation entre ces zones de stockage d'informations de routage.
- Le premier paquet envoyé vers une destination quelconque doit être commuté par processus, afin qu'une entrée soit créée dans le cache de routes.
- Equilibrage inefficace de la charge de trafic dans certaines situations, principalement lorsque plusieurs hôtes communiquent avec un seul serveur.

La plupart de ces inconvénients ne posent pas de problèmes sur un réseau d'entreprise moyen, car les routes ne changent pas souvent, et les tables de routage conservent une taille acceptable. Mais il en va tout autrement dans un environnement tel que l'épine dorsale de l'Internet.

Les routeurs d'épine dorsale Internet doivent gérer des tables de routage très volumineuses (qui affichaient, en 1999, une moyenne de 56 000 routes), qui continuent d'augmenter. Certains de ces routeurs gèrent plus de 100 000 routes. Leur table de routage change également constamment, ce qui entraîne l'invalidation fréquente des entrées. En fait, ces entrées sont invalidées suffisamment souvent, de façon qu'une quantité importante du trafic traité par ces routeurs soit commutée par processus. La commutation CEF a été spécifiquement développée pour améliorer les performances de routage dans ce type d'environnements.

Cette méthode de commutation a été initialement testée sur l'Internet. Des séries d'images logicielles IOS spéciales, qui implémentent la commutation CEF, ont été distribuées aux fournisseurs de services Internet, afin d'observer leur fonctionnement dans des conditions d'utilisation extrêmes. Cette technologie a démontré sa capacité à gérer la charge de trafic de l'épine dorsale de l'Internet. Par conséquent, elle a été intégrée dans le produit Cisco IOS pour devenir le mode de commutation par défaut dans la version 10.2 du système. C'est actuellement la seule méthode de commutation disponible sur certaines plates-formes, en particulier sur le Cisco 12000 et le Catalyst 8500.

Fonctionnement de la commutation CEF

A l'inverse de la commutation rapide, qui crée en cache un sous-ensemble de la table de routage et des tables d'adresses MAC, CEF crée ses propres structures, qui reproduisent exactement le contenu de ces tables. Ces structures, qui sont au nombre de deux, représentent le cache rapide CEF :

- table CEF ;
- table de voisinage.

Table CEF

La table CEF est une version allégée de la table de routage, implémentée sous forme d'un arbre *mtrie* à 256 voies, afin de permettre des performances d'extraction optimales. Sa taille, ainsi que d'autres informations d'ordre général, peuvent être affichées en exécutant la commande `show ip cef summary` :

```
router#show ip cef summary
IP Distributed CEF with switching (Table Version 96)
  33 routes, 0 reresolve, 0 unresolved (0 old, 0 new)
  33 leaves, 31 nodes, 36256 bytes, 96 inserts, 63 invalidations
    1 load sharing elements, 328 bytes, 2 references
    1 CEF resets, 8 revisions of existing leaves
  refcounts: 8226 leaf, 8192 node
```

Adjacency Table has 5 adjacencies

Dans une structure d'arbre *mtrie* à 256 voies, chaque noeud peut comprendre jusqu'à 256 enfants. Dans une table CEF, chaque enfant (ou lien) est utilisé pour représenter une adresse différente dans un octet d'une adresse IP (voir Figure 15.10).

Par exemple, avec l'adresse IP 10.10.10.4, les données seraient localisées en extrayant le dixième enfant à partir de la racine, puis le dixième enfant à partir de ce noeud, puis de nouveau le dixième enfant à partir de ce noeud, et, enfin, le quatrième enfant à partir du dernier noeud, ou *nœud final*. Celui-ci contient un pointeur vers une entrée dans une autre table, appelée *table de voisinage*, qui contient l'en-tête MAC et d'autres informations nécessaires à la commutation du paquet.

NOTE

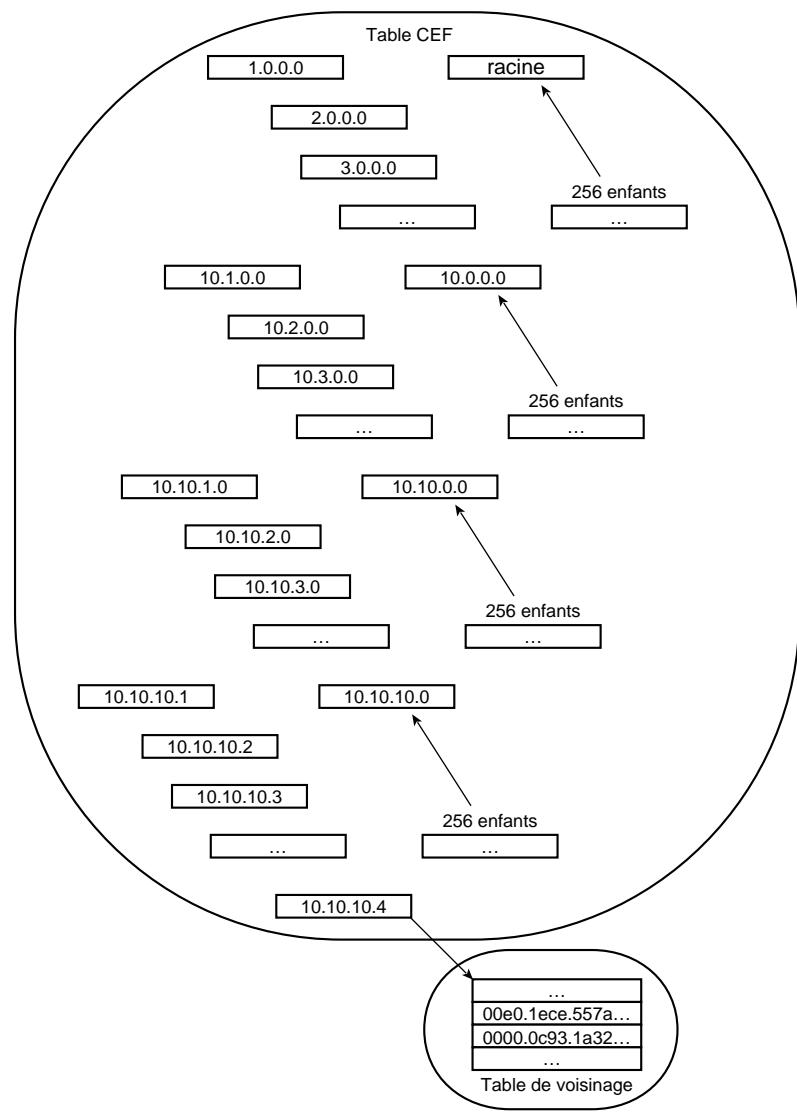
Un arbre *mtree* stocke les données dans la structure arborescente elle-même. Par exemple, lorsque cette structure est employée avec la commutation optimale, les données d'en-tête MAC utilisées afin de transmettre les paquets y sont donc stockées directement. Dans un arbre *mtrie*, la structure est uniquement utilisée pour localiser les données recherchées, qui sont situées ailleurs.

Table de voisinage

La table d'informations de voisinage (*adjacency table*) contient les données d'en-tête MAC qui permettent de se connecter directement aux prochains sauts. Ces données proviennent du cache ARP, de la table Frame Relay, ainsi que d'autres tables de ce type. La commande `show adjacency` permet d'afficher son contenu, par exemple :

```
router#show adjacency
Protocol Interface          Address
IP      POS0/0/0             point2point(15)
IP      Serial1/0/0          point2point(5)
IP      FastEthernet6/0/0    17.1.1.2(16)
IP      Ethernet4/0          10.105.1.1(9)
IP      Ethernet4/0          10.105.1.179(5)
Router#
```

Figure 15.10
Structure mtrie CEF et
table de voisinage.



Il existe plusieurs types d'entrées dans la table de voisinage, parmi lesquelles :

- **Voisin en cache.** Un en-tête MAC précalculé pour le prochain saut vers cette destination.
- **Punt.** Les paquets destinés à cette adresse doivent être transférés sur le prochain chemin de commutation.
- **Route d'hôte.** Cette destination est celle d'un hôte directement connecté.
- **Abandon.** Les paquets destinés à cette adresse sont abandonnés.

- **Incomplet.** L'en-tête MAC pour cette destination est incomplète, ce qui signifie habituellement que l'entrée correspondante dans le cache ARP est également incomplète ou incorrecte.
- **Interrogation.** Il s'agit d'une destination directement connectée, mais pour laquelle il n'existe pas d'en-tête MAC précalculé. Une requête ARP doit être envoyée afin de permettre la constitution de cet en-tête.

Avantages de la commutation CEF

A l'instar de la commutation rapide, la commutation CEF s'appuie sur les entrées en cache pour commuter les paquets lors d'une interruption de processeur. La différence entre ces deux méthodes réside au niveau de la création des entrées dans le cache. La commutation rapide requiert que le premier paquet envoyé vers une destination spécifique soit commuté par processus pour créer une entrée dans le cache. Dans le cas de commutation CEF, la table CEF est élaborée directement à partir de la table de routage, et la table de voisinage directement à partir du cache ARP. Ces structures CEF sont constituées avant que n'importe quel paquet soit commuté.

Avec la commutation CEF, chaque paquet reçu pour une destination accessible peut donc être transmis par le programme d'interruption du système IOS, et n'a pas besoin d'être commuté par processus pour qu'une entrée vers la destination correspondante soit créée. Cela permet d'améliorer considérablement les performances de routage sur les routeurs qui doivent gérer une grande quantité d'entrées de table de routage. Lorsque la commutation rapide classique est mise en œuvre, il arrive que le système IOS soit submergé de trafic de niveau processus, avant que les entrées en cache de routes n'aient pu être créées. La commutation CEF élimine cette lourde charge, ce qui évite que le goulet d'étranglement provoqué par la charge de commutation ne fasse planter le système IOS lorsque les routes du réseau sont instables.

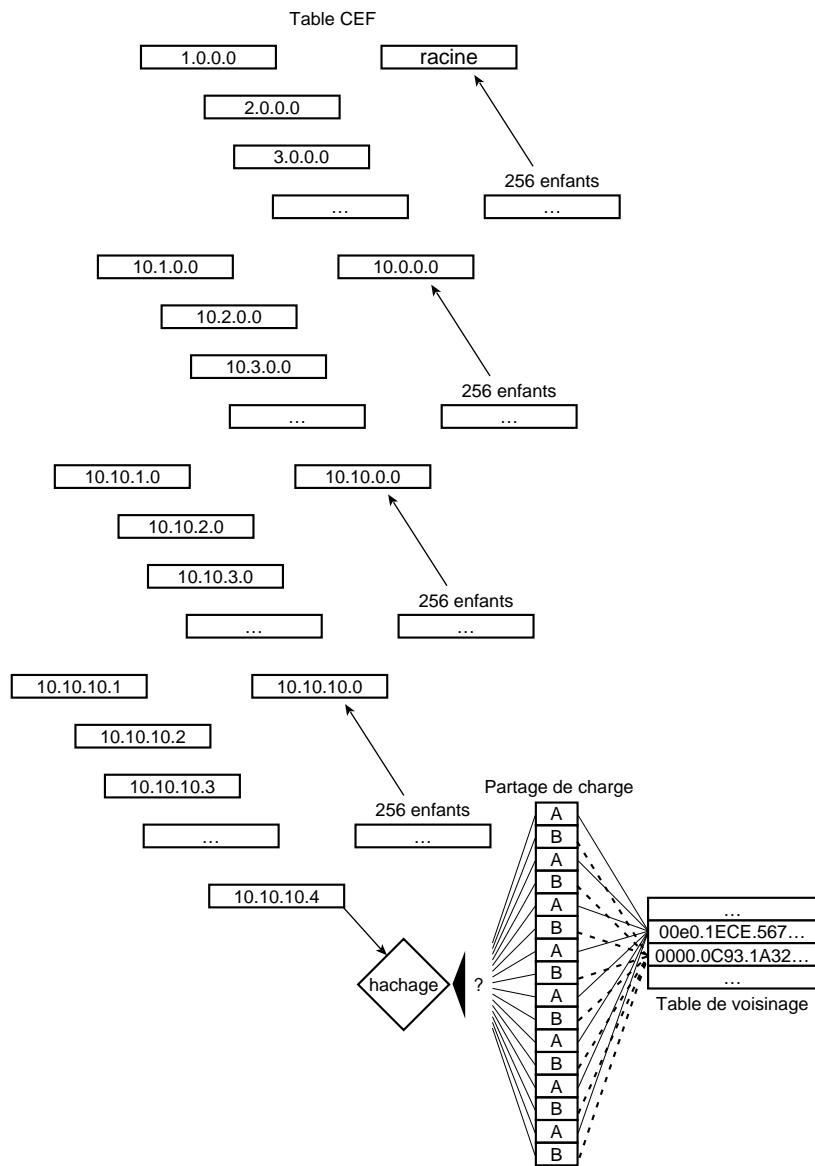
La répartition des données d'accessibilité/interface et des données d'en-têtes MAC dans deux structures reliées directement à leur source d'informations élimine également la nécessité d'un processus de synchronisation.

Les entrées contenues dans les structures CEF ne sont jamais pérémorées. Tout changement qui survient dans la table de routage ou le cache ARP est facilement reflété dans ces structures, ce qui élimine le besoin d'invalider un grand nombre d'entrées dans le cache pour garantir leur pertinence.

Equilibrage de charge avec la commutation CEF

La répartition de la charge de trafic avec la commutation CEF peut être réalisée en fonction des informations de source/destination (par défaut), ou par paquets. La première forme d'équilibrage résout les problèmes décrits précédemment dans l'exemple de commutation rapide, où tout le trafic destiné au serveur empruntait un seul lien, car les informations contenues dans le cache se fondent sur la destination. Pour cela, une entrée de la table CEF peut également pointer vers une structure de *partage de charge*, au lieu de pointer directement vers une entrée dans la table de voisinage (voir Figure 15.11).

Figure 15.11
La structure de partage de charge CEF.



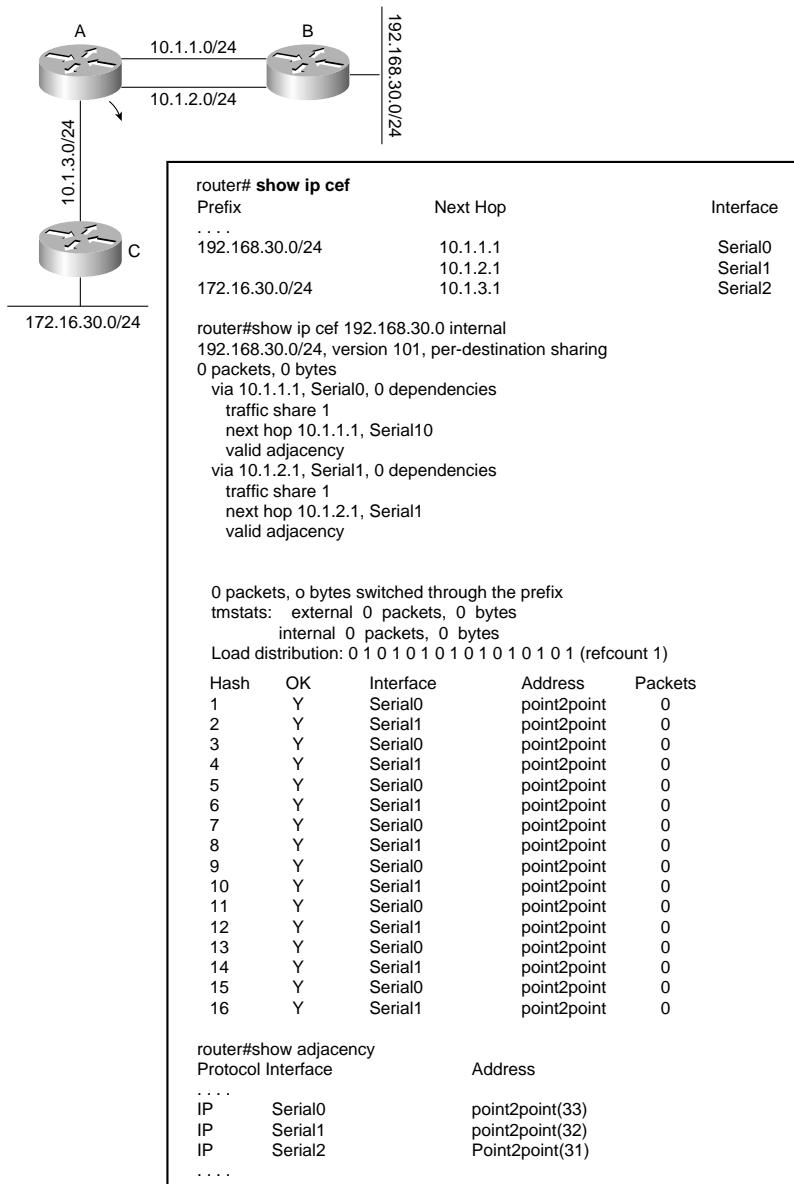
Lorsque le processus de commutation examine la table de partage de charge (plutôt que la table de voisinage), à la suite d'une recherche dans la table CEF, il se base sur les adresses source et de destination pour décider des entrées de partage de charge à utiliser. Chacune de ces entrées pointe vers une entrée de la table de voisinage qui contient l'en-tête MAC et d'autres informations nécessaires à la transmission du paquet.

Révision de CEF

Pour mieux comprendre la relation qui existe entre les structures de commutation CEF, examinez la Figure 15.12.

Figure 15.12

Tables CEF.



Dans cette figure, le routeur A dispose de trois tables CEF, utilisées pour commuter les paquets vers le réseau 192.168.30.0/24, à savoir la table CEF, la table de voisinage et la table de partage de charge. En revanche, pour commuter les paquets vers le réseau 172.16.30.0/24, seules deux tables sont nécessaires : la table CEF et celle de voisinage.

Résumé

Les routeurs Cisco commutent les paquets sur un chemin choisi parmi plusieurs. Les caractéristiques d'un chemin de commutation diffèrent selon qu'un cache est utilisé ou non, selon le moyen d'accès à ce cache et sa constitution, et selon le contexte de commutation (processus ou interruption) :

- La commutation par processus ne place aucune information en cache, et commute les paquets dans le contexte d'un processus.
- La commutation rapide place en cache — dans une table de hachage ou un arbre binaire — les informations d'accessibilité ainsi que les en-têtes MAC nécessaires pour acheminer les paquets, et les commute dans le contexte d'une interruption.
- La commutation CEF place les informations d'accessibilité dans une structure *mtrie*, et les en-têtes MAC nécessaires pour acheminer les paquets dans une table de voisinage. Les paquets sont commutés dans le contexte d'une interruption.

Le Tableau 15.1 résume les caractéristiques de ces méthodes de commutation.

Tableau 15.1 : Méthodes de commutation du système Cisco IOS

Méthode de commutation	Type de cache	Caractéristiques de traitement
Commutation par processus	Aucun	La commutation est réalisée par un processus planifié.
Commutation rapide	Table de hachage ou arbre binaire et cache de routes	Les paquets sont commutés par le processeur central lors d'une interruption.
Commutation optimale	<i>mtrie</i> et cache de routes rapide	Les paquets sont commutés par le processeur central lors d'une interruption.
Commutation CEF (Cisco Express Forwarding)	<i>mtrie</i> et table de voisinage	Les paquets sont commutés par le processeur central lors d'une interruption.

16

Redistribution EIGRP et OSPF

Par Anthony Bruno

Cette étude de cas traite des problèmes d'intégration de réseaux EIGRP (*Enhanced Interior Gateway Routing Protocol*) avec des réseaux OSPF (*Open Shortest Path First*). Cisco supporte ces deux protocoles et offre un moyen d'échanger des informations de routage entre des réseaux EIGRP et OSPF. Ces deux protocoles sans classe sont capables de gérer les masques de sous-réseau de longueur variable (VLSM, *Variable-Length Subnet Mask*) et la synthèse de routes. Cette étude de cas donne des exemples de redistribution d'informations de routage entre des réseaux implémentant ces protocoles et aborde les sujets suivants :

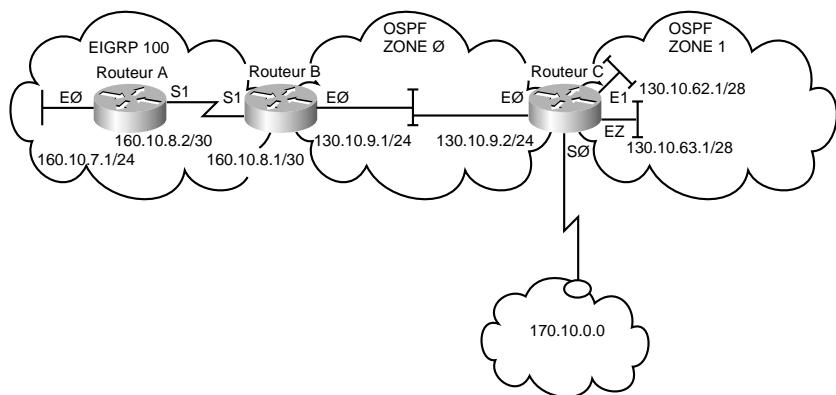
- configuration de la redistribution mutuelle entre EIGRP et OSPF ;
- vérification de la redistribution de routes ;
- ajout d'une route dans une liste de redistribution.

Configuration de la redistribution mutuelle entre EIGRP et OSPF

Il est parfois nécessaire d'adapter des topologies de réseaux complexes, telles que des nuages EIGRP ou OSPF indépendants, en vue d'implémenter une redistribution mutuelle. Par exemple, lorsqu'une société fait l'acquisition d'une autre société, l'une exécute peut-être OSPF et l'autre EIGRP. Il se peut également que la topologie physique d'un des réseaux ne supporte pas la hiérarchie à deux niveaux de OSPF, nécessitant la redistribution à partir d'un autre protocole de routage comme EIGRP. La redistribution est aussi nécessaire lors de la migration d'un protocole de routage existant vers un autre. Dans ce scénario, il est extrêmement important d'éviter les boucles de routage potentielles en filtrant les routes. La Figure 16.1 illustre la connexion d'un nuage EIGRP à un nuage OSPF. Le routeur A se trouve sur le nuage EIGRP. Le routeur B exécute à la fois OSPF et EIGRP,

car il assure la fonction de routeur intersystèmes autonomes (ASBR, *Autonomous System Border Router*) entre ces deux nuages. Le routeur C est un routeur interzones (ABR, *Area Border Router*) situé sur le nuage OSPF qui joue également le rôle de routeur ASBR pour le réseau externe 170.10.0.0.

Figure 16.1
Redistribution
mutuelle entre
des réseaux EIGRP
et OSPF.



Dans la Figure 16.1, il n'existe pas de routeur secondaire ou redondant reliant directement les nuages EIGRP et OSPF. Pourtant, un réseau traditionnel offre souvent des chemins parallèles ou de secours, introduisant d'ailleurs des risques de boucles de réinjection de routes. Afin d'empêcher les boucles de routage potentielles, des cartes de routage et des listes d'accès peuvent être utilisées pour configurer les routes qui doivent être annoncées et acceptées par chaque routeur. A l'aide des commandes suivantes, les routes OSPF sont redistribuées dans EIGRP :

```
!
router eigrp 100
default-metric 10000 1000 255 1 1500
network 160.10.0.0
redistribute ospf 109 route-map OSPFtoEIGRP
!
route-map OSPFtoEIGRP permit 10
match ip address 11
!
access-list 11 permit 130.10.0.0 0.0.255.255
!
```

Utilisez **default-metric** pour définir les métriques d'une route redistribuée dans les mises à jour EIGRP. Toutes les routes redistribuées dans EIGRP possèdent par défaut les métriques suivantes :

default-metric bande-passante délai fiabilité charge mtu

Le Tableau 16.1 présente les plages de valeurs pour chaque paramètre de cette commande.

Dans la configuration du routeur B, la liste d'accès 11 autorise la redistribution du réseau 130.10.0.0 dans EIGRP. Par contre, le réseau OSPF externe 170.10.0.0 n'est pas redistribué dans EIGRP. Ce chapitre décrit plus loin comment ajouter ce réseau dans la liste de redistribution.

Tableau 16.1 : Plages de valeurs pour les paramètres de la commande *default-metric*

<i>Métrique</i>	<i>Plage de valeurs</i>
Bandé passante (en Kbit/s)	1-4294967295
Délai (en unités de 10 microsecondes)	0-4294967295
Fiabilité (où 255 signifie 100% fiable)	0-255
Bandé passante effective, ou charge (où 255 signifie 100% de charge)	0-255
MTU (<i>Maximum Transmission Unit</i>) du chemin	1-4294967295

Exemples de fichiers de configuration

Cette section présente les configurations des routeurs A, B et C visant à implémenter la redistribution. Sur le routeur B, des cartes de routage sont combinées avec des listes d'accès pour spécifier les réseaux qui doivent être redistribués. Le routeur A est configuré avec EIGRP et le routeur C avec OSPF.

La configuration du routeur A est la suivante :

```
!
hostname routerA
!
interface Ethernet0
ip address 160.10.7.1 255.255.255.0
!
interface Serial1
ip address 160.10.8.2 255.255.255.252
!
router eigrp 100
network 160.10.0.0
!
```

La configuration du routeur A est simple et définit deux interfaces ainsi que le processus EIGRP 100. Comme aucune redistribution n'a lieu sur ce routeur, aucune carte de routage ou commande de redistribution n'est utilisée. Le routeur B est le voisin EIGRP du routeur A :

Il est configuré comme suit :

```
!
hostname routerB
!
interface Ethernet0
ip address 130.10.9.1 255.255.255.0
!
interface Serial1
ip address 160.10.8.1 255.255.255.252
!
router eigrp 100
redistribute ospf 109 route-map OSPFtoEIGRP
network 160.10.0.0
default-metric 10000 1000 255 1 1500
!
router ospf 109
redistribute eigrp 100 subnets route-map EIGRPToOSPF
network 130.10.9.0 0.0.0.255 area 0
```

```

!
access-list 10 permit 160.10.0.0 0.0.255.255
access-list 10 deny any
access-list 11 permit 130.10.0.0 0.0.255.255
access-list 11 deny any
!
route-map OSPFtoEIGRP permit 10
  match ip address 11
!
route-map EIGRPtoOSPF permit 10
  match ip address 10
!
```

La configuration du routeur B utilise **route-map OSPFtoEIGRP** avec la liste d'accès 11 pour contrôler les réseaux qui sont redistribués dans EIGRP. **default-metric** définit les métriques EIGRP des routes redistribuées avec les valeurs suivantes : 10 000 pour la bande passante, 1 000 pour le délai, 255 pour la fiabilité, 1 pour la charge et 1 500 octets pour l'unité MTU. Dans cet exemple, tous les sous-réseaux du réseau 130.10.0.0 sont redistribués dans EIGRP. **route-map EIGRP-toOSPF** combinée avec la liste d'accès 10 permet de contrôler les réseaux qui sont redistribués dans OSPF. Les routes redistribuées apparaissent par défaut comme étant des routes externes de type 2 dans OSPF. Dans cet exemple, tous les sous-réseaux du réseau 160.10.0.0 sont redistribués dans OSPF.

NOTE

Pour redistribuer des routes dans OSPF, utilisez le mot clé **subnets**. Il indique à OSPF de redistribuer toutes les routes de sous-réseaux. En son absence, seuls les réseaux non subdivisés sont redistribués par OSPF.

La configuration du routeur C est la suivante :

```

!
hostname routerC
!
interface Ethernet0
  ip address 130.10.9.2 255.255.255.0
!
interface Ethernet1
  ip address 130.10.62.1 255.255.255.240
!
interface Ethernet2
  ip address 130.10.63.1 255.255.255.240
!
router ospf 109
  redistribute static metric 1000
  network 130.10.9.0 0.0.0.255 area 0
  network 130.10.62.0 0.0.0.255 area 1
  network 130.10.63.0 0.0.0.255 area 1
  area 1 range 130.10.62.0 255.255.255.0
  area 1 range 130.10.63.0 255.255.255.0
!
  ip classless
  ip route 170.10.0.0 255.255.0.0 Serial0
!
```

La configuration du routeur C indique qu'il s'agit d'un routeur ABR OSPF pour les zones 0 et 1. **area range** est utilisée pour résumer les sous-réseaux d'une zone particulière sur un routeur ABR. **area 1 range 130.10.62.0 255.255.255.0** synthétise les 16 sous-réseaux suivants (en supposant que le masque 255.255.255.240 soit utilisé sur le réseau 130.10.62.0) en une seule entrée de route. Le réseau 130.10.63.0 est également ramené à 24 bits avec **area 1 range 130.10.63.0 255.255.255.0**. Si le routeur C avait d'autres routeurs voisins OSPF avec ces sous-réseaux, ils seraient synthétisés au niveau de ce routeur avant que la route ne soit transmise vers la zone 0.

Le routeur C est également un routeur ASBR OSPF pour le réseau 170.10.0.0. A l'aide de **redistribute static metric 1000**, la route statique est enregistrée dans la base de données OSPF en tant que route externe de type 2 avec une métrique (coût) de 1000.

Vérification de la redistribution de routes

La table de routage du routeur A, présentée ci-dessous, indique les deux réseaux qui lui sont connectés, c'est-à-dire 160.10.7.0/24 et 160.10.8.0/30. Les routes EIGRP externes (D EX) provenant du routeur B sont celles qui ont été redistribuées par OSPF. Les numéros qui apparaissent entre crochets représentent la distance administrative (170) et la métrique EIGRP calculée. Par défaut, toutes les routes EIGRP externes possèdent une distance administrative de 170 :

```
routerA#show ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
      U - per-user static route, o - ODR
      T - traffic engineered route

Gateway of last resort is not set

      160.10.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        160.10.8.0/30 is directly connected, Serial1
C        160.10.7.0/24 is directly connected, Ethernet0
      130.10.0.0/16 is variably subnetted, 3 subnets, 2 masks
D EX     130.10.9.0/24 [170/2425856] via 160.10.8.1, 00:02:01, Serial1
D EX     130.10.63.0/24 [170/2425856] via 160.10.8.1, 00:02:01, Serial1
D EX     130.10.62.0/24 [170/2425856] via 160.10.8.1, 00:02:01, Serial1
routerA#
```

Examinons maintenant la table de routage du routeur B. Une route OSPF externe de type 2 (O E2) provient du routeur C. Il s'agit d'une route statique qui a été redistribuée dans OSPF sur le routeur C. Le routeur B connaît aussi les routes OSPF interzones (O IA) communiquées par le routeur C. La seule route EIGRP présente est 160.10.7.0/24, car 160.10.8.0/30 est directement connecté à ce routeur. La table de routage n'indique pas si les commandes de redistribution ont été exécutées correctement. Pour le vérifier, examinez la table topologique EIGRP et la base de données OSPF.

```
routerB#show ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
```

```

U - per-user static route, o - ODR
T - traffic engineered route

Gateway of last resort is not set

O E2 170.10.0.0/16 [110/1000] via 130.10.9.2, 00:08:36, Ethernet0
    160.10.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       160.10.8.0/30 is directly connected, Serial1
D       160.10.7.0/24 [90/2297856] via 160.10.8.2, 00:08:37, Serial1
    130.10.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       130.10.9.0/24 is directly connected, Ethernet0
O IA     130.10.63.0/24 [110/11] via 130.10.9.2, 00:08:37, Ethernet0
O IA     130.10.62.0/24 [110/11] via 130.10.9.2, 00:08:37, Ethernet0
routerB#

```

La table topologique EIGRP présente les routes OSPF redistribuées, qui seront propagées sur le nuage EIGRP. Notez que la route OSPF externe 170.10.0.0 n'apparaît pas dans cette table :

```

routerB#show ip eigrp topology

IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 130.10.9.0/24, 1 successors, FD is 512000
    via Redistributed (512000/0)
P 160.10.8.0/30, 1 successors, FD is 2169856
    via Connected, Serial1
P 160.10.7.0/24, 1 successors, FD is 2297856
    via 160.10.8.2 (2297856/128256), Serial1
P 130.10.63.0/24, 1 successors, FD is 512000
    via Redistributed (512000/0)
P 130.10.62.0/24, 1 successors, FD is 512000
    via Redistributed (512000/0)
routerB#

```

show ip ospf database affiche tous les états de liens (*Link States*) présents dans la base de données OSPF pour tous les types d'états de liens. Comme il existe deux routeurs OSPF, il y a donc deux états de liens de routeur (*Router Link States*). Comme il existe un réseau broadcast (Ethernet) dans la zone 0, il y a donc un état de lien de réseau (*Net Link State*). Les deux états de liens de réseau résumés (*Summary Net Link States*) proviennent du routeur ABR C. On peut également remarquer trois états de liens externes (*External Link States*), deux provenant de la redistribution locale sur le routeur B (160.10.8.1) et un provenant du routeur C (130.10.63.1) :

```

routerB#show ip ospf data

OSPF Router with ID (160.10.8.1) (Process ID 109)

        Router Link States (Area 0)

  Link ID      ADV Router      Age      Seq#      Checksum Link count
 130.10.63.1   130.10.63.1   1627  0x80000009  0xF164      1
 160.10.8.1    160.10.8.1   1852  0x80000002  0x3A57      1

        Net Link States (Area 0)

  Link ID      ADV Router      Age      Seq#      Checksum
 130.10.9.2    130.10.63.1   47   0x80000002  0x60F3

```

```

Summary Net Link States (Area 0)

Link ID      ADV Router      Age      Seq#      Checksum
130.10.62.0  130.10.63.1  47       0x80000004 0x168A
130.10.63.0  130.10.63.1  47       0x80000004 0xB94

Type-5 AS External Link States

Link ID      ADV Router      Age      Seq#      Checksum Tag
160.10.7.0   160.10.8.1   506     0x80000001 0xC575   0
160.10.8.0   160.10.8.1   527     0x80000001 0xA894   0
170.10.0.0   130.10.63.1  1647    0x80000001 0x88BE   0
routerB#

```

Passons maintenant à la table de routage du routeur C. Elle contient une entrée statique pour le réseau 170.10.0.0. Les routes provenant du nuage EIGRP apparaissent comme étant des routes OSPF externes (E2). Les autres réseaux sont directement connectés :

```

routerC#show ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
      U - per-user static route, o - ODR
      T - traffic engineered route

Gateway of last resort is not set

S  170.10.0.0/16 is directly connected, Serial0
  160.10.0.0/16 is variably subnetted, 2 subnets, 2 masks
O E2   160.10.8.0/30 [110/20] via 130.10.9.1, 00:11:03, Ethernet0
O E2   160.10.7.0/24 [110/20] via 130.10.9.1, 00:11:03, Ethernet0
  130.10.0.0/24 is subnetted, 3 subnets
C     130.10.9.0 is directly connected, Ethernet0
C     130.10.62.0 is directly connected, Ethernet1
C     130.10.63.0 is directly connected, Ethernet2
routerC#

```

Dans la sortie précédente, deux sous-réseaux proviennent du réseau 160.10.0.0. Utilisez la commande OSPF **summary-address** sur le routeur B pour résumer encore davantage ce réseau. Cette commande permet de synthétiser des routes externes sur des routeurs ASBR, mais pas des routes interzones sur des routeurs ABR :

```

routerB(config)#router ospf 109
routerB(config-router)# summary-address 160.10.0.0 255.255.0.0

```

A présent, le routeur C ne voit qu'un seul réseau :

```

routerC>show ip ro
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
      U - per-user static route, o - ODR
      T - traffic engineered route

```

```

Gateway of last resort is not set

S      170.10.0.0/16 is directly connected, Null0
O E2 160.10.0.0/16 [110/20] via 130.10.9.1, 00:03:04, Ethernet0
      130.10.0.0/24 is subnetted, 3 subnets
C          130.10.9.0 is directly connected, Ethernet0
C          130.10.62.0 is directly connected, Loopback0
C          130.10.63.0 is directly connected, Loopback1
routerC>

```

Ajout d'une route dans une liste de redistribution

Le réseau 170.10.0.0 était une route externe dans OSPF. Il n'a pas été redistribué dans EIGRP sur le routeur B (voir les commandes **route-map OSPFtoEIGRP** et **access-list 11** dans la configuration du routeur B à la section "Exemples de fichiers de configuration"). Supposez à présent que vous souhaitez autoriser les utilisateurs du nuage EIGRP à accéder au réseau 170.10.0.0 (voir Figure 16.2). Pour cela, ajoutez ce réseau dans la liste d'accès 11 afin que cette route puisse figurer dans la table topologique EIGRP. Cette liste d'accès devrait donc être définie comme suit :

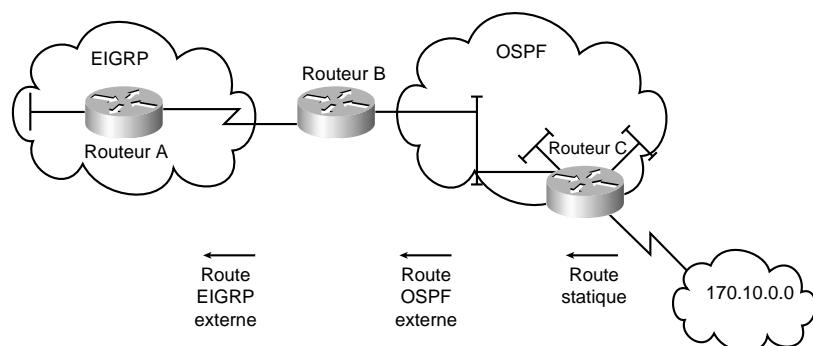
```

access-list 11 permit 130.10.0.0 0.0.255.255
access-list 11 permit 170.10.0.0 0.0.255.255
access-list 11 deny any

```

Figure 16.2

Réseau 170.10.0.0
— Route externe
à EIGRP.



La table topologique EIGRP sur le routeur B inclut maintenant le nouveau réseau :

```

routerB#show ip eigrp top
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 130.10.9.0/24, 1 successors, FD is 512000
      via Redistributed (512000/0)
P 170.10.0.0/16, 1 successors, FD is 512000
      via Redistributed (512000/0)
P 160.10.8.0/30, 1 successors, FD is 2169856
      via Connected, Serial1
P 160.10.7.0/24, 1 successors, FD is 2297856
      via 160.10.8.2 (2297856/128256), Serial1

```

```
P 130.10.63.0/24, 1 successors, FD is 512000
    via Redistributed (512000/0)
P 130.10.62.0/24, 1 successors, FD is 512000
    via Redistributed (512000/0)
```

A présent que cette route figure dans la table topologique du routeur B, on peut voir que la table topologique du routeur A l'inclut également :

```
routerA>show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
      U - per-user static route, o - ODR
      T - traffic engineered route

Gateway of last resort is not set

D EX 170.10.0.0/16 [170/2425856] via 160.10.8.1, 00:01:11, Serial1
  160.10.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       160.10.8.0/30 is directly connected, Serial1
C       160.10.7.0/24 is directly connected, Loopback0
  130.10.0.0/16 is variably subnetted, 3 subnets, 2 masks
D EX     130.10.9.0/24 [170/2425856] via 160.10.8.1, 00:20:47, Serial1
D EX     130.10.63.0/24 [170/2425856] via 160.10.8.1, 00:01:12, Serial1
D EX     130.10.62.0/24 [170/2425856] via 160.10.8.1, 00:01:12, Serial1
routerA>
```

La route vers le réseau 170.10.0.0 est maintenant présente dans le nuage EIGRP et cette étude de cas se termine. Les cartes de routage et listes d'accès ont été utilisées pour contrôler la redistribution des réseaux EIGRP et OSPF, et les commandes **area-range** et **summary-address** ont servi à synthétiser les routes dans OSPF.

Résumé

Sachant qu'il est possible de combiner l'utilisation de OSPF et de EIGRP, il est important de s'en tenir aux méthodes décrites dans ce chapitre pour pouvoir exploiter les fonctionnalités de ces deux protocoles sur un interréseau. Configurez des routeurs ASBR supportant à la fois EIGRP et OSPF et redistribuez les routes EIGRP dans OSPF, et inversement. Dans OSPF, utilisez **summary** pour résumer davantage des réseaux redistribués. Utilisez des cartes de routages et des listes d'accès pour contrôler la redistribution des réseaux. Vous pouvez également créer des zones OSPF au moyen de routeurs ABR assurant la synthèse de routes.

Configuration de EIGRP sur des réseaux Novell et AppleTalk

Par Anthony Bruno

Outre IP, EIGRP (*Enhanced IGRP*) supporte deux autres protocoles de niveau réseau, AppleTalk et Novell IPX (*Internetwork Packet Exchange*). Chacun d'eux présente des fonctionnalités spécifiques à valeur ajoutée. EIGRP pour Novell IPX supporte les mises à jour SAP (*Service Advertisement Protocol*) élimine la limitation de métrique de 15 sauts imposée par RIP (*Routing Information Protocol*), et garantit l'utilisation d'un chemin optimal. Un routeur qui exécute EIGRP pour AppleTalk supporte les mises à jour de routage partielles et assure la répartition de charge ainsi que l'utilisation d'un chemin optimal.

Deux études de cas présentent les avantages et les aspects relatifs à l'intégration de EIGRP sur les types de réseaux suivants :

- **Novell IPX.** Le réseau IPX existant exécute RIP et SAP.
- **AppleTalk.** Le réseau AppleTalk existant exécute le protocole RTMP (*Routing Table Maintenance Protocol*).

Réseau Novell IPX

Cette étude de cas illustre l'intégration de EIGRP sur un réseau Novell IPX en deux étapes : la configuration d'un réseau IPX et l'ajout de EIGRP sur ce réseau.

Les aspects essentiels liés à cette intégration sur un réseau IPX exécutant RIP et SAP sont les suivants :

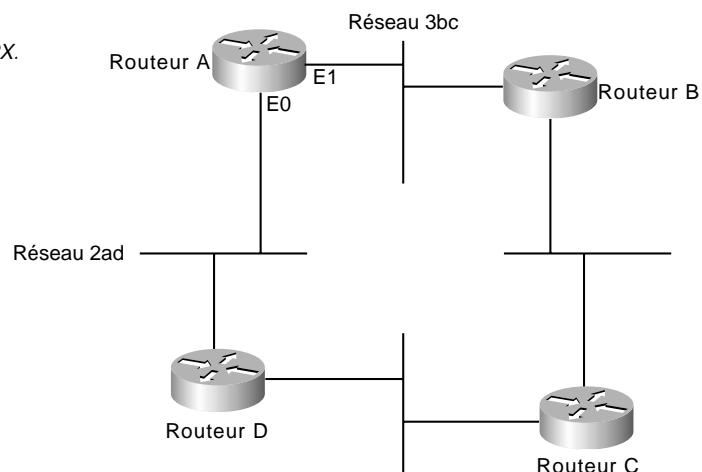
- sélection de route ;
- redistribution et gestion de métriques ;
- redistribution de RIP IPX vers EIGRP, et inversement ;
- réduction du trafic SAP.

Configuration d'un réseau Novell IPX

L'implémentation Cisco du protocole IPX de Novell fournit toutes les fonctions d'un routeur Novell. Cette étude de cas présente la configuration des routeurs pour qu'ils puissent exécuter ce protocole (voir Figure 17.1).

Figure 17.1

Configuration d'un réseau Novell IPX.



Les commandes de configuration qui activent le routage IPX sur le routeur A sont les suivantes :

```

ipx routing
interface ethernet 0
ipx network 2ad
interface ethernet 1
ipx network 3bc

```

NOTE

A partir de la version 9.21 de System Software, la commande servant à activer le routage Novell IPX est **ipx** et non plus **novell**.

Intégration de EIGRP sur un réseau Novell IPX

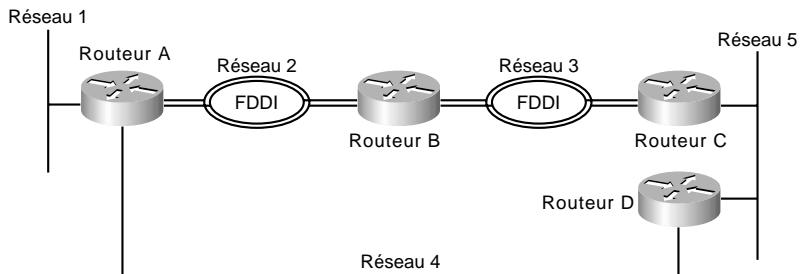
Le protocole EIGRP pour un réseau Novell IPX présente les mêmes fonctionnalités de reroutage rapide et de mises à jour partielles que EIGRP pour IP. De plus, il dispose de plusieurs fonctionnalités facilitant la conception de grands réseaux Novell IPX fiables.

La première caractéristique de ce protocole est le support des mises à jour SAP incrémentielles. Les routeurs RIP IPX envoient des mises à jour RIP et SAP complètes toutes les 60 secondes, qui peuvent consommer une quantité considérable de bande passante. EIGRP pour IPX envoie des mises à jour uniquement lorsque des changements se produisent sur le réseau, et ne transmet que les informations modifiées.

La deuxième caractéristique est qu'il permet de construire de grands réseaux. Les réseaux RIP IPX sont limités à une étendue de 15 sauts (*hops*), alors que les réseaux EIGRP peuvent atteindre 224 sauts.

La troisième caractéristique est la sélection du chemin optimal. La métrique utilisée par RIP pour la détermination de route s'appuie sur le nombre de ticks (*ticks*) (sachant qu'un tic équivaut à 1/18^e de seconde). Lorsque deux routes présentent le même nombre de ticks, le compte de sauts est utilisé pour les départager et c'est la route possédant le compte de sauts le plus faible qui est choisie. A la place des métriques de saut et de tic, EIGRP pour IPX utilise une métrique combinée basée sur le délai et la bande passante. La Figure 17.2 illustre le fonctionnement de la sélection du chemin optimal avec EIGRP pour IPX.

Figure 17.2
Sélection de chemin optimal avec EIGRP pour Novell IPX.

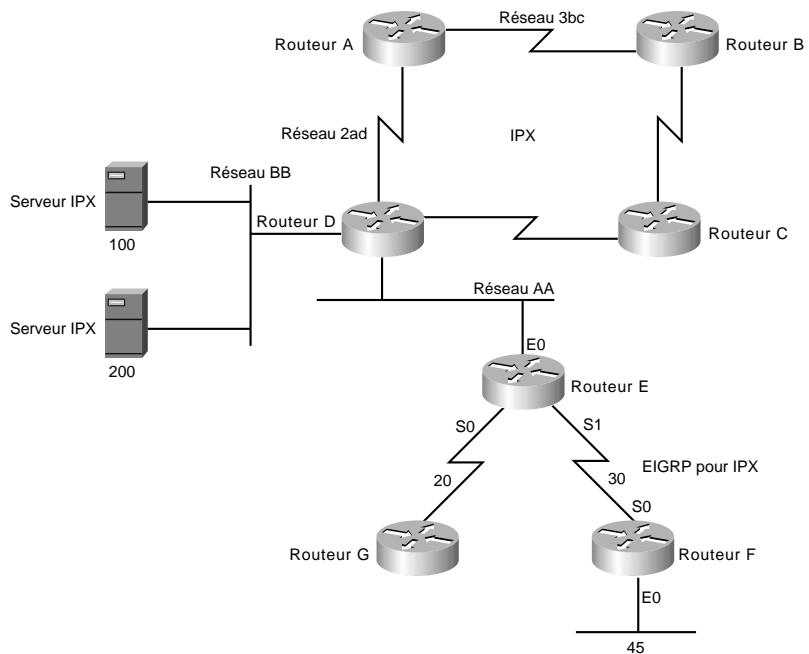


Les interfaces Ethernet et FDDI possèdent une valeur de tic de 1. Lorsque le routeur A est configuré pour Novell RIP, il choisit la connexion Ethernet via le réseau 4 pour atteindre le réseau 5, car le routeur D ne se situe qu'à un saut de lui. Toutefois, le chemin le plus rapide pour atteindre le réseau 5 comprend deux sauts, via les anneaux FDDI. Avec EIGRP pour IPX, le routeur A choisit automatiquement le chemin optimal qui passe ici par les deux routeurs B et C pour atteindre le réseau 5.

Pour ajouter EIGRP sur un réseau Novell RIP et SAP, configurez ce protocole sur les interfaces d'un routeur Cisco, qui est relié à d'autres routeurs Cisco exécutant également EIGRP, et configurez RIP et SAP sur les interfaces connectées vers des hôtes et routeurs Novell ne supportant pas EIGRP.

Dans la Figure 17.3, les routeurs E, F et G exécutent EIGRP pour IPX. Le routeur E redistribue les informations de route EIGRP vers le routeur D via le réseau AA.

Figure 17.3
Ajout de EIGRP sur un réseau Novell IPX.



```
interface serial 0
ipx network 30
ipx router eigrp 10
network 30
network 45
```

Une partie de la sortie produite par **show ipx route** sur le routeur E indique que le réseau 45 a été découvert par EIGRP (E), alors que le réseau BB l'a été via une mise à jour RIP (R) :

```
R Net 3bc
R Net 2ad
C Net 20 (HDLC), is directly connected, 66 uses, Serial0
C Net 30 (HDLC), is directly connected, 73 uses, Serial1
E Net 45 [2195456/0] via 30.0000.0c00.c47e, age 0:01:23, 1 uses, Serial1
C Net AA (NOVELL-ETHER), is directly connected, 3 uses, Ethernet0
R Net BB [1/1] via AA.0000.0c03.8b25, 48 sec, 87 uses, Ethernet0
```

Une partie de la sortie produite par **show ipx route** sur le routeur F indique que les réseaux 20, AA et BB ont été découverts par EIGRP (E) :

```
E Net 20 [2681856/0] via 30.0000.0c01.f0ed, age 0:02:57, 1 uses, Serial0
C Net 30 (HDLC), is directly connected, 47 uses, Serial0
C Net 45 (NOVELL-ETHER), is directly connected, 45 uses, Ethernet0
E Net AA [267008000/0] via 30.0000.0c01.f0ed, age 0:02:57, 1 uses, Serial0
E Net BB [268416000/2] via 30.0000.0c01.f0ed, age 0:02:57, 11 uses, Serial0
```

show ipx servers exécutée sur le routeur E indique que des informations de serveur ont été recueillies via les mises à jour SAP périodiques (P) :

```
Codes: S - Static, I - Incremental, P - Periodic, H - Holddown
5 Total IPX Servers
Table ordering is based on routing and server info
Type Name          Net Address      Port  Route Hops Itf
P   4 Networkers   100.0000.0000.0001:0666  2/02   2   Et1
P   5 Chicago       100.0000.0000.0001:0234  2/02   2   Et1
P   7 Michigan      100.0000.0000.0001:0123  2/02   2   Et1
P   8 NetTest1     200.0000.0000.0001:0345  2/02   2   Et1
P   8 NetTest       200.0000.0000.0001:0456  2/02   2   Et1
```

show ipx servers exécutée sur le routeur F indique que des informations de serveur ont été recueillies via les mises à jour SAP incrémentielles (I) autorisées avec EIGRP :

```
Codes: S - Static, I - Incremental, P - Periodic, H - Holddown
5 Total IPX Servers
Table ordering is based on routing and server info
Type Name          Net Address      Port  Route      Hops Itf
I   4 Networkers   100.0000.0000.0001:0666 268416000/03 3   Se0
I   5 Chicago       100.0000.0000.0001:0234 268416000/03 3   Se0
I   7 Michigan      100.0000.0000.0001:0123 268416000/03 3   Se0
I   8 NetTest1     200.0000.0000.0001:0345 268416000/03 3   Se0
I   8 NetTest       200.0000.0000.0001:0456 268416000/03 3   Se0
```

show ipx servers exécutée sur le routeur E montre que l'état des réseaux est passif (P) et que chaque réseau fournit un successeur avec une distance possible (FD, *Feasible Distance*) via un voisin vers la destination. Par exemple, pour le réseau 45, le voisin est situé à l'adresse 0000.0C00.C47E et la métrique calculée/annoncée pour ce voisin vers la destination est 2195456/281600 :

```
IPX EIGRP Topology Table for process 10
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 20, 1 successors, FD is 1
```

```

        via Connected, Serial0
P 30, 1 successors, FD is 1
        via Connected, Serial1
P 45, 1 successors, FD is 2195456
        via 30.0000.0c00.c47e (2195456/281600), Serial1
P AA, 1 successors, FD is 266496000
        via Redistributed (266496000/0),
P BB, 1 successors, FD is 267904000
        via Redistributed (267904000/0),

```

La sortie de **show ipx eigrp topology** exécutée sur le routeur F liste les informations suivantes :

```

IPX EIGRP Topology Table for process 10
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 20, 1 successors, FD is 2681856
        via 30.0000.0c01.f0ed (2681856/2169856), Serial0
P 30, 1 successors, FD is 1
        via Connected, Serial0
P 45, 1 successors, FD is 1
        via Connected, Ethernet0
P AA, 1 successors, FD is 267008000
        via 30.0000.0c01.f0ed (267008000/266496000), Serial0
P BB, 1 successors, FD is 268416000
        via 30.0000.0c01.f0ed (268416000/267904000), Serial0

```

Sélection de route

Les routes EIGRP pour IPX sont automatiquement prioritaires par rapport aux routes RIP, et ce indépendamment des métriques, à moins qu'une route RIP ne possède un compte de sauts inférieur au compte de sauts externe spécifié dans la mise à jour EIGRP (par exemple, un serveur annonçant son propre réseau interne).

Redistribution et gestion de métriques

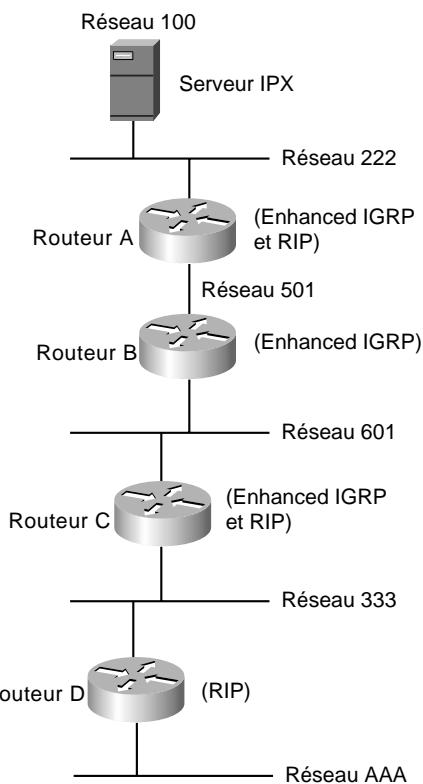
La redistribution est automatique entre RIP et EIGRP et peut être désactivée au moyen de la commande **no redistribute**. Par contre, elle ne se fait pas automatiquement entre différents systèmes autonomes EIGRP.

La métrique utilisée pour l'intégration de RIP avec EIGRP combine la bande passante et le délai, avec un décalage de 8 bits vers la gauche. La métrique utilisée pour intégrer EIGRP avec RIP s'appuie sur la métrique externe plus 1. Un routeur avec EIGRP pour IPX, qui redistribue RIP dans EIGRP, prend en compte la métrique RIP associée à chaque route RIP, l'incrémentera puis la stockera dans la table de routage EIGRP comme métrique externe.

Dans la Figure 17.4, un serveur Novell IPX avec une adresse de réseau interne de 100 annonce cette adresse au moyen de RIP sur le réseau 222. Le routeur A reçoit cette annonce et la place dans sa table de routage comme étant éloignée de 1 saut et de 1 tic. Le routeur A l'annonce ensuite au routeur B sur le réseau 501 au moyen de EIGRP.

Figure 17.4

Exemple de gestion de métrique IPX.



La configuration pour le routeur A est la suivante :

```

ipx routing
!
interface ethernet 0
ipx network 222
!
interface serial 0
ipx network 501
!
ipx router eigrp 9000
network 222
network 501
!
! Les commandes suivantes désactivent RIP IPX sur l'interface série
!
ipx router rip
no network 501
  
```

La configuration pour le routeur B est la suivante :

```

ipx routing
!
interface ethernet 0
ipx network 601
  
```

```

!
interface serial 0
ipx network 501

ipx router eigrp 9000
network 501
network 601
!
! La commande suivante désactive RIP IPX sur ce routeur
!
no ipx router rip

```

La configuration pour le routeur C est la suivante :

```

ipx routing
!
interface ethernet 0
ipx network 333
!
interface ethernet 1
ipx network 601
!
ipx router eigrp 9000
network 333
network 601
!
! Les commandes suivantes désactivent RIP IPX sur Ethernet 1
!
ipx router rip
no network 601

```

La configuration pour le routeur D est la suivante :

```

ipx routing
!
interface ethernet 0
ipx network 333
!
interface ethernet 1
ipx network AAA

```

Voici la sortie de **show ipx route** sur le routeur A :

```

R Net 100 [1/1] via 222.0260.8c4c.4f22, 59 sec, 1 uses, Ethernet0
C Net 222 (ARPA), is directly connected, 1252 uses, Ethernet0
E Net 333 [46277376/0] via 501.0000.0c05.84bc, age 0:04:07, 1 uses, Serial0
C Net 501 (HDLC), is directly connected, 3908 uses, Serial0
E Net 601 [46251776/0] via 501.0000.0c05.84bc, age 5:21:38, 1 uses, Serial0
E Net AAA [268441600/2] via 501.0000.0c05.84bc, age 0:16:23, 1 uses, Serial0

```

Voici la sortie de **show ipx route** sur le routeur B :

```

E Net 100 [268416000/2] via 501.0000.0c05.84b4, age 0:07:30, 2 uses, Serial0
E Net 222 [267008000/0] via 501.0000.0c05.84b4, age 0:07:30, 1 uses, Serial0
E Net 333 [307200/0] via 601.0000.0c05.84d3, age 0:07:30, 1 uses, Ethernet0
C Net 501 (HDLC), is directly connected, 4934 uses, Serial0
C Net 601 (NOVELL-ETHER), is directly connected, 16304 uses, Ethernet0
E Net AAA [267929600/2] via 601.0000.0c05.84d3, age 0:14:40, 1 uses, Ethernet0

```

Voici la sortie de **show ipx route** sur le routeur C :

```
E Net 100 [268441600/2] via 601.0000.0c05.84bf, age 0:07:33, 1 uses, Ethernet1
E Net 222 [267033600/0] via 601.0000.0c05.84bf, age 0:07:34, 1 uses, Ethernet1
C Net 333 (NOVELL-ETHER), is directly connected, 15121 uses, Ethernet0
E Net 501 [46251776/0] via 601.0000.0c05.84bf, age 0:07:32, 9 uses, Ethernet1
C Net 601 (NOVELL-ETHER), is directly connected, 1346 uses, Ethernet1
R Net AAA [1/1] via 333.0000.0c05.8b25, 35 sec, 1 uses, Ethernet0
```

Voici la sortie de **show ipx route** sur le routeur D :

```
R Net 100 [8/2] via 333.0000.0c05.84d1, 18 sec, 1 uses, Ethernet0
R Net 222 [6/1] via 333.0000.0c05.84d1, 18 sec, 1 uses, Ethernet0
R Net 333 [1/1] via 333.0000.0c05.84d1, 18 sec, 1 uses, Ethernet0
R Net 501 [3/1] via 333.0000.0c05.84d1, 17 sec, 3 uses, Ethernet0
R Net 601 [1/1] via 333.0000.0c05.84d1, 18 sec, 1 uses, Ethernet0
C Net AAA (SNAP), is directly connected, 20 uses, Ethernet1
```

La métrique EIGRP est créée en utilisant les tics RIP comme vecteur de délai. Le compte de sauts est incrémenté et stocké comme métrique externe. Le délai externe est également enregistré. Le routeur B calcule la métrique vers le réseau 100 en fonction des informations reçues du routeur A et la place dans sa table de routage. Dans ce cas, la valeur de tics pour le réseau 100 est de 8.

Le "2" après la barre oblique dans l'entrée de routage pour le réseau 100 est la métrique externe. Ce nombre n'augmente pas lorsque la route est dans le système autonome EIGRP. Le routeur C calcule la métrique vers le réseau 100 par l'intermédiaire du routeur B, et la place dans sa table de routage. Finalement, le routeur C redistribue ces informations dans RIP avec un compte de sauts de 2 (la métrique externe) et une valeur de tics dérivée de la valeur de tics originale de la route RIP (1), plus le délai EIGRP, via le système autonome, converti en tics.

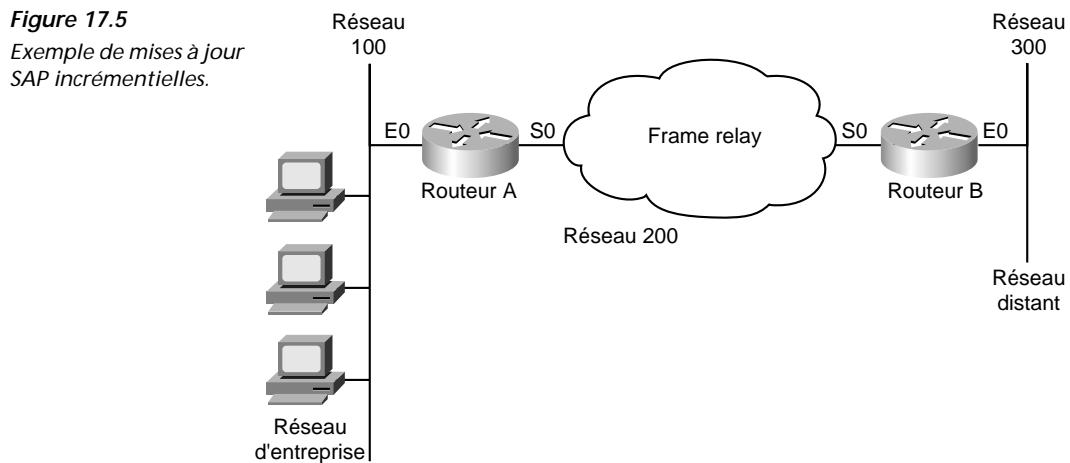
Réduction du trafic SAP

Les routeurs RIP Novell IPX envoient des mises à jour RIP et SAP complètes toutes les 60 secondes, indépendamment du fait qu'il y ait eu ou non des changements ; d'où une consommation très importante de bande passante. Réduisez le trafic des mises à jour SAP pour configurer EIGRP. Il génère alors des mises à jour SAP incrémentielles qui sont transmises uniquement en cas de changement sur le réseau, et transportant uniquement des informations qui ont été modifiées, économisant ainsi la bande passante.

Lorsque vous configurez EIGRP pour des mises à jour SAP incrémentielles, vous disposez de deux solutions :

- **Conserver RIP.** Dans ce cas, seul le transport fiable de EIGRP est utilisé pour l'émission des mises à jour SAP incrémentielles. C'est la configuration choisie sur des connexions sensibles au niveau d'utilisation de la bande passante.
- **Désactiver RIP.** Dans ce cas, EIGRP remplace RIP comme protocole de routage.

La Figure 17.5 illustre une topologie sensible au niveau d'exploitation de la bande passante, et sur laquelle la configuration des mises à jour SAP incrémentielles est particulièrement utile. Cette topologie consiste en un réseau d'entreprise qui utilise une connexion Frame Relay à 56 Kbit/s pour communiquer avec une agence distante. Le réseau d'entreprise supporte plusieurs serveurs Novell, annonçant chacun de nombreux services. Selon le nombre de serveurs et de services annoncés, une grande partie de la bande passante disponible pourrait facilement être consommée par les mises à jour SAP.



Le routeur A est configuré de la manière suivante :

```
ipx routing
!
interface ethernet 0
ipx network 100
!
interface serial 0
encapsulation frame-relay
!
interface serial 0.1 point-to-point
ipx network 200
ipx sap-incremental eigrp 90 rsup-only
frame-relay interface-dlci 101
!
ipx router eigrp 90
network 200
```

La commande de configuration globale **ipx routing** active le routage IPX sur le routeur.

La commande de configuration d'interface **ipx network** active le routage IPX sur l'interface Ethernet 0 pour le réseau 100.

Pour l'interface série 0, la commande de configuration d'interface **encapsulation frame-relay** établit l'encapsulation Frame Relay au moyen de la méthode d'encapsulation Cisco, qui consiste en un en-tête de 4 octets, avec 2 octets pour identifier le DLCI et 2 octets pour identifier le type de paquet.

La commande de configuration globale **interface serial** établit une sous-interface point-à-point (0.1). Les sous-interfaces représentent des interfaces logiques associées à une interface physique. L'emploi de sous-interfaces permet au routeur A de recevoir plusieurs connexions simultanées sur une seule interface Frame Relay.

La commande de configuration d'interface **ipx network** active le routage IPX sur la sous-interface série 0.1 pour le réseau 200.

La commande de configuration d'interface **ipx spa-incremental** active la fonction de mises à jour SAP incrémentielles. Le mot clé **eigrp** active EIGRP et son mécanisme de transport, et dans ce cas spécifie un numéro de système autonome de 90. Comme cette commande utilise le mot clé **rsup-only**, le routeur envoie des mises à jour SAP incrémentielles sur cette liaison.

La commande de configuration d'interface **frame-relay interface-dlci** associe l'identifiant de connexion de liaison de données (DLCI) 101 avec la sous-interface série 0.1.

La commande de configuration globale **ipx router eigrp** démarre un processus EIGRP et lui assigne le numéro de système autonome 90.

La commande de configuration de routeur **ipx network** active EIGRP pour le réseau 200.

Le routeur B est configuré de la façon suivante :

```
ipx routing
!
interface ethernet 0
ipx network 300
!
interface serial 0
encapsulation frame-relay
ipx network 200
ipx sap-incremental eigrp 90 rsup-only
!
ipx router eigrp 90
network 200
```

La commande de configuration globale **ipx routing** active le routage IPX sur le routeur.

La commande de configuration d'interface **ipx network** active le routage IPX sur l'interface Ethernet 0 pour le réseau 300.

Sur l'interface série 0, la commande de configuration d'interface **encapsulation frame-relay** établit l'encapsulation Frame Relay au moyen de la méthode d'encapsulation Cisco, qui consiste en un en-tête de 4 octets, avec 2 octets pour identifier le DLCI et 2 octets pour identifier le type de paquet.

La commande de configuration d'interface **ipx network** active le routage IPX sur la sous-interface série 0.1 pour le réseau 200.

La commande de configuration d'interface **ipx spa-incremental** active la fonction de mises à jour SAP incrémentielles. Le mot clé **eigrp** active EIGRP et son mécanisme de transport, et dans ce cas spécifie un numéro de système autonome de 90. Comme cette commande utilise le mot clé **rsup-only**, le routeur envoie des mises à jour SAP incrémentielles sur cette liaison.

La commande de configuration globale **ipx router eigrp** démarre un processus EIGRP et lui assigne le numéro de système autonome 90.

La commande de configuration de routeur **ipx network** active EIGRP pour le réseau 200.

NOTE

L'absence de la commande **ipx router rip** signifie que RIP IPX est toujours utilisé pour le routage IPX, et l'emploi du mot clé **rsup-only** signifie que le routeur envoie des mises à jour SAP incrémentielles sur la liaison Frame Relay.

Réseau AppleTalk

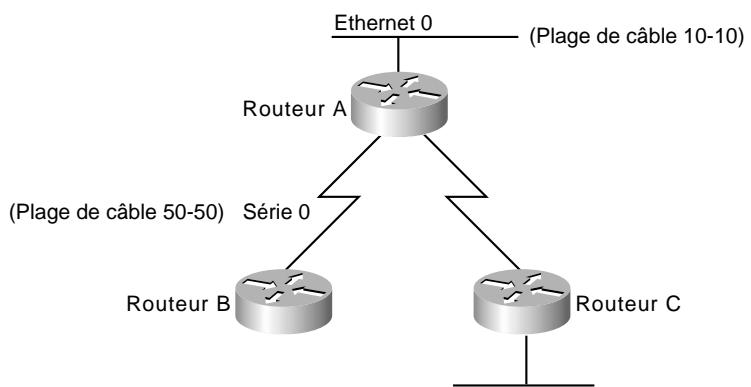
Cette étude de cas illustre l'intégration de EIGRP sur un réseau AppleTalk existant en deux temps : la configuration d'un réseau AppleTalk et l'ajout de EIGRP sur le réseau. Les aspects essentiels à considérer lors de cette intégration sont les suivants :

- sélection de route ;
- gestion de métriques ;
- redistribution de AppleTalk vers EIGRP, et inversement.

Configuration d'un réseau AppleTalk

Les routeurs Cisco supportent AppleTalk Phase 1 et AppleTalk Phase 2. Pour ce dernier, les routeurs Cisco supportent à la fois les réseaux étendus et non étendus. Dans cette étude de cas, les routeurs A, B et C exécutent AppleTalk (voir Figure 17.6).

Figure 17.6
Configuration d'un réseau
AppleTalk.



La configuration pour le routeur A est la suivante :

```

appletalk routing
interface ethernet 0
appletalk cable-range 10-10
appletalk zone casestudy
interface serial 0
appletalk cable-range 50-50
appletalk zone casestudy
  
```

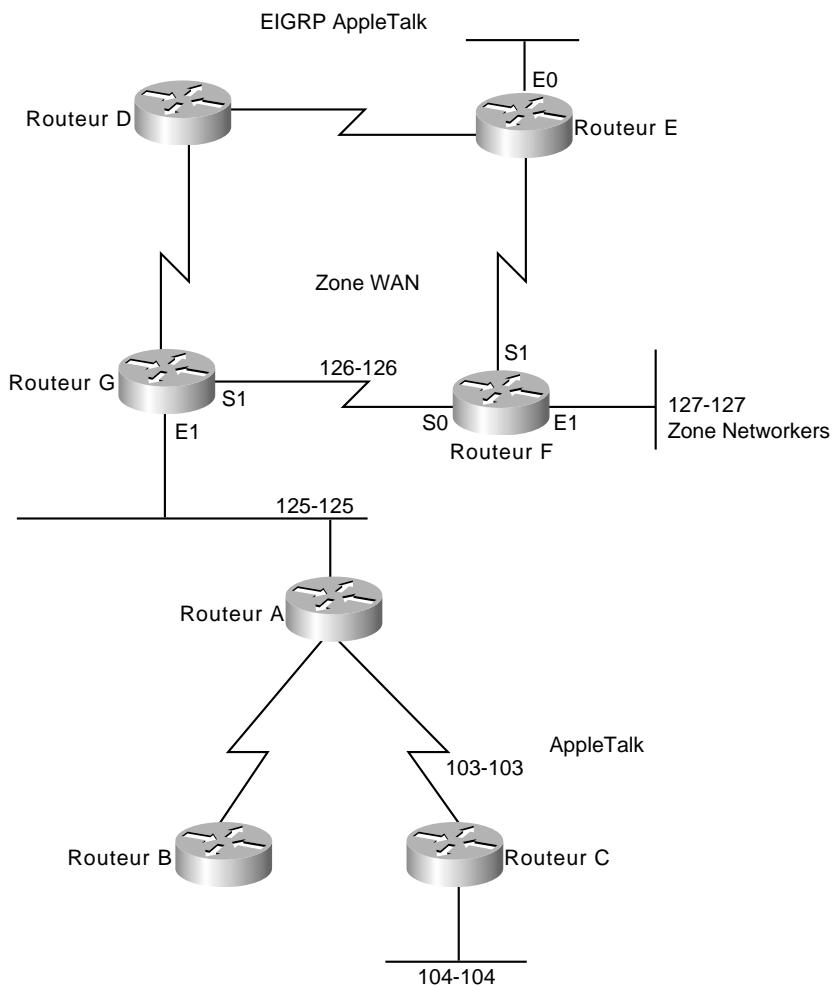
Intégration de EIGRP sur un réseau AppleTalk

Pour intégrer EIGRP sur un réseau AppleTalk, configurez ce protocole sur l'interface qui est connectée aux routeurs. Ne désactivez pas RTMP sur les interfaces connectées vers les hôtes ou routeurs AppleTalk qui ne supportent pas EIGRP. RTMP est activé par défaut lorsque le routage AppleTalk est activé et lorsqu'une plage de câble (*cable range*) AppleTalk est assignée à une interface.

Dans cette étude de cas, les routeurs D et E exécutent EIGRP pour AppleTalk. Les routeurs F et G exécutent à la fois AppleTalk et EIGRP pour AppleTalk. Le routeur G redistribue les routes du réseau AppleTalk vers le réseau EIGRP, et inversement (voir Figure 17.7).

Figure 17.7

Exemple d'ajout de EIGRP sur un réseau AppleTalk.



La configuration pour le routeur G est la suivante :

```
appletalk routing eigrp 1
interface ethernet 1
appletalk cable-range 125-125
appletalk zone Marketing Lab
appletalk protocol eigrp
interface serial 1
appletalk cable-range 126-126
appletalk zone WAN
appletalk protocol eigrp
no appletalk protocol rtmp
```

La configuration pour le routeur F est la suivante :

```
appletalk routing eigrp 2
interface serial 0
appletalk cable-range 126-126
appletalk zone WAN
appletalk protocol eigrp
no appletalk protocol rtmp
```

show appletalk route sur le routeur G montre que le premier ensemble de routes provient d'une mise à jour RTMP, que le deuxième ensemble concerne des routes directement connectées, et que la dernière route est communiquée par EIGRP via l'interface série 1 :

```
R Net 103-103 [1/G] via 125.220, 0 sec, Ethernet1, zone Marketing Lab
R Net 104-104 [1/G] via 125.220, 1 sec, Ethernet1, zone Marketing Lab
R Net 105-105 [1/G] via 125.220, 1 sec, Ethernet1, zone Marketing Lab
R Net 108-108 [1/G] via 125.220, 1 sec, Ethernet1, zone Marketing Lab
C Net 125-125 directly connected, Ethernet1, zone Marketing Lab
C Net 126-126 directly connected, Serial1, zone Wan
E Net 127-127 [1/G] via 126.201, 114 sec, Serial1, zone Networkers
```

show appletalk route sur le routeur F montre que les routes proviennent de EIGRP :

```
E Net 103-103 [2/G] via 126.220, 519 sec, Serial0, zone Marketing Lab
E Net 104-104 [2/G] via 126.220, 520 sec, Serial0, zone Marketing Lab
E Net 105-105 [2/G] via 126.220, 520 sec, Serial0, zone Marketing Lab
E Net 108-108 [2/G] via 126.220, 520 sec, Serial0, zone Marketing Lab
E Net 125-125 [1/G] via 126.220, 520 sec, Serial0, zone Marketing Lab
C Net 126-126 directly connected, Serial0, zone Wan
C Net 127-127 directly connected, Ethernet1, zone Networkers
```

Sélection de route

Les routes EIGRP sont prioritaires par rapport aux routes du protocole RTMP (*Routing Table Maintenance Protocol*). Alors que la métrique AppleTalk pour la détermination de route se base uniquement sur le compte de sauts, EIGRP utilise une combinaison des métriques configurables suivantes : délai, bande passante, fiabilité et charge.

Gestion de métriques

La formule permettant de convertir des métriques RTMP en métriques EIGRP multiplie le compte de sauts par 252 524 800. Il s'agit d'une constante basée sur la bande passante associée à une ligne série à 9,6 Kbit/s et incluant un facteur RTMP. Un saut RTMP distribué dans EIGRP apparaît comme un chemin légèrement moins performant qu'une liaison série à 9,6 Kbit/s en mode EIGRP natif. La formule pour convertir EIGRP vers RTMP ajoute 1 à la valeur de la métrique externe EIGRP.

Redistribution

La redistribution entre AppleTalk et EIGRP est automatique par défaut et implique la conversion de la métrique EIGRP en une métrique de compte de sauts RTMP. En réalité, il n'y a pas de conversion à proprement parler d'une métrique EIGRP composée en une métrique RTMP. En effet, un compte de sauts est transporté dans une métrique EIGRP combinée à mesure que la route EIGRP est propagée sur le réseau. La valeur 1 est ajoutée au compte de sauts, transportée dans les blocs de métrique EIGRP sur le réseau, puis placée dans la métrique de routage RTMP générée.

Il n'y a donc pas de conversion de métrique EIGRP en métrique RTMP, puisque le compte de sauts que RTMP utilise pour métrique est transporté en même temps que la métrique EIGRP sur le réseau. Cette remarque est vraie pour les routes recueillies par EIGRP, mais aussi pour celles qui sont propagées sur le réseau et qui étaient, à l'origine, dérivées d'une route RTMP.

Résumé

Cette étude de cas a illustré l'intégration de EIGRP sur des réseaux Novell et AppleTalk. Pour ajouter EIGRP sur des réseaux IPX, il est capital de configurer RIP et SAP sur les interfaces connectées aux hôtes ou routeurs Novell qui ne supportent pas EIGRP. Lors de l'intégration de EIGRP sur des réseaux AppleTalk, désactivez RTMP sur les interfaces qui sont configurées pour supporter EIGRP.

18

Conception, configuration et dépannage de MPOA

Par Himanshu Desai

Introduction

Ce chapitre traite des méthodes employées pour transférer des protocoles existants vers ATM.

Des protocoles comme IP, IPX, SNA et autres sont depuis longtemps portés sur des médias WAN comme Frame Relay et SMDS. ATM autorise ces protocoles à être portés sur des environnements de campus, ainsi que sur des connexions WAN. Afin d'opter pour la solution qui convient pour votre environnement, les aspects relatifs à la conception doivent être étudiés attentivement. Habituellement, MPOA (*Multiprotocol sur ATM*) avec AAL5 (RFC 1483) est utilisé sur les connexions WAN et LANE sur les épines dorsales ATM de campus.

Ce chapitre couvre ces méthodes séparément en s'appuyant sur des exemples de configuration. Les aspects de conception spécifiques à chacune sont également décrits. Néanmoins, il n'entre pas dans les détails d'implémentation de ces solutions. La section "Considérations relatives à la conception" décrit chaque méthode en mettant en évidence ce qui la distingue des autres, et les sections "Configuration" et "Dépannage" reprennent ces considérations dans un contexte pratique.

Ce chapitre débute par une analyse du RFC 1483 sur les circuits virtuels permanents (PVC, *Permanent Virtual Circuit*) et les circuits virtuels commutés (SVC, *Switched Virtual Circuit*), en exposant leurs avantages. Le RFC 1577 est également décrit, car il simplifie les difficultés de fonctionnement rencontrées avec le RFC 1483. Toutefois, cette section sur le RFC 1577 n'aborde pas en détail le déploiement de protocoles de routage de niveau 3. Par conséquent, pendant la lecture de ce chapitre, étudiez les problèmes liés au déploiement de protocoles de routage avec chacune de ces méthodes.

Le principal objectif de ce chapitre est de mettre en évidence les différences qui existent entre ces solutions de déploiement de protocoles existants sur ATM et de déterminer dans quel contexte chacune d'elle doit être appliquée.

La troisième méthode de déploiement, appelée émulation LAN (*LANE, LAN Emulation*), est principalement exploitée sur les réseaux d'épine dorsale de campus. La section qui lui est consacrée débute par une présentation des aspects de conception LANE. Avant d'implémenter une solution LANE sur une épine dorsale de campus, étudiez attentivement ces considérations afin de garantir l'évolutivité de l'épine dorsale ainsi qu'un dépannage aisé. La compréhension de la structure topologique et la distribution des services LANE vers les différents composants sont des aspects essentiels. Cisco a publié un excellent article sur la conception de réseaux LANE intitulé *Campus ATM LANE Design*.

La dernière section est consacrée à MPOA, qui fonctionne en conjonction avec LANE. Elle décrit brièvement le procédé mis en œuvre par MPOA pour créer un chemin de commutation direct (*cut-through*) sur un domaine LANE, améliorant ainsi les performances de réseaux LANE et réduisant la charge du routage de niveau 3 lors de la traversée d'un nuage LANE vers un autre.

Ce chapitre décrit donc brièvement chaque méthode, incluant des considérations de conception, des exemples de configuration et des conseils pour dépanner les fonctionnalités élémentaires. Reportez-vous aussi à la section "Considérations de conception" pour obtenir une présentation synthétique de chaque méthode, puis examinez les sections "Configuration" et "Dépannage" en rapport avec la méthode que vous aurez choisie, pour obtenir des conseils d'implémentation.

Familiarisez-vous avec les notions fondamentales de la technologie ATM avant de lire ce chapitre, car il n'aborde pas la théorie de base.

MPOA avec AAL5 (RFC 1483)

L'encapsulation multiprotocole sur une configuration AAL5 ATM peut être réalisée de deux manières. La première consiste à utiliser des circuits virtuels permanents, ou PVC, pour configurer des connexions point-à-point sur un nuage ATM. Cette méthode requiert des PVC individuels pour chaque nœud d'un nuage ATM totalement maillé. La seconde méthode fait appel à des circuits virtuels commutés, ou SVC, pour se connecter à chaque nœud d'un nuage ATM totalement maillé.

Cette section couvre ces deux types de circuits virtuels. Comme leur nom l'indique, les PVC sont des circuits virtuels établis de façon permanente. Ils permettent d'éviter la surcharge habituellement associée à l'établissement et à la libération de circuits dans des situations où la présence continue de circuits virtuels est nécessaire.

Les SVC sont des circuits virtuels commutés établis de façon dynamiques à la demande et libérés lorsque la transmission est terminée. Ils sont utilisés dans des environnements où le trafic est sporadique. Dans la terminologie ATM, ils portent le nom de *connexion virtuelle commutée*.

Circuits virtuels permanents (PVC)

Le RFC 1483 décrit deux méthodes permettant de transporter un trafic de réseau sans connexion sur un nuage ATM :

- **AAL5SNAP.** Autorise plusieurs protocoles sur un seul circuit virtuel ATM.
- **AAL5MUX.** Autorise un seul protocole par circuit virtuel ATM.

Les protocoles supportés au moyen de ces méthodes d'encapsulation ATM incluent IP, IPX, Apple-Talk, CLNS, DECnet, VINES et le pontage. Cette section aborde les considérations de conception, de configuration et de dépannage de réseaux ATM mettant en œuvre la spécification du RFC 1483 avec des produits Cisco et AAL5SNAP ou AAL5MUX.

Considérations de conception

Les réseaux s'appuyant sur la spécification du RFC 1483 sont généralement déployés sur une petite échelle. Ce type de réseau convient parfaitement pour des épines dorsales de campus ou de WAN, constituées de 5 à 10 nœuds avec peu de commutateurs intermédiaires. En partant du réseau de trois nœuds de notre exemple (voir Figure 18.1), huit paires VPI/VCI doivent être configurées et trois instructions **map** sont nécessaires (une pour chaque routeur) pour former un nuage ATM totalement maillé. A mesure que le nombre de protocoles et de nœuds d'extrémité augmente, la spécification du RFC 1483 ne s'adapte pas, et il devient par conséquent très difficile de gérer et dépanner le réseau. Par contre, si vous remplacez l'épine dorsale FDDI (ou autre média) existante par une épine dorsale ATM, vous pouvez assurer la transition aisée d'un tel réseau. Un réseau de ce type débutant avec deux nœuds de routeur et un couple de commutateurs intermédiaires peut croître simplement en transférant le nœud d'extrémité de l'ancienne épine dorsale vers l'épine dorsale ATM et en ajoutant ce nœud au nuage nouvellement formé au moyen de l'instruction **map**. Bien que ce procédé assure une transition en douceur, l'épine dorsale requiert une maintenance considérable.

NOTE

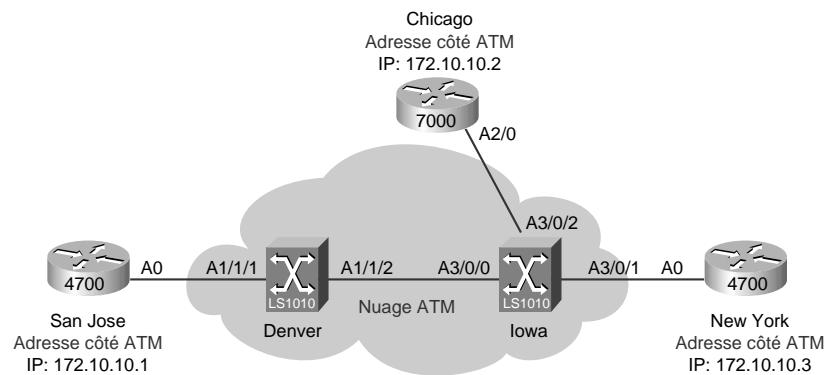
Un VPI (*Virtual Path Identifier*) est un identifiant de chemin virtuel. Il s'agit en fait d'un champ de 8 bits inclus dans l'en-tête d'une cellule ATM. Cet identifiant, associé à celui de canal virtuel (VCI, *Virtual Channel Identifier*), qui est un champ de 16 bits également inclus dans l'en-tête d'une cellule ATM, est utilisé pour identifier la prochaine destination d'une cellule à mesure qu'elle traverse une série de commutateurs ATM. Ces derniers utilisent les champs VPI/VCI pour identifier le prochain VCL par lequel une cellule doit transiter pour atteindre sa destination.

Le RFC 1483 définit un concept simple, facile à configurer et nécessitant une faible surcharge de protocole. Il représente également une solution fiable et reconnue. Toutefois, comme il n'est pas évolutif, il ne s'adapte pas sur de grands réseaux. De plus, il requiert une configuration manuelle importante et ne supporte pas la technologie ATM sur l'ordinateur de bureau.

Topologie ATM avec PVC

La Figure 18.1 illustre un exemple de topologie ATM. Le nuage ATM dans cette topologie pourrait tout aussi bien être constitué de plusieurs commutateurs ATM placés au même endroit que les routeurs dans un environnement LAN, ou de plusieurs commutateurs sur un nuage d'opérateur.

Figure 18.1
Topologie d'un réseau
RFC 1483 avec PVC.



Configuration de PVC

La configuration de PVC requiert la définition manuelle de correspondances vers chaque noeud d'extrêmeur sur tous les commutateurs. Bien que la configuration de ces circuits puisse s'avérer laborieuse et difficile sur de plus grandes topologies, elle est généralement plus simple sur des topologies plus petites.

Celle présentée ici comprend trois routeurs configurés pour ATM, à savoir San Jose, Chicago et New York. Ils sont interconnectés physiquement par l'intermédiaire de deux commutateurs ATM, Denver et Iowa. Imaginez que vous souhaitez implémenter un nuage ATM totalement maillé entre les trois routeurs.

Deux PVC ATM sont configurés sur le routeur San Jose, un pour la connectivité vers Chicago et l'autre pour New York.

L'instruction **atm pvc 1 0 40 aal5snap** permet de configurer le PVC, où 1 est la valeur d'un descripteur de circuit virtuel (VCD, *Virtual Circuit Descriptor*), 0 celle d'un identifiant VPI, et 40 celle d'un identifiant VCI. Les valeurs valides pouvant être utilisées pour configurer des PVC sur des équipements Cisco vont de 0 à 7 pour les VPI, et de 32 à 1023 pour les VCI. Le Forum ATM réserve les valeurs VCI de 0 à 31.

L'instruction **map-group 1483pvc** permet d'appliquer la liste **map-list 1483pvc** sur l'interface ATM, qui à son tour associe les adresses IP de routeur distant au VPI ou VCI local en utilisant le descripteur VCD. Les deux autres routeurs sont configurés de la même manière. Voici la configuration du routeur San Jose :

```
interface ATM0
ip address 172.10.10.1 255.255.255.0
atm pvc 1 0 40 aal5snap
atm pvc 2 0 50 aal5snap
map-group 1483pvc
map-list 1483pvc
ip 172.10.10.2 atm-vc 1 broadcast
ip 172.10.10.3 atm-vc 2 broadcast
```

La configuration du routeur Chicago est la suivante :

```
interface ATM2/0
ip address 172.10.10.2 255.255.255.0
map-group 1483pvc
atm pvc 1 0 40 aal5snap
atm pvc 2 0 60 aal5snap
map-list 1483pvc
ip 172.10.10.1 atm-vc 1 broadcast
ip 172.10.10.3 atm-vc 2 broadcast
```

La configuration du routeur New York est la suivante :

```
interface ATM0
ip address 172.10.10.3 255.255.255.0
atm pvc 1 0 60 aal5snap
atm pvc 2 0 50 aal5snap
map-group 1483pvc
map-list 1483pvc
ip 172.10.10.1 atm-vc 2 broadcast
ip 172.10.10.2 atm-vc 1 broadcast
```

La configuration du commutateur Denver inclut une paire VPI/VCI 0/40 entrante sur l'interface 1/1/1 provenant du routeur San Jose et une paire VPI/VCI 1/40 sortante sur l'interface 1/1/2 vers le commutateur Iowa. La configuration présentée ici reflète le point de vue de l'interface 1/1/2. Elle inclut également une autre paire VPI/VCI 0/50 entrante sur l'interface 1/1/1 en provenance du routeur San Jose et une paire VPI/VCI 1/50 en sortie sur l'interface 1/1/2.

La configuration du commutateur LS1010 Denver est la suivante :

```
interface ATM1/1/2
no keepalive
atm pvc 1 40 interface ATM1/1/1 0 40
atm pvc 1 50 interface ATM1/1/1 0 50
interface ATM1/1/1
```

La configuration du commutateur Iowa inclut une paire VPI/VCI 1/40 entrante provenant du commutateur Denver et une paire sortante VPI/VCI 0/40 sur l'interface 3/0/2 vers le routeur Chicago, permettant de créer un PVC de bout en bout entre les routeurs San Jose et Chicago. Le commutateur Iowa possède une autre paire VPI/VCI 1/50 entrante provenant du commutateur Denver avec une paire sortante VPI/VCI 0/50 sur l'interface 3/0/1 vers le routeur New York. Pour finir, une paire VPI/VCI 0/60 provenant du routeur Chicago sur l'interface 3/0/2 est commutée en sortie sur l'interface 3/0/1 avec une paire VPI/VCI 0/60 vers le routeur New York. Un nuage ATM totalement maillé est ainsi formé avec tous les routeurs directement connectés entre eux.

La configuration du commutateur LS1010 Iowa est la suivante :

```
interface ATM3/0/0
no keepalive
interface ATM3/0/1
no keepalive
atm pvc 0 50 interface ATM3/0/0 1 50
interface ATM3/0/2
no keepalive
atm pvc 0 40 interface ATM3/0/0 1 40
atm pvc 0 60 interface ATM3/0/1 0 60
```

Dépannage de PVC

Une planification efficace est la clé d'un déploiement réussi et stable de réseaux issus de la spécification du RFC 1483.

Tout d'abord, créez une table de paires VPI/VCI pour chaque équipement que vous voulez connecter au nuage. Concevez ensuite un modèle de configuration et commencez à configurer les routeurs et commutateurs individuels. Puis exécutez les commandes décrites ci-dessous pour vérifier que la configuration et la conception déployée fonctionnent comme prévu.

Le résultat de la commande suivante indique que deux PVC sont actifs sur l'interface ATM0. Ces deux circuits virtuels ou VC (*Virtual Circuit*) ont une signification locale et indiquent l'existence d'une connexion active vers le commutateur le plus proche. Ces valeurs VC ne se réfèrent pas à une connexion ATM entre deux routeurs. Pour cela, examinez chaque équipement situé entre les deux routeurs d'extrémité et vérifiez l'état de l'interface et la paire VPI/VCI entrante. La paire VPI/VCI sortante du routeur San Jose devrait correspondre à la paire VPI/VCI entrante du commutateur Denver. Si ce n'est pas le cas, le routeur continuera à envoyer des cellules ATM, mais elles seront supprimées par le commutateur considérant qu'elles proviennent d'une paire VPI/VCI inconnue :

```
SanJose#show atm vc
Interface VCD VPI VCI Type AAL/
                                         Encapsulation      Peak     Avg.     Burst   Status
                                         KBPS    KBPS    Cells
ATM0      1    0    40  PVC   AAL5-SNAP      155000  155000  94      Active
ATM0      2    0    50  PVC   AAL5-SNAP      155000  155000  94      Active
```

NOTE

Un VC (circuit virtuel) est un circuit logique établi pour garantir une communication fiable entre deux équipements de réseau. Un VC est défini par une paire VPI/VCI et peut être soit permanent (PVC) soit commuté (SVC).

NOTE

Une VCC (*Virtual Channel Connection*, connexion de canal virtuel) est une connexion logique entre deux équipements de frontières exécutant ATM (qui peuvent être des hôtes, des routeurs ou des commutateurs ATM). Les VCC s'appuient sur de nombreux VC pour assurer la connexion.

La commande suivante affiche les correspondances d'adresses IP de couche 3 avec des adresses VC ATM, et indique également que la diffusion broadcast est activée en sortie sur les VC :

```
SanJose#show atm map
Map list 1483pvc : PERMANENT
ip 172.10.10.2 maps to VC 1, broadcast
ip 172.10.10.3 maps to VC 2 , broadcast
```

Sur le commutateur Denver, on peut voir que l'état de l'interface est actif :

```
Denver#show atm statistics
NUMBER OF INSTALLED CONNECTIONS: (P2P=Point to Point,
P2MP=Point to MultiPoint)
Type    PVCs    SoftPVCs    SVCs    PVPs    SoftPVPs    SVPs    Total
P2P      11      0          0      0          0          0      11
P2MP     0        0          0      0          0          0      0
```

```
TOTAL INSTALLED CONNECTIONS = 11
PER-INTERFACE STATUS SUMMARY AT 10:11:00 UTC Fri Jan 16 1998:
Interface IF Status Admin Auto-Cfg ILMI Addr SSCOP Hello
Name Status Reg State State State
ATM1/0/0 DOWN down waiting n/a Idle n/a
ATM1/0/1 DOWN down waiting n/a Idle n/a
ATM1/0/2 DOWN down waiting n/a Idle n/a
ATM1/0/3 DOWN down waiting n/a Idle n/a
ATM1/1/0 UP up waiting WaitDevType Idle n/a
ATM1/1/1 UP up done UpAndNormal Idle n/a
ATM1/1/2 UP up done UpAndNormal Active 2way_in
ATM1/1/3 DOWN down waiting n/a Idle n/a
ATM2/0/0 UP up n/a UpAndNormal Idle n/a
ATM3/0/0 DOWN down waiting n/a Idle n/a
ATM3/0/1 DOWN down waiting n/a Idle n/a
```

La commande suivante indique que la paire VPI/VCI 0/40 entrante provenant du routeur San Jose sur l'interface ATM 1/1/1 est commutée en sortie sur l'interface ATM 1/1/2 vers le commutateur Iowa :

```
Denver#show atm vc int atm 1/1/1
Interface VPI VCI Type X-Interface X-VPI X-VCI Status
ATM1/1/1 0 5 PVC ATM2/0/0 0 47 UP
ATM1/1/1 0 16 PVC ATM2/0/0 0 48 UP
ATM1/1/1 0 18 PVC ATM2/0/0 0 49 UP
ATM1/1/1 0 40 PVC ATM1/1/2 1 40 UP
ATM1/1/1 0 50 PVC ATM1/1/2 1 50 UP
```

La commande suivante indique que la paire VPI/VCI 1/40 entrante provenant du commutateur Denver sur l'interface ATM 3/0/0 est commutée en sortie sur l'interface ATM 3/0/0 vers le routeur Chicago :

```
Iowa#show atm vc int atm 3/0/0
Interface VPI VCI Type X-Interface X-VPI X-VCI Status
ATM3/0/0 0 5 PVC ATM2/0/0 0 32 UP
ATM3/0/0 0 16 PVC ATM2/0/0 0 33 UP
ATM3/0/0 0 18 PVC ATM2/0/0 0 34 UP
ATM3/0/0 1 40 PVC ATM3/0/2 0 40 UP
ATM3/0/0 1 50 PVC ATM3/0/1 0 50 UP
```

Après avoir contrôlé les paires VPI/VCI et les instructions de correspondance pour chaque équipement, vous devriez pouvoir effectuer un ping des routeurs Chicago et New York à partir du routeur San Jose :

```
SanJose#ping 172.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.10.10.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

SanJose#ping 172.10.10.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.10.10.3, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

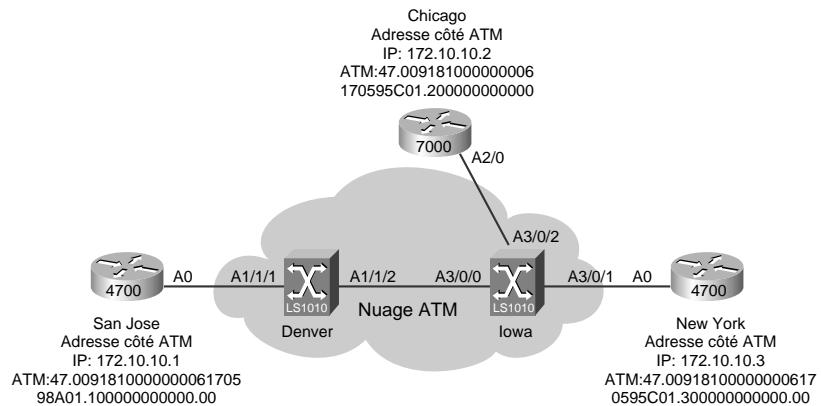
Circuits virtuels commutés (SVC)

Cette section traite de l'utilisation de circuits SVC dans le cadre de la spécification du RFC 1483. Elle décrit la configuration de SVC sur des routeurs et commutateurs, ainsi que certaines techniques de dépannage.

Topologie ATM avec SVC

La Figure 18.2 présente la topologie utilisée pour notre exemple.

Figure 18.2
Topologie d'un réseau
RFC 1483 avec SVC.



Configuration de SVC

La configuration de l'encapsulation multiprotocole sur AAL5 ATM (RFC 1483) avec SVC est semi-dynamique. Elle requiert toujours la définition manuelle de correspondances entre toutes les adresses de nœuds NSAP ATM et les adresses de protocole, mais n'implique aucune définition de correspondances au niveau des commutateurs ATM qui interconnectent les routeurs. Cette configuration est assurée dynamiquement par le protocole PNNI.

NOTE

NSAP (*Network Service Access Point*, point d'accès au service de réseau) est une adresse de réseau, comme spécifié par l'ISO. Un service de réseau OSI est accessible au niveau de ce point d'accès pour une entité de couche transport (couche 4).

PNNI possède deux définitions :

1. Private Network to Network Interface. Il s'agit d'une spécification du Forum ATM pour la distribution d'informations topologiques entre des commutateurs et des clusters de commutateurs. Ces informations sont utilisées pour calculer des chemins à travers le réseau. La spécification s'appuie sur des techniques connues de routage par état de lien et inclut un mécanisme pour la configuration automatique de réseaux sur lesquels la structure d'adresse reflète la topologie.
2. Private Network to Node Interface. Il s'agit d'une spécification du Forum ATM pour une signification visant à établir des connexions point-à-point et point-multipoint sur un réseau ATM. Le protocole s'appuie sur la spécification UNI du Forum ATM et sur des mécanismes additionnels de routage par la source, de renvoi d'appels vers la source (crankback) et de routage alternatif de demandes de connexion.

Dans la topologie de la Figure 18.2, trois routeurs sont configurés pour ATM, à savoir San Jose, Chicago et New York. Ils sont interconnectés physiquement par l'intermédiaire de deux commutateurs ATM, Denver et Iowa. A nouveau, imaginez que vous souhaitez implémenter un nuage ATM totalement maillé entre les trois routeurs.

L'instruction **atm pvc 10 0 5 qsaal** permet de configurer un PVC, fournissant un canal pour l'envoi des messages de signalisation demandant l'établissement de circuits SVC. Les valeurs définies pour les identifiants VPI et VCI doivent correspondre à celles du commutateur local. Les valeurs VPI et VCI standard sont respectivement 0 et 5. Cette configuration utilise un type spécial d'encapsulation de la couche d'adaptation ATM appelé *qsaal*.

L'instruction **atm pvc 20 0 16 ilmi** permet de configurer un PVC, fournissant un canal pour l'envoi de messages ILMI (*Interim Local Management Interface*) vers le commutateur ATM. Pour ILMI, les valeurs VPI et VCI standard sont respectivement 0 et 16. ILMI assure de nombreuses fonctions. Ici, il permet d'enregistrer le préfixe de l'adresse d'interface ATM. Pour cela, il envoie au commutateur une interception lors du redémarrage de l'interface ATM, lui demandant d'enregistrer son préfixe de 13 octets auprès du routeur. Ce préfixe est ensuite utilisé pour constituer une adresse d'interface ATM de 20 octets.

NOTE

ILMI est une spécification développée par le Forum ATM pour intégrer des fonctionnalités de gestion de réseau dans UNI ATM.

L'instruction **atm esi-address 100000000000.00** configure les sept derniers octets de l'adresse d'interface ATM. A l'aide du préfixe de 13 octets appris via ILMI et de l'adresse de 7 octets provenant de l'identifiant ESI (*End System Identifier*), le routeur forme une adresse d'interface ATM de 20 octets. Cette adresse devrait être unique pour chaque équipement sur le nuage ATM. L'identifiant ESI devrait être configuré de façon à permettre la création d'une adresse NSAP unique.

NOTE

ESI est un identifiant de système terminal qui permet de distinguer de nombreux nœuds d'un même niveau lorsque le groupe d'homologues de plus bas niveau est partitionné.

L'instruction **map-group 1483svc** applique la liste **map-list 1483svc** sur l'interface ATM, qui à son tour associe les adresses IP de routeur distant avec leurs adresses NSAP respectives pour les demandes de connexion. Vous pouvez obtenir les adresses NSAP de routeur distant en exécutant la commande **show interface ATM x/x**. L'instruction **map** associe l'adresse IP du routeur Chicago à l'adresse NSAP.

La configuration du routeur San Jose est la suivante :

```
interface ATM0
ip address 172.10.10.1 255.255.255.0
atm esi-address 100000000000.00
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
```

```

map-group 1483svc
map-list 1483svc
ip 172.10.10.2 atm-nsap
    47.009181000000006170595C01.200000000000.00 broadcast
ip 172.10.10.3 atm-nsap
    47.009181000000006170595C01.300000000000.00 broadcast

```

Les deux autres routeurs sont configurés de la même manière avec le protocole approprié pour les adresses NSAP ATM. La configuration du routeur Chicago est la suivante :

```

interface ATM2/0
ip address 172.10.10.2 255.255.255.0
map-group 1483svc
atm esi-address 200000000000.00
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
map-list 1483svc
ip 172.10.10.1 atm-nsap
    47.009181000000006170598A01.100000000000.00 broadcast
ip 172.10.10.3 atm-nsap
    47.009181000000006170595C01.300000000000.00 broadcast

```

La configuration du routeur New York est la suivante :

```

interface ATM0
ip address 172.10.10.3 255.255.255.0
atm esi-address 300000000000.00
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
map-group 1483svc
map-list 1483svc
ip 172.10.10.1 atm-nsap
    47.009181000000006170598A01.100000000000.00 broadcast
ip 172.10.10.2 atm-nsap
    47.009181000000006170595C01.200000000000.00 broadcast

```

L'instruction **atm address 47.00918100.0000.0061.7059.8a01.0061.7059.8a01.00** représente l'adresse ATM du commutateur Denver. Elle est générée automatiquement, bien que les commutateurs LS1010 acceptent les adresses définies par l'utilisateur. Cisco utilise le mécanisme suivant pour générer des adresses ATM uniques pour les commutateurs ATM :

Identifiant AFI	Code ICD CISCO	Assignée par CISCO	Champ ESI	Octet de sélection
47	00 91	81 00 00 00	Adresse MAC	00
3 octets	4 octets	6 octets	1 octet	

L'instruction **atm router pnni** active PNNI sur toutes les interfaces NNI (*Network-to-Network Interface*) après que ILMI ait déterminé le type d'interface. L'instruction **node 1 level 56 lowest** configure le commutateur pour un nœud PNNI avec un indice de nœud de 1 au plus bas niveau de 56.

NOTE

NNI est un standard du Forum ATM qui définit l'interface entre deux commutateurs ATM situés tous les deux sur un réseau privé ou sur un réseau public. L'interface entre un commutateur privé et un commutateur public est définie par le standard UNI.

L'interface ATM du routeur San Jose est directement connectée à l'interface ATM 1/1/1 du commutateur Denver. Comme le révèle la configuration de ce dernier, aucun paramètre n'est défini pour l'interface ATM 1/1/1, ni pour l'interface ATM 1/1/2 en direction du commutateur Iowa. La liaison entre le routeur San Jose et l'interface 1/1/1 du commutateur Denver ATM est appelée UNI (*User-Network Interface*), et celle entre l'interface ATM 1/1/2 du commutateur Denver et l'interface ATM 3/0/0 du commutateur Iowa est appelée NNI. PNNI est exécuté sur les liaisons NNI.

NOTE

UNI est une spécification du Forum ATM qui définit un standard d'interopérabilité pour l'interface entre des équipements ATM (routeur ou commutateur ATM) situés sur un réseau privé et les commutateurs ATM situés sur un réseau d'opérateur public.

La configuration du commutateur Denver est la suivante :

```
atm address47.0091.8100.0000.0061.7059.8a01.0061.7059.8a01.00
atm router pnni
node 1 level 56 lowest
redistribute atm-static
interface ATM1/1/1
no keepalive
interface ATM1/1/2
no keepalive
```

La configuration du commutateur Iowa est semblable à celle du commutateur Denver :

```
atm address
    47.0091.8100.0000.0061.7059.5c01.0061.7059.5c01.00
atm router pnni
node 1 level 56 lowest
redistribute atm-static
interface ATM3/0/0
no keepalive
interface ATM3/0/1
no keepalive
interface ATM3/0/2
no keepalive
```

Dépannage de SVC

La configuration de circuits SVC requiert l'association de l'adresse de protocole avec l'adresse NSAP de routeur distant. Les routeurs forment cette adresse NSAP en combinant le préfixe obtenu via ILMI de la part du commutateur ATM et l'adresse ESI prédéfinie, créant ainsi une adresse NSAP ATM complète de 20 octets pour l'interface ATM du routeur. Par conséquent, assurez-vous que ILMI fonctionne correctement en vous aidant des mesures présentées ici.

Le résultat de la commande suivante indique que le routeur San Jose à reçu le préfixe 47.009181000000006170598A01 de la part du commutateur ATM. Il peut alors constituer l'adresse NSAP de l'interface ATM en ajoutant à ce préfixe l'adresse ESI. Il s'enregistre ensuite dans la table du commutateur pour permettre à PNNI de propager ces informations. Il signale également à l'interface homologue s'il s'agit d'un équipement Cisco :

```
SanJose#show atm ilmi
Interface      ATM0      ILMI VCC:      (0, 16)
ILMI Keepalive:          Disabled
Address Registration:    Enabled
Addr Reg State:         UpAndNormal
Peer IP Addr:           0.0.0.0      Peer IF Name:      ATM1/1/1
Prefix(s):
47.009181000000006170598A01
Addresses Registered:
Local Table :
47.009181000000006170598A01.100000000000.00
Remote Table :
47.009181000000006170598A01.100000000000.00
```

Dans le résultat de la commande suivante, on constate que ILMI fonctionne correctement entre le routeur et le commutateur puisqu'une adresse NSAP a été associée à l'interface ATM. ILMI échange aussi des informations sur la version UNI utilisée et sur la position du routeur, à savoir s'il est situé du côté utilisateur ou du côté réseau. Dans cet exemple, le routeur exécute UNI Version 3 et se trouve du côté utilisateur :

```
SanJose#show int atm 0
ATM0 is up, line protocol is up
Hardware is ATMizer BX-50
Internet address is 172.10.10.1/24
MTU 4470 bytes, sub MTU 4470, BW 156250 Kbit, DLY 100 usec,
  rely 210/255, load 1/255
NSAP address: 47.009181000000006170598A01.100000000000.00
Encapsulation ATM, loopback not set, keepalive set (10 sec)
Encapsulation(s): AAL5 AAL3/4, PVC mode
1024 maximum active VCs, 1024 VCs per VP, 4 current VCCs
VC idle disconnect time: 300 seconds
Signalling vc = 10, vpi = 0, vci = 5
UNI Version = 3.0, Link Side = user
Last input 00:00:20, output 00:00:01, output hang never
Last clearing of "show interface" counters never
```

La commande suivante affiche l'échange de messages ILMI entre le routeur et le commutateur. ILMI utilise des messages SNMP standards. Le résultat inclut l'adresse NSAP transmise par le commutateur. Elle est ensuite enregistrée par le routeur dans sa table locale puis transmise pour enregistrement dans la table du commutateur homologue. Certains paramètres, comme la version UNI et le nom de l'interface homologue, sont également échangés :

```
SanJose#debug atm ilmi
ILMI Transition : Intf := 1 From Restarting To AwaitRestartAck
  <ilmi_initiate_addrreg>
ILMI: REQ_PROCESSING Reqtype = GETNEXT Reqid = 12
  Requestor = ILMI, Transid = 1 (ATM0)
ILMI: Trap Received (ATM0)
ILMI Transition : Intf := 1 From AwaitRestartAck To UpAndNormal
  <ilmi_snmp_callback>
ILMI: REQ_PROCESSING Reqtype = GET Reqid = 13 Requestor =
```

```
ILMI, Transid = 1 (ATM0)
ILMI: REQ_PROCESSING Reqtype = GET Reqid = 14 Requestor =
    ILMI, Transid = 1 (ATM0)
ILMI: REQ_PROCESSING Reqtype = GET Reqid = 15 Requestor =
    ILMI, Transid = 1 (ATM0)
ILMI: VALID_RESP_RCVD Reqtype = GET Reqid = 13 Requestor =
    ILMI, Transid = 1 (ATM0)
ILMI: VALID_RESP_RCVD Reqtype = GET Reqid = 14 Requestor =
    ILMI, Transid = 1 (ATM0)
ILMI: VALID_RESP_RCVD Reqtype = GET Reqid = 15 Requestor =
    ILMI, Transid = 1 (ATM0)
ILMI: Peer UNI Version on 1 = 3
ILMI: TERMINATE Reqtype = GET Reqid = 13 Requestor = ILMI,
    Transid = 1 (ATM0)
ILMI: TERMINATE Reqtype = GET Reqid = 14 Requestor = ILMI,
    Transid = 1 (ATM0)
ILMI: Peer IfName on 1 = ATM1/1/1
ILMI: TERMINATE Reqtype = GET Reqid = 15 Requestor = ILMI,
    Transid = 1 (ATM0)
ILMI: REQ_TIMEOUT Reqtype = GETNEXT Reqid = 12 Requestor =
    ILMI, Transid = 1 (ATM0) ILMI Retry count (before decrement) =
3
ILMI: REQ_PROCESSING Reqtype = GETNEXT Reqid = 12
    Requestor = ILMI, Transid = 1 (ATM0)
ILMI: ERROR_RESP_RCVD (No Such Name) Reqtype = GETNEXT
    Reqid = 12 Requestor = ILMI,
    Transid = 1 (ATM0)
ILMI: TERMINATE Reqtype = GETNEXT Reqid = 12 Requestor =
    ILMI, Transid = 1 (ATM0)
ILMI: No request associated with Expired Timer Reqid = 13
ILMI: No request associated with Expired Timer Reqid = 14
ILMI: No request associated with Expired Timer Reqid = 15
ILMI: Trap sent. Waiting for Prefix ATM0
ILMI: No request associated with Expired Timer Reqid = 12
ILMI: Prefix will be Added (If currently not registered):
470918100006170598A1
ILMI: Notifying Address Addition 470918100006170598A1 (ATM0)
ILMI: REQRCVD Reqtype = SET Reqid = 0 Requestor = atmSmap,
    Transid = 1621657796 (ATM0)
ILMI: Notifying Address Addition 470918100006170598A1 (ATM0)
ILMI: Notifying Address Addition 470918100006170598A1 (ATM0)
ILMI: REQ_PROCESSING Reqtype = SET Reqid = 16 Requestor =
    atmSmap, Transid = 1621657796
    (ATM0)
ILMI: (Local) Reg. validation attempt for
470918100006170598A110000000
ILMI: Address added to local table.
ILMI: Register request sent to peer
ILMI: VALID_RESP_RCVD Reqtype = SET Reqid = 16 Requestor =
    atmSmap, Transid = 1621657796 (ATM0)
ILMI: Set confirmed. Updating peer address table
ILMI: TERMINATE Reqtype = SET Reqid = 16 Requestor =
    atmSmap, Transid = 1621657796 (ATM0)
ILMI: No request associated with Expired Timer Reqid = 16
```

Le résultat de la commande suivante affiche les messages ILMI côté commutateur. Vous pouvez voir que le commutateur envoie son préfixe à réception de l'interception.

Il valide également l'adresse pour que la station finale puisse être enregistrée dans la table distante du système terminal :

```
Denver#debug atm ilmi ATM 1/1/1
ILMI: Querying peer device type. (ATM1/1/1)
ILMI : (ATM1/1/1) From ilmiIntfDeviceTypeComplete To
      ilmiIntfAwaitPortType <ilmi_initiate_portquery>
ILMI: The Maximum # of VPI Bits (ATM1/1/1) is 3
ILMI: The Maximum # of VCI Bits (ATM1/1/1) is 10
ILMI: Response Received and Matched (ATM1/1/1)
The peer UNI Type on (ATM1/1/1) is 2
The Peer UNI Version on (ATM1/1/1) is 2
ILMI: Assigning default device type (ATM1/1/1)
ILMI: My Device type is set to Node (ATM1/1/1)
ILMI: Auto Port determination enabled
ILMI: For Interface (ATM1/1/1)
ILMI: Port Information Complete :
ILMI: Local Information :Device Type = ilmiDeviceTypeNode Port
      Type = ilmiPrivateUNINetworkSide
ILMI: Peer Information :Device Type = ilmiDeviceTypeUser Port
      Type = ilmiUniTypePrivate
MaxVpiBits = 3 MaxVciBits = 10
ILMI: KeepAlive disabled
ILMI : (ATM1/1/1) From ilmiIntfAwaitPortType To
      ilmiIntfPortTypeComplete <ilmi_find_peerPort>
      Restarting Interface (ATM1/1/1)
ILMI : (ATM1/1/1) From ilmiIntfPortTypeComplete To
      AwaitRestartAck <ilmi_process_intfRestart>
ILMI: Response Received and Matched (ATM1/1/1)
ILMI: Errorred response <No Such Name> Intf (ATM1/1/1) Function
      Type = ilmiAddressTableCheck
ILMI : (ATM1/1/1) From AwaitRestartAck To UpAndNormal
      <ilmi_process_response>
ILMI: Response Received and Matched (ATM1/1/1)
ILMI: The Neighbor's IfName on Intf (ATM1/1/1) is ATM0
ILMI: The Neighbor's IP on Intf (ATM1/1/1) is 2886339073
ILMI: Trap Received (ATM1/1/1)
ILMI: Sending Per-Switch prefix
ILMI: Registering prefix with end-system
    47.0091.8100.0000.0061.7059.8a01
ILMI: Response Received and Matched (ATM1/1/1)
ILMI: Validating address
    47.0091.8100.0000.0061.7059.8a01.1000.0000.0000.00
ILMI: Address considered validated (ATM1/1/1)
ILMI: Address added :
    47.0091.8100.0000.0061.7059.8a01.1000.0000.0000.00
    (ATM1/1/1)
ILMI: Sending Per-Switch prefix
ILMI: Registering prefix with end-system
    47.0091.8100.0000.0061.7059.8a01
ILMI: Response Received and Matched (ATM1/1/1)
```

Le résultat de la commande **debug** suivante affiche les événements de signalisation qui se produisent sur le routeur San Jose. Si le VC vers le routeur distant n'est pas présent et si vous tentez de vous y connecter au moyen d'un ping, il établit l'appel en utilisant le protocole de signalisation et, une fois connecté, il commence à envoyer des paquets de données.

Ce processus est très rapide, mais dépend du nombre de demandes d'appel que cet équipement doit gérer à ce moment et du nombre de commutateurs ATM sur le chemin :

```
SanJose#debug atm sig-events
ATMAPI: SETUP
ATMSIG: Called len 20
ATMSIG: Calling len 20
ATMSIG(0/-1 0,0 - 0031/00): (vcnum:0) build Setup msg, Null(U0)
    state
ATMSIG(0/-1 0,0 - 0031/00): (vcnum:0) API - from sig-client
    ATM_OWNER_SMAP
ATMSIG(0/-1 0,0 - 0031/00): (vcnum:0) Input event : Req Setup in
    Null(U0)
ATMSIG(0/-1 0,0 - 0031/00): (vcnum:0) Output Setup
    msg(XferAndTx), Null(U0) state
ATMSIG: Output XferSetup
ATMSIG: Called Party Addr:
    47.009181000000006170595C01.200000000000.00
ATMSIG: Calling Party Addr:
    47.009181000000006170598A01.100000000000.00
ATMSIG(0/-1 0,0 - 0031/00): (vcnum:0) Null(U0) -> Call Initiated(U1)
ATMSIG(0/-1 0,0 - 0031/00): (vcnum:0) Input event : Rcvd Call
    Proceeding in Call Initiated(U1)
ATMSIG(0/-1 0,153 - 0031/00): (vcnum:0) Call Initiated(U1) ->
    Outgoing Call Proceeding(U3)
ATMSIG(0/-1 0,153 - 0031/00): (vcnum:0) Input event : Rcvd
    Connect in Outgoing Call Proceeding(U3)
ATMSIG(0/-1 0,153 - 0031/00): (vcnum:114) API - notifying Connect
    event to client ATM0
ATMSIG(0/-1 0,153 - 0031/00): (vcnum:114) Input event : Req
    Connect Ack in Active(U10)
```

Le résultat de la commande **debug** suivante affiche les événements de signalisation qui se produisent sur le commutateur ATM Denver lorsque le routeur New York tente d'appeler le routeur San Jose. Ce commutateur joue le rôle d'un nœud de transit pour cet appel :

```
Denver#debug atm sig-events
ATMSIG(1/1/2:0 0 - 161222): Input Event : Rcvd Setup in Null(N0)
ATMSIG(1/1/2:0 0 - 161222): Call Control Rcvd Setup in state : Call
    Initiated(N1)
ATMSIG: Called Party Addr:
    47.009181000000006170598A01.100000000000.00
ATMSIG: Calling Party Addr:
    47.009181000000006170595C01.300000000000.00
ATMSIG(1/1/2:0 215 - 161222): Input Event : Req Call Proceeding in
    Call Initiated(N1)
ATMSIG(1/1/2:0 215 - 161222): Output Call Proc msg, Call
    Initiated(N1) state
ATMSIG(1/1/2:0 215 - 161222): Call Initiated(N1) -> Call Proceeding
    sent (NNI) (N3)
ATMSIG: 1/1/1:0 findSvcBlockByCr, Svc not found, callref = 219
ATMSIG: 1/1/1:0 findSvcBlockByCr, Svc not found, callref = 220
ATMSIG(1/1/1:0 36 - 0220): Input Event : Req Setup in Null(N0)
ATMSIG(1/1/1:0 36 - 0220): Output Setup msg(XferAndTx), Null(N0)
    state
ATMSIG(1/1/1:0 36 - 0220): Null(N0) -> Call Present(N6)
ATMSIG: openTransitConnection, svc 0x60685D68, partnerSvc
    0x606863A0
ATMSIG(1/1/2:0 215 - 161222): Null(N0) -> Call Proceeding sent
    (NNI) (N3)
```

```

ATMSIG(1/1/1:0 36 - 0220): Input Event : Rcvd Call Proceeding in
    Call Present(N6)
ATMSIG(1/1/1:0 36 - 0220): Call Present(N6) -> Incoming Call
    Proceeding(N9)
ATMSIG(1/1/1:0 36 - 0220): Input Event : Rcvd Connect in Incoming
    Call Proceeding(N9)
ATMSIG(1/1/1:0 36 - 0220): Call Control Rcvd Connect in state :
    Incoming Call Proceeding(N9)
ATMSIG(1/1/1:0 36 - 0220): Input Event : Req Connect Ack in
    Incoming Call Proceeding(N9)
ATMSIG(1/1/1:0 36 - 0220): Output Connect Ack msg, Incoming Call
    Proceeding(N9) state
ATMSIG(1/1/1:0 36 - 0220): Incoming Call Proceeding(N9) ->
    Active(N10)
ATMSIG(1/1/2:0 215 - 161222): Input Event : Req Connect in Call
    Proceeding sent (NNI) (N3)
ATMSIG(1/1/2:0 215 - 161222): Output Connect msg(XferAndTx),
    Call Proceeding sent (NNI) (N3) state
ATMSIG(1/1/2:0 215 - 161222): Call Proceeding sent (NNI) (N3) ->
    Active(N10)
ATMSIG: connectTransitPath, svc 0x60685D68, partnerSvc
    0x606863A0
ATMSIG(1/1/1:0 36 - 0220): Incoming Call Proceeding(N9) ->
    Active(N10)

```

La commande CLI **show atm map** indique l'association de l'adresse de protocole (IP) avec l'adresse ATM (NSAP). Elle indique également que les connexions vers les routeurs distants sont actives :

```

SanJose#show atm map
Map list 1483svc : PERMANENT
ip 172.10.10.2 maps to NSAP
    47.009181000000006170595C01.200000000000.00, broadcast,
    connection up, VC 2, ATM0
ip 172.10.10.3 maps to NSAP
    47.009181000000006170595C01.300000000000.00, broadcast,
    connection up, VC 1, ATM0

```

La commande CLI **show atm vc** indique les valeurs VCD utilisées par le routeur pour se connecter à un routeur distant (voir commande précédente). Elle indique aussi les valeurs VPI/VCI qui leur sont associées :

```

SanJose#show atm vc
Interface VCD VPI VCI Type AAL/          Peak      Avg      Burst      Status
                           Encapsulation Kbps     Kbps     Cells
ATM0      1   0   32  SVC   AAL5-SNAP    155000  155000  94       ACTIVE
ATM0      2   0   33  SVC   AAL5-SNAP    155000  155000  94       ACTIVE

```

La commande CLI **show atm vcn** fournit le détail des VCD associés au routeur local. Cette commande est utile pour dépanner la connectivité vers le routeur distant, car elle peut indiquer que le routeur local transmet des cellules et qu'il ne reçoit rien en retour :

```

SanJose#show atm vc 1
ATM0: VCD: 1, VPI: 0, VCI: 32, etype:0x0, AAL5 - LLC/SNAP, Flags:
    0x50
PeakRate: 155000, Average Rate: 155000, Burst Cells: 94,
    VCmode: 0x1
OAM DISABLED, InARP DISABLED
InPkts: 42, OutPkts: 46, InBytes: 3796, OutBytes: 4172
InPRoc: 42, OutPRoc: 12, Broadcasts: 34
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0

```

```
OAM F5 cells sent: 0, OAM cells received: 0
Status: ACTIVE , TTL: 4
interface = ATM0, call remotely initiated, call reference = 2
vcnum = 1, vpi = 0, vci = 32, state = Active
aal5snap vc, point-to-point call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = 00:00:00
Remote ATM Nsap address:
47.009181000000006170595C01.300000000000

SanJose#show atm vc 2
ATM0: VCD: 2, VPI: 0, VCI: 33, etype:0x0, AAL5 - LLC/SNAP, Flags:
0x50
PeakRate: 155000, Average Rate: 155000, Burst Cells: 94,
VCmode: 0x1
OAM DISABLED, InARP DISABLED
InPkts: 45, OutPkts: 46, InBytes: 4148, OutBytes: 4220
InPRoc: 45, OutPRoc: 12, Broadcasts: 34
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM F5 cells sent: 0, OAM cells received: 0
Status: ACTIVE , TTL: 4
interface = ATM0, call locally initiated, call reference = 1
vcnum = 2, vpi = 0, vci = 33, state = Active
aal5snap vc, point-to-point call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = 00:00:00
Remote ATM Nsap address:
47.009181000000006170595C01.200000000000
```

Classical IP sur ATM (RFC 1577)

Le RFC 1577 ou "Classical IP et ATMARP sur ATM" définit un mécanisme pour communiquer dynamiquement avec des routeurs configurés pour IP à travers le nuage ATM. Aucune correspondance entre adresse IP et adresse ATM n'est nécessaire pour que des informations puissent circuler d'un routeur à un autre. Pour cela, un mécanisme ARP similaire à ARP Ethernet est mis en œuvre.

Dans la topologie suivante, trois routeurs sont connectés au nuage ATM formé de deux commutateurs ATM. Ces routeurs forment un sous-réseau IP logique ou LIS (*Logical IP Subnetwork*), 172.10.x.x. Classical IP sur ATM leur permet de communiquer dynamiquement avec un minimum de configuration.

Dans l'exemple suivant, considérez le commutateur Denver comme un serveur ARP et les trois routeurs comme des clients. Chaque client se connecte au serveur ARP en utilisant une adresse NSAP ATM de serveur ARP prédefinie et celui-ci obtient l'adresse IP de tous les clients via InARP. Le serveur maintient une table ARP avec des couples adresse IP/adresse NSAP ATM. Si un routeur veut en contacter un autre, il envoie une requête ARP au serveur, lui demandant l'adresse NSAP de l'autre routeur. À réception des informations demandées, il peut communiquer directement avec son homologue à travers le nuage ATM.

Le scénario précédent spécifie un groupe LIS. Vous pouvez disposer d'un autre ensemble de routeurs configurés pour ATM et connecté aux mêmes commutateurs, mais se trouvant dans un groupe LIS différent au niveau de la couche 3. Dans ce cas, ce second LIS est indépendant du premier. Ces deux groupes possèdent chacun leur propre ensemble de serveur ARP et clients correspondants. Si le routeur d'un LIS souhaite dialoguer avec un routeur dans l'autre groupe, il doit

passer par un routeur IP qui est configuré comme membre des deux groupes LIS, c'est-à-dire assurant le routage de niveau 3 même s'il était possible d'ouvrir un VC direct entre les deux sur le nuage ATM.

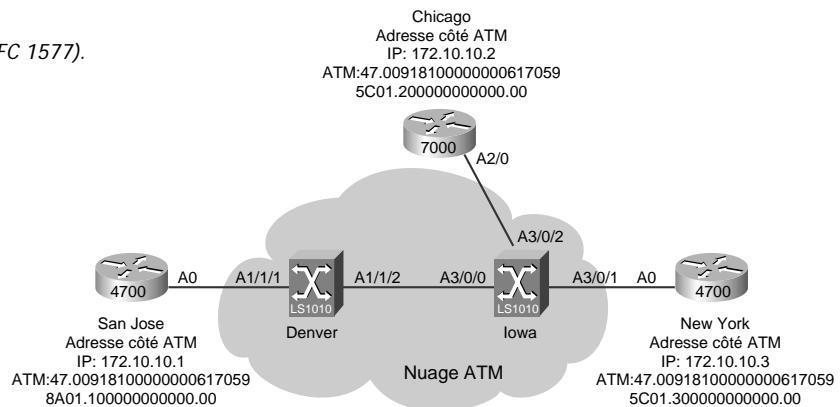
Considérations de conception

La spécification du RFC 1577 est très simple et rapide à implémenter. Cette simplicité provient de la facilité de configuration et de dépannage qu'elle offre. Ce type de réseau est approprié pour dix à quinze nœuds avec un sous-réseau IP logique. Toutefois, il n'est pas capable d'évoluer en raison de problèmes de localisation des voisins au niveau du protocole de routage lorsque des circuits virtuels ne sont pas déjà établis. Généralement, dans un environnement RFC 1577 composé d'équipements multifabricants, la moindre panne (*single point of failure*) peut entraîner un risque d'immobilisation en raison de son serveur ARP centralisé. Cisco supporte donc plusieurs serveurs ARP pour un même LIS, mais il s'agit d'une solution propriétaire.

Topologie

La Figure 18.3 illustre la topologie de l'exemple précédent.

Figure 18.3
Classical IP sur ATM (RFC 1577).



Configuration

Un réseau basé sur la spécification du RFC 1755 requiert la configuration d'un serveur ARP ATM. Des routeurs Cisco dotés d'une interface ATM ou des commutateurs ATM LS1010 peuvent jouer le rôle de serveur ARP ATM pour un tel réseau. Dans l'exemple suivant, le commutateur Denver est un serveur ARP.

La commande **atm arp-server self** active la carte processeur du commutateur Denver pour qu'il agisse comme serveur ARP pour le groupe LIS 172.10.x.x.

La configuration du commutateur Denver est la suivante :

```
interface ATM2/0/0
ip address 172.10.10.4 255.255.255.0
```

```

no keepalive
am esi-address 123456789000.00
atm arp-server self

```

La commande CLI **atm arp-server nsap 47.00918100000006170598A01.123456789000.00** active l'interface ATM du routeur San Jose pour qu'il devienne un client ARP pour le LIS 172.10.x.x, et lui fournit l'adresse NSAP du serveur ARP de ce LIS. Il utilise l'adresse NSAP pour établir une connexion avec le serveur ARP lorsque l'interface ATM a été activée administrativement. La configuration d'autres routeurs du même LIS est semblable :

La configuration du routeur San Jose est la suivante :

```

interface ATM0
ip address 172.10.10.1 255.255.255.0
atm esi-address 100000000000.00
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
atm arp-server nsap
47.00918100000006170598A01.123456789000.00

```

La configuration du routeur Chicago est la suivante :

```

interface ATM2/0
ip address 172.10.10.2 255.255.255.0
atm esi-address 200000000000.00
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
atm arp-server nsap
47.00918100000006170598A01.123456789000.00

```

La configuration du routeur New York est la suivante :

```

interface ATM0
ip address 172.10.10.3 255.255.255.0
atm esi-address 300000000000.00
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
atm arp-server nsap
47.00918100000006170598A01.123456789000.00

```

Dépannage

Classical IP sur ATM nécessite la définition d'une même taille de MTU sur tous les clients ATM et serveurs ARP d'un même LIS. Comprendre l'interaction client-serveur facilite les procédures de dépannage. Les commandes **show** et **debug** donnent les détails de cette interaction.

La commande CLI suivante **show atm map** indique que lorsque l'interface du client est activée, il se connecte au serveur ARP via le VC 159. La commande CLI **debug atm arp** sur le même client révèle qu'il reçoit une requête InARP du serveur ARP (172.10.10.4) pour résoudre l'adresse ATM NSAP en adresse IP et mettre à jour sa table. Le client répond avec son adresse IP et le serveur alimente sa table ARP. Chaque client ainsi activé est enregistré dans la table au moyen du même processus.

```

SanJose#show atm map
Map list ATM0_ATM_ARP : DYNAMIC
arp maps to NSAP
47.00918100000006170598A01.123456789000.00
, connection up, VC 159, ATM0

```

```
SanJose#debug atm arp
ATMARP(ATM0)I: INARP Request VCD#159 from 172.10.10.4
ATMARP(ATM0)O: INARP Response VCD#159 to 172.10.10.4
ATMSM(ATM0): Attaching to VC #159 for type 1 traffic

SanJose#show atm vc
Interface VCD VPI VCI Type AAL/ Peak Avg Burst Status
Encapsulation Kbps Kbps Cells
ATM0 10 0 5 PVC AAL5-SAAL 155000 155000 94 ACTIVE
ATM0 20 0 16 PVC AAL5-ILMI 155000 155000 94 ACTIVE
AMT0 159 0 62 PVC AAL5-SNAP 155000 155000 94 ACTIVE
```

La commande CLI suivante affiche le VC correspondant vers le serveur ATM ARP et indique que l'appel a été initié localement :

```
SanJose#show atm vc 159
ATM0: VCD: 159, VPI: 0, VCI: 62, etype:0x0, AAL5 - LLC/SNAP,
Flags: 0xD0
PeakRate: 155000, Average Rate: 155000, Burst Cells: 94,
VCmode: 0x1
OAM DISABLED, InARP DISABLED
InPkts: 1, OutPkts: 5, InBytes: 52, OutBytes: 376
InPProc: 1, OutPProc: 0, Broadcasts: 4
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
OAM F5 cells sent: 0, OAM cells received: 0
Status: ACTIVE , TTL: 0
interface = ATM0, call locally initiated, call reference = 112
vcnum = 159, vpi = 0, vci = 62, state = Active
aal5snap vc, point-to-point call
Retry count: Current = 0, Max = 10
timer currently inactive, timer value = 00:00:00
Remote ATM Nsap address:
47.00918100000006170598A01.123456789000.00
```

La commande CLI **show atm map** révèle maintenant une entrée avec une correspondance entre l'adresse IP et l'adresse NSAP du serveur ARP :

```
SanJose#show atm map
Map list ATM0_ATM_ARP : DYNAMIC
arp maps to NSAP
 47.00918100000006170598A01.123456789000.00, connection
    up, VC 159, ATM0
  ip 172.10.10.4 maps to NSAP
    47.00918100000006170598A01.123456789000.00, broadcast,
      connection up, VC 159, ATM0
```

La commande CLI **debug atm arp** sur le serveur ARP indique que chaque fois qu'un client devient actif, il établit une connexion ATM avec le serveur ARP au moyen d'une adresse ATM de serveur ARP prédefinie. Le serveur ARP envoie une requête InARP pour obtenir l'adresse IP de chaque client. D'après le texte en gras, vous pouvez constater que le serveur a transmis la requête InARP au client 172.10.10.2, qu'il reçoit une réponse, et met à jour sa table ARP :

```
Denver#debug atm arp
ARPSERVER (ATM2/0/0): tx InARP REQ on vc 254
ATMARP(ATM2/0/0)O: INARP_REQ to VCD#254 for link 7(IP)
ARPSERVER (ATM2/0/0): tx InARP REQ on vc 255
ATMARP(ATM2/0/0)O: INARP_REQ to VCD#255 for link 7(IP)
ATMARP(ATM2/0/0)I: INARP Reply VCD#254 from 172.10.10.2
ARPSERVER (ATM2/0/0): rx InARP REPLY from 172.10.10.2 (vc
254)
```

```

ARP SERVER (ATM2/0/0): New IP address for vcd 254 -- was
0.0.0.0, now 172.10.10.2
ATMARP(ATM2/0/0)I: INARP Reply VCD#255 from 172.10.10.3
ARP SERVER (ATM2/0/0): rx InARP REPLY from 172.10.10.3 (vc
255)
ARP SERVER (ATM2/0/0): New IP address for vcd 255 -- was
0.0.0.0, now 172.10.10.3
ARP SERVER (ATM2/0/0): tx InARP REQ on vc 256
ATMARP(ATM2/0/0)I: INARP_REQ to VCD#256 for link 7(IP)
ARP SERVER (ATM2/0/0): vc 256 wait timer expiry. Retransmitting.
ARP SERVER (ATM2/0/0): tx InARP REQ on vc 256
ATMARP(ATM2/0/0)I: INARP_REQ to VCD#256 for link 7(IP)
ATMARP(ATM2/0/0)I: INARP Reply VCD#256 from 172.10.10.5
ARP SERVER (ATM2/0/0): rx InARP REPLY from 172.10.10.5 (vc
256)
ARP SERVER (ATM2/0/0): New IP address for vcd 256 -- was
0.0.0.0, now 172.10.10.5
ARP SERVER (ATM2/0/0): tx InARP REQ on vc 257
ATMARP(ATM2/0/0)I: INARP_REQ to VCD#257 for link 7(IP)
ARP SERVER (ATM2/0/0): vc 257 wait timer expiry. Retransmitting.
ARP SERVER (ATM2/0/0): tx InARP REQ on vc 257
ATMARP(ATM2/0/0)I: INARP_REQ to VCD#257 for link 7(IP)
ATMARP(ATM2/0/0)I: INARP Reply VCD#257 from 172.10.10.1
ARP SERVER (ATM2/0/0): rx InARP REPLY from 172.10.10.1 (vc 257)
ARP SERVER (ATM2/0/0): New IP address for vcd 257 - was 0.0.0.0, now 172.10.10.1A

```

Jusqu'à présent, vous avez vu comment un client est enregistré dans la table ARP. L'analyse suivante illustre l'interaction entre ces clients enregistrés, et ce qui se produit si un client n'existe pas.

A partir du routeur San Jose, vous effectuez un ping du routeur Chicago (172.10.10.2), mais vous ne connaissez pas son adresse ATM. Le routeur San Jose envoie donc une requête ARP au serveur et reçoit en réponse l'adresse NSAP correspondante :

```

SanJose#ping 172.10.10.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.10.10.2, timeout is 2
seconds:
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/1 ms

SanJose#debug atm arp
ATMARP(ATM0): Sending ARP to 172.10.10.2
ATMARP:(ATM0): ARP reply from 172.10.10.2 ->
    47.009181000000006170595C01.200000000000.00
ATMARP(ATM0): Opening VCC to
    47.009181000000006170595C01.200000000000.00...!!!

```

Le résultat suivant, obtenu à partir du serveur ARP, indique qu'il a reçu la requête ARP de 172.10.10.1 demandant l'adresse NSAP ATM de 172.10.10.2. Il répond en incluant l'adresse appropriée :

```

Denver#debug atm arp
ATMARP:(ATM2/0/0): ARP Request from 172.10.10.1 ->
    47.009181000000006170598A01.100000000000.00
ATMARP(ATM2/0/0): ARP VCD#0 172.10.10.1 replacing NSAP
ARP SERVER (ATM2/0/0): rx ARP REQ from 172.10.10.1 to
    172.10.10.2 (vc 257)
ARP SERVER (ATM2/0/0): tx ARP REPLY from 172.10.10.2 to
    172.10.10.1 (vc 257)
ATMARP:(ATM2/0/0): ARP Request from 172.10.10.2 ->
    47.009181000000006170595C01.200000000000.00
ATMARP(ATM2/0/0): ARP VCD#0 172.10.10.2 replacing NSAP

```

```
ARPSERVER (ATM2/0/0): rx ARP REQ from 172.10.10.2 to
172.10.10.1 (vc 254)
ARPSERVER (ATM2/0/0): tx ARP REPLY from 172.10.10.1 to
172.10.10.2 (vc 254)
```

Voyons maintenant ce qui se produit si vous tentez un ping d'un client non existant dans le LIS :

```
SanJose#ping 172.10.10.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 172.10.10.10, timeout is 2
seconds:
Success rate is 0 percent (0/5)
```

La commande **ping** sur l'adresse 172.10.10.10 d'un client non existant échoue. En supposant que vous ne sachiez pas que le client n'existe pas, vous pourriez penser que le serveur ARP est inopérant. La commande **debug atm arp** indique néanmoins qu'il est actif et qu'il envoie une réponse ARP_NAK signifiant que le client n'existe pas, ou qu'il n'est pas enregistré sur ce serveur :

```
SanJose#debug atm arp
ATMARP(ATM0): Sending ARP to 172.10.10.10
ATMARP(ATM0): ARP_NAK received on VCD#159.
ATMARP(ATM0): Sending ARP to 172.10.10.10
ATMARP(ATM0): ARP_NAK received on VCD#159.
ATMARP(ATM0): Sending ARP to 172.10.10.10
ATMARP(ATM0): ARP_NAK received on VCD#159.
ATMARP(ATM0): Sending ARP to 172.10.10.10
ATMARP(ATM0): ARP_NAK received on VCD#159.
ATMARP(ATM0): Sending ARP to 172.10.10.10
ATMARP(ATM0): ARP_NAK received on VCD#159.
```

La commande CLI **debug atm arp** sur le serveur ARP affiche la réponse du serveur au client demandant la résolution ARP d'une adresse IP non existante en adresse NSAP :

```
Denver#debug atm arp
ATMARP:(ATM2/0/0): ARP Request from 172.10.10.1 ->
47.009181000000006170598A01.100000000000.00
ATMARP(ATM2/0/0): ARP Update from VCD#257 172.10.10.1 MAP
VCD#0
ARPSERVER (ATM2/0/0): rx ARP REQ from 172.10.10.1 to
172.10.10.10 (vc 257)
ARPSERVER (ATM2/0/0): tx ARP NAK to 172.10.10.1 for
172.10.10.10 (vc 257)
ATMARP:(ATM2/0/0): ARP Request from 172.10.10.1 ->
47.009181000000006170598A01.100000000000.00
ATMARP(ATM2/0/0): ARP Update from VCD#257 172.10.10.1 MAP
VCD#0
ARPSERVER (ATM2/0/0): rx ARP REQ from 172.10.10.1 to
172.10.10.10 (vc 257)
ARPSERVER (ATM2/0/0): tx ARP NAK to 172.10.10.1 for
172.10.10.10 (vc 257)
ATMARP:(ATM2/0/0): ARP Request from 172.10.10.1 ->
47.009181000000006170598A01.100000000000.00
ATMARP(ATM2/0/0): ARP Update from VCD#257 172.10.10.1 MAP
VCD#0
ARPSERVER (ATM2/0/0): rx ARP REQ from 172.10.10.1 to
172.10.10.10 (vc 257)
ARPSERVER (ATM2/0/0): tx ARP NAK to 172.10.10.1 for
172.10.10.10 (vc 257)
ATMARP:(ATM2/0/0): ARP Request from 172.10.10.1 ->
47.009181000000006170598A01.100000000000.00
```

La commande CLI **show atm map** montre que le routeur San Jose peut maintenant communiquer directement avec tous les autres routeurs du même LIS en utilisant des circuits SVC. Il n'a donc pas besoin que le serveur lui fournisse l'adresse NSAP du routeur de l'autre côté. Cette table reste effective tant que les deux routeurs continuent d'échanger des paquets/cellules. Dans cette étude de cas, les paquets Hello OSPF sont échangés à intervalles réguliers et maintiennent le circuit virtuel actif.

De plus, il est important de noter que le paquet broadcast ne peut pas initier de circuit virtuel dans le nuage ATM, car ATM lui-même est un média NBMA, c'est-à-dire non broadcast. Un moyen doit donc être mis en œuvre pour permettre au routeur de trouver tous ses voisins dans le nuage ATM ou dans le même LIS. Pour cela, effectuez un ping de chaque routeur du LIS ou bien configurez manuellement ses voisins :

```
SanJose#show atm map
Map list ATM0_ATM_ARP : DYNAMIC
arp maps to NSAP
    47.009181000000006170598A01.123456789000.00, connection
        up, VC 159, ATM0
    ip 172.10.10.1 maps to NSAP
        47.009181000000006170598A01.100000000000.00, broadcast,
            connection up, VC 162, ATM0
    ip 172.10.10.2 maps to NSAP
        47.009181000000006170595C01.200000000000.00, broadcast,
            connection up, VC 160, ATM0
    ip 172.10.10.3 maps to NSAP
        47.009181000000006170595C01.300000000000.00, broadcast,
            connection up, VC 163, ATM0
    ip 172.10.10.4 maps to NSAP
        47.009181000000006170598A01.123456789000.00, broadcast,
            connection up, VC 159, ATM0
```

La commande CLI **show atm arp** affiche la table ARP du serveur avec toutes les entrées relatives aux clients actifs :

```
Denver#show atm arp
Note that a '*' next to an IP address indicates an active call
IP Address ATM2/0/0:      TTL      ATM Address
* 172.10.10.1           19:29    47009181000000006170598a0110000000000000
* 172.10.10.2           12:56    47009181000000006170595c0120000000000000
* 172.10.10.3           19:31    47009181000000006170595c0130000000000000
* 172.10.10.4           9:23     47009181000000006170598a0112345678900000
* 172.10.10.5           16:02    47009181000000006170595c0150000000000000
```

Introduction à LANE

LANE (*LAN Emulation*) est une méthode d'émulation de réseau local (LAN) sur une infrastructure ATM. Les standards pour l'émulation Ethernet 802.3 et Token Ring 802.5 sont définis. Comme la technologie ATM est par nature orientée connexion, il devient difficile de supporter plusieurs protocoles populaires comme IP et IPX qui fonctionnent en mode non connecté. En laissant ATM émuler Ethernet, il devient plus facile de supporter MPOA (*Multiprotocols Over ATM*) et ne pas avoir à créer de nouveaux protocoles. Il est aussi possible de concevoir plusieurs LAN sur la même infrastructure ATM. Ces LAN émulés ou ELAN ne peuvent communiquer directement entre eux au niveau 2 et doivent être routés. Par conséquent, une telle configuration nécessite toujours l'implémentation d'un routeur exécutant plusieurs ELAN.

Considérations de conception

La conception de LANE dans un environnement de campus nécessite une planification et une allocation soigneuse des équipements pour mettre en place des services LANE. Il existe de nombreuses documentations sur ce sujet. Cette section souligne certains des problèmes les plus couramment rencontrés avec l'implémentation de LANE dans un environnement de campus. Finalement, la mise en œuvre des services LANE dépend des modèles de comportement du trafic qui est échangé sur le réseau et de la façon dont les ressources ATM sont allouées pour répondre à cette communication.

L'un des composants les plus utilisés avec LANE est le serveur BUS, car tous les paquets broadcast lui parviennent avant d'être retransmis vers tous les clients LEC sur un ELAN. Les capacités de traitement BUS de la carte LANE du commutateur Cisco Catalyst 5000 avoisinent 120 Kbit/s et celles de la carte AIP de routeur approchent 60 Kbit/s.

NOTE

Le serveur BUS (*Broadcast-and-Unknown Server*) est un serveur multicast utilisé sur les ELAN qui est utilisé pour diffuser par inondation le trafic à destination d'une adresse inconnue et transmettre le trafic multicast et broadcast aux clients appropriés.

Un autre facteur important intervenant dans la conception de réseaux avec LANE est la consommation de circuits virtuels sur les équipements de frontières et dans le nuage ATM lui-même. L'Equation 18.1 illustre cette consommation.

Equation 18.1 : Calcul de la consommation maximale de VC avec LANE

$$\text{Total de circuits virtuels} = E((2N + 2) + (Nx(N-1)/2)) + C$$

Dans cette équation, les valeurs sont les suivantes :

C, nombre total de commutateurs et de routeurs ATM-LAN d'armoire de câblage ;

E, nombre total de ELAN (VLAN) ;

N, nombre typique d'armoires de câblage par ELAN.

Si l'on utilise cette équation, un nuage LANE composé de quatre équipements de frontière et exécutant un seul ELAN nécessite 20 circuits virtuels ou VCC (*Virtual Channel Circuit*). A mesure que le nombre d'ELAN augmente par nuage, les besoins en circuits virtuels croissent aussi. La panne d'un ELAN peut provoquer un engorgement sur l'équipement exécutant les services LANE. Il est donc recommandé de distribuer les services LANE sur différents équipements.

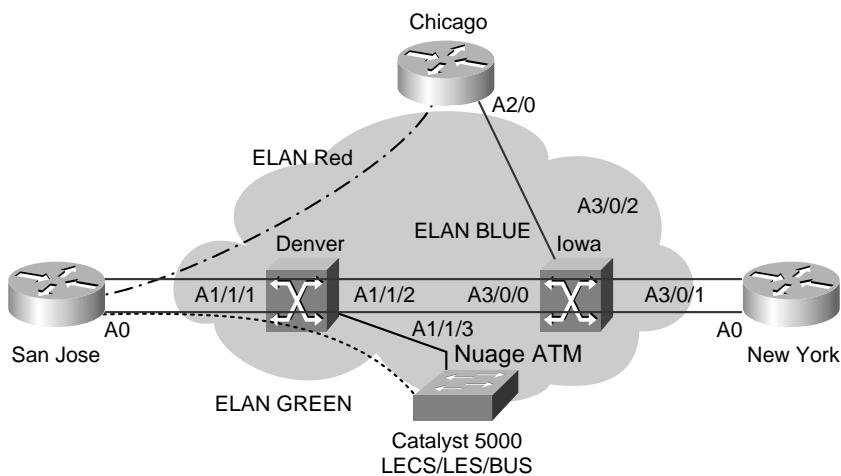
Le dernier facteur à prendre en considération avec l'implémentation de LANE sont les capacités d'établissement d'appels des commutateurs ATM qui forment le nuage ATM. Cette fonction revêt une grande importance, particulièrement dans une situation de panne — par exemple, tous les LEC tentent soudain de se connecter aux services LANE par l'intermédiaire de ces commutateurs. Dans un tel scénario, les commutateurs ATM peuvent faire l'objet de nombreuses requêtes simultanées d'établissement de connexion. S'ils ne sont pas configurés pour gérer correctement la charge, il peut en résulter une escalade de problèmes.

La capacité de gestion des requêtes d'appels d'un LS1010 est d'environ 110 appels par seconde.

Topologie

La Figure 18.4 illustre la topologie pour cet exemple.

Figure 18.4
Emulation LAN.



NOTE

L'émulation LAN est habituellement utilisée dans un environnement de campus. Même si les routeurs portent des noms de ville ils appartiennent au même campus. Ils peuvent être considérés comme des désignations d'immeubles.

Configuration

La configuration de l'émulation LAN nécessite que les trois serveurs LECS/LES/BUS soient tout d'abord configurés avec leurs pleines fonctionnalités. Ces composants LANE peuvent être configurés sur des routeurs ou des commutateurs Catalyst activés pour ATM. La différence entre ces deux types d'équipements réside dans leurs performances. Un commutateur Catalyst offre de meilleures performances qu'un routeur pour assurer ces services.

NOTE

Un LEC (*LAN Emulation Client*, client LANE) est une entité sur un système d'extrémité qui réalise la transmission de données, la résolution d'adresses et d'autres fonctions de contrôle au sein d'un seul ELAN. Un LEC fournit aussi une interface de service LAN standard pour n'importe quelle entité de couche supérieure qui s'interface avec lui. Chaque LEC est identifié par une adresse ATM unique et est associé à une ou plusieurs adresses MAC accessibles par l'intermédiaire de cette adresse ATM.

Un LECS (*LAN Emulation Configuration Server*, serveur de configuration LANE) est une entité qui assigne les clients LANE individuels à des ELAN (ou LAN émulés) donnés en les orientant vers le

LES correspondant à l'ELAN concerné. Il existe logiquement un LECS par domaine administratif et il sert tous les ELAN du domaine.

Un LES (*LAN Emulation Server*, serveur LANE) est une entité qui assure le contrôle d'un ELAN particulier. Il n'y a qu'un LES logique par ELAN et il est identifié par une adresse ATM unique.

La configuration illustrée dans cette section sur un Catalyst 5000 activé pour ATM, implémente les serveurs LECS/LES/BUS.

La commande **lane database ABC** crée une base de données nommée pour le serveur de configuration LANE (LECS). Cette base contient l'adresse ATM d'un serveur LANE (LES) différent ainsi que d'autres informations. Elle contient des données caractéristiques du LANE. Lorsqu'un équipement veut joindre un LANE particulier dans une base de données avec une caractéristique spécifique, le LECS examine la requête, et si les données conviennent, il répond avec l'adresse ATM du LES pour poursuivre le processus de connexion du LEC.

La commande **name red server-atm-address 47.00918100000006170598A01.00602FBCC511.01** relie le LANE *red* avec l'adresse ATM appropriée du serveur LANE. Il en va de même pour les nuages LANE *blue* et *green*. Reportez-vous au manuel de configuration concernant l'assignation d'adresses ATM aux divers services LANE sur les équipements Cisco.

La commande **lane config database ABC** relie le nom de la base de données du serveur de configuration LANE à l'interface principale spécifiée et active le serveur.

La commande **lane auto-config-atm-address** indique que l'adresse ATM du serveur de configuration est calculée par la fonction Cisco d'attribution automatique d'adresses aux divers services LANE.

La commande **lane server-bus ethernet red** active un serveur LANE et un serveur BUS pour le premier LAN émulé. De la même façon pour les LAN émulés *green* et *blue* sur des sous-interfaces différentes, cette commande crée un nuage LANE séparé avec les sous-réseaux IP distincts.

La commande **lane client ethernet 1 green** active le client LANE *green* et relie VLAN1 à l'ELAN *green* sur le Catalyst 5000. Avec cette configuration, VLAN1 et l'ELAN *green* englobent un gros sous-réseau IP. Ainsi, un ELAN est en fait une extension de VLAN dans le réseau commuté ATM du réseau commuté Ethernet/Token.

En bref, le Catalyst 5000 agit dans cet exemple comme LECS pour un grand domaine LANE, et comme serveurs LES/BUS pour les ELAN *red*, *green* et *blue*. Il agit aussi comme LEC pour l'ELAN *green*.

La configuration du Catalyst 5000 est la suivante :

```

lane database ABC
  name red server-atm-address
    47.00918100000006170598A01.00602FBCC511.01
  name blue server-atm-address
    47.00918100000006170598A01.00602FBCC511.03
  name green server-atm-address
    47.00918100000006170598A01.00602FBCC511.02
!
interface ATM0
  atm pvc 1 0 5 qsaal
  atm pvc 2 0 16 ilmi
  lane config database ABC

```

```

lane auto-config-atm-address
!
interface ATM0.1 multipoint
lane server-bus ethernet red
!
interface ATM0.2 multipoint
lane server-bus ethernet green
lane client ethernet 1 green
!
interface ATM0.3 multipoint
lane server-bus ethernet blue

```

Dans la configuration suivante du routeur San Jose, l'interface ATM agit comme client LANE pour trois ELAN différents, créant trois sous-réseaux IP différents. Par conséquent, San Jose est un routeur avec une interface commune pour le routage ou la connectivité intra-ELAN. Le LEC dans le LANE *red* ne peut pas communiquer au niveau de la couche ATM directement avec le LEC de l'ELAN *green*. Il doit passer par le routeur San Jose et le routage de niveau 3 :

```

interface ATM0
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
interface ATM0.1 multipoint
ip address 192.10.10.1 255.255.255.0
lane client ethernet red
!
interface ATM0.2 multipoint
ip address 195.10.10.1 255.255.255.0
lane client ethernet green
!
interface ATM0.3 multipoint
ip address 198.10.10.1 255.255.255.0
lane client ethernet blue

```

Dans la configuration suivante du routeur Chicago, l'interface ATM agit comme LEC pour l'ELAN *red* :

```

interface ATM2/0
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
interface ATM2/0.1 multipoint
ip address 192.10.10.2 255.255.255.0
lane client ethernet red

```

Dans la configuration suivante du routeur New York, l'interface ATM agit comme LEC pour l'ELAN *blue* :

```

interface ATM0
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
!
interface ATM0.1 multipoint
ip address 198.10.10.2 255.255.255.0
lane client ethernet blue

```

Dans la configuration suivante des commutateurs ATM Denver et Iowa, il n'y a pas de configuration nécessaire sur les interfaces si vous exécutez PNNI entre eux. La commande **atm lecs-address-default 47.0091.8100.0000.0061.7059.8a01.0060.2fbc.c513.00 1** fournit l'adresse LECS pour n'importe quel LEC connecté directement lors de l'initialisation. Cette commande est absolument nécessaire pour que les services LANE fonctionnent sur tous les commutateurs ATM de frontière

directement connectés aux routeurs, ou sur le Catalyst 5000 agissant comme LEC, si vous utilisez l’option de configuration automatique pour l’attribution de l’adresse du LECS.

La configuration du commutateur Denver est la suivante :

```
atm lecs-address-default
 47.0091.8100.0000.0061.7059.8a01.0060.2fbc.c513.00 1
atm address
 47.0091.8100.0000.0061.7059.8a01.0061.7059.8a01.00
atm router pnni
node 1 level 56 lowest
redistribute ATM-static
interface ATM1/1/1
no keepalive
interface ATM1/1/2
no keepalive
interface ATM1/1/3
no keepalive
```

Voici la configuration du commutateur Iowa :

```
atm lecs-address-default
 47.0091.8100.0000.0061.7059.8a01.0060.2fbc.c513.00 1
atm address
 47.0091.8100.0000.0061.7059.5c01.0061.7059.5c01.00
atm router pnni
node 1 level 56 lowest
redistribute ATM-static
interface ATM3/0/0
no keepalive
interface ATM3/0/1
no keepalive
interface ATM3/0/2
no keepalive
```

Dépannage

Le dépannage d’un environnement utilisant LANE est plus complexe. Généralement, les points problématiques sont les performances des serveurs LES/BUS ou la connectivité vers le LANE. Les performances des serveurs LES/BUS sont liées à la conception et impliquent de nombreux facteurs. Quant au problème de connectivité, il s’agit le plus souvent d’un LEC qui ne peut joindre un LANE donné. Le problème de connectivité intra-LANE dépend davantage du routage IP que de LANE. Examinez donc le fonctionnement du LEC et sa phase de connexion. Lorsqu’il est opérationnel avec un LANE donné, il devrait être en mesure de communiquer directement avec d’autres LEC.

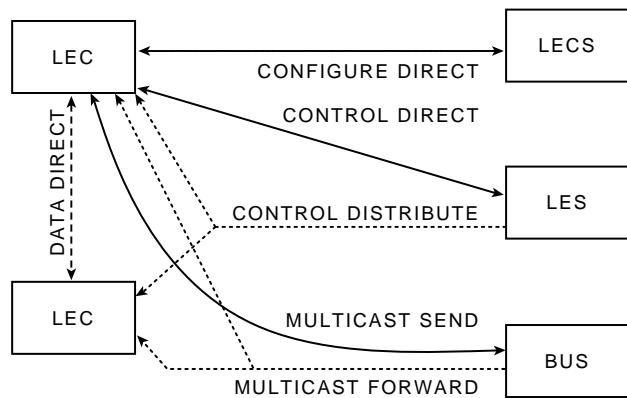
Pour être opérationnel, un LEC doit disposer de tous les circuits virtuels (VCC) suivants, à l’exception de **Data Direct**.

- **ConFigure Direct.** Phase de connexion entre LEC et LECS.
- **Control Direct et Control Distribute.** Circuits de contrôle et de distribution entre LEC et LES.
- **Multicast Send and Multicast Forward.** Phase de connexion entre LEC et BUS.
- **Data Direct.** Phase de connexion entre deux clients LANE.

La Figure 18.5 illustre ces connexions. Cette section traite du dépannage de ces connexions.

Figure 18.5

Circuits de contrôle élémentaires nécessaires au fonctionnement des services LANE.



L'analyse suivante examine la façon dont le LEC sur l'ELAN *blue* sur le routeur New York joint le LANE et devient opérationnel, et comment il communique avec les autres LEC du LANE en question.

NOTE

La mention de couleur n'est en fait pas une couleur, mais le nom d'un LAN logique créé par la technologie ATM LANE. Il y a un LAN logique entre le routeur New York et le routeur San Jose.

NOTE

Même si les routeurs portent des noms de villes, ils appartiennent au même campus. Ils peuvent être considérés comme des désignations d'immeubles.

Pour qu'un LEC puisse appartenir à un ELAN, les serveurs LECS/LES/BUS doivent être opérationnels avant que le LEC ne tente de joindre LANE.

La commande **show lane brief** sur le Catalyst révèle l'adresse du LES et du BUS de l'ELAN *blue*, et confirme qu'ils sont dans le mode opérationnel. C'est nécessaire avant qu'un LEC puisse se connecter à l'ELAN *blue* :

```

Catalyst#show lane brief
  LE Server ATM0.3 ELAN name: blue Admin: up State: operational
  type: ethernet Max Frame Size: 1516
  ATM address: 47.009181000000006170598A01.00602FBCC511.03
  LECS used: 47.009181000000006170598A01.00602FBCC513.00
  connected, vcd 261
  control distribute: vcd 159, 2 members, 4022 packets
  LE BUS ATM0.3 ELAN name: blue Admin: up State: operational
  type: ethernet Max Frame Size: 1516
  ATM address: 47.009181000000006170598A01.00602FBCC512.03
  data forward: vcd 163, 2 members, 6713 packets, 0 unicasts
  
```

La commande **show lane config** révèle que le LECS configuré sur le Catalyst 5000 est opérationnel avec l'adresse du LECS correspondant. Elle indique aussi qu'il sert trois ELAN et qu'ils sont tous actifs :

```
Catalyst#show lane config
LE Config Server ATM0 config table: ABC
Admin: up State: operational
LECS Mastership State: active master
list of global LECS addresses (12 seconds to update):
47.00918100000006170598A01.00602FBCC513.00 <----- me
ATM Address of this LECS:
47.00918100000006170598A01.00602FBCC513.00
vcid rxcnt txcnt callingParty
252 1 1 47.00918100000006170598A01.00602FBCC511.01 LES red 0 active
256 2 2 47.00918100000006170598A01.00602FBCC511.02 LES green 0 active
260 6 6 47.00918100000006170598A01.00602FBCC511.03 LES blue 0 active
cumulative total number of unrecognized packets received so far: 0
cumulative total number of config requests received so far: 100
cumulative total number of config failures so far: 29
cause of last failure: no configuration
culprit for the last failure:
47.00918100000006170595C01.00000C7A5660.01
```

Phase de connexion LEC vers LECS

Cette section couvre l'obtention d'une adresse de LECS *via* ILMI. Le LEC Cisco peut localiser le LECS en utilisant l'une des trois méthodes suivantes :

- une adresse ATM codée en dur ;
- identifier le LECS *via* ILMI VPI=0, VCI=16 ;
- une adresse fixe définie par l'ATM Forum (4700790000000000000000000000.00A03E000001.00).

La commande **debug lane client all** révèle que le LEC sur ATM0.1 tente d'obtenir l'adresse du LECS du commutateur qui lui est directement connecté :

```
NewYork#debug lane client all
LEC ATM0.1: predicate PRED_LEC_NSAP TRUE
LEC ATM0.1: state IDLE event LEC_TIMER_IDLE =>
REGISTER_ADDR
LEC ATM0.1: action A_POST_LISTEN
LEC ATM0.1: sending LISTEN
LEC ATM0.1: listen on
47.00918100000006170595C01.00000C5CA980.01
LEC ATM0.1: state REGISTER_ADDR event
LEC_CTL_ILMI_SET_RSP_POS => POSTING_LISTEN
LEC ATM0.1: received LISTEN
LEC ATM0.1: action A_ACTIVATE_LEC
LEC ATM0.1: predicate PRED_CTL_DIRECT_NSAP FALSE
LEC ATM0.1: predicate PRED_CTL_DIRECT_PVC FALSE
LEC ATM0.1: predicate PRED_LECS_PVC FALSE
LEC ATM0.1: predicate PRED_LECS_NSAP FALSE
LEC ATM0.1: state POSTING_LISTEN event
LEC_SIG_LISTEN_POS => GET_LECS_ADDR
LEC ATM0.1: action A_ALLOC_LECS_ADDR
LEC ATM0.1: state GET_LECS_ADDR event
LEC_CTL_ILMI_SET_RSP_POS => GET_LECS_ADDR
LEC ATM0.1: action A_REGISTER_ADDR
```

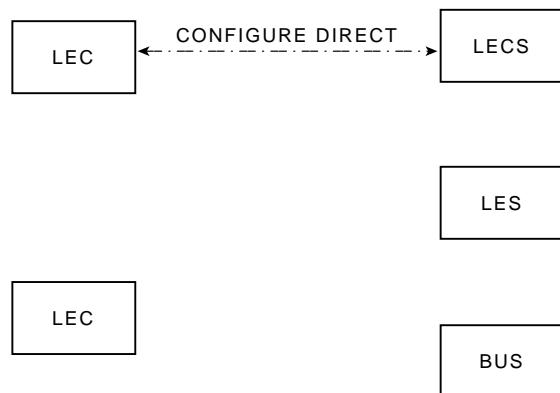
ConFigure Direct :

- établissement d'un VCC bidirectionnel par un LEC dans la phase de connexion avec LECS ;
- utilisé pour obtenir l'adresse ATM du LES.

La Figure 18.6 illustre la phase de connexion LEC vers LECS.

Figure 18.6

Phase de connexion entre LEC et LECS.



Le listing suivant révèle qu'après obtention de l'adresse du LECS, un LEC établit une connexion avec le LECS. Ce VCC est appelé **ConFigure Direct**. Il envoie ensuite la requête de configuration au LECS sur ce même VCC avec ses propres informations, demandant une adresse de LES correspondant à cet ELAN. Le LECS répond en confirmant que les informations de l'ELAN *blue* sollicitées sont définies et fournit au LEC l'adresse du LES en question :

```

NewYork#debug lane client all
LEC ATM0.1: action A_SEND_LECS_SETUP
LEC ATM0.1: sending SETUP
LEC ATM0.1: callid 0x60AC611C
LEC ATM0.1: called party
47.009181000000006170598A01.00602FBCC513.00
LEC ATM0.1: calling_party
47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: state GET_LECS_ADDR event
    LEC_CTL_ILMI_SET_RSP_NEG => LECS_CONNECT
LEC ATM0.1: received CONNECT
LEC ATM0.1: callid 0x60AC611C
LEC ATM0.1: vcd 28
LEC ATM0.1: action A_SEND_CFG_REQ
LEC ATM0.1: sending LANE_CONFIG_REQ on VCD 28
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address
47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: LAN Type 1
LEC ATM0.1: Frame size 1
LEC ATM0.1: LAN Name blue
LEC ATM0.1: LAN Name size 4
LEC ATM0.1: state LECS_CONNECT event LEC_SIG_CONNECT
=> GET_LES_ADDR
  
```

```

LEC ATM0.1: received LANE_CONFIG_RSP on VCD 28
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address
47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: LAN Type 1
LEC ATM0.1: Frame size 1
LEC ATM0.1: LAN Name blue
LEC ATM0.1: LAN Name size 4

```

Connexions de contrôle entre LEC et LES

Après que le LEC a obtenu l'adresse du LES de l'ELAN approprié, il établit les VCC suivants :

Control Direct :

- circuit point à point bidirectionnel avec le LES pour l'envoi de trafic de contrôle ;
- établi par le LEC dans le processus d'initialisation.

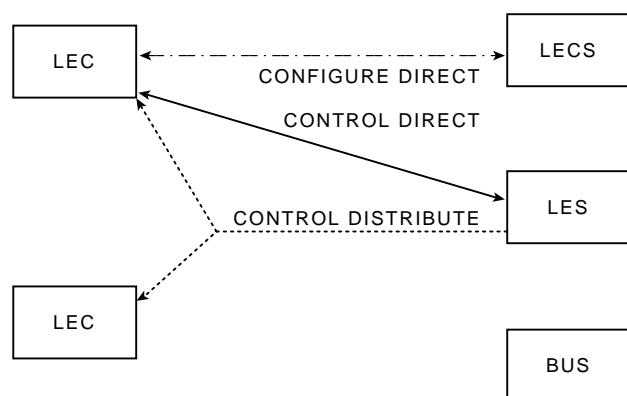
Control Distribute :

- circuit unidirectionnel point à multipoint entre le LES et un ou plusieurs LEC pour distribuer le trafic de contrôle.

La Figure 18. 7 illustre les circuits de contrôle entre LEC et LES.

Figure 18.7

Circuits de contrôle entre LEC et LES.



Le listing de debug suivant révèle que le LEC établit le VCC **Control Direct** avec le LES. Sur ce VCC, il envoie la réponse LANE_JOIN_REQ. Le LES répond avec LECID sur le même VCC. A ce stade, le LES ouvre le circuit **Control Distribute** avec le LEC et celui-ci doit accepter ce VCC pour permettre au LES de distribuer le trafic de contrôle.

```

NewYork#debug lane client all
LEC ATM0.1: action A_SEND_LES_SETUP
LEC ATM0.1: sending SETUP
LEC ATM0.1: callid 0x60ABEDF4
LEC ATM0.1: called party
47.009181000000006170598A01.00602FBCC511.03
LEC ATM0.1: calling_party
47.009181000000006170595C01.00000C5CA980.01

```

```

LEC ATM0.1: received CONNECT
LEC ATM0.1: callid 0x60ABEDF4
LEC ATM0.1: vcd 97
LEC ATM0.1: action A_SEND_JOIN_REQ
LEC ATM0.1: sending LANE_JOIN_REQ on VCD 97
LEC ATM0.1: Status 0
LEC ATM0.1: LECID 0
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address
    47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: LAN Type 1
LEC ATM0.1: Frame size 1
LEC ATM0.1: LAN Name blue
LEC ATM0.1: LAN Name size 4
LEC ATM0.1: received SETUP
LEC ATM0.1: callid 0x60AC726C
LEC ATM0.1: called party
    47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: calling_party
    47.009181000000006170598A01.00602FBCC511.03
LEC ATM0.1: sending CONNECT
LEC ATM0.1: callid 0x60AC726C
LEC ATM0.1: vcd 98
LEC ATM0.1: received CONNECT_ACK
LEC ATM0.1: received LANE_JOIN_RSP on VCD 97
LEC ATM0.1: Status 0
LEC ATM0.1: LECID 1
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address
    47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: LAN Type 1
LEC ATM0.1: Frame size 1
LEC ATM0.1: LAN Name blue
LEC ATM0.1: LAN Name size 4

```

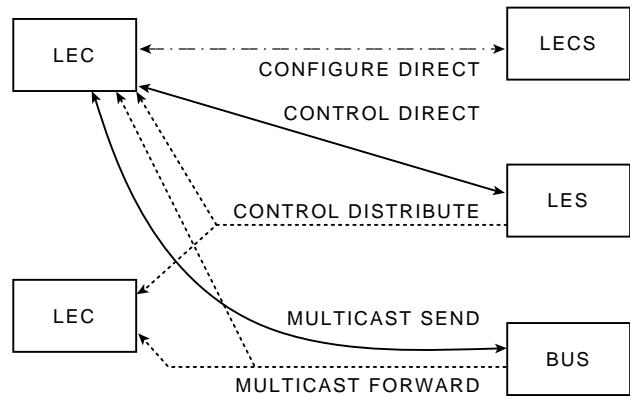
Connexions entre LEC et BUS

Après que le LEC se soit connecté au LES, il sollicite *via* ARP l'adresse ATM du BUS, et le LES lui répond avec l'adresse voulue. Le LEC et le BUS établissent ensuite entre eux les VCC suivants :

- Multicast Send :
 - Le LEC établit ce VCC point-à-point bidirectionnel avec le BUS.
 - Utilisé pour l'envoi de données broadcast/multicast vers le BUS.
- Multicast Forward :
 - Le BUS établit ce VCC point à multipoint vers les LEC.
 - Utilisé pour la transmission de trafic multicast/broadcast vers tous les LEC.

La Figure 18.8 illustre les circuits établis entre LEC et BUS.

Figure 18.8
Circuits établis entre LEC et BUS.



Le listing **debug** suivant révèle que le LEC envoie une requête LANE_ARP_REQ au LES sur le VCC **Control Direct** pour connaître l'adresse ATM du BUS. Le LES répond en lui communiquant sur le VCC **Control Distribute**. Le LEC établit ensuite une connexion directe avec le BUS. Ce VCC est appelé **Multicast Send** et est utilisé pour la transmission de trafic broadcast vers les autres LEC. Le BUS établit aussi un VCC **Multicast Forward** point à multipoint vers les LEC. Chaque fois qu'un nouveau client est connecté, il l'ajoute à ce VCC.

Ce VCC est utilisé par le BUS pour transmettre le trafic broadcast et multicast vers tous les LEC de l'ELAN.

A ce stade, le client LEC sur le routeur New York de l'ELAN *blue* présente un état actif et devient opérationnel. Il est prêt à communiquer avec les autres LEC du même ELAN.

```

NewYork#debug lane client all
LEC ATM0.1: action A_SEND_BUS_ARP
LEC ATM0.1: sending LANE_ARP_REQ on VCD 97
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address
47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: TARGET MAC address ffff.ffff.ffff
LEC ATM0.1: TARGET ATM address
00.000000000000000000000000000000.000000000000.00
LEC ATM0.1: received LANE_ARP_RSP on VCD 98
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address
47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: TARGET MAC address ffff.ffff.ffff
LEC ATM0.1: TARGET ATM address
47.009181000000006170598A01.00602FBCC512.03
LEC ATM0.1: action A_SEND_BUS_SETUP
LEC ATM0.1: predicate PRED_MCAST_SEND_NSAP FALSE
LEC ATM0.1: predicate PRED_MCAST_SEND_PVC FALSE
LEC ATM0.1: sending SETUP
LEC ATM0.1: callid 0x60AC7418
LEC ATM0.1: called party
47.009181000000006170598A01.00602FBCC512.03
LEC ATM0.1: calling_party
47.009181000000006170595C01.00000C5CA980.01
  
```

```

LEC ATM0.1: received CONNECT
LEC ATM0.1: callid 0x60AC7418
LEC ATM0.1: vcd 99
LEC ATM0.1: action A_PROCESS_BUS_CONNECT
LEC ATM0.1: received SETUP
LEC ATM0.1: callid 0x60AC6CA4
LEC ATM0.1: called party
    47.009181000000006170595C01.00000C5CA980.01
LEC ATM0.1: calling_party
    47.009181000000006170598A01.00602FBCC512.03
LEC ATM0.1: action A_SEND_BUS_CONNECT
LEC ATM0.1: sending CONNECT
LEC ATM0.1: callid 0x60AC6CA4
LEC ATM0.1: vcd 100
%LANE-5-UPDOWN: ATM0.1 elan blue: LE Client changed state
    to up
LEC ATM0.1: state MCAST_FORWARD_CONN event
    LEC_SIG_SETUP => ACTIVE
LEC ATM0.1: received CONNECT_ACK
LEC ATM0.1: action A_PROCESS_CONNECT_ACK
LEC ATM0.1: state ACTIVE event LEC_SIG_CONNECT_ACK =>
    ACTIVE

```

La commande **show lane client** sur le routeur New York montre le LEC opérationnel avec tous les VCC correspondants que celui-ci a établis avec les différents services LANE.

Notez que si le LEC échoue dans l'établissement d'un de ces VCC, il doit recommencer le processus d'adhésion depuis le début et le poursuivre jusqu'à ce qu'il le réussisse. Par conséquent, examinez l'état de fonctionnement du client pour déterminer l'origine du problème et réaliser des actions de débogage supplémentaires.

```

NewYork#show lane client
LE Client ATM0.1 ELAN name: blue Admin: up State: operational
Client ID: 1 LEC up for 1 hour 35 minutes 35 seconds
Join Attempt: 1
HW Address: 0000.0c5c.a980 Type: ethernet Max Frame Size: 1516
ATM Address: 47.009181000000006170595C01.00000C5CA980.01

VCD rxFrames txFrames Type ATM Address
0 0 0 configure 47.009181000000006170598A01.00602FBCC513.00
97 1 2 direct 47.009181000000006170598A01.00602FBCC511.03
98 1 0 distribute 47.009181000000006170598A01.00602FBCC511.03
99 0 95 send 47.009181000000006170598A01.00602FBCC512.03
100 190 0 forward 47.009181000000006170598A01.00602FBCC512.03

```

Connexions entre clients LANE

Après qu'un LEC est opérationnel, il peut se connecter aux autres LEC du même ELAN. C'est ce qu'illustre l'analyse suivante.

Ce listing **debug** montre que le LEC envoie une requête LANE_ARP_REQ au LEC avec lequel il souhaite communiquer sur le VCC **Control Direct**. Il reçoit une réponse LANE_ARP_RSP sur le VCC **Control Distribute** avec l'adresse ATM correspondante. Il l'enregistre celle-ci dans sa table de correspondance en cache et établit un VCC **Data Direct** directement avec le LEC :

```

NewYork#debug lane client all
LEC ATM0.1: state ACTIVE event LEC_CTL_READY_IND =>
    ACTIVE

```

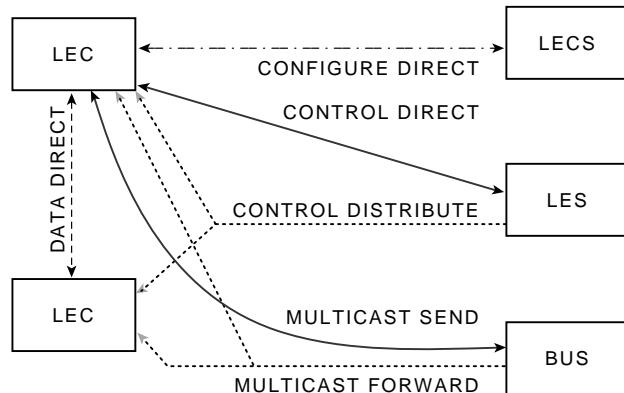
```

LEC ATM0.1: sending LANE_ARP_REQ on VCD 97
LEC ATM0.1: LECID 2
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address 47.00918100000006170595C01.
00000c5ca980.01
LEC ATM0.1: TARGET MAC address 00e0.1eae.fa38
LEC ATM0.1: TARGET ATM address
00.0000000000000000000000000000.000000000000.00
LEC ATM0.1: num of TLVs 0
LEC ATM0.1: received LANE_ARP_REQ on VCD 98
LEC ATM0.1: LECID 2
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address 47.00918100000006170595C01.
00000c5ca980.01
LEC ATM0.1: TARGET MAC address 00e0.1eae.fa38
LEC ATM0.1: TARGET ATM address
00.0000000000000000000000000000.000000000000.00
LEC ATM0.1: num of TLVs 0
LEC ATM0.1: action A_SEND_ARP_RSP
LEC ATM0.1: state ACTIVE event LEC_CTL_ARP_REQ => ACTIVE
LEC ATM0.1: received LANE_ARP_RSP on VCD 98
LEC ATM0.1: LECID 2
LEC ATM0.1: SRC MAC address 0000.0c5c.a980
LEC ATM0.1: SRC ATM address 47.00918100000006170595C01.
00000c5ca980.01
LEC ATM0.1: TARGET MAC address 00e0.1eae.fa38
LEC ATM0.1: TARGET ATM address
47.00918100000006170598A01.00E01EAFA38.03
LEC ATM0.1: num of TLVs 1
LEC ATM0.1: TLV id 0x00A03E2A, len 28, 01 01 47 00 91 81 00 00
00 00
61 70 59 8A 01 00 E0 1E AE FA
3C 00 00 E0 1E AE FA 38
LEC ATM0.1: action A_PROCESS_ARP_RSP
LEC ATM0.1: lec_process_lane_tlv: msg LANE_ARP_RSP,
num_tlv 1
LEC ATM0.1: process_dev_type_tlv:
lec 47.00918100000006170598A01.00E01EAFA38.03, tlv
0x60C90C70

```

La Figure 18.9 illustre le VCC **Data Direct** entre deux clients LANE.

Figure 18.9
Circuit virtuel Data Direct
entre deux LEC.



La commande **show lane client** montre le VCC **Data Direct** en cours d'établissement vers le LEC distant. Comme ce LEC crée des connexions individuelles vers des LEC distants, d'autres VCC **Data Direct** apparaissent dans ce listing. Ce VCC est supprimé s'il y a une absence d'activité entre les deux LEC pendant une certaine période :

```
NewYork#show lane client
LE Client ATM0.1 ELAN name: blue Admin: up State: operational
Client ID: 1 LEC up for 1 hour 35 minutes 35 seconds
Join Attempt: 1
HW Address: 0000.0c5c.a980 Type: ethernet Max Frame Size: 1516
ATM Address: 47.00918100000006170595C01.00000C5CA980.01
VCD rxFrames txFrames Type ATM Address
0 0 0 configure 47.00918100000006170598A01.00602FBCC513.00
97 1 2 direct 47.00918100000006170598A01.00602FBCC511.03
98 1 0 distribute 47.00918100000006170598A01.00602FBCC511.03
99 0 95 send 47.00918100000006170598A01.00602FBCC512.03
100 190 0 forward 47.00918100000006170598A01.00602FBCC512.03
101 6 4 data 47.00918100000006170598A01.00E01EAFA38.03
```

Protocole MPOA (Multiprotocols Over ATM)

Le protocole MPOA fonctionne en collaboration avec LANE. Le transfert de données entre sous-réseaux d'un LANE nécessite la participation d'un routeur même si deux équipements sur deux sous-réseaux différents sont reliés par une infrastructure ATM commune. Cela provoque une dégradation des performances sur un réseau ATM. En même temps, il est absolument nécessaire de séparer l'infrastructure ATM en sous-réseaux de la couche IP pour maintenir les importantes transmissions broadcast au minimum et les limiter aux zones les requérant. MPOA s'accompagne de fonctions permettant la création de petits sous-réseaux et établir des connexions directes entre équipements de sous-réseaux au niveau de la couche ATM si cela s'avère nécessaire.

MPOA possède deux composants principaux : le client multiprotocole ou MPC (*Multiprotocol Client*) et le serveur multiprotocol ou MPS (*Multiprotocol Server*). Le MPC réside généralement sur un équipement de frontière tel qu'un commutateur Catalyst ou un hôte avec ATM activé. Sa fonction principale est d'agir comme point d'entrée et de sortie pour le trafic en utilisant des raccourcis. Il place en cache les informations d'itinéraire direct qu'il obtient de son interaction avec le MPS. Celui-ci est généralement hébergé sur le routeur exécutant plusieurs LEC. Sa fonction première est de fournir des informations de transmission de niveau 3 aux clients MPC.

Considérations de conception

MPOA convient bien à un environnement de campus d'une grande entreprise, et lorsqu'une épine dorsale ATM relie différents campus. Cette infrastructure ATM courante peut être divisée en plusieurs sous-réseaux logiques de niveau 3 pour réduire la transmission broadcast à son minimum tout en autorisant les connexions directes entre sous-réseaux, améliorant ainsi les performances. Vous pouvez voir MPOA comme une solution pour étendre la portée de LANE dans l'environnement de campus sans provoquer de goulet d'étranglement sur le routeur.

Topologie

La topologie suivante possède deux ELAN, l'un entre les routeurs Chicago et San Jose, et l'autre entre les routeurs New York et San Jose. Par conséquent, si l'équipement situé derrière le routeur Chicago doit communiquer avec celui situé après le routeur New York, il passe par le routeur San Jose, car il exécute plusieurs LEC et doit réaliser le routage de niveau 3. Bien qu'il soit évident que les routeurs Chicago et New York sont connectés au même commutateur ATM, l'équipement doit néanmoins utiliser le routeur San Jose pour toute transmission entre sous-réseaux. C'est un emploi inefficace de l'infrastructure ATM et qui dégrade aussi les performances.

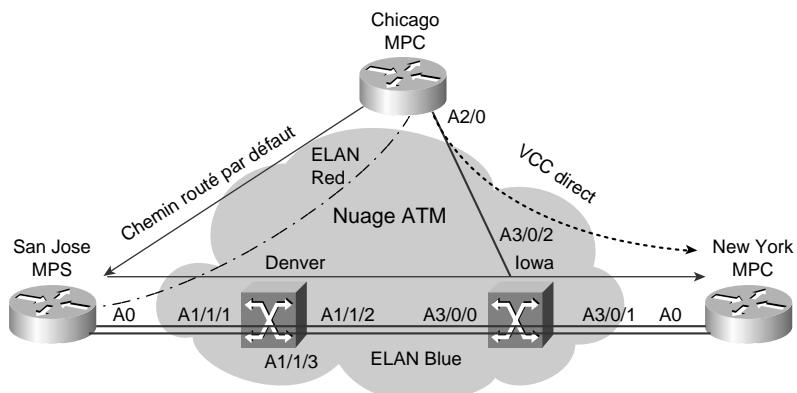
NOTE

MPOA est habituellement utilisé dans un environnement de campus. Même si les routeurs portent des noms de ville ils appartiennent au même campus. Ils peuvent être considérés comme des désignations d'immeubles.

L'utilisation de MPOA dans ce scénario autorise une connexion directe du routeur Chicago vers le routeur New York, même s'ils se trouvent dans des sous-réseaux différents. C'est possible en activant le client MPC sur les routeurs Chicago et New York, et le serveur MPS sur le routeur San Jose.

La Figure 18.10 illustre la topologie pour cet exemple.

Figure 18.10
Exemple de topologie
avec MPOA.



Configuration MPOA

La configuration MPOA fonctionne en relation avec LANE. L'exemple suivant illustre la configuration des MPC et du MPS sur divers équipements supportant ATM.

Dans cet exemple de configuration, le routeur Chicago agit comme client MPOA, le MPC. La commande **mpoa client config name CHI** définit un MPC avec un nom spécifique. Mais le MPC n'est pas fonctionnel tant qu'il n'est pas lié à une interface. La commande **mpoa client name CHI** démarre un processus MPC sur une interface, le rendant totalement opérationnel. Le MPC a obtenu une adresse ATM en utilisant un algorithme particulier et est prêt à accepter des appels. La

commande **lane client mpoa client name CHI** associe un client LANE *red* avec le MPC CHI spécifié. La configuration du routeur Chicago est la suivante :

```
mpoa client config name CHI
interface Loopback1
ip address 40.1.1.1 255.255.255.0
interface ATM2/0
no ip address
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
mpoa client name CHI
!
interface ATM2/0.1 multipoint
ip address 192.10.10.2 255.255.255.0
lane client mpoa client name CHI
lane client ethernet red
```

Dans l'exemple de configuration suivant, le routeur New York agit comme client MPOA pour les équipements situés derrière lui. La configuration du routeur New York est la suivante :

```
mpoa client config name NY
!
interface Loopback0
ip address 50.1.1.1 255.255.255.0
interface ATM0
no ip address
no ip mroute-cache
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
mpoa client name NY
!
interface ATM0.1 multipoint
ip address 198.10.10.2 255.255.255.0
lane client mpoa client name NY
lane client ethernet blue
```

Dans l'exemple de configuration suivant, le routeur San Jose agit comme serveur MPOA pour l'ELAN *red* et *blue*.

La commande **mpoa server config name SJ** définit un MPS avec le nom spécifié, mais il n'est pas encore opérationnel tant qu'il n'est pas lié à une interface.

La commande **mpoa server name SJ** lie un MPS à une interface principale. A ce stade, le MPS peut obtenir une adresse ATM générée automatiquement et une interface par laquelle il peut communiquer aux équipements MPOA voisins. Un MPS n'est fonctionnel que lorsqu'il est défini globalement puis attaché à une interface.

La commande **lane client mpoa server name SJ** associe un LEC avec le MPS nommé. Celui-ci doit déjà exister pour que cette commande soit acceptée.

La configuration du routeur San Jose est la suivante :

```
lane database ABC
name red server-ATM-address
    47.00918100000006170598A01.00E01EAFA39.01
name red elan-id 10
name blue server-ATM-address
    47.00918100000006170598A01.00E01EAFA39.03
name blue elan-id 30
!
```

```

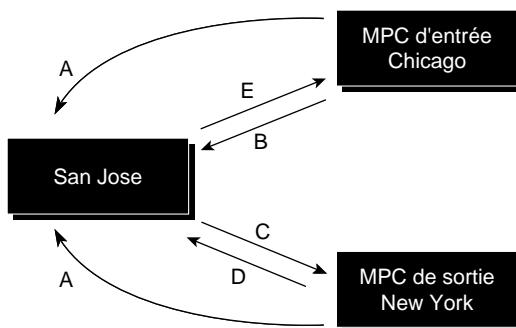
mpoa server config name SJ
!
interface Loopback0
ip address 60.1.1.1 255.255.255.0
interface ATM0
atm pvc 10 0 5 qsaal
atm pvc 20 0 16 ilmi
lane config database ABC
lane auto-config-ATM-address
mpoa server name SJ
!
interface ATM0.1 multipoint
ip address 192.10.10.1 255.255.255.0
lane server-bus ethernet red
lane client mpoa server name SJ
lane client ethernet red
!
interface ATM0.3 multipoint
ip address 198.10.10.1 255.255.255.0
lane server-bus ethernet blue
lane client mpoa server name SJ
lane client ethernet blue

```

Dépannage

Le dépannage de MPOA devient plus facile lorsque vous comprenez l'interaction de ses composants logiques, les MPC et les MPS. La Figure 18.11 illustre le fonctionnement de MPOA.

Figure 18.11
Fonctionnement de MPOA.



Le fonctionnement de MPOA se déroule de la façon suivante :

- **Les MPC doivent connaître leur MPS.** Découverte du MPS.
- **Requête de résolution MPOA.** Une requête d'un MPC pour résoudre une adresse de protocole de destination en adresse ATM pour établir un circuit virtuel commuté direct (SVC) avec l'équipement d'entrée.
- **Requête d'imposition de cache MPOA.** Une requête d'un MPS vers un MPC d'entrée, fournissant les informations de réécriture MAC pour une adresse de protocole de destination.

- **Réponse d'imposition de cache MPOA.** Réponse de la part d'un MPC d'entrée correspondant à une requête MPS précédente d'entrée.
- **Réponse de résolution MPOA.** Réponse d'un MPS, résolvant une adresse de protocole vers une adresse ATM.

L'analyse de dépannage suivante utilise différentes commandes **show** et **debug** pour illustrer l'interaction entre le MPC et le MPS pour créer un VCC direct.

La commande **show mpoa client** sur le routeur Chicago montre qu'il ne connaît pas d'autres MPS ou MPC.

Découverte du MPS

Le listing suivant montre qu'il n'y a pas de MPS connu. Après l'initiation de la requête LE_ARP, comme montré dans le listing **debug**, le client obtient l'adresse MPS. La fin du listing montre le MPS découvert :

```
Chicago#show mpoa client
MPC Name: CHI    Interface: ATM2/0      State: Up
MPC ATM Address:
  47.009181000000006170595C01.00E070CA9045.00
Shortcut-Setup Count: 1    Shortcut-Setup Time: 1
LECs bound to CHI: ATM2/0.1
MPS Neighbors of CHI:
  ATM Address      MPS-ID      VCD      rxPkts      txPkts
  Remote Devices known to CHI:
    ATM Address      VCD      rxPkts      txPkts
```

Le listing de la commande **debug lane client mpoa** montre que le MPC local obtient l'adresse ATM du MPS. Chaque fois qu'une requête LEC_ARP_REQ ou une réponse LEC_ARP_RESP est envoyée à partir d'un LEC, un TLV (type, longueur, valeur) est inclus, spécifiant l'adresse ATM du MPC associé au LEC :

```
Chicago#debug lane client mpoa
LEC ATM2/0.1: received lec_process_lane_tlv: msg
  LANE_ARP_REQ, num_tlv 1
LEC ATM2/0.1: process_dev_type_tlv: lec
  47.009181000000006170598A01.00E01EAFA38.01,
  tlv 0x61039220
LEC ATM2/0.1: type MPOA_MPS, mpc
  00.00000000000000000000000000.000000000000.00
mps 47.009181000000006170598A01.00E01EAFA3C.00 mac
  00e0.1eae.fa38
LEC ATM2/0.1: process_dev_type_tlv: create le_arp for le_mac
  00e0.1eae.fa38
LEC ATM2/0.1: create mpoa_lec
LEC ATM2/0.1: new mpoa_lec 0x611401D4
LEC ATM2/0.1: process_dev_type_tlv: type MPS, tlv-
  >num_mps_mac 1
LEC ATM2/0.1: lec_add_mps: remote lec
  47.009181000000006170598A01.00E01EAFA38.01
mps 47.009181000000006170598A01.00E01EAFA3C.00
  num_mps_mac 1,
  mac 00e0.1eae.fa38
LEC ATM2/0.1: lec_add_mps: add mac 00e0.1eae.fa38, mps_mac
  0x611407C0
LEC ATM2/0.1: lec_append_mpoa_dev_tlv:
```

NOTE

Le protocole LE_ARP (*LAN Emulation Address Resolution Protocol*) fournit l'adresse ATM qui correspond à une adresse MAC.

La commande **show mpoa client** révèle maintenant les adresses ATM du MPS et du MPC voisins avec les circuits virtuels associés :

```
Chicago#show mpoa client
MPC Name: CHI      Interface: ATM2/0      State: Up
MPC ATM Address: 47.009181000000006170595C01.00E01EAFA3C.00
Shortcut-Setup Count: 1      Shortcut-Setup Time: 1
LECs bound to CHI: ATM2/0.1
MPS Neighbors of CHI:
ATM Address          MPS-ID  VCD    rxPkts   txPkts
47.009181000000006170598A01.00E01EAFA3C.00 1      20    1256     836
Remote Devices known to CHI:
ATM Address          VCD
47.009181000000006170595C01.00E01EAFA6D.00      257-----MPC on New York Router
```

Requête et réponse de la résolution MPOA

Dans l'exemple de dépannage suivant, effectuer un suivi de la route 50.1.1.1 à partir de Chicago requiert que les paquets de données soient envoyés par le routeur San Jose, car il exécute les deux ELAN *red* et *blue*. Mais avec le protocole MPOA activé et une infrastructure ATM commune permettant l'établissement du VCC direct, le MPC CHI enverra une requête MPOA de résolution de l'adresse IP 50.1.1.1 en adresse ATM par laquelle il peut atteindre ce réseau.

Le MPS San Jose répond à la requête avec l'adresse ATM. Une fois en possession de l'adresse ATM du réseau 50.1.1.1, le routeur Chicago établit un VCC direct à travers le nuage ATM. Cela peut être confirmé en effectuant une autre procédure de suivi vers 50.1.1.1 qui montre qu'il peut être atteint avec un saut *via* 198.10.10.2 au lieu de deux.

```
Chicago#trace 50.1.1.1
Tracing the route to 50.1.1.1
1 192.10.10.1 0 msec
198.10.10.2 0 msec 0 msec

Chicago#debug mpoa client all
MPAOA CLIENT: mpc_trigger_from_lane: mac 00e0.1eae.fa38 on out
                ATM2/0.1
MPAOA CLIENT: Is MAC 00e0.1eae.fa38 interesting on i/f: ATM2/0.1
MPAOA CLIENT: MAC 00e0.1eae.fa38 interesting
MPAOA CLIENT CHI: Ingress Cache entry created for 50.1.1.1
MPAOA CLIENT CHI: manage_hw_ingress_cache: msgtype
                QUERY_DATA_FLOW_ACTIVE for ip 50.1.1.1
MPAOA CLIENT CHI: ipcache not exist
MPAOA CLIENT CHI: mpc_manage_ingress_cache(): called with
MPC_IN_CACHE_UPDATE_ADD for destIp=50.1.1.1
MPAOA CLIENT CHI: Ingress Cache- curr state=
                MPC_IN_CACHE_INITIALIZED, event=
MPC_ELIGIBLE_PACKET RECEIVED, dest IP= 50.1.1.1
MPAOA CLIENT CHI: Flow detected for IP=50.1.1.1
MPAOA CLIENT CHI: MPOA Resolution process started for 50.1.1.1
MPAOA CLIENT CHI: Sending MPOA Resolution req for 50.1.1.1
```

```

MPOA CLIENT CHI: Ingress Cache state changed- old=0, new=1, IP
    addr=50.1.1.1
MPOA CLIENT: mpc_count_and_trigger: cache state TRIGGER
MPOA DEBUG: nhrp_parse_packet finished, found 1 CIE's and 2
    TLV's
MPOA CLIENT: received a MPOA_RESOLUTION_REPLY (135)
    packet of size 127 bytes on ATM2/0 vcd 1
MPOA CLIENT CHI: Resol Reply-IP addr 50.1.1.1, mpxp
    addr=47.00918100000006170595C01.00E01EAFA6D.00,TA
    G=2217672716
MPOA CLIENT CHI: Ingress Cache- curr state=
    MPC_IN_CACHE_TRIGGER, event=
MPC_VALID_RESOL_REPLY_RECVD, dest IP= 50.1.1.1
MPOA CLIENT CHI: No Active VC-connect to remote MPC
    47.00918100000006170595C01.00E01EAFA6D.00
MPOA CLIENT CHI: connect to remote MPC
    47.00918100000006170595C01.00E01EAFA6D.00 called
MPOA CLIENT CHI: SETUP sent to remote MPC
    47.00918100000006170595C01.00E01EAFA6D.00
MPOA CLIENT CHI: Ingress Cache state changed- old=1, new=4, IP
    addr=50.1.1.1
MPOA DEBUG: nhrp_parse_packet finished, found 1 CIE's and 2
    TLV's

Chicago#trace 50.1.1.1
Tracing the route to 50.1.1.1
1 198.10.10.2 0 msec

```

Requête et réponse MPOA d'imposition de cache

A réception de la requête de résolution MPOA, le MPS San Jose envoie une requête d'imposition de cache au MPC de sortie, comme le montre le listing **debug** suivant. Il obtient la réponse du MPC de sortie avec les informations de la couche liaison de données DLL (*Data Link Layer*) sous la forme d'une réponse MPOA d'imposition de cache. Le MPS convertit ensuite cette réponse en réponse de résolution pour la renvoyer au MPC d'entrée.

Le listing de la commande **show** suivant montre que le MPC d'entrée possède maintenant le cache pour l'adresse IP de destination et qu'il peut maintenant établir la commutation directe de niveau 2 avec le MPC de sortie de destination, en évitant ainsi la commutation de niveau 3 du routeur :

```

SanJose#debug mpoa server
MPOA SERVER: received a MPOA_RESOLUTION_REQUEST
    (134) packet of size 64 bytes on ATM0 vcd 342
MPOA SERVER SJ: packet came from remote MPC
    47.00918100000006170595C01.006070CA9045.00
MPOA SERVER SJ: process_mpoa_res_req called
MPOA SERVER SJ: mps_next_hop_info activated
MPOA SERVER SJ: next hop interface and next hop ip address are
    NOT known, trying to find them
MPOA SERVER SJ: mps_next_hop_info: next hop interface:
    ATM0.3, next hop ip address: 198.10.10.2
MPOA SERVER SJ: ingress cache entry created for:
    47.00918100000006170595C01.006070CA9045.00, 50.1.1.1
MPOA SERVER SJ: ingress cache entry is not yet valid, started the
    giveup timer (40 secs) on it
MPOA SERVER: next_hop_mpoa_device: returning type MPC for
    198.10.10.2
MPOA SERVER SJ: I am the egress router: starting mpoa cache

```

```

impo req procedures
MPOA SERVER SJ: egress cache entry created for:
47.009181000000006170595C01.00E01EAFA6D.00, 50.1.1.1
198.10.10.1 (src)
MPOA SERVER SJ: a NEW cache id (28) is assigned
MPOA SERVER SJ: egress cache entry is not yet valid, started the
giveup timer (40 secs) on it
MPOA SERVER SJ: MPOA_CACHE_IMPOSITION_REQUEST
    packet sent to remote MPC
    47.009181000000006170595C01.00E01EAFA6D.00
MPOA SERVER: received a MPOA_CACHE_IMPOSITION_REPLY
    (129) packet of size 127 bytes on ATM0 vcd 327
MPOA SERVER SJ: packet came from remote MPC
    47.009181000000006170595C01.00E01EAFA6D.00
MPOA SERVER SJ: process_mpoa_cache_imp_reply called
MPOA SERVER: searching cache entry by new req id 58
MPOA SERVER SJ: egress MPS received a 'proper' mpoa cache
    impo REPLY: validating and starting the holding timer on the
    egress cache entry
MPOA SERVER SJ: snooping on the mpoa cache imposition reply
    packet CIE: cli_addr_t1 = 20, cli_nbma_addr =
    47.009181000000006170595C01.00E01EAFA6D.00
MPOA SERVER SJ: tag value 2217672716 extracted
MPOA SERVER SJ: mps_next_hop_info activated
MPOA SERVER SJ: next hop interface and next hop ip address are
    NOT known, trying to find them
MPOA SERVER SJ: mps_next_hop_info: next hop interface:
    ATM0.3, next hop ip address: 198.10.10.1
MPOA SERVER SJ: converting the packet to a nhrp res reply
MPOA SERVER SJ: process_nhrp_res_reply called
MPOA SERVER: searching cache entry by new req id 57
MPOA SERVER SJ: success: ingress MPS picked up holding time of
    1200 seconds from the 1st CIE
MPOA SERVER SJ: validated and started the holding timer on the
    ingress cache entry
MPOA SERVER SJ: converting the packet to an mpoa res reply
MPOA SERVER SJ: MPOA_RESOLUTION_REPLY packet sent to
    remote MPC
    47.009181000000006170595C01.00E01EAFA6D.00

Chicago#show mpoa client cache
MPC Name: CHI Interface: ATM2/0 State: Up
MPC ATM Address:
    47.009181000000006170595C01.00E01EAFA6D.00
Shortcut-Setup Count: 1 Shortcut-Setup Time: 1
Number of Ingress cache entries: 1
MPC Ingress Cache Information:
Dst IP addr State MPSid VCD Time-left Egress MPC ATM addr
RESOLVE 1 57 19:27
    47.009181000000006170595C01.00E01EAFA6D.00
Number of Egress cache entries: 1
MPC Egress Cache Information:
Dst IP addr Dst MAC Src MAC MPSid Elan Time-left CacheId
192.10.10.2 00E0.70CA.9040 00E0.1EAE.FA38 1 10 19:26 29

```

Résumé

Ce chapitre a traité de LANE et des diverses méthodes de déploiement de MPOA (*Multiprotocols Over ATM*). Vous pouvez appliquer des méthodes appropriées en fonction des exigences de votre réseau et de votre environnement, puis utiliser les exemples de configuration présentés pour vous familiariser avec les différentes méthodes. Vous pouvez, bien sûr, également tester certaines procédures de dépannage avant de déployer une méthode. Après la mise en œuvre d'une méthode sur le réseau, gardez à l'esprit les points suivants :

- Le recours au débogage n'est pas aussi simple qu'il ne paraît. Il peut en résulter des problèmes de performances au niveau des ressources processeur. Utilisez cette procédure avec précaution.
- Essayez les commandes **show** autant que possible avant d'activer le débogage.
- En ce qui concerne le débogage du RFC 1483, ILMI ne sollicite pas autant les ressources processeur, mais cela peut être le cas pour les événements de signalisation.
- Concernant le RFC 1577, le débogage du côté du client ARP procure une excellente méthode d'identification des problèmes. Evitez l'analyse du côté du serveur ARP.
- Le débogage de LANE est très sensible du côté des clients LEC et des serveurs LES/BUS. Essayez d'utiliser la commande **show** pour identifier le point de blocage de la connexion du LEC avec l'ELAN. Si vous exécutez plusieurs LEC sur le routeur/commutateur, exécutez **debug** uniquement sur le client posant problème.
- Evitez d'activer le débogage sur les serveurs LES/BUS, car ils sont utilisés intensément et peuvent générer en sortie de gros volumes de données et ralentir le processeur.
- Pour MPOA, le débogage sur le MPC avec désactivation du débogage keepalive, fournira les informations les plus utiles.

Routage DDR

Par Salman Asad

La fonctionnalité de routage par ouverture de ligne à la demande, ou DDR (*Dial-on Demand Routing*), de Cisco, autorise l'exploitation des lignes téléphoniques existantes pour former un réseau étendu (WAN). Lors de l'utilisation courante de ces lignes téléphoniques, vous pouvez analyser les modèles de trafic, afin de déterminer si l'installation de liaisons louées pourrait convenir. DDR permet de réaliser des économies substantielles par rapport aux liaisons louées pour les lignes qui sont utilisées seulement quelques heures par jour, ou qui connaissent une faible densité de trafic.

DDR implanté sur des lignes série requiert l'emploi de dispositifs de numérotation qui supportent V.25bis. Il s'agit d'un standard de l'UIT-T pour la signalisation intrabande (*in-band signaling*) vers des équipements de communication de données (DCE, *Data Communications Equipment*) synchrones. V.25bis est supporté par une variété de dispositifs, tels que les modems V.32 analogiques, les adaptateurs terminaux (TA, *Terminal Adapter*) RNIS, et les multiplexeurs inverses. L'implémentation Cisco de V.25bis supporte les dispositifs qui utilisent la version 1984 de ce standard (qui nécessite l'emploi de la parité impaire), ainsi que ceux qui utilisent la version 1988 (qui ne nécessite pas de parité).

NOTE

L'UIT-T (Union internationale des télécommunications, secteur normalisation) était anciennement connue sous le nom de CCITT (Comité consultatif international pour la télégraphie et la téléphonie).

L'étude de cas que nous présentons ici décrit l'utilisation de DDR afin de connecter un réseau mondial composé d'un site central situé à San Francisco et de sites distants situés à Tokyo, à Singapour, et à Hong Kong. Ce chapitre examine les exemples de scénarios et de fichiers de configuration suivants :

■ Configuration du site central pour les appels sortants.

Configuration du site central et des sites distants pour trois types d'installations : un site central avec une interface pour chaque site distant ; une seule interface pour plusieurs sites distants ; plusieurs interfaces pour plusieurs sites distants. (Des exemples de groupes de rotation et de listes d'accès sont fournis.)

■ Configuration du site central et des sites distants pour les appels entrants et sortants.

Configuration du site central et des sites distants pour trois types d'installations : un site central avec une interface pour chaque site distant ; une seule interface pour plusieurs sites distants ; plusieurs interfaces pour plusieurs sites distants. L'utilisation de l'encapsulation PPP (*Point-to-Point Protocol*) et du protocole CHAP (*Challenge Handshake Authentication Protocol*) est également abordée.

■ Configuration des sites distants pour les appels sortants.

Dans une configuration courante, les sites distants appellent le site central, mais l'inverse n'est pas possible. Sur une topologie en étoile, tous les routeurs distants peuvent posséder leurs interfaces série sur le même sous-réseau que l'interface du site central.

■ Utilisation de DDR en tant que solution de secours pour des liaisons louées.

Emploi de DDR en tant que méthode de secours pour des liaisons louées. Des exemples de l'utilisation de routes statiques flottantes (*floating static routes*) sur des interfaces individuelles et partagées sont fournis.

■ Utilisation de liaisons louées et du secours commuté (*dial backup*).

Utilisation de la numérotation DTR (*Data Terminal Ready*) et de la numérotation V.25bis avec des liaisons louées.

La Figure 19.1 illustre la topologie du réseau DDR qui fait l'objet de cette étude de cas.

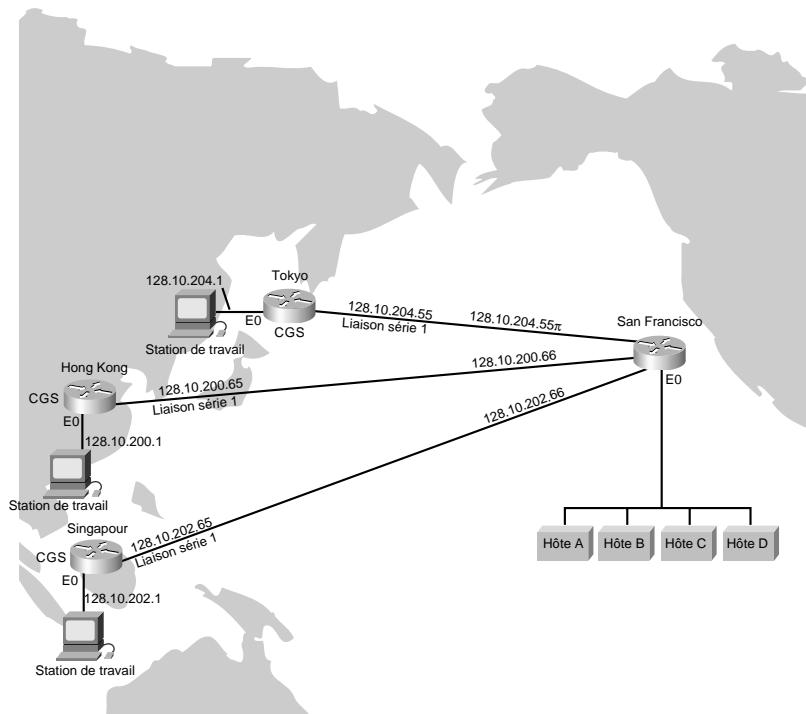
NOTE

Tous les exemples et descriptions de cette étude de cas font référence à des fonctionnalités disponibles dans System Software, version 9.1(9) ou supérieure. Certaines de ces fonctionnalités sont présentes dans les versions antérieures ; les fonctionnalités disponibles uniquement dans la version 9.21 sont spécifiées.

Configuration du site central pour les appels sortants

Dans notre exemple, le site central appelle les sites distants. Le coût d'un appel depuis les Etats-Unis vers des sites internationaux revient souvent moins cher que lorsque les sites distants initient l'appel, et ces derniers n'ont généralement besoin de se connecter au site central que de façon périodique. Cette section étudie les exemples de configuration suivants, dans lesquels le site central est configuré pour les appels sortants :

Figure 19.1
Topologie du réseau DDR.



- configuration d'une interface pour chaque site distant ;
- configuration d'une seule interface pour plusieurs sites distants ;
- configuration de plusieurs interfaces pour plusieurs sites distants.

Configuration d'une interface pour chaque site distant

Initialement, le site central situé à San Francisco est configuré de façon à disposer d'une interface pour chaque site distant.

Site central : appels sortants uniquement

Dans la configuration suivante, le site central effectue des appels à l'aide d'une interface séparée, configurée pour chaque site distant. Aucun support pour répondre aux appels entrants n'est configuré ici :

```
interface serial 5
description DDR connection to Hong Kong
ip address 128.10.200.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118527351625
pulse-time 1
dialer-group 1
```

```

!
interface serial 6
description DDR connection to Singapore
ip address 128.10.202.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 011653367085
pulse-time 1
dialer-group 1
!
interface serial 7
description DDR connection to Tokyo
ip address 128.10.204.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118127351625
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
redistribute static
! route vers Hong Kong
ip route 128.10.200.0 255.255.255.192 128.10.200.65
! route vers Singapour
ip route 128.10.202.0 255.255.255.192 128.10.202.65
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.204.65
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

Configuration des interfaces et des adresses IP

La configuration des interfaces et des adresses IP (*Internet Protocol*) individuelles est simple. L'adresse IP de chaque interface est fournie. L'exemple utilise une portion hôte de 6 bits de l'adresse IP. La commande `dialer in-band` active DDR, ainsi que la numérotation V.25bis sur l'interface. Comme mentionné précédemment, la numérotation V.25bis est un standard de l'UIT-T pour la signification intrabande vers des équipements de communication de données synchrones (DCE). Une variété de dispositifs supportent ce standard, depuis les modems analogiques V.32 jusqu'aux adaptateurs terminaux, en passant par les multiplexeurs inverses.

La commande `dialer wait-for-carrier-time` est définie avec une valeur de 60 secondes. Lorsque la numérotation V.25bis est utilisée, le routeur n'analyse aucune des réponses reçues de la part de l'équipement DCE. A la place, il s'appuie sur le signal de détection de porteuse (CD, *Carrier Detect*) pour savoir si un appel a été connecté. Si le signal CD du modem n'est pas activé durant la période de temps allouée par la commande `dialer wait-for-carrier-time`, le routeur suppose que l'appel a échoué, et déconnecte la ligne. Comme il s'agit ici d'appels internationaux, qui prennent donc plus de temps à s'initialiser que les appels locaux, le temps d'attente du signal est défini à 60 secondes. Dans le cas d'appels locaux, les modems analogiques mettent parfois 20 à 30 secondes pour se synchroniser, temps de numérotation et de réponse inclus.

La commande `dialer string` identifie le numéro de téléphone de la destination cible. Etant donné que le site central appelle une seule destination par interface, la configuration de cette chaîne de

numérotation est extrêmement simple. La commande **pulse-time** spécifie le temps d'inactivité de DTR. Lorsque DDR et les modems V.25bis sont utilisés, le routeur déconnecte les appels en désactivant DTR. Cette commande est automatiquement insérée dans la configuration au moment où la commande **dialer in-band** est entrée.

La commande **dialer-group** sert à identifier chaque interface, grâce à un ensemble de listes de numérotation (*dialer list*). La commande **dialer-list** associe à chaque interface des listes d'accès qui permettent de distinguer les paquets "intéressants" des paquets "inintéressants" pour l'interface. Pour plus de détails sur les listes de numérotation, voyez la section "Configuration de listes d'accès", plus loin dans ce chapitre.

Configuration du routage

Le protocole IGRP (*Interior Gateway Routing Protocol*) est utilisé afin de router le trafic sur le réseau. Les deux premières commandes qui apparaissent dans la section de routage du fichier de configuration sont **router igrp** et **network**. Elles définissent le numéro du routeur IGRP, ainsi que le réseau sur lequel est exécuté le protocole.

La commande **redistribute** provoque l'envoi des informations de routes statiques (définies à l'aide des commandes **ip route** illustrées dans l'exemple de configuration) vers les autres routeurs situés dans la même zone IGRP. En l'absence de cette commande, les autres routeurs connectés au site central ne disposent d'aucune route vers les routeurs distants. Les trois routes statiques définissent les sous-réseaux sur l'épine dorsale Ethernet des routeurs distants. DDR a tendance à utiliser largement les routes statiques, car les mises à jour de routage ne sont pas reçues lorsque la connexion par circuit commuté n'est pas active.

Configuration de listes d'accès

La dernière section du fichier de configuration contient les listes d'accès utilisées par DDR afin de classer les paquets intéressants et inintéressants. Les paquets intéressants sont soumis aux critères de sélection des listes d'accès. Ces paquets initient un appel s'il n'y en a pas déjà un en cours ; dans le cas contraire, ils réinitialisent le temporisateur d'inactivité (*idle timer*). Les paquets inintéressants sont transmis seulement si la liaison est active ; ils sont supprimés si elle est inactive. Ces paquets ne déclenchent pas d'appel et ne réinitialisent pas non plus le temporisateur d'inactivité. La liste d'accès 101 fournit les filtres suivants :

- Les paquets IGRP qui sont envoyés vers l'adresse de broadcast (255.255.255.255) ne déclenchent pas la numérotation.
- Tous les autres paquets IP sont intéressants et peuvent par conséquent déclencher la numérotation et réinitialiser le temporisateur d'inactivité.

Sites distants : appels entrants seulement

A l'exception de l'adresse IP et de la route par défaut, chaque site distant est configuré de façon identique, en tant que site répondant uniquement. L'exemple suivant illustre la configuration de Hong Kong :

```
interface serial 1
description interface to answer calls from San Francisco
ip address 128.10.200.65 255.255.255.192
```

```
dialer in-band
!
ip route 0.0.0.0 0.0.0.0 128.10.200.66
```

Le site répondant ne déconnectera pas l'appel, car c'est le site appelant qui s'en charge lorsque la ligne est inactive. Dans ce cas, le site qui répond utilise le routage statique. La route par défaut pointe sur l'interface série du site central.

Configuration d'une seule interface pour plusieurs sites distants

Il est possible d'utiliser une seule interface pour appeler plusieurs destinations, un site situé à Melbourne et un site situé à Paris, par exemple. Eu égard aux différences de fuseaux horaires, ces sites n'auront jamais besoin d'être connectés au même moment. Par conséquent, une seule interface peut être utilisée pour ces deux sites, sans risque de *contention* pour l'interface, ce qui élimine le coût associé aux ports série et modems dédiés à chaque destination.

Site central : appels sortants seulement

Dans la configuration suivante, le site central effectue les appels. Une seule interface est configurée pour appeler plusieurs sites distants. Aucun support pour répondre aux appels entrants n'est configuré ici :

```
interface serial 5
description DDR connection to Hong Kong and Singapore
ip address 128.10.200.66 255.255.255.192
ip address 128.10.202.66 255.255.255.192 secondary
dialer in-band
dialer wait-for-carrier-time 60
! associe Hong Kong à un numéro de téléphone
dialer map ip 128.10.200.65 0118527351625
! associe Singapour à un numéro de téléphone
dialer map ip 128.10.202.65 011653367085
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
passive-interface serial 5
redistribute static
! route vers Hong Kong
ip route 128.10.200.0 255.255.255.192 128.10.200.65
! route vers Singapour
ip route 128.10.202.0 255.255.255.192 128.10.202.65
! La liste d'accès suivante refuse tout le trafic broadcast IGRP
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
! La liste d'accès suivante autorise tous les paquets IP
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
```

Configuration de l'interface

Dans cet exemple, la configuration de l'interface est un peu plus complexe que celle décrite à la section "Configuration d'une interface pour chaque site distant". En plus de l'adresse IP d'origine, une seconde adresse IP est configurée pour l'interface série 5, car les bureaux de Hong Kong et de Singapour se trouvent sur des sous-réseaux différents.

L'emploi des commandes `dialer in-band`, `dialer wait-for-carrier-time`, `pulse-time`, et `dialer-group` est identique à celui décrit à la section "Configuration d'une interface pour chaque site distant". Néanmoins, la commande `dialer string` précédente a été supprimée, et remplacée par deux commandes `dialer map`.

La première commande `dialer map` associe le numéro de téléphone du routeur de Hong Kong à son adresse de prochain saut, c'est-à-dire l'adresse IP du port série du routeur de Hong Kong. La seconde associe le numéro de téléphone du routeur de Singapour à son adresse de prochain saut.

Configuration du routage

Les routes statiques IP définissent les adresses de prochain saut utilisées dans les commandes `dialer map`. Lorsqu'un paquet est reçu pour un hôte du réseau 128.10.200.0, il est routé vers une adresse de prochain saut, 128.10.200.65. Cette route part de l'interface série 5. DDR se sert de l'adresse de prochain saut pour obtenir le numéro de téléphone du routeur de destination.

NOTE

L'utilisation de la commande `passive-interface` indique que les mises à jour de routage ne doivent pas être envoyées à partir de l'interface série 5. Etant donné que les sites distants utilisent une route par défaut, il est inutile d'envoyer des mises à jour sur cette liaison.

Configuration de listes d'accès

L'utilisation des commandes `dialer map` autorise un filtrage plus granulaire. Lorsqu'un paquet est reçu pour un hôte du réseau 128.10.200.0, il est routé vers une adresse de prochain saut, 128.10.200.65. Cette route part de l'interface série 5. Le paquet est comparé aux listes d'accès. S'il est considéré comme étant intéressant, son adresse de prochain saut est comparée aux commandes `dialer map` définies pour cette interface. Lorsqu'une correspondance est trouvée, l'interface est contrôlée afin de déterminer si elle est connectée au numéro de téléphone qui correspond à l'adresse de prochain saut. Si elle n'est pas connectée, le numéro de téléphone est appelé. Dans le cas contraire, le temporisateur d'inactivité est réinitialisé. Si elle est connectée à un autre numéro de téléphone (d'une autre commande `dialer map`), le temporisateur d'accélération d'inactivité (*fast-idle timer*) est lancé, grâce à une contention sur l'interface. Si aucune entrée n'est trouvée dans les correspondances de numérotation pour l'adresse de prochain saut, et qu'aucune chaîne de numérotation n'a été définie (associée à toutes les adresses de prochain saut), le paquet est supprimé.

Ce niveau de filtrage additionnel pour l'adresse de prochain saut représente un problème pour la diffusion générale de paquets, tels les paquets de mises à jour de routage. Etant donné qu'un paquet broadcast est transmis avec une adresse de prochain saut de l'adresse broadcast, la comparaison avec les commandes `dialer map` échouera. Si vous souhaitez que les paquets broadcast soient transmis vers des numéros de téléphone définis dans ces commandes, des commandes `dialer map` supplémentaires doivent spécifier l'adresse broadcast comme étant l'adresse de prochain saut, avec le même numéro de téléphone. Par exemple, vous pourriez ajouter les commandes `dialer map` suivantes :

```
dialer map ip 255.255.255.255 0118527351625  
dialer map ip 255.255.255.255 011653367085
```

Si l'interface est actuellement connectée à l'un de ces numéros de téléphone, et qu'elle reçoive un paquet broadcast IGRP, celui-ci sera donc transmis, puisqu'il correspond à une commande `dialer map` vers un numéro de téléphone déjà connecté. Si la connexion est déjà établie, les paquets intéressants ainsi que les paquets inintéressants seront envoyés. Si aucune connexion n'est établie, l'ajout des commandes `dialer map` ne permettra pas qu'un paquet IGRP envoyé à une adresse broadcast déclenche la numérotation, car les listes d'accès déterminent de toute façon qu'il est inintéressant.

NOTE

Dans l'exemple de configuration proposé à la section "Configuration d'une seule interface pour chaque site distant", la commande `dialer string` autorise que les paquets broadcast soient envoyés lorsque la ligne est connectée, car la chaîne de numérotation est associée à toutes les adresses de prochain saut qui ne possèdent pas de correspondance de numérotation.

Sites distants : appels entrants seulement

A l'exception de l'adresse IP et de la route par défaut, chaque site distant est configuré de façon identique, en tant que site répondant uniquement. L'exemple suivant illustre la configuration de Hong Kong :

```
interface serial 1
description interface to answer calls from San Francisco
ip address 128.10.200.65 255.255.255.192
dialer in-band
!
ip route 0.0.0.0 0.0.0.0 128.10.200.66
```

Le site répondant ne déconnectera pas l'appel, car c'est le site appelant qui s'en charge lorsque la ligne est inactive. Une route par défaut est définie vers le site central.

Configuration de plusieurs interfaces pour plusieurs sites distants

Lorsqu'une seule interface est utilisée avec plusieurs correspondances de numérotation, elle peut faire l'objet d'une contention. Cette contention déclenche un temporisateur d'accélération d'inactivité (*fast-idle timer*) qui maintient les lignes connectées pendant un laps de temps plus court que d'habitude, ce qui permet à d'autres destinations d'exploiter l'interface. Les groupes de rotation de numérotation (*dialer rotary group*) empêchent les situations de contention de se produire, en créant un groupe de plusieurs interfaces qui peuvent être utilisées pour établir des appels. Plutôt que d'assigner de façon statique une interface à une destination, les groupes de rotation de numérotation autorisent une assignation dynamique des interfaces aux numéros de téléphone. Lorsqu'un appel doit être effectué, une interface disponible est recherchée dans le groupe de rotation, afin d'y placer l'appel. Le temporisateur d'accélération d'inactivité est déclenché seulement lorsque toutes les interfaces du groupe sont occupées.

NOTE

La configuration suivante apparaît telle qu'elle devrait être entrée sur la ligne de commande. En regard au fonctionnement des groupes de rotation, le résultat de l'exécution d'une commande `write terminal` sur le routeur peut différer légèrement de ce qui est présenté ici.

Site central : appels sortants uniquement

La configuration suivante définit un groupe de rotation de numérotation sur le routeur du site central :

```

interface dialer 1
description rotary group for Hong Kong, Tokyo, and Singapore
ip address 128.10.200.66 255.255.255.192
ip address 128.10.202.66 255.255.255.192 secondary
ip address 128.10.204.66 255.255.255.192 secondary
dialer in-band
dialer wait-for-carrier-time 60
! associe Hong Kong à un numéro de téléphone
dialer map ip 128.10.200.65 0118527351625
! associe Singapour à un numéro de téléphone
dialer map ip 128.10.202.65 011653367085
! associe Tokyo à un numéro de téléphone
dialer map ip 128.10.204.65 0118127351625
pulse-time 1
dialer-group 1
!
interface serial 5
dialer rotary-group 1
!
interface serial 6
dialer rotary-group 1
!
router igrp 1
network 128.10.0.0
passive-interface dialer 1
redistribute static
!
! route vers Hong Kong
ip route 128.10.200.0 255.255.255.192 128.10.200.65
! route vers Singapour
ip route 128.10.202.0 255.255.255.192 128.10.202.65
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.204.65
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

Configuration des interfaces

La définition d'une interface de numérotation est la première étape de création d'un groupe de rotation de numérotation. Bien qu'une interface de numérotation ne soit pas une interface physique, elle supporte toutes les commandes qui peuvent être spécifiées pour une interface physique. Par exemple, les commandes répertoriées sous la commande `interface dialer` sont identiques à celles utilisées pour l'interface série physique 5, comme vous pouvez le voir à la section "Configuration d'une seule interface pour plusieurs sites distants". De plus, une commande `dialer map` supplémentaire a été ajoutée, afin d'associer l'adresse de prochain saut pour Tokyo au numéro de téléphone.

La commande `dialer rotary-group` place les interfaces série physiques 5 et 6 dans le groupe de rotation. N'importe laquelle de ces interfaces peut être utilisée pour appeler n'importe laquelle des destinations définies par la commande `interface dialer`.

Comme mentionné précédemment, lorsque vous examinez la configuration du routeur au moyen de la commande `write terminal`, son résultat peut différer légèrement de votre entrée. Par exemple, la commande `pulse-time` associée à l'interface de numérotation apparaîtra avec toutes les interfaces série qui ont été ajoutées à l'aide de la commande `dialer rotary-group`. Certaines informations de configuration associées à l'interface de numérotation sont transmises à toutes les interfaces du groupe de rotation.

Configuration du routage

La section de routage du fichier de configuration pour cet exemple n'est pas différente de celle de l'exemple présenté à la section "Configuration d'une seule interface pour plusieurs sites distants". Toutefois, si vous examinez la table de routage pour l'un des réseaux distants, à l'aide de la commande `show ip route` (par exemple, `show ip route 128.10.200.0`), vous remarquerez que l'interface de sortie à partir de laquelle les paquets ont été envoyés vers ce sous-réseau est l'interface de numérotation 1 (dialer 1). La véritable interface physique à partir de laquelle les paquets seront transmis n'est pas déterminée, tant que les étapes DDR décrites dans le paragraphe suivant n'ont pas été réalisées.

Avant qu'un paquet ne soit envoyé à partir de l'interface de numérotation, DDR contrôle ce paquet pour déterminer s'il est intéressant ou inintéressant, puis consulte la correspondance de numérotation. Ensuite, toutes les interfaces du groupe de rotation sont vérifiées, afin de déterminer si l'une d'elles est connectée au numéro de téléphone. Si une interface appropriée est détectée, le paquet est envoyé à partir de cette interface physique. Si aucune interface n'est détectée et que le paquet soit jugé intéressant, le groupe de rotation est analysé, afin d'y rechercher une interface disponible. La première interface disponible détectée est utilisée pour appeler le numéro de téléphone.

NOTE

Pour utiliser le routage dynamique, dans lequel deux des sites distants communiquent *via* le site central, les commandes `no ip split-horizon` et `passive-interface` doivent être supprimées.

Configuration de listes d'accès

Cette configuration utilise les mêmes listes d'accès que celles de l'exemple illustré à la section "Configuration d'une seule interface pour plusieurs sites distants". Une route par défaut est définie vers le site central.

Sites distants : appels entrants uniquement

A l'exception de l'adresse IP et de la route par défaut, chaque site distant est configuré de façon identique, en tant que site répondant uniquement. L'exemple suivant illustre la configuration de Hong Kong :

```
interface serial 1
description interface to answer calls from San Francisco
ip address 128.10.200.65 255.255.255.192
dialer in-band
!
ip route 0.0.0.0 0.0.0.0 128.10.200.66
```

Le site répondant ne déconnectera pas l'appel, car c'est le site appelant qui s'en charge lorsque la ligne est inactive.

Configuration du site central et des sites distants pour les appels entrants et sortants

Il est souvent plus pratique que les sites distants puissent appeler le site central selon les besoins des utilisateurs, plutôt que ces derniers dépendent du site central pour interroger les sites distants. Cette section examine les exemples de configuration suivants, dans lesquels le site central ainsi que les sites distants peuvent effectuer des appels :

- configuration d'une interface pour chaque site distant ;
- configuration d'une seule interface pour plusieurs sites distants ;
- configuration de plusieurs interfaces pour plusieurs sites distants.

Configuration d'une interface pour chaque site distant

Afin de pouvoir supporter les appels entrants et sortants à la fois sur le site central et sur les sites distants, au moyen d'une interface pour chaque site distant, chacun d'eux doit appeler l'interface spécifique sur le site central qui possède la chaîne de numérotation correspondant à son numéro de téléphone.

Site central : appels entrants et sortants

Dans l'exemple suivant, le site central situé à San Francisco est configuré pour les appels entrants et sortants. Une interface est configurée pour chaque site distant :

```
interface serial 5
description DDR connection to Hong Kong
ip address 128.10.200.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118527351625
pulse-time 1
dialer-group 1
!
interface serial 6
description DDR connection to Singapore
ip address 128.10.202.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 011653367085
pulse-time 1
dialer-group 1
!
interface serial 7
description DDR connection to Tokyo
ip address 128.10.204.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118127351625
pulse-time 1
dialer-group 1
!
router igrp 1
```

```

network 128.10.0.0
redistribute static
!
! route vers Hong Kong
ip route 128.10.200.0 255.255.255.192 128.10.200.65
! route vers Singapour
ip route 128.10.202.0 255.255.255.192 128.10.202.65
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.204.65
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

Sites distants : appels entrants et sortants

La configuration est la même pour chaque site distant. Elle définit une route par défaut vers le site central, et une chaîne de numérotation qui contient le numéro de téléphone du site central.

Hong Kong

Dans l'exemple suivant, le site distant situé à Hong Kong est configuré pour recevoir et établir des appels. Le fichier de configuration contient une chaîne de numérotation 14155551212, qui devrait permettre d'appeler l'interface série 5 à San Francisco :

```

interface serial 1
description DDR connection to San Francisco
ip address 128.10.200.65 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
!
ip route 128.10.0.0 255.255.0.0 128.10.200.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

Singapour

Dans l'exemple suivant, le site distant situé à Singapour est configuré pour recevoir et établir des appels. Le fichier de configuration contient une chaîne de numérotation 14155551213, qui devrait permettre d'appeler l'interface série 6 à San Francisco :

```

interface serial 1
description DDR connection to San Francisco
ip address 128.10.202.65 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551213
pulse-time 1
dialer-group 1
!
```

```

router igrp 1
network 128.10.0.0
!
ip route 128.10.0.0 255.255.0.0 128.10.202.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

Tokyo

Dans l'exemple suivant, le site distant situé à Tokyo est configuré pour recevoir et établir des appels. Le fichier de configuration contient une chaîne de numérotation 14155551214, qui devrait permettre d'appeler l'interface série 7 à San Francisco :

```

interface serial 1
description DDR connection to San Francisco
ip address 128.10.204.65 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551214
pulse-time 1
dialer-group 1
router igrp 1
network 128.10.0.0
!
ip route 128.10.0.0 255.255.0.0 128.10.204.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

Etant donné que tous les appels entrants sont supposés provenir du numéro de téléphone configuré avec la commande `dialer string`, il est important de configurer le site central et les sites distants correctement. Par exemple, si la chaîne de numérotation de Singapour utilise le numéro de téléphone employé par Hong Kong pour appeler le site central, les paquets du site central à destination de Hong Kong seront envoyés à Singapour, et cela chaque fois que Singapour appellera via l'interface de Hong Kong.

Configuration d'une seule interface pour plusieurs sites distants

Lorsque plusieurs sites appellent le site central, celui-ci doit utiliser un mécanisme d'authentification, à moins qu'il dispose d'une interface dédiée pour chaque appel entrant. En l'absence d'un mécanisme d'authentification, le routeur du site central ne possède aucun moyen d'identifier les sites auxquels il est connecté ; il n'est donc pas en mesure de garantir que d'autres appels n'ont pas lieu. L'encapsulation PPP avec CHAP (*Challenge Handshake Authentication Protocol*) ou PAP (*Password Authentication Protocol*) fournit un mécanisme qui permet d'identifier la partie appelante.

NOTE

Un routeur qui dispose d'un port RNIS intégré peut être capable d'utiliser la fonction d'identification de l'appelant. Etant donné que cette fonction n'est pas disponible partout, PPP avec CHAP fournit le mécanisme d'identification. Dans la version 9.21 de System Software, PAP peut être utilisé avec PPP plutôt que CHAP, bien qu'il soit moins sûr. La configuration de PAP serait légèrement différente de celle illustrée dans cette section pour CHAP.

Site central : appels entrants et sortants

Dans l'exemple suivant, le site central de San Francisco est configuré pour recevoir et établir des appels. Une seule interface est configurée pour plusieurs sites distants :

```

hostname SanFrancisco
interface serial 5
description DDR connection to Hong Kong and Singapore
ip address 128.10.200.66 255.255.255.192
ip address 128.10.202.66 255.255.255.192 secondary
encapsulation ppp
ppp authentication chap
dialer in-band
dialer wait-for-carrier-time 60
dialer map ip 128.10.200.65 name HongKong 0118527351625
dialer map ip 128.10.202.65 name Singapore 011653367085
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
passive-interface serial 5
redistribute static
!
! route vers Hong Kong
ip route 128.10.200.0 255.255.255.192 128.10.200.65
! route vers Singapour
ip route 128.10.202.0 255.255.255.192 128.10.202.65
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username HongKong password password1
username Singapore password password2

```

La commande `encapsulation ppp` active l'encapsulation PPP. La commande `ppp authentication chap` active l'authentification CHAP. De plus, une commande `username` est entrée pour chaque site distant qui effectue un appel. Cette commande définit le nom du routeur distant, ainsi qu'un mot de passe, qui lui est associé. Lorsque la commande `ppp authentication chap` est configurée, l'authentification doit être confirmée, sinon le trafic de réseau ne sera pas transmis.

La commande `dialer map` contient le nom d'hôte du routeur distant, et associe ce routeur à une adresse de prochain saut et à un numéro de téléphone. Lorsqu'un paquet est reçu pour un hôte sur le réseau 128.10.200.0, il est routé vers une adresse de prochain saut 128.10.200.65, via l'interface série 5. Le paquet est comparé aux listes d'accès, puis son adresse de prochain saut est comparée aux commandes `dialer map` pour l'interface série 5.

Si le paquet est intéressant et qu'une connexion avec le numéro de téléphone spécifié dans la commande `dialer map` soit déjà active sur l'interface, le temporisateur d'inactivité est réinitialisé. Lorsqu'une correspondance est détectée, DDR vérifie l'interface afin de déterminer si elle est connectée au numéro de téléphone qui correspond à l'adresse de prochain saut. La comparaison avec le numéro de téléphone n'est utile que si le routeur a effectué l'appel, ou si le numéro de téléphone a été reçu via l'identification de l'appelant sur un routeur RNIS. A l'aide de CHAP et du mot clé `name` inclus dans la commande `dialer map`, le numéro de téléphone ainsi que le nom fourni pour une adresse de prochain saut donnée sont tous deux comparés aux noms de routeurs déjà connectés.

De cette façon, on évite de générer des appels vers des destinations pour lesquelles des connexions sont déjà établies.

Sites distants : appels entrants et sortants

Dans les exemples de configuration suivants, les sites distants sont configurés pour établir et recevoir des appels vers, ou à partir, d'une seule interface sur le site central :

Hong Kong

La configuration suivante permet à Hong Kong d'établir et de recevoir des appels vers, et à partir, du site central de San Francisco :

```
hostname HongKong
interface serial 1
description DDR connection to SanFrancisco
ip address 128.10.200.65 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
!
ip route 128.10.0.0 255.255.0.0 128.10.200.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password1
```

Singapour

La configuration suivante permet à Singapour d'établir et de recevoir des appels vers, et à partir, du site central de San Francisco :

```
hostname Singapore
interface serial 1
description DDR connection to San Francisco
ip address 128.10.202.65 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
ip route 128.10.0.0 255.255.0.0 128.10.202.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password2
```

A l'inverse du site central, les sites distants ne contiennent pas la commande `ppp authentication chap`. En effet, seul un site, le site central, appelle les sites distants. Si un seul site appelle, DDR suppose que l'appel provient du numéro défini avec la commande `dialer string`. Par conséquent, la commande `ppp authentication chap` n'est pas nécessaire.

NOTE

Si les sites distants utilisent les commandes `dialer map` au lieu de `dialer string`, la commande `ppp authentication chap` est nécessaire, et les commandes `dialer map` requièrent le mot clé `name`. Lorsque la commande `dialer map` est utilisée, cela suppose que plusieurs sites peuvent appeler ou être appelés.

Notez également que les sites distants possèdent une entrée `username` pour le routeur de San Francisco, et que ce dernier contient les mots de passe de `username` pour Singapour et Hong Kong.

Configuration de plusieurs interfaces pour plusieurs sites distants

Les configurations présentées dans cette section sont semblables à celles vues plus haut, à la section "Configuration d'une seule interface pour plusieurs sites distants". Le type d'encapsulation défini est PPP. L'authentification CHAP est nécessaire.

Site central : appels entrants et sortants

L'exemple suivant configure le routeur de site central pour les appels entrants et sortants sur plusieurs interfaces, vers plusieurs sites distants :

```
hostname SanFrancisco
interface dialer 1
description rotary group for Hong Kong, Tokyo, and Singapore
ip address 128.10.200.66 255.255.255.192
ip address 128.10.202.66 255.255.255.192 secondary
ip address 128.10.204.66 255.255.255.192 secondary
encapsulation ppp
ppp authentication chap
dialer in-band
dialer wait-for-carrier-time 60
dialer map ip 128.10.200.65 name HongKong 0118527351625
dialer map ip 128.10.202.65 name Singapore 011653367085
dialer map ip 128.10.204.65 name Tokyo 0118127351625
pulse-time 1
dialer-group 1
!
interface serial 5
dialer rotary-group 1
!
interface serial 6
dialer rotary-group 1
!
router igrp 1
network 128.10.0.0
passive-interface dialer 1
redistribute static
! route vers Hong Kong
ip route 128.10.200.0 255.255.255.192 128.10.200.65
! route vers Singapour
```

```

ip route 128.10.202.0 255.255.255.192 128.10.202.65
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.204.65
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username HongKong password password1
username Singapore password password2
username Tokyo password password3

```

Sites distants : appels entrants et sortants

Dans les exemples de configuration suivants, les sites distants sont configurés pour établir et recevoir des appels vers, et à partir, de plusieurs interfaces sur le site central. Tous ces sites appellent le même numéro de téléphone. Sur le site de San Francisco, ce même numéro de téléphone entraînera une connexion soit sur l'interface série 5, soit sur l'interface série 6. Cette fonctionnalité est fournie par l'opérateur téléphonique.

Hong Kong

La configuration suivante permet à Hong Kong d'établir et de recevoir des appels vers, et à partir, du site central de San Francisco :

```

hostname HongKong
interface serial 1
description DDR connection to SanFrancisco
ip address 128.10.200.65 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
router igrp 1
network 128.10.0.0
ip route 128.10.0.0 255.255.0.0 128.10.200.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password1

```

Singapour

La configuration suivante permet à Singapour d'établir et de recevoir des appels vers, et à partir, du site central de San Francisco :

```

hostname Singapore
interface serial 1
description DDR connection to San Francisco
ip address 128.10.202.65 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212

```

```

pulse-time 1
dialer-group 1
router igrp 1
network 128.10.0.0
ip route 128.10.0.0 255.255.0.0 128.10.202.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password2

```

Tokyo

La configuration suivante permet à Tokyo d'établir et de recevoir des appels vers, et à partir, du site central de San Francisco :

```

hostname Tokyo
interface serial 1
description DDR connection to San Francisco
ip address 128.10.204.65 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
router igrp 1
network 128.10.0.0
ip route 128.10.0.0 255.255.0.0 128.10.204.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password3

```

Les sites distants n'utilisent pas la commande `ppp authentication chap car`, comme nous l'avons vu, le site central est le seul à appeler les sites distants. Lorsqu'un seul site est appelant, DDR suppose que l'appel provient du numéro défini avec la commande `dialer string` ; la commande `ppp authentication chap` est donc inutile. Néanmoins, si les sites distants utilisent les commandes `dialer map` au lieu de `dialer string`, la commande **ppp authentication chap** est nécessaire, et les commandes `dialer map` requièrent le mot clé `name`.

Vous pouvez également constater que chaque site distant possède une entrée `username San Francisco` qui contient le même mot de passe que celui utilisé par le site central pour identifier le site distant.

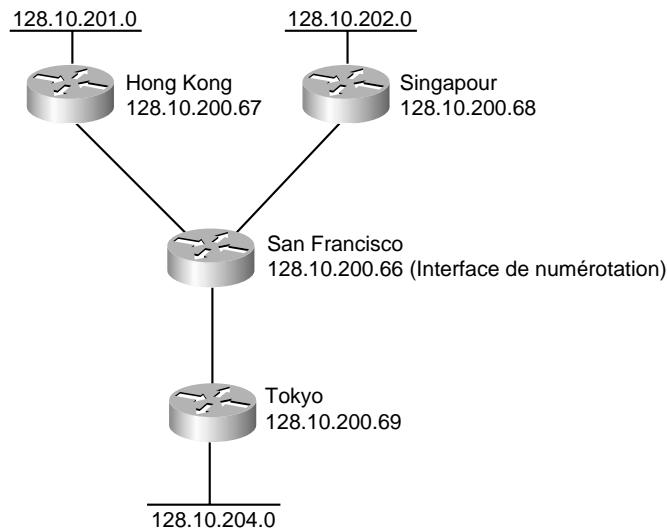
Configuration des sites distants pour les appels sortants

On rencontre souvent une configuration dans laquelle le site central reçoit les appels des sites distants, mais n'effectue pas d'appels sortants.

Configuration de plusieurs interfaces pour plusieurs sites distants

Sur une topologie en étoile, tous les routeurs distants peuvent avoir leurs interfaces série sur le même sous-réseau que l'interface du site central (voir Figure 19.2).

Figure 19.2
Sites distants appellants
(topologie en étoile).



Site central : appels entrants uniquement

L'exemple suivant configure le routeur du site central, afin qu'il accepte les appels entrants sur plusieurs interfaces :

```

hostname SanFrancisco
interface dialer 1
description rotary group for inbound calls
ip address 128.10.200.66 255.255.255.192
encapsulation ppp
ppp authentication chap
dialer in-band
dialer wait-for-carrier-time 60
dialer map ip 128.10.200.67 name HongKong
dialer map ip 128.10.200.68 name Singapore
dialer map ip 128.10.200.69 name Tokyo
pulse-time 1
dialer-group 1
!
interface serial 5
dialer rotary-group 1
!
interface serial 6
dialer rotary-group 1
!
router igrp 1
network 128.10.0.0
  
```

```

passive-interface dialer 1
redistribute static
! route vers Hong Kong
ip route 128.10.201.0 255.255.255.192 128.10.200.67
! route vers Singapour
ip route 128.10.202.0 255.255.255.192 128.10.200.68
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.200.69
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username HongKong password password1
username Singapore password password2
username Tokyo password password3

```

Sites distants : appels sortants uniquement

Dans les configurations suivantes, les sites distants sont configurés afin d'effectuer des appels vers plusieurs interfaces du site central. Cet exemple suppose qu'un seul numéro de téléphone sur le site central permet de joindre n'importe laquelle des deux interfaces série disponibles en entrée (interface série 5 et interface série 6).

Hong Kong

La configuration suivante permet à Hong Kong d'appeler le site central de San Francisco :

```

hostname HongKong
interface ethernet 0
ip address 128.10.201.1 255.255.255.192
interface serial 1
description DDR connection to SanFrancisco
ip address 128.10.200.67 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
router igrp 1
network 128.10.0.0
ip route 128.10.0.0 255.255.0.0 128.10.200.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password1

```

Singapour

La configuration suivante permet à Singapour d'appeler le site central de San Francisco :

```

hostname Singapore
interface ethernet 0
ip address 128.10.202.1 255.255.255.192
interface serial 1
description DDR connection to San Francisco

```

```

ip address 128.10.200.68 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
router igrp 1
network 128.10.0.0
ip route 128.10.0.0 255.255.0.0 128.10.200.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password2

```

Tokyo

La configuration suivante permet à Tokyo d'appeler le site central de San Francisco :

```

hostname Tokyo
interface ethernet 0
ip address 128.10.204.1 255.255.255.192
interface serial 1
description DDR connection to San Francisco
ip address 128.10.200.69 255.255.255.192
encapsulation ppp
dialer in-band
dialer wait-for-carrier-time 60
dialer string 14155551212
pulse-time 1
dialer-group 1
router igrp 1
network 128.10.0.0
ip route 128.10.0.0 255.255.0.0 128.10.200.66
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101
!
username SanFrancisco password password3

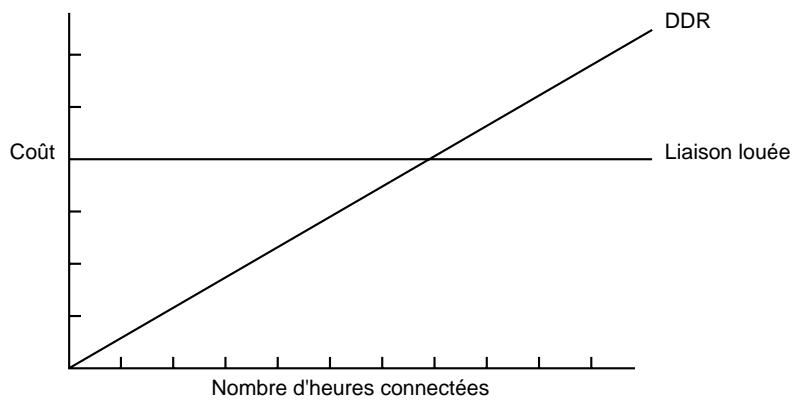
```

DDR : la solution de secours pour des liaisons louées

DDR permet d'activer rapidement une connexion WAN à l'aide des lignes téléphoniques analogiques existantes. Avec DDR, vous pouvez, en outre, réaliser des économies considérables, car les lignes sont exploitées sur la base de besoins ponctuels, alors que les liaisons louées entraînent des frais, même lorsqu'elles ne sont pas utilisées. Il existe néanmoins certaines situations où les liaisons louées peuvent être avantageuses.

La Figure 19.3 montre que lorsqu'une connexion doit être maintenue au-delà d'un certain nombre d'heures par jour, une liaison louée devient plus rentable qu'une ligne DDR. En outre, le coût des lignes DDR est variable, c'est-à-dire qu'il est difficile de prévoir leur coût mensuel, étant donné que les utilisateurs peuvent générer du trafic à tout moment.

Figure 19.3
Transition DDR-liaison louée.



Avec des liaisons louées pour liaisons principales, vous pouvez continuer à utiliser les lignes commutées en tant que solution de secours, au moyen des méthodes suivantes :

- routes statiques flottantes et DDR ;
- numérotation DTR et numérotation V.25bis.

Routes statiques flottantes

Les routes statiques flottantes (*floating static routes*) sont des routes statiques qui présentent une distance administrative supérieure à celle des routes dynamiques. Des distances administratives peuvent être configurées sur une route statique, de façon que celle-ci soit moins tentante qu'une route dynamique. De cette manière, la route statique n'est pas utilisée lorsqu'une route dynamique est disponible. Toutefois, si cette dernière est perdue, la route statique peut prendre le relais, et le trafic peut être envoyé sur cette route alternative. Si celle-ci est assurée par une interface DDR, DDR peut être utilisé en tant que mécanisme de secours.

Site central

L'exemple suivant décrit la configuration d'un site central, qui utilise des liaisons louées pour la connectivité principale, et DDR en tant que solution de secours :

```
interface serial 1
description Leased connection to Hong Kong
ip address 128.10.200.66 255.255.255.192
!
interface serial 2
description leased connection to Singapore
ip address 128.10.202.66 255.255.255.192
!
interface serial 5
description backup DDR connection to Hong Kong
ip address 128.10.200.130 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118527351625
pulse-time 1
```

```

dialer-group 1
!
interface serial 6
description backup DDR connection to Singapore
ip address 128.10.202.130 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 011653367085
pulse-time 1
dialer-group 1
!
interface serial 7
description DDR connection to Tokyo
ip address 128.10.204.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118127351625
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
redistribute static
!
! route vers Hong Kong avec distance administrative
ip route 128.10.200.0 255.255.255.192 128.10.200.129 150
! route vers Singapour avec distance administrative
ip route 128.10.202.0 255.255.255.192 128.10.202.129 150
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.204.65
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

Les interfaces série 1 et 2 sont utilisées en tant que liaisons louées vers Hong Kong et Singapour. Les interfaces série 5 et 6 représentent respectivement les solutions de secours des interfaces série 1 et 2 ; l'interface série 7 est utilisée pour DDR vers Tokyo.

Sites distants

Chaque site distant dispose d'une liaison louée en tant que liaison principale, et de DDR en tant que solution de secours. Voici un exemple :

```

interface serial 0
description leased line from San Francisco
ip address 128.10.200.65 255.255.255.192
!
interface serial 1
description interface to answer backup calls from San Francisco
ip address 128.10.200.129 255.255.255.192
dialer in-band
!
router igrp 1
network 128.10.0.0
! route vers San Francisco avec distance administrative
ip route 128.10.0.0 255.255.0.0 128.10.200.130 150

```

La première interface série est la liaison louée ; la seconde répond aux appels en provenance du site central, au cas où ce dernier aurait besoin d'utiliser DDR en tant que méthode alternative.

Routes statiques flottantes sur interfaces partagées

La configuration du site central requiert un grand nombre de ports série, car chaque port principal dispose d'un port de secours. C'est le prix à payer pour pouvoir bénéficier d'une véritable redondance, mais, dans la plupart des cas, une seule interface (ou un ensemble d'interfaces) peut représenter une solution de secours partagée pour un ensemble de liaisons principales. La configuration suivante illustre comment définir une seule interface pour le secours de toutes les liaisons principales :

```

interface serial 1
description Leased connection to Hong Kong
ip address 128.10.200.66 255.255.255.192
!
interface serial 2
description leased connection to Singapore
ip address 128.10.202.66 255.255.255.192
!
interface serial 5
description backup DDR connection for all destinations except Tokyo
ip address 128.10.200.130 255.255.255.192
ip address 128.10.202.130 255.255.255.192 secondary
dialer in-band
dialer wait-for-carrier-time 60
! associe Hong Kong à un numéro de téléphone
dialer map ip 128.10.200.129 0118527351625
! associe Singapour à un numéro de téléphone
dialer map ip 128.10.202.129 011653367085
pulse-time 1
dialer-group 1
!
interface serial 7
description DDR connection to Tokyo
ip address 128.10.204.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118127351625
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
passive-interface serial 5
redistribute static
!
! route vers Hong Kong avec distance administrative
ip route 128.10.200.0 255.255.255.192 128.10.200.129 150
! route vers Singapour avec distance administrative
ip route 128.10.202.0 255.255.255.192 128.10.202.129 150
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.204.65
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 255.255.255.255 0.0.0.0
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
dialer-list 1 list 101

```

L'interface série 5 est l'interface de secours DDR pour toutes les destinations. Elle est configurée avec plusieurs adresses IP pour le routage. Les commandes `dialer map` associent les adresses de prochain saut aux numéros de téléphone, pour chacune des destinations. Si une route dynamique est perdue, la route statique flottante prend le relais. L'adresse de prochain saut envoie les paquets vers l'interface série 5, sur laquelle les commandes `dialer map` placent l'appel.

Si deux lignes principales sont défaillantes au même moment, il y aura conflit d'utilisation en ce qui concerne l'interface série 5. Dans ce cas, il est possible que le temporisateur d'accélération d'inactivité déconnecte les appels. Si l'interface série 5 se trouve en constante utilisation, l'une des liaisons principales sera déconnectée, et les paquets seront supprimés. Le fait que la route de secours soit indisponible n'est pas communiqué, car il n'existe aucun moyen d'annoncer que l'une des deux adresses IP sur l'interface est indisponible. Les problèmes de conflit d'utilisation peuvent être évités en implémentant un groupe de rotation de numérotation.

Liaisons louées et secours commuté

Cette section décrit comment utiliser les deux méthodes suivantes, en tant que solutions de secours commuté avec des liaisons louées :

- numérotation DTR ;
- numérotation V.25bis.

Numérotation DTR

La version 8.3 de System Software a introduit une fonctionnalité de secours commuté (*dial backup*). Bien que le secours commuté impose parfois davantage de restrictions que les routes statiques flottantes, il peut être utilisé en cas de non-disponibilité des modems V.25bis, ou si des protocoles qui ne supportent pas les routes statiques flottantes sont exécutés.

Site central

Le secours commuté nécessite que les modems effectuent un appel lors du déclenchement du signal DTR. Le numéro de téléphone est configuré au niveau du modem, ou d'un autre équipement de communication. Ce numéro est appelé lorsque le signal DTR est déclenché ; l'appel est déconnecté une fois que le signal est désactivé. La configuration suivante illustre comment tirer parti du secours commuté et de la numérotation DTR :

```
interface serial 1
description Leased connection to Hong Kong
ip address 128.10.200.66 255.255.255.192
backup interface serial 4
backup delay 0 20
!
interface serial 2
description leased connection to Singapore
ip address 128.10.202.66 255.255.255.192
backup interface serial 5
backup delay 0 20
!
interface serial 4
description backup connection for Hong Kong
ip address 128.10.200.67 255.255.255.192
```

```

pulse-time 10
!
interface serial 5
description backup connection for Singapore
ip address 128.10.202.67 255.255.255.192
pulse-time 10
!
interface serial 7
description DDR connection to Tokyo
ip address 128.10.204.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118127351625
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0

```

Cette solution requiert un port série par liaison principale. Etant donné que les ports de secours sont placés sur le même sous-réseau que les ports série principaux, aucune route statique n'est nécessaire. La commande `backup delay` sert à spécifier le temps d'attente avant l'activation de la ligne de secours, suite à la défaillance de la liaison principale, ainsi que le délai d'attente avant la désactivation de la ligne de secours, après rétablissement de la liaison principale. Dans ce cas, la liaison principale sera active pendant 20 secondes avant la désactivation de la ligne de secours. Ce délai peut donc provoquer des problèmes d'instabilité de route (*flapping*) lors du rétablissement de la ligne principale.

Sites distants

Les routes statiques flottantes ne sont pas nécessaires pour les sites distants. L'adresse IP de l'interface de secours doit se trouver sur le même sous-réseau que l'interface principale. L'exemple suivant illustre la configuration du routeur de Hong Kong. L'interface série 0 correspond à la liaison louée, et l'interface série 1 répond aux appels en tant que solution de secours :

```

interface serial 0
description leased line from San Francisco
ip address 128.10.200.65 255.255.255.192
!
interface serial 1
description interface to answer backup calls from San Francisco
ip address 128.10.200.68 255.255.255.192
!
router igrp 1
network 128.10.0.0

```

Numérotation V.25 bis

La fonction de numérotation V.25bis convient mieux que la numérotation DTR lorsque plusieurs numéros de téléphone sont requis. Avec DTR, la plupart des dispositifs appelleront un seul numéro. Avec V.25bis, le routeur peut tenter d'appeler plusieurs autres numéros, si le premier ne répond pas. La configuration suivante illustre la numérotation V.25bis :

```

interface serial 1
description Leased connection to Hong Kong
ip address 128.10.200.66 255.255.255.192

```

```
backup interface serial 4
backup delay 0 20
!
interface serial 2
description leased connection to Singapore
ip address 128.10.202.66 255.255.255.192
backup interface serial 5
backup delay 0 20
!
interface serial 4
description backup connection for Hong Kong
ip address 128.10.200.67 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer map IP 128.10.200.68 0118527351625
dialer map IP 128.10.200.68 0118527351872
dialer-group 1
pulse-time 1
!
interface serial 5
description backup connection for Singapore
ip address 128.10.202.67 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 011653367085
dialer-group 1
pulse-time 1
!
interface serial 7
description DDR connection to Tokyo
ip address 128.10.204.66 255.255.255.192
dialer in-band
dialer wait-for-carrier-time 60
dialer string 0118127351625
pulse-time 1
dialer-group 1
!
router igrp 1
network 128.10.0.0
redistribute static
!
! route vers Hong Kong
ip route 128.10.200.0 255.255.255.192 128.10.200.68
! route vers Singapour
ip route 128.10.202.0 255.255.255.192 128.10.202.68
! route vers Tokyo
ip route 128.10.204.0 255.255.255.192 128.10.204.65
!
dialer-list 1 protocol IP PERMIT
```

Plusieurs numéros de téléphone sont configurés pour l'interface série 4. Les deux commandes `dialer map` utilisent la même adresse de prochain saut. Le logiciel tente tout d'abord d'appeler le numéro de téléphone spécifié dans la première commande `dialer map`. Si l'appel n'aboutit pas — c'est-à-dire si aucune connexion n'est établie avant l'expiration du délai d'attente du signal de porteuse (*wait-for-carrier timer*) —, le second numéro est composé. Chacune des autres interfaces de secours utilise une chaîne de numérotation pour le numéro de téléphone de secours. Lorsque V.25bis est utilisé avec le secours commuté, la commande `dialer-list protocol`, montrée à

l'exemple précédent, devrait être utilisée. La liste de numérotation déclare que tout le trafic IP est intéressant, et déclenchera par conséquent la numérotation. Les mises à jour de routage sont incluses. Lorsqu'une ligne série est utilisée en tant que solution de secours, c'est normalement l'état de la liaison principale, et non le temporisateur d'accélération d'inactivité, qui détermine quand déconnecter l'appel.

Scripts de dialogue (chat script)

L'exemple suivant présente la configuration de deux scripts de dialogue sur un routeur RTP (nommé sanjose). Un script de numérotation (*dial*) est utilisé pour appeler le modem qui est connecté au routeur, et un script d'ouverture de session (*login*) est utilisé pour se connecter au routeur. La chaîne de numérotation 5555555 correspond au numéro du modem connecté au routeur RTP ; l'adresse IP 10.2030.1 est celle du routeur :

```
chat-script dial ABORT ERROR "" "AT Z" OK "ATDT \T" TIMEOUT 60 CONNECT \c
chat-script login ABORT invalid TIMEOUT 30 name: sasad word: sraza ">"
    "slip default"

interface async 10
dialer in-band
dialer map ip 10.20.30.1 modem-script dial system-script login 5555555
```

Création et implémentation de scripts de dialogue

Dans l'exemple de configuration suivant, une ligne aléatoire est utilisée en cas de trafic dense. Le code exécuté pour la numérotation tentera de localiser un script qui corresponde à la fois au script de modem et au script système RTP. S'il ne parvient pas à les localiser, un message spécifiant qu'aucun script de dialogue n'a été trouvé ("no matching chat script found") sera envoyé à l'utilisateur :

```
interface dialer 1
! Définition des interfaces de rotation de sanjose
dialer rotary-group 1
! Utilisation du script générique de sanjose
dialer map ip 10.10.10.10 modem-script sanjose system-script rtp 5555555
```

Dans le script suivant, les guillemets représentent une chaîne nulle, et \r représente un retour à la ligne :

```
" " \r "name:" "your_name" "ord:" "your_password" ">" "slip default"
```

Dans la configuration suivante, des scripts de dialogue séparés sont définis pour les lignes connectées aux modems Best Data et US Robotics :

```
! Les modems Best Data sont connectés aux lignes 1 à 5
line 1 5
modem chat-script bestdata.*
! Les modems US Robotics sont connectés aux lignes 6 à 9
line 6 9
modem chat-script usrobotics.*
```

Scripts de dialogue et correspondances de numérotation

Dans la configuration suivante, deux scripts de dialogue, un script de numérotation et un script d'ouverture de session, sont définis. La commande *dialer in-band* configure l'interface 0 pour DDR ; la commande *dialer map* compose le numéro 5555555, après que les scripts spécifiés ont été localisés.

```
chat-script dial ABORT ERROR "" "AT Z" OK "ATDT \T" TIMEOUT 60 CONNECT \c
chat-script login ABORT invalid TIMEOUT 30 name: sasad word: sraza ">"
    "slip default"

interface async 0
dialer in-band
dialer map ip 10.10.10.10 modem-script dial system-script login 55555555
```

Lorsqu'un paquet est reçu pour l'adresse 10.10.10.10, la première chose qui se produit est la localisation du script de dialogue dial. Le code suivant explique le traitement réalisé pour chaque séquence attendre-envoyer dans ce script de modem :

```
ABORT ERROR: Si "ERROR" est rencontré, terminer exécution du script.

" " "AT Z": Envoyer une commande "AT Z" au modem sans rien attendre d'autre. Les
↳guillemets sont utilisés pour autoriser un espace dans la chaîne d'envoi.

OK "ATDT \T: Attendre "OK." Envoyer "ATDT 5555555.

TIMEOUT 60: Attendre pendant 60 secondes la chaîne suivante. Ce délai peut
↳différer en fonction du modem.

CONNECT \c: Attendre "connect", mais ne rien envoyer d'autre, \c signifiant
↳effectivement rien. Des guillemets " " auraient signifié une chaîne nulle
↳suivie d'un retour à la ligne.
```

Une fois que le script de modem a été exécuté avec succès, la seconde étape consiste à exécuter le script d'ouverture de session, login. Le code suivant explique le traitement réalisé pour chaque séquence attendre-envoyer dans ce script :

```
ABORT invalid: Si le message "invalid username or password" ("nom d'utilisateur
↳ou mot de passe invalide") est affiché, terminer exécution du script.

TIMEOUT 30: Attendre 15 secondes.

name: sasad: Rechercher "name:" et envoyer "sasad.".

word: sraza: Attendre "word:" et envoyer le mot de passe qui est sraza.

">" "slip default": Attendre l'invite ts et basculer en mode slip avec son
↳adresse par défaut.
```

Résumé

Ainsi que l'a montré cette étude de cas, il existe de nombreuses façons d'utiliser le routage par ouverture de ligne à la demande ou DDR (*Dial-on Demand Routing*), à la fois pour l'accès principal et l'accès de secours. Les sites distants peuvent effectuer des appels, ou en recevoir, ou bien les deux. De plus, la souplesse de fonctionnement peut être améliorée, grâce à l'implémentation de groupes de rotation de numérotation. Ce chapitre a également décrit brièvement l'utilisation et l'implémentation de scripts de dialogue.

20

Evolutivité du routage DDR

Par Salman Asad

L'étude de cas que nous présentons ici décrit la conception d'un réseau d'accès, qui autorise un grand nombre de sites distants à communiquer avec un réseau de site central existant. Les sites distants sont constitués de réseaux locaux (LAN) qui supportent plusieurs stations de travail. Celles-ci exécutent un logiciel de traitement transactionnel, afin d'accéder à une base de données, située sur le site central. Les objectifs suivants ont guidé la conception de la partie accès du réseau :

- Le réseau existant ne peut pas être modifié pour gérer l'accès des sites distants.
- Le site central doit pouvoir se connecter à n'importe quel site distant, à tout moment, et inversement.
- Lorsqu'un choix entre plusieurs techniques doit être fait, la plus rentable est retenue.
- La conception doit être suffisamment souple pour s'adapter à l'augmentation du nombre de sites distants.

Conception du réseau

Les considérations suivantes influent sur la conception du réseau :

- modèles de trafic ;
- choix du média ;
- protocoles requis.

Modèles de trafic

Une analyse du trafic par anticipation indique que chaque site distant appellera le site central environ quatre fois par heure, tout au long de la journée de travail. Ce type de trafic donne la possibilité de réaliser des économies au niveau du site central, en fournissant une ligne téléphonique pour environ 2,5 sites distants, ce qui donne 48 lignes au total. Pour répartir équitablement les appels sur les 48 lignes, les sites distants se connectent par l'intermédiaire d'un groupe de recherche de lignes (*hunt group*). Le groupe de recherche de lignes présente un avantage : tous les routeurs distants composent le même numéro de téléphone afin d'accéder au site central, ce qui rend la configuration des routeurs de sites distants plus facile à maintenir.

Pour terminer une transaction initiée par un site distant, le site central doit parfois appeler le site en question, peu de temps après qu'il s'est déconnecté du site central. Pour cela, le réseau d'accès doit converger rapidement. Le site central appelle également les sites distants périodiquement, afin de mettre à jour le logiciel de traitement transactionnel sur les stations distantes.

Choix du média

Les concepteurs choisissent une technologie d'accès commuté asynchrone sur le réseau téléphonique public commuté (RTC) pour les raisons suivantes :

- **Disponibilité.** Le réseau RTC est disponible au niveau de tous les sites distants. Certains réseaux, tels le Frame Relay et RNIS (Réseau numérique à intégration de services), ne sont pas accessibles sur tous les sites distants.
- **Bande passante.** Le logiciel de traitement transactionnel génère une faible quantité de trafic entre les sites distants et le site central. Pour ce type d'application à faible trafic, la bande passante fournie par les liaisons asynchrones est acceptable. De façon occasionnelle, le site central appelle les sites distants afin de maintenir à jour le logiciel de traitement transactionnel sur les clients distants. Cette activité se produira la nuit (en l'absence d'activité du logiciel), afin que la bande passante disponible pour les liaisons asynchrones soit suffisante.
- **Coût.** Eu égard aux faibles exigences en matière de bande passante, le coût d'installation et de fonctionnement d'un équipement Frame Relay ou RNIS ne serait pas justifié.

NOTE

Bien que le réseau décrit dans cette étude de cas utilise une technique de numérotation asynchrone sur le réseau RTC, la plupart des concepts, tels que l'adressage et les stratégies de routage, s'appliquent également lors de l'adaptation d'autres technologies par circuits commutés (tel RNIS).

Protocoles requis

Les stations distantes exécutent une application de traitement transactionnel, qui utilise TCP/IP (*Transmission Control Protocol/Internet Protocol*) afin de se connecter à la base de données située sur le site central. Elles n'ont aucun besoin d'exécuter un autre protocole de la couche réseau. Par conséquent, le choix le plus rentable pour un routeur de site distant est un routeur qui fournit une interface Ethernet, ainsi qu'une interface asynchrone, et qui supporte le protocole RIP (*Routing Information Protocol*).

Solution matérielle

Un serveur d'accès Cisco AS5100 est installé sur le site central afin de fournir 48 interfaces asynchrones. Etant donné qu'il est constitué de trois cartes de serveur d'accès fondées sur le serveur d'accès Cisco 2511, il équivaut en fait à trois serveurs Cisco 2511. Chaque carte de serveur d'accès fournit 16 lignes asynchrones, équipées chacune d'un modem U.S. Robotics Courier intégré.

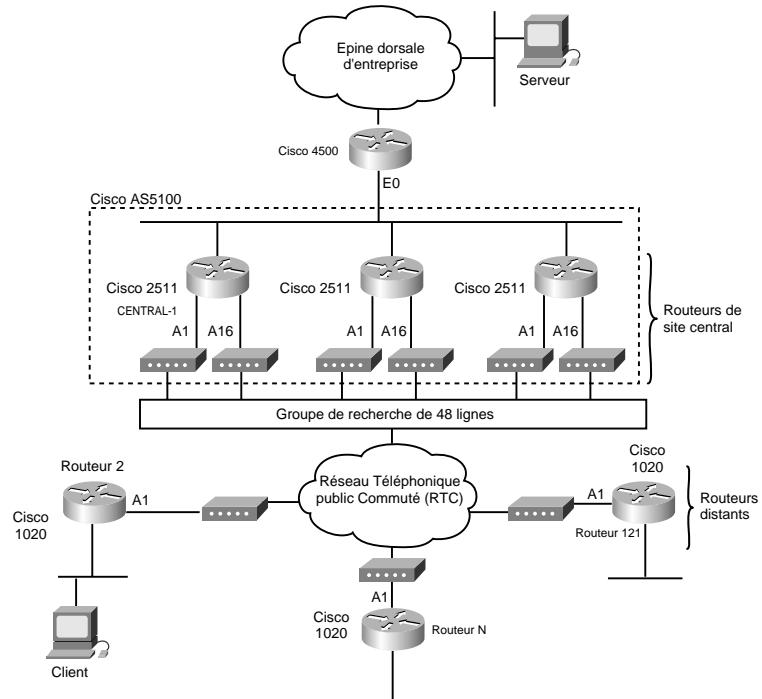
NOTE

Pour les besoins de cette étude de cas, nous nous référerons aux trois cartes du serveur d'accès Cisco AS5100 en tant que routeurs d'accès de site central.

Chaque site distant est doté d'un routeur Cisco 1020, qui fournit une seule interface de ligne asynchrone, ainsi qu'une interface Ethernet pour la connexion au réseau local distant. Ce routeur exécute un ensemble limité de protocoles, dont TCP/IP et RIP. Des modems U.S. Robotics Sportser assurent la connectivité des sites distants. Le fait d'utiliser une même marque de modem sur tout le réseau d'accès simplifie la définition des scripts de dialogue ainsi que la configuration des modems, et en facilite également la gestion.

Un routeur Cisco 4500 contrôle le routage entre la nouvelle zone d'accès du réseau et l'épine dorsale. Plus précisément, lorsque des hôtes situés de l'autre côté de l'épine dorsale souhaitent se connecter à un site distant, ce routeur leur garantit une connexion *via* le routeur d'accès de site central qui présente le meilleur chemin. La Figure 20.1 illustre la topologie de la portion d'accès du réseau.

Figure 20.1
Topologie d'accès distant.



Solution logicielle

La configuration des routeurs d'accès de site central et des routeurs de sites distants doit fournir les informations suivantes :

- authentification ;
- adressage de la couche réseau ;
- stratégie de routage.

Authentification

Le trafic entre les sites distants et le site central contient des informations confidentielles. Pour cette raison, l'authentification est un souci majeur. Les sites peuvent s'authentifier de deux façons :

- **Authentification PPP (*Point-to-Point Protocol*)**. Les protocoles PAP (*Password Authentication Protocol*) ou CHAP (*Challenge Handshake Authentication Protocol*) peuvent être utilisés.
- **Authentification d'ouverture de session**. Le routeur demande au routeur distant appelant de fournir un nom d'hôte et un mot de passe. Le routeur distant ouvre ensuite une session, puis lance PPP.

Dans les deux cas, la base de données des noms d'utilisateurs et des mots de passe peut être stockée localement, ou sur un serveur TACACS (*Terminal Access Controller Access Control System*) étendu. TACACS+ assure une gestion centralisée des mots de passe pour tous les routeurs d'accès de site central, et fournit des informations détaillées de comptabilité des connexions entrantes et sortantes relatives aux sites distants.

Cette conception de réseau implique la mise en œuvre de l'authentification d'ouverture de session, car elle permet aux sites distants d'annoncer leur adresse IP aux routeurs d'accès de site central, tel que décrit à la prochaine section : "Adressage de la couche réseau". PPP pourrait être lancé automatiquement si TACACS+ était employé pour supporter l'assignation d'adresses IP par utilisateur.

Adressage de la couche réseau

L'adressage de la couche réseau est accompli au moyen de deux méthodes :

- assignation d'adresses de sous-réseau ;
- adresses de prochain saut.

Assignation d'adresses de sous-réseau

Etant donné que les routeurs distants et les routeurs d'accès de site central n'ont pas besoin de se connecter à l'Internet, ils utilisent des adresses RFC 1597. L'adresse de Classe B 172.16.0.0 est employée pour l'ensemble de la portion d'accès du réseau ; des adresses de Classe C équivalentes sont assignées aux routeurs distants. Chaque sous-réseau reçoit une adresse de Classe C équivalente (172.16.x.0, avec un masque de 255.255.255.0), ce qui facilite la gestion de l'adressage. Le réseau 172.16.1.0 est réservé à l'adressage ultérieur du nuage de numérotation, si besoin. Le nuage de numérotation est défini comme étant un sous-réseau, auquel sont connectées toutes les interfaces asynchrones.

A l'origine, le nuage de numérotation ne possède pas d'adresse dédiée. S'il devait en avoir une dans le futur, les questions suivantes devraient être prises en considération :

- Le nuage de numérotation peut-il utiliser le même masque de sous-réseau que les sites distants ? Dans la négative, le support des masques de sous-réseau de longueur variable (VLSM, *Variable Length Subnet Mask*) sera nécessaire, sachant que RIP ne supporte pas VLSM.
- L'utilisation de plusieurs adresses de sous-réseau de Classe C peut-elle entraîner un adressage discontinu des sous-réseaux au niveau des sites distants ? Dans l'affirmative, le support de sous-réseaux discontinus sera requis, sachant que RIP ne fournit pas un tel support.

Sur ce réseau, ces questions sont sans importance. Etant donné qu'un masque de 255.255.255.0 peut être utilisé partout sur le réseau, la question des VLSM ne se pose pas. De plus, étant donné que tous les sous-réseaux appartiennent au même réseau principal de classe B, il n'y a pas de problème de discontinuité des sous-réseaux. Le Tableau 25.1 résume l'adressage de la portion d'accès du réseau.

Tableau 20.1 : Adressage de la portion d'accès du réseau

Site	Sous-réseau	Masque
Site d'accès central*	172.16.1.0	255.255.255.0
Routeur2	172.16.2.0	255.255.255.0
Routeur3	172.16.3.0	255.255.255.0
...
Routeur121	172.16.121.0	255.255.255.0

* Peut être utilisée pour l'adressage du nuage de numérotation.

Adresses de prochain saut

Pour obtenir une table de routage précise et une négociation d'adresse IPCP (*IP Control Protocol*) réussie, l'ensemble de l'adressage IP de prochain saut doit être exact, à tout moment. Pour cela, les sites distants doivent connaître l'adresse IP à laquelle ils se connectent, et **le site central doit connaître l'adresse IP de chaque site distant qui s'est connecté.**

Tous les routeurs d'accès de site central utilisent la même adresse IP sur toutes leurs interfaces asynchrones. Pour parvenir à ce résultat, il faut configurer l'interface de numérotation Dialer20 pour un adressage IP non dédié (*IP unnumbered*), en dehors d'une interface de bouclage. **L'adresse IP de l'interface de bouclage (*loopback*) est la même pour tous les routeurs de site central.** De cette façon, les routeurs distants peuvent être configurés avec l'adresse IP du routeur auquel ils se connectent, quel qu'il soit.

Le routeur distant doit annoncer son adresse IP au routeur de site central au moment où il se connecte. A cette fin, il lance PPP sur le site central au moyen de la commande EXEC `ppp 172.16.x.1`. Pour supporter cette opération, chaque routeur de site central est configuré avec la commande de configuration d'interface `async dynamic address`.

NOTE

La fonction **Autoselect** permet au routeur de lancer automatiquement un processus approprié, tel PPP, lorsqu'il reçoit un caractère de départ de la part du routeur qui a ouvert une session. Pour pouvoir utiliser cette fonction, un mécanisme qui permet de gérer l'adressage IP dynamique est nécessaire, tel le support d'adresses par utilisateur de TACACS+.

Stratégie de routage

Le développement d'une stratégie de routage pour ce réseau se fonde sur les deux exigences suivantes :

- Lorsqu'un site distant particulier *n'est pas* connecté au site central, il doit être joignable par l'intermédiaire de n'importe quel routeur d'accès de site central, au moyen d'une route statique configurée sur chacun d'eux.
- Lorsqu'un site distant particulier *a ouvert* une session sur un routeur d'accès de site central, il doit être joignable par l'intermédiaire de ce routeur, au moyen d'une route dynamique qui a été établie pour cette connexion, et propagée vers l'épine dorsale.

Pour satisfaire ces exigences, les routeurs d'accès de site central indiquent au routeur Cisco 4500 les routes de réseau principales qui mènent aux sites distants. Toutes les routes vers les sites distants sont de coût égal, à partir des routeurs de site central. Chacun d'eux est configuré avec une route statique vers chaque site distant. Pour permettre au routeur Cisco 4500 de se connecter aux sites distants par l'intermédiaire de n'importe quel routeur de site central, la commande de configuration d'interface `no ip route-cache` est configurée sur son interface Ethernet 0, ce qui désactive la commutation rapide d'IP vers le sous-réseau partagé avec les routeurs de site central. Le routeur Cisco 4500 peut ainsi utiliser, en alternance, les trois routeurs d'accès lorsqu'il déclenche des appels sortants. Cette stratégie augmente la fiabilité du réseau, en cas de défaillance de l'un des routeurs d'accès.

Lorsqu'un site distant ouvre une session, il annonce son adresse IP, puis envoie un message flash RIP. Ce message provoque l'écriture immédiate d'une route dynamique vers le site distant, dans la table de routage du routeur d'accès de site central. Cette route dynamique remplace la route statique pour la durée de la connexion.

Ensuite, le routeur de site central redistribue la route RIP dans OSPF (*Open Shortest Path First*), et l'envoie à tous ses voisins OSPF, y compris le routeur Cisco 4500, qui l'enregistrent dans leur table de routage. Le routeur Cisco 4500 dispose à présent de routes de réseau principales vers tous les sites distants, ainsi que d'une route dynamique vers le site distant spécifique qui a ouvert la session. Si un hôte de site central doit communiquer avec un site distant particulier actuellement connecté, il utilise alors la route dynamique.

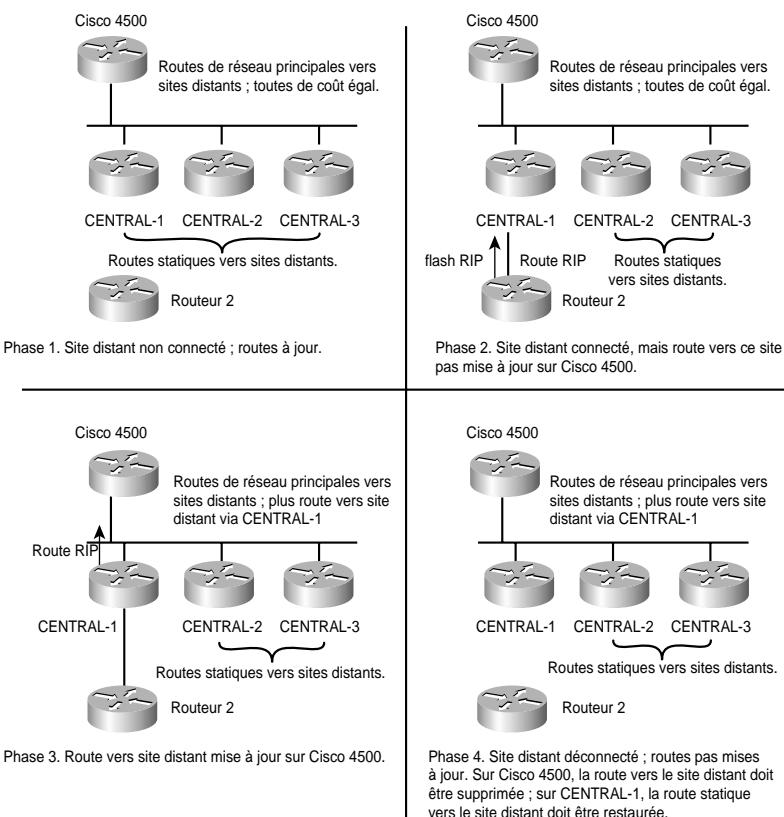
Lorsque le site distant ferme la session, la route dynamique est supprimée de la table de routage du routeur Cisco 4500, et la route statique vers le site distant est rétablie sur le routeur d'accès de site central auquel il s'est connecté.

Si un hôte de site central doit communiquer avec un site distant non connecté, il emprunte la route de réseau principale définie sur le routeur Cisco 4500. Parmi les routeurs d'accès de site central (sélectionnés à tour de rôle), l'un d'eux est choisi afin d'établir l'appel vers le site distant, *via* la route statique définie dans sa configuration. A l'image d'un site distant qui appelle le site central,

une fois la connexion établie, le routeur distant envoie un message flash RIP, qui provoque l'écriture immédiate d'une route dynamique vers le site distant, dans la table de routage du routeur d'accès. La route dynamique est redistribuée dans OSPF, puis enregistrée dans la table de routage du routeur Cisco 4500. La Figure 20.2 présente un diagramme qui synthétise les différentes phases de la stratégie de routage.

Figure 20.2

Diagramme des phases de la stratégie de routage.



Les problèmes de convergence suivants se rapportent aux phases du diagramme illustré à la Figure 20.2 :

- Entre la phase 2 et la phase 3, un hôte sur le site central établit un appel vers un site distant. Tant que la phase 3 n'a pas eu lieu (au cours de laquelle la route est mise à jour sur le routeur Cisco 4500), tout routeur d'accès de site central qui tente d'appeler le site distant obtiendra un signal d'occupation. Dans la pratique, un seul appel échoue en général, car, avant qu'une seconde tentative d'appel ait eu lieu, la route est mise à jour avec la phase 3. La route dynamique étant alors disponible, il n'est pas nécessaire d'effectuer un autre appel.
- Lorsque le site distant se déconnecte, un intervalle minimal de 120 secondes s'écoule avant que la route statique ne soit rétablie, dans la table de routage du routeur d'accès de site central sur

lequel le site distant a ouvert la session. Tout d'abord, RIP met 35 secondes pour déterminer que le site distant s'est déconnecté et qu'il n'envoie plus de mises à jour RIP. Six secondes plus tard, le routeur de site central examine sa table de routage, puis restaure l'une des deux routes statiques pour le site distant ; encore six secondes plus tard, il examine de nouveau sa table de routage pour rétablir la seconde route statique. Pour plus d'informations sur l'existence de deux routes statiques pour chaque site distant, voyez la section "Configuration du routage statique", plus bas dans ce chapitre.

NOTE

L'installation rapide de routes statiques est une nouvelle fonctionnalité de la version 11.1 de Cisco IOS . Elle permet le rétablissement rapide d'une route statique, suite à la déconnexion d'un site distant.

Avant que la mise à jour ait lieu, si le routeur Cisco 4500 dirige un appel vers le routeur 2 *via* le routeur CENTRAL-1, il n'aboutira pas : il devra donc être renouvelé. Etant donné que la commutation rapide d'IP est désactivée sur le routeur Cisco 4500 (qui utilise des chemins de même coût vers chaque routeur d'accès de site central), il enverra le prochain paquet vers le routeur CENTRAL-2 ou vers le routeur CENTRAL-3 (qui possède toujours une route statique vers le routeur 2), et l'appel aboutira.

NOTE

Lors du développement de la stratégie de routage pour ce réseau, les concepteurs ont envisagé l'utilisation du routage Snapshot, car il réduit le coût des connexions, en limitant l'échange de mises à jour de protocoles de routage. Pour que le routage Snapshot fonctionne correctement, chaque site distant doit se connecter au même routeur d'accès, chaque fois qu'il appelle le site central. Dans une telle conception, les routeurs distants se connectent aux routeurs de site central par l'intermédiaire d'un groupe de recherche de lignes, de façon qu'il n'y ait aucun moyen de contrôler sur quel routeur de site central un routeur distant s'est connecté pour une connexion donnée. Par conséquent, le routage Snapshot ne convient pas pour cette conception.

Configuration des routeurs d'accès de site central

Cette section décrit de quelle manière la configuration des routeurs d'accès de site central implémente l'authentification, l'adressage de la couche réseau et la stratégie de routage. La configuration est la même pour chaque routeur d'accès, à l'exception des éléments suivants :

- l'adresse IP spécifiée pour l'interface de bouclage 0 ;
- l'adresse IP spécifiée pour l'interface Ethernet 0 ;
- le nom du routeur, tel que spécifié par la commande de configuration globale `hostname`.

Cette section traite des sujets suivants :

- configuration du nom d'utilisateur pour les sites distants ;
- configuration de la numérotation pour les sites distants ;
- configuration des interfaces de bouclage ;

- configuration des interfaces asynchrones ;
- configuration de l'interface de numérotation ;
- configuration du routage OSPF ;
- configuration du routage RIP ;
- configuration du routage statique ;
- problèmes de sécurité ;
- taille du fichier de configuration.

Pour obtenir un exemple de configuration complet, voyez la section "Configuration de CENTRAL-1", plus bas dans ce chapitre.

Configuration du nom d'utilisateur pour les sites distants

La configuration de chaque routeur d'accès de site central inclut les commandes de configuration globale suivantes :

```
username Router2 password 7 071C2D4359
...
username Router121 password 7 0448070918
```

Chaque routeur distant peut appeler l'un des trois routeurs de site central, ce qui explique la présence d'une commande de configuration globale `username` pour chaque routeur distant. Lorsqu'un routeur distant ouvre une session, il indique un nom (par exemple, "Router2") et un mot de passe (par exemple, "secret"), qui doivent correspondre aux valeurs spécifiées par une commande `username`. Chaque site distant utilise un script de dialogue (*chat script*) pour ouvrir une session, ainsi que fournir son nom d'hôte et son mot de passe. Pour plus d'informations sur le script de dialogue utilisé par le site distant, voyez la section "Configuration de scripts de dialogue pour appeler le site central", plus bas dans ce chapitre.

Configuration de la numérotation pour les sites distants

La configuration de chaque routeur d'accès de site central inclut les commandes de configuration globale suivantes :

```
chat-script CALL1020 ABORT ERROR ABORT BUSY TIMEOUT 30 "" "ATDT\T" "CONNECT" \c
chat-script REM TIMEOUT 40 "name:" "CENTRAL" "word:" "secret"
chat-script usrv32bis "" "AT&F1S0=1&d2" "OK" ""
!
interface dialer 20
dialer map ip 172.16.2.1 name Router2 modem-script CALL1020 system-script REM 5551234
...
dialer map ip 172.16.121.1 name Router2 modem-script CALL1020 system-script REM 5555678
!
line 1 16
script reset USRV32BIS
```

Les trois commandes de configuration globale `chat-script` définissent trois scripts de dialogue, CALL1020, REM et USRV32BIS. Les scripts CALL1020 et REM sont invoqués par les commandes `dialer map` pour, respectivement, appeler les sites distants et y ouvrir une session. La commande `script reset` spécifie que le script USRV32BIS doit être exécuté chaque fois qu'une

ligne asynchrone est réinitialisée, afin de garantir que les modems de site central sont toujours configurés correctement.

Configuration des interfaces de bouclage

La configuration de chaque routeur d'accès de site central inclut des commandes pour configurer les interfaces de bouclage. L'adresse IP de l'interface de bouclage 0 est unique pour chaque routeur d'accès et, afin de respecter les règles selon lesquelles OSPF sélectionne l'identifiant de routeur, il doit s'agir de l'adresse IP de bouclage la plus haute sur chaque routeur. L'adresse IP pour l'interface de bouclage 1 est la même pour tous les routeurs d'accès. Voici les commandes utilisées :

```
interface loopback 0
ip address 172.16.254.3 255.255.255.255
...
interface loopback 1
ip address 172.16.1.1 255.255.255.0
```

L'objectif pour les trois routeurs est d'apparaître comme ayant la même adresse IP durant la négociation IPCP avec les sites distants (IPCP est la portion de PPP qui active et configure le support pour IP). Cet objectif est atteint par la création d'une interface de bouclage, à laquelle on assigne la même adresse IP sur chaque routeur de site central, puis par l'exécution de la commande de configuration d'interface `ip unnumbered`, avec l'adresse de cette interface. Le problème avec cette stratégie est que OSPF tire l'identifiant de routeur de l'adresse IP d'une interface de bouclage, s'il en existe une configurée ; il en résulte un même identifiant de routeur OSPF pour les trois routeurs d'accès.

La solution consiste à créer une interface de bouclage 0, et à lui assigner une adresse IP unique pour chaque routeur (ce qui procure un identifiant de routeur OSPF unique à chacun). La configuration crée ensuite une interface de bouclage 1, puis lui assigne la même adresse sur chaque routeur. Cette interface permet l'application de la commande `ip unnumbered` au groupe de rotation 20, plus tard dans la configuration.

Configuration des interfaces asynchrones

La configuration de chaque routeur d'accès de site central inclut les commandes suivantes pour configurer chaque interface asynchrone :

```
interface async 1
ip unnumbered loopback 1
async dynamic address
async dynamic routing
async mode interactive
dialer in-band
dialer rotary-group 20
```

Pour chacune des seize interfaces asynchrones fournies par le routeur d'accès, la configuration utilise la commande de configuration d'interface `ip unnumbered`, afin de spécifier que l'interface doit utiliser l'adresse IP de l'interface de bouclage 1 en tant qu'adresse source pour les paquets qu'elle génère. L'adresse IP de l'interface de bouclage 1 sert également à déterminer quels processus de routage envoient des mises à jour sur l'interface asynchrone.

La commande de configuration d'interface `async dynamic address` active l'adressage dynamique sur l'interface asynchrone. Cette commande est nécessaire afin de permettre à chaque routeur

distant d'indiquer son adresse IP lorsqu'il ouvre une session. La commande de configuration d'interface `async dynamic routing` autorise l'interface à exécuter un protocole de routage, dans ce cas RIP.

La commande de configuration d'interface `async mode interactive` autorise un routeur distant à se connecter et à accéder à l'interface de commande EXEC, ce qui lui permet de lancer PPP, et de spécifier son adresse IP.

La commande de configuration d'interface `dialer in-band` autorise l'usage des scripts de dialogue sur l'interface asynchrone. Ces scripts permettent au routeur d'accès d'appeler les sites distants. La commande de configuration d'interface `dialer rotary-group` assigne chaque interface asynchrone au groupe de rotation de numérotation 20.

Configuration de l'interface de numérotation

La configuration de chaque routeur d'accès de site central inclut les commandes suivantes pour configurer l'interface de numérotation 20 :

```
interface dialer 20
ip unnumbered loopback 1
encapsulation ppp
dialer in-band
dialer idle-timeout 60
dialer map ip 172.16.2.1 name Router2 modem-script CALL1020 system-script REM 5551234
...
dialer map ip 172.16.121.1 name Router121 modem-script CALL1020 system-script REM
↳5555678
dialer-group 3
dialer-list 3 list 101
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 520
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

La commande de configuration globale `interface dialer` définit le groupe de rotation 20. Toutes les commandes de configuration d'interface qui sont appliquées à un groupe de rotation de numérotation s'appliquent également aux interfaces physiques qui en sont membres. Lorsque la configuration d'un routeur inclut de nombreuses destinations, chacune des interfaces du groupe de rotation peut être utilisée pour effectuer un appel.

La commande de configuration d'interface `ip unnumbered` indique que l'adresse IP de l'interface de bouclage 1 doit être utilisée pour tous les paquets IP susceptibles d'être générés par le groupe de rotation 20. La commande de configuration d'interface `dialer idle-timeout` provoque une déconnexion, en l'absence de trafic intéressant au bout de 60 secondes.

La configuration inclut une commande de configuration d'interface `dialer map` pour chaque routeur distant susceptible d'être appelé par le routeur central. Le mot clé `ip` indique que la correspondance de numérotation doit être utilisée pour les paquets IP, et que l'adresse IP est l'adresse de prochain saut de la destination à appeler. Le mot clé `name` indique le nom d'hôte du routeur distant qui doit être appelé. Les mots clés `modem-script` et `system-script` spécifient respectivement l'utilisation des scripts de dialogue CALL1020 et REM. La dernière valeur fournie par la commande `dialer map` est le numéro de téléphone du routeur distant. Ces commandes `dialer map` n'utilisent pas le mot clé `broadcast`, ce qui empêche les mises à jour RIP d'être envoyées vers les sites distants.

Pour l'interface de numérotation Dialer20, la commande de configuration d'interface `dialer-group` indique que les paquets intéressants sont ceux qui sont définis par la commande correspondante `dialer-list`. Les paquets intéressants provoquent l'établissement, ou la maintenance, d'une connexion. Dans ce cas, la liste d'accès 101 définit RIP comme étant inintéressant (RIP utilise le port UDP 520). Tous les autres paquets sont déclarés comme étant intéressants.

Configuration du routage OSPF

Chaque routeur d'accès de site central utilise les commandes suivantes pour configurer OSPF. Ces commandes limitent les routes qui sont redistribuées dans OSPF aux routes principales statiques de classe B, ainsi qu'à toute autre éventuelle route de sous-réseau dynamique pour les sites distants actuellement connectés. Le fait de limiter la redistribution de routes dans OSPF simplifie considérablement la maintenance de la table de routage du routeur Cisco 4500 :

```
router ospf 110
 redistribute static subnets route-map STATIC-TO-OSPF
 redistribute rip subnets route-map rip-to-ospf
 passive-interface async 1
 ...
 passive-interface async 16
 network 172.19.0.0 0.0.255.255 area 0
 distance 210
 !
 route-map rip-to-ospf permit
 match ip address 20
 !
 access-list 20 permit 172.16.0.0 0.0.255.0
 !
 route-map static-to-ospf permit
 match ip address 21
 !
 access-list 21 permit 172.16.0.0
```

La commande de configuration globale `router ospf` active le processus de routage OSPF, puis lui assigne un identifiant de processus 110.

La première commande de configuration de routeur `redistribute` entraîne la redistribution des routes IP statiques dans OSPF. Le mot clé `subnets` indique que les sous-réseaux doivent être redistribués, et le mot clé `route-map` spécifie que seules les routes autorisées par la correspondance de route STATIC-TO-OSPF doivent être redistribuées. Cette dernière autorise la redistribution des routes qui correspondent à la liste d'accès 21, qui, elle, autorise uniquement le réseau 172.16.0.0 principal.

La seconde commande de configuration de routeur `redistribute` entraîne la redistribution des routes RIP statiques dans OSPF. Le mot clé `subnets` indique que les sous-réseaux doivent être redistribués, et le mot clé `route-map` spécifie que seules les routes autorisées par la correspondance de route RIP-TO-OSPF doivent être redistribuées. Cette dernière autorise la redistribution des routes qui correspondent à la liste d'accès 20, qui, elle, autorise uniquement les routes qui commencent par 172.16 et se terminent par .0 (le troisième octet est générique). En effet, la correspondance de route RIP-TO-OSPF autorise uniquement les sous-réseaux qui correspondent à l'adresse 172.16.x.0.

Une commande de configuration de routeur `passive-interface` est appliquée pour chaque interface asynchrone, ce qui signifie qu'aucune information de routage OSPF n'est envoyée ou reçue *via* ces interfaces. La commande de configuration de routeur `distance` assigne une distance administrative de 210 au processus de routage OSPF. Cela permet aux routeurs d'accès de site central de choisir leurs routes statiques (avec une distance administrative de 200) à la place des routes apprises par OSPF.

NOTE

Lorsqu'un site distant ouvre une session et qu'une route dynamique est établie pour cette connexion, les autres routeurs d'accès conservent leur route statique pour ce site distant. Lorsqu'un site distant se déconnecte, les autres routeurs d'accès n'ont pas besoin de mettre à jour leurs tables de routage, puisqu'elles contiennent toujours la route statique nécessaire pour appeler le site distant.

Configuration du routage RIP

Chaque routeur d'accès de site central utilise les commandes suivantes pour configurer RIP :

```
router rip
timers basic 30 35 0 1
network 172.16.0.0
distribute-list 10 out Dialer20
!
access-list 10 deny 0.0.0.0 255.255.255.255
```

La commande de configuration de routeur `timers basic` définit les valeurs des temporiseurs de mise à jour (*update*), d'invalidité (*invalid*), de retenue (*holddown*) et de nettoyage (*flush*). Cette commande spécifie que les mises à jour RIP doivent être envoyées toutes les 30 secondes, qu'une route doit être déclarée invalide si aucune mise à jour n'est reçue pour cette route dans un délai de 35 secondes après la mise à jour précédente, que le temps durant lequel les meilleures routes doivent être supprimées est de 0 seconde, et qu'une route invalide est éliminée de la table de routage au bout de 1 seconde. La modification de ces temporiseurs, telle qu'elle est effectuée ici, résulte en un temps de convergence optimal, lors de la déconnexion d'un site distant.

La commande de configuration de routeur `network` indique que le réseau 172.16.0.0 doit participer au processus de routage RIP. Puisqu'il n'est pas nécessaire de propager les routes RIP vers les routeurs Cisco 1020, la commande de configuration de routeur `distribute-list out` spécifie que la liste d'accès 10 doit être utilisée pour contrôler les annonces dans les mises à jour. La liste d'accès 10 empêche que les routes RIP ne soient envoyées vers les sites distants.

Configuration du routage statique

La configuration de chaque routeur d'accès de site central inclut plusieurs commandes `ip route`, à l'image de ce qui suit, pour configurer les routes statiques vers les sites distants :

```
ip route 172.16.0.0 255.255.0.0 Dialer20
```

La première commande de configuration globale `ip route` crée une route statique pour le réseau principal 172.16.0.0, puis l'assigne à l'interface de numérotation 20. Lorsqu'elle est redistribuée dans OSPF, la route indique au routeur Cisco 4500 que ce routeur d'accès de site central peut accéder aux sites distants. Si ce routeur d'accès tombe en panne, le routeur Cisco 4500 apprend que la

route n'est plus disponible il la supprime alors de sa table de routage. Cette route est redistribuée dans OSPF au moyen du filtre STATIC-TO-OSPF. La première commande `ip route` est suivie de couples de routes statiques, un couple pour chaque site distant :

```
ip route 172.16.2.0 255.255.255.0 172.16.2.1 200
ip route 172.16.2.1 255.255.255.255 Dialer20
...
ip route 172.16.121.0 255.255.255.0 172.16.121.1 200
ip route 172.16.121.1 255.255.255.255 Dialer20
```

Dans des environnements sans adressage IP dédié, deux routes statiques sont nécessaires pour chaque site distant :

- Une route statique pointe sur le prochain saut dans la correspondance de numérotation. Notez que le chiffre "200" fait de cette route une route statique flottante, mais qui est inférieure aux routes OSPF (définies à 210 par la commande `distance`, plus haut dans la configuration). Cela signifie qu'une route RIP déclenchée par une connexion vers un site distant (qu'elle l'ait été au moyen d'un site distant ou du site central) remplace la route statique. Une mise à jour OSPF initiée par un site distant qui se connecte n'entraîne pas le remplacement de la route statique qui pointe sur l'adresse de prochain saut dans la correspondance de numérotation.
- Une route statique qui définit l'interface sur laquelle peut être trouvée l'adresse de prochain saut (dans ce cas, l'interface de numérotation 20). Cette route est requise par les interfaces sans adresse dédiée. Notez qu'il n'est pas nécessaire de faire de cette route une route statique flottante.

Problèmes de sécurité

La configuration de chaque routeur d'accès de site central inclut la commande de configuration de ligne `login` pour chaque ligne asynchrone, et spécifie le mot clé `local`. Avec cette commande, le routeur d'accès compare le nom d'utilisateur et le mot de passe, spécifiés par la commande de configuration globale `username`, avec ceux fournis par le site distant lorsqu'il ouvre une session. Cette méthode de sécurité est requise pour permettre au site distant d'ouvrir une session et de spécifier son adresse IP.

Taille du fichier de configuration

Au fur et à mesure que le nombre de sites distants augmente, la taille du fichier de configuration sur chaque routeur d'accès de site central peut croître, de telle manière que le fichier ne puisse plus être stocké en mémoire NVRAM. Il existe deux moyens de résoudre ce problème :

- Compresser le fichier de configuration à l'aide de la commande de configuration globale `service compress-config`.
- Faire en sorte que les routeurs d'accès de site central démarrent en utilisant des fichiers de configuration stockés sur un serveur TFTP (*Trivial File Transfer Protocol*).

Configuration des routeurs de site distant

Les configurations de tous les routeurs d'accès de site central sont identiques, à l'exception du nom d'hôte et de l'adresse IP de l'interface Ethernet de chaque routeur.

Cette configuration repose sur les éléments suivants :

- configuration des scripts de dialogue pour appeler le site central ;
- configuration des interfaces asynchrones ;
- utilisation de la commande **site** ;
- configuration du routage statique.

Pour obtenir un exemple de configuration complète, voyez la section "Configuration du routeur 2", plus loin dans ce chapitre.

Configuration de scripts de dialogue pour appeler le site central

La configuration de chaque routeur distant inclut la commande de configuration globale **chat-script** suivante :

```
chat-script CENTRALDIAL "" "ATDT 5551111" "CONNECT" "" "name:" "Router2" "word:"
"secret" ">" "ppp 172.16.2.1"
```

La commande **chat-script** définit un script de dialogue, CENTRALDIAL, qui est utilisé pour appeler le site central. Ce script spécifie le numéro de téléphone (55-1111) du site central, ainsi que la séquence attendre-envoyer qui guide le modem au cours du processus de numérotation. Une fonction essentielle de ce script est que, au moment où le routeur distant reçoit la chaîne ">" (l'invite qui lui indique une ouverture de session réussie sur le routeur d'accès), il envoie la commande EXEC ppp 172.16.2.1, afin de fournir au routeur d'accès son adresse IP.

Configuration des interfaces asynchrones

La configuration de chaque routeur distant inclut les commandes suivantes pour configurer une interface asynchrone :

```
interface async 1
speed 38400
modem-type usr-sport-v32
dialer rotary-group 1
!
modem-def usr-sport-v32 "USR Sportster v.32bis" 38400 "" "AT&F1" "OK"
```

La commande de configuration de ligne **speed** définit le débit (en bauds) à 38 400 bits par seconde, en émission comme en réception. La commande **modem-type** spécifie la chaîne d'initialisation envoyée au modem, lorsque l'interface est réinitialisée ou que la commande **clear interface-async** est exécutée. La chaîne d'initialisation est définie pour **usr-sport-v32** au moyen de la commande **modem-def**. La commande de configuration d'interface **dialer rotary-group** assigne l'interface asynchrone 1 au groupe de rotation de numérotation 1.

Commande **site**

La configuration de chaque routeur distant inclut la commande de configuration **site** suivante :

```
site CENTRAL
dial-on demand
encapsulation ppp
ip address 172.16.1.1 255.255.255.0
routing rip broadcast
dialgroup 1
```

```
session-timeout 5
system-script CENTRALDIAL
password secret
max-ports 1
```

La commande de configuration globale `site` définit un emplacement distant, nommé CENTRAL, auquel le routeur distant peut se connecter, ou qui peut se connecter au routeur distant, ou encore les deux. Ce nom sert à authentifier le site central, lorsqu'il se connecte.

La commande de configuration de site `dial-on` utilise le mot clé `demand`, afin d'indiquer que le site central doit être appelé et qu'une connexion doit être établie, uniquement lorsque des paquets sont placés en file d'attente pour ce site. La commande de configuration de site `encapsulation` spécifie l'utilisation de l'encapsulation PPP, lorsque le routeur établit une connexion avec le site central.

La commande de configuration d'interface `ip address` associe l'adresse IP 172.16.1.1 au site central. Notez que cette adresse est celle de l'interface de numérotation 20 sur chacun des routeurs d'accès de site central. La commande de configuration d'interface `routing ip` et le mot clé `broadcast` indiquent que, au moment où le routeur est connecté au site central, les mises à jour IP doivent être envoyées en mode broadcast, mais doivent être ignorées en entrée.

La commande `dialgroup` indique que le groupe de numérotation 1 doit être utilisé lors de la connexion au site central. Plus haut dans cette configuration, la commande `dialer rotary-group` a assigné l'interface asynchrone 1 au groupe 1.

La commande de configuration de site `session-timeout` indique au routeur de mettre fin à la connexion, en l'absence de trafic en entrée ou en sortie durant plus de cinq minutes. La commande de configuration de site `system-script` spécifie que le script de dialogue CENTRALDIAL doit être utilisé afin d'appeler le site central. La commande de configuration de site `password` indique que le routeur d'accès doit utiliser la chaîne "secret" comme mot de passe lorsqu'il se connecte.

Configuration du routage statique

La configuration de chaque routeur distant inclut les commandes de configuration globale `ip route` suivantes :

```
ip route 150.10.0.0 172.16.1.1 1
ip route 172.18.0.0 172.16.1.1 1
ip route 172.19.0.0 172.16.1.1 1
ip route 172.21.0.0 172.16.1.1 1
ip route 172.22.0.0 172.16.1.1 1
```

Ces commandes `ip route` définissent les routes IP statiques des réseaux situés au niveau du site central, tous joignables par le biais d'une adresse de prochain saut 172.16.1.1 (l'adresse IP partagée par tous les routeurs d'accès sur le site central). Toutes ces commandes spécifient une distance administrative de 1, qui est la valeur par défaut.

Configuration complète

Cette section présente les configurations complètes des routeurs CENTRAL-1 et Router 2.

Configuration du routeur CENTRAL-1

Voici la configuration complète du routeur CENTRAL-1. Les portions qui doivent être uniques pour chaque routeur d'accès de site central sont mises en gras :

```
!
version 10.2
service timestamps debug datetime
service timestamps log datetime
service udp-small-servers
service tcp-small-servers
!
hostname CENTRAL-1
!
enable-password as5100
!
username Router2 password 7 071C2D4359
...
username Router121 password 7 0448070918
!
chat-script CALL1020 ABORT ERROR ABORT BUSY TIMEOUT 30 "" "ATDT\T" "CONNECT" \c
chat-script REM TIMEOUT 40 "name:" "CENTRAL" "word:" "secret"
chat-script usrv32bis "" "AT&F1S0=1&d2" "OK" ""
!
interface loopback 0
ip address 172.16.254.3 255.255.255.255
!
interface loopback 1
ip address 172.16.1.1 255.255.255.0
!
interface ethernet 0
ip address 172.19.1.8 255.255.0.0
!
interface serial 0
no ip address
shutdown
!
interface async 1
ip unnumbered loopback 1
encapsulation ppp
async dynamic address
async dynamic routing
async mode interactive
dialer in-band
dialer idle-timeout 60
dialer rotary-group 20
...
interface async 16
ip unnumbered loopback 1
encapsulation ppp
async dynamic address
async dynamic routing
async mode interactive
dialer in-band
dialer idle-timeout 60
```

```
dialer rotary-group 20
!
interface dialer 20
ip unnumbered loopback 1
encapsulation ppp
dialer in-band
dialer idle-timeout 60
dialer fast-idle 60
dialer map ip 172.16.2.1 name Router2 modem-script CALL1020 system-script REM 5551234
...
dialer map ip 172.16.121.1 name Router121 modem-script CALL1020 system-script REM
↳5555678
dialer-group 3
!
router ospf 110
redistribute static subnets route-map STATIC-TO-OSPF
redistribute rip subnets route-map RIP-TO-OSPF
passive-interface async 1
...
passive-interface async 16
network 172.19.0.0 0.0.255.255 area 0
distance 210
!
router rip
timers basic 30 35 0 1
network 172.16.0.0
distribute-list 10 out Dialer20
!
ip default-gateway 172.19.1.10
!
ip route 172.16.0.0 255.255.0.0 Dialer20
ip route 172.16.2.0 255.255.255.0 172.16.2.1 200
ip route 172.16.2.1 255.255.255.255 Dialer20
...
ip route 172.16.121.0 255.255.255.0 172.16.121.1 200
ip route 172.16.121.1 255.255.255.255 Dialer20

access-list 10 deny 0.0.0.0 255.255.255.255
access-list 20 permit 172.16.0.0 0.0.255.0
access-list 21 permit 172.16.0.0
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 520
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255

route-map rip-to-ospf permit
match ip address 20
!
route-map static-to-ospf permit
match ip address 21
!
snmp-server community public RO
snmp-server community private RW
dialer-list 3 list 101
!
line con 0
line 1 16
login local
modem inout
script reset USRV32BIS
transport input all
rxspeed 38400
```

```
txspeed 38400
flowcontrol hardware
line aux 0
transport input all
line vty 0 4
exec-timeout 20 0
password cisco
login
!
end
```

Configuration de Router 2

Voici la configuration complète de Router 2. Les portions qui doivent être uniques pour chaque routeur distant sont mises en gras :

```
version 1.1(2)
!
hostname Router2
!
enable-password cisco-a
!
chat-script CENTRALDIAL "" "ATDT 5551111" "CONNECT" "" "name:" "Router2" "word:"
"secret" ">" "ppp 172.16.2.1"
!
interface ethernet 0
ip address 172.16.2.1 255.255.255.0
!
interface async 1
speed 38400
modem-type usr-sport-v32
dialer rotary-group 1
!
site CENTRAL
dial-on demand
encapsulation ppp
ip address 172.16.1.1 255.255.255.0
routing rip broadcast
dialgroup 1
session-timeout 5
system-script CENTRALDIAL
password secret
max-ports 1
!
modem-def usr-sport-v32 "USR Sportster v.32bis" 38400 "" "AT&F1" "OK"
!
ip route 150.10.0.0 172.16.1.1 1
ip route 172.18.0.0 172.16.1.1 1
ip route 172.19.0.0 172.16.1.1 1
ip route 172.21.0.0 172.16.1.1 1
ip route 172.22.0.0 172.16.1.1 1
```

Réseaux d'entreprise commutés

Lors de la mise en œuvre de réseaux d'entreprise commutés, certains aspects importants, tels que l'évolutivité et les problèmes de conception, doivent être considérés avec attention. Au fur et à mesure que le nombre d'employés augmente, le nombre d'utilisateurs distants qui doivent se

connecter au réseau augmente également. Une solution de connexion à distance évolutive est nécessaire afin de faire face à la demande en ports de connexions entrantes. Il est fréquent, pour une entreprise à croissance rapide, de passer en moins d'un an de 50 à 200 modems. Il est recommandé de toujours prévoir un certain nombre de ports de connexions entrantes afin de pouvoir s'adapter à l'expansion de la société ainsi qu'aux pointes occasionnelles de demandes d'accès. Dans une entreprise à croissance rapide qui dispose, à ses débuts, de 50 modems installés pour 3 000 utilisateurs distants enregistrés, seuls 20 à 30 modems sont actifs la plupart du temps. Un an plus tard, 200 modems pourraient être installés pour supporter 8 000 utilisateurs.

Gardez toujours à l'esprit que la demande globale d'accès distant peut également augmenter ponctuellement de façon considérable, par exemple lors d'occasions spéciales pour l'entreprise. Dans ces situations, les lignes entrantes sont fortement sollicitées, de jour, mais également dans la soirée, en raison d'accès à distance à la messagerie et aux fichiers partagés *via* des ordinateurs portatifs, ce qui signifie que des utilisateurs travaillent à partir de leur domicile. Les administrateurs de réseau doivent se préparer à ces pointes d'accès à distance, qui font soudain croître la demande. De plus, vous pouvez parfois observer, à certains moments de la journée, une utilisation intensive des lignes, sans qu'il y ait de rapport avec l'activité en cours. Cela peut s'expliquer par des opérations de téléchargement de fichiers ou de consultation de messagerie sur le site central, initiées par des utilisateurs qui travaillent dans des succursales, ou itinérants. Ces utilisateurs se connectent souvent au réseau d'entreprise à partir du réseau local de leur bureau distant en utilisant RNIS, ou bien à partir d'une chambre hôtel, au moyen d'un modem.

Il existe plusieurs profils d'utilisateurs qui se connectent au réseau d'entreprise à distance :

- Les utilisateurs qui emploient des stations de travail afin de se connecter au réseau de l'entreprise à partir d'un petit bureau distant ou de leur domicile. Ils exploitent des connexions RNIS avec adaptateurs de terminaux, ou cartes PC sur le réseau RTC, qui ne nécessitent pas de modem.
- Les utilisateurs itinérants, tels que les commerciaux, qui se connectent habituellement au réseau de l'entreprise *via* le réseau RTC, au moyen d'un ordinateur portatif doté d'un modem, et qui consultent surtout la messagerie ou transfèrent de nouveaux fichiers.
- Les utilisateurs qui travaillent la plupart du temps dans les bureaux de la société, mais qui se connectent occasionnellement à distance, à l'aide d'une station de travail mobile ou fixe avec modem, afin d'accéder principalement à la messagerie et aux fichiers partagés.

Les réseaux locaux de bureaux distants utilisent principalement RNIS pour se connecter à d'autres réseaux, en raison de la bande passante que fournit ce média et que les connexions téléphoniques analogiques ne peuvent atteindre. Ceux qui utilisent le Frame Relay pour accéder à d'autres réseaux requièrent une liaison dédiée. Dans certaines situations, les connexions initiées par ces bureaux distants ou par des utilisateurs itinérants sont établies uniquement lorsque cela est nécessaire, ce qui implique des économies pour l'entreprise. Lorsque le routage DDR est mis en œuvre, les utilisateurs peuvent demeurer non connectés pendant de longs moments. Le nombre de noeuds distants qui nécessitent un accès est relativement faible, et le temps d'établissement des connexions est court. Si le routage DDR est exploité sur des configurations purement IP, des routes statiques sont généralement utilisées pour les connexions à distance. Sur les réseaux IPX, le routage Snapshot permet de limiter la complexité de configuration.

Ce sont rarement les sites centraux qui se connectent aux réseaux LAN ou utilisateurs distants, mais plutôt l'inverse ; cette communication est unidirectionnelle. A de très rares occasions, le serveur d'accès de site central (par exemple, un Cisco AS5300) doit contacter un site distant (par exemple, un routeur RNIS Cisco 1604) en même temps qu'il reçoit des appels entrants. Une fois la connexion établie, le site distant exécute une application de traitement par lots avec le mainframe du site central. Pendant le transfert des fichiers entre les deux sites, un autre site distant peut se connecter au site central. Les appels distants analogiques ou numériques se font habituellement vers des routeurs RNIS distants, tel le Cisco 1604. De plus, comme nous l'avons mentionné, ils sont plutôt initiés par un PC distant en direction du site central. Il peut également arriver qu'un site central appelle un site distant, en réponse à une demande de livraison de courrier électronique. La fonction de rappel (*callback*) est activée uniquement pour les connexions entrantes. N'oubliez pas que MMP (*MultiChassis MultiLink PPP*) et VPDN (*Virtual Private Dialup Network*) sont des solutions de connexion entrante uniquement.

Réseaux de FAI commutés

Les problèmes d'évolutivité et de conception doivent également être pris en compte lors de la création de réseaux de fournisseurs d'accès Internet (FAI). Au fur et à mesure que le nombre de clients de ces fournisseurs augmente, les besoins en connexions distantes augmentent également. Il est donc essentiel d'implémenter une solution de connexion à distance qui soit évolutive, afin de répondre à la demande croissante en ports d'appels entrants. Lors de la mise en place d'un point d'accès à l'Internet (POP, *Point Of Presence*) de grande échelle, l'évolutivité et la densité d'appels doivent être examinés. Etant donné que les serveurs d'accès présentent des limitations physiques (par exemple le nombre d'utilisateurs qui peuvent être supportés simultanément sur un équipement), il faut étudier attentivement les conditions et recommandations de différents serveurs d'accès. De nombreux FAI de petite et moyenne tailles configurent un ou deux serveurs d'accès pour supporter les connexions entrantes de leurs clients distants. Parmi ces derniers, beaucoup utilisent des PC individuels, qui ne sont pas reliés à un LAN. Grâce au service Accès réseau à distance (RAS, *Remote Access Service*) de Windows 95, les clients distants peuvent initier soit des connexions analogiques au moyen de modems, soit des connexions numériques avec adaptateurs de terminaux RNIS BRI SOHO.

Les fournisseurs de services Internet peuvent implémenter trois types de configurations pour les appels entrants de la part d'utilisateurs individuels :

- Configuration d'un seul serveur d'accès Cisco, par exemple un AS52/53/5800, au niveau du point d'accès afin de recevoir les appels analogiques de la part de PC distants connectés à des modems. Pour les solutions de petite taille, le point d'accès du FAI au niveau du site central pourrait également utiliser un serveur d'accès Cisco 2511 connecté à des modems externes. Dans ce cas, les PC des clients distants se connecteraient au moyen de modems analogiques sur des lignes T1 traditionnelles. Les appels RNIS ne sont pas supportés sur les anciennes lignes fractionnées. La configuration suppose que le client peut appeler et se connecter au routeur en mode d'émulation de terminal (texte seulement) ou en mode paquet PPP.
- Configuration d'un seul serveur d'accès Cisco, par exemple un AS52/53/5800, afin de recevoir des appels multilignes numériques de la part de PC distants connectés à des adaptateurs de terminaux. Le point d'accès au niveau du site central du FAI peut être n'importe quel routeur

Cisco qui supporte RNIS PRI, tel le Cisco 4700-M chargé avec un module de réseau PRI T1 fractionné.

- Configuration d'un seul serveur d'accès Cisco, par exemple un AS52/53/5800, afin de recevoir des appels de PC distants connectés à des adaptateurs de terminaux ou à des modems. Etant donné que l'Internet croît de façon exponentielle, ainsi que les demandes d'accès à l'Internet, de nombreux opérateurs téléphoniques et fournisseurs FAI doivent mettre en place des points d'accès de grande taille. Les configurations de l'accès à l'Internet peuvent être définies de façon à autoriser les appels entrants d'utilisateurs distants qui se connectent à partir d'ordinateurs individuels, ainsi qu'à établir des connexions mixtes, *via* des liaisons multilignes RNIS ou par modem, à une pile de serveurs d'accès universels qui exécutent MMP. Lors d'appels RNIS entrants, un élément d'information de capacité du canal porteur contenu dans le paquet de demande de connexion indique si l'appel est de type voix ou données. Une fois que les appels ont été acceptés par le serveur d'accès, ils sont routés soit vers la configuration série, soit vers la configuration avec modems et groupe asynchrone.

Résumé

Cette étude de cas montre qu'il est possible d'adapter le routage DDR à de grands réseaux à commutation de circuits. Dans le futur, si le nombre de sites distants dépasse la capacité des 48 interfaces asynchrones, des routeurs supplémentaires pourront être installés, sans avoir à modifier la stratégie de routage. Ce chapitre a également abordé les aspects relatifs à la conception de réseaux commutés d'entreprise et de fournisseurs de services Internet.

Emploi efficace de RNIS en milieu multiprotocole

Par Salman Asad

Le développement de RNIS en tant que moyen de connexion pour les sites distants est lié à la multiplication des services RNIS proposés par les opérateurs téléphoniques. Cette étude de cas couvre les scénarios RNIS suivants :

- **Configuration de DDR sur RNIS.** Ce scénario de télétravail décrit la configuration de bureaux installés au domicile des utilisateurs, qui exploitent RNIS en tant que moyen de connexion à un réseau central d'entreprise. Il illustre l'utilisation des numéros d'identification de lignes appelantes pour empêcher les accès non autorisés au réseau central.
- **Configuration du routage Snapshot sur RNIS.** Le routage Snapshot assure un accès rentable au réseau d'entreprise, à partir d'une agence ou d'un bureau à domicile. Cette méthode de routage est employée pour faire évoluer le réseau de télétravail et contrôler les mises à jour de routage sur les réseaux Novell IPX.
- **Configuration d'AppleTalk sur RNIS.** Ce scénario illustre comment contrôler les paquets AppleTalk susceptibles de déclencher des connexions RNIS inutiles.
- **Configuration de IPX sur RNIS.** Ce scénario décrit comment configurer IPX comme étant un protocole de niveau 3 pour RNIS.

Configuration de DDR sur RNIS

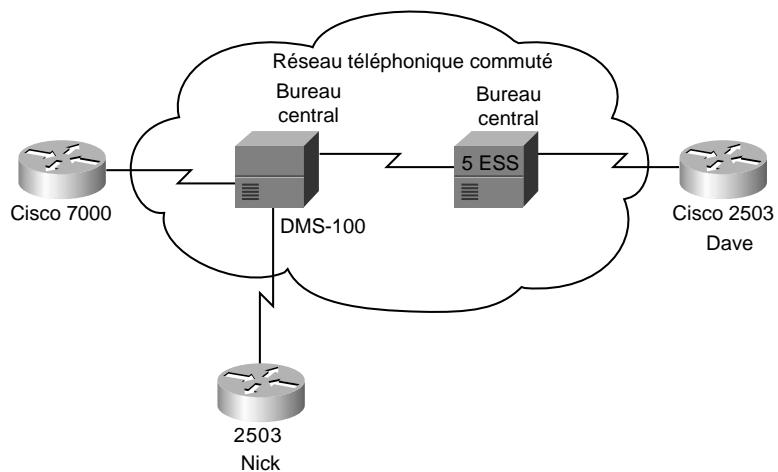
Aux Etats-Unis, de nombreuses entreprises considèrent aujourd'hui le télétravail comme étant un moyen de résoudre les problèmes de manque d'espace, conformément à la loi de protection de

l'environnement *Clean Air Act*, et de développer la productivité des employés. En Europe, les entreprises recherchent des solutions qui permettent à des bureaux distants de se connecter aux sites centraux. Par le passé, les modems analogiques assuraient la connectivité nécessaire sur des lignes série, mais ils ne sont pas assez rapides pour des connexions entre réseaux locaux (LAN) ou pour l'utilisation distante de programmes graphiques, tels les outils de CAO (conception assistée par ordinateur). Le principal avantage de RNIS est qu'il fournit la bande passante supplémentaire nécessaire, sans avoir à utiliser de lignes louées.

Un accès RNIS de base via l'interface BRI (*Basic Rate Interface*) fournit deux canaux B à 64 Kbit/s pour le transport de la voix et des données, et un canal D à 16 Kbit/s pour la signalisation. Les informations vocales et les données sont transportées numériquement sur les canaux B. Aux Etats-Unis, l'accès RNIS primaire avec l'interface PRI (*Primary Rate Interface*) peut fournir 23 canaux B à 64 Kbit/s pour le transport de la voix et des données sur une ligne T1, et un canal D à 64 Kbit/s pour la signalisation. En Europe, un accès RNIS primaire fournit 30 canaux B pour le transport de la voix et des données, et un canal D pour la signalisation sur une ligne E1.

La Figure 21.1 illustre le réseau qui sert d'exemple pour cette étude de cas. Il utilise plusieurs commutateurs RNIS de bureau central.

Figure 21.1
Exemple de réseau RNIS.



Dans cette étude de cas, les sites distants (à domicile) exploitent des routeurs Cisco 2503 qui fournissent une interface BRI, une interface Ethernet et deux interfaces série à haute vitesse. Sur le site central de l'entreprise, un routeur de la série Cisco 7000 équipé d'une ligne T1 fractionnée répond aux appels. La carte de ligne T1 fractionnée fournit une interface PRI.

Dans de nombreux endroits des Etats-Unis, les compagnies de téléphone n'ont pas déployé le système de signalisation SS7 (*Signaling System 7*), ce qui signifie que les appels entre certains bureaux centraux doivent être établis à la vitesse de 56 Kbit/s. Cette restriction ne s'applique pas à l'ensemble des Etats-Unis, ou à d'autres pays, mais elle concerne certains exemples de réseaux RNIS décrits dans ce chapitre.

Interface pour RNIS natif

Si vous utilisez un adaptateur de terminal RNIS externe, également désigné *modem RNIS*, vous pouvez vous inspirer des exemples de configuration fournis au Chapitre 19. Bien qu'un modem RNIS assure une connectivité RNIS et permette l'usage d'interfaces série existantes, il ne représente pas toujours une solution optimale, eu égard à l'investissement nécessaire à l'acquisition d'un dispositif externe et du câblage supplémentaire. De plus, l'emploi de la numérotation V.25bis n'apporte pas au routeur un accès complet à certaines informations, pourtant disponibles sur un réseau RNIS, telles que la vitesse de l'appel ou le numéro de l'appelant.

L'interface pour RNIS natif sur le routeur Cisco 2503 lui permet d'être directement connecté à une terminaison numérique de réseau (TNR), ou NT1 (*Network Termination-1*). Dans de nombreux pays, la terminaison est fournie par le prestataire de services. Aux Etats-Unis, cet équipement appartient au client. En se connectant directement au réseau, le routeur dispose d'un meilleur contrôle sur les paramètres RNIS, et peut accéder aux informations RNIS.

Configuration d'une interface RNIS

La configuration d'une interface pour RNIS natif est semblable à celle d'une interface série qui utilise le routage DDR (voir Chapitre 19). Il y a toutefois deux différences principales :

- La commande `dialer in-band` n'est pas requise avec RNIS. Les interfaces PRI et BRI apparaissent pour le routeur comme étant une interface DDR.
- Les canaux B individuels ne peuvent pas être configurés séparément. Ceux d'une interface BRI apparaissent comme étant un groupe de rotation de numérotation avec deux membres. Ceux d'une interface PRI apparaissent, aux Etats-Unis, avec 23 membres, et en Europe avec 30 membres. Etant donné qu'une interface PRI ou BRI est un groupe de rotation de numérotation, toutes les commandes de configuration qui lui sont associées s'appliquent à tous les canaux B.

Les sections suivantes décrivent la configuration de routeurs de site central et de sites distants. Dans cette étude de cas, ces deux types de sites peuvent effectuer des appels. Le site central utilise un routeur Cisco 7000, qui est connecté à un commutateur RNIS de bureau central NorTel DMS-100. L'un des routeurs de site distant (*nick-isdn*) est connecté au même commutateur que le routeur de site central. Les connexions en provenance de l'autre routeur de site distant (*dave-isdn*) passent par deux commutateurs de bureau central pour atteindre le routeur du site central.

Site central

Deux utilisateurs de sites distants, Dave et Nick, établissent des appels à partir de leur domicile respectif vers le routeur du site central, qui est configuré comme suit. Une partie de la configuration est spécifique au commutateur DMS-100, alors que les autres commandes s'appliquent à tout type de commutateur RNIS de bureau central :

```
hostname central-isdn
!
username dave-isdn password 7 130318111D
username nick-isdn password 7 08274D02A02
isdn switch-type primary-dms100
!
interface ethernet 0
ip address 11.108.40.53 255.255.255.0
```

```

no mop enabled
!
controller t1 1/0
framing esf
linecode b8zs
pri-group timeslots 2-6
!
interface serial 1/0:23
ip address 11.108.90.53 255.255.255.0
encapsulation ppp
dialer idle-timeout 300
dialer map ip 11.108.90.1 name dave-isdn speed 56 914085553680
dialer map ip 11.108.90.7 name nick-isdn 8376
dialer-group 1
ppp authentication chap
!
router igrp 10
network 11.108.0.0
redistribute static
!
! route vers nick-isdn
ip route 11.108.137.0 255.255.255.0 11.108.90.7
! route vers dave-isdn
ip route 11.108.147.0 255.255.255.0 11.108.90.1
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!NTP
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123
!SNMP
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 161
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.25 du nom
↳d'hôte.255
!
dialer-list 1 list 101

```

La configuration débute par la définition du nom d'hôte du routeur central, au moyen de la commande `hostname`. Les instructions qui utilisent la commande `username` définissent les noms des routeurs qui sont autorisés à appeler ce routeur (du site central). Les noms correspondent au nom d'utilisateur du routeur de Dave et à celui du routeur de Nick. La commande `isdn switch-type` indique que ce routeur se connecte à un commutateur NorTel DMS-100. Le nom d'hôte, les noms d'utilisateurs et le type de commutateur RNIS varient selon le routeur configuré.

Configuration de contrôleur

La commande `controller` utilise la valeur `t1` pour déclarer une interface de contrôleur T1. La valeur `1` indique que la carte de contrôleur est située dans le connecteur numéro `1` du panneau arrière de connexion. La valeur `0` désigne le port `0`.

La commande `framing` sélectionne le type de trame pour la ligne de données T1. Dans ce cas, elle utilise le mot clé `esf` pour indiquer le type ESF (*Extended Super Frame*). Le fournisseur de services détermine le type de trame approprié pour votre circuit T1/E1 parmi les types `sf`, `esf` ou `crc4`.

La commande `linecode` définit le type de code de ligne pour la ligne de données T1. Dans cet exemple, elle utilise le mot clé `b8zs` pour indiquer l'utilisation du code B8ZS (*Bipolar 8 Zéro Substitution*, code bipolaire à substitution de huit zéros). Le fournisseur de services détermine le type de code de ligne requis pour votre circuit T1/E1 entre les codes AMI (*Alternate Mark Inversion*) et BZ8.

La commande `pri-group` désigne une interface PRI sur une carte T1 fractionnée, sur un routeur de la série Cisco 7000. Le mot clé `timeslots` définit les canaux B. Dans cet exemple, seuls 5 canaux B (canaux 2 à 6) sont utilisés sur ce contrôleur.

Configuration d'interface

La commande `ip address` définit l'adresse IP de l'interface ; la commande `encapsulation ppp` définit le protocole PPP (*Point-to-Point Protocol*) en tant que méthode d'encapsulation. PPP supporte les protocoles CHAP (*Challenge Handshake Authentication Protocol*) et PAP (*Password Authentication Protocol*) en tant que mécanismes d'authentification de l'appelant, et également afin d'assurer un certain niveau de sécurité. La commande `dialer idle-timeout` définit un délai d'inactivité de cinq minutes.

Les commandes `dialer map` définissent les sites distants que le routeur peut appeler. Etant donné que le routeur de Dave se connecte à un commutateur de bureau central qui n'utilise pas le système de signalisation SS7, la commande `dialer map` exécutée pour l'appeler contient le mot clé `speed`, valide seulement avec les interfaces pour RNIS natif. L'interface pour RNIS natif sur le Cisco 2503 opère à 64 Kbit/s ou à 56 Kbit/s. Si l'appelant et l'appelé utilisent le même commutateur RNIS, ils peuvent communiquer à 64 Kbit/s. Sinon, ils doivent communiquer à 56 Kbit/s.

Etant donné que la ligne RNIS de Nick se connecte sur le site central au moyen du même commutateur que le routeur du site central, le numéro de téléphone — dans la commande `dialer map` — utilisé pour se connecter au routeur de Nick n'a pas besoin d'inclure le préfixe à trois chiffres.

Note : étant donné que le routeur de site central utilise des lignes qui font partie d'un Centrex, les numéros de téléphone pour les appels sortants commencent par un 9, s'ils ne sont pas composés de quatre chiffres.

La commande `dialer-group` associe l'interface BRI au groupe d'accès de numérotation 1. La commande `ppp authentication chap` active l'authentification CHAP.

Configuration du routage

Dans le listing de configuration relative au routage, la commande `router igrp` active le protocole IGRP (*Interior Gateway Routing Protocol*), et définit le système autonome avec le numéro 10. La commande `network` assigne le numéro de réseau. La commande `redistribute` envoie des informations de route statique (définies avec les commandes `ip route`) aux autres routeurs de la même zone IGRP. Sans cette commande, les autres routeurs connectés au site central ne disposeraient pas de chemin vers les routeurs distants.

DDR a tendance à faire une utilisation intensive des routes statiques, car les mises à jour de routage ne sont pas reçues lorsque la connexion par circuit commuté n'est pas active. Les deux premières commandes `ip route` créent les routes statiques qui définissent les sous-réseaux que Dave et Nick utilisent.

NOTE

Les commandes IGRP sont les mêmes sur tous les routeurs de site central ; cependant, les routes statiques correspondent aux sites à domicile qui appellent le routeur de site central.

Configuration de liste d'accès

DDR utilise des listes d'accès pour déterminer si un paquet est *intéressant* ou *inintéressant*. Si un paquet est intéressant, et qu'aucune connexion n'est active, un appel est établi. Si une connexion existe, elle est maintenue. Dans le listing de configuration, quatre lignes utilisent la commande `access-list` pour distinguer les paquets. Les première, deuxième et troisième commandes indiquent respectivement que les mises à jour IGRP, les paquets NTP (*Network Time Protocol*) et les paquets SNMP (*Simple Network Management Protocol*) sont inintéressants. Les quatrième et dernière commandes spécifient que tous les paquets IP sont intéressants. La commande `dialer-list` assigne l'ensemble des listes d'accès au groupe d'accès de numérotation 1.

Site à domicile

Les configurations des routeurs de sites à domicile sont analogues, mais celle de Nick est plus simple, car son routeur se connecte au même commutateur de bureau central que le routeur du site central.

Configuration de Nick

La configuration pour le routeur de Nick est la suivante :

```
hostname nick-isdn
!
username central-isdn password 7 050D130C2A5
isdn switch-type basic-dms100
!
interface ethernet 0
ip address 11.108.137.1 255.255.255.0
no mop enabled
!
interface bri 0
ip address 11.108.90.7 255.255.255.0
encapsulation ppp
no ip route-cache
isdn spid1 415555837601 5558376
isdn spid2 415555837802 5558378
dialer idle-timeout 300
dialer map ip 11.108.90.53 name central-isdn 8362
dialer map ip 11.108.90.53 name central-isdn 8370
dialer-group 1
ppp authentication chap
!
ip route 11.108.0.0 255.255.0.0 11.108.90.53
!
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 177
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
dialer-list 1 list 101
```

A l'instar du routeur du site central, la commande `isdn switch-type` indique que le commutateur est un dispositif NT DMS-100. Etant donné que le routeur de Nick se connecte au DMS-100, les identifiants de profil de service SPID (*Service Profile Identifier*) sont requis pour l'interface BRI. PPP et CHAP sont configurés à l'aide d'une commande `username` pour le routeur de site central. La configuration pour le routeur de Nick diffère de celle du site central en ce qui concerne les commandes `dialer map` et la section de routage. Deux commandes `dialer map` pointent vers la même adresse

de prochain saut. Si une tentative d'appel du premier numéro échoue, le second sera utilisé pour la connexion vers l'adresse de prochain saut.

Les commandes `isdn spid1` et `isdn spid2` représentent les identifiants SPID. Ils sont utilisés lorsqu'une interface BRI se connecte à un commutateur NorTel DMS-100 ou National ISDN-1. Les SPID sont assignés par le fournisseur de services afin d'associer un numéro de profil de service à un numéro de téléphone. Les autres types de commutateurs ne nécessitent pas de SPID. Votre fournisseur de services peut vous indiquer si votre commutateur exige ou non l'emploi d'identifiants SPID. Dans cet exemple, le SPID 1 identifie 415 comme étant le code de zone, 555 comme étant le code d'autocommutateur, 8376 comme étant l'identifiant de station et 01 comme étant l'identifiant de terminal. Le format de SPID requis par votre fournisseur de services peut différer des exemples présentés dans cette étude de cas.

Configuration de Dave

La configuration du routeur de Dave est analogue à celle du routeur de Nick, excepté qu'il ne se trouve pas dans le même Centrex que le site central de l'entreprise. Voici sa configuration :

```
hostname dave-isdn
!
username central-isdn password 7 08274341
isdn switch-type basic-5ess
!
interface ethernet 0
ip address 11.108.147.1 255.255.255.0
no mop enabled
!
interface bri 0
ip address 11.108.90.1 255.255.255.0
encapsulation ppp
no ip route-cache
bandwidth 56
dialer map ip 11.108.90.53 name central-isdn speed 56 14155558370
dialer-group 1
ppp authentication chap
!
ip route 11.108.0.0 255.255.0.0 11.108.90.53
!
dialer-list 1 list 101
```

Le routeur de Dave se connecte au commutateur RNIS de bureau central AT&T 5ESS, qui n'utilise pas la signalisation SS7. La commande `isdn switch-type` spécifie un commutateur AT&T, avec un débit de base qui n'exige pas l'emploi des commandes `isdn spid1` et `isdn spid2` que requiert le commutateur DMS-100. La commande `bandwidth` indique aux protocoles de routage que la ligne opère à 56 Kbit/s. La commande `dialer map` utilise le mot clé `speed` afin que la ligne soit établie à une vitesse de 56 Kbit/s lors d'un appel effectué vers le site central. Ce paramètre est nécessaire lorsque la connexion traverse un commutateur qui n'utilise pas la signalisation SS7.

Configuration des numéros d'identification de lignes appelantes

Etant donné que Nick se trouve dans le même Centrex que le routeur du site central, ce dernier peut utiliser le numéro d'identification de ligne appelante (CLID, *Calling Line Identification*) reçu du commutateur RNIS afin d'identifier Nick. Avec le service CLID, la configuration de Nick ne

nécessite pas l'emploi de CHAP ou PAP, mais elle doit être modifiée afin d'inclure le CLID. Les sections suivantes présentent les modifications apportées aux configurations des routeurs de Nick et du site central.

NOTE

Le service CLID n'est pas disponible dans toutes les régions des Etats-Unis, ni dans tous les pays. Certains pays ne nécessitent pas l'utilisation d'un Centrex pour le CLID.

Site central

Voici la configuration de l'interface PRI du site central, modifiée pour l'utilisation du CLID :

```
controller t1 1/0
framing esf
linecode b8zs
pri-group timeslots 2-6
!
interface serial 1/0:23
ip address 11.108.90.53 255.255.255.0
dialer idle-timeout 300
dialer map ip 11.108.90.7 name 5558376 8376
dialer-group 1
```

Le mot clé **name**, dans la commande **dialer map**, spécifie la chaîne réelle que l'identification de ligne appelante renvoie. Cette chaîne diffère du numéro appelé, celui-ci étant un numéro de Centrex à quatre chiffres ; le numéro retourné est le numéro complet à sept chiffres.

Site à domicile

A l'instar du site central, la principale différence dans la configuration de Nick est l'utilisation du mot clé **name**, avec la commande **dialer map**, qui spécifie le vrai numéro de ligne appelante renvoyé :

```
interface bri 0
ip address 11.108.90.7 255.255.255.0
no ip route-cache
isdn spid1 415555837601 5558376
isdn spid2 415555837802 5558378
dialer idle-timeout 300
dialer map ip 11.108.90.53 name 5558362 8362
dialer map ip 11.108.90.53 name 5558370 8370
dialer-group 1
```

NOTE

Si la commande EXEC **debug isdn-q931** est activée, le décodage pour un appel entrant peut être vu, et le numéro CLID apparaît.

Configuration du service de rappel (callback)

Etant donné que Dave est situé à plusieurs kilomètres du bureau central, les appels entrants sur le routeur du site central sont comptés et facturés sur son numéro. La fonction de rappel (introduite dans Cisco IOS 11.0) permet au routeur de Dave d'effectuer un appel pour demander au routeur du

site central de le rappeler. Lors d'un appel de Dave, le routeur central interrompt la connexion établie, puis rappelle le routeur appelant. Avec cette fonction, la facture téléphonique de Dave est réduite, car les transferts de données réels se produisent lorsque le routeur du site central rappelle. Les commandes suivantes configurent le rappel sur le routeur de Dave :

```
interface bri 0
ppp callback request
dialer hold-queue 100 timeout 20
```

La commande `ppp callback`, avec le mot clé `request`, spécifie que, lorsqu'une interface établit une connexion, c'est pour demander le rappel. La commande `dialer hold-queue` spécifie qu'un maximum de 100 paquets peuvent être maintenus dans une file d'attente, jusqu'à ce que le routeur de site central rappelle. S'il ne le fait pas dans un délai de 20 secondes, auquel on ajoute le délai d'expiration du temporisateur d'activation `enable-timeout`, les paquets sont supprimés. Les commandes suivantes configurent le routeur du bureau central :

```
map-class dialer class1
dialer callback-server username
interface serial 1/0:23
dialer map ip 11.108.90.1 name dave-isdn speed 56 class class1 914085553680
ppp callback accept
dialer callback-secure
dialer enable-timeout 1
dialer hold-queue
```

La commande `map-class` définit un paramètre de qualité de service (QoS), qui doit être associé à une entrée statique. Le mot clé `dialer` spécifie que l'entrée assignée est une correspondance de numérotation. Le paramètre `class1` est une valeur définie par l'utilisateur, qui crée une classe de correspondance à laquelle des commandes d'encapsulation spécifiques s'appliquent.

La commande `dialer map` a été modifiée afin d'inclure le mot clé `class` ainsi que le nom de la classe spécifiée dans la commande `map-class`. Le mot clé `name` est requis pour que, lors d'un appel en provenance du routeur de Dave, l'interface puisse localiser cette instruction de correspondance de numérotation, et obtenir la chaîne qui permet de le rappeler.

La commande `ppp callback`, avec le mot clé `accept`, permet à l'interface d'honorer les demandes de rappel qu'elle reçoit. Le service de rappel dépend du mécanisme d'authentification PPP, à savoir PAP ou CHAP.

La commande `dialer callback-server` permet à l'interface de retourner des appels, lorsque la demande a été négociée avec succès. Le mot clé `username` indique à l'interface de localiser la chaîne de numérotation pour le rappel, en recherchant le nom d'hôte authentifié dans la commande `dialer map`.

La commande `dialer callback-secure` spécifie que le routeur doit déconnecter l'appel initial, et rappeler uniquement s'il possède une commande `dialer map`, avec une classe définie pour le routeur distant. Dans le cas où la commande `dialer callback-secure` n'est pas présente, le routeur central ne relâchera pas la connexion si elle ne possède pas de commande `dialer map`, avec une classe définie. La commande `dialer enable-timeout` précise que l'interface doit attendre une seconde après la libération de la connexion initiale avant de rappeler.

Configuration du routage Snapshot sur RNIS

Le routage Snapshot représente une méthode simple qui permet de réduire les temps de connexion sur les réseaux RNIS, en supprimant le transfert des mises à jour de routage pour une période spécifiée. Il convient mieux sur les réseaux dont les connexions de transfert de données durent généralement plus de cinq minutes, et qui exécutent les protocoles par vecteur de distance suivants :

- RIP (*Routing Information Protocol*) et IGRP (*Integrated Gateway Routing Protocol*) ;
- RTMP (*Routing Table Maintenance Protocol*) pour AppleTalk ;
- RIP et SAP (*Service Advertisement Protocol*) pour Novell IPX (*Internet Packet Exchange*) ;
- RTP (*Routing Table Protocol*) pour Banyan VINES.

L'objectif du routage Snapshot est de permettre aux protocoles de routage d'échanger des mises à jour, comme ils le feraient normalement. Etant donné que EIGRP ainsi que les protocoles par état de lien, tels Novell NSLP (*Novell Link Services Protocol*), OSPF (*Open Shortest Path First*) et IS-to-IS (*Intermediate System-to-Intermediate System*), s'appuient sur l'envoi fréquent de messages Hello aux routeurs adjacents afin de découvrir et de maintenir les routes, ils sont incompatibles avec le routage Snapshot.

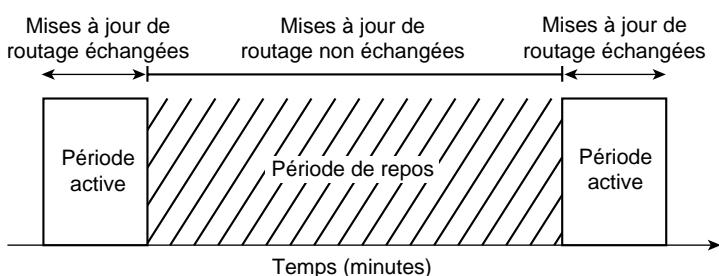
NOTE

Cette étude de cas applique le routage Snapshot sur un réseau RNIS, mais d'autres médias semblables, tels que les lignes louées dédiées, peuvent bénéficier de la réduction des mises à jour périodiques que le routage Snapshot assure.

Avant l'apparition du routage Snapshot, introduit avec la version 10.2 du système Cisco IOS, les interfaces RNIS étaient configurées au moyen de routes statiques. A l'instar des routes définies par les commandes `ip route` dans la section "Site central", plus haut dans ce chapitre, les routes statiques empêchent la bande passante d'être consommée par les mises à jour de routage. Elles sont toutefois difficiles à maintenir au fur et à mesure que le réseau grandit.

Le routage Snapshot supporte les routes dynamiques en autorisant les mises à jour de routage durant une période active, et réduit les coûts de connexion en supprimant les mises à jour qui se produisent durant une période de repos, qui peut atteindre 65 jours. Durant cette période de repos, les tables de routage des routeurs situés aux deux extrémités d'une liaison sont gelées. La Figure 21.2 illustre la succession de ces périodes.

Figure 21.2
Période active et période de repos.

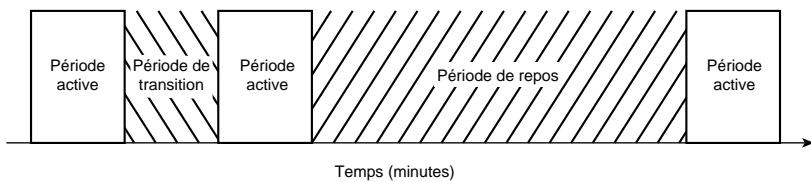


Durant la période active, les routeurs situés à chaque extrémité de la connexion s'échangent normalement les mises à jour pour leurs protocoles de routage configurés. Ils poursuivent ces échanges jusqu'à ce que la période active se termine. Ensuite, chaque routeur gèle ses tables de routage, arrête l'envoi des mises à jour, puis entre dans une période de repos. Chaque routeur demeure dans cet état jusqu'à ce qu'un temporisateur configurable expire. A ce moment, les routeurs initient une connexion pour envoyer et recevoir de nouveau les mises à jour.

Pour s'assurer que les tables de routage sont bien mises à jour, la période active doit être suffisamment longue, afin que plusieurs mises à jour soient échangées. Une période trop brève pourrait ne permettre qu'à une seule mise à jour de traverser la liaison. De plus, si la mise à jour est perdue, en raison du bruit par exemple, le routeur situé à l'autre extrémité pourrait considérer une route valide comme étant inutilisable, ou ne pas prendre connaissance d'une nouvelle route valide. Pour s'assurer que les mises à jour se produisent correctement, la période active doit représenter au minimum cinq minutes (c'est-à-dire trois fois plus que l'intervalle de mise à jour des protocoles de routage). Étant donné que les protocoles de routage mettent à jour leur table de routage durant la période active, comme ils le font normalement, il n'est pas nécessaire d'ajuster un temporisateur quelconque de protocole de routage.

Si la ligne n'est pas disponible lorsque le routeur passe de la période de repos à la période active, il entre dans une période de transition. Durant cette période, le routeur tente continuellement de se connecter, jusqu'à ce qu'il puisse entrer dans la période active (voir Figure 21.3).

Figure 21.3
Période de transition
durant laquelle
le routeur tente
continuellement
de se connecter.



Le Tableau 21.1 présente les durées minimale et maximale de chaque période.

Tableau 21.1 : Périodes de routage Snapshot

Période	Configurable	Durée minimale	Durée maximale
Active	Oui	5 minutes	100 minutes
Repos	Oui	5 minutes	65 jours
Transition	Non	8 minutes	8 minutes

Par défaut, le routage Snapshot autorise l'échange des mises à jour sur des connexions établies pour transférer les données utilisateur. Ainsi, en cas de besoin, le routage Snapshot force la connexion à durer aussi longtemps que la période active de mise à jour. Si vous ne souhaitez pas que les routeurs échangent des mises à jour sur les connexions utilisateur, utilisez le mot clé `suppress-state-change-updates`.

Evolution du réseau de télétravail

Le routage Snapshot convient bien sur la topologie hub-and-spoke du réseau de télétravail, décrit à la section "Configuration de DDR sur RNIS", au début de ce chapitre. Le routage Snapshot est conçu pour la relation client-serveur. Les routeurs clients, tels ceux des sites à domicile, déterminent la fréquence selon laquelle ils échangent les mises à jour, grâce à la configuration d'une période de repos ; le routeur serveur accepte les connexions Snapshot entrantes de la part de plusieurs routeurs clients.

NOTE

Le routage Snapshot n'est pas recommandé pour les topologies maillées. En effet, sur ces topologies, la configuration de routes statiques est plus efficace que le routage Snapshot.

Configuration du routeur central pour le routage Snapshot

Voici la configuration du routeur de site central, modifiée pour le routage Snapshot :

```
hostname central-isdn
!
username dave-isdn password 7 130318111D
username nick-isdn password 7 08274D02A02
isdn switch-type primary-dms100
!
interface ethernet 0
ip address 11.108.40.53 255.255.255.0
no mop enabled
!
controller t1 1/0
framing esf
linecode b8zs
pri-group timeslots 2-6
ip address 11.108.90.53 255.255.255.0
encapsulation ppp
dialer idle-timeout 300
dialer map ip 11.108.90.1 name dave-isdn speed 56 914085553680
dialer map ip 11.108.90.7 name nick-isdn 8376
dialer-group 1
isdn spid1 415555836201 5558362
isdn spid2 415555837002 5558370
snapshot server 5
ppp authentication chap
!
router igrp 10
network 11.108.0.0
redistribute static
!
! route vers nick-isdn
ip route 11.108.137.0 255.255.255.0 11.108.90.7
! route vers dave-isdn
ip route 11.108.147.0 255.255.255.0 11.108.90.1
!
access-list 101 deny igrp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!NTP
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123
!SNMP
```

```
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 161
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
!
dialer-list 1 list 101
```

Les commandes `ip route`, qui configuraient les routes statiques pour les sites à domicile, ont été supprimées de la configuration. La commande `snapshot server` active le routage Snapshot. La valeur "5" définit une durée de période active de cinq minutes.

— NOTE —

Le routage Snapshot doit être configuré sur des interfaces de rotation définies au moyen de la commande `dialer rotary-group`. Les interfaces RNIS étant par définition des interfaces de rotation, vous n'avez donc pas besoin d'utiliser cette commande sur des configurations RNIS.

Configuration du routeur distant pour le routage Snapshot

Voici la configuration du routeur du site de Dave, après modification pour le routage Snapshot :

```
hostname dave-isdn
!
username central-isdn password 7 08274341
isdn switch-type basic-5ess
!
interface ethernet 0
ip address 11.108.147.1 255.255.255.0
no mop enabled
!
interface bri 0
ip address 11.108.90.1 255.255.255.0
encapsulation ppp
no ip route-cache
bandwidth 56
dialer map snapshot 1 name central-isdn 14155558370
dialer map ip 11.108.90.53 name central-isdn speed 56 14155558370
dialer-group 1
snapshot client 5 43200 suppress-statechange-updates dialer
ppp authentication chap
!
dialer-list 1 list 101
```

Les commandes `ip route`, qui configuraient les routes statiques pour les sites à domicile, ont été supprimées de la configuration. La commande `dialer map snapshot` définit une correspondance (dont le numéro de séquence est 1), que le routeur utilise pour se connecter au routeur de site central pour l'échange de mises à jour de routage. Le mot clé `name` spécifie le nom du routeur distant qui est associé à la chaîne de numérotation. Etant donné que la commande `ppp authentication chap` active l'authentification CHAP, ce routeur reçoit le nom du routeur central lorsqu'il l'appelle, puis le compare avec le nom spécifié, à l'aide du mot clé `name`.

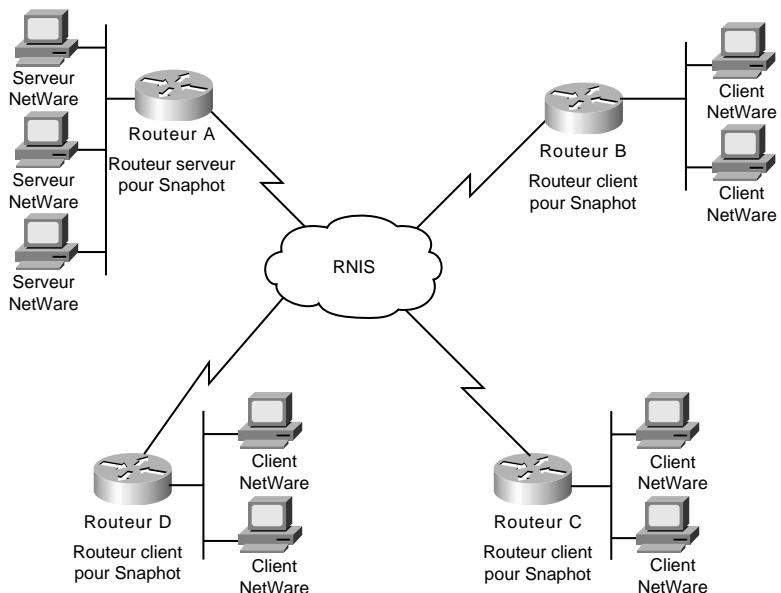
La commande `snapshot client` définit une période active de cinq minutes (la valeur doit correspondre à celle définie dans la configuration du serveur Snapshot), et une période de repos de 43 200 secondes (12 heures). Le mot clé `suppress-statechange-updates` empêche les routeurs d'échanger des mises à jour sur des connexions établies pour le transfert des données utilisateur. Le mot clé

dialer autorise le routeur client à appeler le routeur serveur en l'absence de trafic ordinaire ; il est nécessaire lorsque vous utilisez le mot clé `suppress-statechange-update`.

Réseau Novell IPX avec routage Snapshot

Cette section décrit un réseau Novell IPX pour lequel le routage Snapshot a été configuré. Les routeurs clients sur les sites d'agence utilisent DDR pour se connecter à un routeur central, *via* RNIS. Sur le site central, des serveurs NetWare utilisent le protocole Novell IPX pour fournir des services aux clients NetWare de chaque agence. Certaines connexions client-serveur sont nécessaires pendant une période limitée de la journée. La Figure 21.4 illustre ce réseau.

Figure 21.4
Topologie du réseau Novell IPX.



Sur cette topologie, les routeurs clients se chargent de la mise à jour de leur table de routage, en se connectant au routeur serveur lorsque la période de repos expire. Les routeurs clients recueillent également les informations de mises à jour lors d'un rechargeement.

NOTE

Le routage Snapshot fonctionne avec les réseaux Novell 3.x et 4.x. Toutefois, Novell 4.x inclut un protocole de synchronisation de temps, qui provoque l'envoi d'une mise à jour toutes les dix minutes par les serveurs de temps Novell 4.x. Pour empêcher ces serveurs de générer des paquets de mises à jour qui provoqueraient des connexions indésirables, vous devez charger un module NLM (*Netware Loadable Module*), nommé TIME-SYNC.NLM, qui vous autorise à étendre à plusieurs jours l'intervalle des mises à jour pour ces paquets. Un problème analogue est provoqué par les tentatives de synchronisation des réplications NDS de Novell. NetWare 4.1 inclut deux NLM, DSFILTER.NLM et PINGFILT.NLM, qui fonctionnent de concert, afin de contrôler les mises à jour de synchronisation NDS. Il est recommandé d'utiliser ces deux modules afin de vous assurer que le trafic de synchronisation NDS est envoyé uniquement aux serveurs spécifiés, et aux moments voulus.

Configuration du routeur serveur

Voici la configuration complète pour le routeur serveur :

```
hostname RouterA
!
username RouterB password 7 120D0A031D
username RouterC password 7 111D161118
username RouterD password 7 43E7528384
isdn switch-type vn3
!
ipx routing

interface Ethernet 0
ip address 192.104.155.99 255.255.255.0
ipx network 300
!
interface bri 0
ip address 1.0.0.1 255.0.0.0
encapsulation ppp
ipx network 10
no ipx route-cache
ipx update-time 20
ipx watchdog-spoof
dialer idle-timeout 60
dialer wait-for-carrier-time 12
dialer map ipx 10.0000.0000.0002 name RouterB broadcast 041389082
dialer map ipx 10.0000.0000.0003 name RouterC broadcast 041389081
dialer map ipx 10.0000.0000.0004 name RouterD broadcast 041389083
!
dialer-group 1
snapshot server 10
ppp authentication chap
!
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 457
access-list 901 deny 1 10.0000.0000.0001 0 10.ffff.ffff.ffff 453
access-list 901 deny 4 10.0000.0000.0001 0 10.ffff.ffff.ffff 452
access-list 901 deny 4 FFFFFFFF 0 FFFFFFFF 456
access-list 901 permit -1
!
dialer-list 1 list 901
```

La configuration commence avec le nom d'hôte utilisé pour l'authentification CHAP. Les noms d'utilisateurs correspondent au nom d'hôte des routeurs B, C et D. La commande `isdn switch-type` indique que le routeur se connecte à un commutateur français RNIS BRI VN3.

Configuration d'interface

La commande `dialer idle-timeout` spécifie une durée d'inactivité de 60 secondes, qui doit s'écouler avant que le routeur n'interrompe la connexion. La commande `dialer wait-for-carrier-time` définit une durée d'attente de porteuse de 60 secondes.

La commande `dialer map` définit l'adresse de prochain saut 10.0000.0000.0002 pour le routeur B. Lorsque le routeur B appelle le routeur serveur A, ce dernier utilise l'adresse de prochain saut pour transmettre les paquets vers le routeur B. Le mot clé `broadcast` définit 041389082 en tant qu'adresse pour les diffusions broadcast IPX. Les deuxième et troisième commandes `dialer map` définissent des valeurs analogues pour les routeurs C et D.

La commande `snapshot server` définit une période active de 10 minutes. La commande `ppp authentication chap` définit CHAP en tant que protocole d'authentification.

Configuration de liste d'accès

Les listes d'accès servent à déterminer si un paquet entrant ou sortant est intéressant ou inintéressant. Les paquets qui ne sont pas intéressants sont supprimés, les autres provoquent un appel si aucune connexion n'est active, ou maintiennent une connexion active existante. Cette configuration définit des listes d'accès étendues Novell IPX. Les première, deuxième, troisième et quatrième commandes `access-list` définissent respectivement comme étant inintéressants les paquets à destination du socket de sérialisation Novell, les paquets RIP, les paquets SAP, ainsi que les paquets générés par la fonction de découverte automatique de route. La dernière commande `access-list` précise que tous les autres paquets sont intéressants. La commande `dialer-list` assigne la liste d'accès 901 au groupe d'accès de numération 1, qui est lui-même associé à l'interface BRI 0, au moyen de la commande `dialer-group`.

Configuration du routeur client

Les configurations pour les routeurs clients sont les mêmes, à l'exception des commandes qui configurent le nom d'hôte du routeur, le nom utilisateur qu'il utilise lorsqu'il appelle le routeur A, ainsi que ses adresses de réseau. Voici la configuration du routeur B :

```
hostname RouterB
!
username RouterA password 7 105A060D0A
ipx routing
isdn switch-type vn3
isdn tei first-call
!
interface ethernet 0
ip address 192.104.155.100 255.255.255.0
ipx network 301
!
interface bri 0
no ip address
encapsulation ppp
ipx network 10
no ipx route-cache
ipx update-time 20
ipx watchdog-spoof
dialer idle-timeout 60
dialer wait-for-carrier-time 12
dialer map snapshot 1 name RouterA 46148412
dialer map ipx 10.0000.0000.0001 name RouterA broadcast 46148412
dialer-group 1
snapshot client 10 86400 dialer
ppp authentication chap
!
access-list 901 deny 0 FFFFFFFF 0 FFFFFFFF 457
access-list 901 deny 1 10.0000.0000.0002 0 10.ffff.ffff.ffff 453
access-list 901 deny 4 10.0000.0000.0002 0 10.ffff.ffff.ffff 452
access-list 901 deny 4 FFFFFFFF 0 FFFFFFFF 456
access-list 901 permit 0
!
dialer-list 1 list 901
```

La configuration commence avec le nom d'hôte utilisé pour l'authentification CHAP. Le nom d'utilisateur correspond au nom du routeur A. La commande `isdn switch-type` spécifie que le routeur se connecte à un routeur français RNIS BRI VN3.

La commande `isdn tei` utilise le mot clé `first-call` pour spécifier que la négociation du TEI RNIS (*Terminal Endpoint Identifier*, identifiant de terminaison de terminal) doit se produire lorsque le routeur A effectue ou reçoit son premier appel RNIS. Par défaut, elle se produit lorsque le routeur démarre.

Configuration d'interface

La commande `dialer wait-for-carrier` définit une période d'attente de la porteuse de 12 secondes, observée par l'interface lors d'un appel.

La commande `snapshot client` définit une période active de 10 minutes (la valeur doit correspondre à celle qui est configurée pour le serveur Snapshot), et une période de repos de 86 400 secondes (24 heures). Etant donné que le mot clé `suppress-statechange-updates` n'est pas utilisé, les routeurs peuvent échanger des mises à jour lors des connexions établies pour le transfert de données utilisateur. Le mot clé `dialer` autorise le routeur client à appeler le routeur serveur, en l'absence de trafic ordinaire.

Configuration d'AppleTalk sur RNIS

Pour exécuter efficacement AppleTalk sur un réseau RNIS, vous devez empêcher les paquets NBP (*Name Binding Protocol*) et les mises à jour RTMP de déclencher des connexions inutiles sur les lignes RNIS.

La Figure 21.5 présente un exemple de réseau AppleTalk, qui utilise RNIS pour connecter deux réseaux situés dans des villes différentes. Les utilisateurs sur le réseau du bureau régional ont parfois besoin d'accéder aux serveurs sur le réseau du bureau principal, et vice versa. Dans ce scénario, les deux routeurs s'appellent lorsque des données utilisateurs doivent être transmises dans l'autre partie du réseau.

Les utilisateurs des hôtes connectés au réseau du bureau principal n'ont pas besoin d'accéder à la zone Formation. Lors de la configuration du routeur A, un des objectifs est donc d'empêcher les paquets NBP générés par la zone Formation de déclencher une connexion RNIS avec le réseau du bureau principal. Un autre objectif de la configuration des deux routeurs est d'empêcher les paquets NBP générés par les imprimantes de chaque réseau de déclencher également des connexions RNIS.

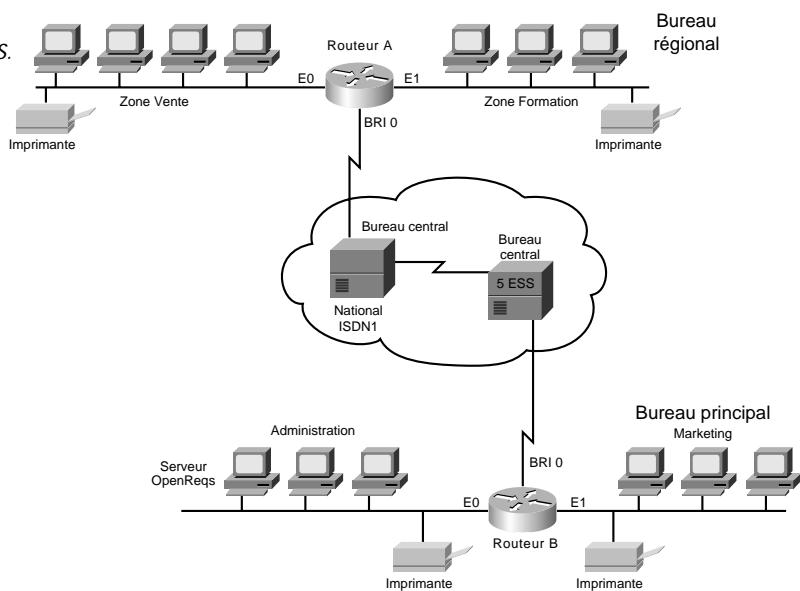
Pour contrôler la transmission des paquets NBP, utilisez les listes d'accès de style AppleTalk. Ces listes permettent de contrôler le flux des paquets NBP, en se fondant sur le type d'entité qui est à l'origine d'un paquet, sur son nom, ainsi que sur la zone où elle se trouve.

NOTE

La fonction qui permet de contrôler la transmission des paquets NBP a été introduite dans Cisco IOS version 11.0.

Figure 21.5

Réseau AppleTalk sur RNIS.



Les deux routeurs ont également besoin de contrôler les paquets RTMP. Pour cela, configurez les plages de câble (*cable ranges*) AppleTalk ainsi que les numéros de noeud, et utilisez la commande `no appletalk send rtmps` sur l'interface BRI ou PRI qui se connecte aux deux réseaux AppleTalk.

Configuration du routeur A

D'après la Figure 21.5, le routeur A est situé sur le bureau régional. Le réseau de ce bureau se compose de deux zones : Vente et Formation. Sur le routeur A, une liste d'accès de style AppleTalk est assignée à l'interface BRI 0 pour empêcher la transmission des paquets NBP qui proviennent des imprimantes et de la zone Formation. Si le routeur autorisait la transmission de ces paquets, ceux-ci provoqueraient l'établissement de connexions RNIS inutiles avec le réseau du bureau principal.

```

hostname RouterA
!
username RouterB password 7 125D063D2E
appletalk routing
appletalk static cable-range 20-20 to 15.43 zone Administration
appletalk static cable-range 25-25 to 15.43 zone Marketing
isdn switch-type basic-ni1
!
interface ethernet 0
appletalk cable-range 5-5 5.128
appletalk zone Sales
!
interface ethernet 1
appletalk cable-range 10-10 10.26
appletalk zone Service
!
interface bri 0
appletalk static cable-range 15-15 15.42

```

```
appletalk zone PhoneZone
no appletalk send-rtmps
encapsulation ppp
ppp authentication chap
dialer idle-timeout 240
bandwidth 56
dialer map appletalk 15.43 name RouterA speed 56 912065553240
dialer-group 1
isdn spid1 602555463101 5554631
!
access-list 601 deny nbp 1 type LaserWriter
access-list 601 deny nbp 2 zone Training
access-list 601 permit nbp 3 zone Sales
access-list 601 deny other-nbps
access-list 601 permit other-access
!
dialer-list 1 list 601
```

La commande `hostname` définit le nom d'hôte du routeur A. La commande `username` définit le nom du routeur qui est autorisé à appeler le routeur A, ici le routeur B. Le mot clé `password` indique que la commande `username` spécifie un mot de passe. La valeur "7" indique que le mot de passe est crypté au moyen d'un algorithme défini par Cisco. La commande `appletalk routing` active le routage AppleTalk.

Les commandes `appletalk static cable-range` créent des routes AppleTalk statiques vers les zones du réseau du bureau principal. Les routes statiques sont nécessaires, car la commande `no appletalk send-rtmps` empêche l'échange des mises à jour RTMP entre les deux réseaux. Sans ces routes statiques, les zones du bureau principal n'apparaîtraient pas lors de l'ouverture du sélecteur (chooser) sur les hôtes connectés au réseau du bureau régional. La commande `isdn switch-type` spécifie que le routeur se connecte à un commutateur National ISDN-1.

Configuration d'interface

Les commandes `appletalk cable-range`, pour chaque interface Ethernet, définissent le numéro de réseau pour le segment de câble auquel l'interface se connecte, ainsi que le numéro de noeud de l'interface. Pour chaque interface, la commande `appletalk zone` définit le nom de zone pour le réseau qui y est connecté. Aucune des configurations d'interface ne spécifie un protocole de routage AppleTalk ; les interfaces utilisent par conséquent le protocole de routage par défaut RTMP.

La commande `appletalk send-rtmps` empêche le routeur A d'envoyer des mises à jour RTMP sur l'interface BRI 0. Pour compenser l'absence d'échanges RTMP, vous devez configurer des routes statiques AppleTalk (au moyen de la commande `appletalk static cable-range`).

La commande `encapsulation ppp` spécifie l'encapsulation PPP ; la commande `ppp authentication chap` active l'authentification CHAP. La commande `dialer idle-timeout` définit une durée d'inactivité de 240 secondes (4 minutes). La commande `bandwidth` indique aux protocoles de routage que la ligne opère à une vitesse de 56 Kbit/s.

La commande `dialer map` définit le site distant que le routeur A doit appeler. Dans ce cas, elle définit 15.43 comme étant l'adresse de prochain saut. Le mot clé `name` définit le nom du routeur distant qui est associé à la chaîne de numérotation. Le mot clé `speed` spécifie que le routeur A doit établir un débit de ligne de 56 Kbit/s, requis lorsque la connexion traverse un commutateur qui ne

supporte pas la signalisation SS7. La commande `dialer-group` associe l'interface BRI 0 au groupe d'accès de numérotation 1.

Les commandes `isdn spid1` spécifient les identifiants de profil de service, ou SPID, qui sont requis par les commutateurs National ISDN-1. Les fournisseurs de services assignent ces identifiants afin qu'un numéro de téléphone leur soit associé. Votre fournisseur de services peut vous indiquer si votre commutateur exige l'utilisation de ces identifiants. Dans cet exemple, SPID 1 identifie 602 comme étant le code de zone, 555 comme étant le code d'autocommutateur, 4631 comme étant l'identifiant de station, et 01 comme étant l'identifiant de terminal.

Configuration de liste d'accès

La première commande `access-list nbp` définit la liste d'accès 601, et empêche la transmission des paquets NBP générés par toute imprimante LaserWriter sur le réseau du bureau régional. La deuxième commande `access-list nbp` empêche la transmission des paquets NBP générés par la zone Formation. La troisième commande `access-list nbp` autorise la transmission des paquets NBP générés par la zone Vente.

La commande `access-list other-nbps` empêche la transmission de tous les autres paquets NBP qui n'ont pas été explicitement autorisés, ou interdits, par les précédentes commandes `access-list nbp`.

La commande `access-list other-access` autorise tous les autres accès qui auraient autrement été rejetés, car non explicitement autorisés par une commande `access-list`. La commande `dialer-list` assigne la liste d'accès 601 au groupe d'accès de numérotation 1 associé à l'interface BRI 0.

Configuration du routeur B

A la Figure 21.5, le routeur B est connecté au réseau du bureau principal. Celui-ci se compose de deux zones : Marketing et Administration. A l'exception du serveur OpenReqs, dans la zone Administration, les utilisateurs des hôtes connectés au réseau du bureau régional n'ont pas besoin d'accéder au serveur situé dans la zone Administration. A l'instar du bureau régional, chaque zone du bureau principal possède sa propre imprimante. Le routeur B n'a donc pas besoin de transmettre les paquets NBP générés par les imprimantes. La liste d'accès pour le routeur B empêche les paquets NBP en provenance des imprimantes et de tous les serveurs de la zone Administration (à l'exception de OpenReqs) de déclencher une connexion RNIS vers le réseau du bureau régional :

```
hostname RouterB
!
username RouterA password 7 343E821D4A
appletalk routing
appletalk static cable-range 5-5 to 15.42 zone Sales
appletalk static cable-range 10-10 to 15.42 zone Training
isdn switch-type basic-5ess
!
interface ethernet 0
appletalk cable-range 20-20 20.5
appletalk zone Administration
!
interface ethernet 1
appletalk cable-range 25-25 25.36
appletalk zone Marketing
!
interface bri 0
```

```
appletalk static cable-range 15-15 15.43
appletalk zone PhoneZone
no appletalk send-rtmps
encapsulation ppp
ppp authentication chap
dialer idle-timeout 240
bandwidth 56
dialer map appletalk 15.42 name RouterB speed 56 917075553287
dialer-group 1
!
access-list 601 deny nbp 1 type LaserWriter
access-list 601 permit nbp 2 object OpenReqs
access-list 601 permit nbp 3 zone Marketing
access-list 601 deny other-nbps
access-list 601 permit other-access
dialer-list 1 list 601
```

La configuration pour le routeur B est analogue à celle du routeur A, à l'exception des points suivants :

- La commande `isdn switch-type` spécifie que le routeur B se connecte à un commutateur RNIS de bureau central AT&T 5ESS. Etant donné que ce type de commutateur n'utilise pas les numéros SPID, la commande `isdn spid1` n'est pas employée.
- La commande `access-list nbp` définit la liste d'accès 601, et empêche la transmission des paquets NBP générés par les imprimantes LaserWriter connectées au bureau principal. La deuxième commande `access-list nbp` autorise la transmission des paquets générés par le serveur OpenReqs. La troisième commande `access-list nbp` accepte la transmission des paquets générés par la zone Marketing.

Configuration de IPX sur RNIS

Lorsque IPX est utilisé en tant que protocole de niveau 3, RNIS peut être configuré comme illustré dans les exemples de cette section. Cette section décrit également le diagramme de réseau ainsi que les commandes de configuration utilisés.

Exemple de réseau pour la configuration de IPX sur RNIS

Sur le réseau suivant, l'adresse IPX interne, le réseau IPX, et l'adresse IPX de l'interface BRI du routeur ont été définis. Les numéros SPID ont également été configurés sur l'interface BRI.

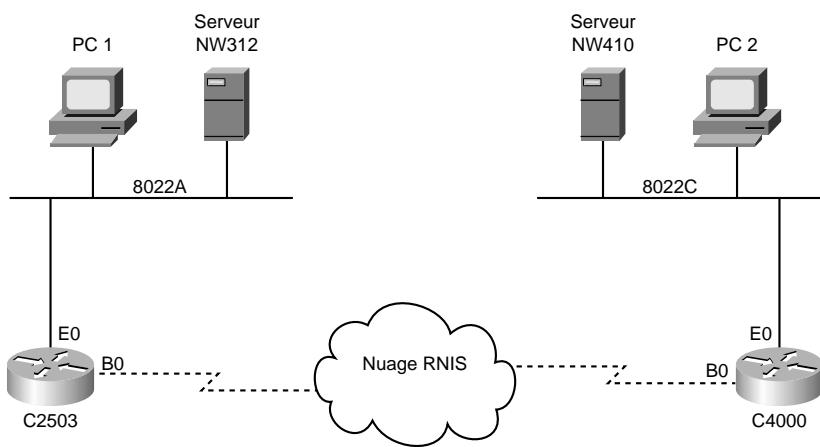
Les informations suivantes s'appliquent au réseau illustré à la Figure 21.6 :

Adresse IPX interne NW312	2EE67FE3.0000.0000.0001
Réseau IPX PC1/NW312	8022A
Adresse IPX interne NW410	301586E0.0000.0000.0001
Réseau IPX PC2/NW410	8022C
Adresse IPX interface B0 C2503	8022B.0000.0c09.509f
Numéros de téléphone RNIS C2503	4085554321 4085559876
SPID RNIS C2503	408555432101 5554321 408555987601 5559876

Adresse IPX interface B0 C4000	8022B.0000.0c02.e649
Numéros de téléphone RNIS C4000	4155551234 4155556789
SPID RNIS C4000	415555123401 5551234 415555678901 5556789

Figure 21.6

Configuration de IPX sur un réseau RNIS.



Configuration du routeur C2503

Le code suivant présente la configuration du routeur C2503 pour l'implémentation de IPX sur RNIS. Cette configuration inclut des numéros de ligne auxquels se référeront les explications données dans cette section :

```

1 C2503#wr t
2 #####
3 Current configuration:
4 !
5 version 10.2
6 !
7 hostname C2503
8 !
9 enable password test
10 !
11 username C4000 password cisco
12 ipx routing 0000.0c09.509f
13 ipx gns-response-delay 1000
14 isdn switch-type basic-dms100
15 !
16 interface Ethernet0
17 ipx network 8022A
18 ipx encapsulation SAP
19 !
20 interface Serial0
21 no ip address
22 shutdown

```

```
23 !
24 interface Serial1
25 no ip address
26 shutdown
27 !
28 interface BRI0
29 encapsulation ppp
30 bandwidth 56
31 ipx network 8022B
32 no ipx route-cache
33 ipx watchdog-spoof
34 dialer idle-timeout 300
35 dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast 14155551234
36 dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast 14155556789
37 dialer hold-queue 5
38 dialer load-threshold 100
39 dialer-group 1
40 isdn spid1 408555432101 5554321
41 isdn spid2 408555987601 5559876
42 ppp authentication chap
43 !
44 access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 452
45 access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 453
46 access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 457
47 access-list 900 permit -1
48 ipx route 8022C 8022B.0000.0c02.e649
49 ipx route 301586E0 8022B.0000.0c02.e649
50 !
51 ipx sap 4 NW410 301586E0.0000.0000.0001 451 2
52 !
53 !
54 dialer-list 1 list 900
55 !
56 line con 0
57 line aux 0
58 line vty 0 4
59 password test
60 login
61 !
62 end
```

Explication de la configuration du routeur C2503

Cette section propose une explication détaillée de la configuration du routeur C2503, en se référant aux numéros de ligne :

Lignes 1 à 11

```
C2503#wr t
#####
Current configuration:
!
version 10.2
!
hostname C2503
!
enable password test
!
username C4000 password cisco
```

Le nom d'utilisateur C4000 est le nom d'hôte du routeur distant ; il est utilisé par la commande `dialer map`. Le nom d'utilisateur est sensible à la casse, et doit donc correspondre exactement au nom d'hôte du routeur distant.

Le mot de passe, utilisé par le processus d'authentification CHAP, est également sensible à la casse, et doit donc être identique à l'entrée correspondante sur le routeur distant.

— NOTE —

Pour éviter toute confusion, la forme non cryptée du mot de passe `cisco` est donnée dans cet exemple de configuration. Dans la véritable configuration, le mot de passe apparaîtrait dans sa forme cryptée, c'est-à-dire :`7 13061E010803`, où 7 indique le type de cryptage, et `13061E010803` est le mot de passe crypté. Lorsque vous entrez ou modifiez la commande `username`, veillez à saisir le mot de passe dans sa forme non cryptée, sans spécifier le type de cryptage (7), qui est défini automatiquement.

Ligne 12

```
ipx routing 0000.0c09.509f
```

Cette commande active le routage IPX. Etant donné que le routeur associe l'adresse MAC de l'une de ses interfaces au processus, vous n'avez pas besoin de l'indiquer. Saisissez simplement la commande `ipx routing`.

Ligne 13

```
ipx gns-response-delay 1000
```

La commande SAP statique de la ligne 51 annonce le serveur distant, même lorsque la liaison RNIS n'est pas active. Par conséquent, il peut être nécessaire d'augmenter l'intervalle de temps qui doit s'écouler avant que le routeur ne réponde à la requête GNS (*Get Nearest Server*) d'une station de travail, afin de garantir que le serveur de fichiers local puisse répondre en premier.

Ligne 14

```
isdn switch-type basic-dms100
```

Le type de commutateur RNIS doit correspondre à l'équipement de votre opérateur. Si vous modifiez ce paramètre, vous devez recharger le routeur afin que le nouveau type devienne effectif.

Lignes 16 et 17

```
interface Ethernet0
ipx network 8022A
```

8022A est le numéro du réseau local. Pour déterminer ce numéro, saisissez `config`, à l'invite de console du serveur local, puis associez le numéro de réseau de l'interface du routeur au numéro de réseau du protocole LAN. Grâce à cette commande, vous n'avez pas besoin d'inclure les zéros de début, affichés pour le numéro de réseau du protocole LAN.

Ligne 18

```
ipx encapsulation SAP
```

Cette commande définit le type de trame Ethernet de l'interface, afin qu'il corresponde à celui du serveur de fichiers local. Pour déterminer le type de trame du serveur, saisissez **config**, à l'invite de console du serveur local, puis utilisez le type spécifié pour configurer l'encapsulation sur l'interface IPX du routeur.

Types de trames supportées par Cisco

Type de trame Novell	Encapsulation Cisco
Novell Ethernet_II	arpa
Novell Ethernet_802.3	novell-ether
IEEE 802.2	sap
IEEE 802.2 SNAP	snap

Lignes 20 à 29

```
interface Serial0
no ip address
shutdown
!
interface Serial1
no ip address
shutdown
!
interface BRI0
encapsulation ppp
```

L'encapsulation PPP est recommandée sur HDLC pour permettre l'utilisation de l'authentification CHAP.

Ligne 30

```
bandwidth 56
```

Le paramètre par défaut pour la bande passante d'une interface BRI est 64 Kbit/s. Si vous configuez vos instructions **dialer map** avec l'option **speed 56**, vous devrez inclure une commande **bandwidth** dans votre configuration.

NOTE

Cette commande ne contrôle pas la vitesse de la ligne RNIS, mais sert à définir le point de référence correct pour les statistiques **show interface de port BRI**, pour la commande **dialer load-threshold**, ainsi que pour les métriques de routage de IGRP/EIGRP.

Ligne 31

```
ipx network 8022B
```

8022B est le numéro de réseau IPX du segment RNIS pour les deux routeurs. Ce numéro devrait être unique pour votre réseau.

Ligne 32

```
no ipx route-cache
```

La mise en cache des routes IPX doit être désactivée lorsque la simulation watchdog IPX est activée.

Ligne 33

```
ipx watchdog-spoof
```

Cette commande permet au routeur de répondre aux paquets watchdog du serveur local, de la part du client distant. En l'absence de cette commande, les paquets watchdog du serveur seraient considérés comme intéressants, et activeraient la liaison RNIS.

Ligne 34

```
dialer idle-timeout 300
```

Cette commande définit le nombre de secondes pendant lequel une connexion RNIS demeure ouverte, lorsqu'aucun trafic intéressant n'est transmis. Le temporisateur est réinitialisé chaque fois qu'un paquet intéressant est transmis.

Lignes 35 et 36

```
dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast 14155551234  
dialer map ipx 8022B.0000.0c02.e649 name C4000 speed 56 broadcast 14155556789
```

La commande `dialer map` est utilisée avec l'authentification CHAP pour établir l'appel initial vers le routeur distant lorsqu'un trafic intéressant est envoyé vers l'interface BRI. Une fois la connexion active, la commande `dialer idle-timeout` détermine sa durée d'activité. Une instruction `dialer map` est nécessaire pour chaque numéro de téléphone RNIS qui doit être appelé. Toutefois, sachez que deux instructions `dialer map` pointant vers le même lieu pourraient activer deux canaux B, alors que l'utilisation d'un seul canal est souhaitée.

Les paramètres de cette commande sont les suivants :

- **8022B.0000.0c02.e649.** Adresse IPX de l'interface BRI du routeur distant. Pour déterminer cette adresse, saisissez `show ipx interface B 0`, à l'invite de console du routeur distant.
- **name C4000.** Nom d'hôte du routeur distant. Le nom est sensible à la casse ; il doit correspondre exactement à celui configuré avec la commande `username`, montrée plus haut.
- **speed 56.** Définit à 56 Kbit/s la vitesse de numérotation pour les circuits RNIS qui n'offrent pas 64 Kbit/s de bout en bout. Il est recommandé d'intégrer ce paramètre dans les instructions `dialer map` des deux routeurs. Aux Etats-Unis, la plupart des installations doivent être configurées pour une vitesse de 56 Kbit/s.
- **broadcast.** Autorise la transmission des paquets broadcast. Toutefois, l'utilisation de ce paramètre ne rend pas ces paquets intéressants. A moins que ces paquets ne soient explicitement spécifiés

comme étant intéressants *via* la commande **dialer-list**, ils sont uniquement transmis lorsque la liaison RNIS est active.

- **1415551234 1415556789.** Numéros de téléphone RNIS du routeur distant.

Ligne 37

```
dialer hold-queue 5
```

Cette commande autorise les paquets intéressants à être placés en file d'attente, jusqu'à ce que la connexion RNIS soit établie. Elle est particulièrement utile lorsqu'un identifiant d'ouverture de session NetWare est utilisé pour activer la connexion, afin d'empêcher la station de travail d'abandonner. Dans cet exemple, cinq paquets intéressants sont placés en file d'attente.

Ligne 38

```
dialer load-threshold 100
```

Cette commande est utilisée pour configurer la charge de trafic maximale supportée par le premier canal B ; lorsqu'elle est atteinte, le routeur établit un autre appel sur le second canal B. La charge de trafic est la valeur moyenne pondérée, calculée pour l'interface (où 1 signifie charge nulle, et 255 charge maximale). La valeur de charge à configurer dépend des caractéristiques de votre réseau. Dans cet exemple, le second canal B est activé lorsque la charge du premier canal B atteint 39 % de l'utilisation maximale, c'est-à-dire 100 divisé par 255.

Ligne 39

```
dialer-group 1
```

La commande **dialer-group 1** active la liste de numérotation 1 sur l'interface BRI qui détermine quels paquets intéressants activent la connexion RNIS.

Lignes 40 et 41

```
isdn spid1 408555432101 5554321  
isdn spid2 408555987601 5559876
```

Les commandes **isdn spid** sont utilisées lorsque votre opérateur assigne des SPID à vos lignes RNIS.

Ligne 42

```
ppp authentication chap
```

Cette commande active l'authentification CHAP.

Lignes 44 à 47

```
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 452  
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 453  
access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 457  
access-list 900 permit -1
```

Cette liste d'accès détermine quels paquets IPX sont intéressants et activent la liaison RNIS. La liste d'accès que vous devez créer dépend de la conception de votre réseau.

Pour cet exemple, les paramètres de cette commande sont les suivants :

- **access-list 900 deny -1 -1 0 -1 452.** Définit tous les paquets SAP comme étant inintéressants.
- **access-list 900 deny -1 -1 0 -1 453.** Définit tous les paquets RIP comme étant inintéressants.
- **access-list 900 deny -1 -1 0 -1 457.** Définit tous les paquets de sécurité comme étant inintéressants.
- **access-list 900 permit -1.** Définit tous les autres paquets comme étant intéressants.

Ligne 48

```
ipx route 8022C 8022B.0000.0c02.e649
```

Cette commande crée une route statique vers le réseau Ethernet du routeur distant, *via* son interface BRI. Elle est nécessaire, car les routes dynamiques sont perdues lorsque la liaison RNIS n'est plus active.

Pour cet exemple, les paramètres de cette commande sont les suivants :

- **8022C.** Numéro de réseau IPX externe du réseau distant. Pour déterminer ce numéro, saisissez **config**, à l'invite de console du serveur distant, puis associez le numéro de réseau à l'instruction de protocole LAN.
- **8022B.0000.0c02.e649.** Adresse de l'interface BRI du routeur distant. Pour déterminer cette adresse, saisissez **show ipx interface B 0**, à l'invite de console du routeur distant.

Ligne 49

```
ipx route 301586E0 8022B.0000.0c02.e649
```

La commande **ipx route** crée une route statique vers le serveur distant, *via* l'interface BRI du routeur distant. Elle est nécessaire, car les routes dynamiques sont perdues lorsque la liaison RNIS n'est plus active.

Pour cet exemple, les paramètres de cette commande sont les suivants :

- **301586E0.** Portion réseau de l'adresse IPX interne du serveur distant. Pour déterminer cette adresse, saisissez **show ipx servers**, à l'invite de console du routeur distant.
- **8022B.0000.0c02.e649.** Adresse IPX de l'interface BRI du routeur distant. Pour déterminer cette adresse, saisissez **show ipx interface B 0**, à l'invite de console du routeur distant.

Ligne 51

```
ipx sap 4 NW410 301586E0.0000.0000.0001 451 2
```

Cette commande crée une entrée SAP statique pour le serveur distant, que le routeur local annoncera, même si la liaison RNIS n'est pas active.

Pour cet exemple, les paramètres de cette commande sont les suivants :

- **4.** Type SAP (serveur).
- **NW410.** Nom du service SAP.
- **301586E0.0000.0000.0001.** Réseau IPX interne, et adresse d'hôte du serveur distant. Pour déterminer cette adresse, saisissez **show ipx servers**, à l'invite de console du routeur distant.

- **451.** Numéro de socket (port) du serveur distant, qui est déterminé au moyen de la commande `show ipx servers` sur le routeur distant.
- **2.** Compte de sauts RIP vers le serveur distant.

Ligne 54

```
dialer-list 1 list 900
```

Cette commande pointe vers la liste d'accès 900, qui détermine quels paquets IPX sont intéressants.

Lignes 56 à 62

```
line con 0
line aux 0
line vty 0 4
password test
login
!
end
```

Ces lignes se passent de commentaires.

Configuration du routeur C4000

Le code suivant présente la configuration du routeur C4000 pour l'implémentation de IPX sur RNIS. Pour obtenir une description des commandes, reportez-vous à la section "Explication de la configuration du routeur C2503 ", plus haut dans ce chapitre. Bien que cette explication concerne la configuration du routeur C2503, la description générale des commandes s'applique néanmoins :

```
1 C4000#wr t
2 #####
3 Current configuration:
4 !
5 version 10.2
6 !
7 hostname C4000
8 !
9 enable password test
10 !
11 username C2503 password cisco
12 ipx routing 0000.0c02.e649
13 ipx gns-response-delay 1000
14 isdn switch-type basic-dms100
15 !
16 interface Ethernet0
17 ipx network 8022C
18 ipx encapsulation SAP
19 !
20 interface Serial0
21 no ip address
22 shutdown
23 !
24 interface Serial1
25 no ip address
26 shutdown
27 !
28 interface BRI0
29 encapsulation ppp
```

```
30 bandwidth 56
31 ipx network 8022B
32 no ipx route-cache
33 ipx watchdog-spoof
34 dialer idle-timeout 300
35 dialer map ipx 8022B.0000.0c09.509f name C2503 speed 56 broadcast 14085554321
36 dialer map ipx 8022B.0000.0c09.509f name C2503 speed 56 broadcast 14085559876
37 dialer hold-queue 5
38 dialer load-threshold 100
39 dialer-group 1
40 isdn spid1 415555123401 5551234
41 isdn spid2 415555678901 5556789
42 ppp authentication chap
43 !
44 access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 452
45 access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 453
46 access-list 900 deny -1 FFFFFFFF 0 FFFFFFFF 457
47 access-list 900 permit -1
48 ipx route 8022A 8022B.0000.0c09.509f
49 ipx route 2EE67FE3 8022B.0000.0c09.509f
50 !
51 ipx sap 4 NW312 2EE67FE3.0000.0000.0001 451 2
52 !
53 !
54 dialer-list 1 list 900
55 !
56 line con 0
57 line aux 0
58 line vty 0 4
59 password test
60 login
61 !
62 end
```

Résumé

Lorsque vous configurez RNIS, le contrôle des paquets qui génèrent des connexions inutiles est un problème primordial à régler. Par le passé, il était possible de le résoudre en configurant des routes statiques. Le routage Snapshot et le filtrage des paquets NBP permettent de contrôler les mises à jour de routage. Le routage Snapshot permet de configurer le réseau, afin que les protocoles routés mettent à jour leur table de routage dynamiquement, sans déclencher des connexions RNIS fréquentes et coûteuses. Le routage Snapshot convient idéalement pour les réseaux relativement stables, sur lesquels toutes les mises à jour de routage passent par un seul routeur central. Ce chapitre a également examiné la configuration de RNIS dans un environnement IPX.

Amélioration de la sécurité sur les réseaux IP

Par Thomas M. Thomas II

C'est l'été, les enfants ont terminé l'école. Alors que les autoroutes et les aéroports sont envahis par les vacanciers, des interruptions de courant inexplicables touchent certaines parties des Etats-Unis. Les avions de ligne disparaissent mystérieusement des écrans de contrôle, puis réapparaissent, ce qui provoque des mouvements de panique dans de nombreux aéroports.

Des rumeurs sur l'existence d'un nouveau virus "Rosebud" se répandent dans les forums de discussion. Au même moment, les administrateurs système tentent de faire face à ce nouveau virus, de type "Melissa". Le virus, non content d'infecter le courrier électronique, s'attache aux navigateurs Web, accélérant sa prolifération par le biais d'activités de déni de service (*DoS, Denial of Service*) sur les sites de communication et de commerce électronique, via l'Internet. Un ralentissement inquiétant se fait sentir sur le Web.

Dans les principales grandes villes des Etats-Unis, des sections du service de télécommunications 911 connaissent des défaillances. Les responsables du Département de la défense américain découvrent que leurs services de messagerie électronique et de téléphonie sont interrompus. Et des officiers embarqués sur un navire de la U.S. Navy constatent que leur système informatique a été victime d'une attaque !

A mesure que ces incidents mystérieux et perturbateurs se généralisent, les indices des marchés financiers chutent brusquement. Une vague de panique envahit la planète. L'infrastructure qui relie les quatre coins du monde est sérieusement ébranlée, et commence à se retourner contre ses créateurs.

Pour une grande part, ce scénario s'est produit en 1997, lorsque 35 hackers engagés par l'agence américaine pour la sécurité nationale, la NSA (*National Security Agency*), ont simulé des attaques sur l'infrastructure électronique américaine.

Cet exercice de simulation, baptisé *Eligible Receiver*, a permis d'obtenir un accès de niveau root sur 36 000 des 40 000 réseaux du Département de la défense américain. Ces attaques ont également paralysé des sections entières du réseau électrique national, perturbé le service 911 à Washington D.C., ainsi que dans d'autres villes, et permis d'accéder aux systèmes informatiques d'un navire de la marine américaine.

Bien que cet exercice ait été initié aux Etats-Unis, qui regroupent environ 40 % de la puissance informatique de la planète, la menace du cyber-terrorisme et de la guerre de l'information est bien mondiale. Les incidents suivants vous donneront une idée de l'étendue des risques :

- Durant la guerre du Golfe, des pirates hollandais se sont introduits dans des ordinateurs du Département de la défense américain, afin d'y dérober des informations concernant les mouvements des troupes américaines, en vue de les vendre aux Irakiens. Ces derniers, pensant qu'il s'agissait d'un canular, ont décliné cette offre...
- En 1997 et 1998, un jeune Israélien, qui se faisait appeler "The Analyzer", aurait pénétré sur les ordinateurs du Pentagone, avec l'aide d'adolescents californiens. Ehud Tenebaum, 20 ans, a été inculpé à Jérusalem, en février 1999, pour association de malfaiteurs et préjudices envers des systèmes informatiques.
- En février 1999, des pirates non identifiés ont pris le contrôle d'un satellite militaire de télécommunications britannique, exigeant de l'argent pour sa restitution. Cet incident a été vivement récusé par les responsables militaires britanniques.
- En janvier 1999, le président Bill Clinton a annoncé qu'une somme de 1,46 milliards de dollars serait consacrée à la sécurité informatique du gouvernement américain, ce qui représente une augmentation de 40 % par rapport à 1998. Le Pentagone, qui est la forteresse militaire de la nation la plus puissante du monde, est particulièrement concerné, puisqu'il est également connu comme étant la cible de choix des pirates, leur Saint Graal.

Il est clair que les sites gouvernementaux ne représentent qu'une partie des cibles recherchées par ceux qui mènent cette guerre de l'information. Dans la plupart des cas, l'expérience a démontré qu'il était plus avantageux pour les pirates d'attaquer des réseaux d'entreprises. C'est pourquoi des compétences expertes en matière de sécurisation des réseaux sont obligatoires dans de tels environnements. Le droit à l'erreur est à exclure lorsqu'il s'agit de protéger un réseau. Une seule vulnérabilité peut mettre en péril toutes les données du réseau, l'élément vital de l'entreprise. Que la menace provienne d'un concurrent qui recherche des secrets industriels, d'un individu mal intentionné visitant votre réseau, ou d'employés mécontents qui souhaitent se venger, il en résulte invariablement des pertes financières (secrets industriels dérobés, immobilisation du réseau, ou altération des données).

Services de sécurité Cisco

Pour toutes ces raisons, Cisco offre des services de conseil en sécurité des réseaux, qui mettent à profit son expertise hautement spécialisée et non égalée dans ce domaine, fondée sur des années d'expérience dans les domaines militaire et de la sécurité nationale.

Plutôt que se consacrer entièrement à des exercices d'application de stratégies de sécurité, puis à leur analyse, les équipes de consultants en sécurité de Cisco se concentrent sur les moindres détails du réseau, c'est-à-dire sur la localisation des vulnérabilités, la recherche de solutions et, dans les moments difficiles, sur l'expulsion d'intrus hors du réseau. Deux types de services principaux sont proposés :

- les services SPA (*Security Posture Assessments*) d'évaluation de l'état de la sécurité ;
- les services ICR (*Incident Control and Recovery*) de rétablissement et de contrôle après incident.

Les ingénieurs en sécurité de Cisco fournissent des services SPA. Ces évaluations comprennent une analyse exhaustive de la sécurité de réseaux distribués à grande échelle, à la fois d'un point de vue extérieur (celui du pirate), et d'un point de vue intérieur (celui de l'employé mal intentionné). Les informations relatives aux failles de sécurité sont compilées, analysées, puis présentées en détail au client. Elles s'accompagnent de recommandations fonctionnelles en vue de sécuriser le réseau de l'entreprise et d'atteindre un potentiel de gestion optimal.

Des services de rétablissement et de contrôle après intrusion, qui consistent en des déploiements rapides sur des sites clients, afin de mettre fin à des attaques en cours, sont également disponibles pour des clients qualifiés.

Evaluation de l'état de la sécurité

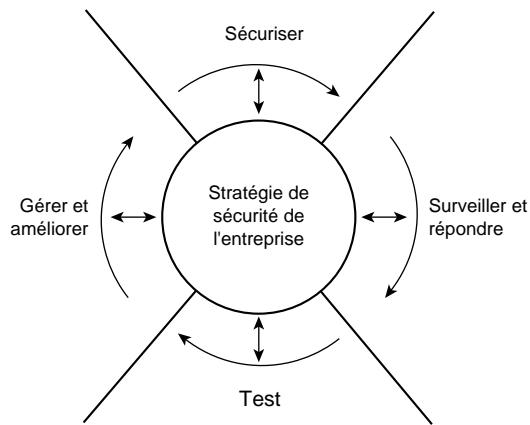
Avant qu'une entreprise puisse entreprendre les étapes nécessaires à l'amélioration de la sécurité de son réseau, elle doit établir un bilan précis de ses vulnérabilités. En offrant une vision de la sécurité sur la durée, et en adoptant une approche unique de quantification du niveau de sécurité actuel du réseau, les services SPA (*Security Posture Assessments*) de Cisco peuvent aider une entreprise à comprendre de façon efficace et objective l'état de sécurité de son réseau, et à identifier les zones à améliorer.

Lors de la mise en œuvre de ces services, les experts en sécurité de réseau de Cisco examinent la connectivité interne et externe du réseau client afin de déterminer les éléments suivants :

- efficacité des mécanismes de protection actuels ;
- étendue actuelle de chaque vulnérabilité de niveau réseau ;
- capacité de l'entreprise à détecter une attaque et à y répondre.

Les services SPA représentent davantage qu'un simple test de simulation d'intrusion, qui ne contrôle que certains points d'accès. En effet, les équipes de sécurité de Cisco fournissent un ensemble complet de données sur toutes les failles de sécurité, ainsi que les moyens potentiels d'obtenir un accès non autorisé à l'intégralité du réseau. La première phase de la simulation SPA consiste à examiner le réseau depuis l'extérieur, comme le ferait un pirate *via* l'Internet ou une liaison commutée. La seconde phase permet d'explorer le réseau depuis l'intérieur, comme le ferait un employé mal intentionné (voir Figure 22.1).

Figure 22.1
Roue d'évaluation de la sécurité.



Les ingénieurs en sécurité de Cisco valident, puis confirment la présence de chacune des vulnérabilités spécifiques détectées, en réalisant des pénétrations étendues non destructrices sur le réseau, en vue de déterminer plus précisément le niveau d'accès non autorisé pouvant être obtenu.

Plus précisément, le processus SPA inclut les étapes suivantes :

- Cartographie du réseau et analyse de cible, afin de déterminer la topologie du réseau, de mettre en évidence sa présence sur l'Internet grâce aux informations collectées dans des rapports publics et privés de l'entreprise, et de fournir une vision exacte du degré de probabilité d'une attaque réussie.
- Découverte d'hôtes et de services, afin de déterminer le nombre d'hôtes présents sur le réseau, et d'identifier les services de réseau exécutés actuellement par chaque hôte.
- Analyse des vulnérabilités, afin de déterminer toutes les failles potentielles qui existent pour chaque service de réseau exécuté, sur chaque hôte identifié. Cette phase inclut également une analyse complémentaire qui consiste, dans un premier temps, à confirmer la présence de ces vulnérabilités sur des systèmes spécifiques, en exploitant les failles potentielles qui ont été identifiées, puis à déterminer quelles vulnérabilités additionnelles pourraient être exploitées lorsque celles de premier niveau le sont de façon appropriée.
- Mesure du niveau de vulnérabilité, et collecte des données qui permettent d'identifier les méthodes d'accès non autorisées auxquelles le réseau est exposé, via l'exploitation des failles du réseau, au moyen d'outils SPA spécialisés.
- Analyse des données, et révision de la conception de la sécurité dans le cadre d'une comparaison des résultats de tests avec les exigences fonctionnelles actuelles, afin d'identifier les failles critiques.
- Recommandations et rapports permettant d'identifier les moyens de protection optimaux qui peuvent être déployés, ainsi que conclusions et recommandations spécifiques pour chaque système, à l'attention des responsables de l'entreprise, des administrateurs système et des utilisateurs.

Les ingénieurs en sécurité de Cisco présentent les données de résultat dans des rapports détaillés, ainsi que lors de réunions. Ils expliquent les failles de sécurité, à la fois aux responsables de l'entreprise et aux ingénieurs de réseau, de façon concise et strictement confidentielle. Outre les recommandations relatives aux améliorations spécifiques au niveau de la sécurité, le processus SPA donne également aux clients des mesures qui leur permettent de caractériser l'état de sécurité de leurs réseaux et systèmes. Ces données peuvent ensuite être exploitées, afin de définir un profil de base de la sécurité du réseau d'entreprise, ou de mesurer les améliorations progressives et les orientations à envisager, eu égard à des évaluations précédentes.

Afin de maintenir la sécurité sur des réseaux en constante évolution, Cisco recommande aux entreprises de procéder régulièrement à des évaluations SPA, dans le cadre d'un programme continu de protection des informations d'entreprise. De plus, les clients Cisco ont trouvé utile de faire réaliser des évaluations SPA avant et après des changements majeurs sur leur réseau, telles qu'une fusion de réseaux résultant du rachat d'une entreprise ou bien l'implémentation d'un site Internet de commerce électronique. Ces examens périodiques permettent d'éliminer les risques de violation de la sécurité qu'introduisent invariablement les changements qui surviennent sur de tels réseaux.

Contrôle et rétablissement après incident

Bien que les entreprises ignorent souvent les failles de sécurité qui existent sur leur réseau, elles reconnaissent parfois qu'un incident s'est produit ou est en train de se produire. Dans le cas d'une intrusion, une entreprise ne doit pas uniquement mettre un terme à l'activité malveillante en cours, mais également connaître l'heure à laquelle elle a commencé, sa source, son type, et son étendue. De plus, elle doit pouvoir disposer immédiatement de ces informations, car l'immobilisation du réseau et l'altération des données ont une conséquence directe sur les résultats financiers.

Les services ICR (*Incident Control and Recovery*) de Cisco assistent les clients qui sont victimes d'attaques. Les ingénieurs en sécurité réseau de Cisco sont déployés sur le site du client dans les heures qui suivent sa demande d'assistance. Une fois sur le site, l'équipe ICR collabore étroitement avec les administrateurs de réseau et le personnel de sécurité, afin de répondre aux priorités fonctionnelles du client, au moyen des services ICR appropriés, qui peuvent inclure :

- Isolation des hôtes et réseaux victimes pour limiter l'activité douteuse et empêcher qu'elle ne s'étende davantage.
- Reconfiguration des ressources du réseau pour que le client puisse revenir en ligne en toute sécurité.
- Confirmation de l'incident de sécurité.
- Identification de l'heure(s), de la source(s), et des moyens d'intrusion.
- Identification des ressources affectées et quantification des pertes.
- Assistance dans la récupération des données.
- Réalisation d'une évaluation SPA pour identifier d'autres failles.
- Proposition de solutions de sécurité, afin d'éviter des incidents de sécurité futurs.

Les professionnels Cisco possèdent une grande expérience dans la fourniture de services ICR. Ils ont développé des outils spécialisés pour des analyses légales, l'évaluation des dégâts, et la limitation des intrusions. Ces services font l'objet d'une offre limitée, et dépendent de la disponibilité du personnel qualifié.

Vous trouverez davantage d'informations sur les services de conseil en sécurité de Cisco, ainsi que sur tous ses produits, services et technologies de sécurité en visitant le site www.cisco.com/security.

La guerre de l'information a-t-elle lieu ?

La guerre de l'information se déroule partout autour de vous, comme le confirment les médias. C'est pourquoi la sécurité doit être prise en compte à chaque étape de la conception de votre réseau. La menace est réelle, comme le montrent certains articles et récits récents :

- "Urgent Care Needed, Stat", *Internet Week*, 1^{er} mars 1999.
- "Cyber-Vigilantes Hunt Down Hackers", *Network World*, 12 janvier 1999, www.nwfusion.com.
- "Large Companies Now See Outside Security Threat", *Computerworld*, 17 août 1998.
- "Cyberweapons: Information Warfare", Radio Free Europe/Radio Liberty, 28 juillet 1998, www.rferl.org.
- "Security Breach", *Computerworld*, 15 juin 1998, www.computerworld.com.
- "Attacks Spur Intrusion-Detection Efforts", *Internet Week*, 28 mai 1998.

NOTE

Ces documents ne représentent qu'une infime partie des informations disponibles sur le sujet, mais ils permettent de voir que cette guerre est bien réelle. Votre réseau est-il protégé ? Seriez-vous en mesure de déceler une attaque éventuelle ?

Cette guerre s'intensifie au fur et à mesure que le commerce électronique se développe. L'Internet est la première ressource véritablement mondiale, regroupant des individus du monde entier au sein d'une communauté virtuelle. Et, à l'image de toutes les grandes communautés, certaines personnes respectent les règles, d'autres les enfreignent.

La sécurité a probablement été l'un des aspects le plus ignorés du fonctionnement et de la conception des réseaux. Au fur et à mesure que les réseaux d'entreprise évoluent et se connectent à l'Internet, cet aspect est devenu un souci majeur pour la plupart des organisations. Cette inquiétude est, bien entendu, justifiée, mais la prise de conscience est lente. Des statistiques récentes effectuées par FBI estiment à 10 milliards de dollars la perte financière subie par les entreprises américaines en 1997, suite aux intrusions sur leurs réseaux. Ce chiffre dépasse le montant du produit national brut de nombreux pays. Vu sous cet angle, vous pouvez plus facilement comprendre pourquoi certains individus consacrent toute leur énergie au piratage informatique. Même si votre réseau n'est pas victime d'une intrusion en ce moment, d'autres réseaux le sont. Comme mentionné précédemment, les médias témoignent de l'intensification de la guerre de l'information, et bon nombre des plus importantes sociétés au monde font également état de menaces et de failles de sécurité.

Menaces de la guerre de l'information

Les informations suivantes proviennent de la page d'accueil du site de la société Cisco (<http://www.cisco.com>). Elles concernent des annonces que la société Cisco a formulées récemment au sujet de la sécurité. Ces annonces sont même plus importantes que celles mentionnées précédemment, car

Cisco, en tant que numéro un mondial des équipements de réseau, a déjà reconnu cette menace, et développe des solutions pour s'en protéger.

L'infrastructure de campus est vulnérable aux attaques initiées par un très grand nombre d'intrus, divers et difficiles à détecter. Parmi les types d'intrus les plus courants, on trouve :

- les employés actuels : ce groupe est parfois le plus difficile à détecter et à éviter, en raison des relations de confiance qui existent entre le personnel et son employeur ;
- les anciens employés ;
- les employés ou utilisateurs qui initient des activités de façon involontaire ;
- les employés qui exploitent l'environnement informatique en dépit du bon sens ;
- les espions.

Motivations des cyber-pirates

Les objectifs de la guerre de l'information sont aussi variés que leurs acteurs, et il semble que chacun d'eux possède une raison différente d'opérer. Par exemple, certaines des menaces peuvent provenir des catégories d'individus suivantes :

- les individus à la recherche de sensations ;
- les employés hostiles ;
- les espions et les escrocs ;
- les individus à la recherche de reconnaissance ;
- les individus qui souhaitent faire une déclaration ou se faire entendre ;
- les groupes radicaux et marginaux.

Les motivations de ces individus sont diverses. Voici les plus courantes :

- profit, vol ;
- vengeance, revanche ;
- anarchie ;
- ignorance, ennui, curiosité ;
- espionnage (industriel ou national) ;
- défi, amusement.

Vulnérabilité des réseaux

L'infrastructure de réseau de campus est vulnérable à de multiples menaces de sécurité :

- sécurité physique insuffisante ;
- accès aux ports de console et Telnet d'équipements de réseau ;
- accès aux réseaux internes sensibles ;
- routage erroné, *via* des mises à jour de routage avec usurpation de l'adresse source ;
- accès aux configurations d'équipements, *via* des chaînes de communauté SNMP.

Vulnérabilité de l'authentification CHAP de Cisco

Le protocole CHAP (*Challenge Handshake Authentication Protocol*) est une fonctionnalité de sécurité qui permet d'éviter des accès non autorisés. Il est supporté sur les lignes qui utilisent l'encapsulation PPP. CHAP n'empêche pas lui-même l'accès, mais identifie l'extrémité distante, de façon que le routeur ou le serveur d'accès puisse ensuite déterminer si un utilisateur possède un accès autorisé.

Une faille de sécurité sérieuse (identifiant de bogue : CSCdi91594) existe dans le mécanisme d'authentification CHAP de PPP de toutes les versions "classiques" du logiciel Cisco IOS. Cette vulnérabilité permet à des intrus qui possèdent les compétences et connaissances appropriées de contourner totalement le processus d'authentification. Les autres méthodes d'authentification de PPP ne sont pas concernées.

Attaques par déni de service avec boucle TCP (land.c)

Un programme lancé sur l'Internet, nommé `land.c`, peut être utilisé pour initier des attaques par déni de service contre différentes implémentations de TCP. Ce programme envoie un paquet TCP SYN (initiation de connexion) en utilisant comme adresse source et de destination l'adresse de l'hôte cible.

Attaques par déni de service "smurf"

L'attaque "smurf", qui tire son nom du programme exécuté, est la plus récente dans la catégorie des attaques de niveau réseau contre des hôtes. Un individu malveillant envoie un paquet d'écho ICMP (ping) vers une adresse broadcast. Ce paquet contient une adresse source (*spoofed source address*) usurpée à une victime. Si l'équipement de routage intermédiaire qui reçoit ce paquet initie une diffusion broadcast IP sur le réseau, la plupart des hôtes accepteront la requête d'écho ICMP, et enverront un paquet de réponse d'écho ICMP en retour, multipliant ainsi le trafic par le nombre d'hôtes répondants. Sur un réseau broadcast multi-accès, cette attaque peut provoquer de graves problèmes de congestion du réseau, mais également de l'hôte dont l'adresse a été usurpée, auquel toutes les réponses ICMP sont envoyées.

Attaques par déni de service vers port de diagnostic UDP

Lors de cette attaque, un émetteur transmet une grande quantité de requêtes pour des services de diagnostic UDP sur le routeur. Toutes les ressources processeur sont ainsi consommées pour satisfaire ces fausses requêtes. Les FAI sont exposés à un risque d'attaque par déni de service qui a pour cible les équipements de réseau.

Cryptage des mots de passe Cisco IOS

Une source non Cisco a récemment publié un nouveau programme, qui permet de décrypter les mots de passe utilisateur (et d'autres mots de passe) dans les fichiers de configuration Cisco. Ce programme ne peut pas décrypter ceux qui ont été définis au moyen de la commande `enable secret`.

Eu égard à l'inquiétude soudaine que ce programme a soulevé parmi les clients Cisco, il semblerait qu'ils soient nombreux à s'appuyer sur la fonction de cryptage de mots de passe Cisco pour un

niveau de sécurité supérieur à celui qu'elle offre réellement. Ce chapitre décrit le modèle de sécurité sous-jacent à cette fonction de cryptage, ainsi que ses limitations en matière de sécurité.

Evaluation des besoins en sécurité

Au fur et à mesure que le nombre d'utilisateurs qui accèdent à l'Internet augmente et que les sociétés étendent leurs réseaux, il devient de plus en plus difficile d'assurer la sécurité des réseaux internes. Les entreprises doivent donc déterminer les zones de leurs réseaux internes à protéger, apprendre à limiter l'accès utilisateur à ces zones, et identifier les types de services qui devraient être filtrés pour éviter les risques de failles dans la sécurité.

Il apparaît aujourd'hui de façon évidente que la sécurité doit représenter une préoccupation majeure à tous les niveaux du réseau. Evitez d'être trop rapidement satisfait lorsqu'il est question de sécurité. La sophistication rapide des technologies implique que l'efficacité des mesures de sécurité que vous avez implantées n'est que de courte durée.

La sécurité des réseaux est un vaste sujet, qui peut être abordé au niveau liaison de données, ou média (c'est-à-dire là où les problèmes d'usurpation d'adresses et de cryptage se manifestent), au niveau réseau, ou protocole (là où les paquets IP et les mises à jour de routage sont contrôlés), ou au niveau application (là où les bogues qui interviennent sur les hôtes deviennent des problèmes).

Cisco Systems fournit plusieurs fonctionnalités de la couche réseau, ou protocole, afin d'améliorer la sécurité sur les réseaux IP. Ces fonctionnalités incluent des méthodes de contrôle qui permettent de restreindre l'accès aux routeurs et aux serveurs de communication, par le biais de ports de console, Telnet, SNMP (*Simple Network Management Protocol*), TACACS (*Terminal Access Controller Access Control System*), cartes d'accès (*token card*), et de listes d'accès. La création d'architectures pare-feu est également étudiée dans ce chapitre.

ATTENTION

Bien que cette étude de cas aborde des problèmes de sécurité de la couche réseau — les plus significatifs dans le contexte d'une connexion Internet —, le fait d'ignorer la sécurité de niveau hôte peut se révéler dangereux, même en cas de mise en œuvre d'un filtrage de niveau réseau. Pour savoir quelles mesures de sécurité de niveau hôte peuvent être implémentées, reportez-vous à la documentation de vos applications et aux suggestions de lectures répertoriées à la fin de ce chapitre.

Stratégies de sécurité

Les stratégies de sécurité représentent un sujet d'étude pour les cyber-pirates. Il s'agit en fait d'un élément constitutif des procédures de sécurité mises en œuvre sur un réseau. La citation suivante est extraite du RFC 2196, intitulé *Site Security Handbook* :

"Une stratégie de sécurité est une déclaration formelle des règles auxquelles doivent se soumettre les utilisateurs ayant accès aux ressources technologiques et informatives d'une entreprise."

Une stratégie de sécurité doit couvrir à la fois les aspects de sécurité internes et externes. En effet, les menaces proviennent des deux côtés, ce qui oblige à prendre en compte tous les risques si on veut protéger correctement son réseau.

Ces stratégies présentent de nombreux avantages, et méritent par conséquent le temps et les efforts consacrés à leur développement. La liste suivante présente les raisons qui justifient leur création :

- Fournir un processus de contrôle de la sécurité du réseau existant.
- Aider à déterminer les outils et procédures nécessaires à l'entreprise.
- Aider un groupe de décideurs à se mettre d'accord, et à définir les responsabilités des utilisateurs et des administrateurs.
- Permettre une implémentation et une application globale de la sécurité. La sécurité informatique concerne aujourd'hui tous les secteurs de l'entreprise, et les sites doivent tous se conformer à la stratégie de sécurité du réseau.
- Créer une base de référence pour pouvoir intenter un procès en cas de besoin.

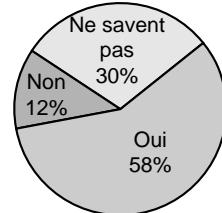
De nombreuses sociétés ont implanté des stratégies de sécurité dans le cadre de leur programme de sécurité de réseau. Ces stratégies fournissent un ensemble accessible de standards qui permettent de déterminer les actions à entreprendre, et préconisent une procédure de réponse en cas d'attaque, afin que tous les utilisateurs soient à la fois informés et responsables.

La Figure 22.2 est extraite d'une étude menée par WarRoom Research. Elle illustre le niveau de risque auquel sont exposées les sociétés du classement Fortune 1000. Pour obtenir davantage d'informations sur cette étude, visitez le site <http://www.warroomresearch.com/ResearchCollabor/SurveyResults.htm>.

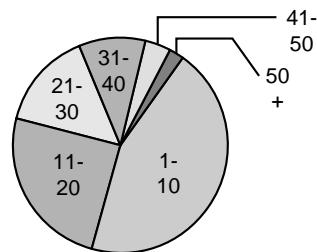
Figure 22.2

Les résultats de l'étude de WarRoom Research démontrent que la majorité des sociétés interrogées ont été victimes d'intrusions l'an passé.

Plus de 200 sociétés du classement Fortune 1000 ont été interrogées pour savoir si elles ont détecté des tentatives d'accès non autorisés de la part d'intrus au cours des 12 derniers mois



Parmi celles qui ont répondu oui, combien d'accès réussis ont-ils été dénombrés ?



Le RFC 2196 est une excellente référence en matière de développement de stratégies de sécurité de réseau. Il précise qu'une telle stratégie est essentiellement constituée d'un document qui résume de quelle manière les ressources de traitement et de réseau de l'entreprise doivent être utilisées et protégées.

Les caractéristiques essentielles d'une stratégie de sécurité efficace sont les suivantes :

- Possibilité d'implémentation, à la fois sur le plan technique et sur le plan organisationnel.
- Applicable au moyen d'outils de sécurité aux endroits appropriés, sinon au moyen de sanctions là où une protection réelle ne peut être implémentée techniquement.
- Définition du niveau de responsabilité des utilisateurs, des administrateurs et de la direction.
- Souple et facile à gérer, afin de s'adapter aux environnements changeants.
- Implémente le niveau maximal de sécurité sur le réseau, tout en étant également transparente que possible pour les utilisateurs.
- Utilise des procédures de gestion et des processus de notification.

Création d'une stratégie de sécurité

Lorsque vous entreprenez de développer une stratégie de sécurité, commencez par recueillir des informations sur les procédures de sécurité qui sont déjà en place (la fréquence à laquelle les utilisateurs modifient leur mot de passe d'ouverture de session, les chaînes de communauté SNMP en lecture/écriture, etc.). Vous devez également déterminer à quel moment ces mesures de sécurité ont été modifiées pour la dernière fois. Vous pouvez bien sûr faire appel à des spécialistes extérieurs à votre entreprise pour vous assister dans l'évaluation de vos procédures et stratégies de sécurité existantes. Peut-être ne l'aviez-vous jamais envisagé, avant de vous lancer dans le développement complet d'une stratégie. Ainsi que vous pouvez le voir, la création (et l'évolution) d'une stratégie de sécurité dépend de votre situation spécifique. Cependant, les actions suivantes (au minimum) sont à effectuer lors de la mise au point d'une stratégie :

- Réaliser une évaluation des risques et une analyse coûts/avantages.
- Identifier les ressources que vous tentez de protéger.
- Identifier les ennemis potentiels contre lesquels vous voulez protéger vos ressources.
- Déterminer les coûts des mesures de sécurité du réseau.
- Concevoir et implémenter des mesures qui protégeront vos ressources de façon rentable.
- Réviser régulièrement le processus, et apporter les améliorations nécessaires chaque fois qu'une vulnérabilité est identifiée.
- Recenser les procédures existantes, documentées ou non, comme la modification des mots de passe tous les mois, etc.

Il est important de se souvenir qu'une stratégie de sécurité n'est *pas* statique, et qu'elle se développe, change, et s'améliore continuellement selon les exigences. Une conception et une implémentation proactives importent autant pour une stratégie de sécurité que pour un réseau. Une fois que vous avez développé votre stratégie, documentez-la.

NOTE

Une stratégie de sécurité n'est pas *la* solution à vos problèmes de sécurité. Elle représente plutôt un cadre de travail qui permet d'implémenter une sécurité sur votre réseau. Associée à d'autres aspects traités dans ce chapitre, une stratégie efficace peut garantir une sécurité complète et fiable.

Documenter et analyser une stratégie de sécurité

Au fur et à mesure que vous avancez dans le processus d'identification et de conception de la sécurité de votre réseau, documentez vos découvertes ainsi que les actions entreprises. Un document écrit et amélioré constamment est vital pour l'implémentation de votre stratégie de sécurité globale. Il permettra à ceux qui vous succèdent de comprendre les raisons qui ont motivé vos choix d'implémentation et de conception de la sécurité. Il pourra même être utilisé à des fins d'apprentissage par de futurs ingénieurs de réseau. Toutefois, ce document ne devrait pas être disponible pour le public.

Veillez à ce que votre stratégie de sécurité bénéficie d'un budget suffisant afin de pouvoir réaliser des audits réguliers et complets. Ces audits permettront de tester de façon continue votre stratégie ainsi que le degré d'exposition global du réseau à de nouvelles vulnérabilités ou attaques.

Approche Cisco de la sécurité

Une autre préoccupation sur les réseaux partagés est d'empêcher les données de tomber dans les mains d'individus mal intentionnés. Quiconque dispose d'un outil d'analyse en mode transparent peut capturer les trames du réseau et décoder leur contenu. Sur les réseaux partagés, le trafic reçu sur n'importe quel port d'un hub est retransmis sur tous ses ports, car ils font tous partie du même domaine de collision.

Les mesures de sécurité incitent les individus à rester honnêtes, de la même manière que les verrous. Cette étude de cas décrit les actions spécifiques que vous pouvez entreprendre afin d'améliorer la sécurité de votre réseau. Mais, avant d'entrer dans les détails, cette section révise certains principes de base que vous devez garder à l'esprit lorsque vous planifiez la sécurité de votre réseau.

Connaître son ennemi

Le terme ennemi se réfère au cyber-pirate, qui est soit un *attaquant* soit un *intrus*. Pensez aux individus qui pourraient mettre en péril vos mesures de sécurité, et identifiez leurs motivations. Quelles actions pourraient-ils entreprendre, et quelles en seraient les conséquences sur le réseau. Par exemple, votre entreprise est-elle versée dans la finance, le commerce électronique, ou les données sensibles ? Car ces domaines d'activité sont souvent la cible des cyber-pirates.

Les mesures de sécurité ne permettent jamais d'éliminer complètement le risque qu'un utilisateur exécute des tâches non autorisées sur un système informatique. Elles peuvent simplement lui rendre la tâche plus difficile. L'objectif est de s'assurer que le contrôle de la sécurité est hors de portée de l'attaquant.

Evaluer les coûts

Les mesures de sécurité s'accompagnent toujours de certains inconvénients, surtout pour les utilisateurs avancés. Elles peuvent ralentir le travail et générer une surcharge coûteuse en matière d'administration

et de formation. Elles peuvent également entraîner une consommation très importante des ressources de traitement, et nécessiter un matériel dédié.

Lorsque vous élaborez vos mesures de sécurité, examinez-en le coût et les bénéfices que vous pourrez en tirer. A cet effet, vous devez connaître les coûts associés aux mesures elles-mêmes, ainsi que ceux liés aux risques de brèches dans la sécurité. Si vous engagez des dépenses exagérées par rapport aux dangers réels, vous pourriez le regretter. Par exemple, peu d'entreprises pourraient justifier le coût de mesures de sécurité extrêmes, telles celles mises en œuvre sur le réseau du Département de la défense américain.

Identifier les dangers potentiels

Tout système de sécurité est fondé en partie sur certaines supputations. Vous pensez que votre réseau n'est pas sous écoute clandestine, ou que les attaquants ont moins de connaissances que vous, qu'ils utilisent des programmes standards, ou bien qu'une pièce verrouillée est un endroit sûr, etc. Veillez à examiner de plus près vos hypothèses, et à en vérifier le bien-fondé. Toute supposition représente un risque de vulnérabilité.

Une règle importante ici est de toujours reconnaître le plus objectivement possible les exigences de sécurité de votre réseau, et de ne pas oublier que toute supposition non confirmée peut avoir des conséquences graves. Lors de l'identification et de la vérification de vos suppositions, vous pourriez tomber sur un problème de réseau ne relevant pas du tout de la sécurité. C'est pourquoi vous devez être vigilant et capable de déterminer les réelles vulnérabilités.

Contrôler les informations confidentielles

La plupart des systèmes de sécurité reposent sur des données "secrètes", ou confidentielles, telles que les mots de passe, les clés de cryptage, et les chaînes de communauté SNMP. Trop souvent, ce que l'on considère comme étant secret ne l'est pas. L'étape la plus importante dans la dissimulation de ces informations consiste à connaître les zones qui doivent être protégées. Quels renseignements pourraient être exploités par l'ennemi pour s'introduire sur votre système ? Vous devez garder jalousement ces informations, et considérer que vos adversaires connaissent tout le reste. Plus vous avez de secrets, plus ils sont difficiles à conserver. Les systèmes de sécurité doivent être conçus de façon à limiter le nombre de ces informations confidentielles.

Considérer le facteur humain

La majorité des procédures de sécurité échouent, car leurs concepteurs n'ont pas tenu compte du comportement des utilisateurs. Par exemple, les mots de passe générés automatiquement peuvent être difficiles à mémoriser, c'est pourquoi on les retrouve souvent écrits sous le clavier des utilisateurs. Par négligence, une porte de sécurité qui sert à empêcher l'accès à un système de sauvegarde sur bandes est parfois laissée ouverte. De la même manière, des modems non autorisés sont souvent connectés à un réseau, ce qui évite de devoir implémenter des mesures de sécurité onéreuses au niveau des appels entrants.

Si vos mesures de sécurité interfèrent trop avec l'usage principal du système ou du réseau, les utilisateurs leur opposeront une certaine résistance et tenteront peut-être même de les contourner. Pour gagner leur confiance, vous devez veiller à ce qu'ils puissent accomplir leur travail normalement, et les convaincre de la pertinence de ces mesures. Ils doivent comprendre et accepter la nécessité

d'une sécurité. La communication avec les utilisateurs est donc essentielle, car une fois qu'ils ont compris les raisons pratiques qui motivent ces mesures, ils sont plus enclins à les accepter. Mais, quel que soit le mal que vous leur donnez, vous tomberez toujours sur des utilisateurs qui tenteront de les contourner.

Tout utilisateur peut mettre en péril le système de sécurité, tout au moins dans une certaine mesure. Les mots de passe, par exemple, peuvent souvent être obtenus en appelant simplement les utilisateurs au téléphone et en se faisant passer pour un administrateur système. Si vos utilisateurs sont conscients des problèmes de sécurité, et s'ils comprennent les raisons de ces mesures, ils feront tout leur possible pour éviter qu'un intrus ne pénètre dans le système.

Au minimum, les utilisateurs doivent savoir qu'il ne faut jamais communiquer des mots de passe ou autres informations confidentielles sur des lignes téléphoniques non sécurisées (plus particulièrement les téléphones cellulaires) ou par courrier électronique (e-mail). Ils doivent se méfier des questions qu'on leur pose par téléphone. Certaines entreprises ont mis en place un programme officiel de formation de leur personnel à la sécurité de réseau, et les employés ne sont pas autorisés à accéder à l'Internet tant qu'ils n'ont pas suivi cette formation. Une telle politique est efficace afin de sensibiliser une communauté d'utilisateurs, et devrait être formulée par écrit, de façon à être accessible à tous. Dernière remarque importante : ne violez jamais vos propres procédures de sécurité, quelles que soient vos raisons.

Connaître les faiblesses du système de sécurité

Chaque système de sécurité possède ses vulnérabilités, et leur identification requiert honnêteté et franchise. Il peut parfois être très utile de se faire aider lors de la recherche de ces faiblesses. Vous devez être capable de connaître les points faibles de votre système, ainsi que la manière dont ils pourraient être exploités par l'ennemi. Vous devez également savoir quelles zones représentent le plus grand danger d'intrusion, et contrôler l'accès à ces zones immédiatement. L'identification des points faibles est la première étape vers la sécurisation de ces zones.

Limiter l'étendue de l'accès

Il est nécessaire de créer des barrières au sein même de votre réseau, afin que d'éventuels intrus, qui parviendraient à accéder à une partie du réseau, ne puissent accéder à la totalité. Le niveau de sécurité globale d'un réseau se limite toujours au degré de vulnérabilité de l'équipement le moins sûr. Le fait d'adopter une approche hiérarchique de la sécurité permet certainement de ralentir un intrus, et de le localiser plus facilement. Installer un gros verrou sur la porte de sa maison est une bonne chose, mais s'il représente le seul moyen de protection, il vaudrait mieux envisager l'acquisition de caméras de surveillance, d'un chien de garde, ou bien d'un système d'alarme additionnel. Cette analogie un peu simpliste n'en est pas moins objective, car il est toujours plus difficile de commettre un acte délictueux lorsque les obstacles à franchir sont nombreux.

Comprendre son environnement

Le fait de comprendre le fonctionnement de votre réseau en temps normal, de distinguer les événements prévisibles de ceux qui ne le sont pas, et de connaître l'utilisation habituelle des différents équipements vous permettra de détecter plus facilement les problèmes de sécurité. Vous pourrez ainsi remarquer les événements inhabituels, et repérer les intrus avant qu'ils n'endommagent votre

système. Des outils d'audit vous aideront dans cette tâche. Bien sûr, en complément de cette approche préventive, vous pouvez mettre en place des mécanismes d'alarme qui signalent les tentatives de violation ou de contournement des mesures de sécurité en place.

Limiter sa confiance

Vous devez connaître précisément les logiciels et matériels que vous utilisez, et ne pas baser votre système de sécurité sur l'hypothèse que tous les programmes sont exempts de bogues. Sachez mettre à profit l'expérience et les découvertes d'autrui, qui font l'objet de nombreuses annonces et publications, et pensez à toujours tout remettre en question.

Penser à la sécurité physique

L'accès physique à une station de travail, à un serveur, à un commutateur, à un pare-feu, ou à un routeur offre en général à un utilisateur avancé un contrôle total de l'équipement en question. L'accès physique à une liaison de réseau permet habituellement à une personne d'écouter clandestinement cette liaison, d'y provoquer des interférences ou d'y injecter du trafic. Il est inutile d'implémenter des mesures de sécurité logicielles complexes lorsque l'accès au matériel n'est pas contrôlé.

La sécurité est envahissante

La plupart des modifications apportées à votre réseau peuvent avoir des répercussions sur la sécurité. C'est particulièrement vrai lors de la création de nouveaux services. Les ingénieurs de réseau, les administrateurs système, les programmeurs et les utilisateurs devraient mesurer les conséquences de chaque modification. Cela implique une certaine expérience pratique, une réflexion latérale, ainsi que la volonté d'explorer tous les moyens par lesquels un service pourrait être manipulé. Evitez donc les changements irréfléchis, qui peuvent engendrer de graves problèmes de sécurité.

Contrôle de l'accès aux routeurs Cisco

Il est important de contrôler l'accès à vos routeurs Cisco. Voici les méthodes dont vous disposez :

- accès par console ;
- accès Telnet ;
- accès SNMP ;

Vous pouvez sécuriser l'accès à un routeur en utilisant son logiciel IOS. Pour chaque méthode, vous pouvez accorder un accès non privilégié ou privilégié à un utilisateur (ou groupe d'utilisateurs) ;

- **Accès non privilégié.** Il permet aux utilisateurs de surveiller le routeur, mais non de le configurer. Il s'agit d'un accès en lecture seule.
- **Accès privilégié.** Il permet aux utilisateurs de configurer complètement le routeur. Il s'agit d'un accès en lecture-écriture.

Pour les accès par port de console et Telnet, vous pouvez créer deux types de mots de passe. Le premier, le mot de passe d'ouverture de session, accorde à l'utilisateur un accès non privilégié au routeur. Une fois connecté, il peut entrer dans le mode privilégié *via* la commande enable et le mot de passe approprié. Le mode privilégié fournit à l'utilisateur les fonctions de configuration complète.

L'accès SNMP permet de définir plusieurs chaînes de communauté SNMP pour les accès non privilégié et privilégié. L'accès non privilégié permet aux utilisateurs, sur un hôte, d'envoyer au routeur des messages SNMP get-request et get-next-request, qui servent à recueillir des informations statistiques auprès du routeur. L'accès privilégié permet aux utilisateurs, sur un hôte, d'envoyer au routeur des messages SNMP set-request afin d'en modifier les paramètres de configuration et le mode de fonctionnement.

Accès par console

Une console est un terminal directement rattaché au routeur *via* le port de console. La sécurité intervient au niveau de la console : les utilisateurs sont invités à s'authentifier au moyen de mots de passe. Par défaut, aucun mot de passe n'est associé à l'accès par console.

Mot de passe pour le mode non privilégié

Vous configurez un mot de passe pour le mode non privilégié en entrant les commandes suivantes, dans le fichier de configuration du routeur. Les mots de passe sont sensibles à la casse (dans cet exemple, le mot de passe est `1forAll`) :

```
line console 0
  login
    password 1forAll
```

Lorsque vous ouvrez une session sur le routeur, l'invite d'ouverture de session se présente de la façon suivante :

```
User Access Verification
Password:
```

Vous devez saisir le mot de passe `1forAll`, afin d'obtenir un accès non privilégié au routeur. La réponse apparaît comme suit :

```
router>
```

Le mode non privilégié est signifié sur le routeur par l'invite `>`. A ce stade, vous pouvez saisir une variété de commandes, afin de consulter des informations statistiques sur ce routeur, mais vous n'êtes pas autorisé à en modifier la configuration.

N'utilisez jamais `cisco` comme mot de passe, ou autre variante évidente, telle que `pancho`. Ce sont les premiers mots de passe utilisés par les intrus lorsqu'ils reconnaissent une invite Cisco.

Mot de passe pour le mode privilégié

Configurez un mot de passe pour le mode privilégié en ajoutant les commandes suivantes, dans le fichier de configuration du routeur (dans cet exemple, le mot de passe est `san-fran`) :

```
enable-password san-fran
```

Pour accéder au mode privilégié, saisissez la commande suivante :

```
router> enable
Password:
```

Saisissez le mot de passe `san-fran`, afin d'obtenir l'accès privilégié au routeur. Ce dernier répond comme suit :

```
router#
```

Le mode privilégié est signifié par l'invite #. Dans ce mode, vous pouvez entrer toutes les commandes qui permettent de consulter des statistiques, ou de configurer le routeur.

Une autre façon de définir le mot de passe du mode privilégié est d'utiliser la commande `enable secret`. Elle remplace la commande `enable-password`, et crypte automatiquement le mot de passe du mode privilégié lorsque vous visualisez la configuration.

Accès Telnet

Vous pouvez accéder au routeur en modes non privilégié et privilégié, *via* Telnet. A l'image du cas du port de console, la sécurité Telnet intervient lorsque le routeur invite les utilisateurs à s'authentifier en fournissant un mot de passe. Un grand nombre des éléments décrits à la section "Accès par console" sont applicables à l'accès Telnet. Vous devez fournir un mot de passe, afin de transiter du mode non privilégié au mode privilégié. Vous pouvez crypter les mots de passe, et spécifier des délais d'expiration pour chaque session Telnet.

Mot de passe pour le mode non privilégié

Chaque port Telnet sur le routeur est connu sous la dénomination *terminal virtuel*. Un routeur comprend un maximum de cinq ports de terminal virtuel (VTY, *Virtual Terminal*), ce qui autorise cinq sessions Telnet concurrentes (le serveur de communication fournit plus de ports VTY). Sur le routeur, les ports de terminal virtuel sont numérotés de 0 à 4. Vous pouvez configurer des mots de passe non privilégiés pour un accès *via* Telnet sur les ports VTY, à l'aide des commandes suivantes (dans cet exemple, les ports VTY 0 à 4 utilisent le mot de passe `marin`) :

```
line vty 0 4
login
password marin
```

Lorsqu'un utilisateur établit une communication Telnet avec l'adresse d'un routeur IP, ce dernier présente une invite semblable à celle-ci :

```
% telnet router
Trying ...
Connected to router.
Escape character is '^]'.
User Access Verification
Password:
```

Si l'utilisateur fournit le mot de passe non privilégié correct, l'invite suivante apparaît :

```
router>
```

Mot de passe pour le mode privilégié

A présent que l'utilisateur dispose d'un accès non privilégié au routeur, il peut entrer dans le mode privilégié en saisissant la commande `enable`, tel que décrit à la section "Mot de passe pour le mode privilégié", plus haut dans ce chapitre.

Accès SNMP

Le protocole SNMP (*Simple Network Management Protocol*) représente une autre méthode d'accès aux routeurs. Avec SNMP, vous pouvez recueillir des statistiques ou configurer les routeurs. La collecte de statistiques se fait au moyen des messages `get-request` et `get-next-request`, et la configuration des

routeurs au moyen des messages set-request. Chacun de ces messages comprend une *chaîne de communauté*, qui est en fait un mot de passe en texte clair, envoyé dans chaque paquet entre une station gestionnaire et le routeur (qui héberge un agent SNMP). La chaîne de communauté SNMP sert à authentifier les messages envoyés entre le gestionnaire et l'agent. L'agent répond uniquement lorsque le gestionnaire lui envoie la chaîne de communauté correcte.

L'agent SNMP situé sur le routeur permet de configurer plusieurs chaînes de communauté pour des accès non privilégié et privilégié. Pour cela, la commande de configuration `snmp-server community <chaîne> [RO | RW] [liste-accès]` est employée. Les sections suivantes examinent les différentes utilisations de cette commande.

Malheureusement, ces chaînes sont envoyées sur le réseau en texte clair, au format ASCII. Par conséquent, quiconque est capable de capturer un paquet sur le réseau peut découvrir la chaîne. Ainsi, des utilisateurs non autorisés ont la possibilité d'interroger ou de modifier les routeurs, *via* SNMP. Pour éviter cela, la commande `no snmp-server trap authentication` empêche les intrus d'utiliser des messages d'interception (envoyés entre les gestionnaires et les agents) pour découvrir les chaînes de communauté.

La communauté Internet, consciente du problème, a considérablement amélioré la sécurité de la version 2 de SNMP, tel que décrit dans le RFC 1446. SNMP version 2 utilise un algorithme, appelé MD5, afin d'authentifier les communications entre les deux parties SNMP. MD5 vérifie l'intégrité de ces communications, en authentifie l'origine, puis en contrôle la validité. De plus, cette version de SNMP emploie le standard de cryptage DES (*Data Encryption Standard*) pour crypter les informations.

Mode non privilégié

Employez le mot clé `RO` de la commande `snmp-server community`, afin d'autoriser un accès non privilégié sur vos routeurs, *via* SNMP. La commande de configuration suivante configure l'agent sur le routeur afin qu'il autorise uniquement les messages SNMP get-request et get-next-request envoyés avec la chaîne de communauté "public" :

```
snmp-server community public RO 1
```

Vous pouvez également spécifier une liste des adresses IP qui sont autorisées à envoyer des messages au routeur, au moyen de l'instruction `access-list`, avec la commande `snmp-server community`. Dans l'exemple de configuration suivant, seuls les hôtes 1.1.1.1 et 2.2.2.2 se voient accorder un accès SNMP non privilégié au routeur :

```
access-list 1 permit 1.1.1.1
access-list 1 permit 2.2.2.2
snmp-server community public RO 1
```

Mode privilégié

Employez le mot clé `RW` de la commande `snmp-server community` pour autoriser un accès privilégié sur vos routeurs, *via* SNMP. La commande de configuration suivante configure l'agent sur le routeur pour qu'il n'autorise que les messages SNMP set-request envoyés avec la chaîne de communauté "private" :

```
snmp-server community private RW 1
```

Vous pouvez également spécifier une liste des adresses IP qui sont autorisées à envoyer des messages au routeur, au moyen de l'instruction `access-list`, avec la commande `snmp-server community`. Dans l'exemple de configuration suivant, seuls les hôtes 5.5.5.5 et 6.6.6.6 se voient accorder un accès SNMP privilégié au routeur :

```
access-list 1 permit 5.5.5.5
access-list 1 permit 6.6.6.6
snmp-server community private RW 1
```

Techniques additionnelles de sécurisation d'un routeur

Ces techniques additionnelles peuvent être utilisées selon les besoins pour protéger encore davantage l'accès à vos routeurs.

Délais d'expiration de session

Parfois, la configuration de l'ouverture de session et l'activation des mots de passe ne suffisent pas à fournir une sécurité acceptable. Le délai d'expiration pour une console laissée sans surveillance (qui est de 10 minutes par défaut) représente une mesure de sécurité supplémentaire. Si la console est laissée sans surveillance dans le mode privilégié, n'importe quel utilisateur peut modifier la configuration du routeur. Vous pouvez modifier ce délai, grâce à la commande `exec-timeout mm ss`, où `mm` représente les minutes, et `ss` les secondes. Les commandes suivantes définissent la valeur du délai d'expiration à 1 minute et 30 secondes :

```
line console 0
exec-timeout 1 30
```

Cryptage des mots de passe

Tous les mots de passe entrés sur le routeur sont visibles par le biais des commandes du mode privilégié `write terminal` et `show configuration`. Si vous disposez d'un accès au routeur en mode privilégié, vous pouvez, par défaut, visualiser tous les mots de passe en texte clair.

Il existe un moyen de masquer ces mots de passe. La commande `service password-encryption` permet de les stocker sous forme cryptée, de façon qu'ils ne puissent pas être visualisés en texte clair par quiconque exécute les commandes `write terminal` et `show configuration`. Néanmoins, si vous oubliez votre mot de passe, vous devrez alors disposer d'un accès physique pour pouvoir accéder au routeur.

NOTE

Bien que le cryptage soit utile, il peut être forcé, et ne doit donc pas constituer l'unique stratégie de sécurité.

Restrictions d'accès Telnet pour certaines adresses IP

Si vous souhaitez autoriser uniquement certaines adresses IP à utiliser Telnet pour accéder au routeur, vous devez employer la commande `access-class`. La commande `access-class nn in` définit une liste d'accès (de 1 à 99) pour les lignes de terminal virtuel sur le routeur. Les commandes de configuration suivantes limitent l'accès, via Telnet, aux hôtes du réseau 192.85.55.0 :

```
access-list 12 permit 192.85.55.0 0.0.0.255
line vty 0 4
access-class 12 in
```

Restrictions d'accès Telnet sur des ports TCP

Il est possible d'accéder, *via* Telnet, aux produits Cisco sur des ports TCP spécifiés. Le type d'accès Telnet dépend de la version du logiciel System Software utilisée, à savoir :

- versions 9.1 (11.4) et antérieures, ainsi que versions 9.21 (3.1) et antérieures ;
- versions 9.1 (11.5), 9.21 (3.2), 10.0 et ultérieures.

Versions antérieures de System Software

Pour les versions 9.1 (11.4) et antérieures, ainsi que les versions 9.21 (3.1) et antérieures de System Software, il est possible (par défaut) d'établir des connexions TCP sur les ports TCP listés au Tableau 22.1, pour les produits Cisco.

Tableau 22.1 : Ports TCP pour l'accès Telnet aux produits Cisco (versions antérieures de System Software)

<i>Numéro de port TCP</i>	<i>Méthode d'accès</i>
7	Echo
9	Discard (détruire)
23	Telnet (sur ports de terminal virtuel VTY en mode rotation)
79	Finger
1993	SNMP sur TCP
2001 à 2999	Telnet, sur port auxiliaire (AUX), ports de terminal (TTY), et ports de terminal virtuel (VTY)
3001 à 3999	Telnet, sur ports de rotation (l'accès sur ces ports est possible uniquement si les rotations ont d'abord été explicitement configurées à l'aide de la commande <i>rotary</i>)
4001 à 4999	Miroir Telnet (mode flux) de la plage 2000
5001 à 5999	Miroir Telnet (mode flux) de la plage 3000 (l'accès sur ces ports est possible uniquement si les rotations ont d'abord été explicitement configurées)
6001 à 6999	Miroir Telnet (mode binaire) de la plage 2000
7001 à 7999	Miroir Telnet (mode binaire) de la plage 3000 (l'accès sur ces ports est possible uniquement si les rotations ont d'abord été explicitement configurées)
8001 à 8999	Xremote (serveurs de communication uniquement)
9001 à 9999	Reverse Xremote (serveurs de communication uniquement)
10001 à 19999	Groupe Reverse Xremote (serveurs de communication uniquement ; l'accès sur ces ports est possible uniquement s'ils ont d'abord été explicitement configurés)

ATTENTION

Etant donné que les routeurs Cisco ne disposent pas de lignes TTY, la configuration de l'accès (sur les serveurs de communication) aux ports terminaux 2002, 2003, 2004, et plus, pourrait potentiellement fournir un accès (sur les routeurs) sur les lignes de terminal virtuel 2002, 2003, 2004, et plus. Pour fournir un accès aux ports TTY uniquement, vous pouvez créer des listes qui interdisent l'accès aux ports VTY.

De plus, lors de la configuration de groupes de rotation, n'oubliez pas que l'accès est possible par le biais de n'importe lequel des ports disponibles dans le groupe (sauf si des listes d'accès ont été définies). Si vous utilisez des pare-feu qui autorisent les connexions TCP entrantes sur un grand nombre de ports, Cisco recommande d'appliquer les listes d'accès appropriées à ses produits.

L'exemple suivant illustre une liste d'accès qui refuse tous les accès Telnet entrants sur le port auxiliaire, et qui autorise l'accès Telnet au routeur uniquement pour l'adresse 192.32.6.7 :

```
access-class 51 deny 0.0.0.0 255.255.255.255
access-class 52 permit 192.32.6.7
line aux 0
access-class 51 in
line vty 0 4
access-class 52 in
```

Pour désactiver les connexions sur les ports Echo et Discard, vous devez désactiver complètement ces services, au moyen de la commande `no service tcp-small-servers`.

NOTE

Si la commande `ip alias` est activée sur les produits Cisco, les connexions TCP sur n'importe quel port de destination sont considérées comme étant valides. Il se peut que vous souhaitiez désactiver cette commande.

Dans certaines situations, il peut être utile de créer des listes d'accès pour empêcher l'accès aux produits Cisco sur ces ports TCP. Pour obtenir des informations sur la création de listes d'accès pour des routeurs, voyez la section "Configuration du routeur pare-feu", plus bas dans ce chapitre. Pour obtenir des informations sur la création de listes d'accès pour des serveurs de communication, consultez la section "Configuration du serveur de communication pare-feu", plus bas dans ce chapitre.

Versions ultérieures de System Software

Avec les versions 9.1 (11.5), 9.21 (3.2), ainsi que toute autre version 10.x de System Software, les améliorations suivantes ont été implémentées :

- L'accès direct aux lignes de terminal virtuel (VTY), par l'intermédiaire des plages de ports 2000, 4000 et 6000, a été désactivé. Pour maintenir un accès ouvert, vous pouvez configurer des correspondances biunivoques entre VTY et le port de rotation.
- Les connexions aux ports Echo et Discard (respectivement 7 et 9) peuvent être désactivées, à l'aide de la commande `no service tcp-small-servers`.
- Tous les produits Cisco autorisent des connexions à des équipements IP alias uniquement sur le port de destination 23.

Avec les versions ultérieures, un routeur Cisco accepte par défaut les connexions sur les ports répertoriés au Tableau 22.2.

Tableau 22.2 : Ports TCP pour l'accès Telnet aux produits Cisco (versions ultérieures de System Software)

<i>Numéro de port TCP</i>	<i>Méthode d'accès</i>
7	Echo
9	Discard (détruire)
23	Telnet
79	Finger
1993	SNMP sur TCP
2001	Port auxiliaire (AUX)
4001	Port (flux) auxiliaire (AUX)
6001	Port (binaire) auxiliaire (AUX)

L'accès sur le port 23 peut être restreint en créant une liste d'accès, que l'on assigne ensuite aux lignes de terminal virtuel. L'accès sur le port 79 peut être désactivé à l'aide de la commande `no service finger`. L'accès sur le port 1993 peut être contrôlé avec des listes d'accès SNMP. L'accès sur les ports 2001, 4001 et 6001 peut être contrôlé au moyen d'une liste d'accès placée sur le port auxiliaire.

Listes de contrôle d'accès

Comme beaucoup d'autres listes, les listes de contrôle d'accès (ACL, *Access Control List*) ne représentent qu'un ensemble de critères, qui vont des plus simples aux plus avancés. Ces critères peuvent, par exemple, spécifier les adresses autorisées à établir une connexion Telnet vers un port VTY du routeur. Ces listes peuvent être exploitées à de nombreuses fins, parmi lesquelles :

- filtrer le trafic entrant ou sortant ;
- organiser une stratégie de gestion des files d'attente ;
- déterminer quels types de trafics peuvent activer des circuits DDR (*Dial-on Demand Routing*, routage avec ouverture de ligne à la demande) ;
- filtrer les mises à jour de routage en entrée ou en sortie.

Indépendamment des critères de filtrage définis, si une liste n'est pas exploitée correctement, elle ne fonctionnera pas normalement, voire pas du tout.

Fonctionnement

La définition d'une liste de contrôle d'accès fournit un ensemble de critères, qui sont appliqués à chaque paquet traité par le routeur. Celui-ci décide de transmettre ou de bloquer un paquet, en fonction des critères auxquels ce paquet correspond.

Des critères de liste d'accès typiques spécifient l'adresse source, l'adresse de destination, ou le protocole de couche supérieure d'un paquet. Toutefois, chaque protocole possède son propre ensemble de critères, qui peut être défini plus précisément au moyen de numéros de port.

Pour une liste d'accès donnée, chaque critère peut être défini dans une instruction de liste d'accès séparée. Ces instructions indiquent de transmettre ou de bloquer les paquets qui correspondent aux critères listés. En fait, une liste d'accès est la somme des instructions individuelles qui partagent toutes le même nom ou numéro d'identifiant.

NOTE

Chaque instruction de liste d'accès que vous ajoutez est placée à la suite des instructions déjà définies. De plus, vous ne pouvez pas supprimer des instructions individuelles une fois qu'elles ont été créées. Vous pouvez seulement supprimer la liste entière.

Chaque paquet est comparé à chaque entrée de la liste, c'est-à-dire à chaque critère. Lorsqu'une correspondance est trouvée, le paquet est accepté ou refusé. Une entrée de liste d'accès peut soit autoriser (permit) soit rejeter (deny) le trafic.

A la fin des listes d'accès est spécifiée une instruction implicite de rejet de tout le trafic. Par conséquent, si un paquet ne correspond à aucun des critères, il est bloqué. Il s'agit du comportement par défaut d'une liste d'accès sur un routeur Cisco. Lors de la configuration de listes d'accès, il est donc important d'avoir à l'esprit que tout le trafic non explicitement autorisé est rejeté.

Le comportement d'une liste d'accès peut être comparé à une condition "if... then" en programmation. Chaque entrée d'une liste d'accès comporte un critère séparé. La portion "if" de la ligne est le critère, et la portion "then" est une instruction d'acceptation ou de rejet. Par exemple :

```
if <critère 1> then <permit | deny>
if <critère 2> then <permit | deny>
.
.
.
rejeter tout le trafic
```

L'ordre des instructions dans une liste d'accès est également important. Lorsque le routeur doit décider de transmettre ou de bloquer un paquet, le logiciel Cisco IOS compare le paquet à chaque critère, dans l'ordre de création des instructions. Une fois qu'une correspondance a été trouvée, aucune autre instruction n'est exécutée pour ce paquet. Ce mode de fonctionnement est désigné *processus descendant*.

Le processus descendant est l'un des concepts les plus simples utilisés par les routeurs Cisco, si vous respectez les règles. Lors de la création d'une liste de contrôle d'accès, ayez à l'esprit les règles suivantes :

- Les éléments spécifiques, tels que des adresses IP individuelles, sont placés en début de liste.
- Les éléments généraux, tels que des numéros de sous-réseaux, devraient être placés en milieu de liste.
- Les éléments ouverts, tels que des numéros de réseaux, devraient se situer en fin de liste.

Si vous créez une instruction qui autorise explicitement tout le trafic, aucune des instructions suivantes ne sera exécutée. Si, par la suite, vous voulez ajouter des instructions supplémentaires, vous devrez supprimer la liste d'accès, puis la recréer avec les nouvelles entrées.

NOTE

Lors de la création ou de la modification de listes d'accès, il est vivement recommandé de ne pas les modifier à la volée. Il est préférable de les concevoir sur un serveur TFTP, dans un traitement de texte, ou sur papier. L'utilisation de listes d'accès induit une charge de traitement supplémentaire au niveau du processeur du routeur, car chaque entrée d'une liste doit être contrôlée, jusqu'à ce qu'une correspondance soit trouvée.

ATTENTION

N'enregistrez pas les modifications apportées à la configuration d'un routeur tant que vous n'avez pas la certitude que la sécurité mise en œuvre fonctionne correctement, de façon à pouvoir revenir en arrière en cas d'erreur.

Application de listes d'accès sur un routeur

Le Tableau 22.3 présente différentes méthodes qui permettent d'appliquer des listes d'accès dans la configuration d'un routeur.

Tableau 22.3 : Commandes d'application de listes d'accès

<i>Commande</i>	<i>Niveau d'application</i>	<i>Description</i>
ip access-group	Interface de routeur	Restreint le trafic en entrée ou en sortie
access-class	Lignes VTY	Restreint l'accès Telnet en entrée ou en sortie
distribute-list	Protocole de routage	Restreint les mises à jour de routage en entrée ou en sortie

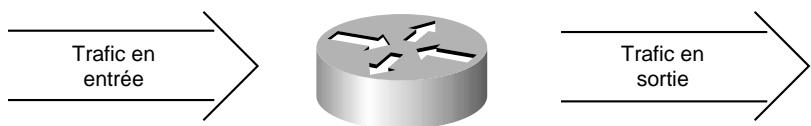
Une seule liste d'accès peut être appliquée à une interface, pour un protocole donné. Avec la plupart des protocoles, les listes d'accès peuvent être configurées sur des interfaces, en entrée ou en sortie. Dans le cas d'un filtrage en entrée, le paquet reçu est comparé aux critères de la liste par le système IOS, à la recherche d'une correspondance. Si une correspondance est trouvée et que le paquet soit autorisé, le système poursuit son traitement, sinon il le supprime.

Dans le cas d'un filtrage en sortie, le paquet reçu est routé vers l'interface de sortie, puis comparé aux critères de la liste par le système IOS, à la recherche d'une correspondance. Si une correspondance est trouvée et que le paquet soit autorisé, le système le transmet, sinon il le supprime.

Pour bien comprendre le fonctionnement de base des listes ACL, il faut savoir que le sens dans lequel une liste est appliquée (entrée ou sortie) est une question de perspective. En l'occurrence, il est vu depuis le routeur. La Figure 22.3 illustre ce principe.

Figure 22.3

Le sens d'application des listes ACL est fonction du routeur.

**ATTENTION**

Pour la plupart des protocoles, si vous définissez une liste d'accès en entrée, afin de filtrer le trafic, vous devez inclure des critères explicites qui autorisent la transmission des mises à jour de routage. Sinon, vous pourriez perdre la communication sur une interface, les mises à jour étant bloquées par l'instruction implicite de rejet de tout le trafic en fin de liste.

Souvenez-vous que les listes d'accès sont configurées sur le routeur, quelle que soit la façon dont vous les exploitez. Tant que vous parvenez à vous représenter la situation par rapport au routeur, vous pouvez différencier les notions de trafic *entrant* et *sortant*.

Masque générique

Les listes d'accès IP standards et étendues utilisent un masque générique (*wildcard mask*). A l'instar d'une adresse IP, un masque générique est une valeur sur 32 bits, exprimée au moyen de nombre décimaux séparés par un point. Lors du processus de comparaison, les bits marqués 1 dans le masque générique signifient qu'il faut ignorer la valeur des bits correspondants dans l'adresse de paquet, et les bits marqués 0 dans le masque signifient qu'il faut comparer la valeur des bits correspondants dans l'adresse de paquet.

L'utilisation du masque générique peut également être décrite comme suit :

- Lorsqu'un bit est marqué 0 dans le masque, la valeur du bit de même position dans l'adresse du paquet et dans l'adresse de la liste d'accès doit être identique, que ce soit 0 ou 1.
- Lorsqu'un bit est marqué 1 dans le masque, la valeur du bit de même position dans l'adresse de paquet est d'emblée considérée comme étant correspondante, que ce soit 0 ou 1. Il n'y a donc pas de comparaison avec l'adresse de liste d'accès. Pour cette raison, les bits marqués 1 sont dits *génériques*.

Une liste d'accès peut comporter un nombre indéfini d'adresses réelles et de masques génériques. Un masque générique, lorsqu'il est non nul, peut correspondre à plusieurs adresses réelles. Souvenez-vous que l'ordre des instructions de liste d'accès est important, car lorsqu'une correspondance est trouvée pour un paquet, le reste des instructions n'est pas exécuté.

NOTE

Les masques génériques offrent un grand avantage : ils permettent au routeur de comparer rapidement les paquets avec les entrées ACL, ce qui réduit les temps de traitement ainsi que la quantité de cycles processeur utilisés.

En fait, un masque générique est l'opposé d'un masque de sous-réseau. Il permet au routeur de rapidement déterminer si une seule adresse IP est référencée, ou bien s'il s'agit d'une plage d'adresses IP. Imaginez une adresse IP 172.19.1.1 avec un masque de sous-réseau 255.255.255.255 (32 bits). Ce masque couvre la totalité de l'adresse ; pour pouvoir s'y référer dans une liste ACL, le masque générique 0.0.0.0 serait utilisé. Vous pouvez donc voir que le masque générique est le contraire du masque de sous-réseau.

Prenons un exemple plus complexe. Imaginez un réseau 172.19.0.0, qui a été subdivisé à l'aide d'un masque de 28 bits. Les sous-réseaux suivants sont donc disponibles :

```
172.19.0.16/28
172.19.0.32/28
172.19.0.48/28
```

Pour désigner un sous-réseau spécifique dans une liste ACL, le masque générique utilisé serait le contraire du masque de sous-réseau, soit :

```
255.255.255.255
255.255.255.240—masque de sous-réseau
-----
0 . 0 . 0 . 15—masque générique
```

Listes de contrôle d'accès standards

Les listes de contrôle d'accès standards peuvent être très efficaces et bloquer une plage entière d'adresses sources. Elles acceptent (permit) ou rejettent (deny) les paquets uniquement en se basant sur leur adresse IP source. Les listes de contrôle d'accès standards sont numérotées de 1 à 99, et sont beaucoup plus simples à configurer que les listes d'accès étendues.

Configuration de listes d'accès standards

La syntaxe suivante est utilisée pour configurer une liste d'accès standard :

```
Router (config)#  
access-list numéro-liste-accès {permit | deny} source masque-source
```

La commande access-list permet de déterminer l'implémentation de la liste d'accès au moyen des paramètres présentés au Tableau 22.4.

La syntaxe suivante active la liste d'accès sur une interface spécifique (une seule liste est supportée par interface) :

```
Router (config-if)#  
ip access-group numéro-liste-accès {in | out}
```

Le Tableau 22.4 décrit les paramètres utilisés dans ces deux commandes.

NOTE

Pour supprimer une liste d'accès, saisissez conséutivement les commandes no access-group, puis no access-list, suivies de leurs paramètres respectifs.

Tableau 22.4 : Paramètres des commandes *access-list* et *ip access-group* (listes d'accès standards)

<i>Commande access-list</i>	<i>Description</i>
<i>numéro-liste-accès</i>	Identifie la liste à laquelle l'entrée appartient. Pour les listes d'accès standards, il s'agit d'un numéro situé entre 1 et 99.
permit deny	Indique si cette entrée autorise ou bloque le paquet lorsque son adresse correspond au critère.
<i>source</i>	Identifie l'adresse source.
<i>masque-source</i>	Identifie les bits à comparer dans le champ d'adresse source. Les bits marqués 1 dans le masque indiquent ceux à ignorer ; les bits marqués 0 ceux à comparer.
<i>Commande ip access-group</i>	<i>Description</i>
<i>numéro-liste-accès</i>	Indique le numéro de la liste d'accès à associer à cette interface.
in out	Spécifie si la liste d'accès est appliquée en entrée ou en sortie sur l'interface. Si ce paramètre n'est pas spécifié, elle est appliquée en sortie par défaut.

Exemple de liste d'accès standard

La liste d'accès suivante autorise uniquement la transmission du trafic en provenance du réseau source 10.10.0.0. Les paquets provenant des autres réseaux sont bloqués :

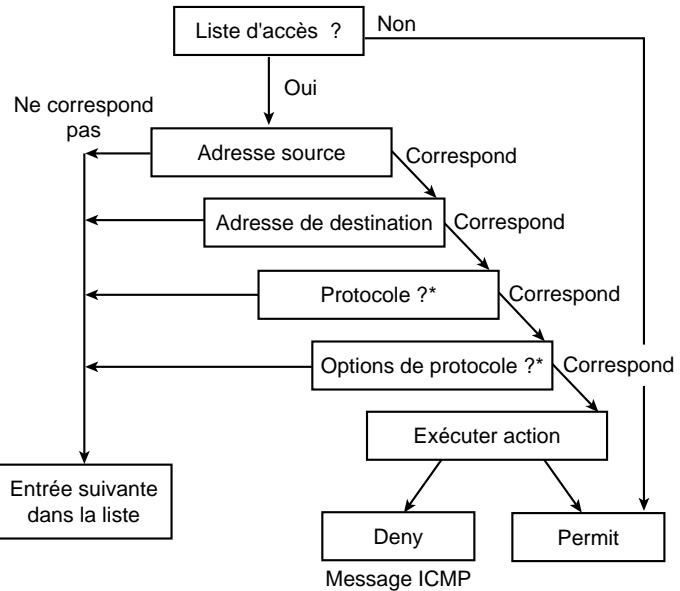
```
access-list 1 permit 10.10.0.0 0.0.255.255
! N'oubliez pas l'instruction implicite de rejet
! de tout le trafic à la fin de chaque liste d'accès :
! access-list 1 deny 0.0.0.0 255.255.255.255
interface ethernet 0
ip access-group 1 out
interface ethernet 1
ip access-group 1 out
```

Listes de contrôle d'accès étendues

Alors que les listes d'accès standards sont rapides à configurer, et permettent de limiter la surcharge au niveau des ressources en contrôlant le trafic sur la base de l'adresse source des paquets, les listes d'accès étendues offrent un plus haut niveau de contrôle, en autorisant également un filtrage basé sur le protocole de niveau session, l'adresse de destination et le numéro de port. Ces fonctionnalités permettent de restreindre le trafic en fonction du type d'utilisation du réseau. La Figure 22.4 illustre le traitement d'une liste de contrôle d'accès étendue par le système IOS du routeur.

Dans une instruction, chaque condition testée doit être vraie pour que l'action *permit* ou *deny* qu'elle spécifie soit exécutée. Lorsqu'un paramètre, ou condition, testé ne résulte pas en une correspondance, l'entrée suivante dans la liste d'accès est traitée.

Figure 22.4
Traitement d'une liste de contrôle d'accès étendue.



*Si présent dans la liste d'accès

Configuration de listes d'accès étendues

Les listes d'accès étendues offrent davantage d'options de configuration ainsi qu'un plus grand degré de précision que les listes standards (voir Tableau 22.5). Voici la syntaxe utilisée pour configurer une liste d'accès étendue :

```
access-list numéro-liste-accès {permit|deny} protocole source masque-source  
destination masque-destination [opérateur opérande] [established]
```

Tableau 22.5 : Paramètres des commandes *access-list* et *ip access-group* (listes d'accès étendues)

Commande <i>access-list</i>	Description
<i>numéro-liste-accès</i>	Identifie la liste à laquelle l'entrée appartient. Pour les listes d'accès étendues, il s'agit d'un numéro situé entre 100 et 199.
permit deny	Indique si cette entrée autorise ou bloque le paquet lorsqu'il correspond à toutes les conditions.
protocole	ip, tcp, udp, icmp, gre, igrp.
<i>source et destination</i>	Identifie l'adresse IP source et l'adresse de destination.

Tableau 22.5 : Paramètres des commandes *access-list* et *ip access-group* (listes d'accès étendues) (suite)

<i>Commande access-list</i>	<i>Description</i>
<i>masque-source</i> et <i>masque-destination</i>	Identifie les bits à comparer dans les champs d'adresse. Les bits marqués 1 dans le masque indiquent ceux à ignorer ; les bits marqués 0 ceux à comparer.
<i>opérateur et opérande</i>	lt , gt , eq , neq (inférieur à, supérieur à, égale, non égale) plus un numéro de port.
established	Autorise le paquet à être transmis s'il s'agit d'une réponse au trafic initié par un réseau ou sous-réseau directement connecté.
<i>Commande ip access-group</i>	<i>Description</i>
<i>numéro-liste-accès</i>	Indique le numéro de la liste d'accès à associer à cette interface.
in out	Spécifie si la liste d'accès est appliquée en entrée ou en sortie sur l'interface. Si ce paramètre n'est pas spécifié, elle sera appliquée en sortie, par défaut.

Exemple de liste d'accès étendue

Voici un exemple de configuration de liste d'accès étendue :

```
access-list 100 permit icmp 10.251.3.48 0.0.0.7 66.34.40.45 0.0.0.0
access-list 100 permit tcp 10.251.3.48 0.0.0.7 66.34.40.45 0.0.0.0 established
access-list 100 permit tcp 10.251.3.48 0.0.0.7 66.34.40.45 0.0.0.0 eq 21
access-list 100 permit tcp 10.251.3.48 0.0.0.7 66.34.40.45 0.0.0.0 eq 161
access-list 100 permit tcp 10.251.3.48 0.0.0.7 66.34.40.45 0.0.0.0 eq 162
access-list 100 deny ip 10.251.3.48 0.0.0.7 0.0.0.0 255.255.255.255
access-list 100 permit ip any any
```

La formulation des instructions précédentes au moyen d'une condition de programmation "if-then" permet de mieux comprendre la logique de traitement :

```
If la source est du réseau et de 10.251.3.48
Then autorise un accès icmp total vers la destination 66.34.40.45
Else if la source est du réseau et égale à 10.251.3.48
Then autorise accès TCP vers les ports 21, 161 et 162
Else if la source est du réseau et non de 10.251.3.48
    Then autoriser un accès ouvert
End if BLOQUER TOUT LE TRAFIC
```

Listes de contrôle d'accès réflexives

Les listes de contrôle d'accès réflexives représentent un nouveau type de listes ACL. Elles possèdent les caractéristiques suivantes :

- Elles filtrent le trafic IP de façon que le trafic des sessions TCP ou UDP soit autorisé uniquement par l'intermédiaire du pare-feu lorsque la session provient du réseau interne.
- Elles offrent une protection contre l'usurpation d'adresses (*spoofing*) et contre certaines attaques par déni de service (*denial-of-service*).

- Elles ne contiennent pas d'instruction implicite de rejet de tout le trafic, car elles sont imbriquées dans des listes d'accès étendues nommées.
- Une liste d'accès réflexive entraîne la création d'une entrée `permit` temporaire, lorsqu'une nouvelle session IP débute (par exemple, un paquet sortant). Cette entrée est ensuite supprimée, à l'issue de la session.
- Une liste d'accès réflexive n'est pas directement appliquée à une interface, mais imbriquée dans une liste d'accès étendue nommée, qui, elle, est appliquée à une interface.
- Deux listes d'accès étendues nommées sont nécessaires, une en entrée et une autre en sortie.
- Pour définir une liste d'accès réflexive, vous devez utiliser une entrée dans une liste d'accès IP étendue nommée. Cette entrée doit inclure le mot clé `reflect`. Ensuite, une autre liste d'accès IP étendue nommée doit contenir le mot clé `evaluate`.

Fonctionnement des listes d'accès réflexives

Pour bien comprendre le mécanisme des listes d'accès réflexives, imaginez qu'un agent de la sécurité soit chargé d'enregistrer les informations de trafic (adresse IP, protocole, et numéro de port) qui quittent le site et de créer une entrée `permit` temporaire au moyen du mot clé `reflect` afin de contrôler le trafic qui est reçu en réponse.

Il vérifie ensuite le trafic reçu en retour en se référant à l'entrée temporaire, grâce à l'utilisation du mot clé `evaluate`. Si le trafic correspond à l'entrée temporaire, il l'accepte, sinon, il l'évalue à l'aide des entrées de la liste étendue.

Pour définir des listes d'accès réflexives, exécutez les étapes suivantes, en commençant avec le mode de configuration globale :

1. Pour une interface externe, spécifiez la liste d'accès en sortie ; pour une interface interne, spécifiez-la en entrée. Pour cela, vous devez entrer dans le mode de configuration de liste d'accès, et utiliser la commande suivante :

```
ip access-list extended nom
```

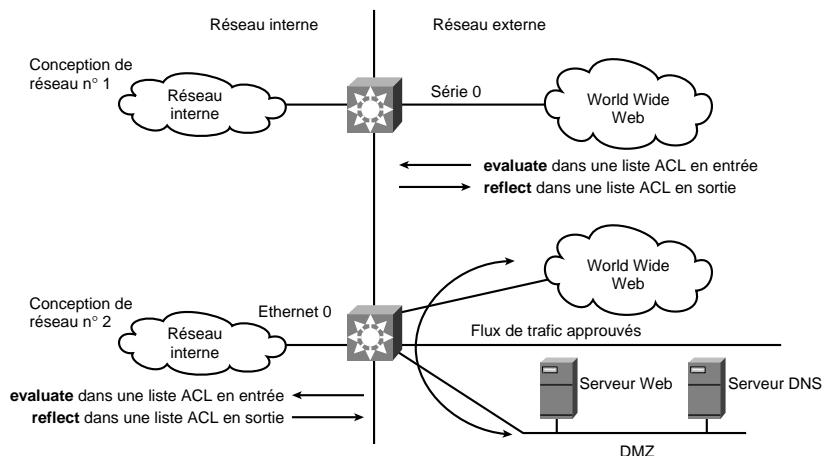
2. Définissez la liste d'accès réflexive à l'aide d'une entrée `permit` réflexive. Répétez cette étape pour chaque protocole de couche supérieure pour IP. Par exemple, vous pouvez configurer un filtrage réflexif des sessions TCP, mais également des sessions UDP. Vous pouvez employer le même nom pour plusieurs protocoles. Cette étape est une étape d'imbrication ; elle utilise la commande suivante :

```
permit protocol any any reflect nom [timeout secondes]
```

3. Les listes d'accès réflexives sont le plus souvent mises en œuvre à l'aide de deux topologies de réseau de base. Le fait de déterminer celle dont votre réseau se rapproche le plus peut vous aider à décider si vous devez appliquer ces listes sur une interface interne ou externe. La Figure 22.5 illustre ces deux topologies.

Figure 22.5

Topologies courantes pour l'implémentation de listes d'accès réflexives.



Interface externe

La première topologie illustrée est intitulée "Conception de réseau n°1". Dans cette topologie simple, les listes d'accès réflexives sont configurées sur l'interface externe Série 0, ce qui empêche le trafic IP d'entrer sur le routeur et d'atteindre le réseau interne, à moins qu'il ne fasse partie d'une session déjà établie depuis le réseau interne.

Interface interne

La seconde topologie illustrée est intitulée "Conception de réseau n°2". Dans cette topologie, les listes d'accès réflexives sont configurées sur l'interface interne Ethernet 0, ce qui autorise le trafic externe à accéder aux services au sein de la zone démilitarisée (DMZ, *Demilitarized Zone*), tels les services DNS, mais empêche le trafic IP d'entrer sur le réseau interne, à moins qu'il ne fasse partie d'une session déjà établie depuis le réseau interne.

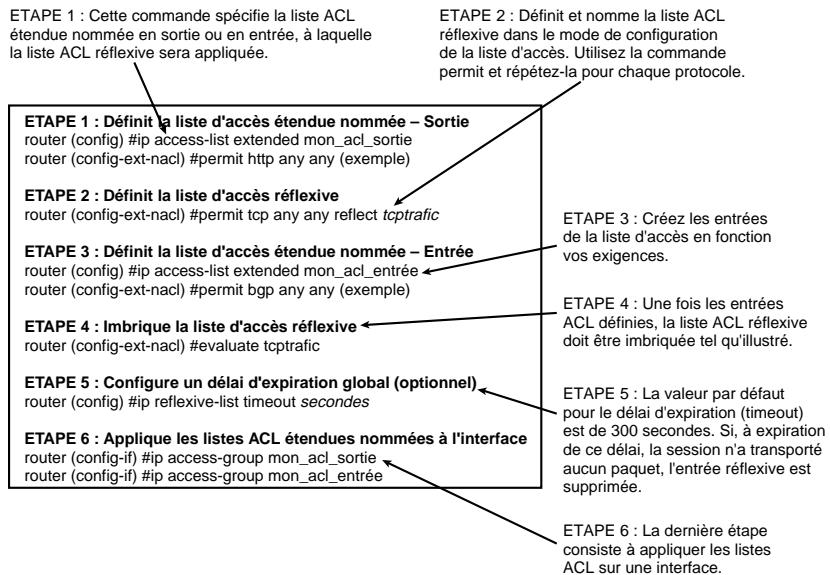
Configuration de listes d'accès réflexives

Les listes ACL réflexives offrent une sécurité plus granulaire. En effet, elles permettent au routeur de mémoriser certaines informations relatives au trafic qu'il a transmis, de façon qu'il accepte uniquement les paquets envoyés en réponse par l'intermédiaire de ce trafic. Un paquet de données est accepté comme étant une réponse valide seulement s'il provient de l'hôte et du port vers lesquels le paquet sortant a été initialement envoyé, et qu'il est adressé à l'hôte et au port qui ont émis le paquet.

Les informations du paquet de données utilisées pour générer une entrée ACL réflexive sont l'adresse IP et le port source, l'adresse IP et le port de destination, et le type de protocole. Lorsque le type de protocole est TCP ou UDP, les informations de port doivent correspondre exactement. Lorsque ICMP est utilisé, une réponse d'écho doit correspondre à une requête d'écho (c'est-à-dire une réponse ping pour une requête ping). Pour tous les autres protocoles, aucune information de port ne doit correspondre.

En fait, vous ne configurez pas explicitement des listes ACL réflexives. Une liste est générée automatiquement en réponse à un paquet qui correspond à une entrée ACL contenant la clause `reflect`. La Figure 22.6 illustre les étapes nécessaires à la configuration d'une liste ACL réflexive.

Figure 22.6
Configuration d'une liste d'accès réflexive.



Exemple de liste d'accès réflexive

L'entrée ACL suivante a été appliquée sur une interface en sortie :

```
ip access-list extended données_sortantes
! n'importe quelle clause permit/deny nécessaire.
permit udp any any reflect contrôle_données_udp
! n'importe quelle autre clause permit/deny nécessaire. Peut inclure
! une autre clause reflect.
```

L'entrée ACL suivante a été appliquée sur une interface en entrée :

```
ip access-list extended données_entrantes
! n'importe quelle clause permit/deny nécessaire.
evaluate contrôle_données_udp
! n'importe quelle autre clause permit/deny nécessaire. Peut inclure
! une autre clause reflect.
```

Le paquet en sortie est évalué par l'entrée `reflect` uniquement si aucune autre correspondance n'est trouvée auparavant. Si le paquet correspond au protocole spécifié dans l'entrée `reflect`, une entrée temporaire est créée dans la liste ACL réflexive indiquée, et le paquet est transmis en sortie sur l'interface. L'entrée temporaire spécifie les critères qui autorisent le trafic entrant (en retour), pour la même session uniquement.

Si une entrée temporaire correspondante existe déjà, cela signifie que le paquet sortant appartient à une session en cours. Par conséquent, aucune autre entrée n'a besoin d'être créée et il faut simplement réinitialiser le temporisateur d'activité (*activity timer*).

Lorsqu'un paquet de données est évalué au moyen de la liste ACL *données_sortantes*, s'il s'agit d'un paquet UDP, les informations d'adresse IP et de port source, ainsi que celles d'adresse IP et de port de destination qu'il contient sont extraites, et une clause *permit* est créée dans la liste ACL *contrôle_données_udp*. Une seule entrée ACL par session ou flux est créée.

NOTE

Si un paquet de données sortant correspond à une autre clause *permit* ou *deny*, située avant la clause *reflect* dans la liste ACL *données_sortantes*, aucune entrée temporaire n'est créée.

Lorsqu'un paquet de données est évalué au moyen de la liste ACL *données_entrantes*, et que le routeur atteint la clause *evaluate*, le paquet est contrôlé par la liste ACL *contrôle_données_udp*. S'il correspond, il est accepté ; sinon, le routeur continue l'évaluation avec la liste ACL *données_entrantes*.

NOTE

Si un paquet entrant correspond à une clause *permit* ou *deny* dans la liste *données_entrantes*, avant que la clause *evaluate* ne soit atteinte, l'entrée réflexive n'est pas contrôlée.

Lorsque le routeur reçoit un paquet, il l'évalue au moyen de la liste d'accès étendue. Si une correspondance est trouvée avant que le routeur n'ait atteint la liste d'accès réflexive, celle-ci n'est pas utilisée. Si le paquet ne correspond à aucune condition de la liste d'accès étendue, il est comparé aux instructions de la liste réflexive.

Si le paquet correspond à une entrée *permit* de la liste réflexive, une entrée temporaire est créée, et le paquet est géré en fonction des critères de correspondance. L'entrée demeure active jusqu'à ce que la session se termine.

Pour les sessions TCP, l'entrée temporaire est supprimée cinq secondes après que deux bits FIN activés aient été détectés, ou immédiatement après qu'un paquet TCP avec le bit RST activé ait été détecté. Sinon, l'entrée temporaire est supprimée lorsqu'aucun paquet de session n'a été détecté pendant un laps de temps prédéterminé, c'est-à-dire pendant l'intervalle défini au moyen du temporisateur *timeout*.

NOTE

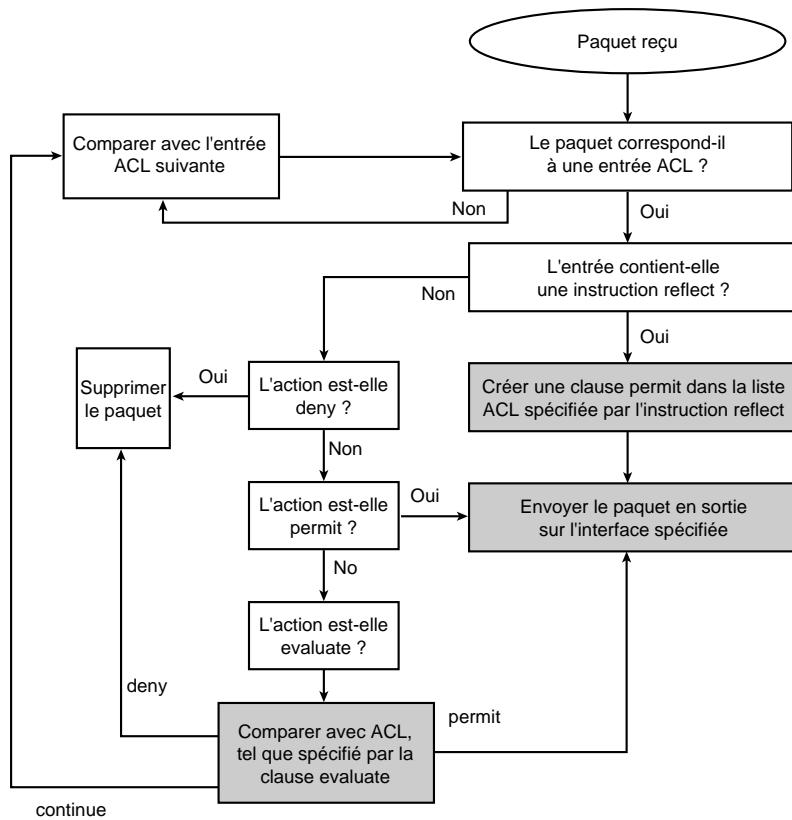
Deux bits FIN activés dans une session signifient que celle-ci est sur le point de se terminer. La fenêtre de cinq secondes laisse le temps à la session de se terminer proprement. Un bit RST activé indique une fin de session brusque.

Pour UDP et d'autres protocoles fonctionnant en mode non connecté (*connectionless*), la fin d'une session est déterminée différemment. Etant donné qu'aucune information de suivi de session n'est contenue dans ces paquets, la fin d'une session est signifiée lorsqu'aucun paquet n'a été détecté pendant un intervalle de temps configurable.

Le processus mis en œuvre par le routeur afin de traiter les entrées d'une liste d'accès réflexive est illustré à la Figure 22.7. Ayez à l'esprit les concepts essentiels suivants, lors de l'examen de ce processus :

- Comme pour n'importe quelle liste ACL, l'ordre des entrées dans une liste réflexive est critique pour son fonctionnement.
- Si le paquet correspond à une entrée de la liste étendue avant que la liste réflexive ne soit atteinte, il ne sera pas comparé avec cette dernière, et aucune entrée temporaire ne sera créée.
- Une entrée temporaire de liste ACL réflexive est créée uniquement s'il n'en existe pas déjà une pour cette session.

Figure 22.7
Fonctionnement
d'une liste ACL
réflexive.



Règles d'implémentation de listes d'accès réflexives

Les recommandations suivantes (*pour* et *contre*) sont essentielles, afin de garantir une conception réussie de vos listes ACL réflexives. Il est recommandé d'en tenir compte lors de l'implémentation d'un réseau de campus.

POUR :

- Définir ces listes uniquement avec des listes d'accès IP étendues nommées.
- Toujours utiliser deux listes d'accès IP étendues nommées, une en entrée et une autre en sortie.

CONTRE :

- Définir ces listes avec des listes d'accès IP standards numérotées ou nommées, ou avec d'autres listes d'accès de protocoles.
- Utiliser ces listes avec des applications qui emploient des numéros de port changeants, tel FTP dans le mode actif.

Listes de contrôle d'accès dynamiques (sécurité Lock-and-Key)

Pour autoriser un accès distant à des services locaux, une solution de sécurité couramment implémentée consiste à créer des listes d'accès, comme mentionné précédemment. Les listes d'accès standards et étendues présentent les limitations suivantes :

- Elles peuvent exposer le réseau à des risques d'intrusion de la part de pirates.
- Elles sont difficiles à gérer sur de grands réseaux.
- Elles imposent une surcharge de traitement au niveau du routeur, qui dépend des entrées configurées.
- Elles ne fournissent pas de mécanisme de défi permettant d'authentifier des utilisateurs individuels.

Une solution de sécurité plus efficace est d'employer la fonctionnalité d'accès *lock-and-key*, disponible uniquement avec les listes d'accès IP étendues. Cette fonctionnalité permet de configurer des listes d'accès dynamiques, qui opèrent un filtrage individuel en fonction des adresses source/destination. Le filtrage est mis en œuvre au moyen d'un processus d'authentification de l'utilisateur. Vous pouvez autoriser un accès utilisateur dynamique par l'intermédiaire d'un pare-feu, sans mettre en péril les restrictions de sécurité en place.

ATTENTION

Les améliorations apportées à la commande `access-list` pour supporter la fonctionnalité *lock-and-key*, sont compatibles en amont. Par conséquent, lors de la migration depuis une version du système Cisco IOS antérieure à la version 11.1, vos listes d'accès sont automatiquement converties afin de refléter ces améliorations. Toutefois, les versions du système Cisco IOS antérieures à la version 11.1 ne présentent pas de compatibilité avec ces améliorations. Aussi, si vous enregistrez une liste d'accès dans une version antérieure, puis que vous utilisez la version 11.1, la liste d'accès ne sera pas correctement interprétée. En fait, cela pourrait provoquer de sérieux problèmes de sécurité. Pour bien faire, vous devez sauvegarder vos anciens fichiers de configuration avec la version 11.1, ou ultérieure, avant de démarrer une image avec ces fichiers.

Dans la version 11.1 du système Cisco IOS, la fonctionnalité d'accès *lock-and-key* s'appuie sur Telnet. L'application Telnet standard est nécessaire sur la plate-forme hôte qui active le processus d'authentification.

Remarques d'implémentation de l'accès Lock-and-Key

Etant donné que la fonctionnalité *lock-and-key* offre une voie d'accès potentielle, par l'intermédiaire du pare-feu de votre réseau, vous devez examiner attentivement les aspects suivants :

- La première considération concerne l'accès dynamique. En effet, avec la mise en œuvre de listes d'accès dynamiques, il existe un risque qu'un hôte non autorisé, qui usurperait une adresse authentifiée, puisse accéder de l'autre côté du pare-feu. Toutefois, il faut savoir que la fonctionnalité d'accès *lock-and-key* n'est pas la cause du problème d'usurpation d'adresse (*spoofing*).
- Les performances sont affectées dans les deux situations suivantes :
 - Chaque liste d'accès dynamique provoque une régénération de liste d'accès sur le moteur de commutation (SSE, *Silicon Switching Engine*), ce qui entraîne un ralentissement momentané sur le chemin de commutation SSE.
 - Les listes d'accès dynamiques requièrent la fonctionnalité de temporisation d'inactivité (*idle timeout*), même si la valeur par défaut est utilisée ; elles ne peuvent par conséquent pas être commutées par le moteur SSE. Ces entrées doivent être gérées dans le chemin de commutation rapide du protocole.
- Soyez très attentif à la configuration des routeurs interzones. Lorsque des utilisateurs distants déclenchent des accès *lock-and-key* sur un routeur interzones, des entrées de liste d'accès supplémentaires sont créées sur son interface. La liste d'accès augmente et diminue de façon dynamique. Les entrées sont supprimées de la liste dynamiquement, à expiration du délai d'inactivité (*idle-timeout*) ou du délai maximal (*max-timeout*). De grandes listes d'accès peuvent entraîner une dégradation des performances de commutation des paquets.

ATTENTION

L'accès *lock-and-key* autorise un événement extérieur à provoquer une ouverture dans le système pare-feu. Une fois cette ouverture faite, le routeur est exposé à l'usurpation d'adresse source. Pour éviter cela, vous devez fournir un support pour le cryptage. Ce problème est décrit en détail, plus loin dans cette section. L'usurpation d'adresse source est un problème inhérent à toutes les listes d'accès.

Voici deux situations dans lesquelles l'accès *lock-and-key* pourrait être implémenté :

- Lorsque vous souhaitez qu'un hôte distant puisse accéder à un hôte de votre réseau *via* l'Internet. Dans ce cas, la fonctionnalité *lock-and-key* limite l'accès au-delà de votre pare-feu, en réalisant un filtrage par hôtes ou par réseaux.
- Lorsque vous voulez qu'un sous-ensemble d'hôtes sur un réseau puisse accéder à un hôte sur un réseau distant protégé par un pare-feu. Dans ce cas, l'accès *lock-and-key* permet d'accorder un accès uniquement à l'ensemble d'hôtes souhaité, en procédant à leur authentification par l'intermédiaire d'un serveur TACACS+.

Le processus suivant décrit le fonctionnement de l'accès *lock-and-key* :

1. Un utilisateur ouvre une session Telnet sur un routeur interzones configuré pour l'accès *lock-and-key*.

2. Le système Cisco IOS reçoit le paquet Telnet, et procède à l'authentification de l'utilisateur. Ce dernier doit être authentifié afin de pouvoir obtenir un accès. Le processus d'authentification peut être exécuté par le routeur ou par un serveur d'accès central, tels TACACS+ ou RADIUS.

NOTE

Il est vivement recommandé d'utiliser un serveur TACACS+ pour le processus de requêtes d'authentification. TACACS+ assure des services d'authentification, d'autorisation, et de comptabilité, et fournit également une base de données de sécurité centralisée.

3. Une fois que l'utilisateur a été authentifié, le système IOS crée une entrée temporaire dans la liste d'accès dynamique. Cette entrée hérite des paramètres de la liste. Vous pouvez limiter la plage de réseaux pour lesquels l'utilisateur a reçu une autorisation d'accès temporaire.
4. L'utilisateur échange des données par l'intermédiaire du pare-feu, puis met fin à la session.
5. L'entrée temporaire est supprimée de la liste d'accès dynamique par le système IOS, lorsqu'un délai (d'inactivité ou absolu) configuré arrive à expiration, ou bien lorsque l'administrateur système la supprime manuellement.

NOTE

Lorsque l'utilisateur met fin à une session, l'entrée temporaire demeure dans la liste d'accès dynamique, jusqu'à ce qu'elle soit supprimée par le système IOS ou l'administrateur système.

Pour configurer l'accès *lock-and-key*, réalisez les étapes suivantes, en vous plaçant dans le mode de configuration globale :

1. Configurez une liste d'accès dynamique qui servira de modèle et de contenu aux entrées temporaires. Voici les commandes que vous devez utiliser :

```
access-list numéro-liste-accès
  [dynamic nom-dynamique [timeout minutes]] {deny | permit}
  protocole source masque-source destination masque-destination
  [precedence priorité] [tos tos] [established] [log]
```

2. Configurez une interface au moyen de la commande suivante :

```
interface type numéro
```

3. Dans le mode de configuration d'interface, appliquez la liste d'accès à l'interface, à l'aide de la commande suivante :

```
ip access-group numéro-liste-accès
```

4. Dans le mode de configuration globale, définissez un ou plusieurs ports de terminal virtuel (VTY, *Virtual Terminal*). Si vous en spécifiez plusieurs, ils doivent tous être configurés de façon identique, car le système IOS recherche les ports VTY disponibles à tour de rôle. Si vous ne souhaitez pas configurer tous les ports VTY pour la fonction *lock-and-key*, vous pouvez spécifier un groupe de ports VTY uniquement. La commande suivante est utilisée pour définir des ports (VTY) :

```
line VTY numéro-ligne [numéro-dernière-ligne]
```

5. Configurez l'authentification utilisateur (des informations supplémentaires sur la mise en œuvre de ce type d'authentification sont données dans la prochaine section). Pour cela, utilisez les commandes suivantes :

```
login tacacs nom-utilisateur nom mot-de-passe secret
password mot-de-passe login local
```

6. Autorisez la création d'entrées temporaires de listes d'accès. Si l'argument host n'est pas spécifié, tous les hôtes du réseau sont autorisés à en créer. La liste d'accès dynamique contient le masque de réseau, qui permet la nouvelle connexion de réseau. La commande suivante est utilisée :

```
autocommand access-enable [host] [timeout minutes]
```

Configuration de l'authentification utilisateur

Il existe trois méthodes de configuration d'un processus de requêtes d'authentification (voir l'étape 5 de la liste de tâches précédente), qui sont les suivantes :

- Utilisez un serveur de sécurité d'accès de réseau comme TACACS+. Cette méthode implique des étapes de configuration supplémentaires au niveau du serveur TACACS+, mais permet d'utiliser des requêtes d'authentification plus précises ainsi que des fonctions de suivi sophistiquées :

```
Router(config)# login tacacs
```

- La commande **username**. Cette méthode est plus efficace, car chaque utilisateur doit être authentifié individuellement. La syntaxe employée est la suivante :

```
Router# username nom password mot-de-passe
```

- Les commandes **password** et **login**. Cette méthode est moins efficace, car le mot de passe est configuré pour le port, mais non pour l'utilisateur. Par conséquent, n'importe quel utilisateur connaissant le mot de passe peut se faire authentifier. La syntaxe employée est la suivante :

```
Router# password mot-de-passe
Router# login local
```

Règles d'implémentation de listes d'accès dynamiques

Il est conseillé de suivre ces recommandations lors de la configuration de listes d'accès dynamiques :

- Assignez des paramètres à la liste d'accès dynamique, de la même manière que pour les listes d'accès statiques. Les entrées temporaires héritent des paramètres assignés à la liste.
- Configurez Telnet comme protocole pour que les utilisateurs soient soumis au processus de requêtes d'authentification. L'accès à Telnet doit être autorisé pour mettre en œuvre l'authentification utilisateur.
- Définissez soit une valeur de délai d'inactivité (à l'aide de la commande **access-enable**, dans la commande **autocommand**), soit une valeur de délai absolu (à l'aide du mot clé **timeout**, dans la commande **access-list**). Si vous ne le faites pas, l'entrée temporaire demeurera configurée indéfiniment sur l'interface, même après que l'utilisateur aura mis fin à la session (et jusqu'à ce que l'administrateur la supprime manuellement).
- Lorsque vous configurez à la fois le délai d'inactivité et le délai absolu, faites en sorte que la valeur du premier paramètre soit inférieure à celle du second.

- Lorsque vous configurez un délai d'inactivité, spécifiez une valeur égale à celle du délai d'inactivité WAN.
- Ne créez pas plus d'une liste d'accès dynamique pour une liste d'accès donnée. Le système se réfère uniquement à la première liste dynamique définie.
- N'assignez pas un nom de liste dynamique existant à une autre liste d'accès, sinon le système réutilisera la liste existante. Toutes les entrées nommées dans la configuration doivent être uniques.
- Si le routeur exécute la commande `autocommand`, configurez tous les ports VTY avec la même commande `autocommand`. L'omission de cette commande sur un port VTY autorise n'importe quel hôte à accéder au mode EXEC du routeur, et ne crée pas d'entrée temporaire dans la liste d'accès dynamique.

Lorsque vous créez des listes d'accès dynamiques, ayez à l'esprit les éléments suivants :

- Les seules valeurs remplacées dans l'entrée temporaire sont l'adresse source ou de destination, selon que la liste dynamique a été placée dans une liste d'accès en entrée ou en sortie. Tous les autres paramètres, tel le port, sont hérités de la liste d'accès dynamique.
- Chaque ajout dans une liste dynamique est toujours placé en début de liste. Vous ne pouvez pas spécifier l'ordre des entrées.
- Les entrées temporaires de liste d'accès ne sont jamais écrites en NVRAM.

L'authentification utilisateur est réussie lorsque les événements de routeur suivants se produisent :

- L'utilisateur se connecte sur le port VTY du routeur.
- Le routeur exécute la commande `autocommand`, configurée pour la commande `access-enable`.
- Une entrée temporaire de liste d'accès est créée, et la session Telnet est terminée. L'hôte spécifié peut maintenant accéder de l'autre côté du pare-feu.

Vous pouvez vérifier que l'implémentation sur le routeur est réussie en demandant à l'utilisateur de tester la connexion, ou bien en utilisant la commande `show-access-lists`, afin de visualiser les listes d'accès dynamiques.

L'exemple suivant illustre ce que l'utilisateur pourrait obtenir, une fois le processus d'authentification réussi. Notez que la connexion Telnet a été fermée immédiatement après que le mot de passe a été fourni, puis authentifié. L'entrée temporaire a déjà été créée ; l'hôte qui a initié la session Telnet peut accéder de l'autre côté du pare-feu :

```
Router# telnet corporate
Trying 172.21.52.1 ...
Connected to corporate.abc.com.
Escape character is '^]'.
User Access Verification
Password:
Connection closed by foreign host.
```

Suppression d'une liste d'accès dynamique

Si vous avez besoin de supprimer une liste d'accès dynamique, saisissez la commande suivante (en mode EXEC privilégié) :

```
clear access-template [numéro-liste-accès | nom]
[ nom-dynamique ] [source] [destination]
```

Vous pouvez afficher les entrées temporaires de liste d'accès lorsqu'elles sont en cours d'utilisation. Une fois qu'une entrée a été supprimée par le système ou l'administrateur, elle ne peut plus être affichée. Le nombre de correspondances affiché représente le nombre de fois où l'entrée de liste a permis de trouver une correspondance.

Exemple de liste d'accès dynamique

L'exemple suivant montre comment configurer l'accès *lock-and-key*. Etant donné que l'authentification est assurée par un serveur TACACS+, aucune commande autocmd n'apparaît dans cette configuration. L'accès *lock-and-key* est configuré sur l'interface BRI0, et quatre ports VTY sont définis avec le mot de passe cisco :

```
aaa authentication login default tacacs+ enable
aaa accounting exec stop-only tacacs+
aaa accounting network stop-only tacacs+
enable password ciscotac
!
isdn switch-type basic-dms100
!
interface ethernet0
ip address 172.18.23.9 255.255.255.0
!
!
interface BRI0
ip address 172.18.21.1 255.255.255.0
encapsulation ppp
dialer idle-timeout 3600
dialer wait-for-carrier-time 100
dialer map ip 172.18.21.2 name diana
dialer-group 1
isdn spid1 2036333715291
isdn spid2 2036339371566
ppp authentication chap
ip access-group 102 in
!
access-list 102 dynamic testlist timeout 5 permit ip any any
access-list 102 permit tcp any host 172.18.21.2 eq 23
!
ip route 172.18.250.0 255.255.255.0 172.18.21.2
priority-list 1 interface BRI0 high
tacacs-server host 172.18.23.21
tacacs-server host 172.18.23.14
tacacs-server key test1
tftp-server rom alias all
!
dialer-list 1 protocol ip permit
!
line con 0
password cisco
line aux 0
```

```
line VTY 0 4
password cisco
!
```

TACACS (*Terminal Access Controller Access Control System*)

Les mots de passe des modes non privilégié et privilégié sont globaux, et s'appliquent à chaque utilisateur qui accède au routeur à partir du port de console ou d'une session Telnet. Le système d'authentification TACACS représente un autre moyen de valider chaque utilisateur individuellement, avant qu'il ne puisse accéder au routeur ou au serveur de communication. TACACS a été initialement développé par le Département de la défense américain (DoD, *Department of Defense*) ; il est décrit dans le RFC 1492. Ce système est utilisé par Cisco pour permettre un contrôle plus granulaire des accès utilisateur au routeur dans les modes non privilégié et privilégié.

Lorsque TACACS est activé, le routeur invite l'utilisateur à fournir un nom et un mot de passe. Il interroge ensuite un serveur TACACS afin de déterminer si le mot de passe communiqué par l'utilisateur est correct. Un serveur TACACS s'exécute en général sur une station de travail Unix. Les serveurs TACACS du domaine public peuvent être obtenus via FTP anonyme à [ftp.cisco.com](ftp://ftp.cisco.com), dans le répertoire */pub*. Utilisez le fichier */pub/README* pour trouver le nom de fichier. La version 3 de CiscoWorks fournit un support complet pour un serveur TACACS.

La commande de configuration `tacacs-server host` spécifie l'hôte Unix qui exécute un serveur TACACS qui validera les requêtes envoyées par le routeur. Vous pouvez entrer cette commande plusieurs fois afin de spécifier plusieurs hôtes de serveur TACACS pour un routeur.

Accès non privilégié

Si aucun serveur n'est disponible, vous ne pourrez peut-être pas accéder au routeur. Dans ce cas, la commande de configuration `tacacs-server last-resort [password | succeed]` permet d'indiquer si l'utilisateur est autorisé à se connecter sans mot de passe (mot clé `succeed`) ou s'il doit fournir le mot de passe d'ouverture de session standard (mot clé `password`).

Les commandes suivantes spécifient un serveur TACACS, et autorisent une ouverture de session réussie si le serveur est défaillant ou injoignable :

```
tacacs-server host 129.140.1.1
tacacs-server last-resort succeed
```

Pour obliger l'utilisateur qui souhaite accéder au routeur via Telnet à s'authentifier auprès du serveur TACACS, utilisez les commandes de configuration suivantes :

```
line vty 0 4
login tacacs
```

Accès privilégié

Cette méthode de vérification de mots de passe peut également s'appliquer à ceux du mode privilégié, grâce à la commande `enable use-tacacs`. Si aucun serveur n'est disponible, vous ne pourrez peut-être pas accéder au routeur. Dans ce cas, la commande de configuration `enable last-resort [password | succeed]` permet d'indiquer si l'utilisateur est autorisé à se connecter sans mot de passe (mot clé `succeed`) ou s'il doit fournir le mot de passe du mode privilégié (mot clé `password`). L'utilisation du mot clé `succeed` comprend de nombreux risques. Si vous employez la commande `enable use-tacacs`, vous devez également spécifier la commande `tacacs-server authenticate enable`.

La commande `tacacs-server extended` autorise un équipement Cisco à s'exécuter dans le mode TACACS étendu. Le système Unix doit exécuter le démon TACACS étendu, qui peut être obtenu via FTP anonyme, à [ftp.cisco.com](ftp://ftp.cisco.com). Le nom de fichier est `xtacacs.shar`. Ce démon permet aux serveurs de communication, ainsi qu'à d'autres équipements, de dialoguer avec le système Unix et de mettre à jour un historique d'audit avec des informations d'utilisation de port, de comptabilité, ou toute autre information pouvant être envoyée par l'équipement.

La commande `username utilisateur password [0 | 7] mot-de-passe` permet de stocker et de maintenir une liste des utilisateurs et de leurs mots de passe sur un équipement Cisco, plutôt que sur un serveur TACACS. La valeur 0 stocke le mot de passe en texte clair dans le fichier de configuration, et la valeur 7 le stocke sous forme cryptée. Si vous ne disposez pas d'un serveur TACACS et que vous souhaitez quand même authentifier les utilisateurs de façon individuelle, vous pouvez définir des utilisateurs de la manière suivante :

```
username steve password 7 steve-pass
username allan password 7 allan-pass
```

Cartes d'accès à jetons (token card)

L'emploi des services TACACS sur des routeurs et des serveurs de communication permet de supporter des équipements avec cartes d'accès physiques, ou l'ajout de cartes d'accès à jetons. Le code du serveur TACACS peut être modifié afin d'exploiter ces fonctions, sans nécessiter de modifications dans l'installation ou la configuration des routeurs et des serveurs de communication. Ce code modifié n'est pas directement disponible auprès de Cisco.

Le système de cartes d'accès à jetons s'appuie sur une carte physique que l'utilisateur doit posséder afin de fournir une authentification. A l'aide des liens appropriés dans le code de serveur TACACS, des sociétés tierces peuvent proposer aux clients des serveurs TACACS améliorés. Le système logiciel de sécurité Enigma Logic SafeWord en est un exemple. D'autres systèmes de cartes d'accès, tel Security Dynamics SmartCard, peuvent également être ajoutés au TACACS.

Autres mesures de sécurité Cisco

Ce chapitre a présenté bon nombre des fonctionnalités de sécurité les plus importantes et les plus connues actuellement disponibles. Il existe toutefois d'autres techniques importantes, qui ne devraient pas être négligées lors de la conception de solutions de sécurité complètes. Elles sont présentées dans cette section.

Contrôle de l'accès aux serveurs de réseau hébergeant des fichiers de configuration

Si un routeur télécharge régulièrement des fichiers de configuration à partir d'un serveur TFTP (*Trivial File Transfer Protocol*) ou MOP (*Maintenance Operations Protocol*), quiconque possédant l'accès au serveur peut également modifier les fichiers de configuration du routeur qui y sont stockés.

Les serveurs de communication peuvent être configurés pour accepter les connexions LAT (*Local Area Transport*) entrantes. Les traducteurs de protocoles et leur routeur traducteur peuvent accepter les connexions X.29. Ces différents types d'accès devraient être examinés lors de la création d'une architecture pare-feu.

Messages de notification d'utilisations non autorisées

Il est également prudent de définir des messages qui notifient des utilisations non autorisées, qui seront affichés sur toutes les nouvelles connexions. Pour cela, vous disposez de deux méthodes. La première consiste à recourir à la commande de configuration globale EXEC banner sur le serveur de communication pour saisir, par exemple, le message suivant :

```
banner exec ^C
Si vous rencontrez des problèmes avec les lignes d'appels entrants, envoyez
→ un e-mail à helpdesk@sociétéX.com. Si vous obtenez le message "% Votre compte a
→ expiré", envoyez un e-mail indiquant votre nom et votre boîte de messagerie
→ vocale à helpdesk@sociétéX.com, et quelqu'un vous contactera pour renouveler
→ votre compte. Une utilisation non autorisée de ces ressources est interdite.
```

Vous avez également la possibilité d'utiliser la commande de configuration globale EXEC motd banner sur n'importe quel équipement de réseau :

```
OSPF_Router (config)# motd banner
*****
*           ! ! ! ! ! ! ! ATTENTION ! ! ! ! ! ! !
*           CE SYSTEME EST LA PROPRIETE DE <nom-société>.
*           TOUS ACCES ET UTILISATION NON AUTORISES DE CE SYSTEME
*           SONT FORMELLEMENT INTERDITS PAR <nom-société>
*           ET SONT CONTRAIRES AUX STRATEGIES DE SECURITE,
*           AU REGLEMENT ET A LA LOI.
*
*           LES UTILISATEURS NON AUTORISES SONT PASSIBLES DE POURSUITES
*           JUDICIAIRES ET SERONT SOUMIS AUX PROCEDURES
*           DISCIPLINAIRES INITIEES PAR LA SOCIETE.
*****
```

Afficher un message comme celui-ci sur un équipement de réseau est très efficace. Il vous couvre dans tous les cas, et spécifie même que les actions entreprises par des utilisateurs non autorisés ne resteront pas impunies.

Sécurisation de services non standards

Il existe un certain nombre de services non standards disponibles à partir de l'Internet, qui offrent des fonctionnalités à valeur ajoutée lors de la connexion au monde extérieur. Dans le cas d'une connexion à l'Internet, ces services peuvent être très sophistiqués et complexes. En voici des exemples : le Web (*World Wide Web*), le service WAIS (*Wide Area Information Service*), Gopher et Mosaic. La plupart de ces systèmes sont conçus pour fournir à l'utilisateur une quantité d'informations sous forme organisée, ce qui permet une navigation et une recherche structurées.

La majorité de ces systèmes utilisent un protocole défini spécifiquement pour eux. Certains, comme Mosaic, utilisent plusieurs protocoles différents, afin d'obtenir les informations demandées. Soyez prudent lorsque vous concevez des listes d'accès applicables à chacun de ces services. Dans de nombreux cas, ces listes deviendront étroitement liées avec l'interaction de ces services.

Sécurité avec niveaux de privilèges

Cette fonctionnalité a été introduite par Cisco dans la version 10.3 de Cisco IOS. Elle autorise la définition de 16 niveaux de sécurité d'accès sur un routeur. Les niveaux de privilège par défaut sont 1 = utilisateur et 15 = privilégié.

Ces niveaux de privilège peuvent être exploités de différentes manières :

- Ils peuvent être établis pour des commandes et des lignes de terminal entrantes.
- Des mots de passe spéciaux peuvent leur être associés.
- Ils peuvent être assignés à des commandes EXEC et de configuration spéciales pour contrôler l'accès.

Modes de commandes et niveaux de privilège

Vous pouvez implémenter les modes de commandes suivants, en utilisant des niveaux de privilège (ce sont toutes des commandes de configuration globale, excepté EXEC) :

configuration	line	hub	route-map
controller	map-class	interface	router
EXEC	map-list	ipx-router	

Exemple de configuration de niveaux de privilège

Pour associer un niveau de privilège à une commande spécifique, vous devez configurer le routeur comme suit :

```
Router(config)# privilege exec level 6 ping
Router(config)# privilege exec level 6 clear
```

Ces deux commandes, lorsqu'elles sont appliquées à un port VTY de routeur (ceux qui supportent les connexions Telnet), autorisent quiconque à accéder au routeur simplement au moyen de la commande vty, afin d'y exécuter des pings étendus ainsi qu'une variété de commandes de réinitialisation (*clear*), telles que counters, interface, router, etc.

Pour définir un mot de passe de mode privilégié pour un niveau de privilège, saisissez la commande suivante :

```
Router(config)# enable password level numéro-niveau mot-de-passe
```

Pour associer un niveau de privilège à une ligne de terminal, saisissez la commande suivante :

```
Router(config)# line vty 0 4
Router(config-line)# privilege level numéro-niveau
```

Cryptage des données de réseau

Pour protéger les données de votre réseau, Cisco fournit des services de cryptage de données de réseau et d'authentification de routeur. Cette section décrit brièvement leur implémentation, ainsi que les avantages qu'ils présentent. Une description détaillée des techniques et processus impliqués dans le déploiement de ces fonctionnalités sur votre réseau dépasserait le cadre de ce livre. A la fin de cette section, des ressources supplémentaires sont répertoriées, au cas où vous souhaiteriez en apprendre davantage sur le sujet.

Le cryptage des données de réseau est assuré au niveau paquet IP. Le cryptage de niveau paquet IP protège les données contre des écoutes clandestines. Lorsqu'il est mis en œuvre, les paquets IP peuvent être observés durant la transmission, mais leur contenu (charge utile) n'est pas lisible. Plus précisément, l'en-tête IP et les en-têtes de protocole de couche supérieure (TCP ou UDP) ne sont pas cryptés, à

l'inverse de la charge utile dans le paquet TCP ou UDP, ce qui garantit une non lisibilité des données durant leur transmission.

Le cryptage et le décryptage des paquets IP a lieu uniquement au niveau des routeurs qui sont configurés pour cette fonctionnalité, et pour l'authentification de routeur. Ces routeurs sont désignés par les termes *routeurs de cryptage homologues (peer encrypting routers)*, ou tout simplement *routeurs homologues*. Les nœuds intermédiaires ne participent pas au processus de cryptage/décryptage.

En règle générale, lorsqu'un paquet IP est généré initialement sur un hôte, il n'est pas crypté (texte clair), car la création du paquet a lieu sur une portion sécurisée (interne) du réseau. Lorsque le routeur de cryptage reçoit le paquet de l'hôte en question, il détermine s'il doit ou non le crypter. S'il décide de le faire, le paquet est ensuite envoyé sur une portion non sécurisée du réseau (habituellement un réseau externe, tel l'Internet) vers le routeur de cryptage homologue. A réception du paquet, le routeur homologue le décrypte, puis le transmet en texte clair à l'hôte de destination sur son réseau.

NOTE

Il faut savoir que, lorsque vous implémentez le cryptage de niveau IP, vous appliquez une charge de traitement supplémentaire au niveau des routeurs. Vous devriez donc vous assurer qu'ils sont capables de gérer cette surcharge, en procédant à un test préalable.

La fonction d'authentification de routeur autorise deux homologues de cryptage à identifier la source des données cryptées entrantes. Cela signifie que des intrus ne peuvent pas falsifier ou manipuler des données transmises, sans que cela ne se remarque. Le processus d'authentification est exécuté entre deux routeurs homologues chaque fois qu'une nouvelle session cryptée est établie. L'établissement d'une session cryptée a lieu lorsqu'un routeur de cryptage reçoit un paquet IP qui doit être crypté, a moins qu'une telle session ne soit déjà en cours.

ATTENTION

N'oubliez pas que les données se retrouvent dans une forme cryptée uniquement lorsqu'elles quittent le routeur de cryptage pour être envoyées vers le routeur homologue. Ce qui veut dire qu'elles circulent depuis l'hôte vers le routeur de cryptage dans une forme non cryptée, c'est-à-dire non sécurisée.

Pour assurer le cryptage de niveau paquet IP avec une authentification de routeur, Cisco implémente les standards suivants : le standard de signature numérique DSS (*Digital Signature Standard*), l'algorithme avec clé publique Diffie-Hellman (DH), et le standard de cryptage de données DES (*Data Encryption Standard*). DSS est utilisé pour l'authentification de routeur ; l'algorithme DH et le standard DES sont utilisés pour initier des sessions de communication cryptées entre les routeurs participants.

Etude de cas 1 : authentification de protocole de routage

Cette étude de cas est tirée d'un ouvrage sur OSPF qui fait autorité, *OSPF Network Design Solutions*, de Thomas M. Thomas II, publié chez Cisco Press (en langue anglaise). Les informations

fournies ici ont été mises à jour afin de refléter plus précisément le contenu et la pertinence de ce chapitre, mais vous pouvez vous reporter à cet ouvrage pour une étude de cas complète.

Authentification de routeur voisin OSPF

La conception du protocole OSPF intègre un niveau de sécurité minimale, c'est-à-dire qu'il n'empêche pas les données de circuler sur le réseau, mais offre une protection des informations de routage exploitées par les routeurs OSPF. Cette idée qu'un protocole soit conçu avec une sécurité, même minimale, semble contradictoire avec sa fonction ? En fait, lorsque OSPF a été conçu, les champs nécessaires pour assurer cette sécurité ont été inclus dans la structure des paquets, ce qui assurait la protection des annonces LSA, mais, du même coup, l'intégrité des tables de routage et du domaine de routage OSPF. Vous pouvez empêcher n'importe quel routeur OSPF de recevoir des mises à jour de routes frauduleuses en configurant cette sécurité, également connue sous le nom *d'authentification de routeur voisin*.

Cette section décrit ce mécanisme d'authentification dans le cadre d'une politique de sécurité globale, en répondant aux questions suivantes : Qu'est-ce que l'authentification de routeur voisin ? Comment fonctionne-t-elle ? Quels sont les avantages qu'elle présente pour améliorer la sécurité globale du réseau ?

Vous pouvez l'implémenter de deux manières sur un réseau OSPF. L'une consiste à assigner la même clé d'authentification OSPF sur tout le réseau ; l'autre à assigner une clé d'authentification différente à chaque liaison.

NOTE

Cette section se réfère à l'authentification de routeur voisin au moyen de l'expression *authentification de voisin*. Cette fonctionnalité est parfois également appelée *authentification de route*.

Avantages de l'authentification de voisin OSPF

Lorsque l'authentification de voisin est configurée, elle est exploitée chaque fois que des mises à jour de routage sont échangées entre des routeurs OSPF voisins. Ce mécanisme garantit qu'un routeur reçoit des informations de routage fiables de la part d'une source approuvée.

En l'absence de cette authentification, des mises à jour non autorisées ou délibérément malveillantes pourraient mettre en péril la sécurité du trafic sur le réseau. Par exemple, si une personne hostile parvenait à détourner ou à analyser le trafic de votre réseau, la sécurité de celui-ci serait sérieusement remise en question.

Un routeur non autorisé pourrait envoyer de fausses mises à jour de routage indiquant à votre routeur de transmettre le trafic vers une destination erronée. Ce trafic détourné pourrait ensuite être analysé, en vue d'obtenir des données confidentielles sur votre entreprise, ou plus simplement de perturber la communication sur votre réseau. L'authentification de voisin protège un routeur contre ce genre d'activités.

Conditions de déploiement de l'authentification de voisin OSPF

Vous devriez configurer un routeur pour l'authentification de voisin OSPF, s'il répond à l'une des conditions suivantes :

- Il est exposé au risque de recevoir une fausse mise à jour de routage.
- S'il venait à recevoir une fausse mise à jour de routage, la sécurité du réseau serait affectée.
- Votre politique de sécurité exige qu'il soit configuré pour cette fonctionnalité.

N'oubliez pas que, lorsque vous configurez un routeur pour l'authentification, vous devez également configurer ses routeurs voisins.

Fonctionnement de l'authentification de voisin

Une fois que l'authentification de voisin a été configurée sur un routeur, celui-ci authentifie la source de chaque paquet de mise à jour de routage qu'il reçoit. Pour cela, une clé d'authentification (parfois appelée mot de passe) est échangée entre le routeur émetteur et le routeur destinataire.

Deux types d'authentications de voisin sont utilisées : l'authentification en texte clair et l'authentification MD5 (algorithme *Message Digest*, version 5). Les deux mécanismes fonctionnent de la même manière, à la différence que MD5 envoie un "condensé de message" à la place de la clé d'authentification. Ce condensé est créé à partir de la clé et du message, mais la clé n'est pas envoyée, ce qui évite qu'elle soit capturée pendant la transmission. L'authentification en texte clair transmet la clé d'authentification sur la ligne.

NOTE

La mise en œuvre de l'authentification en texte clair n'est pas recommandée dans le cadre d'une politique de sécurité. Elle sert principalement à éviter des changements accidentels dans l'infrastructure de routage. Il est recommandé d'utiliser à la place l'authentification MD5.

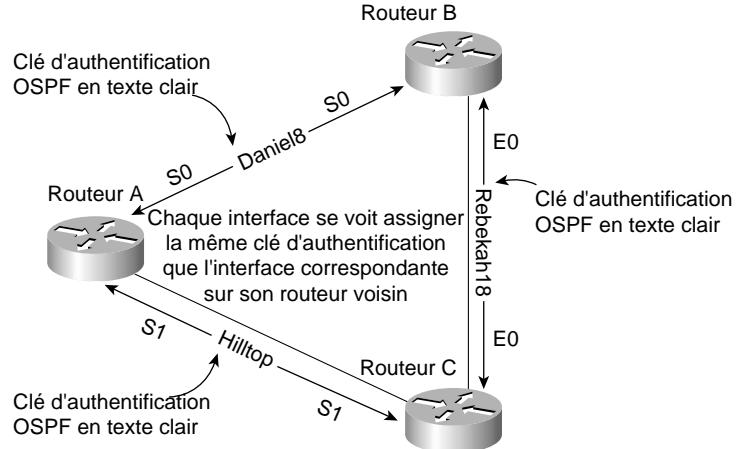
ATTENTION

A l'instar des mots de passe, il est impératif de conserver les clés d'authentification à l'abri des regards indiscrets. Les avantages qu'offre cette authentification en matière de sécurité reposent sur la confidentialité des clés. De plus, lorsque vous effectuez des tâches de gestion de routeur *via* SNMP(*Simple Network Management Protocol*), n'ignorez pas le risque associé à la transmission de clés avec des versions de SNMP qui n'utilisent pas le cryptage.

Authentification en texte clair

Tous les routeurs voisins participants doivent partager une clé d'authentification, qui est spécifiée sur chacun d'eux lors de la configuration. Plusieurs clés peuvent être spécifiées avec OSPF, chacune d'elle devant être identifiée par un numéro de clé. Par exemple, chaque interface WAN située sur un routeur qui exploite OSPF peut se voir assigner une clé différente. L'inconvénient est que le routeur voisin de chaque interface doit être configuré avec la clé correspondante sur son interface entrante (voir Figure 22.8).

Figure 22.8
Authentification OSPF en texte clair.



En règle générale, lorsqu'une mise à jour de routage est envoyée, la séquence d'authentification suivante a lieu :

1. Un routeur envoie une mise à jour de routage avec une clé d'authentification.
2. Le routeur destinataire (voisin) compare la clé qu'il reçoit avec celle qui est stockée dans sa mémoire.
3. Si les deux clés sont identiques, le routeur destinataire accepte le paquet de mise à jour. Si elles diffèrent, le paquet de mise à jour est rejeté.

Authentification MD5

L'authentification MD5 fonctionne de façon semblable à l'authentification en texte clair, excepté que la clé n'est jamais envoyée sur la liaison. Au lieu de cela, le routeur utilise l'algorithme de hachage MD5 afin de générer un condensé de message (ou signature) de la clé, qui est envoyé à la place de la clé. Cela signifie qu'il est impossible pour quiconque écoute clandestinement la ligne de découvrir la clé.

Dépannage de OSPF et authentification

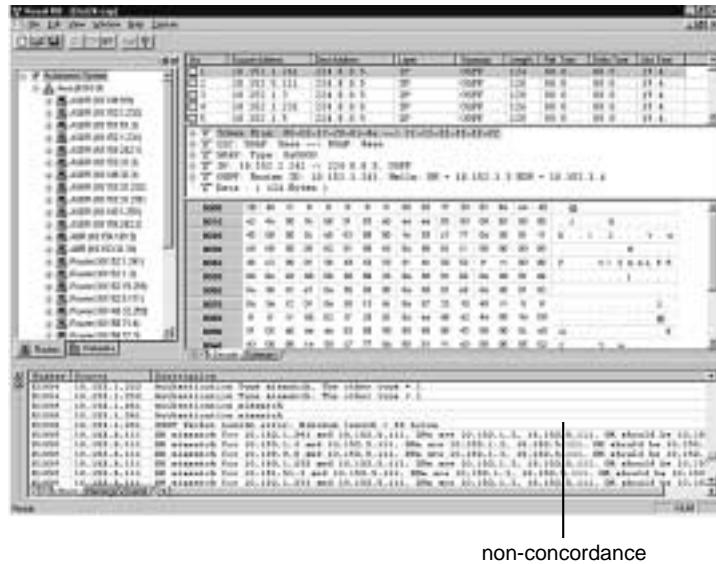
Une implémentation OSPF peut parfois être très difficile à dépanner. Bien que l'ingénieur de réseau dispose déjà d'un grand nombre d'outils différents, il existe un nouvel outil prometteur, qui facilite grandement cette tâche laborieuse.

A la Figure 22.9, vous pouvez voir que l'authentification OSPF a été délibérément mal configurée.

Le premier message, "Authentication type mismatch. The other type = 1" ("non-concordance de type d'authentification. Autre type = 1") se réfère au fait qu'un routeur a été configuré pour l'authentification OSPF avec MD5, mais pas l'autre, ce qui engendre une non-concordance du type d'authentification utilisé par le processus OSPF.

Figure 22.9

Programme de dépannage VisualOSPF de VisualProtocols.



Le second message, "Authentication mismatch" ("non-concordance d'authentification") se réfère au fait que les deux routeurs en question ont été configurés avec un mot de passe différent, ce qui engendre une non-concordance de l'authentification par mot de passe.

La société Visual Protocols propose d'autres outils intéressants du même genre. Pour plus d'informations sur ces programmes, visitez les sites <http://www.netcerts.com> et <http://www.visualprotocols.com>.

Etude de cas 2 : conception d'une architecture pare-feu

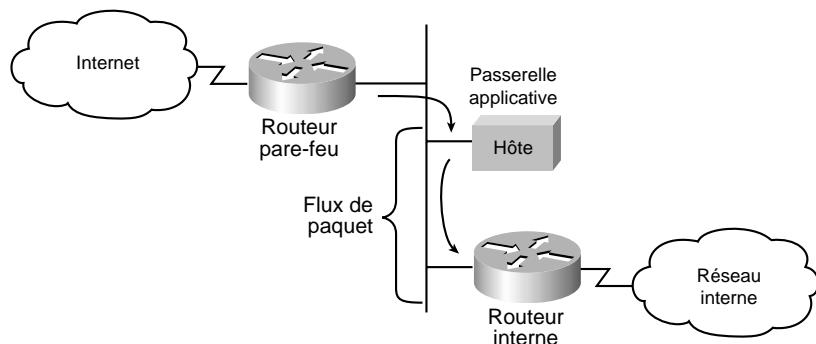
Cette étude de cas est tirée d'un ouvrage sur OSPF qui fait autorité, *OSPF Network Design Solutions*, de Thomas M. Thomas II, publié chez Cisco Press (en langue anglaise). Les informations fournies ici ont été mises à jour afin de refléter plus précisément le contenu et la pertinence de ce chapitre, mais vous pouvez vous reporter à cet ouvrage pour une étude de cas complète.

Cette étude de cas décrit le déploiement d'un pare-feu Cisco PIX Firewall sur un réseau. Une architecture avec routeur pare-feu est une structure qui se situe entre le monde extérieur (l'Internet, par exemple) et votre réseau, et qui sert à protéger ce dernier contre les intrus potentiels (c'est-à-dire, les cyber-pirates). Dans la plupart des cas, ces intrus s'infiltreront par l'intermédiaire du réseau Internet dans son ensemble et des milliers de réseaux distants qu'il interconnecte. En général, un pare-feu est constitué de plusieurs machines différentes (voir Figure 22.10).

Dans cette architecture, le routeur qui est connecté à l'Internet (routeur externe) oblige tout le trafic entrant à passer par la passerelle applicative. Le routeur qui est connecté au réseau interne (routeur interne) accepte uniquement les paquets provenant de la passerelle.

Figure 22.10

Architecture pare-feu type.



La passerelle logicielle met en œuvre des stratégies par applications et par utilisateurs. En effet, elle contrôle la livraison des services de réseau à destination et en provenance du réseau interne. Par exemple, seules certaines applications sont autorisées à établir des connexions entre un hôte intérieur au réseau et un hôte extérieur, ou bien seuls certains utilisateurs ont le droit de communiquer à l'aide de l'Internet.

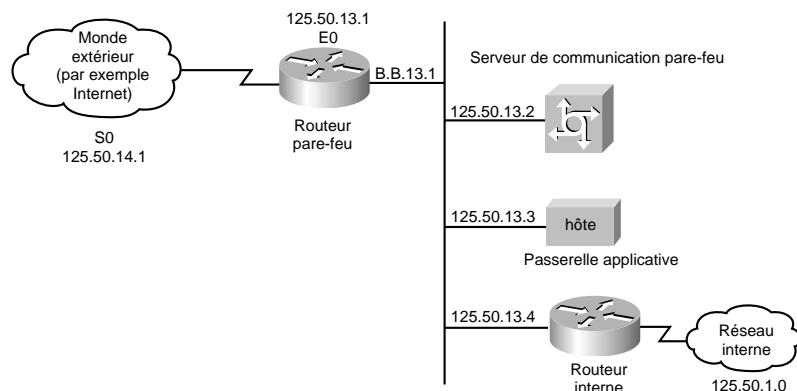
Des filtres de routes et de paquets doivent être définis pour refléter ces stratégies. Si la seule application acceptée est une application de messagerie, seuls les paquets de messagerie doivent être autorisés à traverser le routeur interne. Cela permet de protéger la passerelle, et évite de la submerger de paquets qu'elle supprimerait autrement.

Contrôle du flux de trafic

Cette section s'appuie sur le scénario illustré à la Figure 22.11. Elle décrit l'utilisation de listes d'accès, qui visent à limiter le trafic entrant et sortant sur un routeur pare-feu et sur un serveur de communication pare-feu. Ce dernier est configuré pour gérer les connexions entrantes.

Figure 22.11

Contrôle du flux de trafic via le routeur pare-feu.



Dans cette étude de cas, le routeur pare-feu autorise les nouvelles connexions entrantes vers un ou plusieurs serveurs de communication ou hôtes. Il est préférable de disposer d'un routeur désigné pour servir de pare-feu. Cela permet d'identifier clairement son rôle en tant que passerelle extérieure, et évite également d'encombrer les autres routeurs avec cette tâche. Au cas où le réseau interne aurait besoin d'être isolé, le routeur pare-feu assure la protection de la structure interne du réseau.

Les connexions aux hôtes se limitent aux requêtes FTP (*File Transfer Protocol*) entrantes et aux services de messagerie, tel que décrit à la section "Définition de listes d'accès de pare-feu", plus bas dans ce chapitre. Les connexions Telnet, ou par modem, entrantes sur le serveur de communication sont filtrées sur ce serveur, qui exécute le système d'authentification de nom utilisateur TACACS, tel que décrit à la section "Configuration du serveur de communication pare-feu", dans ce chapitre.

NOTE

Les connexions entre une ligne de modem de serveur de communication et une autre ligne de modem sortante (ou vers le monde extérieur) devraient être refusées, afin d'empêcher que des utilisateurs non autorisés exploitent les ressources de votre réseau pour lancer une attaque vers l'extérieur. Puisque à ce stade les intrus auront déjà réussi l'authentification TACACS, il est fort probable qu'ils possèdent le mot de passe d'un utilisateur. Il est vivement conseillé d'utiliser des mots de passe TACACS différents des mots de passe d'hôte.

Configuration du routeur pare-feu

Dans la configuration de routeur pare-feu suivante, le sous-réseau 152.50.13.0 du réseau de classe B 152.50.0.0 est le sous-réseau pare-feu ; le sous-réseau 152.50.14.0 fournit la connexion à l'Internet via un fournisseur de services :

```
interface ethernet 0
ip address 152.50.13.1 255.255.255.0
interface serial 0
ip address 152.50.14.1 255.255.255.0
router ospf 500
network 152.50.0.0
```

Cette configuration simple ne fournit *aucune sécurité* et autorise tout le trafic en provenance de l'extérieur à circuler sur la totalité du réseau interne. Pour implémenter la sécurité sur le routeur pare-feu, utilisez des listes d'accès et des groupes d'accès, tel que décrit dans les prochaines sections.

Définition de listes d'accès de pare-feu

Les listes d'accès permettent de spécifier le trafic qui sera réellement accepté ou rejeté sur le réseau interne. Les groupes d'accès mettent en application les définitions de listes d'accès sur des interfaces spécifiques de routeur. Les listes d'accès peuvent être exploitées de deux façons :

- pour refuser les connexions qui comportent un risque pour la sécurité, ce qui autorise toutes les autres ;
- pour autoriser les connexions considérées comme acceptables, ce qui rejette toutes les autres.

Dans le cadre d'une implémentation de routeur pare-feu, la seconde méthode est la plus sûre. C'est celle que nous allons décrire.

Dans cette étude de cas, les messages électroniques et les news sont autorisés en entrée pour quelques hôtes seulement, et les services FTP, Telnet et rlogin sont acceptés uniquement pour les hôtes situés sur le sous-réseau protégé par pare-feu. Les listes d'accès IP étendues (allant de 100 à 199) et les numéros de ports TCP ou UDP sont employés pour filtrer le trafic. Lorsqu'une connexion doit être établie pour la messagerie électronique, Telnet, FTP ou autre, elle tentera d'ouvrir un service sur un numéro de port spécifié. Par conséquent, vous pouvez filtrer des types de connexions spécifiques en refusant les paquets qui tentent d'utiliser le service correspondant.

Souvenez-vous qu'une liste d'accès est invoquée après une décision de routage, mais avant que le paquet ne soit envoyé vers une interface. Pour définir une liste d'accès, vous pouvez utiliser votre éditeur de texte favori, par exemple Notepad. Vous pouvez créer un fichier qui contiendra les commandes `access-list`, puis les copier directement sur le routeur, dans le mode de configuration.

Il est préférable de supprimer toute instance d'une ancienne liste d'accès, avant de charger une liste nouvelle ou modifiée. Les listes d'accès peuvent être supprimées au moyen de la commande suivante, dans le mode de configuration :

```
no access-list 101
```

La commande `access-list` peut à présent être utilisée pour autoriser n'importe quel paquet provenant de machines déjà connectées. Avec le mot clé `established`, une correspondance a lieu si le bit d'acquittement (ACK) ou de réinitialisation (RST) du datagramme IP est activé :

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255  
established
```

Si des routeurs pare-feu partagent un même réseau avec un fournisseur extérieur, vous souhaiterez sans doute donner à ces hôtes l'accès à votre réseau. Dans cette étude de cas, le fournisseur extérieur dispose d'un port série, qui utilise l'adresse de classe B du routeur pare-feu (152.50.14.2) en tant qu'adresse source. Votre instruction de liste d'accès autorisant ces hôtes serait donc celle-ci :

```
access-list 101 permit ip 152.50.14.2 0.0.0.0 0.0.0.0 255.255.255.255
```

L'exemple suivant illustre comment refuser l'accès à un utilisateur qui tente d'usurper l'une de vos adresses internes à partir de l'extérieur :

```
access-list 101 deny ip 152.50.0.0 0.0.255.255 0.0.0.0 255.255.255.255
```

Les exemples de listes d'accès suivants se fondent sur de nombreux numéros de ports connus (*well-known*) ou utilisés par défaut avec la pile de protocoles TCP/IP. Reportez-vous au Tableau 22.6, plus loin dans cette étude de cas, afin d'obtenir la liste de certains de ces numéros de ports.

NOTE

Le port 111 est uniquement un service d'annuaire. Lorsque vous parvenez à découvrir sur quels ports les véritables services de données sont exécutés, vous pouvez y accéder. La plupart des services RPC n'utilisent pas de numéro de port fixe. Vous devez rechercher les ports sur lesquels ces services sont assurés, et les bloquer. Malheureusement, comme les ports peuvent être liés à n'importe quel niveau, Cisco recommande de bloquer tous les ports UDP, excepté DNS, lorsque c'est possible.

Cisco recommande également de filtrer le service TCP finger sur le port 79, afin d'empêcher des intrus d'obtenir des informations sur les répertoires d'utilisateurs internes et le nom des hôtes à partir desquels les utilisateurs ouvrent des sessions.

Les deux commandes access-list suivantes autorisent les requêtes et réponses DNS (port 53) et NTP (port 123) en fonction de leur adresse de port TCP/IP :

```
access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 53  
access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123
```

La commande suivante rejette le port UDP du serveur NFS (*Network File Server*) :

```
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2049
```

Les commandes suivantes rejettent OpenWindows sur les ports 2001 et 2002, et X11 sur les ports 6001 et 6002. Cela permet de protéger les deux premiers écrans sur n'importe quel hôte. Si une machine utilise plus de deux écrans, veillez à bloquer les ports appropriés :

```
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 6001  
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 6002  
  
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2001  
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2002
```

La commande suivante autorise quiconque à accéder au serveur de communication (152.50.13.2), *via Telnet* :

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.13.2 0.0.0.0 eq 23
```

Les commandes suivantes autorisent quiconque à accéder à l'hôte 152.50.13.100 sur le sous-réseau 152.50.13.0, *via FTP*:

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.13.100 0.0.0.0 eq 21  
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.13.100 0.0.0.0 eq 20
```

Dans les exemples suivants, le réseau 152.50.1.0 se trouve sur le réseau interne (voir Figure 22.11).

Les commandes access-list suivantes autorisent les connexions TCP et UDP sur les numéros de port supérieurs à 1023 pour un nombre d'hôtes très restreint. Vérifiez que cette liste ne comprend aucun serveur de communication ou traducteur de protocole :

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.13.100 0.0.0.0 gt 1023  
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.1.100 0.0.0.0 gt 1023  
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.1.101 0.0.0.0 gt 1023  
access-list 101 permit udp 0.0.0.0 255.255.255.255 152.50.13.100 0.0.0.0 gt 1023  
access-list 101 permit udp 0.0.0.0 255.255.255.255 152.50.1.100 0.0.0.0 gt 1023  
access-list 101 permit udp 0.0.0.0 255.255.255.255 152.50.1.101 0.0.0.0 gt 1023
```

Les commandes access-list suivantes autorisent un accès DNS aux serveurs DNS répertoriés par le NIC (*Network Information Center*) :

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.13.100 0.0.0.0 eq 53
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.1.100 0.0.0.0 eq 53
```

Les commandes suivantes autorisent les messages électroniques SMTP entrants pour quelques machines seulement :

```
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.13.100 0.0.0.0 eq 25
access-list 101 permit tcp 0.0.0.0 255.255.255.255 152.50.1.100 0.0.0.0 eq 25
```

Les commandes suivantes autorisent les serveurs de news NNTP (*Network News Transfer Protocol*) internes à recevoir des connexions NNTP en provenance d'une liste d'homologues autorisés :

```
access-list 101 permit tcp 56.1.0.18 0.0.0.1 152.50.1.100 0.0.0.0 eq 119
access-list 101 permit tcp 182.12.18.32 0.0.0.0 152.50.1.100 0.0.0.0 eq 119
```

La commande suivante autorise l'envoi de messages d'erreurs ICMP (*Internet Control Message Protocol*) :

```
access-list 101 permit icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Chaque liste d'accès inclut une instruction implicite de rejet de tout le trafic (c'est-à-dire, qu'elle rejette tout ce qui n'est pas mentionné) en fin de liste pour s'assurer que les paramètres qui ne sont pas expressément autorisés soient refusés. Voici à quoi ressemblerait une liste d'accès complète :

```
access-list 101 permit udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 123
access-list 101 deny udp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2049
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 6001
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 6002
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2001
access-list 101 deny tcp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255 eq 2002
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.13.2 0.0.0.0 eq 23
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.13.100 0.0.0.0 eq 21
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.13.100 0.0.0.0 eq 20
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.13.100 0.0.0.0 gt 1023
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.1.100 0.0.0.0 gt 1023
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.1.101 0.0.0.0 gt 1023
access-list 101 permit udp 0.0.0.0 255.255.255.255 150.50.13.100 0.0.0.0 gt 1023
access-list 101 permit udp 0.0.0.0 255.255.255.255 150.50.1.100 0.0.0.0 gt 1023
access-list 101 permit udp 0.0.0.0 255.255.255.255 150.50.1.101 0.0.0.0 gt 1023
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.13.100 0.0.0.0 eq 53
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.1.100 0.0.0.0 eq 53
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.13.100 0.0.0.0 eq 25
access-list 101 permit tcp 0.0.0.0 255.255.255.255 150.50.1.100 0.0.0.0 eq 25
access-list 101 permit tcp 56.1.0.18 0.0.0.0 150.50.1.100 0.0.0.0 eq 119
access-list 101 permit tcp 182.12.18.32 0.0.0.0 150.50.1.100 0.0.0.0 eq 119
access-list 101 permit icmp 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Application de listes d'accès sur des interfaces

Une fois que cette liste d'accès a été chargée sur le routeur et stockée en mémoire NVRAM (*NonVolatile Random Access Memory*), il faut l'assigner à l'interface qui convient. Dans cette étude de cas, le trafic en provenance de l'extérieur, via l'interface série 0 du pare-feu, est filtré (au moyen de la liste d'accès 101) avant d'être placé sur le sous-réseau 152.50.13.0 (Ethernet 0).

Par conséquent, la commande `access-group`, qui applique une liste d'accès pour filtrer les connexions entrantes, doit être assignée à l'interface Ethernet 0, de la façon suivante :

```
interface ethernet 0
 ip access-group 101 in
```

Pour contrôler l'accès à l'Internet à partir du réseau interne, définissez une liste d'accès, et appliquez-la aux paquets sortants sur l'interface série 0 du routeur pare-feu. Pour cela, les paquets en retour en provenance des hôtes qui utilisent Telnet ou FTP doivent être autorisés à accéder au sous-réseau pare-feu 152.50.13.0.

Configuration du serveur de communication pare-feu

Dans cette étude de cas, le serveur de communication pare-feu dispose d'un seul modem en entrée sur la ligne 2 :

```
interface Ethernet0
 ip address 152.50.13.2 255.255.255.0
!
access-list 10 deny 152.50.14.0 0.0.0.255
access-list 10 permit 152.50.0.0 0.0.255.255
!
access-list 11 deny 152.50.13.2 0.0.0.0
access-list 11 permit 152.50.0.0 0.0.255.255
!
line 2
login tacacs
location FirewallCS#2
!
access-class 10 in
access-class 11 out
!
modem answer-timeout 60
modem InOut
telnet transparent
terminal-type dialup
flowcontrol hardware
stopbits 1
rxspeed 38400
txspeed 38400
!
tacacs-server host 152.50.1.100
tacacs-server host 152.50.1.101
tacacs-server extended
!
line vty 0 15
login tacacs
```

Définition de listes d'accès sur le serveur de communication

Dans cet exemple, l'adresse de réseau est utilisée pour autoriser ou refuser l'accès. Par conséquent, des numéros de listes d'accès IP standards (de 1 à 99) sont employés. Pour les connexions entrantes sur des lignes de modem, seuls les paquets des hôtes du réseau interne de Classe B, et ceux des hôtes sur le sous-réseau pare-feu sont acceptés :

```
access-list 10 deny 152.50.14.0 0.0.0.255
access-list 10 permit 152.50.0.0 0.0.255.255
```

Les connexions sortantes sont autorisées uniquement pour les hôtes des réseaux internes et le serveur de communication. Cela permet d'éviter qu'une ligne de modem extérieure appelle vers l'extérieur à partir d'une seconde ligne de modem :

```
access-list 11 deny 152.50.13.2 0.0.0.0
access-list 11 permit 152.50.0.0 0.0.255.255
```

Application de listes d'accès sur des lignes

Vous pouvez appliquer une liste d'accès sur une ligne asynchrone à l'aide de la commande `access-class`. Dans cette étude de cas, les restrictions de la liste d'accès 10 sont appliquées aux connexions entrantes sur la ligne 2, et celles de la liste 11 sont appliquées aux connexions sortantes sur la ligne 2 :

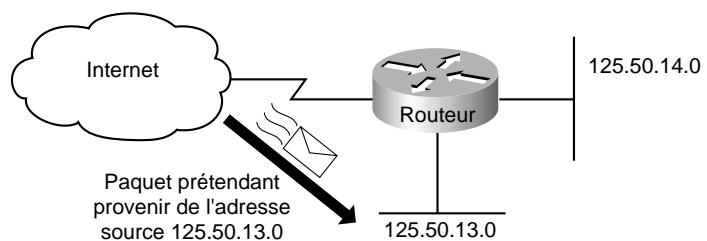
```
access-class 10 in
access-class 11 out
```

Listes d'accès en entrée et usurpation d'adresse (spoofing)

Dans System Software 9.21, Cisco a introduit la possibilité d'assigner des listes d'accès en entrée à une interface, ce qui permet à un administrateur réseau de filtrer les paquets avant qu'ils ne pénètrent sur le routeur, plutôt qu'à leur sortie. Dans la plupart des cas, les listes d'accès en entrée et en sortie accomplissent les mêmes fonctionnalités. Néanmoins, les listes en entrée sont plus intuitives pour certaines personnes, et peuvent être utilisées afin d'empêcher certains types d'usurpations d'adresses IP là où les listes en sortie ne fournissent pas suffisamment de sécurité.

La Figure 22.12 illustre le cas d'un cyber-pirate qui usurpe l'adresse d'un autre hôte, c'est-à-dire qui prétend posséder une adresse qui n'est pas la sienne. Il prétend que son trafic provient du réseau 152.50.13.0. Bien que cette adresse IP soit usurpée, l'interface du routeur avec l'extérieur suppose que le paquet provient de cette adresse source. Si la liste d'accès en entrée sur le routeur autorise le trafic provenant de ce réseau, le paquet illégal sera autorisé.

Figure 22.12
Exemple d'usurpation d'adresse.



Pour éviter l'usurpation d'adresse, une liste d'accès sera appliquée en entrée sur l'interface du routeur avec l'extérieur. Cette liste rejette tous les paquets dont l'adresse provient de réseaux internes, et que le routeur connaît (13.0 et 14.0).

ATTENTION

Si plusieurs réseaux internes sont connectés au routeur pare-feu, et que ce dernier utilise des filtres en sortie, le trafic entre ces réseaux subira une baisse des performances provoquée par les filtres de listes d'accès. Pour se prémunir de cette dégradation des performances sur les réseaux internes, il faut implémenter des filtres en entrée sur l'interface du routeur avec l'extérieur uniquement.

Si une adresse utilise le routage par la source, elle peut envoyer et recevoir du trafic *via* le routeur pare-feu. Pour cette raison, il est recommandé de toujours désactiver le routage par la source sur les routeurs pare-feu, à l'aide de la commande `no ip source-route`.

Assignation de numéros de ports

Chaque application qui est censée recevoir des données de la part d'un réseau TCP/IP appelle le service TCP/IP pour se voir attribuer un *port*, c'est-à-dire un numéro de 16 bits unique, pour cette application, sur cet hôte particulier. Tout datagramme entrant correctement structuré, qui contient ce numéro de port dans son en-tête TCP ou UDP, est transmis à l'application en question. Dans le cas de datagrammes fragmentés, seul le premier datagramme contient des informations de port (fragment 0). Par convention, n'importe quelle application communicante possède également un numéro de port sur son hôte, qu'elle inclut dans le champ de port de destination des datagrammes qu'elle envoie. Les numéros de port sont répartis sur trois plages, comme suit :

- ports connus (*well-known*) [utilisés par défaut] : plage 0-1023 ;
- ports enregistrés : plage 1024-49151 ;
- ports dynamiques et/ou privés : plage 49152-65535.

Les ports réservés sont contrôlés et assignés par l'IANA (*Internet Assigned Numbers Authority*). Sur la plupart des systèmes, seuls les processus système (ou root) ou les programmes exécutés par des utilisateurs privilégiés peuvent utiliser ces ports. Ils sont utilisés par TCP (RFC 793) pour désigner les extrémités de connexions logiques qui transportent des conversations longues. Afin de fournir des services à des appelants inconnus, un port de contact de service est défini. Cette liste spécifie le port utilisé en tant que port de contact par le processus serveur. Le Tableau 22.6 répertorie certains des numéros de ports réservés.

Tableau 22.6 : Assignation des numéros de ports

<i>Numéro de port</i>	<i>Type de port</i>	<i>Protocole</i>
0	TCP et UDP	Réservé
1-4	TCP et UDP	Non assignés
5	TCP et UDP	Remote Job Entry
7	TCP et UDP	Echo
9	TCP et UDP	Discard
11	TCP et UDP	Active Users
13	TCP et UDP	Daytime

Tableau 22.6 : Assiguation des numéros de ports (*suite*)

<i>Numéro de port</i>	<i>Type de port</i>	<i>Protocole</i>
15	TCP et UDP	Who is up ou Netstat
17	TCP et UDP	Quote of the Day
19	TCP et UDP	Character Generator
20	TCP et UDP	File Transfer (par défaut, Data)
21	TCP et UDP	File Transfer (Contrôle)
23	TCP et UDP	Telnet
25	TCP et UDP	Simple Mail Transfer Protocol (SMTP)
37	TCP et UDP	Time
39	TCP et UDP	Resource Location Protocol
42	TCP et UDP	Host Name Server
43	TCP et UDP	Who Is
49	TCP et UDP	Terminal Access Controller Access Control System (TACACS)
53	TCP et UDP	Domain Name Server
67	TCP et UDP	Bootstrap Protocol Server
68	TCP et UDP	Bootstrap Protocol Client
69	TCP et UDP	Trivial File Transfer Protocol
70	TCP et UDP	Gopher
75	TCP et UDP	N'importe quel service privé de connexion à distance sortante
77	TCP et UDP	N'importe quel service RJE
79	TCP et UDP	Finger
80	TCP et UDP	Hypertext Transfer Protocol (HTTP)
87	TCP	Link (habituellement utilisé par les intrus)
88	TCP et UDP	Kerberos
89	TCP et UDP	Open Shortest Path First
95	TCP	SUPDUP Protocol
101	TCP	NIC Host Name Server
102	TCP	ISO-TSAP
103	TCP	X400
104	TCP	X400-SND

Tableau 22.6 : Assигнation des numéros de ports (suite)

<i>Numéro de port</i>	<i>Type de port</i>	<i>Protocole</i>
107	TCP et UDP	Remote Telnet Service
109	TCP	Post Office Protocol v2
110	TCP	Post Office Protocol v3
111	TCP et UDP	SUN Remote Procedure Call
113	TCP et UDP	Authentication Service
117	TCP et UDP	UUCP Path Service
119	TCP et UDP	USENET Network News Transfer Protocol
123	TCP et UDP	Network Time Protocol (NTP)
133-136	TCP et UDP	Non assignés
137	UDP	NetBIOS Name Service
137	TCP	Non assigné
138	UDP	NetBIOS Datagram Service
138	TCP	Non assigné
139	UDP	NetBIOS Session Service
144	TCP	NeWS
161	TCP et UDP	Simple Network Management Protocol Q/R
162	TCP et UDP	SNMP Event Traps
177	UDP	X Display Manager Control Protocol
179	TCP et UDP	Border Gateway Protocol (BGP)
194	TCP et UDP	Internet Relay Chat
195	UDP	Audit de protocole de sécurité DNSIX
389	TCP et UDP	Lightweight Directory Access Protocol
434	UDP	Mobile IP Registration
512	TCP	UNIX rexec (Control)
513	TCP et UDP	UNIX rlogin
514	TCP et UDP	UNIX rsh et rcp, commandes à distance
514	TCP	System Logging
515	TCP	UNIX Line Printer Remote Spooling
517	TCP et UDP	Two User Interaction — talk

Tableau 22.6 : Assiguation des numéros de ports (suite)

<i>Numéro de port</i>	<i>Type de port</i>	<i>Protocole</i>
518	TCP et UDP	ntalk
520	UDP	Routing Information Protocol
525	UDP	Time Server
540	TCP	Demon UNIX-to-UNIX Copy Program
543	TCP	Kerberos login
544	TCP	Kerberos shell
1993	TCP	SNMP sur TCP
2000	TCP et UDP	Open Windows
2001		Port auxiliaire (AUX)
2049	UDP	Network File System (NFS)
4001		Port auxiliaire (AUX), flux
6000	TCP et UDP	X11 (X Windows)

Suggestions de lectures

Cette section propose une liste de publications relatives à la sécurité sur les réseaux.

Livres et périodiques

- Cheswick B. et Bellovin S. *Firewalls and Internet Security*. Reading, MA: Addison-Wesley, 1994.
- Comer D.E. et Stevens D.L. *Internetworking with TCP/IP*. Volumes I-III. Englewood Cliffs, NJ: Prentice Hall, 1991-1993.
- Curry D. *UNIX System Security — A Guide for Users and System Administrators*, 1992.
- Garfinkel et Spafford. *Practical UNIX and Internet Security*. Cambridge, MA: O'Reilly & Associates, 1996.
- Quarterman J. et Carl-Mitchell S. *The Internet Connection*. Reading, MA: Addison-Wesley, 1994.
- Ranum M.J. *Thinking about Firewalls*. Santa Clara, CA: Trusted Information Systems, Inc.
- Stoll C. *The Cuckoo's Egg*. New York, NY: Doubleday, 1995.
- Thomas Thomas M. II. *OSPF Network Design Solutions*. Indianapolis, IN: Cisco Press, 1998.
- Treese G. W. et Wolman A. *X through the Firewall and Other Application Relays*.

RFC (Requests For Comments)

- RFC 1118. *The Hitchhiker's Guide to the Internet*, septembre 1989.
- RFC 1175. *A Bibliography of Internetworking Information*, août 1990.

RFC1244. *Site Security Handbook*, juillet 1991.

RFC 1340. *Assigned Numbers*, juillet 1992.

RFC 1446. *Security Protocols for SNMPv2*, avril 1993.

RFC 1463. *FYI on Introducing the Internet — A Short Bibliography of Introductory Internetworking Readings for the Network Novice*, mai 1993.

RFC 1492. *An Access Control Protocol, Sometimes Called TACACS*, juillet 1993.

Sites Internet

Certaines références peuvent être consultées sur les sites suivants :

- Documents, sur le site gopher.nist.gov.
- *Computer Underground Digest*, sur le site [site ftp.eff.org](http://ftp.eff.org) (répertoire /pub/cud).
- Documents, sur le site research.att.com (répertoire /dist/internet_security).

Résumé

Ce chapitre a donné un aperçu des menaces internes et externes qui pèsent sur la sécurité des réseaux et a fourni des recommandations relatives au développement d'une politique de sécurité permettant de s'en protéger. Il a également couvert l'implémentation de cette sécurité sur les équipements Cisco, à l'aide de listes d'accès et d'autres méthodes. Pour finir, il a présenté deux études de cas sur l'implémentation de la sécurité.

HSRP pour un routage IP avec tolérance aux pannes

Cette étude de cas examine le protocole HSRP (*Hot Standby Routing Protocol*) de Cisco. Ce protocole assure le secours automatique de routeurs lorsqu'il est configuré sur des routeurs Cisco qui exécutent le protocole IP (*Internet Protocol*) sur des réseaux locaux Ethernet, FDDI (*Fiber Distributed Data Interface*) ou Token Ring. HSRP est compatible avec IPX (*Internetwork Packet Exchange*), AppleTalk et Banyan VINES, ainsi qu'avec DECnet et XNS (*Xerox Network Systems*) dans certaines configurations.

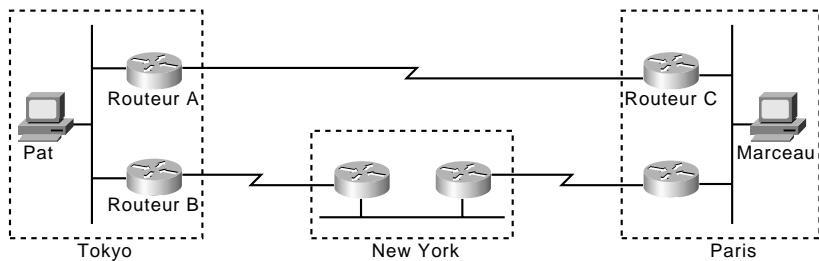
NOTE

Les clients Banyan VINES sans serveur ne réagissent pas bien aux changements de topologie (que HSRP soit configuré ou non). Cette étude de cas décrit les effets de tels changements sur des réseaux incluant les clients Banyan VINES sans serveur.

Pour IP, HSRP autorise un routeur à assumer automatiquement la fonction d'un autre routeur si celui-ci est défaillant. HSRP est particulièrement utile lorsque les utilisateurs sur un sous-réseau requièrent un accès continu aux ressources du réseau.

Examinez la Figure 23.1. Le routeur A gère les paquets entre le segment Tokyo et le segment Paris, et le routeur B gère les paquets entre le segment Tokyo et le segment New York. Si la connexion entre le routeur A et le routeur C devient impraticable, ou si l'un des deux routeurs est indisponible, les protocoles de routage à convergence rapide, comme Enhanced IGRP (*Enhanced Interior Gateway Routing Protocol*) ou OSPF (*Open Shortest Path First*), peuvent répondre en quelques secondes de façon que le routeur B soit prêt à transmettre les paquets qui auraient sinon été envoyés par le routeur A.

Figure 23.1
Un réseau WAN typique.



Néanmoins, en dépit de la convergence rapide, si la connexion entre le routeur A et le routeur C devient impraticable, ou si l'un des deux routeurs est indisponible, l'utilisateur Pat sur le segment Tokyo ne pourra probablement pas communiquer avec l'utilisateur Marceau, même après que les protocoles de routage ont convergé. La raison est que les hôtes IP, comme la station de travail de Pat, ne participent généralement pas au routage des protocoles. Au lieu de cela, ils sont configurés de façon statique avec l'adresse d'un seul routeur, tel le routeur A. Tant que la configuration de l'hôte de Pat n'est pas modifiée manuellement pour utiliser l'adresse du routeur B à la place de celle du routeur A, Pat ne peut pas communiquer avec Marceau.

Certains hôtes IP utilisent le protocole ARP (*Address Resolution Protocol*) pour sélectionner un routeur. Si la station de travail de Pat exécutait un proxy ARP, elle enverrait une requête ARP pour l'adresse de la station de Marceau. Le routeur A répondrait de la part de la station de Marceau et donnerait à la station de Pat sa propre adresse MAC (*Media Access Control*) à la place de l'adresse IP de la station de Marceau. Avec un proxy ARP, la station de Pat se comporte comme si la station de Marceau était connectée sur le même segment qu'elle. Si le routeur A tombe en panne, la station de Pat continuera à envoyer des paquets à destination de la station de Marceau vers l'adresse MAC du routeur A, même si ces paquets ne peuvent aller nulle part et sont perdus. Pat attend que ARP prenne connaissance de l'adresse MAC du routeur B en envoyant une autre requête ARP, ou bien redémarre la station pour l'obliger à envoyer une requête ARP. Dans les deux cas, Pat ne peut pas communiquer avec Marceau pendant un laps de temps donné, même si les protocoles de routage ont convergé et que le routeur B prêt à envoyer les paquets qui, sinon, auraient été transmis par le routeur A.

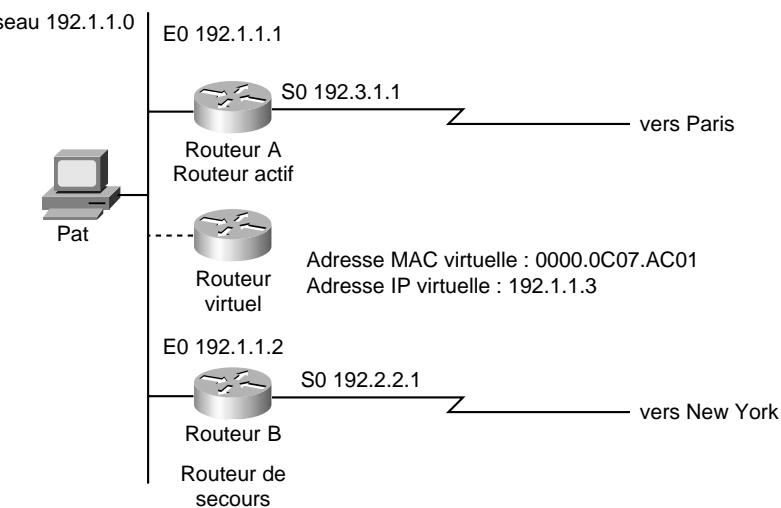
Certains hôtes IP utilisent le protocole RIP (*Routing Information Protocol*) pour découvrir les routeurs. L'inconvénient de RIP est qu'il s'adapte lentement aux changements de topologie. Si la station de Pat est configurée pour utiliser RIP, il faudra attendre de 3 à 10 minutes avant que RIP ne trouve un autre routeur disponible.

Certains hôtes IP plus récents utilisent le protocole IRDP (*ICMP Router Discovery Protocol*) pour trouver un nouveau routeur lorsqu'un itinéraire devient impraticable. Un hôte qui exécute IRDP écoute les messages multicast Hello provenant de son routeur configuré, et utilise une route alternative lorsqu'il ne reçoit plus de messages Hello. Si la station de Pat utilisait IRDP, elle s'apercevrait que le routeur A n'envoie plus de messages Hello, et commencerait à envoyer ses paquets vers le routeur B.

Pour les hôtes IP qui ne supportent pas IRDP, HSRP de Cisco permet de maintenir la communication lorsqu'un routeur devient indisponible. HSRP autorise un ou plusieurs routeurs configurés pour HSRP à utiliser l'adresse MAC et l'adresse IP d'un routeur virtuel. Ce routeur est virtuel, il

n'existe pas physiquement, mais il représente la cible commune pour les routeurs configurés pour se secourir les uns les autres. La Figure 23.2 illustre le segment Tokyo du WAN configuré pour HSRP. Chaque routeur véritable est configuré avec l'adresse MAC et l'adresse IP du routeur virtuel.

Figure 23.2
Adressage HSRP sur
le segment Tokyo.



Dans l'exemple de la Figure 23.2, l'adresse MAC du routeur virtuel est 0000.0C07.AC01. Lorsque vous configurez HSRP, le routeur sélectionne automatiquement l'une des adresses MAC virtuelles du bloc d'adresses du logiciel Cisco IOS. Les réseaux locaux Ethernet et FDDI utilisent comme adresse MAC virtuelle, une des adresses préassignées, et les réseaux locaux Token Ring utilisent une adresse fonctionnelle.

Ainsi les hôtes du réseau 192.1.1.0 avec l'adresse IP du routeur A, ils sont configurés avec l'adresse IP du routeur virtuel, qui devient leur routeur par défaut. Lorsque la station de Pat envoie des paquets à la station de Marceau sur le segment Paris, il les envoie en fait vers l'adresse MAC du routeur virtuel.

Le routeur A est configuré comme routeur actif, avec l'adresse IP et l'adresse MAC du routeur virtuel. Il envoie tous les paquets adressés à ce routeur vers l'interface 1 du segment Paris. En tant que routeur De secours, le routeur B est également configuré avec l'adresse IP et l'adresse MAC du routeur virtuel. Si, pour une raison quelconque, le routeur A cesse de transmettre des paquets, le protocole de routage converge, et le routeur B prend en charge les fonctions du routeur A en devenant le routeur actif. C'est-à-dire que le routeur B répond à l'adresse IP virtuelle et à l'adresse MAC virtuelle. La station de Pat continue à utiliser l'adresse IP du routeur virtuel pour envoyer des paquets destinés à la station de Marceau. Le routeur B reçoit et envoie ces paquets vers le segment Paris *via* le segment New York. Tant que le routeur A n'est pas redevenu actif, HSRP autorise le routeur B à fournir un service continu aux utilisateurs du segment Tokyo qui ont besoin de communiquer avec des utilisateurs du segment Paris. Pendant qu'il est actif, le routeur B continue à assurer ses fonctions habituelles, c'est-à-dire la gestion des paquets entre le segment Tokyo et le segment New York.

HSRP fonctionne aussi lorsque les hôtes sont configurés pour proxy ARP. Lorsque le routeur HSRP actif reçoit une requête ARP pour un hôte qui ne se trouve pas sur le réseau local, il envoie en réponse l'adresse MAC du routeur virtuel. Si le routeur actif devient indisponible, ou si sa connexion vers le LAN distant n'est plus exploitable, le routeur qui devient le routeur actif reçoit les paquets adressés au routeur virtuel et les transmet tel qu'il est prévu.

NOTE

Vous pouvez configurer HSRP sur n'importe quel routeur Cisco sur lequel tourne le système Cisco IOS version 10.0 ou ultérieure. Si vous le configurez sur un réseau Token Ring, tous les routeurs Cisco sur ce LAN doivent exécuter une version 10.0 ou ultérieure. Les versions 10.2(9), 10.3(6) et 11.0(2) permettent des réponses aux requêtes PING avec les adresses IP de secours. La version 11.0(3)(1) fournit un support amélioré pour l'emploi d'adresses IP secondaires avec HSRP.

Fonctionnement de HSRP

HSRP implémente un schéma de priorité pour déterminer quel routeur configuré pour HSRP doit être le routeur actif par défaut. Pour configurer un routeur comme routeur actif, vous devez lui assigner une priorité supérieure à celle des autres routeurs HSRP. La priorité par défaut est de 100. Par conséquent, si vous configurez un seul routeur avec la plus haute priorité, il sera le routeur actif par défaut.

HSRP fonctionne en échangeant des messages multicast qui annoncent les priorités des routeurs HSRP. Lorsque le routeur actif manque d'envoyer un message Hello dans un intervalle de temps configurable, le routeur De secours possédant la plus haute priorité devient le routeur actif. La passation des fonctions de transmission de paquets d'un routeur à un autre est complètement transparente pour tous les hôtes du réseau.

Les routeurs configurés pour HSRP échangent trois types de messages multicast :

- **Hello.** Le message Hello communique aux autres routeurs HSRP le niveau de priorité et les informations d'état du routeur.
- **Coup.** Lorsqu'un routeur De secours assure les fonctions du routeur actif, il envoie un message Coup.
- **Resign.** Un routeur actif envoie ce message lorsqu'il est sur le point de s'arrêter, ou quand un routeur Doté d'une priorité plus haute envoie un message Hello.

A n'importe quel moment, les routeurs HSRP peuvent se trouver dans l'un des états suivants :

- **Actif.** Le routeur assure des fonctions de transmission de paquets.
- **Secours.** Le routeur est prêt à assurer les fonctions de transmission de paquets en cas de défaillance du routeur actif.
- **Emission et écoute.** Le routeur envoie et reçoit des messages Hello.
- **Ecoute.** Le routeur reçoit des messages Hello.

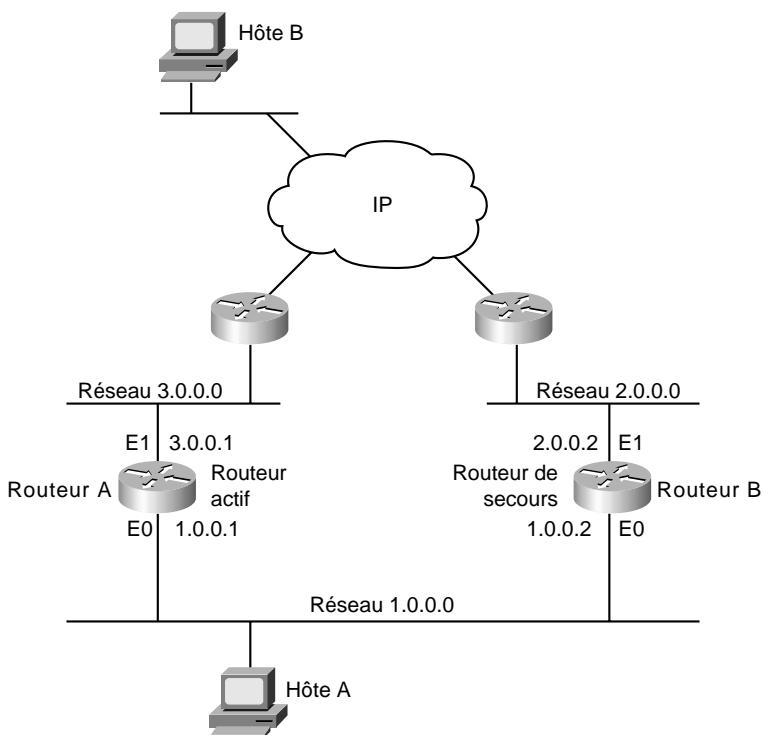
NOTE

Lorsqu'il est configuré sur les routeurs AG, AGS+ et Cisco 7000, HSRP tire parti de fonctionnalités matérielles spéciales qui ne sont pas disponibles sur les autres routeurs Cisco. Cela signifie que HSRP fonctionne de façon légèrement différente sur ces routeurs. Pour obtenir un exemple, voyez la section "Interaction de HSRP avec des protocoles routés", plus bas dans ce chapitre.

Configuration de HSRP

La Figure 23.3 illustre la topologie d'un réseau IP sur lequel deux routeurs sont configurés pour HSRP.

Figure 23.3
Exemple d'un réseau configuré pour HSRP.



Tous les hôtes du réseau sont configurés pour utiliser l'adresse IP du routeur virtuel (dans ce cas, 1.0.0.3) comme passerelle par défaut. La commande de configuration de la passerelle par défaut dépend du système d'exploitation, de l'implémentation de TCP/IP, et de la configuration de l'hôte.

NOTE

La configuration présentée dans cette étude de cas utilise le protocole de routage EIGRP. HSRP peut être utilisé avec n'importe quel protocole de routage supporté par le logiciel Cisco IOS. Certaines configurations utilisant HSRP requièrent encore un protocole de routage pour converger lorsqu'un changement survient. Le routeur De secours devient actif, mais la connectivité n'est pas établie tant que le protocole de routage n'a pas convergé.

Voici la configuration du routeur A :

```
hostname RouterA
!
interface ethernet 0
ip address 1.0.0.1 255.0.0.0
standby 1 ip 1.0.0.3
standby 1 preempt
standby 1 priority 110
standby 1 authentication denmark
standby 1 timers 5 15
!
interface ethernet 1
ip address 3.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 3.0.0.0
```

Voici la configuration du routeur B :

```
hostname RouterB
!
interface ethernet 0
ip address 1.0.0.2 255.0.0.0
standby 1 ip 1.0.0.3
standby 1 preempt
standby 1 authentication denmark
standby 1 timers 5 15
!
interface ethernet 1
ip address 2.0.0.2 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 2.0.0.0
```

La commande de configuration d'interface **standby ip** active HSRP et spécifie l'adresse 1.0.0.3 comme étant l'adresse IP du routeur virtuel. Les configurations des deux routeurs incluent cette commande afin qu'ils puissent partager la même adresse IP virtuelle. Le "1" spécifie le groupe de secours Hot Standby 1. Si vous ne spécifiez pas de numéro de groupe, il sera de 0 par défaut. La configuration d'au moins un routeur Dans le groupe doit spécifier l'adresse IP du routeur virtuel ; cette spécification est optionnelle pour les autres routeurs du groupe.

La commande de configuration d'interface **standby preempt** permet au routeur De devenir actif lorsque sa priorité est plus haute que celle d'autres routeurs HSRP dans le groupe de secours. Les configurations des deux routeurs incluent cette commande afin que chacun puisse être le routeur De

secours de l'autre. Le "1" indique que cette commande s'applique au groupe Hot Standby 1. Si vous n'utilisez pas cette commande dans la configuration d'un routeur, il ne pourra pas devenir actif.

La commande de configuration d'interface **standby priority** définit la priorité HSRP du routeur à 110, qui est supérieure à la priorité par défaut de 100. Seule la configuration du routeur A inclut cette commande, qui en fait le routeur actif. Le "1" indique que cette commande s'applique au groupe Hot Standby 1.

La commande de configuration d'interface **standby authentication** définit une chaîne d'authentification dont la valeur est une chaîne non cryptée de huit caractères incorporée dans chaque message multicast HSRP. Cette commande est optionnelle. Si vous choisissez de l'employer, chaque routeur HSRP dans le groupe devrait utiliser la même chaîne pour que chacun puisse authentifier la source des messages HSRP qu'il reçoit. Le "1" indique que cette commande s'applique au groupe Hot Standby 1.

La commande de configuration **standby timers** définit à 5 secondes l'intervalle entre chaque message Hello (appelé *temps hello*), et définit à 8 secondes le délai d'attente à l'issue duquel un routeur Déclare le routeur actif comme étant défaillant (appelé *temps de retenue* ou *hold time*). Les valeurs par défaut de ces intervalles sont respectivement 3 et 10. Si vous décidez de les modifier, vous devez configurer les deux routeurs pour qu'ils utilisent les mêmes valeurs. Le "1" indique que cette commande s'applique au groupe Hot Standby 1.

NOTE

Il peut y avoir jusqu'à 255 groupes Hot Standby sur un réseau local Ethernet ou FDDI, alors qu'un réseau local Token Ring n'en accepte pas plus de trois.

Configuration de groupes de secours Hot Standby

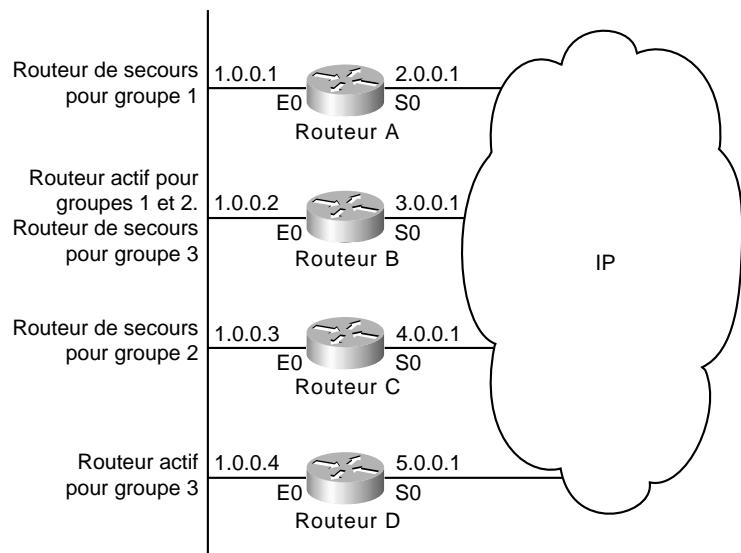
MHSRP (*Multigroup HSRP*) est une extension de HSRP qui permet à une interface de routeur D'appartenir à un ou plusieurs groupes de secours Hot Standby. MHSRP requiert l'utilisation de la version 10.3, ou plus, de Cisco IOS ; il est supporté uniquement sur les routeurs équipés d'un matériel spécial permettant d'associer une interface Ethernet à plusieurs adresses MAC unicast. Il s'agit des routeurs AGS et AGS+, et des routeurs de la série Cisco 7000 ou Cisco 7500. Ce matériel spécial vous permet de configurer une seule interface sur un routeur AGS, AGS+ ou Cisco 7000 de façon qu'il soit le routeur De secours pour plus d'un groupe Hot Standby (voir Figure 23.4).

A la Figure 23.4, l'interface Ethernet 0 du routeur A appartient au groupe 1, celle du routeur B aux groupes 1, 2 et 3, celle du routeur C au groupe 2 et celle du routeur D au groupe 3. Lorsque vous créez des groupes, vous pouvez les aligner sur la structure départementale de l'entreprise. Dans ce cas, le groupe 1 pourrait supporter le département Ingénierie, le groupe 2 le département Fabrication et le groupe 3 le département Finances.

Le routeur B est configuré comme routeur actif pour les groupes 1 et 2, et comme routeur De secours pour le groupe 3. Le routeur D est configuré comme routeur actif pour le groupe 3. Si le routeur D est victime d'une défaillance quelconque, le routeur B assurera alors les fonctions de transmission de paquets de ce routeur, et continuera à fournir aux utilisateurs du département Finances un accès aux données des autres sous-réseaux.

Figure 23.4

Exemple de groupes de secours Hot Standby.



Voici la configuration du routeur A :

```
hostname RouterA
!
interface ethernet 0
ip address 1.0.0.1 255.0.0.0
standby 1 ip 1.0.0.5
standby authentication sclara
!
interface serial 0
ip address 2.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 2.0.0.0
```

Voici la configuration du routeur B, qui doit être un routeur AGS, AGS+, Cisco 7000 ou Cisco 7500 :

```
hostname RouterB
!
interface ethernet 0
ip address 1.0.0.2 255.0.0.0
standby 1 ip 1.0.0.5
standby 1 priority 110
standby 1 preempt
standby 1 authentication sclara
standby 2 ip 1.0.0.6
standby 2 priority 110
standby 2 preempt
standby 2 authentication mtview
standby 3 ip 1.0.0.7
standby 3 preempt
standby 3 authentication svale
!
interface serial 0
```

```
ip address 3.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 3.0.0.0
```

Voici la configuration du routeur C :

```
hostname RouterC
!
interface ethernet 0
ip address 1.0.0.3 255.0 0.0
standby 2 ip 1.0.0.6
standby 2 preempt
standby 2 authentication mtview
!
interface serial 0
ip address 4.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 4.0.0.0
```

Voici la configuration du routeur D :

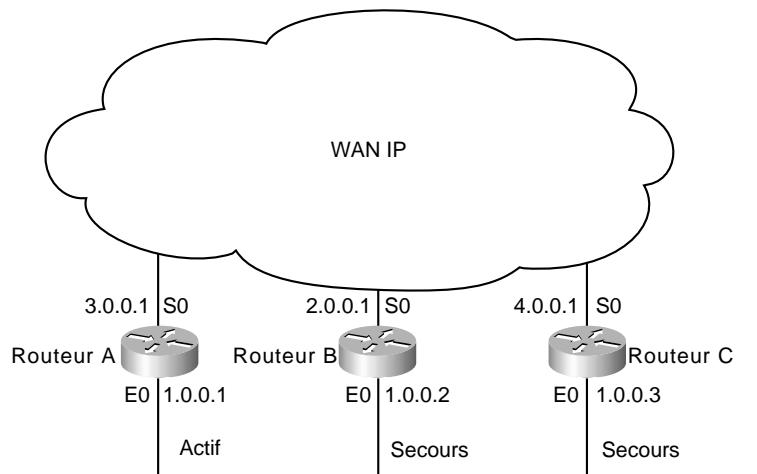
```
hostname RouterD
!
interface ethernet 0
ip address 1.0.0.4 255.0 0.0
standby 3 ip 1.0.0.7
standby 3 priority 110
standby 3 preempt
standby 3 authentication svale
!
interface serial 0
ip address 5.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 5.0.0.0
```

Suivi d'interface

Pour HSRP et MHSRP, vous disposez d'une fonction de suivi d'interface (*tracking*) permettant d'ajuster la priorité d'un routeur en fonction de la disponibilité de certaines de ses interfaces. Lorsqu'une interface qui est suivie devient indisponible, la priorité HSRP du routeur est réduite. Vous pouvez utiliser cette fonction pour limiter la probabilité qu'un routeur ne devienne actif alors que l'une de ses interfaces principales est indisponible. Pour configurer le suivi d'interface, utilisez la commande de configuration d'interface **standby track**. La Figure 23.5 illustre un réseau sur lequel cette fonction a été configurée.

Figure 23.5

Un réseau sur lequel le suivi d'interface a été configuré.



A la Figure 23.5, le routeur A est configuré comme routeur actif, et les routeurs B et C comme routeurs de secours. Voici la configuration du routeur A :

```

hostname RouterA
!
interface ethernet 0
ip address 1.0.0.1 255.0.0.0
standby 1 ip 1.0.0.4
standby 1 preempt
standby 1 priority 110
standby authentication microdot
!
interface serial 0
ip address 2.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 2.0.0.0
    
```

La commande de configuration d'interface **standby ip** active HSRP et définit l'adresse 1.0.0.4 comme étant l'adresse IP du routeur virtuel. Le "1" spécifie le groupe de secours Hot Standby 1. La commande de configuration d'interface **standby preempt** permet au routeur A de devenir actif lorsque sa priorité est supérieure à celle d'autres routeurs HSRP dans le groupe de secours.

La commande de configuration d'interface **standby priority** définit la priorité HSRP du routeur à 110, qui est la priorité la plus haute assignée dans notre exemple. Comme le routeur A possède la plus haute priorité, il est le routeur actif. Voici la configuration du routeur B :

```

hostname RouterB
!
interface ethernet 0
ip address 1.0.0.2 255.0.0.0
standby 1 ip 1.0.0.4
standby 1 preempt
standby 1 priority 105
standby track serial 0
    
```

```
standby 1 authentication microdot
interface serial 0
ip address 3.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 2.0.0.0
```

La commande de configuration d'interface **standby preempt** autorise le routeur B à devenir immédiatement le routeur actif si sa priorité est la plus haute, même avant que le routeur actif actuel ne soit défaillant. La commande de configuration d'interface **standby priority** définit la priorité du routeur à 105 (inférieure à celle du routeur A et supérieure à celle du routeur C) afin qu'il soit un routeur De secours.

Avec la commande de configuration d'interface **standby track**, l'interface Ethernet 0 réalise le suivi de l'interface série 0. Si l'interface série 0 devient indisponible, la priorité du routeur B est réduite de 10 (par défaut). Voici la configuration du routeur C :

```
hostname RouterC
!
interface ethernet 0
ip address 1.0.0.3 255.0.0.0
standby 1 ip 1.0.0.4
standby 1 preempt
standby 1 priority
standby track serial 0
standby 1 authentication microdot
!
interface serial 0
ip address 4.0.0.1 255.0.0.0
!
router eigrp 1
network 1.0.0.0
network 4.0.0.0
```

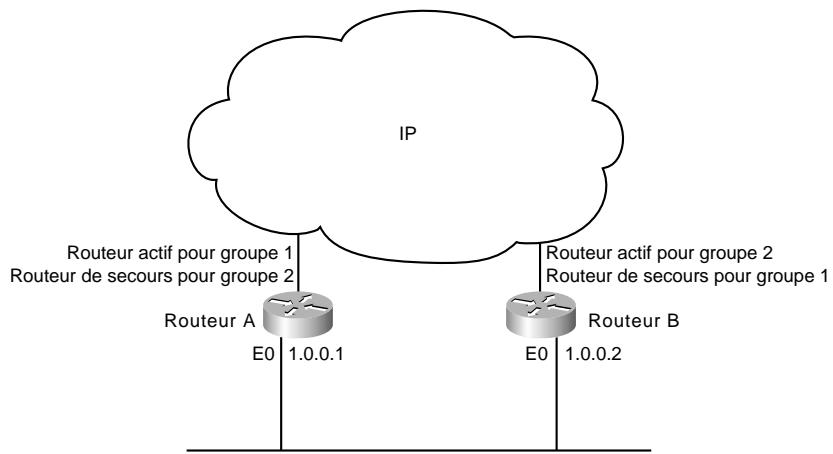
La commande de configuration d'interface **standby preempt** permet au routeur C de devenir actif si sa priorité est la plus haute en cas de défaillance du routeur actif. Puisque la commande de configuration d'interface **standby priority** ne spécifie aucune priorité, elle est par défaut de 100.

Si le routeur A est indisponible et que l'interface série 0 sur le routeur B soit disponible, ce dernier devient le routeur actif (avec sa priorité de 105). Toutefois, si l'interface série 0 sur le routeur B se trouve indisponible avant le routeur A, la priorité HSRP du routeur B passe de 105 à 95. Si le routeur A devient à son tour indisponible, le routeur C (dont la priorité est de 100) devient le routeur actif.

Equilibrage de charge

Vous pouvez utiliser HSRP ou MHSRP lorsque vous configurez l'équilibrage de charge. A la Figure 23.6, la moitié des stations de travail sur le réseau local est configurée pour le routeur A, et l'autre moitié des stations est configurée pour le routeur B.

Figure 23.6
Exemple de répartition
de la charge.



Voici une configuration partielle du routeur A :

```
hostname RouterA
!
interface ethernet 0
ip address 1.0.0.1 255.0.0.0
standby 1 ip 1.0.0.3
standby 1 priority 110
standby 1 preempt
standby 2 ip 1.0.0.4
standby 2 preempt
```

Voici une configuration partielle du routeur B :

```
hostname RouterB
!
interface ethernet 0
ip address 1.0.0.2 255.0.0.0
standby 1 ip 1.0.0.3
standby 1 preempt
standby 2 ip 1.0.0.4
standby 2 priority 110
standby 2 preempt
```

Ensemble, les fichiers de configuration pour les routeurs A et B établissent deux groupes de secours Hot Standby. Pour le groupe 1, le routeur A est le routeur actif par défaut, et le routeur B est le routeur De secours. Pour le groupe 2, le routeur B est le routeur actif par défaut, et le routeur A est le routeur De secours. En mode de fonctionnement normal, les deux routeurs se partagent la charge du trafic IP. Lorsque l'un d'eux devient indisponible, l'autre devient actif et assure les fonctions de transmission de paquets du routeur Défaillant. Les commandes de configuration d'interface **standby preempt** sont nécessaires en cas de défaillance d'un routeur pour que son rétablissement soit anticipé de manière à restaurer le partage de la charge.

Interaction de HSRP avec des protocoles routés

Cette section décrit l'interaction entre HSRP et les protocoles routés suivants :

- AppleTalk, Banyan VINES et Novell IPX ;
- DECnet et XNS.

AppleTalk, Banyan VINES et Novell IPX

Vous pouvez configurer HSRP sur des réseaux qui, en plus de IP, exécutent AppleTalk, Banyan VINES et Novell IPX. AppleTalk et Novell IPX continuent de fonctionner même lorsque le routeur De secours devient le routeur actif, mais ils mettent un certain temps à s'adapter au changement de topologie. En règle générale, les hôtes AppleTalk découvrent un nouveau routeur actif en moins de 30 secondes, les hôtes Novell 4.x ont besoin de 10 secondes ; les hôtes Novell 2.x et 3.x requièrent plus de temps pour s'adapter.

NOTE

Indépendamment du fait que HSRP soit configuré ou non, Banyan VINES ne réagit pas très efficacement aux changements de topologie. Lorsque HSRP est configuré, les conséquences d'un changement de topologie varient selon le type du routeur qui devient actif.

Lorsque le routeur actif devient indisponible, ou si sa connexion au réseau devient impraticable, toutes les sessions Banyan VINES qui reposent sur ce routeur sont arrêtées et doivent être réinitialisées. Si un routeur AGS, AGS+ ou Cisco 7000 devient le routeur actif, le trafic Banyan VINES circulant *via* ce routeur n'est pas affecté par la transition qu'il opère à partir de l'état de secours vers l'état actif. La raison est que ces routeurs sont équipés d'un matériel spécial qui leur permet de disposer de plusieurs adresses MAC à la fois. Si le routeur qui devient actif *n'est pas* de type AGS, AGS+ ou Cisco 7000, le trafic Banyan VINES passant par le routeur marque un temps d'arrêt et reprend après exactement 90 secondes pendant que le routeur change d'état.

Quel que soit le type du routeur qui devient actif, tout client sans serveur Banyan VINES qui obtient son adresse de couche réseau auprès de l'hôte indisponible devra redémarrer afin de se procurer une autre adresse de réseau.

DECnet et XNS

DECnet et XNS sont compatibles avec HSRP et MHSRP sur Ethernet, FDDI et Token Ring avec les routeurs Cisco 7000 et Cisco 7500. Certaines restrictions s'appliquent lorsque ces deux protocoles sont configurés sur d'autres routeurs, comme Cisco 2500, Cisco 3000, Cisco 4000 et Cisco 4500, qui ne disposent pas du matériel requis pour pouvoir supporter plusieurs adresses MAC. Le Tableau 23.1 identifie les combinaisons supportées.

Tableau 23.1 : Compatibilités HSRP et MHSRP avec DECnet et XNS

<i>Combinaison de protocoles par interface</i>	<i>Cisco 2500</i>	<i>Cisco 3000</i>	<i>Cisco 4000</i>	<i>Cisco 4500</i>	<i>Cisco 7000</i>	<i>Cisco 7500</i>
MHSRP avec ou sans DECnet ou XNS	Non	Non	Non	Non	Oui	Oui
HSRP sans DECnet ou XNS	Oui	Oui	Oui	Oui	Oui	Oui
HSRP avec DECnet ou XNS	Non	Non	Non	Non	Oui	Oui

Résumé

Les protocoles HSRP et MHSRP assurent un routage des paquets IP avec tolérance aux pannes sur les réseaux où tous les hôtes doivent pouvoir accéder en continu aux ressources sur tous les segments. Pour fournir une tolérance aux pannes, HSRP et MHSRP ont besoin d'un protocole qui converge rapidement, comme EIGRP. Un protocole à convergence rapide garantit une vitesse de propagation des informations d'état du routeur suffisamment rapide pour rendre transparente, pour les utilisateurs du réseau, la transition à partir de l'état de secours vers l'état actif.

III

Annexes

- | | |
|----------|---|
| A | <i>Segmentation d'un espace d'adresse IP</i> |
| B | <i>Implémentation de liaisons série IBM</i> |
| C | <i>Configuration d'hôte SNA pour des réseaux SRB</i> |
| D | <i>Configuration d'hôte SNA pour des réseaux SDLC</i> |
| E | <i>Diffusions broadcast sur des réseaux commutés</i> |
| F | <i>Réduction du trafic SAP sur les réseaux Novell IPX</i> |
| G | <i>Introduction au transport de la voix en paquets</i> |
| H | <i>Références et suggestions de lectures</i> |
| I | <i>Présentation de la technologie multicast IP</i> |

A

Segmentation d'un espace d'adresse IP

Cette annexe fournit une liste partielle d'une zone de Classe B devant être divisée en 500 zones OSPF (*Open Shortest Path First*) environ. Pour cet exemple, le réseau est supposé faire partie de la Classe B et posséder l'adresse 150.100.0.0.

NOTE

Bien qu'un réseau de 500 zones OSPF semble irréel, son utilisation pourra servir à illustrer la méthodologie générale employée pour segmenter un espace d'adresse OSPF.

Le Tableau A.1 ne présente que l'espace d'adresse pour deux des 512 zones. Ces zones sont définies avec l'adresse de base 150.100.2.0. L'illustration de la totalité de l'espace d'adresse pour ce réseau nécessiterait des centaines de pages supplémentaires d'informations d'adressage. Chaque zone demanderait le même nombre d'entrées que chacune des zones illustrées dans notre exemple.

Le Tableau A.1 illustre l'assignation de 255 adresses IP qui ont été partagées entre deux zones OSPF. Il montre également les frontières des sous-réseaux et les deux zones OSPF présentées (zone 8 et zone 17).

Pour notre démonstration, nous imaginerons un réseau qui nécessite que les liaisons série point-à-point dans chaque zone reçoivent un masque de sous-réseau autorisant deux hôtes par sous-réseau. Tous les autres sous-réseaux doivent recevoir chacun quatorze hôtes. Une segmentation au niveau bit et l'emploi de masques de sous-réseau de longueur variable (VLSM, *Variable Length Subnet Mask*) permettent de personnaliser l'espace d'adresse en facilitant la division en groupes plus petits qu'avec une segmentation au niveau octet. Le modèle d'adresse présenté dans le Tableau A.1 illustre une approche structurée pour assigner des adresses qui utilisent VLSM. Ce tableau présente deux sous-réseaux : 255.255.255.240 et 255.255.255.252. Le premier masque crée des espaces d'adresse de sous-réseau de quatre bits de long ; le second masque crée des espaces de deux bits.

En raison de l'assignation prudente des adresses, chaque zone peut être synthétisée avec une seule commande de configuration de routeur De zone **area** (utilisée pour définir la plage d'adresse). Le

premier ensemble d'adresses commençant par 150.100.2.0xxxxxx (dernier octet représenté ici en binaire) peut être synthétisé sur l'épine dorsale avec la commande suivante :

```
area 8 range 150.100.2.0 255.255.255.128
```

Cette commande assigne toutes les adresses de 150.100.2.0 à 150.100.2.127 à la zone 8. De la même manière, les adresses de 150.100.2.128 à 150.100.2.255 pour la deuxième zone peuvent être résumées avec la commande suivante :

```
area 17 range 150.100.2.128 255.255.255.128
```

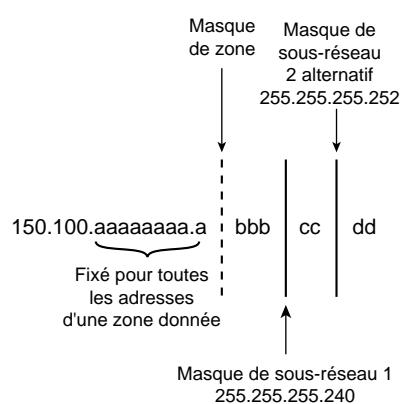
Cette commande assigne toutes les adresses de 150.100.2.128 à 150.100.2.255 à la zone 17.

L'assignation de sous-réseaux permet de définir la limite entre sous-réseau et hôte (au moyen d'un masque de sous-réseau) au sein de chaque zone. Notez dans cet exemple qu'il ne reste que 7 bits à utiliser en raison de la création du masque de zone artificiel. Les 9 bits sur la gauche du masque de zone font, en réalité, partie de la portion sous-réseau de l'adresse. En conservant ces 9 bits identiques pour toutes les adresses d'une zone donnée, la synthèse de routes est facilement réalisée sur les routeurs de frontières, comme l'illustre le modèle utilisé dans le Tableau A.1.

Le Tableau A.1 recense les sous-réseaux individuels, les adresses IP valides, les identifiants de sous-réseau et les adresses de broadcast. Cette méthode d'assignation d'adresses pour la portion VLSM de l'espace d'adresse garantit qu'il n'y a pas de chevauchement d'adresses. Si les exigences étaient différentes, les sous-réseaux les plus grands auraient pu être choisis et divisés en plages plus petites avec moins d'hôtes, ou combinés en plusieurs plages pour créer des sous-réseaux avec davantage d'hôtes.

L'approche utilisée dans cette annexe permet à la limite du masque de zone et aux masques de sous-réseaux d'être assignés à n'importe quel niveau de l'espace d'adresse, ce qui apporte une grande souplesse de conception. Un changement dans la spécification de la limite de masque de zone ou des masques de sous-réseaux peut être requis si un réseau grandit et dépasse sa conception initiale d'espace d'adresse. Dans le Tableau A.1, la limite de masque de zone se trouve à droite du bit le plus significatif du dernier octet de l'adresse (voir Figure A.1).

Figure A.1
Répartition des adresses assignées dans l'exemple.



Avec un masque de sous-réseau de 255.255.255.240, les bits *a* et *b* représentent ensemble la portion sous-réseau de l'adresse, alors que les bits *c* et *d* fournissent ensemble les identifiants d'hôtes de quatre bits. Avec un masque de sous-réseau de 255.255.255.252 (un masque typique pour des lignes série point-à-point), les bits *a*, *b* et *c* représentent ensemble la portion sous-réseau de l'adresse, et les bits *d* fournissent les identifiants d'hôtes de deux bits. Comme mentionné plus haut, l'objectif du masque de zone est de conserver tous les bits *a* constants dans une zone OSPF donnée (indépendante du masque de sous-réseau) pour que la synthèse de route soit facile à appliquer.

Les étapes suivantes décrivent la procédure utilisée pour allouer des adresses :

1. Déterminez le nombre de zones requises pour votre réseau OSPF. La valeur 500 a été utilisée dans cet exemple.
2. Créez une *limite de masque de zone* artificielle dans votre espace d'adresse. Notre exemple utilise 9 bits d'espace d'adresse de sous-réseau pour identifier les zones de façon unique. Comme $2^9=512$, 9 bits pour le sous-réseau répondent à notre besoin de création de 500 zones.
3. Déterminez le nombre de sous-réseaux requis dans chaque zone et le nombre maximal d'hôtes requis par sous-réseau. Cela vous permet de déterminer le placement des masques de sous-réseau. Dans le Tableau A.1, les exigences sont sept sous-réseaux avec quatorze hôtes chacun, et quatre sous-réseaux avec deux hôtes chacun.

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM

Adresse IP (décimale)	Portion sous-réseau du dernier octet (binaire)	Portion hôte du dernier octet (binaire)	Adresse de sous-réseau	Masque de sous-réseau	Notes
150.100.2.0	0000	0000	150.100.2.0	255.255.255.240	Identifiant de sous-réseau ; limite de zone ; la zone 8 commence
150.100.2.1	0000	0001	150.100.2.0	255.255.255.240	
150.100.2.2	0000	0010	150.100.2.0	255.255.255.240	
150.100.2.3	0000	0011	150.100.2.0	255.255.255.240	
150.100.2.4	0000	0100	150.100.2.0	255.255.255.240	
150.100.2.5	0000	0101	150.100.2.0	255.255.255.240	
150.100.2.6	0000	0110	150.100.2.0	255.255.255.240	
150.100.2.7	0000	0111	150.100.2.0	255.255.255.240	
150.100.2.8	0000	1000	150.100.2.0	255.255.255.240	
150.100.2.9	0000	1001	150.100.2.0	255.255.255.240	
150.100.2.10	0000	1010	150.100.2.0	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.11	0000	1011	150.100.2.0	255.255.255.240	
150.100.2.12	0000	1100	150.100.2.0	255.255.255.240	
150.100.2.13	0000	1101	150.100.2.0	255.255.255.240	
150.100.2.14	0000	1110	150.100.2.0	255.255.255.240	
150.100.2.15	0000	1111	150.100.2.0	255.255.255.240	Broadcast de sous-réseau
150.100.2.16	0001	0000	150.100.2.16	255.255.255.240	Identifiant de sous-réseau
150.100.2.17	0001	0001	150.100.2.16	255.255.255.240	
150.100.2.18	0001	0010	150.100.2.16	255.255.255.240	
150.100.2.19	0001	0011	150.100.2.16	255.255.255.240	
150.100.2.20	0001	0100	150.100.2.16	255.255.255.240	
150.100.2.21	0001	0101	150.100.2.16	255.255.255.240	
150.100.2.22	0001	0110	150.100.2.16	255.255.255.240	
150.100.2.23	0001	0111	150.100.2.16	255.255.255.240	
150.100.2.24	0001	1000	150.100.2.16	255.255.255.240	
150.100.2.25	0001	1001	150.100.2.16	255.255.255.240	
150.100.2.26	0001	1010	150.100.2.16	255.255.255.240	
150.100.2.27	0001	1011	150.100.2.16	255.255.255.240	
150.100.2.28	0001	1100	150.100.2.16	255.255.255.240	
150.100.2.29	0001	1101	150.100.2.16	255.255.255.240	
150.100.2.30	0001	1110	150.100.2.16	255.255.255.240	
150.100.2.31	0001	1111	150.100.2.16	255.255.255.240	Broadcast de sous-réseau
150.100.2.32	0010	0000	150.100.2.32	255.255.255.240	Identifiant de sous-réseau
150.100.2.33	0010	0001	150.100.2.32	255.255.255.240	
150.100.2.34	0010	0010	150.100.2.32	255.255.255.240	
150.100.2.35	0010	0011	150.100.2.32	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.36	0010	0100	150.100.2.32	255.255.255.240	
150.100.2.37	0010	0101	150.100.2.32	255.255.255.240	
150.100.2.38	0010	0110	150.100.2.32	255.255.255.240	
150.100.2.39	0010	0111	150.100.2.32	255.255.255.240	
150.100.2.40	0010	1000	150.100.2.32	255.255.255.240	
150.100.2.41	0010	1001	150.100.2.32	255.255.255.240	
150.100.2.42	0010	1010	150.100.2.32	255.255.255.240	
150.100.2.43	0010	1011	150.100.2.32	255.255.255.240	
150.100.2.44	0010	1100	150.100.2.32	255.255.255.240	
150.100.2.45	0010	1101	150.100.2.32	255.255.255.240	
150.100.2.46	0010	1110	150.100.2.32	255.255.255.240	
150.100.2.47	0010	1111	150.100.2.32	255.255.255.240	Broadcast de sous-réseau
150.100.2.48	0011	0000	150.100.2.48	255.255.255.240	Identifiant de sous-réseau
150.100.2.49	0011	0001	150.100.2.48	255.255.255.240	
150.100.2.50	0011	0010	150.100.2.48	255.255.255.240	
150.100.2.51	0011	0011	150.100.2.48	255.255.255.240	
150.100.2.52	0011	0100	150.100.2.48	255.255.255.240	
150.100.2.53	0011	0101	150.100.2.48	255.255.255.240	
150.100.2.54	0011	0110	150.100.2.48	255.255.255.240	
150.100.2.55	0011	0111	150.100.2.48	255.255.255.240	
150.100.2.56	0011	1000	150.100.2.48	255.255.255.240	
150.100.2.57	0011	1001	150.100.2.48	255.255.255.240	
150.100.2.58	0011	1010	150.100.2.48	255.255.255.240	
150.100.2.59	0011	1011	150.100.2.48	255.255.255.240	
150.100.2.60	0011	1100	150.100.2.48	255.255.255.240	
150.100.2.61	0011	1101	150.100.2.48	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.62	0011	1110	150.100.2.48	255.255.255.240	
150.100.2.63	0011	1111	150.100.2.48	255.255.255.240	Broadcast de sous-réseau
150.100.2.64	010000	00	150.100.2.64	255.255.255.252	Identifiant de sous-réseau
150.100.2.65	010000	01	150.100.2.64	255.255.255.252	
150.100.2.66	010000	10	150.100.2.64	255.255.255.252	
150.100.2.67	010000	11	150.100.2.64	255.255.255.252	Broadcast de sous-réseau
150.100.2.68	010001	00	150.100.2.68	255.255.255.252	Identifiant de sous-réseau
150.100.2.69	010001	01	150.100.2.68	255.255.255.252	
150.100.2.70	010001	10	150.100.2.68	255.255.255.252	
150.100.2.71	010001	11	150.100.2.68	255.255.255.252	Broadcast de sous-réseau
150.100.2.72	010010	00	150.100.2.72	255.255.255.252	Identifiant de sous-réseau
150.100.2.73	010010	01	150.100.2.72	255.255.255.252	
150.100.2.74	010010	10	150.100.2.72	255.255.255.252	
150.100.2.75	010010	11	150.100.2.72	255.255.255.252	Broadcast de sous-réseau
150.100.2.76	010011	00	150.100.2.76	255.255.255.252	Identifiant de sous-réseau
150.100.2.77	010011	01	150.100.2.76	255.255.255.252	
150.100.2.78	010011	10	150.100.2.76	255.255.255.252	
150.100.2.79	010011	11	150.100.2.76	255.255.255.252	Broadcast de sous-réseau
150.100.2.80	0101	0000	150.100.2.80	255.255.255.240	Identifiant de sous-réseau
150.100.2.81	0101	0001	150.100.2.80	255.255.255.240	
150.100.2.82	0101	0010	150.100.2.80	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.83	0101	0011	150.100.2.80	255.255.255.240	
150.100.2.84	0101	0100	150.100.2.80	255.255.255.240	
150.100.2.85	0101	0101	150.100.2.80	255.255.255.240	
150.100.2.86	0101	0110	150.100.2.80	255.255.255.240	
150.100.2.87	0101	0111	150.100.2.80	255.255.255.240	
150.100.2.88	0101	1000	150.100.2.80	255.255.255.240	
150.100.2.89	0101	1001	150.100.2.80	255.255.255.240	
150.100.2.90	0101	1010	150.100.2.80	255.255.255.240	
150.100.2.91	0101	1011	150.100.2.80	255.255.255.240	
150.100.2.92	0101	1100	150.100.2.80	255.255.255.240	
150.100.2.93	0101	1101	150.100.2.80	255.255.255.240	
150.100.2.94	0101	1110	150.100.2.80	255.255.255.240	
150.100.2.95	0101	1111	150.100.2.80	255.255.255.240	Broadcast de sous-réseau
150.100.2.96	0110	0000	150.100.2.96	255.255.255.240	Identifiant de sous-réseau
150.100.2.97	0110	0001	150.100.2.96	255.255.255.240	
150.100.2.98	0110	0010	150.100.2.96	255.255.255.240	
150.100.2.99	0110	0011	150.100.2.96	255.255.255.240	
150.100.2.100	0110	0100	150.100.2.96	255.255.255.240	
150.100.2.101	0110	0101	150.100.2.96	255.255.255.240	
150.100.2.102	0110	0110	150.100.2.96	255.255.255.240	
150.100.2.103	0110	0111	150.100.2.96	255.255.255.240	
150.100.2.104	0110	1000	150.100.2.96	255.255.255.240	
150.100.2.105	0110	1001	150.100.2.96	255.255.255.240	
150.100.2.106	0110	1010	150.100.2.96	255.255.255.240	
150.100.2.107	0110	1011	150.100.2.96	255.255.255.240	
150.100.2.108	0110	1100	150.100.2.96	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.109	0110	1101	150.100.2.96	255.255.255.240	
150.100.2.110	0110	1110	150.100.2.96	255.255.255.240	
150.100.2.111	0110	1111	150.100.2.96	255.255.255.240	Broadcast de sous-réseau
150.100.2.112	0111	0000	150.100.2.112	255.255.255.240	Identifiant de sous-réseau
150.100.2.113	0111	0001	150.100.2.112	255.255.255.240	
150.100.2.114	0111	0010	150.100.2.112	255.255.255.240	
150.100.2.115	0111	0011	150.100.2.112	255.255.255.240	
150.100.2.116	0111	0100	150.100.2.112	255.255.255.240	
150.100.2.117	0111	0101	150.100.2.112	255.255.255.240	
150.100.2.118	0111	0110	150.100.2.112	255.255.255.240	
150.100.2.119	0111	0111	150.100.2.112	255.255.255.240	
150.100.2.120	0111	1000	150.100.2.112	255.255.255.240	
150.100.2.121	0111	1001	150.100.2.112	255.255.255.240	
150.100.2.122	0111	1010	150.100.2.112	255.255.255.240	
150.100.2.123	0111	1011	150.100.2.112	255.255.255.240	
150.100.2.124	0111	1100	150.100.2.112	255.255.255.240	
150.100.2.125	0111	1101	150.100.2.112	255.255.255.240	
150.100.2.126	0111	1110	150.100.2.112	255.255.255.240	
150.100.2.127	0111	1111	150.100.2.112	255.255.255.240	Subnet broadcast; area boundary; area 8 ends
150.100.2.128	1000	0000	150.100.2.128	255.255.255.240	Identifiant de sous-réseau; area boundary; area 17 starts
150.100.2.129	1000	0001	150.100.2.128	255.255.255.240	
150.100.2.130	1000	0010	150.100.2.128	255.255.255.240	
150.100.2.131	1000	0011	150.100.2.128	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.132	1000	0100	150.100.2.128	255.255.255.240	
150.100.2.133	1000	0101	150.100.2.128	255.255.255.240	
150.100.2.134	1000	0110	150.100.2.128	255.255.255.240	
150.100.2.135	1000	0111	150.100.2.128	255.255.255.240	
150.100.2.136	1000	1000	150.100.2.128	255.255.255.240	
150.100.2.137	1000	1001	150.100.2.128	255.255.255.240	
150.100.2.138	1000	1010	150.100.2.128	255.255.255.240	
150.100.2.139	1000	1011	150.100.2.128	255.255.255.240	
150.100.2.140	1000	1100	150.100.2.128	255.255.255.240	
150.100.2.141	1000	1101	150.100.2.128	255.255.255.240	
150.100.2.142	1000	1110	150.100.2.128	255.255.255.240	
150.100.2.143	1000	1111	150.100.2.128	255.255.255.240	Broadcast de sous-réseau
150.100.2.144	1001	0000	150.100.2.144	255.255.255.240	Identifiant de sous-réseau
150.100.2.145	1001	0001	150.100.2.144	255.255.255.240	
150.100.2.146	1001	0010	150.100.2.144	255.255.255.240	
150.100.2.147	1001	0011	150.100.2.144	255.255.255.240	
150.100.2.148	1001	0100	150.100.2.144	255.255.255.240	
150.100.2.149	1001	0101	150.100.2.144	255.255.255.240	
150.100.2.150	1001	0110	150.100.2.144	255.255.255.240	
150.100.2.151	1001	0111	150.100.2.144	255.255.255.240	
150.100.2.152	1001	1000	150.100.2.144	255.255.255.240	
150.100.2.153	1001	1001	150.100.2.144	255.255.255.240	
150.100.2.154	1001	1010	150.100.2.144	255.255.255.240	
150.100.2.155	1001	1011	150.100.2.144	255.255.255.240	
150.100.2.156	1001	1100	150.100.2.144	255.255.255.240	
150.100.2.157	1001	1101	150.100.2.144	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.158	1001	1110	150.100.2.144	255.255.255.240	
150.100.2.159	1001	1111	150.100.2.144	255.255.255.240	Broadcast de sous-réseau
150.100.2.160	1010	0000	150.100.2.160	255.255.255.240	Identifiant de sous-réseau
150.100.2.161	1010	0001	150.100.2.160	255.255.255.240	
150.100.2.162	1010	0010	150.100.2.160	255.255.255.240	
150.100.2.163	1010	0011	150.100.2.160	255.255.255.240	
150.100.2.164	1010	0100	150.100.2.160	255.255.255.240	
150.100.2.165	1010	0101	150.100.2.160	255.255.255.240	
150.100.2.166	1010	0110	150.100.2.160	255.255.255.240	
150.100.2.167	1010	0111	150.100.2.160	255.255.255.240	
150.100.2.168	1010	1000	150.100.2.160	255.255.255.240	
150.100.2.169	1010	1001	150.100.2.160	255.255.255.240	
150.100.2.170	1010	1010	150.100.2.160	255.255.255.240	
150.100.2.171	1010	1011	150.100.2.160	255.255.255.240	
150.100.2.172	1010	1100	150.100.2.160	255.255.255.240	
150.100.2.173	1010	1101	150.100.2.160	255.255.255.240	
150.100.2.174	1010	1110	150.100.2.160	255.255.255.240	
150.100.2.175	1010	1111	150.100.2.160	255.255.255.240	Broadcast de sous-réseau
150.100.2.176	101100	00	150.100.2.176	255.255.255.252	Identifiant de sous-réseau
150.100.2.177	101100	01	150.100.2.176	255.255.255.252	
150.100.2.178	101100	10	150.100.2.176	255.255.255.252	
150.100.2.179	101100	11	150.100.2.176	255.255.255.252	Broadcast de sous-réseau
150.100.2.180	101101	00	150.100.2.180	255.255.255.252	Identifiant de sous-réseau

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.181	101101	01	150.100.2.180	255.255.255.252	
150.100.2.182	101101	10	150.100.2.180	255.255.255.252	
150.100.2.183	101101	11	150.100.2.180	255.255.255.252	Broadcast de sous-réseau
150.100.2.184	101110	00	150.100.2.184	255.255.255.252	Identifiant de sous-réseau
150.100.2.185	101110	01	150.100.2.184	255.255.255.252	
150.100.2.186	101110	10	150.100.2.184	255.255.255.252	
150.100.2.187	101110	11	150.100.2.184	255.255.255.252	Broadcast de sous-réseau
150.100.2.188	101111	00	150.100.2.188	255.255.255.252	Identifiant de sous-réseau
150.100.2.189	101111	01	150.100.2.188	255.255.255.252	
150.100.2.190	101111	10	150.100.2.188	255.255.255.252	
150.100.2.191	101111	11	150.100.2.188	255.255.255.252	Broadcast de sous-réseau
150.100.2.192	1100	0000	150.100.2.192	255.255.255.240	Identifiant de sous-réseau
150.100.2.193	1100	0001	150.100.2.192	255.255.255.240	
150.100.2.194	1100	0010	150.100.2.192	255.255.255.240	
150.100.2.195	1100	0011	150.100.2.192	255.255.255.240	
150.100.2.196	1100	0100	150.100.2.192	255.255.255.240	
150.100.2.197	1100	0101	150.100.2.192	255.255.255.240	
150.100.2.198	1100	0110	150.100.2.192	255.255.255.240	
150.100.2.199	1100	0111	150.100.2.192	255.255.255.240	
150.100.2.200	1100	1000	150.100.2.192	255.255.255.240	
150.100.2.201	1100	1001	150.100.2.192	255.255.255.240	
150.100.2.202	1100	1010	150.100.2.192	255.255.255.240	
150.100.2.203	1100	1011	150.100.2.192	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.204	1100	1100	150.100.2.192	255.255.255.240	
150.100.2.205	1100	1101	150.100.2.192	255.255.255.240	
150.100.2.206	1100	1110	150.100.2.192	255.255.255.240	
150.100.2.207	1100	1111	150.100.2.192	255.255.255.240	Broadcast de sous-réseau
150.100.2.208	1101	0000	150.100.2.208	255.255.255.240	Identifiant de sous-réseau
150.100.2.209	1101	0001	150.100.2.208	255.255.255.240	
150.100.2.210	1101	0010	150.100.2.208	255.255.255.240	
150.100.2.211	1101	0011	150.100.2.208	255.255.255.240	
150.100.2.212	1101	0100	150.100.2.208	255.255.255.240	
150.100.2.213	1101	0101	150.100.2.208	255.255.255.240	
150.100.2.214	1101	0110	150.100.2.208	255.255.255.240	
150.100.2.215	1101	0111	150.100.2.208	255.255.255.240	
150.100.2.216	1101	1000	150.100.2.208	255.255.255.240	
150.100.2.217	1101	1001	150.100.2.208	255.255.255.240	
150.100.2.218	1101	1010	150.100.2.208	255.255.255.240	
150.100.2.219	1101	1011	150.100.2.208	255.255.255.240	
150.100.2.220	1101	1100	150.100.2.208	255.255.255.240	
150.100.2.221	1101	1101	150.100.2.208	255.255.255.240	
150.100.2.222	1101	1110	150.100.2.208	255.255.255.240	
150.100.2.223	1101	1111	150.100.2.208	255.255.255.240	Broadcast de sous-réseau
150.100.2.224	1110	0000	150.100.2.224	255.255.255.240	Identifiant de sous-réseau
150.100.2.225	1110	0001	150.100.2.224	255.255.255.240	
150.100.2.226	1110	0010	150.100.2.224	255.255.255.240	
150.100.2.227	1110	0011	150.100.2.224	255.255.255.240	
150.100.2.228	1110	0100	150.100.2.224	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (suite)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.229	1110	0101	150.100.2.224	255.255.255.240	
150.100.2.230	1110	0110	150.100.2.224	255.255.255.240	
150.100.2.231	1110	0111	150.100.2.224	255.255.255.240	
150.100.2.232	1110	1000	150.100.2.224	255.255.255.240	
150.100.2.233	1110	1001	150.100.2.224	255.255.255.240	
150.100.2.234	1110	1010	150.100.2.224	255.255.255.240	
150.100.2.235	1110	1011	150.100.2.224	255.255.255.240	
150.100.2.236	1110	1100	150.100.2.224	255.255.255.240	
150.100.2.237	1110	1101	150.100.2.224	255.255.255.240	
150.100.2.238	1110	1110	150.100.2.224	255.255.255.240	
150.100.2.239	1110	1111	150.100.2.224	255.255.255.240	Broadcast de sous-réseau
150.100.2.240	1111	0000	150.100.2.240	255.255.255.240	Identifiant de sous-réseau
150.100.2.241	1111	0001	150.100.2.240	255.255.255.240	
150.100.2.242	1111	0010	150.100.2.240	255.255.255.240	
150.100.2.243	1111	0011	150.100.2.240	255.255.255.240	
150.100.2.244	1111	0100	150.100.2.240	255.255.255.240	
150.100.2.245	1111	0101	150.100.2.240	255.255.255.240	
150.100.2.246	1111	0110	150.100.2.240	255.255.255.240	
150.100.2.247	1111	0111	150.100.2.240	255.255.255.240	
150.100.2.248	1111	1000	150.100.2.240	255.255.255.240	
150.100.2.249	1111	1001	150.100.2.240	255.255.255.240	
150.100.2.250	1111	1010	150.100.2.240	255.255.255.240	
150.100.2.251	1111	1011	150.100.2.240	255.255.255.240	
150.100.2.252	1111	1100	150.100.2.240	255.255.255.240	
150.100.2.253	1111	1101	150.100.2.240	255.255.255.240	

Tableau A.1 : Exemple partiel d'assignation d'adresses de sous-réseaux au moyen de VLSM (*suite*)

<i>Adresse IP (décimale)</i>	<i>Portion sous-réseau du dernier octet (binaire)</i>	<i>Portion hôte du dernier octet (binaire)</i>	<i>Adresse de sous-réseau</i>	<i>Masque de sous-réseau</i>	<i>Notes</i>
150.100.2.254	1111	1110	150.100.2.240	255.255.255.240	
150.100.2.255	1111	1111	150.100.2.240	255.255.255.240	Broadcast de sous-réseau ; limite de zone ; la zone 17 se termine

B

Implémentation de liaisons série IBM

Cette annexe tente de clarifier certaines confusions à propos des connexions semi-duplex, duplex et multipoint.

Semi-duplex versus duplex

Les notions de liaison série semi-duplex et duplex (*full-duplex*) sont souvent confuses. Cela s'explique par les différents contextes dans lesquels ces deux termes sont employés, à savoir les implémentations de liaisons asynchrones, les implémentations spécifiques de SNA (*Systems Network Architecture*) d'IBM, et les implémentations d'équipements de communication ETCD (Équipement terminal de circuit de données). Chacun de ces contextes est étudié dans les prochaines sections.

Liaisons asynchrones

En ce qui concerne les liaisons de communication asynchrones (et les paramètres logiciels d'émulation de terminal), le terme *duplex* implique un *duplex intégral (full-duplex)* en ce qui concerne l'écho des caractères envoyés par un hôte vers un terminal. Ce mode porte également le nom de mode *echoplex*. Dans ce contexte, le mode *semi-duplex* implique l'absence d'écho de caractère. On rencontre couramment certaines configurations de terminaux et d'hôtes inadéquates :

- Le mode duplex spécifié sur un terminal lorsque l'hôte est configuré pour le mode semi-duplex résulte en une saisie aveugle sur le terminal.
- Le mode semi-duplex spécifié sur un terminal lorsque l'hôte est configuré pour le mode duplex résulte en des caractères doubles sur le terminal. La raison est que le terminal affiche les caractères entrés si sa configuration indique que l'hôte n'enverra pas d'écho de caractère.

NOTE

Cette interprétation du mode duplex ne s'applique pas dans un contexte de routeur.

SNA d'IBM

Le glossaire de base d'IBM définit les modes *duplex* et *semi-duplex* pour les termes VTAM, NCP et NetView de la façon suivante :

- **Duplex.** Dans les communications de données, se rapporte à une connexion autorisant le transport bidirectionnel simultané des données ; contraire de semi-duplex.
- **Semi-duplex.** Dans les communications de données, se rapporte à une connexion autorisant le transport unidirectionnel à l'alternat des données ; contraire de duplex.

Ces définitions peuvent s'appliquer dans deux contextes représentant les deux sources principales de confusion :

- Tout d'abord, il existe des *transferts de données duplex* et *semi-duplex*. Cela concerne généralement la capacité ou l'incapacité d'un ETCD à supporter les flots de données bidirectionnels simultanés. Les dispositifs PU 4 SNA (ordinateurs frontaux tels que 3705, 3720, 3725 et 3745) sont capables de gérer le transfert de données en mode duplex. Chacun de ces dispositifs utilise un chemin de données et de contrôle distincts dans les tampons de réception et de transmission du programme de contrôle.
- Certains dispositifs PU 2.1 sont aussi capables de gérer le mode duplex, qui est négociable dans la trame de format XID-3, à moins que l'instruction DATMODE=FULL de définition NCP du PU ne soit spécifiée. La présence du paramètre FULL impose le mode duplex. Les dispositifs PU 2 et PU 1 fonctionnent dans le mode semi-duplex.

ETCD

Enfin, les termes *duplex* et *semi-duplex* s'appliquent aux équipements de communication, ou ETCD. C'est dans ce domaine que la majorité des avancées technologiques a été réalisée en ce qui concerne ces deux modes de transmission. Les installations de ETCD consistent principalement en des unités de services de données (DSU, *Data Service Unit*), des unités de services de canal (CSU, *Channel Service Unit*), ou des modems, et une ligne de communication. Le modem peut être synchrone ou asynchrone, et analogique ou numérique. La ligne de communication peut être à deux ou quatre fils, et peut être louée ou commutée (c'est-à-dire établie par appel).

Les anciens modems ne sont capables que de transmettre ou de recevoir des données, mais non de réaliser ces opérations en même temps. Lorsqu'un ETTD (Equipement Terminal de Traitement de Données) souhaite transmettre des données en utilisant un ancien modem, il émet un RTS (*Request To Send*) vers le modem. Si le modem *n'est pas* en mode réception, il active son signal de porteuse en préparation de la transmission de données et active un signal CTS (*Clear To Send*). Si le modem est en mode réception, son signal DCD (*Data Carrier Detect*), c'est-à-dire le signal de la porteuse du modem distant, est actif. Le modem n'active donc pas le signal CTS, et l'ETTD ne transmet pas, car le signal DCD est actif.

Les modems récents sont capables de transmettre et de recevoir des données simultanément sur des lignes louées ou commutées à deux ou quatre fils. Une méthode utilise plusieurs signaux de porteuse à différentes fréquences, de façon que les signaux de transmission et de réception du modem local et ceux du modem distant disposent chacun de leur propre fréquence de porteuse.

Un ETTD dans un environnement SDLC possède des options de configuration qui spécifient le mode de fonctionnement supporté par un ETCD. Les paramètres par défaut pour la plupart des dispositifs PU 2 sont définis pour le mode semi-duplex, bien qu'ils puissent également supporter le mode duplex. Si l'équipement est capable de fonctionner en mode duplex, le signal RTS peut être activé en permanence. Si l'équipement supporte le mode semi-duplex ou bien fonctionne dans un environnement multipoint qui recourt à des dispositifs de partage de modems (et non pas un environnement multipoint fourni par une compagnie de téléphone), RTS doit être activé uniquement lors de la transmission. Un équipement de communication qui supporte le mode duplex et qui connecte un dispositif PU 4 à un autre dispositif PU 2 ou PU 1 (chaque PU étant configuré pour un ETCD assurant le mode duplex) fournit un meilleur temps de réponse en raison de la réduction des changements d'état.

Les anciens dispositifs PU 2 et PU 1 ne peuvent pas être configurés pour le mode ETCD duplex. Par conséquent, comme ils ne peuvent supporter que les transferts de données semi-duplex, la transmission et la réception de données ne peuvent pas avoir lieu en même temps sur la ligne (contrairement à un échange duplex entre PU 4).

Connexions multipoints

Le mode multipoint représente une méthode de partage d'un équipement de communication entre plusieurs emplacements. Les compagnies de téléphone offrent des configurations multipoints à deux fils et à quatre fils pour un service analogique (connexion par modem) ou à quatre fils pour un service numérique (CSU/DSU). La plupart des implémentations sont *master-polling*, *multislave-drop* (un maître, plusieurs esclaves). Le maître ne se connecte qu'à un esclave à la fois. La commutation prend place au niveau d'un autocommutateur local à proximité du site ETTD maître. Certains fournisseurs de services offrent des services multipoints analogiques qui supportent une communication bidirectionnelle simultanée, ce qui permet aux ETTD d'être configurés pour un RTS permanent.

Les dispositifs de partage de modems et les dispositifs de partage de lignes fournissent également des fonctions multipoints. Ces implémentations autorisent le partage d'une seule liaison point-à-point entre plusieurs dispositifs. Certains d'entre eux disposent de ports configurables pour ETTD et ETCD, ce qui leur permet d'être configurés pour une adaptation à plusieurs sites (appelés *configuration en cascade*). La principale contrainte de ces dispositifs est que les autres utilisateurs sont bloqués lorsque le signal RTS est actif. Vous ne pouvez pas configurer des ETTD pour un signal RTS permanent et vous devez accepter les délais de changement d'état associés à ce mode de fonctionnement.

C

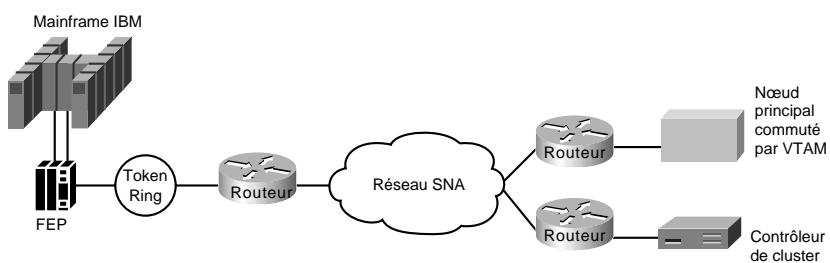
Configuration d'hôte SNA pour des réseaux SRB

Lors de la conception de réseaux SRB (*Source Routing Bridge*, "pont à routage par la source") comportant des routeurs et des entités SNA IBM, vous devez configurer avec soin les nœuds SNA ainsi que les nœuds de routage. Cette annexe donne des exemples mettant en jeu les trois équipements SNA spécifiques suivants :

- FEP (*Front End Processor*) ;
- nœuds principaux commutés par VTAM (*Virtual Telecommunications Access Method*) ;
- contrôleurs de cluster.

La Figure C.1 illustre un environnement typique. Les Tableaux C.1 à C.6 présentent les paramètres de définition des équipements présentés dans la même figure.

Figure C.1
Environnement
d'hôte SNA typique.



Configuration FEP

Les paramètres répertoriés dans les Tableaux C.1 à C.6 illustrent l'entrée pour le processus de génération de système NCP (*Network Control Program*) qui est exécuté par le processeur de l'hôte au moyen du NDF (*Network Definition Facility*). Le NDF fait partie de l'utilitaire ACF/NCP/System Support Program. La sortie produite par le processus de génération est un *module de chargement*

qui s'exécute sur un FEP. Sa taille peut en général être légèrement inférieure à 1 Mo et dépasser les 3 Mo. L'utilitaire ACF/NCP/System Support Program est également utilisé pour le chargement et le dumping d'un FEP.

Les tableaux suivants mettent en valeur les paramètres pour la génération de ressources Token Ring.

Tableau C.1 : Paramètres de définition pour BUILD

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
LOCALTO	1.5	Temporisateur d'acquittement d'anneau local (secondes).
REMOTTO	2.5	Temporisateur d'acquittement d'anneau distant (secondes).
MAXSESS	5000	Quantité maximale de sessions pour toutes les ressources connectées.
MXRLINE	Rien	Nombre maximal de connexions NTRI physiques (Version 5.2.1 et avant seulement).
MXVLINE	Rien	Nombre maximal de connexions NTRI logiques (Version 5.2.1 et avant seulement).
T2TIMER	(<i>localt2</i> , <i>remott2</i> , <i>N3</i>)	(Version 5.R4 et ultérieure seulement). Les paramètres spécifient un acquittement/temporisateur de réception (T2) pour anneaux Token Ring locaux et distants de la part de nœuds périphériques ou de nœuds de sous-zone. Valeurs acceptables : la plage <i>localt2</i> est de 0 à 2,0 secondes ; la plage <i>remott2</i> est de 0 à 2,0 secondes ; la plage <i>N3</i> est de 1 à 127 (par défaut 2). Les valeurs pour <i>localt2</i> et <i>remott2</i> devraient être de 10,0 % de la valeur du temporisateur T1 des stations adjacentes. <i>N3</i> spécifie le nombre maximal de trames d'informations (<i>I-frame</i>) reçues sans envoi d'un acquittement pour les connexions de sous-zone.

La définition LUDRPOOL présentée dans le Tableau C.2 spécifie le nombre de ressources périphériques nécessaires pour la quantité correcte d'espace de stockage de blocs de contrôle à réservier pour les nouvelles connexions.

Tableau C.2 : Paramètres de définition pour LUDRPOOL

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
NUMTYP2	Aucun	Le maximum est 16,000
NUMILU	Aucun	Requis pour les dispositifs LU Type 2.1 (LU indépendants)

La définition GROUP présentée dans le Tableau C.3 spécifie les paramètres de définition de groupe.

Tableau C.3 : Paramètres de définition pour GROUP

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
AUTOGEN	<i>Nombre</i>	Spécifie le nombre de paires de LINE/PU pour ce groupe
COMPWN	Y	Ressource potentielle de secours pour FEP double
COMPSPW	Y	TIC avec port échangeable (secours à chaud)
COMPTAD	Y	TIC avec FEP utilisant le chargement IPL
DIAL	YES or NO	S'applique aux spécifications de paramètres ECLTYPE YES requis pour (LOGICAL, PERIPHERAL) ; NO requis pour toutes les autres combinaisons indiquées dans la spécification ECLTYPE
ECLTYPE	(PHYSICAL, ANY) (PHYSICAL, PERIPHERAL) (PHYSICAL, SUBAREA) (LOGICAL, PERIPHERAL) (LOGICAL, SUBAREA)	Autorise la connexion des équipements PU 4 et PU 2 Autorise les dispositifs PU 2 uniquement Autorise les dispositifs PU4 uniquement Définit les dispositifs connectés comme PU 2 Définit les dispositifs connectés comme PU 4
LNCTL	SDLC	Requis pour la compatibilité de traitement NCP
PHYPORT	Aucun	Requis pour ECLTYPE LOGICAL uniquement ; le relie à un ECLTYPE PHYSICAL
TIMER	error, ras, stap ou lstap	Points d'entrée pour les routines de temporisateur NTRI

La définition LINE présentée dans le Tableau C.4 spécifie les paramètres de définitions de ligne.

Tableau C.4 : Paramètres de définition pour LINE

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
ADAPTER	TIC1 TIC2	Interface Token Ring 4 Mbit/s Interface Token Ring 4 Mbit/s ou 16 Mbit/s
ADDRESS	1088 à 1095	Plage d'adresse valides pour les TIC ; une seule spécifiée par définition LINE
BEACTO	52	Temps en secondes durant lequel l'anneau peut émettre un signal <i>beacon</i> avant que le TIC ne le considère comme défaillant ; le maximum est 600
LOCADD	4000 a bbbbbb	Adresses TIC administrées localement, où a est une valeur de 0 à 7 ; et b est une valeur entière de 0 à 9
LOCALTO	1,5	V5R4 ; pareil à BUILD (voir Tableau C.1), mais seulement pour les dispositifs PU 4 (LOGICAL, SUBAREA) ; autorise la granularité pour les TIC individuels pour les connexions SUBAREA

Tableau C.4 : Paramètres de définition pour LINE (suite)

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
REMOTTO	2,5	Paramètre V5R4 ; pareil à LOCALTO ; voir les paramètres BUILD dans le Tableau C.1
T2TIMER	<i>localt2, remott2, N3</i>	Paramètre V5.4 ; voir les paramètres BUILD dans le Tableau C.1 ; peut être défini dans la définition LINE seulement si un nœud de sous-zone a été défini dans la définition GROUP
MAXTSL	2044 à 16732	Spécifie les données maximales en octets que le NTRI peut transmettre ; le maximum pour TIC1 est 2044 ; le maximum pour TIC2 à TRSPEED16 est 16732
PORTADD	<i>Nombre</i>	Pour l'association des ECLTYPE physiques à des ECLTYPE logiques ; correspond à la spécification ECLTYPE physique ou logique
RETRIES	<i>m, t, n, ml</i>	Où <i>m</i> = nombre de tentatives pour les sessions d'anneau distant, <i>t</i> = pause entre les séquences de tentatives, <i>n</i> = nombre de séquences de tentatives et <i>ml</i> = nombre de tentatives par séquence pour des sessions d'anneau local
TRSPEED	4 ou 16	Vitesse de TIC

Le Tableau C.5 spécifie les paramètres de définition d'unité physique (PU).

Tableau C.5 : Paramètres de définition d'unité physique de FEP (PU)

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
ADDR	<i>aa4000bcccccc</i>	Point d'accès de service de destination (DSAP) et adresse MAC pour le PU du dispositif Token Ring dans le FEP, où <i>aa</i> = le DSAP et représente un multiple hexadécimal non égal à zéro de 4 ; <i>b</i> = 0 à 7 ; <i>c</i> = 0 à 9 ; taper 4000 comme indiqué ; seulement spécifié si le ECLTYPE défini dans la définition GROUP est l'un des suivants : (LOG,SUB), (PHY,SUB), (PHY,ANY).
PUTYPE	1, 2 ou 4	Dépend du ECLTYPE: <ul style="list-style-type: none"> • Pour les ressources NTRI LOGICAL, seul PUTYPE=2 est valide ; pour les ressources NTRI PHYSICAL, seul PUTYPE=1 est valide. • Pour NTRI PHYSICAL/SUBAREA LINES et PHYSICAL PERIPHERAL LINES, seul PUTYPE=1 est valide ; pour NTRI LOGICAL PERIPHERAL LINES, seul PUTYPE=2 est valide.

Tableau C.5 : Paramètres de définition d'unité physique de FEP (PU) (suite)

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
XID	YES ou NO	Définit la capacité d'un PU à recevoir et à répondre à un XID en mode normal déconnecté ; pour NTRI LOGICAL LINES, seul YES est valide ; pour NTRI PHYSICAL LINES, seul NO est valide.

Le Tableau C.6 spécifie les paramètres de définition d'unité logique (LU).

Tableau C.6 : Paramètre de définition d'unité logique (LU) de FEP

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
LOCADDR	0	Spécifie cette réponse seulement

Définitions de nœud principal commuté par VTAM

Les équipements qui sont connectés à un réseau Token Ring et qui communiquent avec une application d'hôte IBM doivent être définis au moyen de la méthode d'accès VTAM associée à l'hôte. Ces équipements sont vus comme des ressources de ligne commutée par l'hôte, et sont définis dans un composant de configuration nommé *Switched Major Node* (composant principal commuté). Certaines définitions courantes de configuration de réseau sont présentées dans les Tableaux C.7 à C.9.

Tableau C.7 : Paramètre de définition pour VBUILD

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
TYPE	SWNET	Spécifie un type de ressource pour VTAM ; SWNET indique <i>switched major node type</i>

Tableau C.8 : Paramètres de définition pour une PU de VTAM

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
IDBLK	017	Valeurs typiques : <ul style="list-style-type: none"> • 017 = 3X74. • 05D = PU VTAM basé PC • 0E2 = SDLLC Cisco (enregistré avec IBM)
IDNUM	xxxxx	Numéro unique identifiant un équipement
MAXOUT	1 à 7	Nombre de trames d'informations (<i>I-frame</i>) envoyées avant que l'acquittement ne soit requis

Tableau C.8 : Paramètres de définition pour une PU de VTAM (suite)

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
MAXDATA	265	Indique un nombre maximal d'octets qu'une PU 2 peut recevoir ; ignoré pour une PU 2.1, car cette valeur est négociable La valeur par défaut pour un 3174 est 521
PUTYPE	2	Seule valeur valide
XID	YES or NO	La valeur YES devrait être utilisée pour les dispositifs PU 2.1 La valeur NO devrait être indiquée pour tout autre dispositif

Tableau C.9 : Paramètre de définition pour une LU de VTAM

<i>Paramètre</i>	<i>Exemple, paramètre, valeur ou plage</i>	<i>Description de paramètre et notes d'implémentation</i>
LOCADDR	2 à FF	Adresses d'unité logique (LU) connectée à une PU

Exemple de configuration d'un contrôleur de cluster 3174

La configuration suivante provient d'un contrôleur de cluster 3174-13R, numéro de série 45362, connecté à un réseau Token Ring. Ces entrées ont été utilisées avec un 3174 spécifique s'exécutant sur un Token Ring 4 Mbit/s. La configuration de ce 3174-13R a impliqué trois écrans de configuration spécifiques. Les Tableaux C.10 à C.12 présentent les numéros de lignes de configuration, les entrées utilisées et les descriptions de lignes de configuration. Lorsque cela était possible, des descriptions étendues ont été données pour les entrées qui sont pertinentes pour les exigences de réseau routé.

NOTE

Les lignes de configuration intéressantes lors de la configuration de dispositifs 3174 pour un environnement SRB sont les lignes 106, 107 et 384 sur l'écran de configuration 2 (voir Tableau C.11). Elles spécifient les adresses requises et le type de Token Ring pertinent pour le contrôleur de cluster.

Tableau C.10 : Détails de l'écran de configuration 1 pour le 3174-13R

<i>Numéro de ligne de configuration</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
98		Mot de passe de test en ligne
99	TKNRNG	Champ de description
100	13R	Numéro de modèle
101	7	Type de raccordement de l'hôte

Tableau C.11 : Détails de l'écran de configuration 2 pour le 3174-13R

<i>Numéro de ligne de configuration</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
106	4000 2222 4444 04	Les 12 premiers chiffres hexadécimaux forment l'adresse MAC source du contrôleur de cluster (4000 2222 4444) ; les deux derniers chiffres représentent le SAP source (SSAP) pour LLC2 (0x04 = SNA).
107	4000 0037 4501 04	Les 12 premiers chiffres hexadécimaux forment l'adresse MAC source du FEP (4000 0037 4501) ; les deux derniers chiffres représentent le DSAP pour LLC2 (0x04 for SNA).
108	0045362	Numéro de série du contrôleur de cluster.
110	0	Support de stockage MLT.
116	0	Assignation de port individuel.
121	01	Langage du clavier.
123	0	Support de page de codes nationaux étendus.
125	00000000	Options diverses (A).
126	00000000	Options diverses (B).
127	0 0	Définition RTM.
132	0000	Choix alternatif de clavier de base.
136	0000	Disposition standard de clavier.
137	0000	Disposition de clavier modifiée.
138	0	Disposition standard de pavé numérique.
141	A	Ensemble de caractères magnétiques.
165	0	Symboles de programme compressés.
166	A	Pavé de sélection d'attribut.
168	0	Extension supplémentaire ; définition de touche de mode.
173	0000	Options DFT.
175	000000	Mot de passe DFT.
179	000	Stockage au format local.
213	0	Partage d'imprimante.
215	45362	Identification PU.
222	0	Support pour renouvellement de commande.

Tableau C.11 : Détails de l'écran de configuration 2 pour le 3174-13R (*suite*)

<i>Numéro de ligne de configuration</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
382	0521	Taille maximale de trame d'information d'anneau ; la plage de valeurs est de 265 à 2057.
383	2	Nombre maximal de trames d'informations que le 3174 transmettra avant d'attendre un acquittement (taille de fenêtre de transmission).
384	0	Vitesse d'anneau du réseau Token Ring : <ul style="list-style-type: none"> • 0 = 4 Mbit/s. • 1 = 16 Mbit/s libération normale du jeton. • 2 = 16 Mbit/s libération anticipée du jeton.

Tableau C.12 : Détails de l'écran de configuration 2 pour le 3174-13R

<i>Numéro de configuration de ligne</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
500	0	CSCM unique
501	TOSFNID	Identifiant de réseau
503	TOSFCTRLR	Nom de l'unité LU

Les stations terminales SNA implémentent LLC2 (*Logical Link Control Type 2*) lorsqu'elles sont connectées à un réseau local (LAN). LLC2 implémente les éléments suivants :

- des temporisateurs ;
- le séquencement ;
- la récupération après erreur ;
- le fenêtrage ;
- la livraison garantie ;
- la connexion garantie.

La Figure C.2 illustre de quelle façon le temporisateur de réponse T1 et la fonction de récupération après erreur opèrent pour un 3174. Supposons que la liaison entre les deux routeurs vienne de tomber en panne. La séquence suivante caractérise le processus de récupération après erreur :

1. Le 3174 envoie une trame de données et démarre son temporisateur T1.
2. Le temporisateur T1 expire après 1,6 seconde.
3. Le 3174 entre dans le processus de récupération.
4. Le 3174 envoie une requête LLC : une trame *receiver ready* avec le bit d'interrogation (*poll*) activé, qui demande au 3745 d'acquitter immédiatement cette trame.

5. Le 3174 démarre son temporisateur T1.

6. Le temporisateur T1 expire après 1,6 seconde.

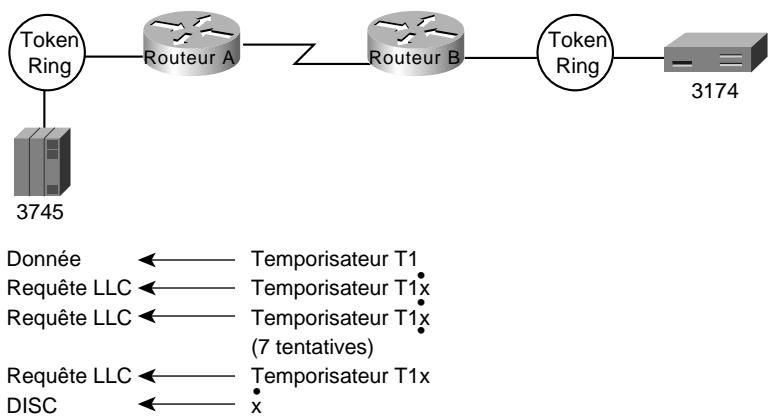
Cette procédure est répétée sept fois. Le délai d'attente avant la déconnexion de la session est calculé de la manière suivante :

■ La première tentative plus sept autres tentatives multipliées par 1,6 seconde :

$$= 8 \times 1,6 \text{ seconde} ;$$

$$= 12,8 \text{ secondes.}$$

Figure C.2
Procédure de temporisation T1 et de récupération après erreur pour le 3174.



D

Configuration d'hôte SNA pour des réseaux SDLC

Cette annexe présente les informations d'implémentation de routeur en rapport avec les éléments suivants :

- configuration de FEP pour des liaisons SDLC ;
- exemple de tableaux de configuration SDLC de 3174.

Le Tableau D.1 présente le support de connexion point-à-point SDLC 3x74 pour les appliques AGS+, MGS et DCE CGS.

Tableau D.1 : Support de connexion point-à-point SDLC 3x74 pour les appliques AGS+, MGS et DCE CGS

Type de contrôleur	RS-232 ETCD	RS-232 NRZI/ETCD
3274 1^e génération		
• 3274-1C	Supporté	Supporté
3274 2^e génération		
• 3274-21C	Non testé	Supporté
3274 3^e génération		
• 3274-31C	Supporté	Non testé
• 3274-51C	Supporté	Non testé
3274 4^e génération		
• 3274-41C	Doit lier ensemble DSR et DTR sur le côté CU ; interrompre DSR vers le routeur	Non testé
• 3274-61C	Pareil à 3274-41C	Supporté

Tableau D.1 : Support de connexion point-à-point SDLC 3x74 pour les appliques AGS+, MGS et DCE CGS (suite)

Type de contrôleur	RS-232 ETCD	RS-232 NRZI/ETCD
• Telex 274	Supporté	Non testé
• Telex 1274	Supporté	Non testé
Emulation 3274 DCA/IRMA pour les stations DOS	Non testé	Supporté
Passerelle DEC SNA	Non testé	Supporté
Adaptateur multiprotocole RS 6000	Non testé	Supporté
CU sous-système de 3174		
• 3174-01R	Non testé	3174 place la broche 11 en position basse (-11VDC), ce qui provoque le mode ETTD de l'applique ETTD (le mode ETCD est activé lorsque la broche 11 est en position haute)
• 3174-03R	Pareil à 3174-01R	Pareil à 3174-01R
• 3174-51R	Pareil à 3174-01R	Pareil à 3174-01R
CU d'établissement de 3174		
• 3174-11R	Non testé	Supporté
• 3174-13R	Pareil à 3174-11R	Non testé
• 3174-61R	Pareil à 3174-11R	Non testé
• 3174-91R	Pareil à 3174-11R	Supporté
• Telex 1174	Supporté	Non testé

Configuration FEP pour liaisons SDLC

Les Tableaux D.2 à D.5 présentent des définitions de paramètres pertinentes pour un FEP configuré pour opérer avec un environnement basé sur un routeur. Ces paramètres font partie du processus de génération système associé au NCP sur un hôte IBM.

Tableau D.2 : Paramètres pour GROUP d'un exemple de configuration SDLC pour FEP

Paramètre	Exemple de valeur	Description et notes d'implémentation
LNCTL	SDLC	Paramètre de contrôle de ligne qui spécifie le protocole de ligne
REPLYTO	2	Temporisateur T1 ; il spécifie la valeur pour le délai de réponse pour les LINE dans ce GROUP

Tableau D.3 : Paramètres pour LINE d'un exemple de configuration SDLC pour FEP

<i>Paramètre</i>	<i>Exemple de valeur</i>	<i>Description et notes d'implémentation</i>
ADDRESS	(001,HALF)	La valeur 001 est l'adresse d'interface physique LINE du FEP. Le deuxième paramètre spécifie si le mode semi-duplex ou duplex est utilisé pour le transfert de données sur le FEP. Il affecte aussi le paramètre DUPLEX. Si la valeur FULL est spécifiée ici, DUPLEX prend par défaut la valeur FULL, et les tentatives de modification de cette caractéristique sont ignorées.
DUPLEX	HALF	Ce paramètre spécifie si la ligne de communication et le modem constituent des dispositifs semi-duplex ou duplex. Si la valeur HALF est spécifiée, le signal RTS du modem est activé uniquement lors de l'envoi de données. Si la valeur FULL est spécifiée, le signal RTS est toujours actif. Reportez-vous au paramètre ADDRESS dans ce tableau.
NRZI	YES	Encodage pour cette ligne ; les options sont NRZ ou NRZI.
RETRIES	(6,5,3)	Nombre de tentatives lorsque REPLYTO expire. Options d'entrée : (m, t, n) où m = nombre de tentatives, t = pause en secondes entre les cycles de tentatives et n = nombre de cycles de tentatives à réitérer. Cet exemple entraînerait six tentatives avec une pause équivalente à la valeur de REPLYTO entre chaque tentative RETRY (deux secondes par Tableau D.2), attend cinq secondes, et répète cette séquence trois fois pour un total de 63 secondes. A la fin de cette période, la session est terminée.
PAUSE	2	La durée en millisecondes entre les cycles d'interrogation (<i>poll</i>). Le cycle s'étend dès l'instant où le NCP interroge la première entrée dans la table d'ordre de services jusqu'au moment où le cycle d'interrogation suivant commence à la même entrée. Durant cette pause, toutes les données disponibles pour être envoyées vers une station finale sont transmises. Si des stations possèdent des données à transmettre lorsqu'elles y sont invitées, et que la durée d'envoi s'étende au-delà du paramètre PAUSE, le cycle d'interrogation suivant commence immédiatement.

Tableau D.4 : Paramètres pour unité PU d'un exemple de configuration SDLC pour FEP

<i>Paramètre</i>	<i>Exemple de valeur</i>	<i>Description et notes d'implémentation</i>
ADDR	C1	Adresse SDLC de la station terminale secondaire
MAXDATA	265	Quantité maximale de données en octets (en-têtes compris) que l'unité PU peut recevoir en un transfert de données ; c'est-à-dire une PIU complète ou un segment de PIU
MAXOUT	7	Nombre maximal de trames non acquittées que le NCP peut avoir en suspens avant de demander une réponse de la part de la station terminale

Tableau D.4 : Paramètres pour unité PU d'un exemple de configuration SDLC pour FEP (suite)

<i>Paramètre</i>	<i>Exemple de valeur</i>	<i>Description et notes d'implémentation</i>
PASSLIM	7	Nombre maximal de PIU ou de segments de PIU consécutifs que le NCP envoie en une fois vers la station terminale représentée par cette définition de PU
PUTYPE	2	Spécifie le type de PU ; PU type 2 et 2.1 sont tous deux spécifiés comme PUTYPE=2

Tableau D.5 : Paramètres pour unité LU d'un exemple de configuration SDLC pour FEP

<i>Paramètre</i>	<i>Exemple de valeur</i>	<i>Description et notes d'implémentation</i>
LOCADDR	2	Adresse LU de dispositifs connectés à la station terminale PU

Tableau de configuration SDLC pour 3174

Les Tableaux D.6 à D.8 présentent une configuration provenant d'un contrôleur de cluster 3174-91R connecté *via* SDLC. Cette configuration comprend trois écrans de configuration spécifiques. Les tableaux listent les numéros de lignes de configuration, les entrées utilisées et les descriptions des lignes de configuration de chaque écran. Quand cela a été possible, des descriptions supplémentaires ont été incluses pour les entrées pertinentes liées aux exigences de réseau routé.

Tableau D.6 : Détails de configuration de l'écran 1 du 3174-91R

<i>Numéro de ligne de configuration</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
98		Mot de passe de test en ligne
99	TKNRNG	Champ de description
100	91R	Numéro de modèle
101	2	Type de raccordement de l'hôte : <ul style="list-style-type: none"> • 2 = SDLC • 5 = SNA (<i>via</i> canal) • 7 = réseau Token Ring

NOTE

Les lignes de configuration 104, 313 et 340 sur l'écran de configuration 2 (voir Tableau D.7) sont intéressantes lors de la configuration de dispositifs 3174 pour un environnement SDLC basé sur un routeur. Ces lignes spécifient l'adresse SDLC requise et les options SDLC pertinentes pour le contrôleur de cluster.

Tableau D.7 : Détails de configuration de l'écran 2 du 3174-91R

<i>Numéro de ligne de configuration</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
104	C2	Spécifie l'adresse du contrôleur de cluster SDLC. Il s'agit de la même adresse que celle qui est configurée sur l'interface série du routeur. Elle représente aussi l'adresse PU du contrôleur. Dans les environnements multipoints, plusieurs adresses SDLC peuvent être spécifiées sur une seule interface série.
108	0045448	Numéro de série du contrôleur de cluster.
110	0	Support de stockage MLT.
116	0	Assignation de port individuel.
121	01	Langage pour le clavier.
123	0	Support pour page de codes nationaux étendus.
125	00000000	Options diverses (A).
126	00000000	Options diverses (B).
127	00	Définition RTM.
132	0000	Choix alternatif de clavier de base.
136	0000	Disposition standard de clavier.
137	0000	Disposition modifiée de clavier.
138	0	Disposition standard de pavé numérique.
141	A	Ensemble de caractères magnétiques.
150	0	Contrôleur de passerelle de réseau Token Ring.
165	0	Symboles de programme compressés.
166	A	Pavé de sélection d'attribut.
168	0	Extension supplémentaire ; définition de touche de mode.
173	0000	Options DFT.
175	000000	Mot de passe DFT.
179	000	Stockage au format local.
213	0	Partage d'imprimante entre.
215	45448	Identification PU.
220	0	Fonction d'alerte.
310	0	Données de connexion vers ligne.
313	0	NRZ = 0 ; NRZI = 1

Tableau D.7 : Détails de configuration de l'écran 2 du 3174-91R (suite)

<i>Numéro de ligne de configuration</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
317	0	Dispositif de télécommunication : • 0 = non commuté • 1 = commuté (numérotation)
318	0	Transmission à pleine vitesse/semi-vitesse ; 0 = pleine vitesse, 1 = semi-vitesse. Contrôle la vitesse du modem ; peut être utilisé dans les zones où les conditions de ligne sont mauvaises.
340	0	Options de contrôle de RTS : • 0 = RTS contrôlé (pour le fonctionnement LSD/MSD) • 1 = Permanent RTS (améliore les performances) • 2 = BSC (non valide pour le fonctionnement avec SDLC)
365	0	Connexion ETTD avec hôte commuté via X.21.
370	0	Taille maximale de trame d'information (<i>I-frame</i>) entrante : • 0 = 265 octets • 1 = 521 octets (recommandé pour de meilleures performances)

Tableau D.8 : Détails de configuration de l'écran 3 du 3174-91R

<i>Numéro de configuration de ligne</i>	<i>Exemple de valeur</i>	<i>Description de paramètre et notes d'implémentation</i>
500	0	Unique CSCM (<i>Central Site Change Management</i>)
501	xxxxxxxx	Identifiant de réseau
503	xxxxxxxx	Nom de l'unité LU (pour CSCM)

E

Diffusions broadcast sur des réseaux commutés

Pour communiquer avec toutes les portions d'un réseau, les protocoles utilisent des datagrammes broadcast et multicast de la couche 2 du modèle OSI (*Open Systems Interconnection*, interconnexion de systèmes ouverts). Cela suppose évidemment un média qui supporte le mode broadcast, tel Ethernet. Lorsqu'un nœud souhaite communiquer avec toutes les stations du réseau, il envoie un datagramme à l'adresse MAC FF-FF-FF-FF, une adresse broadcast qui doit être écoutée par la carte réseau de chaque hôte. Les routeurs, qui opèrent au niveau 3 du modèle OSI, ne transmettent généralement pas ces diffusions broadcast, mais les limitent au segment dont elles proviennent. Lorsqu'un hôte doit communiquer uniquement avec une portion du réseau, il envoie un datagramme à une adresse MAC spécifique, avec le bit de poids le plus fort de l'identifiant du fabricant activé (01-00-0C-CC-CC-CC, par exemple). C'est ce qu'on appelle une diffusion multicast. Les cartes réseau y répondent lorsqu'elles ont été configurées pour écouter cette adresse particulière. Aujourd'hui, une grande variété d'applications utilisent le multicast IP de façon intensive, afin d'optimiser l'utilisation de la bande passante. Au lieu d'envoyer n flux de x mégaoctets, où n est le nombre de destinataires, un seul flux de x mégaoctets est nécessaire. La prochaine section examine de plus près le multicast IP.

Multicast IP

Une plage entière d'adresses IP (une classe) a été réservée pour l'utilisation de la diffusion multicast (224.0.0.0 à 239.255.255.255). A l'aide d'une formule prédéfinie, il est possible d'associer une telle adresse IP de classe D à une adresse MAC multicast de niveau 2. Un bloc d'adresse MAC a été réservé pour permettre à des adresses IP de classe D d'être traduites en adresses MAC de niveau 2 (01-00-5E-xx-xx-xx). La correspondance est obtenue en plaçant les 23 bits de poids le plus faible de l'adresse IP de classe D dans les 23 bits de poids le plus faible de l'adresse multicast de niveau 2. Par exemple, l'adresse IP 236.123.1.2 correspondrait à l'adresse MAC 01-00-5E-7B-01-02.

Toutes les stations LAN qui supportent le multicast IP savent comment réaliser cette traduction, et peuvent donc facilement envoyer une diffusion multicast sur n'importe quel réseau LAN basé sur le standard IEEE 802. Etant donné que l'espace de classe D contient davantage d'adresses (2^{28}) que

le champ OUI (champ de fabricant) IETF au niveau de la couche MAC (2^{23}), de nombreuses adresses de groupe correspondent à chaque adresse IEEE 802. Certains groupes réservés ont été affectés à des utilisations spécifiques, les plus connus étant probablement 224.0.0.1 (tous les systèmes sur ce sous-réseau) et 224.0.0.2 (tous les routeurs sur ce sous-réseau). Les autres groupes sont 224.0.0.4 (tous les routeurs DVMRP), 224.0.0.6 (routeurs désignés OSPF), 224.0.0.9 (RIP version 2) et 224.0.0.10 (routeurs EIGRP).

Etant donné que les commutateurs fonctionnent comme des ponts, ils doivent propager tout le trafic broadcast, multicast et unicast inconnu. Cette procédure est connue sous le nom *d'inondation (flooding)*. L'ajout de trafic broadcast et multicast de la part de chaque équipement sur le réseau est appelée *propagation de diffusions broadcast*. Notez cependant que l'inondation est limitée à un VLAN. Par exemple, si une station faisant partie d'un VLAN tente d'atteindre une adresse MAC de destination qui n'a pas encore été découverte par le commutateur, la trame sera envoyée vers tous les ports de ce VLAN, excepté celui sur lequel la trame a été reçue. C'est pourquoi un VLAN est parfois appelé *domaine de broadcast*. Etant donné que les cartes réseau doivent interrompre le processeur afin de traiter chaque diffusion broadcast, la propagation de ce trafic affecte les performances des hôtes du réseau. La majorité des cartes réseau récentes peuvent filtrer les diffusions multicast non souhaitées ; aussi, elles n'ont pas besoin de les transmettre au processeur. Toutefois, toutes les cartes n'en sont pas capables ; dans ce cas, le trafic multicast doit être traité de la même manière que le trafic broadcast. Le plus souvent, l'hôte ne tire aucun bénéfice du traitement des diffusions broadcast ou multicast : soit il n'est pas le destinataire recherché, soit il ne s'intéresse pas au service annoncé, ou bien il en connaît déjà l'existence. Les routeurs qui supportent le mode multicast n'ont pas besoin d'être directement adressés, car leurs interfaces doivent opérer de façon transparente, et recevoir tout le trafic IP multicast.

Cisco a développé deux fonctionnalités qui réduisent considérablement l'inondation des trames multicast. Il s'agit de CGMP et de la surveillance IGMP. Une conversation CGMP a lieu entre un commutateur et un routeur Cisco. Le routeur indique au commutateur les adresses MAC qui ont demandé à rejoindre un groupe multicast (les stations utilisent des paquets IGMP pour demander aux routeurs de joindre des groupes). En retour, le commutateur effectue une recherche dans sa table de transmission, afin d'identifier les ports sur lesquels se trouvent ces stations. Il peut ensuite limiter la transmission des paquets multicast à ces stations en créant des entrées statiques. La surveillance IGMP remplit le même objectif global, mais sans impliquer le routeur. Néanmoins, le commutateur doit disposer de fonctionnalités suffisantes pour pouvoir analyser les paquets IP et identifier les requêtes IGMP.

IP n'est pas le seul protocole à utiliser la diffusion multicast. Les sections suivantes décrivent de quelle manière les protocoles IP, Novell et AppleTalk utilisent les diffusions broadcast et multicast pour localiser des hôtes, et annoncer des services. Elles examinent aussi en quoi le trafic lié à ces diffusions affecte les performances processeur des hôtes sur le réseau.

Réseaux IP

On dénombre trois sources de diffusion sur les réseaux IP :

- **Stations de travail.** Une station de travail IP envoie une requête ARP (*Address Resolution Protocol*) en mode broadcast chaque fois qu'elle a besoin de localiser une nouvelle adresse IP

sur le réseau. Par exemple, la commande `telnet cio.cisco.com` traduit un nom en adresse IP par le biais d'une recherche DNS (*Domain Name System*), puis une requête ARP broadcast est envoyée pour trouver la véritable station. En règle générale, les stations de travail IP placent dix à cent adresses en cache en deux heures de temps environ. Le taux ARP pour une station typique se situe autour de cinquante adresses toutes les deux heures, soit 0,007 requête ARP par seconde. Par conséquent, 2 000 stations IP produisent environ quatorze requêtes ARP par seconde.

- **Routeurs.** Un routeur IP représente tout routeur, ou station de travail, qui exécute un protocole de routage. Par exemple, RIP est un protocole qui fait une utilisation intensive des diffusions broadcast. Certains administrateurs configurent toutes les stations de travail pour qu'elles exécutent RIP en tant que stratégie de redondance et d'accessibilité. Toutes les 30 secondes, RIP utilise des diffusions broadcast pour retransmettre la table de routage complète aux autres routeurs RIP. Si 2 000 stations de travail étaient configurées afin d'exécuter RIP et que cinquante paquets soient nécessaires pour retransmettre la table de routage, les stations généreraient 3 333 diffusions broadcast par seconde. La plupart des administrateurs configurent un petit nombre de routeurs afin d'exécuter RIP, habituellement entre cinq et dix. Pour une table de routage qui requiert cinquante paquets, dix routeurs RIP généreraient environ seize diffusions broadcast par seconde. De façon plus générale, l'importance du problème est proportionnelle au nombre de routeurs. Heureusement, il existe des alternatives au mécanisme de broadcast RIP systématique, tel RIP version 2. Beaucoup d'autres protocoles de routage utilisent le multicast IP afin d'échanger des informations (OSPF, EIGRP, etc.), mais la quantité de trafic qu'ils génèrent est bien moindre que celle de protocoles tels que RIP, une fois que les informations de routage ont convergé.
- **Applications multicast.** Les applications multicast IP peuvent entraîner une dégradation des performances sur les grands réseaux linéaires à commutation de paquets. Bien que le multicast représente un moyen efficace pour envoyer un flot de données multimédias (vidéo) à de nombreux utilisateurs sur un hub de média partagé, il affecte chaque utilisateur sur un réseau commuté, en raison du processus d'inondation. Par exemple, une application vidéo par paquets peut générer un flot multimégaoctets de données multicast qui, sur un réseau commuté, serait envoyé vers chaque segment, ce qui provoquerait une grave congestion.

La Figure E.1 présente les résultats de tests réalisés par Cisco relatifs aux effets de la propagation de diffusions broadcast sur une station Sun SPARCstation 2, avec une carte Ethernet standard. La station exécutait SunOS version 4.1.3, avec la fonction de filtrage multicast IP activée. Si cette fonction avait été désactivée, les paquets multicast auraient affecté les performances du processeur.

Ainsi que le montrent les résultats de la Figure E.1, une station de travail IP peut être réellement arrêtée par une inondation de trafic broadcast. Bien qu'excessives, des pointes de diffusion broadcast de milliers de paquets par seconde ont été observées durant des tempêtes de broadcast. Des tests en environnement contrôlé, avec une plage de diffusions broadcast et multicast donnée sur le réseau, font apparaître des dégradations du système à partir de cent diffusions broadcast ou multicast par seconde. Le Tableau E.1 présente le pourcentage moyen de pertes de ressources processeur pour des réseaux IP allant de 100 à 10 000 hôtes.

Figure E.1
Effets de la propagation de diffusions broadcast sur les hôtes d'un réseau IP.

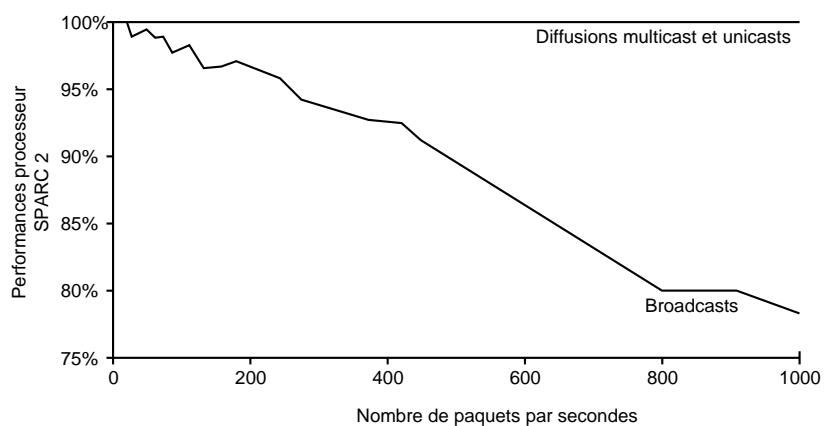


Tableau E.1 : Pertes de ressources processeur dues aux diffusions sur des réseaux IP

Nombre d'hôtes	Pourcentage moyen de pertes processeur par hôte
100	0,14
1 000	0,96
10 000	9,15

Bien que les chiffres du Tableau E.1 semblent faibles, ils correspondent à un réseau IP moyen bien conçu, qui n'exécute pas RIP. Lors de pointes de trafic broadcast et multicast provoquées par des comportements de type tempête, les pertes de ressources processeur peuvent excéder la moyenne. Durant une tempête de broadcast ou unicast provoquée par une boucle de niveau 2, de puissants systèmes terminaux peuvent être paralysés. La source d'une tempête de broadcast peut être un équipement qui demande des informations sur un réseau devenu trop grand. Le demandeur reçoit une quantité de réponses telle, qu'elle dépasse sa capacité à les traiter, ou bien la première requête déclenche des requêtes semblables de la part d'autres équipements, ce qui paralyse le flux de trafic normal sur le réseau.

Toutefois, n'allez pas en conclure que l'utilisation de la diffusion multicast ne doit pas être envisagée. Une utilisation correcte de cette fonctionnalité résulte en une exploitation bien plus efficace de la bande passante disponible. Au lieu d'envoyer n flux de m Mbit/s à n destinataires, par exemple, seul *un* flux de m Mbit/s est envoyé à un seul groupe multicast. Limiter les trafics broadcast et multicast au réseau local fait partie du processus de conception de réseaux commutés efficaces. Plusieurs techniques sont disponibles aujourd'hui sur les commutateurs multicouches de Cisco. Par exemple, le protocole CGMP de Cisco empêche l'inondation du trafic multicast sur tous les ports, grâce à une interaction entre le commutateur et le routeur Cisco. Le routeur communique au commutateur les adresses MAC qui ont demandé à rejoindre un groupe particulier, de façon que le commutateur sache (à partir de sa table de transmission) quels ports sont intéressés par ce flux multicast. De plus, la surveillance IGMP pour les commutateurs de niveau 3 élimine le besoin de

disposer d'un routeur externe, en fournissant au commutateur les fonctionnalités nécessaires afin d'examiner le contenu des paquets IGMP utilisés par les hôtes et les routeurs, dans le but d'échanger des informations d'appartenance à des groupes.

Réseaux Novell

Bon nombre de réseaux locaux fondés sur des PC utilisent encore le système d'exploitation de réseau NOS (*Network Operating System*) de Novell et des serveurs NetWare. La technologie Novell pose des problèmes d'évolutivité :

- Les serveurs NetWare emploient des paquets broadcast pour s'identifier et annoncer leurs services et routes aux autres réseaux, *via* le protocole SAP (*Service Advertisement Protocol*).
- Les clients NetWare utilisent des diffusions broadcast pour rechercher des serveurs NetWare, *via* des requêtes GNS (*Get Nearest Server*).
- La version 4.0 des applications de gestion de réseau basées sur SNMP de Novell, telle NetExplorer, envoie périodiquement des paquets broadcast afin de découvrir les changements survenus sur le réseau.

Un réseau inactif, avec un seul serveur qui comporte un volume partagé et ne propose aucun service d'impression, génère un paquet broadcast toutes les 4 secondes. Un grand réseau local, avec des serveurs haut de gamme, pourrait comprendre jusqu'à 150 utilisateurs par serveur. Si le réseau comptait 900 utilisateurs assez bien répartis, il pourrait y avoir six ou sept serveurs. Dans un état d'inactivité avec plusieurs volumes et imprimantes partagés, environ quatre diffusions broadcast seraient émises, uniformément réparties. En cas de forte activité, avec des requêtes de route et de service fréquentes, le taux de trafic broadcast atteindrait entre 15 et 20 paquets broadcast par seconde.

La Figure E.2 montre les résultats de tests réalisés par Cisco afin de connaître les effets de la propagation de diffusions broadcast sur un processeur 80386 fonctionnant à une vitesse de 25 MHz. Les performances ont été mesurées avec l'utilitaire Norton Utilities. Le trafic a été généré par un outil de surveillance de réseau. Il se composait d'un paquet broadcast et d'un paquet multicast comportant des zéros en tant que données. Les performances du processeur ont été affectées à partir de 30 paquets broadcast ou multicast par seconde. Les paquets multicast ont un effet un peu plus négatif que les paquets broadcast. Bien que ce test ait été réalisé à l'aide d'une technologie existante, il montre clairement l'impact que peut avoir la propagation de diffusions broadcast sur les équipements du réseau.

Le Tableau E.2 présente le pourcentage moyen de pertes de ressources processeur pour des réseaux Novell, avec de 100 à 10 000 hôtes.

Figure E.2
Effets de la propagation de diffusions broadcast sur les hôtes d'un réseau Novell.

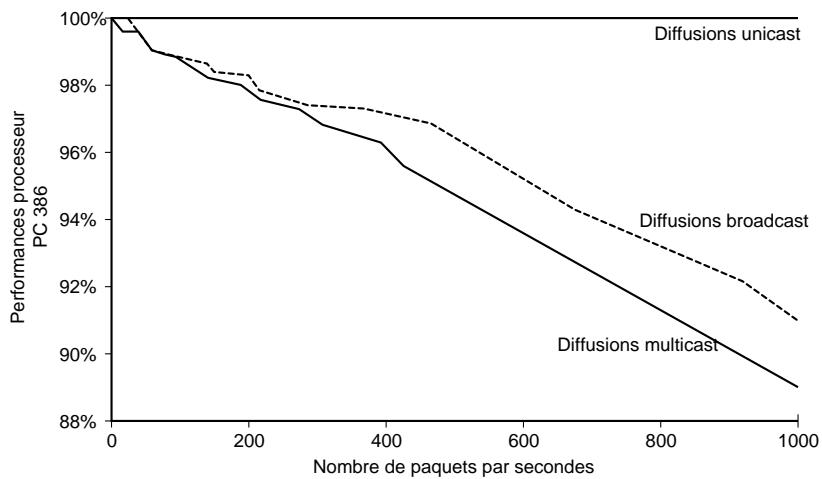


Tableau E.2 : Pertes de ressources processeur dues aux diffusions sur des réseaux Novell

Nombre d'hôtes	Pourcentage moyen de pertes processeur par hôte
100	0,12
1 000	0,22
10 000	3,15

Les résultats présentés au Tableau E.2 correspondent à un fonctionnement moyen du réseau sur plusieurs heures. La charge du trafic et la perte de ressources processeur en cas de pointe, pour chaque station de travail, peuvent dépasser celles d'une utilisation moyenne du réseau. Un scénario courant indique que le lundi à 9 heures, tous les employés allument leur ordinateur. Normalement, lorsque le niveau d'utilisation ou de demande est moyen, le réseau est capable de gérer un nombre raisonnable de stations. Néanmoins, dans des situations où tous les employés émettent une demande de service en même temps (pointe de demandes), la capacité du réseau ne permet de supporter qu'un nombre beaucoup moins important de stations. Le fait de déterminer au préalable les exigences en matière de capacité autorise des pointes de demandes et des temps de pointe plus importants que les exigences de services moyennes.

Réseaux AppleTalk

AppleTalk utilise le multicast de façon intensive pour annoncer ou demander des services, et résoudre des adresses. Au démarrage, un hôte AppleTalk transmet une série de vingt paquets pour résoudre son adresse de réseau (une adresse de nœud AppleTalk de couche 3) et obtenir des informations de "zone" locale. A l'exception du premier paquet, qui est adressé à lui-même, ces fonctions sont assurées par le biais de diffusions multicast AppleTalk.

En ce qui concerne le trafic d'ensemble du réseau, le sélecteur AppleTalk utilise les diffusions broadcast de façon intensive. Le sélecteur est l'interface logicielle qui permet à un utilisateur de sélectionner des services de réseau partagés. Cette interface emploie des diffusions multicast AppleTalk afin de rechercher des serveurs de fichiers, des imprimantes et d'autres services. Lorsqu'un utilisateur ouvre le sélecteur et choisit un type de services (par exemple, une imprimante), il transmet 45 diffusions multicast au rythme d'un paquet par seconde. Si le sélecteur demeure ouvert, il envoie une salve de 5 paquets, selon un intervalle de plus en plus long. S'il demeure ouvert pendant plusieurs minutes, il atteint un délai maximal, et transmet une salve de 5 paquets toutes les 270 secondes. En soi, cela ne pose aucun problème, mais, sur un grand réseau, ces paquets s'ajoutent au trafic total de propagation de diffusions broadcast que chaque hôte doit interpréter, puis supprimer.

D'autres protocoles AppleTalk, tel NBP (*Name Binding Protocol*), qui est utilisé pour lier un client à un serveur, et RDP (*Router Discovery Protocol*), une implémentation de RIP qui est transmise par tous les routeurs et qu'écoulent toutes les stations, utilisent également les diffusions broadcast de façon intensive. Le système qu'il inclut (appelé *AutoRemounter*, et qui fait partie du système d'exploitation Macintosh) utilise également beaucoup les diffusions broadcast.

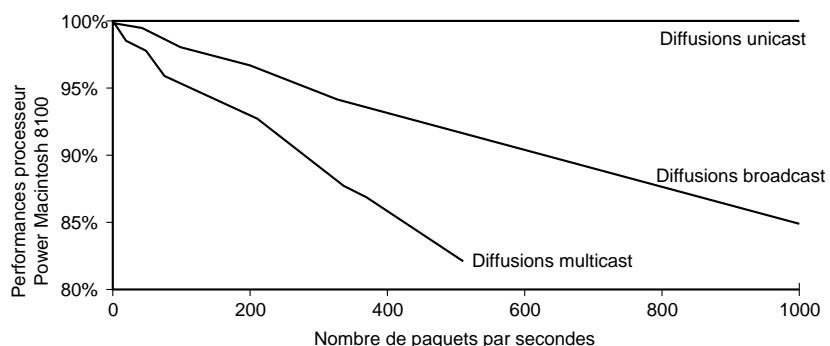
NOTE

La pile AppleTalk est plus efficace que la pile Novell, car elle supprime les diffusions broadcast non AppleTalk plus tôt que la pile Novell ne supprime les diffusions broadcast non Novell.

La Figure E.3 présente les résultats de tests réalisés par Cisco pour connaître les effets de la propagation de diffusions broadcast sur un Power Macintosh 8100 et sur un Macintosh IIci. Les deux processeurs ont été affectés à partir de quinze trames broadcast ou multicast par seconde.

Une fois encore, bien que ce test ait été réalisé à l'aide d'une technologie assez ancienne, il montre clairement l'impact du trafic broadcast.

Figure E.3
Effets de
la propagation de
diffusions broadcast
sur les hôtes d'un
réseau AppleTalk.



Le Tableau E.3 présente le pourcentage moyen de pertes de ressources processeur pour des réseaux AppleTalk, avec 100 à 10 000 hôtes.

Tableau E.3 : Pertes de ressources processeur dues aux diffusions sur des réseaux AppleTalk

<i>Nombre d'hôtes</i>	<i>Pourcentage moyen de pertes processeur par hôte</i>	<i>Pourcentage maximal de pertes processeur par hôte</i>
100	0,28	6,00
1 000	2,10	58,00
10 000	16,94	100,00

Les équipements à connexion lente LocalTalk vers Ethernet constituent un problème majeur sur les grands réseaux AppleTalk. Ils ne fonctionnent pas sur ces réseaux, car la capacité de leur cache ARP est limitée et ne permet de traiter que quelques diffusions broadcast par seconde. Les tempêtes de broadcast les plus importantes surviennent lorsque ces équipements ne sont plus en mesure de recevoir les mises à jour RTMP (*Routing Table Maintenance Protocol*). Dans ces conditions, ils envoient des requêtes ARP à tous les équipements connus, ce qui accélère la dégradation des performances du réseau, car il s'ensuit une défaillance de leurs voisins, qui transmettent à leur tour des requêtes ARP.

Réseaux multiprotocoles

Voici ce que l'on peut dire de l'interaction entre AppleTalk, IPX et IP :

- La pile AppleTalk ignore tout autre protocole de la couche 3.
- Les paquets broadcast et multicast AppleTalk et IP affectent le fonctionnement des piles IP et IPX. Les paquets AppleTalk et IP entrent dans la pile et sont ensuite supprimés, ce qui consomme des ressources processeur.

F

Réduction du trafic SAP sur les réseaux Novell IPX

La quantité de bande passante consommée par les importantes mises à jour SAP (*Service Advertisement Protocol*) est un des facteurs limitatifs dans l'exploitation de grands réseaux Novell IPX (*Internetwork Packet Exchange*). Les serveurs Novell envoient périodiquement aux clients des informations sur les services qu'ils proposent : ils les diffusent sur leurs interfaces de réseau local (LAN) ou de réseau étendu (WAN). Les routeurs sont nécessaires à la propagation des mises à jour SAP sur un réseau IPX ; ainsi tous les clients peuvent lire les messages de services. Il est possible de réduire le trafic SAP sur ces réseaux grâce aux moyens suivants :

- **Filtrage de mises à jour SAP au moyen de listes d'accès.** Les mises à jour SAP peuvent être filtrées en empêchant les routeurs d'annoncer les services de certains serveurs Novell spécifiés.
- **Configuration de routeurs Cisco sur les réseaux Novell IPX pour l'exécution de EIGRP.** Bien que les filtres fournissent un moyen *d'éliminer* les annonces de services spécifiques, EIGRP fournit des mises à jour SAP *incrémentielles* pour bénéficier d'une granularité de contrôle plus fine. Des mises à jour SAP complètes sont envoyées périodiquement sur chaque interface jusqu'à ce qu'un voisin EIGRP IPX soit trouvé. Ensuite, elles ne sont envoyées que lorsqu'il y a des *changements* dans la table SAP. De cette manière, la bande passante est préservée et les annonces de services sont réduites sans être éliminées.

Les mises à jour SAP incrémentielles sont automatiques sur les interfaces série ; elles peuvent être configurées sur les médias de LAN. EIGRP fournit également des mises à jour de routage partielles et la convergence rapide pour les réseaux IPX. Les administrateurs peuvent choisir d'exécuter seulement les mises à jour SAP partielles, ou d'exploiter à la fois le protocole SAP fiable et une portion des mises à jour de routage partielles de EIGRP.

- **Configuration des routeurs Cisco sur les réseaux Novell IPX pour l'envoi de mises à jour SAP incrémentielles.** Avec la version 10.0 du logiciel System Software, les mises à jour SAP incrémentielles déjà décrites peuvent être configurées pour les routeurs Cisco sur les réseaux Novell IPX, et ce, *sans* devoir recourir à l'exécution de la fonction de mise à jour d'informations de routage de EIGRP (seules les mises à jour SAP partielles sont activées). Cette fonction est

supportée sur tous les types d'interfaces. Encore une fois, les mises à jour SAP ne sont envoyées que lorsque des changements se produisent sur un réseau. Seules les modifications dans les tables SAP sont envoyées comme mises à jour.

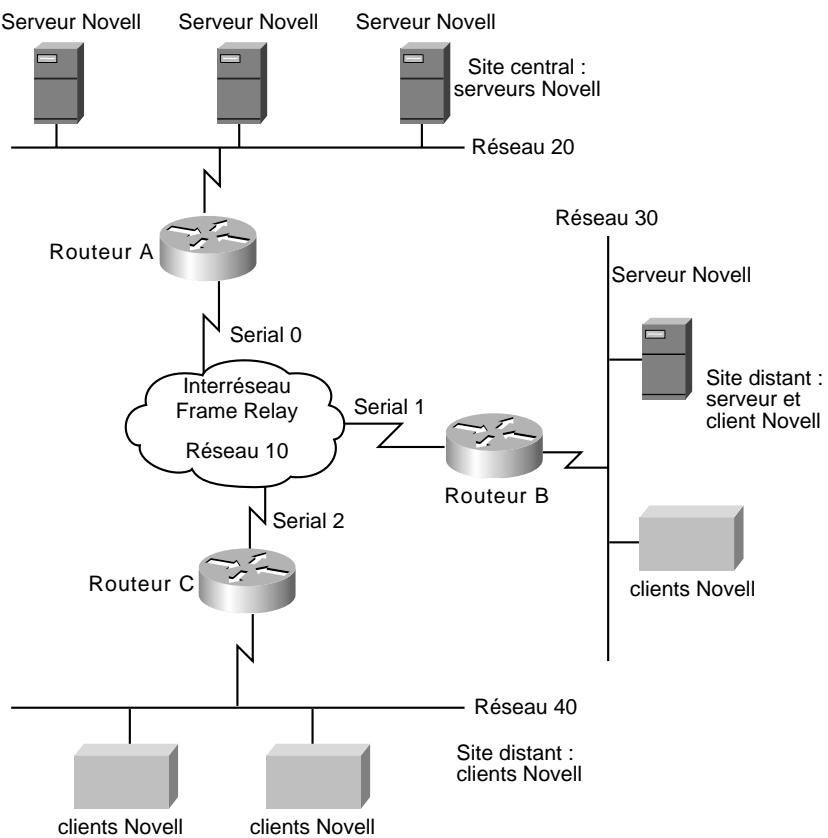
Pour illustrer la façon de réduire le trafic SAP, cette étude de cas est divisée en deux parties :

- la configuration des listes d'accès pour filtrer les mises à jour SAP ;
- la configuration des mises à jour SAP incrémentielles.

Le réseau pour cette étude de cas est illustré à la Figure F.1. Les parties suivantes d'un réseau Novell IPX de grande taille s'étendant sur un WAN Frame Relay sont examinées :

- Le routeur A se connecte à partir du réseau Frame Relay vers le site central avec trois serveurs Novell.
- Le routeur B se connecte à partir du réseau Frame Relay vers un site distant avec un client Novell et un serveur Novell.
- Le routeur C se connecte à partir du réseau Frame Relay vers un site distant avec deux clients Novell.

Figure F.1
Interréseau
Novell IPX étendu.



Listes d'accès de filtrage des mises à jour SAP

Les listes d'accès peuvent contrôler les routeurs qui doivent envoyer ou recevoir des mises à jour SAP et ceux qui ne le font pas. Elles peuvent être définies pour filtrer les mises à jour SAP en s'appuyant sur l'adresse de réseau source d'une entrée SAP, sur le type de l'entrée SAP (serveurs de fichiers, serveurs d'impression, etc.) et sur le nom du serveur SAP. Elles sont constituées d'entrées respectant le format suivant :

```
access-list n [deny|permit] réseau[ .noeud] [type-de-service [nom-serveur]]
```

où *n* est une valeur de l'intervalle 1000 à 1099. Une adresse de réseau -1 signifie n'importe quel réseau, et un type de service 0 indique n'importe quel service. Par exemple, la liste d'accès suivante accepte les entrées SAP de serveur d'impression du serveur PRINTER_1, tous les serveurs de fichiers, et toutes les autres entrées SAP du réseau 123, à l'exception de celles d'un serveur appelé UNTRUSTED. Toutes les autres entrées SAP doivent être ignorées :

```
access-list 1000 permit -1 47 PRINTER_1
access-list 1000 permit -1 4
access-list 1000 deny 123 0 UNTRUSTED
access-list 1000 permit 123
```

Lors de la vérification des entrées dans une mise à jour SAP, toutes les instructions d'une liste d'accès sont traitées dans l'ordre, et s'il n'y a pas de correspondance pour une entrée SAP, elle n'est pas acceptée. Aussi, pour bloquer le serveur UNTRUSTED, l'instruction **deny** doit être placée avant l'instruction **permit** pour tous les autres dispositifs de réseau 123.

Deux techniques peuvent être utilisées pour le filtrage : les entrées SAP qui sont requises peuvent être autorisées et les autres rejetées : les entrées SAP non souhaitées peuvent être rejetées et les autres autorisées. En général, la première méthode est préférée, car elle évite que les nouveaux services inattendus soient propagés à travers le réseau.

La forme de filtrage SAP la plus courante sert à limiter les services disponibles sur un réseau étendu. Par exemple, il est abnormal pour les clients d'un site de pouvoir accéder au serveur d'impression d'un autre site, car il s'agit plutôt d'une opération locale. Dans cette étude de cas, seuls les serveurs de fichiers pourront être vus à travers le réseau étendu.

Site central

Le routeur est connecté au site central. Les listes d'accès suivantes configurées sur le routeur autorisent tout, sauf aux serveurs d'impression d'être annoncés sur l'interface série.

```
access-list 1000 deny -1 47
access-list 1000 permit -1
!
interface serial 0
ipx network 10
ipx output-sap-filter 1000
```

Pour autoriser uniquement les serveurs de fichiers IPX, et rejeter tous les autres serveurs IPX, servez-vous de la configuration suivante :

```
access-list 1000 permit -1 4
!
interface serial 0
ipx network 10
ipx out-sap-filter 1000
```

Sites distants

Cette section fournit des informations relatives à la configuration des routeurs sur les sites distants :

- Le routeur B est connecté à un serveur et à un client IPX.
- Le routeur C est connecté à deux clients IPX.

Serveur et client IPX

Pour le routeur B, les listes d'accès suivantes autorisent tout, sauf aux serveurs d'impression d'être annoncés sur l'interface série.

```
access-list 1000 deny -1 47
access-list 1000 permit -1
!
interface serial 1
ipx network 10
ipx output-sap-filter 1000
```

Pour n'autoriser que les serveurs de fichiers IPX, et rejeter tous les autres types de serveurs IPX, servez-vous de la configuration suivante :

```
access-list 1000 permit -1 4
!
interface serial 1
ipx network 10
ipx out-sap-filter 1000
```

Client IPX

Le routeur C ne requiert pas la configuration d'une liste d'accès, car le site distant ne possède pas de serveur. Seuls les serveurs Novell génèrent des mises à jour SAP.

Mises à jour SAP incrémentielles

Les mises à jour SAP incrémentielles autorisent une connectivité *any-to-any* avec une surcharge de réseau SAP réduite. Au lieu d'éliminer totalement la réception des mises à jour SAP, tous les services IPX nécessaires peuvent être diffusés vers les sites distants, mais uniquement lorsque des changements se sont produits dans les tables SAP.

Site central

Pour configurer l'envoi des mises à jour SAP EIGRP encapsulées sur une base incrémentielle, utilisez la configuration ci-dessous. Bien que le numéro du système autonome EIGRP défini soit 999, le routage EIGRP (et les mises à jour de routage) n'est pas effectué, car le mot clé **rsup-only** est utilisé avec la commande **ipx sap-incremental**. Ce mot clé indique une mise à jour SAP fiable.

```
interface ethernet 0
ipx network 20
!
interface serial 0
ipx network 10
ipx sap-incremental eigrp 999 rsup-only
!
ipx router eigrp 999
network 10
```

Pour configurer à la fois les mises à jour SAP incrémentielles et le routage EIGRP, configurez simplement EIGRP avec les commandes suivantes :

```
interface ethernet 0
ipx network 20
!
interface serial 0
ipx network 10
!
ipx router eigrp 999
network 10
```

Sites distants

Cette section procure des informations relatives à la configuration de routeurs sur des sites distants :

- Le routeur B est connecté à un serveur et à un client IPX.
- Le routeur C est connecté à deux clients IPX.

Serveur et client IPX

Pour configurer l'envoi des mises à jour SAP EIGRP encapsulées uniquement sur une base incrémentielle, utilisez la configuration ci-dessous pour le routeur B. Bien que le numéro du système autonome EIGRP défini soit 999, le routage EIGRP n'est pas effectué, car le mot clé **rsup-only** est utilisé avec la commande **ipx sap-incremental**.

```
interface ethernet 1
ipx network 30
!
interface serial 1
ipx network 10
ipx sap-incremental eigrp 999 rsup-only
!
ipx router eigrp 999
network 10
```

Pour configurer à la fois les mises à jour SAP incrémentielles et le routage EIGRP, configurez simplement EIGRP avec les commandes suivantes :

```
interface ethernet 1
ipx network 30
!
interface serial 1
ipx network 10
!
ipx router eigrp 999
network 10
```

Clients IPX

Pour configurer l'envoi des mises à jour SAP EIGRP encapsulées uniquement sur une base incrémentielle, utilisez la configuration suivante pour le routeur C :

```
interface se ethernet 2
ipx network 40
!
interface serial 2
ipx network 10
```

```
ipx sap-incremental eigrp 999 rsup-only
!
ipx router eigrp 999
network 10
```

Même s'il n'y a pas de serveurs, ces commandes de configuration sont requises pour supporter les mises à jour SAP incrémentielles annoncées à partir du site central et d'autres sites distants vers le routeur C.

Résumé

Cette étude de cas illustre deux méthodes pour réduire le trafic SAP sur les réseaux Novell IPX : l'emploi de listes d'accès pour éliminer les annonces de services spécifiques ; l'utilisation de la fonction de mises à jour SAP incrémentielles pour échanger des modifications SAP lorsqu'elles se produisent. Cette technique élimine les mises à jour SAP périodiques.

G

Introduction au transport de la voix en paquets

De tous les outils technologiques, le téléphone est sans doute celui qui a bénéficié de la plus grande percée, en particulier dans les entreprises. Celles-ci établissent chaque jour des milliers d'appels et si le coût d'un seul appel est négligeable, le total des frais de l'ensemble des communications est significatif.

Pour un grand nombre de sociétés, une partie de ce coût pourrait être évitée. Le système téléphonique public traditionnel est une combinaison complexe de tarifs et de subsides, provoquant bien souvent des situations dans lesquelles un appel de "A" vers "B" coûte une fraction du tarif d'un appel de "B" vers "A". Les entreprises se sont appuyées depuis longtemps sur des réseaux privés de lignes louées pour contourner les frais téléphoniques publics, mais les tarifs appliqués à ces liaisons sont souvent élevés. Un grand nombre d'entre elles ont alors cherché des stratégies de remplacement.

Sur les réseaux, il existe aujourd'hui plusieurs alternatives à la téléphonie classique et aux liaisons louées. Parmi les plus intéressantes, on trouve des technologies de réseau se basant sur un type différent de transmission de la voix appelées *voix en paquets*. La voix en paquets apparaît comme des données sur un réseau et peut par conséquent être transportée sur des liaisons de réseaux normalement réservées pour les données où les coûts sont bien inférieurs.

Comme la voix en paquets utilise moins de bande passante qu'un système téléphonique traditionnel, davantage de signaux peuvent être transportés sur une connexion donnée. Là où la téléphonie standard nécessitait 64 000 bit/s, les besoins de la voix en paquets se situent au-dessous de 10 000 bit/s. Pour de nombreuses entreprises, il existe suffisamment de capacités en réserve sur les réseaux de données nationaux et internationaux pour pouvoir transmettre une grande quantité de trafic voix à un coût très faible ou quasiment nul.

Même si, dans certaines situations, de nouvelles ressources de transport doivent être ajoutées ou acquises pour supporter la voix en paquets, les bénéfices obtenus justifient l'investissement. Le réseau

téléphonique public impose souvent des tarifs basés sur la distance et des frais supplémentaires pour subventionner les appels résidentiels. L'emploi de réseaux de données pour transporter la voix, lorsqu'une telle utilisation n'est pas contraire à la loi, peut éliminer ces coûts. Même dans les situations où aucune économie ne pourrait être attendue au niveau de la tarification, la voix en paquets reste vingt fois — voire davantage — plus efficace qu'un transport traditionnel numérique de la voix à 64 Kbit/s en matière d'exploitation de la bande passante.

Comme toutes les bonnes choses, la voix en paquets a un prix. Bien que les concepteurs de réseaux soient familiarisés avec les exigences de qualité de service (QoS) des applications de données spécialisées telles que le traitement de transactions en ligne, la voix en paquets s'accompagne souvent de besoins encore plus stricts. Si le réseau n'est pas correctement préparé pour satisfaire à ces exigences, il peut en résulter une détérioration de la qualité de la communication. Ceci est particulièrement vrai si la voix est transportée sur des réseaux de données publics tels que l'Internet, où les utilisateurs de la voix disposent de peu d'options pour obtenir une qualité de service de bout en bout.

En dépit de ces problèmes de qualité de service, la voix en paquets jouit d'un élan de popularité en raison des économies potentielles importantes pouvant être réalisées. Même aux Etats-Unis, où les coûts de télécommunications sont faibles à côté des standards internationaux, les entreprises peuvent obtenir un coût par minute ne représentant que la moitié ou le tiers de celui de la téléphonie, même sur des réseaux privés virtuels (VPN). Les sociétés générant des frais de communication importants se doivent de considérer toutes les options de transport de la voix par paquets.

Malheureusement pour les utilisateurs potentiels de cette technologie, il existe peu de textes informatifs sur ce concept, et lorsqu'ils existent, ils sont plutôt orientés sur les intérêts des entreprises. Par conséquent, Cisco propose, dans cette annexe, une exploration de cette technologie.

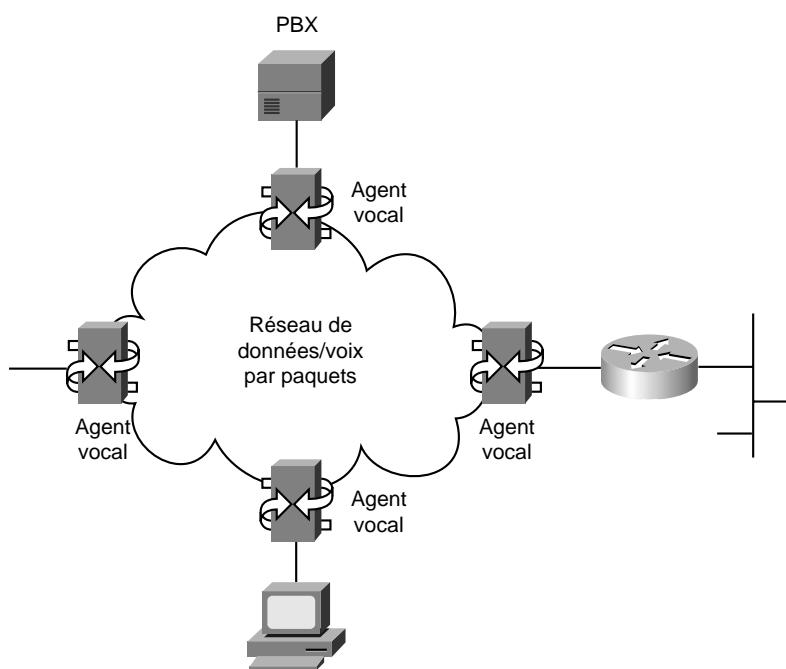
Introduction

Tous les systèmes de voix en paquets suivent un modèle commun, comme illustré dans la Figure G.1. Le réseau de transport de la voix par paquets, qui peut se baser sur IP, Frame Relay, ou ATM, forme le "nuage" traditionnel. Aux frontières de ce réseau, il existe des équipements ou des composants que l'on peut appeler "agents vocaux". Leur mission est de modifier l'information vocale de sa forme traditionnelle en téléphonie vers une forme adaptée à la transmission par paquets. Le réseau transmet ensuite les paquets à un agent vocal servant la destination ou l'interlocuteur appelé.

Ce modèle de connexion par agents vocaux soulève deux problèmes qui doivent être considérés pour garantir que ce service satisfera aux exigences de l'utilisateur. Le premier problème est le codage de la voix — la façon dont les informations vocales sont transformées en paquets, et comment ceux-ci sont utilisés ensuite pour recréer la voix. Le second problème est la signalisation associée à l'identification de l'interlocuteur appelé et de son emplacement sur le réseau. Les sections qui suivent étudient davantage ces questions.

Figure G.1

Modèle de transport de la voix par paquets.



Codage de la voix

La parole humaine, et tout ce que nous entendons, se présente naturellement sous une forme analogique. Les premiers systèmes téléphoniques fonctionnaient aussi sous cette forme. Les signaux analogiques sont souvent illustrés sous forme d'ondes sinusoïdales, mais la voix ou d'autres signaux contiennent de nombreuses fréquences et possèdent des structures plus complexes.

Bien que les humains soient "équipés" pour les communications analogiques, cette forme de transmission n'est pas particulièrement efficace. Lorsque les signaux s'affaiblissent, en raison de pertes dans la transmission, il est difficile de différencier la structure complexe du signal analogique de celle des bruits aléatoires de la transmission. L'amplification des signaux analogiques entraîne aussi une augmentation du bruit, ce qui rend les connexions analogiques trop bruyantes à l'usage.

Les signaux numériques, qui ne disposent que de deux états (0 et 1), sont plus facilement différenciés du bruit et peuvent être amplifiés sans provoquer d'altération. Peu à peu, on s'est aperçu que le codage numérique était mieux protégé contre l'altération par le bruit sur les connexions interurbaines, et les systèmes de communications mondiaux se sont tournés vers un format de transmission numérique appelé PCM (*Pulse Code Modulation*) ou MIC (*Modulation par impulsion et codage*).

PCM convertit la voix dans un format numérique en échantillonnant les signaux vocaux 8 000 fois par seconde et en transformant chaque échantillon en un code. Ce taux d'échantillonnage de 8 000 fois par seconde (125 microsecondes entre les échantillons) a été choisi car tous les échanges de parole sont essentiellement transportés à des fréquences inférieures à 4 000 Hz (ou 4 kHz). Un échantillonnage des formes d'ondes vocales toutes les 125 microsecondes est suffisant pour détecter des fréquences inférieures à 4 kHz.

Après que l'onde de forme ait été échantillonnée, les échantillons sont convertis dans un format numérique avec un code représentant l'amplitude de l'onde de forme au moment où l'échantillon a été enregistré. Le codage PCM du système téléphonique standard utilise 8 bits pour le code et consomme par conséquent 64000 bit/s. Un autre standard de codage téléphonique, appelé ADPCM (*Adaptive Differential PCM*, codage MIC différentiel adaptif), code la voix en valeurs de 4 bits et ne consomme donc que 32000 bit/s. Ce codage est souvent utilisé sur les connexions interurbaines.

Dans les applications traditionnelles de téléphonie, les standards PCM ou ADPCM sont utilisés sur des canaux numériques synchrones, ce qui signifie qu'un flux constant de bits est généré à un rythme spécifique, qu'il y ait ou non des paroles échangées. Il existe en fait des centaines de brèves périodes de silence au cours d'une conversation téléphonique moyenne, et chacune d'elles gaspille de la bande passante et entraîne un coût. Avec les connexions téléphoniques standard, il n'y a aucun remède à ce gaspillage.

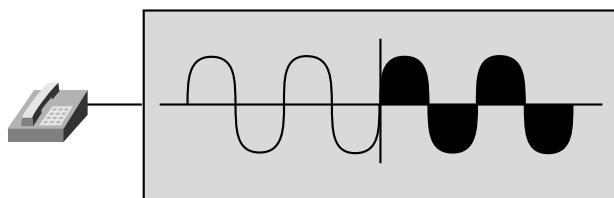
Le transport de la voix en paquets offre une alternative. Dans les applications basées sur cette technologie, les paquets ne sont générés que s'il y a réellement des informations vocales à transmettre. L'élimination de la bande passante perdue lors des périodes de silence réduit du même coup d'un tiers ou plus la bande passante effective requise pour le transport.

Standards de codage de la voix

D'autres stratégies peuvent même réduire davantage les exigences en bande passante. L'UIT (*Union Internationale du Téléphone*) a défini une série de standards pour le codage de la voix, incluant les codages PCM et ADPCM à 64 et 32 Kbit/s introduits plus haut. Une bonne connaissance des caractéristiques et des stratégies de ces différents standards est tout indiquée avant d'envisager la transmission de la voix par paquet.

Le premier groupe de ces standards fait appel à "l'échantillonnage fixe", et appartient à la famille G.711. Ils utilisent la stratégie de 8 000 échantillons par seconde du codage décrit précédemment. Pour chaque échantillon, le codage stocke l'amplitude du signal au moment du prélèvement. Le résultat de l'échantillonnage est une représentation approximative en blocs du signal vocal original, comme illustré Figure G.2. Les échantillons peuvent ensuite être utilisés (par lissage) pour reconstruire le signal vocal analogique sur l'autre extrémité de la communication.

Figure G.2
Modulation PCM (ou MIC).



Le problème avec les stratégies d'échantillonnage est que pour réduire la bande passante utilisée pour transporter la parole numérique, il est nécessaire de coder les signaux avec moins de bits. L'utilisation de 8 bits pour un échantillon permet de reconnaître 256 niveaux différents d'amplitude. Pour réduire la bande passante à 32 Kbit/s, seuls 4 bits (64 valeurs) sont utilisés, et la valeur

binnaire représente le changement par rapport à la valeur précédente (c'est le sens du terme "différentiel" dans le codage ADPCM). ADPCM peut être réduit à 16 Kbit/s en n'utilisant que 2 bits (4 valeurs), mais à chaque fois que le nombre de valeurs d'amplitude différentes est réduit, la représentation en blocs créée ne ressemble pas au signal original et il s'ensuit une dégradation de la qualité.

Un deuxième groupe de standards fournit une meilleure compression de la voix et du même coup une meilleure qualité. Dans ces standards, le codage de la voix utilise un algorithme spécial — appelé LPC (*Linear Predictive Code*, codage linéaire prédictif) — qui modélise le fonctionnement de la parole humaine. Comme cet algorithme peut tirer parti de la compréhension du processus d'élocution, il peut être plus efficace sans sacrifier la qualité de la voix. La plupart des équipements utilisant ce codage reçoivent en entrée le codage PCM à 64 Kbit/s présenté plus haut, pour deux raisons :

- Cette forme de voix représente la sortie standard des autocommutateurs privés et des commutateurs téléphoniques.
- Les puces de codage PCM sont peu coûteuses en raison de leur usage répandu sur les réseaux téléphoniques.

Le codage LPC et PCM/ADPCM des informations vocales est standardisé par l'UIT dans ses recommandations de la série G. Les standards de codage les plus populaires pour la téléphonie et la voix par paquets comprennent les familles suivantes :

- G.711, qui décrit le codage vocal PCM à 64 Kbit/s. Les signaux ainsi codés sont déjà dans le format approprié pour le transport numérique sur le réseau téléphonique public ou par l'intermédiaire des autocommutateurs privés.
- G.726, qui décrit le codage ADPCM à 40, 32, 24, et 16 Kbit/s. Le codage ADPCM peut également être échangé entre les réseaux par paquets et ceux du système téléphonique et d'autocommutateurs privés, à condition que ces derniers possèdent des fonctions ADPCM.
- G.728, qui décrit la compression vocale CELP (*Code-Excited Linear Predictive*, codage prédictif avec excitation algébrique), ne requérant que 16 Kbit/s de bande passante. Ce codage doit être transformé dans le format de téléphonie publique pour être transporté vers ou par l'intermédiaire de réseaux téléphoniques.
- G.729, qui décrit le codage CELP adaptif permettant à la voix d'être codée en flux de 8 Kbit/s. Ce standard existe sous deux formes et toutes deux fournissent une qualité de parole équivalente à celle du codage ADPCM à 32 Kbit/s.
- G.733.1, qui décrit une représentation codée pouvant être utilisée pour compresser la parole ou d'autres composants de signaux audio de services multimédias à un très faible taux binaire dans le cadre de la famille générale de standards H.324. Ce codeur possède deux taux binaires de codage : 5,3 et 6,3 Kbit/s. Le taux le plus élevé produit une meilleure qualité, mais le plus faible fournit une bonne qualité et met davantage de souplesse à la disposition des concepteurs de systèmes.

Qualité de compression

On peut se demander pourquoi la voix compressée ne serait pas simplement un concept de standard. Et si elle n'était pas compressée ? La réponse est que la compression ne peut qu'approcher l'onde de forme analogique. Bien que cette approximation puisse être très bonne dans le cas de certains standards, tels que G.729, d'autres standards souffrent quelque peu de la distorsion de cette approximation de compression, tout particulièrement si la voix subit plusieurs phases successives de codage : tout d'abord dans une forme numérique, puis dans une forme analogique, et à nouveau en numérique. Ces codages en tandem devraient être évités autant que possible dans les systèmes de transport de la voix compressée.

La qualité de la voix selon la stratégie de compression a été mesurée par une étude, MOS (*Mean Opinion Score*), qui représente la référence la plus courante. Sur l'échelle MOS, où 0 désigne une mauvaise qualité et 5 une qualité excellente, le standard PCM possède une qualité d'environ 4,4. Le standard G.726 ADPCM est évalué par une qualité de 4,2 pour la version 32 Kbit/s.

Le codage G.728 CELP atteint une qualité de 4,2, tout comme G.729. Comme le montrent ces chiffres, les codeurs de voix du modèle linéaire prédictif plus modernes obtiennent de meilleurs résultats que leurs homologues plus anciens basés sur l'échantillonnage.

Délai

Un autre facteur, le délai, peut avoir un impact important sur la qualité de la voix compressée. La compression de la voix pour le transport par paquets entraîne un délai. Le Tableau G.1, illustre le délai moyen associé à chacun des standards de codage décrits plus haut. Comme vous pouvez le constater, le délai associé avec le codage/décodage de la voix peut atteindre 25 ms pour deux échantillons CS-ACELP (un délai initial de 5 ms plus 20 ms pour les deux trames de 10 octets). Ce délai n'affecte pas en lui-même la qualité de la parole, bien qu'il puisse nécessiter un recours à l'annulation d'écho pour éviter la formation d'un effet de réverbération indésirable. La plupart des dispositifs de compression de la voix pour le transport par paquets incluent une forme quelconque d'annulation d'écho. Mais d'autres sources de délai sur le réseau viennent s'ajouter à ce délai de base du codage, et entraînent un retard suffisant sur la totalité de la transmission de bout en bout pour interférer avec la parole.

Tableau G.1 : Délai moyen associé aux standards de codage les plus connus

Méthode	Résultat MOS	Délai (ms)
PCM (G.711)	4,4	0,75
ADPCM 32 Kbit/s (G.726)	4,2	1
LD-CELP 16 Kbit/s (G.728)	4,2	3-5
CS-ACELP 8 Kbit/s (G.729)	4,2	10
CS-ACELP Kbit/s (G.729a)	4,2	10
MPMLG 6,3 Kbit/s (G.723.1)	3,98	30
ACLEP 5,3 Kbit/s (G.723.1)	3,5	30

Les réseaux téléphoniques traditionnels et les réseaux pour la voix en paquets sont confrontés à deux types de délais : le délai de propagation et le délai de traitement. Le premier est provoqué par la limitation de la vitesse de la lumière sur les réseaux à fibre optique ou à micro-ondes, ou de celle des électrons sur les réseaux de cuivre. Le deuxième délai est lié au traitement de la voix sur les équipements le long de l'itinéraire.

La lumière voyage à une vitesse de 300 000 km/s, et les électrons circulent à une vitesse avoisinant 160 000 km/s dans un conducteur en cuivre. Un réseau à micro-ondes ou à fibre optique s'étendant sur la moitié du globe couvrirait environ 20 000 km et entraînerait un délai dans une direction d'environ 70 ms. Ce niveau de retard n'est presque pas perceptible et ne représente jamais un problème.

Les délais de traitement peuvent influer négativement sur les réseaux traditionnels de transport de la voix. Chaque trame T1/41/J1 requiert 125 ms pour être assemblée dans un commutateur et routée vers la ligne de destination, en supposant que chaque trame est envoyée à sa vitesse native (1 544 ou 2 048 Mbit/s). Ce délai de sérialisation s'accumule à mesure que les trames sont traitées à travers le réseau. Le délai total de sérialisation peut atteindre 20 ms, voire plus, sur des liaisons transcontinentales. Lorsqu'il est ajouté au délai de propagation, le délai de sérialisation peut provoquer un délai dans une direction avoisinant les 100 ms, ce qui est perceptible mais admissible.

C'est dans le délai de traitement que les réseaux de voix en paquets et les réseaux traditionnels commencent à afficher leurs différences. Les délais de traitement sur les réseaux de données peuvent être considérables, tout particulièrement lorsqu'il se produit des phénomènes de congestion et que le trafic doit être placé en file d'attente de transmission sur des lignes de tronçons fortement encombrées. Sur l'Internet, des délais de bout en bout sur des routes internationales avoisinent parfois une seconde. Lorsque de tels délais apparaissent, les interlocuteurs ont comme recours de s'appuyer sur une structure formelle de conversation : en parlant à tour de rôle, ils risqueront moins de prendre simultanément la parole à un moment où le délai de transmission génère une période de silence.

La raison pour laquelle le délai sur les réseaux de données peut représenter un problème pour la qualité de la voix est que les informations locales possèdent un "timing" caractéristique. Une syllabe particulière est prononcée dans un intervalle de temps précédant le début de la syllabe suivante. Cette petite pause faisant partie de l'élocution comme de l'expression, son timing doit être préservé. Sur les réseaux téléphoniques traditionnels, le canal de la voix est un flux binaire synchronisé qui préserve précisément le timing de tous les éléments d'élocution. Sur les réseaux de données, un délai variable peut être introduit suite à la congestion ou au traitement des informations et peut altérer la qualité de la parole.

Après ces explications, il apparaît comme évident que le problème posé par le délai se présente en fait sous deux formes : le délai absolu, qui peut gêner la conversation et le rythme des échanges ; et les variations de délai appelées la *gigue*, qui créent des pauses inattendues entre les prononciations et peuvent influer négativement sur l'intelligibilité du dialogue. C'est le problème le plus important auquel les réseaux de transports de la voix par paquets doivent répondre.

L'élimination de la gigue sur un réseau avec des délais de traitement et de congestion variables est confiée à la fonction de retenue. Les applications vocales mesurent le délai moyen d'un réseau et retiennent sur l'agent vocal de destination suffisamment de données vocales compressées pour compenser le délai moyen de la gigue. Cette fonction garantit que les paquets sont libérés pour être

convertis en signaux vocaux analogiques à un débit constant, indépendamment des variations de délai rencontrées sur le réseau. La retenue provoque bien sûr un délai absolu supérieur, et les réseaux sur lesquels la gigue est significative subiront un délai total suffisamment élevé pour être perceptible par les interlocuteurs.

Lorsque la fonction de tampon de retenue est utilisée pour contrôler la gigue, il est souvent nécessaire de fournir une estampille de temps sur chaque paquet de données vocales pour s'assurer qu'il soit libéré sur la destination avec le même timing que les autres éléments vocaux trouvés sur le signal vocal en entrée. Avec la voix sur IP par exemple, ce type d'estampille est fourni par le protocole RTP (*Real-Time Protocol*).

Par conséquent, tout ce qui influe sur le délai de traversée du réseau peut également avoir une influence sur les performances de transport de la voix. Cette constatation est critique pour la conception des réseaux se destinant à la voix par paquets. Dans les applications de gestion de la voix par paquets, on préfère normalement risquer la perte ou l'altération d'un paquet qu'introduire une stratégie de récupération d'erreur qui augmenterait la gigue. C'est la raison pour laquelle les protocoles de transport de la voix par paquets ne comportent presque jamais de fonction de récupération d'erreur.

En résumé, le codage de la voix pour le transport par paquets a un double impact positif sur les coûts d'exploitation d'un réseau : d'abord en réduisant la bande passante consommée par le trafic vocal, et ensuite en éliminant les périodes de silence. Pour tirer parti de ces avantages, le réseau de transport sous-jacent doit être capable de supporter des flux de trafic de faible bande passante et d'intercaler d'autres trafics durant les périodes de silence des conversations, afin d'exploiter la bande passante inactive produite par le transport de la voix en paquets. Les services fournis pour assurer ces fonctions varient selon le type de réseau.

Options et problèmes du transport de la voix par paquets

A la lumière de la section précédente sur la compression vocale, il est clair que le couplage de plusieurs phases de codage, le délai et la perte de synchronisation de timing, sont les problèmes les plus sérieux que rencontrent les réseaux de transport de la voix par paquets. Bien qu'ils soient tous confrontés à ces mêmes problèmes, les solutions qui leur sont offertes sont différentes selon les cas, et la conception des applications associées doit prendre en compte la technologie de transport avant de décider de la façon de traiter ces problèmes de délai ou de perte.

La voix en paquets peut être transportée sur tous les types de connexions de réseaux étendus suivants :

- Les réseaux de lignes louées à circuits commutés. Ils sont souvent basés sur des liaisons T1/E1/J1 louées auprès de transporteurs fournissant une bande passante synchrone fixe.
- Les connexions ATM à débit constant ou à émulation de circuits. Elles émulent les connexions du réseau à commutation de circuits et sont parfois appelées services ATM Classe A.
- Les connexions ATM basées sur les classes de services à débit variable (VBR), à débit possible (ABR), ou à débit non spécifié (UBR).
- Les réseaux Frame Relay, à la fois ceux fournis par les fournisseurs de service public et ceux de réseaux privés élaborés par les entreprises.

- Les réseaux de paquets publics (X.25), qui assurent des services de données publics dans de nombreuses applications internationales et qui sont aussi utilisés comme réseaux de données nationaux en Europe et en bordure du Pacifique.
- Les réseaux IP publics, y compris l'Internet.
- Les réseaux de données privés d'entreprises de tous types.

Ces nombreux choix peuvent heureusement être groupés en larges catégories pour étudier les applications vocales.

Réseaux synchrones à circuits commutés

Les technologies de circuits commutés synchrones, telles que les réseaux de lignes louées ou les réseaux ATM à débit constant (CBR), fournissent les mêmes fonctions de transport que les réseaux téléphoniques standards et ne présentent par conséquent pas de risques spéciaux de détérioration de la qualité de la parole ou de délais de livraison. Si le nuage dans la Figure G.1 est constitué par un tel réseau, la voix est transportée par un système de téléphonie normal et aucune fonction d'agent vocal spéciale n'est nécessaire sur le réseau, excepté pour réaliser des appels comme le ferait les réseaux téléphoniques ou les réseaux d'autocommutateurs privés.

La plupart des réseaux privés nationaux et internationaux se basent sur une technologie de réseaux à circuits commutés que le trafic voix traverse à l'intérieur de tranches de temps à bande passante fixe. Cette méthode de transmission, bien qu'équivalente à celle utilisée dans la téléphonie publique, gaspille de la bande passante pour les raisons déjà étudiées plus haut. Si le codage de la voix en paquets est utilisé sur les connexions à circuits commutés, les seuls bénéfices qui peuvent être obtenus sont ceux associés au faible débit binaire (par exemple 8 Kbit/s pour G.729), et ils dépendent de la capacité du réseau à allouer des tranches de temps inférieures à 64 Kbit/s par une technique de multiplexage appelée *Subrate Multiplexing*.

Sur les réseaux ATM, il est particulièrement important de s'assurer que les services de débit constant puissent supporter des connexions de 32, 16, ou 8 Kbit/s. De nombreux réseaux ATM fournissent ces types de connexions uniquement pour des débits à 64 Kbit/s car les standards promulgués en 1997 par l'ATM Forum pour la voix sur ATM ont spécifié le codage G.711. Les efforts pour tenter de réaliser des économies au moyen de la compression de la voix sur une bande passante plus faible seraient alors investis en vain.

Réseaux de trames/cellules

Les réseaux de trames/cellules utilisant le Frame Relay ou les services de débit variable d'ATM, transportent la voix sous une forme codée compressée. Pour ces réseaux, il est nécessaire de recourir à un agent vocal pour coder la voix dans des cellules ou des trames pour le transport, puis décoder ces dernières sur la destination. L'agent vocal doit également comprendre n'importe quelle signalisation téléphonique utilisée par la source et la destination afin de pouvoir recevoir le numéro de l'interlocuteur à appeler et émettre des signaux de progression d'appel. Finalement, il peut aussi avoir besoin de comprendre la signalisation ou l'adressage requis dans le nuage du réseau de trames/cellules pour atteindre les divers agents vocaux de destination. Cette fonction est importante lors de la traduction intervenant entre les réseaux traditionnels pour la voix et un réseau de trames/cellules.

Sur les réseaux Frame Relay ou ATM, le délai et la gigue sont souvent contrôlés par les commutateurs eux-mêmes, si chacun des commutateurs et des points finaux est synchronisé par rapport à une source commune reconnaissable sur le réseau. Normalement, la gigue sur ces réseaux est tellement faible que le timing des paquets de données voix en sortie avoisine celui de la parole en entrée, et aucune estampille de temps spéciale ne doit être appliquée aux paquets pour garantir un timing de sortie approprié. Des exceptions existent sur les réseaux qui ne sont pas synchronisés par rapport à une source de référence commune. La pratique de l'ajout d'une estampille de temps dans une cellule ATM est appelée SRTS (*Synchronous Residual Time Stamps*, estampille de temps résiduel synchrone) et représente une méthode de transmission des informations de timing de bout en bout.

Certains commutateurs et multiplexeurs ATM et Frame Relay fournissent un codage de la voix pour un ATM à débit variable, ce qui rend les produits essentiellement destinés au rôle d'agent vocal. Comme les standards pour la voix sur Frame Relay et ATM sont toujours en cours d'évolution, les acheteurs devraient s'assurer que cette fonction est disponible, et également que les capacités des commutateurs correspondent aux exigences des applications. S'il n'y a pas d'interface native pour la voix pour un réseau de trames ou de cellules, un produit externe de compression de la voix peut être utilisé. Tous les avantages des réseaux ATM ou Frame Relay permettant de contrôler la gigue et le délai global du réseau restent disponibles pour un tel produit externe.

Réseaux de données en mode non connecté

Avec les réseaux de données fonctionnant en mode non connecté comme les intranets IP et l'Internet, on rencontre les mêmes problèmes de codage et d'adressage de la voix que ceux spécifiés pour les réseaux de trames/cellules. Avec ce type de réseaux cependant, il n'y a normalement aucun niveau de délai ou de gigue garanti par le réseau. Il peut donc s'avérer nécessaire d'adopter des mesures spéciales pour garantir que la "provision" pour le délai du réseau reste basse. Par exemple, les protocoles de haut niveau tels que TCP (*Transmission Control Protocol*) fournissent des fonctions de contrôle de flux et de récupération d'erreurs qui en se combinant, provoquent une gigue significative. Pour cette raison, TCP n'est pas utilisé à ce niveau.

Au lieu de cela, le trafic voix est transporté au moyen de UDP (*User Datagram Protocol*). Malheureusement, aucune estampille de temps n'est fournie pour contrôler le timing de sortie, et même de faibles variations de gigue peuvent interférer dans la compréhension de la conversation. Pour empêcher ce problème, le standard H.323 demande le transport de la voix sur IP en utilisant RTP qui coiffe UDP. RTP fournit les services d'estampille et permet — via RTCP (*Real-Time Control Protocol*) — l'établissement de connexions vocales point-multipoint. Cette fonction est rarement disponible avec les autres options de transport de la voix par paquets.

Un nombre croissant de réseaux sont aujourd'hui proposés avec des niveaux de services garantis. Ils utilisent généralement un protocole appelé RSVP (*Resource Reservation Protocol*, protocole de réservation de ressources). C'est un protocole de signalisation qui peut être utilisé pour indiquer aux commutateurs de paquets et aux routeurs de réserver des ressources pour réduire le délai global et la gigue qui résulteraient de la concurrence pour les ressources.

Réseaux de paquets X.25

Les réseaux de données publics basés sur le protocole de transport de paquets X.25 possèdent des fonctions intégrées de récupération d'erreurs de niveau 2 et de contrôle de flux de niveau 3 qui

peuvent échouer. Ces réseaux opèrent normalement avec des niveaux d'utilisation très élevés et souffrent par conséquent régulièrement de congestion. Pour ces raisons, le transport de la voix sur ces réseaux répond rarement aux attentes de l'utilisateur. Excepté pour les situations où les problèmes de coûts sont essentiels, ils ne devraient pas être envisagés comme solution de transport de la voix.

Réseaux de données privés

L'adéquation des réseaux de données privés peut être évaluée d'après leur niveau de conformité par rapport au modèle non connecté de IP (Novell SPX/IPX, OSI non connecté, pontage IEEE 802.2, etc.) ou au modèle orienté connexion de X.25 (IBM SNA, DEL LAT, etc.). Comme les réseaux fonctionnant en mode non connecté offrent normalement aux utilisateurs la possibilité de contourner les fonctions de récupération d'erreurs et de contrôle de flux, ils peuvent être utilisés comme mécanismes de transport de la voix par paquets si les autres sources de délai (en particulier le délai dû à la congestion) peuvent être maîtrisées. Pratiquement tous les protocoles de réseaux de données privés orientés connexion réclament l'emploi des fonctions de contrôle de flux et de récupération d'erreurs, ils ne conviennent donc probablement pas pour le transport de la voix.

Sur tous les types de réseaux convenant pour le transport de la voix, la question évidente est de savoir si le réseau "convenant" pour le transport justifierait l'emploi de la voix en paquets. La réponse dépend des aspects économiques du réseau de transport par rapport à l'offre de transport d'un réseau téléphonique public, et de la sensibilité des applications de gestion de la voix à supporter avec les limitations de qualité quelles qu'elles soient que peut générer le réseau de voix en paquets.

Dans la plupart des applications de gestion de la voix par paquets, le délai joue un rôle décisif dans la qualité d'écoute. Avec le codage LPC, comme prévu par le standard G.729, la qualité dans un environnement à faible délai équivaut à celle des liaisons interurbaines standard du système téléphonique public. Pouvoir maintenir un faible délai est le problème essentiel.

Les réseaux Frame Relay et ATM sont conçus pour assurer le délai de transport le plus faible possible sur le plan pratique. Des mesures spéciales de gestion de délai sont rarement requises, excepté dans les situations où l'agent vocal de l'utilisateur est connecté au réseau. Le taux d'utilisation de ces connexions devraient être maintenu au-dessous de 70 % pour garantir un délai maîtrisable, 50 % ou moins étant même préférable. Cela se traduit souvent par la sélection d'une vitesse de ligne d'accès supérieure à celle qui serait normalement choisie pour des applications de données seules.

Sur les réseaux en mode non connecté tels que IP, le délai peut être géré de différentes façons. Comme mentionné plus haut, le protocole de réservation de ressources RSVP peut être utilisé pour inciter les différents fournisseurs de routeurs à inclure des améliorations spéciales dans leurs produits pour attribuer des priorités selon certains types de trafic et garantir ainsi un transport de la voix par paquets moins exposé à la congestion. Ces améliorations sont très utiles pour limiter le délai provoqué par la congestion et fournir une meilleure qualité d'écoute.

Une autre possibilité avec les réseaux en mode non connecté est de s'assurer que les ressources sont suffisantes pour transporter le trafic sans attribuer de priorités spéciales et avec un faible niveau de délai. En général, des taux d'utilisation supérieurs à 70 % provoquent des augmentations importantes dans le délai de congestion pour une faible augmentation de trafic. Les réseaux fortement utilisés sont ainsi plus vraisemblablement exposés aux problèmes de qualité de la parole. Comme les

économies réalisables dépendent en grande partie de l'assurance de niveaux importants d'utilisation, les stratégies de gestion de délai basées sur le routeur sont préférables.

Quelle est la meilleure stratégie de transport de la voix par paquets ? Généralement, il s'agit d'une stratégie qu'une entreprise utilise déjà pour le transport de ses données, mais toutes les formes de réseau public de trames ou de cellules devraient néanmoins être examinées et comparées en termes de prix et de qualité de services. Une question souvent incontournable est la stratégie de tarification des services publics. Dans de nombreux pays, des services de données publics tels que Frame Relay sont facturés sans tenir compte d'une composante d'éloignement. Par conséquent, pour les connexions à forte activité, ces services peuvent s'avérer plus économiques que des lignes louées ou un système téléphonique, lesquels sont généralement facturés en se basant en partie sur la distance séparant les points de connexions.

Les tarifs de réseaux publics peuvent également subventionner des services résidentiels en appliquant des tarifs plus élevés aux communications d'entreprises et aux appels internationaux. Ces subsides créent une économie artificielle pour toute forme de transport de la voix par paquets, et malgré le fait que l'avantage provienne d'une politique de tarification et non d'une technologie de réseau, les économies sont bien réelles. Les administrations nationales peuvent toutefois voir ces tentatives échapper à cette tarification élevée comme contraire à la stratégie du système public, et les réseaux procédant de la sorte peuvent se retrouver dans une position illégale dans certains pays. Les problèmes relatifs à la légalité du transport de la voix sur des réseaux à paquets doivent être examinés pays par pays. Un ensemble général de directives est fourni plus loin dans ce chapitre.

Signalisation : établissement de la connexion pour la voix

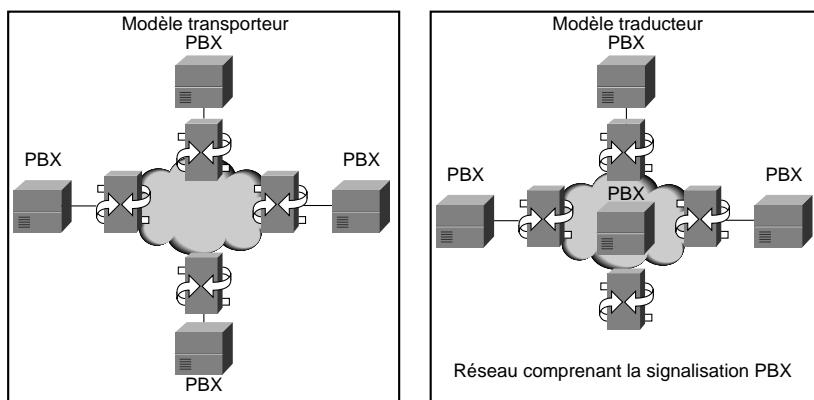
A bien des égards, les méthodes de codage et la qualité de communication sont les aspects les plus simples de la voix en paquets. Une application utile comme celle de la Figure G.1 nécessite que les participants d'une zone puissent se connecter à un agent vocal qui les assiste en utilisant leur mécanisme standard de numérotation, afin de pouvoir établir un appel avec, au minimum, un ensemble sélectionné d'utilisateurs accessibles sur les autres agents vocaux.

Il existe deux modèles de base de connexion et de signalisation pour la voix utilisés dans les applications, comme illustré Figure G.3.

- **Le modèle transporteur.** Dans ce modèle, deux agents vocaux sont connectés par un tronçon à travers le nuage du réseau de transport. Tous les appels établis par un agent doivent être terminés sur l'autre agent pour que tout le trafic provenant du premier soit juste envoyé sur le tronçon vers le second agent. Ce modèle est souvent utilisé pour les applications point à point de gestion de la voix sur l'Internet. Il peut être comparé au modèle de ligne de jonction d'un réseau d'autocommutateurs (PBX), où la connexion et la logique de commutation reposent entièrement sur les autocommutateurs.
- **Le modèle traducteur.** Dans ce modèle, n'importe quel nombre d'agents vocaux peut être connecté via un nuage de réseau capable de comprendre les requêtes de signalisation et d'adressage. Les agents établissent une correspondance entre les numéros de téléphones natifs et les adresses ATM, Frame Relay, ou IP via un annuaire ou un plan de numérotation qui spécifie les adresses voix (numéros de téléphone, postes) pouvant être atteintes sur chaque agent. Lors d'un appel, le plan de numérotation est utilisé par l'agent d'origine pour identifier l'agent qui "possède" l'interlocuteur

à joindre et établir une connexion avec lui. Ce modèle transforme le nuage de réseau en un commutateur virtuel pour la voix ou un commutateur tandem.

Figure G.3
Modèles de connexion/
signalisation.



La Figure G.3 montre qu'il y a deux relations de signalisation très différentes sur un réseau transportant du trafic voix. L'une, appelée signalisation externe, prend place entre l'agent vocal et les équipements de traitement de la voix qu'il sert. Comme ces équipements ont été conçus pour participer sur des réseaux ordinaires de téléphonie, cette signalisation externe suit les standards qui y sont appliqués. L'autre type de signalisation intervient entre les agents eux-mêmes à travers le nuage du réseau de transport. Cette signalisation interne se déroule selon les standards du réseau chargé du transport, ou ceux des agents.

Signalisation externe

Les agents vocaux doivent être interconnectés avec la source et la destination d'une manière cohérente par rapport aux systèmes téléphoniques habituels, sous peine d'obtenir un fonctionnement de la voix en paquets ne s'apparentant pas au système téléphonique traditionnel. Les quatre options suivantes de signalisation externe sont couramment supportées par les systèmes de voix par paquets :

- La signalisation DTMF (*Dual-Tone Multi-Frequency*) ou la signalisation analogique par impulsions. Ce type de signalisation est approprié pour les applications de gestion de la voix par paquets dans les situations où les appareils téléphoniques doivent être branchés directement sur l'agent vocal en utilisant le type de prise téléphonique approprié à l'administration nationale.
- La signalisation de ligne de jonction, également appelée signalisation E&M, utilisée le plus souvent sur les tronçons analogiques à quatre fils.
- La signalisation intrabande, appelée signalisation CAS (*Channel Associated Signaling*, signalisation associée à un canal voix), qui est utilisée sur les tronçons numériques T1/E1. Les standards pour cette signalisation varient en fonction des zones géographiques principales (Amérique du Nord et l'UIT par exemple). Avec CAS, les informations de signalisation circulent sur le même chemin que les informations vocales.

- La signalisation hors bande, appelée CCS (*Common Channel Signaling*, signalisation par canal commun), avec laquelle la signalisation d'un tronçon numérique multiconexion (T1/E1/J1) est combinée en un ou plusieurs canaux communs et distincte des données voix. Ce type de signalisation est celui qui est normalement employé par les PBX (par exemple, DPNSS et QSIG). Le canal D de RNIS est également un canal CCS.

Une autre forme de signalisation appelée SS7 (*Signaling System 7*) est utilisée avec les réseaux téléphoniques publics. Il s'agit d'un protocole interne à ces réseaux fonctionnant hors bande entre les équipements du réseau pour établir des appels et demander des services spéciaux. Les futurs produits de gestion de la voix par paquets peuvent supporter SS7 comme protocole de signalisation externe.

Un réseau de transport de la voix par paquets fonctionnant avec un modèle traducteur agit comme un commutateur tandem lorsqu'il comprend les protocoles de signalisation de l'agent vocal et connecte les appels à travers le réseau de transport en se basant sur les numéros transmis. Cette fonction peut représenter une source supplémentaire d'économies pour les concepteurs de réseau voix car ce type de commutateurs est normalement coûteux.

Les commutateurs tandem et les commutateurs sources (par exemple PBX) sont combinés pour créer le plan d'adressage ou de numérotation d'un réseau. Ce plan associe des stations spécifiques aux numéros composés, et il doit être complet et cohérent pour que le réseau puisse fonctionner correctement. Il est important qu'un réseau de paquets transportant la voix conçu sur le modèle traducteur, dispose de services appropriés pour gérer sa part de plan d'accès et garantir qu'il soit cohérent avec le plan de numérotation des réseaux voix qu'il assiste.

Signalisation interne

La signalisation interne, comme évoqué plus haut, doit fournir deux caractéristiques : le contrôle de la connexion et les informations de progression ou d'état. La signalisation de contrôle est utilisée pour créer des relations ou des chemins entre les agents vocaux pour permettre à la voix en paquets de circuler. Les informations de progression d'appel ou d'état sont échangées entre les agents vocaux et renseignent sur les divers états de la connexion, sonnerie, occupation, etc.

Avec le modèle transporteur, la signalisation interne est utilisée principalement pour éviter le maintien d'une connexion permanente à travers le réseau de paquets afin de pouvoir supporter chaque appel entre les agents vocaux. Par conséquent, la signalisation interne dans ce modèle est associée avec les réseaux orientés connexion qui allouent des ressources fixes de bande passante. Avec les applications gérant la voix en paquets sur des réseaux orientés sans connexion, il n'y a aucun besoin d'établir une connexion, les deux agents vocaux s'envoyant des datagrammes lorsque le trafic se présente.

Dans le modèle traducteur, la signalisation de connexion peut s'avérer nécessaire pour pouvoir router un flot de paquets vers un agent vocal approprié lorsque l'identification de celui-ci a été satisfaite par la fonction de plan de numérotation. La multiplicité des connexions possibles sur les réseaux disposant d'une grande variété d'agents vocaux peut rendre impossible la création d'une connexion avec chaque partenaire pour tous les appels.

Les différentes solutions de transport telles que ATM, Frame Relay, et IP ont toutes leurs standards de signalisation. Pour ATM, il s'agit de Q.931, et pour Frame Relay, c'est FRF.11. Ces différents

standards pourraient nécessiter l'adoption par les utilisateurs d'agents vocaux spéciaux pour chaque réseau de transport.

Le modèle accepté pour la signalisation interne sur les réseaux IP transportant la voix, à la fois pour la connexion et les informations d'état, est spécifié dans le standard H.323. Bien que celui-ci soit généralement vu comme un standard vidéo, il définit en fait un ensemble de standards de communication multimédia entre les utilisateurs. En fait, seuls des services de traitement de la voix sont requis pour l'exploitation de H.323, le support de la vidéo et des données est optionnel.

H.323 définit un réseau multimédia complet, des équipements jusqu'aux protocoles. La liaison de toutes les entités à l'intérieur de H.323 est définie par le standard H.245, qui prévoit la négociation de services entre les participants et les éléments d'un réseau H.323. Une version réduite du protocole d'appel Q.931 de RNIS est utilisée pour assurer l'établissement de la connexion.

Selon les termes du standard H.323, les agents vocaux sont des terminaux, bien que l'usage courant de ce concept suggère plutôt l'implication d'un seul utilisateur. Il définit aussi une fonction de poste de frontière qui exécute les traductions d'adresse et les recherches requises pour le modèle traducteur du réseau voix par paquets.

Si le nuage du réseau de transport d'un point de vue de l'application de gestion de la voix est en fait constitué de plusieurs types de réseaux de transport, H.323 définit une fonction de passerelle qui réalise la traduction du format des données et de la signalisation nécessaires à une communication correcte aux frontières de réseaux. L'affectation la plus courante de cette passerelle est pour la conversion des données de vidéoconférence du format H.320 vers le format H.323, permettant aux utilisateurs de la vidéo en paquets de communiquer avec des systèmes traditionnels qui s'appuient sur une forme de vidéo par circuits commutés.

Le standard H.323 peut venir coiffer des standards spécialisés pour chaque option de réseau de transport. Sur les réseaux IP en mode non connecté, le protocole RTP et le protocole de contrôle RTCP sont utilisés et transportés à leur tour sur UDP. Pour Frame Relay, le standard FRF.11 décrit un mécanisme standard de signalisation.

Ces standards de niveau inférieur peuvent bien sûr être utilisés sans H.323. Bien que celui-ci ne soit pas nécessaire pour les applications de gestion de la voix par paquets, disposer d'une compatibilité avec ce standard apporte des avantages significatifs. Il permet de rendre optionnelle toute forme de compression de la voix autre que la méthode PCM (ou MIC)/G.711. Il n'y a cependant aucune garantie que des systèmes compatibles avec ce standard fourniront un codage optimal de la voix.

Le meilleur modèle pour une application de gestion de la voix en paquets dépend de la nature des utilisateurs. Alors qu'une connexion transportant la voix en paquets est utilisée comme un type de ligne de jonction entre deux communautés d'utilisateurs de système téléphonique privé ou public, le modèle transporteur associé à un système propriétaire de codage de la voix et de signalisation est approprié si les exigences de l'application sont satisfaites par le système de compression utilisé et que les ressources de transport du réseau sont disponibles.

Lorsqu'il faut gérer plusieurs communautés d'utilisateurs, ceci signifiant qu'il pourrait y avoir beaucoup d'agents sur le nuage du réseau de transport, le modèle traducteur pourrait apporter une meilleure économie et davantage de souplesse. S'il y a une possibilité que ces agents vocaux soient fournis et supportés par différentes organisations, il est essentiel que l'ensemble du système soit basé sur le standard H.323 pour garantir que les agents et les fonctions d'annuaire (terminaux,

postes de frontière, passerelles, selon la terminologie H.323) puissent interopérer. Dans cette situation toutefois, l'acquéreur devra s'assurer que les composants H.323 supportent des standards supplémentaires de codage de la voix, s'ils sont requis pour sécuriser les niveaux de qualité de la voix et d'économie du réseau comme prévu par les applications.

Les services de réseaux publics basés sur H.323 sont de plus en plus disponibles et continueront probablement à gagner en popularité. Le choix entre ces services et les solutions alternatives d'un réseau public de transport de la voix par paquets est une affaire de garantie des performances requises (c'est-à-dire, la qualité de la parole) au coût le plus bas.

Dans les applications privées, opter pour une conformité avec H.323 peut être nécessaire dès la procédure d'acquisition de l'équipement vidéo en paquets s'il est prévu d'employer du matériel provenant de différents fournisseurs. Il peut cependant s'avérer utile de réaliser des tests de conformité ou d'interopérabilité. Comme c'est souvent le cas avec les standards internationaux, H.323 prévoit de nombreux domaines "optionnels" de support, englobant certaines des méthodes de codage les plus efficaces de la voix. Un équipement peut être conforme aux standards et ne pas fournir de support pour toutes les options. Ce type de matériel peut ne prévoir que le mode minimal d'interopérabilité comme prévu par le standard H.323.

Souvent, les utilisateurs éventuels d'applications de gestion de voix en paquets disposent de réseaux multicouches, par exemple, IP sur Frame Relay ou ATM. Sur ce type de réseaux, il est possible de transporter la voix à n'importe quel niveau ou à tous les niveaux, et choisir la meilleure méthode peut se révéler problématique. Les points suivants font partie des facteurs à prendre en compte :

- Il faut tout d'abord prendre en compte la portée des diverses couches de réseaux. La connectivité Frame Relay peut être disponible de site en site par exemple, mais pas à l'intérieur de sites où d'emplacements desservis par des ressources de transmission telles que la fibre optique ou les micro-ondes. Quant à IP, il est capable en raison de son omniprésence de supporter les utilisateurs de ces applications dans n'importe quel lieu.
- Lorsque que l'étendue des options de couches convient à l'application, il est généralement préférable de transporter la voix au niveau le plus bas, c'est-à-dire avec Frame Relay ou ATM plutôt qu'avec IP. La charge de service est inférieure et la connexion avec qualité de services est souvent contrôlée plus naturellement.

Applications de la voix par paquets

Les réseaux de voix par paquets peuvent être utilisés dans deux contextes globaux, dépendant de facteurs géographiques ou de types d'utilisateurs à satisfaire. Les aspects économiques et technologiques du réseau peuvent ne pas être influencés par ces facteurs mais certaines régions peuvent introduire des contraintes liées à la législation pour certaines combinaisons de ces deux contextes, et les utilisateurs ou opérateurs de réseaux devraient en être conscients.

Le domaine des télécommunications est régulé à l'intérieur des pays par des administrations nationales ou des branches du gouvernement sur la base de réglementations locales. Dans certains pays, comme aux Etats-Unis, il peut y avoir plusieurs niveaux d'autorité. Dans tous les cas, des traités définissent les règles de connexions internationales, les débits, et ainsi de suite. Il est important qu'une entreprise projetant d'utiliser ou de construire un réseau de transport de la voix par paquets s'assure qu'elle agit en conformité avec toutes les lois et réglementations en vigueur dans les

régions desservies par le réseau. Ceci nécessite normalement d'effectuer des recherches directes, mais l'état actuel des réglementations peut être résumé de façon suivante :

- A l'intérieur d'une administration nationale ou d'une zone de juridiction téléphonique, une entreprise peut presque toujours employer la voix en paquets pour supporter ses propres communications à travers ses propres sites.
- Avec de telles applications, il est normalement prévu que certains des appels transportés sur le réseau de paquets proviennent à l'origine du réseau téléphonique public. Ce genre d'appels "externes" acheminés par paquets est toléré de façon uniforme d'un point de vue de la réglementation, en se basant sur le fait qu'ils émanent d'employés, de clients, ou de fournisseurs, et qu'ils représentent les opérations de l'entreprise.
- Lorsqu'une connexion transportant la voix par paquets est établie entre deux administrations nationales pour supporter les activités d'une seule entreprise (pour connecter deux ou plusieurs sites de l'entreprise dans plusieurs pays) l'application est uniformément tolérée d'un point de vue de la réglementation.
- Dans une telle situation, un appel extérieur provenant du réseau public d'un pays se terminant sur un site d'entreprise à l'intérieur d'un autre pays via un transport de la voix par paquets peut représenter une violation technique des monopoles ou des traités nationaux relatifs aux services d'appels de longue distance. Lorsqu'une telle violation concerne un appel établi entre des employés de l'entreprise, ou entre ces derniers et des fournisseurs ou des clients, il est peu probable qu'elle attire l'attention des autorités.
- Lorsqu'un réseau de paquets transportant la voix est utilisé pour connecter des appels publics à une entreprise, le fournisseur du réseau assure techniquement un service téléphonique local ou national qui est soumis en tant que tel à une réglementation.
- Lorsqu'un réseau de voix par paquets est utilisé pour connecter des appels publics entre pays différents, le fournisseur du réseau est soumis aux réglementations nationales en vigueur dans chaque pays desservi et aussi à toutes les prévisions d'accords sur les appels internationaux dont les pays desservis sont signataires.

Par conséquent, on peut affirmer en toute sécurité que des entreprises peuvent employer la voix en paquets pour toutes les applications dans lesquelles des lignes louées, ou des réseaux d'autocommutateurs privés, pourraient être employés en toute légalité. En fait, un bon modèle à suivre pour déployer un réseau transportant la voix par paquets, sans introduire de problèmes supplémentaires liés aux réglementations, est de dupliquer un réseau de tronçons PBX ou de lignes de jonction en utilisant des services de voix par paquets.

Résumé

Le réseau téléphonique public d'aujourd'hui possède encore beaucoup de points communs avec le système du début des années 1980. Durant cette période, de grandes avancées technologiques dans le domaine des réseaux de données ont permis d'améliorer les coûts d'exploitation de réseaux ainsi que le contrôle de la qualité de services. Ces avancées orientent aujourd'hui le marché vers le transport de la voix par paquets.

La voix en paquets utilise des algorithmes de compression avancés tels que le codage G.729 basé sur ACELP, qui peut transporter seize fois plus de trafic vocal par unité de bande passante de réseaux que les systèmes basés sur le codage PCM (ou MIC) utilisé par le système téléphonique public. Les utilisateurs de réseaux de données existants peuvent souvent intercaler du trafic voix et du trafic données avec un coût supplémentaire de transport faible ou inexistant, et avec peu ou pas d'impact sur les performances de l'application. Les utilisateurs de réseaux voix de circuits commutés T1/E1/J1, employant la transmission de la voix par paquets, peuvent souvent libérer suffisamment de bande passante sur les tronçons voix existants pour transporter la totalité de leur charge de données.

La plupart des discussions sur le transport de la voix par paquets abordent les thèmes de l'arbitrage de la tarification — en tirant parti de la facturation Frame Relay indépendante de la distance ou en évitant les tarifs internationaux de communication vocale. Bien que ces formes de suppression de coûts permettent souvent de réaliser quelques économies, tant qu'il y a des différences de tarification, c'est l'efficacité fondamentale du transport de la voix par paquets qui rend cette technologie toujours plus intéressante aux yeux des entreprises.

Tous les réseaux et tous les utilisateurs ne pourront pas tirer parti des avantages de la transmission de la voix par paquets pour réduire les coûts de communication. Certains réseaux disposent de capacités résiduelles insuffisantes pour transporter la voix, même si elle était soumise à une très forte compression, et les faire évoluer par l'intermédiaire de services supplémentaires de transporteurs publics pourrait s'avérer coûteux. Il est toutefois intéressant de noter que la voix en paquets ne sera jamais plus coûteuse qu'une communication traditionnelle par circuits commutés. Elle est même souvent bien moins onéreuse et vaut la peine d'être envisagée à court terme comme à long terme.

Les informations de ce chapitre proviennent du site Web de Cisco, à l'adresse : www.cisco.com.

H

Références et suggestions de lectures

Ouvrages et publications périodiques

- Apple Computer, Inc. *AppleTalk Network System Overview*. Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1989.
- Apple Computer, Inc. *Planning and Managing AppleTalk Networks*. Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1991.
- Black, U. *Data Networks : Concepts, Theory and Practice*. Englewood Cliffs, New Jersey : Prentice Hall ; 1989.
- Black, U. *Physical Level Interfaces and Protocols*. Los Alamitos, California : IEEE Computer Society Press ; 1988.
- Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Network Management and the Design of SNMP". *ConneXions : The Interoperability Report*, Vol. 3 : March 1989.
- Case, J.D., J.R. Davins, M.S. Fedor, and M.L. Schoffstall. "Introduction to the Simple Gateway Monitoring Protocol". *IEEE Network* : March 1988.
- Clark, W. "SNA Internetworking". *ConneXions : The Interoperability Report*, Vol. 6, No. 3 : March 1992.
- Coltun, R. "OSPF : An Internet Routing Protocol". *ConneXions : The Interoperability Report*, Vol. 3, No. 8 : August 1989.
- Comer, D.E. *Internetworking with TCP/IP : Principles, Protocols, and Architecture*, Vol. I, 2nd ed. Englewood Cliffs, New Jersey : Prentice Hall ; 1991.
- Davidson, J. *An Introduction to TCP/IP*. New York, New York : Springer-Verlag ; 1992.
- Ferrari, D. *Computer Systems Performance Evaluation*. Englewood Cliffs, New Jersey : Prentice Hall ; 1978.
- Garcia-Luna-Aceves, J.J. "Loop-Free Routing Using Diffusing Computations". *IEEE/ACM Transactions on Networking*, Vol. 1, No. 1, 1993.

- Green, J.K. *Telecommunications*, 2nd ed. Homewood, Illinois : Business One Irwin ; 1992.
- Hagans, R. "Components of OSI : ES-IS Routing". *ConneXions : The Interoperability Report*, Vol. 3, No. 8 : August 1989.
- Hares, S. "Components of OSI : Inter-Domain Routing Protocol (IDRP)". *ConneXions : The Interoperability Report*, Vol. 6, No. 5 : May 1992.
- Jones, N.E.H. and D. Kosiur. *Macworld Networking Handbook*. San Mateo, California : IDG Books Worldwide, Inc. ; 1992.
- Joyce, S.T. and J.Q. Walker II. "Advanced Peer-to-Peer Networking (APPN) : An Overview". *ConneXions : The Interoperability Report*, Vol. 6, No. 10 : October 1992.
- Kousky, K. "Bridging the Network Gap". *LAN Technology*, Vol. 6, No. 1 : January 1990.
- LaQuey, Tracy. *The Internet Companion : A Beginner's Guide to Global Networking*, Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1994.
- Leinwand, A. and K. Fang. *Network Management : A Practical Perspective*. Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1993.
- Lippis, N. "The Internetwork Decade." *Data Communications*, Vol. 20, No. 14 : October 1991.
- McNamara, J.E. *Local Area Networks*. Digital Press, Educational Services, Digital Equipment Corporation, 12 Crosby Drive, Bedford, MA 01730.
- Malamud, C. *Analyzing DECnet/OSI Phase V*. New York, New York : Van Nostrand Reinhold ; 1991.
- Malamud, C. *Analyzing Novell Networks*. New York, New York : Van Nostrand Reinhold ; 1991.
- Malamud, C. *Analyzing Sun Networks*. New York, New York : Van Nostrand Reinhold ; 1991.
- Martin, J. *SNA : IBM's Networking Solution*. Englewood Cliffs, New Jersey : Prentice Hall ; 1987.
- Martin, J., with K.K. Chapman and the ARBEN Group, Inc. *Local Area Networks. Architectures and Implementations*. Englewood Cliffs, New Jersey : Prentice Hall ; 1989.
- Medin, M. "The Great IGP Debate—Part Two : The Open Shortest Path First (OSPF) Routing Protocol". *ConneXions : The Interoperability Report*, Vol. 5, No. 10 : October 1991.
- Meijer, A. *Systems Network Architecture : A tutorial*. New York, New York : John Wiley & Sons, Inc. ; 1987.
- Miller, M.A. *LAN Protocol Handbook*. San Mateo, California : M&T Books ; 1990.
- Miller, M.A. *LAN Troubleshooting Handbook*. San Mateo, California : M&T Books ; 1989.
- O'Reilly, T. and G. Todino. *Managing UUCP and Usenet*, 10th ed. Sebastopol, California : O'Reilly & Associates, Inc. ; 1992.
- Perlman, R. *Interconnections : Bridges and Routers*. Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1992.
- Perlman, R. and R. Callon. "The Great IGP Debate—Part One : IS-IS and Integrated Routing". *ConneXions : The Interoperability Report*, Vol. 5, No. 10 : October 1991.

- Rose, M.T. *The Open Book : A Practical Perspective on OSI*. Englewood Cliffs, New Jersey : Prentice Hall ; 1990.
- Rose, M.T. *The Simple Book : An Introduction to Management of TCP/IP-based Internets*. Englewood Cliffs, New Jersey : Prentice Hall ; 1991.
- Ross, F.E. "FDDI—A Tutorial". *IEEE Communications Magazine*, Vol. 24, No. 5 : May 1986.
- Schlar, S.K. *Inside X.25 : A Manager's Guide*. New York, New York : McGraw-Hill, Inc. ; 1990.
- Schwartz, M. *Telecommunications Networks : Protocols, Modeling, and Analysis*. Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1987.
- Sherman, K. *Data Communications : A User's Guide*. Englewood Cliffs, New Jersey : Prentice Hall ; 1990.
- Sidhu, G.S., R.F. Andrews, and A.B. Oppenheimer. *Inside AppleTalk*, 2nd ed. Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1990.
- Spragins, J.D. et al. *Telecommunications Protocols and Design*. Reading, Massachusetts : Addison-Wesley Publishing Company, Inc. ; 1991.
- Stallings, W. *Data and Computer Communications*. New York, New York : Macmillan Publishing Company ; 1991.
- Stallings, W. *Handbook of Computer-Communications Standards*, Vols. 1-3. Carmel, Indiana : Howard W. Sams, Inc. ; 1990.
- Stallings, W. *Local Networks*, 3rd ed. New York, New York : Macmillan Publishing Company ; 1990.
- Sunshine, C.A. (ed.). *Computer Network Architectures and Protocols*, 2nd ed. New York, New York : Plenum Press ; 1989.
- Tannenbaum, A.S. *Computer Networks*, 2nd ed. Englewood Cliffs, New Jersey : Prentice Hall ; 1988.
- Terplan, K. *Communication Networks Management*. Englewood Cliffs, New Jersey : Prentice Hall ; 1992.
- Tsuchiya, P. "Components of OSI : IS-IS Intra-Domain Routing". *ConneXions : The Interoperability Report*, Vol. 3, No. 8 : August 1989.
- Tsuchiya, P. "Components of OSI : Routing (An Overview)". *ConneXions : The Interoperability Report*, Vol. 3, No. 8 : August 1989.
- Zimmerman, H. "OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection". *IEEE Transactions on Communications* COM-28, No. 4 : April 1980.

Publications techniques et standards

Advanced Micro Devices. *The Supernet Family for FDDI*. Technical Manual Number 09779A. Sunnyvale, California ; 1989.

——— *The Supernet Family for FDDI*. 1989 Data Book Number 09734C. Sunnyvale, California ; 1989.

American National Standards Institute X3T9.5 Committee. *FDDI Station Management (SMT)*. Rev. 6.1 ; March 15, 1990.

———. Revised Text of ISO/DIS 8802/2 for the Second DIS Ballot, "Information Processing Systems—Local Area Networks". Part 2 : Logical Link Control. 1987-01-14.

——— T1.606. Integrated Services Digital Network (ISDN)—Architectural Framework and Service Description for Frame-Relaying Bearer Service. 1990.

——— T1.617. Integrated Services Digital Network (ISDN)—Signaling Specification for Frame Relay Bearer Service for Digital Subscriber Signaling System Number 1 (DSS1). 1991.

——— T1.618. Integrated Services Digital Network (ISDN)—Core Aspects of Frame Protocol for Use with Frame Relay Bearer Service. 1991.

ATM Data Exchange Interface (DXI) Specification, Version 1.0. Document ATM_FORUM/93-590R1 ; August 4, 1993.

Banyan Systems, Inc. *VINES Protocol Definition*. DA254-00, Rev. 1.0. Westboro, Massachusetts ; February 1990.

Bellcore. *Generic System Requirements in Support of a Switched Multi-Megabit Data Service*. Technical Advisory, TA-TSY-000772 ; October 1989.

———. *Local Access System Generic Requirements, Objectives, and Interface Support of Switched Multi-Megabit Data Service*. Technical Advisory TA-TSY-000773, Issue 1 ; December 1985.

———. *Switched Multi-Megabit Data Service (SMDS) Operations Technology Network Element Generic Requirements*. Technical Advisory TA-TSY-000774.

Chapman, J.T. and M. Halabi. *HSSI : High-Speed Serial Interface Design Specification*. Menlo Park, California and Santa Clara, California : Cisco Systems and T3Plus Networking, Inc. ; 1990.

Consultative Committee for International Telegraph and Telephone. *CCITT Data Communications Networks—Services and Facilities, Terminal Equipment and Interfaces, Recommendations X.1-X.29*. Yellow Book, Vol. VIII, Fascicle VIII.2 ; 1980.

———. *CCITT Data Communications Networks—Interfaces, Recommendations X.20-X.32*. Red Book, Vol. VIII, Fascicle VIII.3 ; 1984.

DDN Protocol Handbook. Four volumes ; 1989.

Defense Communications Agency. *Defense Data Network X.25 Host Interface Specification*. Order number AD A137 427 ; December 1983.

Digital Equipment Corporation. *DECnet/OSI Phase V : Making the Transition from Phase IV*. EK-PVTRN-BR ; 1989.

- _____. *DECserver 200 Local Area Transport (LAT) Network Concepts*. AA-LD84A-TK ; June 1988.
- _____. *DIGITAL Network Architecture (Phase V)*. EK-DNAPV-GD-001 ; September 1987.
- Digital Equipment Corporation, Intel Corporation, Xerox Corporation. *The Ethernet, A Local-Area Network, Data Link Layer and Physical Layer Specifications*. Ver. 2.0 ; November 1982.
- Feinler, E.J., et al. *DDN Protocol Handbook*, Vols. 1-4, NIC 50004, 50005, 50006, 50007. Defense Communications Agency. Alexandria, Virginia ; December 1985.
- Garcia-Luna-Aceves, J.J. "A Unified Approach to Loop-Free Routing Using Distance Vectors or Link States". ACM 089791-332-9/89/0009/0212, pp. 212-223 ; September 1989.
- Hemrick, C. and L. Lang. "Introduction to Switched Multi-megabit Data Service (SMDS), an Early Broadband Service". *Proceedings of the XIII International Switching Symposium (ISS 90)*, May 27-June 1, 1990.
- Hewlett-Packard Company. X.25 : The PSN Connection ; An Explanation of Recommendation X.25. 5958-3402 ; October 1985.
- IEEE 802.2—*Local Area Networks Standard, 802.2 Logical Link Control*. ANSI/IEEE Standard ; October 1985.
- IEEE 802.3—*Local Area Networks Standard, 802.3 Carrier Sense Multiple Access*. ANSI/IEEE Standard ; October 1985.
- IEEE 802.5—*Local Area Networks Standard, 802.5 Token Ring Access Method*. ANSI/IEEE Standard ; October 1985.
- IEEE 802.6—*Local & Metropolitan Area Networks Standard, 802.6 Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network (MAN)*. ANSI/IEEE Standard ; December 1990.
- International Business Machines Corporation. *ACF/NCP/VSC network control program, system support programs : general information*. GC30-3058.
- _____. *Advanced Communications Function for VTAM (ACF/VTAM)*, general information : introduction. GS27-0462.
- _____. *Advanced Communications Function for VTAM, general information : concepts*. GS27-0463.
- _____. *Dictionary of Computing*. SC20-1699-7 ; 1987.
- _____. *Local Area Network Technical Reference*. SC30-3883.
- _____. *Network Problem Determination Application : general information*. GC34-2010.
- _____. *Synchronous Data Link Control : general information*. GA27-3093.
- _____. *Systems Network Architecture : concepts and products*. GC30-3072.
- _____. *Systems Network Architecture : technical overview*. GC30-3073-1 ; 1985.
- _____. *Token-Ring Network Architecture Reference*. SC30-3374.
- _____. *Token-Ring Problem Determination Guide*. SX27-3710-04 ; 1990.

International Organization for Standardization. *Information Processing System—Open System Interconnection ; Specification of Abstract Syntax Notation One (ASN.1)*. International Standard 8824 ; December 1987.

McGraw-Hill/Data Communications. *McGraw-Hill's Compilation of Data Communications Standards*. Edition III ; 1986.

National Security Agency. *Blacker Interface Control Document*. March 21, 1989.

Novell, Inc. IPX Router Specification, Version 1.10. Part Number 107-000029-001. October 16, 1992.

_____. NetWare Link Services Protocol (NLSP) Specification, Revision 0.9. Part Number 100-001708-001. March 1993.

StrataCom. *Frame Relay Specification with Extensions*. 001-208966, Rev.1.0 ; September 18, 1990.

Xerox Corporation. *Internet Transport Protocols*. XNSS 029101 ; January 1991

I

Présentation de la technologie multicast IP

Cette annexe a pour objectif de fournir les notions de base relatives au protocole PIM-SM, étudié au Chapitre 13. Son contenu vient du site Web de Cisco.

Avantages du multicast

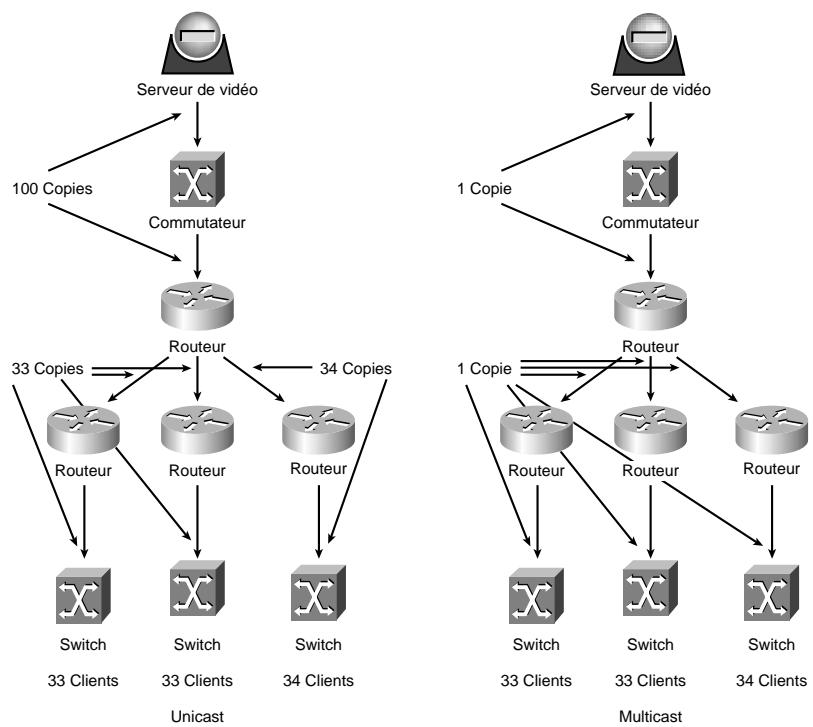
N'importe quelle forme de communication qui implique la transmission d'informations vers plusieurs destinataires peut tirer parti de l'exploitation efficace de la bande passante assurée par la technologie multicast. Des exemples d'applications qui implémentent des communications *one-to-many* (un seul émetteur, plusieurs récepteurs passifs) ou *many-to-many* (applications coopératives et interactives) incluent les diffusions broadcast audio et vidéo, la vidéoconférence/collaboration, la diffusion de valeurs cotées en bourse et de news, la réPLICATION de bases de données, les téléchargements de programmes, et la mise en cache de sites Web.

Pour comprendre l'efficacité de la technologie multicast, prenons l'exemple d'un serveur de vidéo qui offre un seul canal de contenu vidéo (voir Figure I.1). Pour une diffusion vidéo animée en mode plein écran, un flux vidéo requiert environ 1,5 Mbit/s de bande passante dans le sens serveur-client. Dans un environnement unicast, le serveur doit envoyer sur le réseau un flux vidéo séparé pour chaque client (qui consomme $1,5 \times n$ Mbit/s de la bande passante du média, où n représente le nombre de clients visionneurs). Avec une interface Ethernet à 10 Mbit/s sur le serveur, 6 à 7 flux dans le sens serveur-client suffiraient à la saturer complètement. Même dans le cas d'une interface Gigabit Ethernet hautement intelligente, avec un serveur hautement performant, la limite pratique se situerait entre 250 et 300 flux vidéo de 1,5 Mbit/s. Par conséquent, la capacité de l'interface d'un serveur peut représenter un goulet d'étranglement significatif, ce qui limite le nombre de flux vidéo unicast par serveur de vidéo. Les transmissions unicast répliquées consomment énormément de bande passante sur un réseau, ce qui représente une autre limitation de taille. Si le chemin qui relie un serveur et un client traverse trois sauts de routeur et deux sauts de commutateur, la vidéo "multi-unicast" consomme $1,5 \times n \times 3$ Mbit/s de bande passante de routeur, plus $1,5 \times n \times 2$ Mbit/s de bande passante de commutateur. En admettant que 100 clients soient séparés du serveur par deux sauts de routeur et deux sauts de commutateur (tel qu'illustre à la Figure I.1), un seul canal multicast

consommerait 300 Mbit/s de bande passante de routeur et 300 Mbit/s de bande passante de commutateur. Même si la bande passante du flux vidéo était ramenée à 100 Kbit/s (ce qui offre une qualité acceptable dans le cas de l'affichage d'une fenêtre plus petite à l'écran), la vidéo multi-unicast consommerait 20 Mbit/s de bande passante de routeur et 20 Mbit/s de bande passante de commutateur.

Figure I.1

Transmission de vidéo sur des réseaux unicast et multicast.



Dans un environnement multicast, le serveur de vidéo doit transmettre un seul flux vidéo à chaque groupe multicast, indépendamment du nombre de clients qui le visualiseront. Le flux est donc répliqué, lorsque cela est nécessaire, par les routeurs et commutateurs multicast du réseau, afin de permettre à un nombre arbitraire de clients de souscrire une adresse multicast et de recevoir la diffusion. Sur le réseau de routeurs, la réplication se produit uniquement au niveau des branches de l'arbre de distribution, c'est-à-dire au niveau du dernier saut de commutateur. Dans le scénario multicast, seulement 1,5 Mbit/s de la bande passante serveur-réseau est utilisée ; le reste est disponible pour d'autres utilisations ou canaux de contenu vidéo. Sur le réseau, la transmission multicast offre une efficacité analogue ; elle consomme seulement $1/n^e$ de la bande passante de la solution multi-unicast (par exemple, 3 Mbit/s de bande passante de routeur et de commutateur, à la Figure I.1).

Il apparaît de façon évidente que, dans des environnements où les destinataires d'une transmission répliquée sont nombreux, la technologie multicast fait la différence, aussi bien en termes de charge de serveur que de charge de réseau, même sur un réseau simple qui comprend un nombre limité de

sauts de routeur et de commutateur. Des fonctionnalités multicast additionnelles sont également avantageuses dans le cas d'applications spécifiques, telles que des services financiers. Les transmissions multicast sont délivrées presque simultanément à tous les membres d'un groupe destinataire. La variation du délai de livraison est limitée aux différences de délais de réseau de bout en bout dans la plage des chemins serveur-client. Dans un scénario unicast, le serveur transmet, par séquences, de nombreuses copies des données ; les variations de délai sont donc très importantes, plus particulièrement dans le cas de transmissions volumineuses ou de longues listes de distribution. Une autre fonctionnalité propre au multicast est que le serveur ignore l'adresse de réseau des destinataires d'une transmission. Etant donné que tous les participants partagent la même adresse de réseau multicast, ils peuvent joindre un groupe multicast tout en préservant leur anonymat.

Notions élémentaires sur le multicast

La technologie de transmission multicast est disponible au niveau de la couche liaison de données (couche 2) et de la couche réseau (couche 3). Par exemple, Ethernet, FDDI (*Fiber Distributed Data Interface*), et SMDS (*Switched Multimegabit Data Service*) supportent tous deux les adresses MAC unicast, multicast et broadcast. Par conséquent, un ordinateur situé sur n'importe lequel de ces réseaux peut écouter simultanément une adresse unicast, plusieurs adresses multicast, et une adresse de broadcast. Token Ring supporte également le concept de diffusion multicast, mais il utilise une technique différente pour adresser des groupes de destinataires.

Si la portée d'une application multicast est limitée à un seul LAN physique ou logique, la transmission multicast au niveau de la couche liaison de données suffit. Toutefois, la plupart des applications multipoints n'ont d'intérêt que si leur portée peut atteindre un réseau de campus distribué, voire un environnement WAN qui intègre de nombreuses technologies de réseau différentes, telles que Ethernet, FDDI, Token Ring, Frame Relay et ATM. En ce qui concerne ces environnements étendus, le multicast doit en outre être implémenté au niveau de la couche réseau. La transmission multicast au niveau 3 implique certaines caractéristiques spécifiques :

- adressage ;
- enregistrement dynamique ;
- livraison multicast ;
- routage multicast.

Adressage

Une adresse de niveau 3 doit être utilisée afin de pouvoir communiquer avec un groupe de destinataires (au lieu d'un seul destinataire). De plus, cette adresse doit pouvoir être associée aux adresses multicast de niveau 2 des réseaux physiques sous-jacents. Pour les réseaux IP, des adresses de classe D ont été définies spécifiquement pour l'adressage multicast. Une adresse de cette classe comprend le chiffre binaire 1110 dans les bits de poids le plus fort du premier octet, suivi d'une adresse de groupe de 28 bits non structurée. Pour associer des adresses multicast IP à des adresses Ethernet, les 23 bits de poids le plus faible de l'adresse de classe D sont appliqués à un bloc d'adresses Ethernet réservées pour le multicast. Grâce à cette stratégie d'association, chaque adresse multicast Ethernet correspond à 32 adresses multicast IP. Cela signifie qu'un hôte qui reçoit des paquets multicast peut avoir besoin de refuser les paquets indésirables, envoyés à d'autres groupes avec la

même adresse multicast MAC. Ces adresses comprennent le chiffre binaire 01 dans le premier octet de l'adresse de destination, afin de permettre à l'interface de réseau de distinguer facilement les paquets multicast des paquets unicast.

Enregistrement dynamique

Un mécanisme doit permettre d'informer le réseau qu'un ordinateur donné est membre d'un groupe multicast particulier. En l'absence de cette information, le réseau serait obligé d'inonder le trafic, plutôt qu'envoyer la transmission en multicast pour chaque groupe. Sur les réseaux IP, le protocole IGMP (*Internet Group Multicast Protocol*), qui est un protocole de datagrammes IP utilisé entre les routeurs et les hôtes, assure la maintenance dynamique de listes de membres de groupes. L'hôte envoie au routeur un rapport d'adhésion IGMP (*Join*) pour rejoindre un groupe multicast. De son côté, le routeur envoie régulièrement une requête pour savoir quels membres participent toujours à un groupe donné. Si un hôte souhaite demeurer membre d'un groupe, il répond en envoyant un rapport. S'il n'envoie pas de rapport, le routeur élimine (*Prune*) l'hôte en question de la liste des membres, ce qui évite une transmission multicast inutile. Avec la version 2 de IGMP, un hôte peut envoyer un message de départ (*Leave*) afin d'informer le routeur qu'il ne souhaite plus participer à un groupe multicast. Cela permet au routeur de réduire la liste de membres, avant d'entamer le processus de requête suivant. Cette méthode réduit ainsi la période pendant laquelle des transmissions inutiles sont envoyées sur le réseau.

Livraison multicast

La majorité des applications multicast s'appuient sur le protocole UDP, qui assure une livraison au mieux (*best-effort delivery*) et n'utilise pas le mécanisme de fenêtrage de TCP qui permet d'éviter les congestions. Par conséquent, les paquets multicast sont plus souvent perdus que les paquets TCP. Il est peu pratique pour les applications en temps réel de demander des transmissions. Il arrive donc que les diffusions broadcast audio et vidéo subissent des dégradations de performances en raison de pertes de paquets. Avant le déploiement de la qualité de service (QoS, *Quality of Service*), le meilleur moyen pour limiter les pertes de paquets sur les réseaux fondés trames était de fournir une bande passante suffisante, surtout aux frontières du réseau. La fiabilité des transmissions multicast sera améliorée lorsque le protocole de réservation RSVP (*Reservation Protocol*), le protocole de transport en temps réel RTP (*Real-Time Protocol*), le standard 802.1p, et d'autres mécanismes de gestion de priorité de niveau 2, rendront possible la livraison de bout en bout de fonctionnalités de qualité de service sur un réseau de niveau 2/3.

Routage multicast

Un réseau doit pouvoir créer des arbres de distribution de paquets qui définissent un chemin de transmission unique entre le sous-réseau source et chaque sous-réseau membre d'un groupe multicast. Un des principaux objectifs de la construction d'un arbre de distribution est de garantir qu'une seule copie de chaque paquet sera envoyée sur chaque branche de l'arbre. Pour cela, un arbre recouvrant, dont la racine est le routeur multicast désigné de l'hôte émetteur, assure la connectivité vers les routeurs multicast désignés des hôtes destinataires. Pour le multicast IP, l'IETF a proposé plusieurs protocoles de routage multicast, dont DVMRP (*Distance Vector Multicast Routing Protocol*), MOSPF (*Multicast extensions to OSPF*), PIM (*Protocol-Indépendant Multicast*) et CBT (*Core-Based Tree*).

Les protocoles de routage multicast construisent des arbres de distribution en examinant la table de routage d'un protocole d'accès unicasting. Certains protocoles, tels que PIM et CBT, utilisent la table de transmission unicasting. D'autres emploient leurs propres tables de routage d'informations d'accès unicasting. DVMRP utilise son propre protocole de routage par vecteur de distance, et OSPF sa propre base de données d'états de liens, afin de déterminer comment élaborer des arbres de distribution basés sur la source.

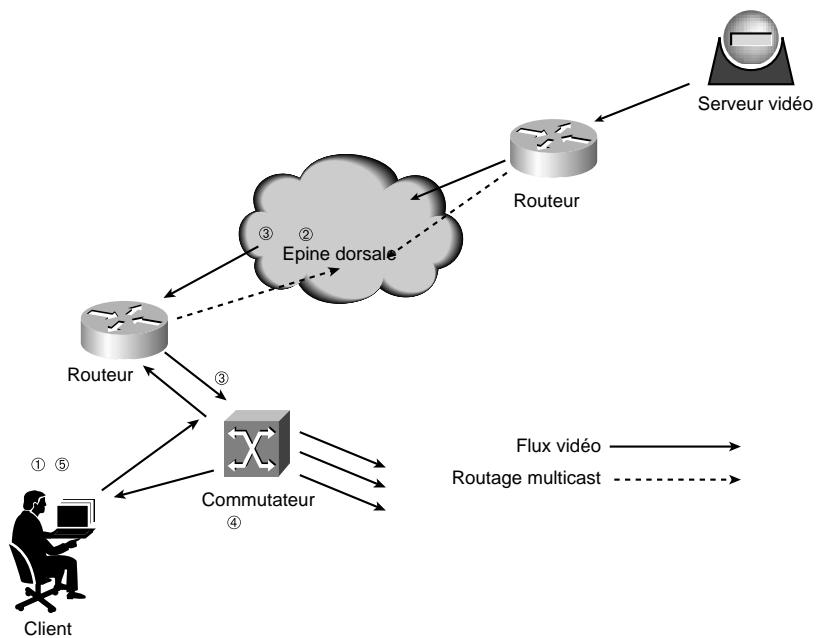
Ces protocoles sont divisés en deux catégories : ceux qui opèrent en mode dense (DM, *Dense Mode*), et ceux qui opèrent en mode clairsemé (SP, *Sparse Mode*). Les protocoles DM supposent que tous les routeurs sur le réseau auront besoin de distribuer du trafic multicast pour chaque groupe multicast (par exemple, presque tous les hôtes du réseau participent à chaque groupe multicast). Par conséquent, ils construisent des arbres en inondant initialement le réseau tout entier, puis en éliminant le faible de nombre de chemins exempts de destinataires. À l'inverse, les protocoles SM supposent que relativement peu de routeurs sur le réseau seront impliqués dans chaque multicast. Ils débutent donc par un arbre vide, auquel ils ajoutent des branches uniquement lorsqu'ils reçoivent des demandes explicites d'adhésion à un groupe multicast. Les protocoles DM (MOSPF, DVMRP et PIM-DM) conviennent mieux dans des environnements LAN avec des groupes de destinataires denses, tandis que les protocoles SM (CBT et PIM-SM) sont plus appropriés dans des environnements WAN. PIM est également capable de fonctionner en mode dense, en adaptant son comportement en fonction des caractéristiques de chaque groupe de destinataires.

Processus multicast

La Figure I.2 illustre un processus multicast dans lequel un client reçoit un flux multicast vidéo de la part d'un serveur. Ce processus comprend les étapes suivantes :

1. Le client envoie un message d'adhésion IGMP (*Join*) vers son routeur multicast désigné. L'adresse MAC de destination utilisée correspond à l'adresse de classe D du groupe rejoint, et non à celle du routeur. Le corps du datagramme IGMP inclut également l'adresse de groupe de classe D.
2. Le routeur enregistre le message d'adhésion, et utilise PIM, ou un autre protocole de routage multicast, afin d'ajouter ce segment dans l'arbre de distribution multicast.
3. Le trafic multicast IP émis par le serveur est maintenant distribué sur le sous-réseau du client *via* le routeur désigné. L'adresse MAC de destination correspond à l'adresse de classe D du groupe.
4. Le commutateur reçoit le paquet multicast, et examine sa table de transmission. S'il n'existe pas d'entrée pour cette adresse MAC, le paquet est transmis sur tous les ports dans le domaine de broadcast. Lorsqu'une entrée existe dans la table du commutateur, le paquet est transmis uniquement sur les ports désignés.
5. Avec IGMPv2, le client peut mettre fin à son appartenance au groupe en envoyant un message Leave IGMP au routeur. Avec IGMPv1, le client reste membre du groupe, jusqu'à ce qu'il omette de répondre à la requête du routeur. Les routeurs multicast envoient une requête IGMP périodique à tous les groupes d'hôtes multicast ou à un groupe spécifique sur le réseau, afin de déterminer ceux qui sont toujours actifs. Chaque hôte respecte un court délai aléatoire avant de répondre à la requête, et répond seulement si aucun autre hôte dans le groupe n'a encore répondu. Ce mécanisme évite une congestion sur le réseau.

Figure I.2
Processus multicast.



Exigences du multicast IP sur un réseau d'entreprise

Le support du multicast IP requiert des systèmes serveurs et clients configurés pour cette technologie, et au minimum une portion de l'infrastructure de réseau de routeurs, ainsi que des commutateurs de niveau 2 et 3 pour les interconnecter. Le multicast IP se prête bien à une implémentation progressive, en commençant par des sous-réseaux isolés, pour être ensuite étendu à un réseau de campus entier, voire à un réseau WAN. Ses exigences sont les suivantes :

- Les serveurs et les hôtes clients doivent utiliser une pile de protocoles IP qui supportent le multicast, tel que spécifié dans le RFC 1112. Le support complet de ce RFC (support de niveau 2) autorise les hôtes à envoyer et à recevoir des données multicast. Les piles TCP/IP qui supportent Windows Sockets V1.1 et V2.0 sont prévues pour le multicast.
- Les applications exécutées par les serveurs et les clients, telles que la diffusion broadcast audio, la diffusion broadcast vidéo et la vidéoconférence, doivent supporter le multicast IP. Ces applications imposent parfois des exigences spécifiques au niveau des ressources système, relatives par exemple à la vitesse du processeur, à la taille de la mémoire et, dans certains cas, à des cartes réseau ou cartes d'accélération graphique recommandées.
- Les cartes réseau de tous les hôtes destinataires doivent être configurées en vue de surveiller les paquets multicast, en plus des paquets unicast et broadcast habituels. En fonction de l'infrastructure du réseau, les hôtes destinataires peuvent également être dotés de cartes réseau intelligentes, capables de rejeter les paquets multicast de groupes indésirables, ce qui évite que le processeur de l'hôte ne soit inutilement interrompu.

- Une épine dorsale routée hautement performante, avec une connexion commutée vers l'émetteur et les hôtes destinataires, représente une infrastructure LAN hautement évolutive pour le multicast. Le summum de l'évolutivité serait atteint au moyen d'un réseau commuté de couche 2/3 de bout en bout entre l'émetteur et le destinataire. Une infrastructure commutée est préférable, car elle fournit en général suffisamment de bande passante pour pouvoir supporter la cohabitation d'applications unicast et multimédia sur un sous-réseau, sans nécessiter pour autant des mécanismes particuliers de gestion de priorité ou de réservation de bande passante. Dans le cas d'une bande passante dédiée pour chaque ordinateur de bureau, la commutation permet de réduire considérablement les collisions Ethernet qui peuvent perturber le trafic multimédia en temps réel (à noter qu'une bande passante duplex élimine complètement ces collisions). Un réseau à média partagé peut également être adopté pour des applications audio de faible bande passante ou pour des projets pilotes limités.
- Les commutateurs ne sont pas tous adaptés à la transmission multicast. Ceux qui conviennent le mieux possèdent une structure de commutation qui permet la transmission du trafic multicast vers un grand nombre de membres de groupes directement connectés, sans avoir à subir une charge excessive. Le commutateur peut ainsi gérer le nombre grandissant d'applications multicast, sans que d'autres trafics ne soient affectés. Les commutateurs de niveau 2 doivent également être dotés de certaines fonctionnalités multicast, afin d'éviter d'inonder tous leurs ports avec ce trafic. Pour cela, différents types de contrôles peuvent être appliqués au trafic multicast :
 - Des VLAN peuvent être définis en fonction des limites d'un groupe multicast. Bien que cette approche soit simple, elle ne supporte pas les changements dynamiques d'appartenance à des groupes, et ajoute la charge administrative des VLAN unicast.
 - Des commutateurs de niveau 2 peuvent examiner les requêtes et rapports IGMP, afin de connaître les correspondances de ports de membres de groupes multicast, ce qui permet de suivre dynamiquement les changements d'appartenance. Toutefois, l'examen de chaque paquet de données et de contrôle multicast peut consommer une grande quantité de ressources processeur, mais également dégrader les performances de transmission et augmenter la latence.
 - Le protocole GARP (*Generic Attribute Registration Protocol*) [IEEE 802.1p] peut être utilisé afin de permettre à un système terminal de communiquer directement avec le commutateur, de façon à joindre un groupe 802.1p correspondant à un groupe multicast. Ainsi, la charge de configuration de groupes multicast peut, en grande partie, être transférée de la couche 3 vers la couche 2, ce qui convient mieux sur de grands réseaux linéaires commutés.
 - Le rôle traditionnel du routeur en tant que point de contrôle du réseau peut être préservé en définissant un protocole multicast de communication routeur-commutateur, tel le protocole CGMP (*Cisco Group Multicast Protocol*), ce qui permet au routeur de configurer la table de transmission multicast du commutateur afin de refléter les informations d'appartenance actuelles.
- Le large déploiement de la transmission multicast sur des intranets ou sur des réseaux WAN implique obligatoirement de traverser plusieurs limites de sous-réseaux et sauts de routeur. Les routeurs intermédiaires et les commutateurs de niveau 3 entre les émetteurs et les destinataires doivent être configurés pour le multicast IP. Au minimum, les routeurs en entrée et en sortie de

l'épine dorsale devraient implémenter la transmission multicast IP. Si les routeurs d'épine dorsale ne supportent pas cette fonctionnalité, un tunnel IP (qui encapsule les paquets multicast dans des paquets unicast) peut être exploité en tant que solution temporaire, afin de relier des routeurs multicast. Bien que la plupart des versions récentes de logiciels de routeurs incluent un support pour le multicast IP, il n'existe pas encore de protocole de routage multicast reconnu comme standard de l'industrie et supporté par tous les fabricants, ce qui entraîne un problème d'interopérabilité sur les épines dorsales qui comprennent des routeurs multifabricants. Le choix d'un protocole de routage multicast (entre DVMRP, MOSPF, PIM et CBT) devrait être fondé sur les caractéristiques de l'application multicast déployée, ainsi que sur la densité et l'emplacement géographique des hôtes destinataires.

Microsoft NetShow et réseau multicast Microsoft

Microsoft NetShow est une solution complète de fourniture de services multimédias unidirectionnels unicast (*one-to-one*) et multicast (*one-to-many*) sur des réseaux d'entreprises ou sur l'Internet. Cette solution intègre des composants pour la création de contenus, le codage et le stockage, ainsi que des applications client-serveur pour délivrer du trafic multimédia sur des réseaux LAN et WAN. Elle s'accompagne d'un produit associé, Microsoft NetMeeting, qui constitue une solution pour les applications multimédias coopératives et interactives (*many-to-many*), telles que la vidéoconférence et les tableaux blancs partagés.

NetShow inclut un lecteur universel, qui permet d'accéder au contenu de fichiers au format ASF (*Advanced Streaming Format*) de Microsoft, et également à d'autres formats multimédias connus, tels que WAV, AVI, QuickTime, RealAudio et RealVideo. NetShow propose également le support logiciel d'une grande gamme de stratégies de compression/décompression (codecs) qui autorisent les auteurs de contenus à choisir l'algorithme le plus approprié en ce qui concerne leurs applications et la bande passante dont ils disposent. Le logiciel codec est automatiquement téléchargé sur le poste client, ce qui permet une décompression transparente de toutes les formes de contenus. La diffusion multimédia en temps réel (*streaming*) de haute qualité est supportée sur des bandes passantes allant de 3 Kbit/s (pour une qualité audio mono) à 8 Mbit/s (pour une qualité de broadcast vidéo, avec Microsoft NetShow Theater Server, et une compression MPEG au niveau matériel). Du contenu en temps réel peut être archivé sur disque en vue d'une visualisation ultérieure, à la demande. Dans NetShow, le support natif des protocoles de réseau inclut à la fois le mode unicast sur TCP, le multicast sur UDP et IGMPv2 pour le client. NetShow sur HTTP permet de visualiser du contenu NetShow hébergé sur l'Internet, sans nécessiter une configuration de pare-feu particulière ne sur le réseau de visualisation.

NetShow est étroitement intégré à d'autres applications Microsoft, telles que NT Site Server et Microsoft Office. Son intégration avec Site Server facilite la création de sites Web commerciaux qui proposent des contenus publicitaires et audio/vidéo. Son intégration avec PowerPoint autorise la création de présentations qui contiennent des pistes audio ou vidéo synchronisées.

Le réseau de campus de Microsoft, situé à Redmond dans l'état de Washington, supporte la diffusion multicast de contenus NetShow sur plus de 30 000 ordinateurs de bureau. La programmation multimédia locale inclut trois stations de radio et une chaîne de télévision, MSNBC. D'autres chaînes sont disponibles pour des utilisations plus ponctuelles, telles que la couverture d'événements ou d'annonces qui concernent l'entreprise. Ce contenu multimédia est ensuite archivé sur disque, afin

de pouvoir être visualisé à la demande. Microsoft prévoit d'étendre la couverture vidéo des événements de l'entreprise à tous les sites Microsoft d'Amérique du Nord. Il a également fait savoir que les récentes utilisations du réseau NetShow avaient permis de réaliser des économies quotidiennes de l'ordre de plusieurs millions de dollars. Par exemple, la diffusion multicast d'une réunion importante de la société élimine les coûts associés à la location d'une salle et au transport des 5 000 employés du campus. Microsoft a également réalisé des économies substantielles en matière de productivité, puisque de nombreux employés exploitent la visualisation à la demande, afin de limiter les interruptions de leurs cycles de travail. Un autre bénéfice moins évident du réseau multicast est l'amélioration de la qualité des communications, car tous les employés peuvent maintenant être pris en compte dans la diffusion des messages importants de l'entreprise pour un coût supplémentaire insignifiant.

Pour assurer une utilisation économique de l'espace de stockage sur disque, et maintenir les ressources du réseau, la bande passante des transmissions vidéo est optimisée à 110 Kbit/s. Les serveurs NetShow utilisés pour stocker le contenu multimédia sont situés dans le service informatique central, en compagnie d'environ 2 000 autres serveurs. Le contenu NetShow en temps réel est délivré à partir du site de campus Microsoft Studios. L'épine dorsale pour le trafic multicast est formée d'un maillage de routeurs de site Cisco 7500 qui exécutent PIM et CGMP, interconnectés sur un réseau d'épine dorsale de campus LAN ATM. L'un des cinq ELAN de l'épine dorsale est dédié au trafic multicast. La réplication des paquets multicast au niveau des branches de l'arbre de distribution PIM est réalisée par les commutateurs ATM, avec l'aide du serveur BUS (*Broadcast and Unknown Server*) point-multipoint. La connectivité physique des commutateurs ATM de site s'appuie sur l'infrastructure SONET privée de Microsoft. Chaque ordinateur de bureau dispose d'une connexion commutée Ethernet 10 Mbit/s dédiée, assurée par des commutateurs Cisco Catalyst 5000 ou 5500 qui exécutent CGMP, situés dans les armoires de câblage. Ces commutateurs sont regroupés au moyen de la technologie Cisco Fast EtherChannel, afin d'augmenter leur bande passante.

Index

A

AAL (ATM Adaptation Layer) *Voir Couches d'adaptation ATM*
Accès
 au média, sécurité 48
 commuté 31
 local, services de réseau 44
 RNIS
 de base 686, 687
 primaire 686
 Voir aussi Listes de contrôle d'accès
Access Control List *Voir Liste de contrôle d'accès*
ACF/VTAM (Advanced Communications Function/Virtual Telecommunication Access Method)
 200
Acquittement local, DLSw+ 257
Administration réseau
 composants du modèle d'événement Cisco 462
 conception et armoires de câblage 464
 configuration
 seuils RMON 469
 SNMP 480
 détermination du respect de l'accord SLA 496
 documentations MIB 473
 données de référence 467
 collecte régulière 471
 réduction 470
 erreurs
 CRC 499
 d'alignement 498
 événements de plates-formes 461
 filtrage Syslog 526

gestion des performances 517
instance MIB 478
interceptions SNMP
 introduction 460
 mise en œuvre 467
interrogations SNMP 472, 474
journalisation Syslog 466
messages Syslog 460
modèle d'événements Cisco 460
objets MIB à surveiller 473
outils d'acquisition de données 472
plate-forme NMS 472
ports vitaux 465
protocoles 459
recommandations
 sur les commutateurs 471
 sur les routeurs 511
reporting de temps de réponse 497
requêtes ping 466
scénarios de corrélation d'événements 508, 524
suivi des erreurs 466
surveillance des routeurs
 analyse et mise au point 515
 fonctions RMON 514
 interrogations SNMP 512
 messages Syslog 515
 suivi de l'environnement 516
traitement des événements 461
trames runts 499
utilisation des ressources processeur et mémoire 518
Voir aussi MIB (Management Information Base)
Voir aussi RMON

- Adressage**
- ATM 146
 - de la couche réseau 666
 - de nuage DDR 323
 - de soutien 44
 - de zone OSPF 85
 - EIGRP 75, 76
 - IP, segmentation 793
 - multicast IP 867
 - OSPF
 - privé 87
 - synthèse de routes 84
 - Résolution LANE 160
 - synthèse de routes 68
- Adresses**
- ATM, structure 146
 - connues, LECS LANE 168
 - MAC
 - code fabricant 21
 - commutation de niveau 2 21
- ADSL (Asymmetric Digital Subscriber Line) 9**
- Agrégats d'adresses, CIDR 133**
- AIP (ATM Interface Processor), interface du circuit de commutation 161**
- Algorithmes**
- de compression
 - de la voix 192
 - de Stacker 363
 - de routage
 - DUAL (Diffusing Update Algorithm) 77
 - HPR (High Performance Routing) 208
 - ISR (Intermediate Session Routing) 208
 - par état de lien 26
 - par vecteur de distance 26
 - RAND 363
 - services de l'épine dorsale 26
 - Spanning Tree et ELAN *Voir* Arbre recouvrant
- Alimentation redondante 53**
- Annuaire APPN**
- cache sécurisé 218
 - central 219
 - local 218
- AppleTalk**
- broadcast 832
 - configuration
 - d'un réseau 582
 - sur RNIS 701
 - intégration de EIGRP 582
- APPN (Advanced Peer-to-Peer Networking)**
- classe de service 204
 - conception avec FRAS BNN
 - APPN
 - dans le centre de données 253
 - sur les sites distants 253
 - centre de données et sites distants 252
 - réduction des nœuds de réseau 255
 - configuration
 - avec CIP, ESCON CMPC pour HPR 298
 - avec DLSW+ 236
 - avec stations terminales 233
 - réseau simple 230
 - RSRB et adresses virtuelles 221
 - emploi des DLUR/DLUS 209
 - encapsulation DLSw+ de SNA 206
 - environnement multiprotocole 224
 - établissement d'une session 207, 208
 - évolutivité 210
 - implémentation Cisco 210
 - intégration et routage 202
 - interréseaux 199
 - migration de sous-zone SNA 239
 - outils Cisco de gestion de réseau 228
 - réduction
 - des mises à jour *Voir* Nœuds APPN
 - des requêtes de localisation *Voir* Nœuds APPN
 - réseau de connexion 211
 - routage entre succursales 204
 - routeurs CIP et Sysplex 244
 - solutions de secours
 - liaisons WAN secondaires 220
 - prise en charge SSCP 223
 - redondance totale 221
 - sous-zones SNA 200
 - transport SNA natif 205
 - types de nœuds *Voir* Nœuds APPN
 - VTAM et nœuds interzones 254
- Arbres**
- binaires, commutation rapide 546
 - PIM-SM
 - de plus court chemin (SPT) 428
 - partagés 422
 - recouvrants (Spanning-Tree) 456
 - évolution d'un ELAN 164
 - problèmes inhérents 395

Architecture

- de commutation de paquets 537
- pare-feu 763

ARP (Address Resolution Protocol)

- découverte de routeurs 778
- fonctions proxy 46

ASIC, circuit 454**Asymmetric Digital Subscriber Line (ADSL)** 9**Asynchronous Transfer Mode** *Voir ATM***ATM (Asynchronous Transfer Mode)** 139-140, 153

- adressage 146
- AIP (ATM Interface Processor) 161
- avec LANE 609
- canal virtuel ou circuit virtuel 154
- cellules 154
- chemin virtuel 154
- circuits virtuels
 - commutés (SVC)
 - configuration 594
 - dépannage 597
 - topologie ATM avec SVC 594
 - permanents (PVC) 588
 - conception 589
 - configuration 590
 - dépannage 592
 - topologie ATM avec PVC 589

Classical IP sur ATM 603

commutateurs

- d'accès multiservice 390, 393
- d'entreprise 391
- groupes de travail et de campus 391

commutation 7

composants LANE 154

connexion VCC 592

couches fonctionnelles 141

- ATM 142

- d'adaptation ATM 143

- physique 141

définition PNNI 594

formats d'adresse 146

identifiant VPI 589

intégration 148

interfaces

- AIP 161

- NNI 152, 597

- UNI 152, 597

modules, PLIM 161

MPOA 587

PNNI sur réseaux LANE 162

réseaux multiservices 148

structure

- d'adresse ATM 146

- d'un réseau 152

supports de transmission 141, 147

technologies, médias WAN 9

Voir aussi LANE

ATM Interface Processor *Voir AIP***Attributs BGP** 113**Authentification**

- CHAP 341, 361

- DDR 666

- en texte clair 761

- MD5 762

- PAP 342, 361

- PPP 364

- voisin OSPF 760

B**Bandé passante**

- APPN 225

- commutation LAN 6

- Frame Relay 74

- gestion 38

- protocoles 73

Base de données de transmission 454**BECN (Backward Explicit Congestion Notification)** 186**Besoins utilisateur sur un réseau** 13**BGP (Border Gateway Protocol)** 103

- attributs 113

- d'origine (Origin) 114

- de cheminement (AS_path) 113

- de communauté (Community) 123

- de poids (Weight) 117

- de préférence

- d'accès AS (MED) 121

- locale (Local Preference) 119

- de prochain saut (Next Hop) 114

- BGP (Border Gateway Protocol) (*suite*)**
- cartes de routages 108
 - confédérations 134
 - contrôle d'instabilité 138
 - critères de sélection de chemin 124
 - distances administratives 125
 - externe 107
 - désactivation de la synchronisation 108
 - synchronisation 107
 - filtrage 125
 - d'attribut de cheminement AS_path 127
 - de communauté 129
 - de préfixe 126
 - par carte de routage 128
 - homologues
 - groupes 131
 - routeurs 104
 - interfaces de bouclage 106
 - Interne 105
 - redistribution de routes
 - dynamiques 111
 - statiques 110
 - rélecteurs de route 136
 - routing CIDR 133
 - stratégies de routage 125
- BNN/BAN (Border Network Node/Border Access Node)** 205
- BPX 8600, commutateur large bande** 151
- Broadcast**
- AppleTalk 832
 - Frame Relay
 - files broadcast 185
 - problèmes de diffusion broadcast 184
 - IP 828
 - niveaux de trafic 176
 - Novell 831
 - PSDN 176
 - réseaux commutés 827
 - services d'accès local 45
- BUS (Broadcast and Unknown Server), composant LANE** 156
- C**
- CAM (Content-Addressable Memory)** 454
- Campus**
- commutateurs ATM 150
 - Catalyst 5000 61
 - commutation
 - LAN 388
 - niveaux 2 et 3 5
 - conception et tendances 5
 - groupe de LAN 4
 - réseau commuté 63
 - technologies LAN 6
- Canaux virtuels, ATM** 154
- Cartes**
- d'accès à jeton 756
 - de routage, BGP 108
- Catalyst, commutateurs**
- ATM 150
 - Cisco 453
- CCITT (Comité Consultatif International pour la Télégraphie et la Téléphonie)** 633
- CCP (Compression Control Protocol)** 363
- CDP (Cisco Discovery Protocol)** 457
- CEF (Cisco Express Forwarding)** 553
- Cellules ATM** 154
- CGMP (Cisco Group Management Protocol)** 64
- Challenge Handshake Authentication Protocol**
Voir CHAP
- CHAP (Challenge Handshake Authentication Protocol)**
- authentification 341
 - contrôle d'accès 49
- Chemins**
- alternatifs
 - gestion du trafic 31
 - tolérance aux pannes 56
 - virtuels, groupe de circuits virtuels 154
- CIDR (Classless InterDomain Routing)** 133
- CIP (Channel Interface Processor)** 289
- chargement du microcode 298
 - combinaison avec SNA 292
 - configurations
 - DLSw+ 297
 - DLUR/DLUS 297
 - ESCON CMPC pour APPN HPR 298
 - exemples 309

- configurations
 - groupe de transmission CMPC 309
 - PCA, ESCON et MPC 294
 - RSRB 295
 - serveur TN3270 297
 - sous-canux CMPC 308
 - VTAM 297
 - VTAM XCA 302
 - fonctions réunies 291
 - utilisé seul 292
- CIR (Committed Information Rate)** 177
- Circuits**
 - DLSw+ 259
 - pour applications spécifiques 454
 - virtuels 154
 - permanents (PVC), sur ATM 588
- Cisco**
 - BPX 8600 151
 - Catalyst 5500 150
 - implémentation
 - APPN 210
 - LANE 161
 - logiciel de commutation Cisco IOS 394
 - modèle d'événements, administration 462
 - outils de gestion de réseaux APPN 228
 - sécurité
 - approche 726
 - cryptage des mots de passe 722
 - services 717
 - techniques
 - d'encapsulation 32
 - de commutation 537
- Classical IP sur ATM (RFC 1577)** 603
- CMPC (Cisco Multipath Channel)**
 - configurations CIP et VTAM
 - groupe de transmission CMPC 309
 - nœud
 - local SNA 308
 - principal VTAM TRL 307
 - sous-canaux CMPC 308
- Code MFG d'adresse MAC** 21
- Collecte de données de référence, administration** 467
- Commandes**
 - access-class 733
 - access-group 769
 - access-list 700, 766
 - access-list nbp 704
 - access-list other-access 704
 - access-list other-nbps 704
 - activate-on-demand 221
 - adapter 302
 - adjacent-cp-name 221
 - aggregate-address 134
 - appletalk cable-range 703
 - appletalk routing 703
 - appletalk send-rtmps 703
 - appletalk static 334
 - appletalk static cable-range 703
 - appletalk zone 703
 - appn link-station 231
 - area 793
 - async dynamic address 672
 - async dynamic routing 673
 - async mode interactive 673
 - backup delay 332
 - backup interface 332
 - backup load 332
 - bandwidth 691
 - banner 757
 - bgp default local-preference 120
 - chat-script 671
 - clear interface-async 677
 - cnsa, Cisco SNA 300
 - compress 363
 - controller 688
 - debug bri 374
 - debug dialer 325, 339
 - debug isdn 6q931 358
 - debug ppp authentication 363
 - debug ppp negotiation 359, 363
 - debug isdn q921 353
 - dialer callback-secure 693
 - dialer callback-server 693
 - dialer enable-timeout 693
 - dialer hold-queue 693
 - dialer idle-timeout 673, 689, 699
 - dialer in-band 637, 639, 673
 - dialer map 324, 360, 639, 671, 689, 699
 - dialer map snapshot 697
 - dialer rotary-group 356, 641, 673
 - dialer string 636, 650
 - dialer wait-for-carrier-time 636, 639, 699

Commandes (*suite*)

dialer-group 335, 637, 639, 674, 689, 700
dialer-in-band 636
dialer-list 335, 637, 674
dialer-list protocol 659
dialgroup 678
dial-on 678
distance 675
distribute-list out 675
dlsw duplicate-path-bias 273
dlsw explorer-wait-time 276
dlsw icannotreach 273
dlsw icanreach 273
dlsw local-peer 266
dlsw peer-on-demand-defaults tcp 284
dlsw remote-peer 266
dlsw remote-peer frame-relay 280
dlur 306
dlus-backup 306
enable 729
enable last-resort 755
enable use-tacacs 755
encapsulation 678
encapsulation frame-relay 580
encapsulation ppp 689
exec-timeout 733
frame-relay interface-dlci 281, 581
frame-relay map llc2 33 281
framing 688
hostname 703
interface dialer 641, 673
interface loopback 266
interface serial 580
ip address 678, 689
ip alias 735
ip community-list 130
ip route 637, 675, 689, 697
ip unnumbered 672
ipx network 580
ipx route 333
ipx router eigrp 581
ipx routing 580
ipx sap 333
ipx sap-incremental 581, 838
isdn answer1 365
isdn answer2 365
isdn caller 364

isdn incoming-voice data 359
isdn incoming-voice modem 358
isdn not end-to-end 360
isdn spid 691
isdn switch-type 355, 688, 690, 703
isdn tei 701
lan 302
lane config fixed-config-atm-address 169
linecode 688
link nom 307
login 676
map-class 693
match 108
maximum-lus 304
max-llc2-sessions 304
modem-def 677
modem-type 677
neighbor route-map 128
neighbor send-community 130
neighbor weight 119
network 112, 637, 675, 689
no appletalk send-rtmps 703
no connect-at-startup 221
no ip route-cache 668
no ip source-route 771
no redistribute 576
no service tcp-small-servers 735
no snmp-server trap authentication 732
passive-interface 639, 675
peer-on-demand-defaults 286
ppp authentication 364, 697, 700
ppp authentication chap 650
ppp callback 693
preferred-nnserver nom 306
pri-group 689
pri-group timeslots 355
prom-peer-default 286
ps -c 484
pu 304
pulse-time 637, 639
qllc dlsw 271
redistribute 110, 637, 674, 689
route-map 108
router igrp 637, 689
router ospf 674
routing ip 678
script reset 671

-
- sdlc address 269
 - sdlc role 269
 - sdlc role prim-xid-poll 269
 - sdlc xid 269
 - service compress-config 676
 - service password-encryption 733
 - session-timeout 678
 - set route map 108
 - set snmp 480
 - set speed 360
 - SGBP 369
 - show appletalk route 584
 - show biga 482
 - show buffers 518
 - show cam count dynamic 492
 - show configuration 733
 - show controller t1 356
 - show dialer 325
 - show dialer map 325
 - show inband 483
 - show interface 363, 518
 - show ip route 642
 - show ipx eigrp topology 576
 - show ipx route 575
 - show ipx servers 575
 - show isdn service 357
 - show isdn status 353, 357
 - show lane default 168
 - show log 485
 - show mac 496
 - show mbul 484
 - show memory 518
 - show module 490
 - show port counters 494
 - show ppp multilink 362
 - show processes 518
 - show spantree 491
 - show status 354
 - show system 488
 - show test 488, 490
 - show user 362
 - site 678
 - snapshot client 697
 - snapshot server 700
 - snmp-server community 732
 - source-bridge 267, 302
 - source-bridge ring-group 267, 302
 - speed 677
 - standby authentication 783
 - standby ip 782
 - standby preempt 782
 - standby priority 783
 - standby timers 783
 - standby track 785
 - tacacs-server authenticate enable 755
 - tacacs-server extended 756
 - tacacs-server host 755
 - tacacs-server last-resort 755
 - test appletalk nbp lookup 339
 - timers basic 675
 - tn3270-server 304
 - username 342, 671, 688, 690, 703
 - VPDN 370
 - vrn 307
 - write terminal 640, 733
- Committed Information Rate** *Voir CIR*
- Commutateurs** 20
- administration, état
 - de châssis 486
 - des ressources 482
- ATM 148
- BPX 8600 151
 - Catalyst 5500 150
 - d'accès multiservice 393
 - d'entreprise 61, 151, 391
 - de groupe de travail et de campus 61, 150, 391
 - modules redondants 170
 - multiservices 152, 390, 393
- avantages 58
 - Catalyst 453
 - d'accès multiservice 62
 - de liaisons
 - DLSw+ 258
 - WAN 7
- EARL, reconnaissance d'adresses 454
- fonctions RMON 458
- introduction 453
- LAN 60, 391
- LANE 161
- mémoire
- fonctions RMON 477
 - journalisation Syslog 478
- recommandations, administration 471

Commutateurs (*suite*)

- RNIS 351
 - AT&T 5ESS 352
 - configuration 687
 - DMS-100 352
 - National ISDN-1 352
 - table de transmission 454
 - VLAN 62
- Commutation**
 - administration
 - erreurs
 - CRC 499
 - d'alignement 498
 - trames runts 499
 - ATM 387
 - interface AIP 161
 - réseaux LAN 7
 - structure d'un réseau 152
 - CEF 553
 - avantages 556
 - équilibrage de charge 556
 - table
 - CEF 554
 - de voisinage 554
 - chemin d'un paquet 455
 - d'accès 31
 - de liaisons DLSw+ 257
 - de niveau 2 6, 21
 - de niveau 3 21
 - de paquets 171, 537
 - de réseau de campus 5
 - et routage 21
 - Ethernet 7
 - implications 22
 - LAN 387
 - augmentation de bande passante 6
 - microsegmentation 388
 - sur réseaux de campus 388
 - Token Ring 7
 - liaisons à la demande 31
 - locale 287
 - multicouche 453
 - optimale 551
 - par processus
 - équilibrage de charge 540
 - fonctionnement 538
 - inconvénients 541

plates-formes évolutives 390

- rapide
 - cache rapide 543
 - arbre binaire 546
 - limitations pour le routage IP 547
 - maintenance 548
 - structure 545
 - table de hachage 545
 - équilibrage de charge 550
- solutions de réseaux commutés 389
- store-and-forward (mode différé) 21
- système Cisco IOS (Internetwork Operating System) 394
- tables (de) 21
- via DLSW+ 216
- via FRAS BNN/BAN 217

Composants LANE

- client d'émulation LAN (LEC) 155
- serveurs
 - d'émulation LAN (LES) 155
 - de broadcast BUS 156
 - de configuration d'émulation LAN (LECS) 155

Confédérations BGP 134**Configuration**

- AppleTalk 582
 - sur RNIS 701
- APPN
 - avec DLSW+ 236
 - avec stations terminales 233
 - dans le centre de données 253
 - DLUR avec équilibrage de charge 249
 - DLUS 249
 - FRAS BNN 255
 - réseau simple 230
 - sur les sites distants 253
 - VTAM et noeuds inter-zones 254
- CIP (Channel Interface Processor)
 - DLSw+ 297
 - DLUR/DLUS 297
 - ESCON CMPC pour APPN HPR 298
 - PCA, ESCON, et MPC 294
 - RSRB 295
 - serveur TN3270 297
 - VTAM 297
 - VTAM XCA 302

- Classical IP sur ATM 604
- contrôleur de cluster 3174 816, 824
- DDR** 634
 - commande site 677
 - interfaces
 - asynchrones 672, 677
 - de bouclage 672
 - de numérotation 673
 - nom d'utilisateur 671
 - problèmes de sécurité 676
 - routage
 - OSPF 674
 - RIP 675
 - statique 675, 678
 - scripts de dialogue 677
- DLSw+ 266
- ELAN avec LANE 157
- HSRP 781
- IPX 572
- LANE sur ATM 611
- listes d'accès 837
- mises à jour SAP incrémentielles 838
- MPOA 624
- OSPF On Demand Circuit 97
- pour filtrage SNMP 336
- RNIS 687
- routage
 - DDR 326
 - avec Snapshot 330
 - IGRP pour DDR 637
 - Snapshot 696
 - routeur pare-feu 765
 - RSRB 221
 - serveur de communication pare-feu 769
 - SSRP 168
 - zones NSSA OSPF 94
- Congestion** 225
- Connectivité**
 - RNIS 348
 - ROBO 345
 - SOHO 345, 347
- Connexions**
 - à distance *Voir WAN*
 - d'homologues
 - à la demande 284
 - DLSw+ 259, 273
 - duplex *Voir Mode duplex*
- multipoint 809
- semi-duplex *Voir Mode semi-duplex*
- UNI, ATM 152
- VCC LANE 157
- virtuelles permanentes, Frame Relay 178
- Console, sécurité d'accès** 730
- Control Point, nœuds APPN** 201
- Contrôle**
 - d'accès 729
 - d'instabilité de route 138
 - de congestion 225
 - de flux, standard DLSw 260
- Contrôleurs de cluster**
 - configuration 816, 824
 - support de connexions point à point 821
- Convergence** 26, 71
 - EIGRP 77
 - OSPF 91
- Conversion de médias** 287
- Corrélation d'événements, administration** 462
- Correspondances de numérotation DDR** 323
- CoS (Class of Service)**
 - APPN 28
 - SNA 200
- Couches**
 - ATM 142
 - centrale 24
 - couche réseau 666
 - d'accès 25
 - d'adaptation ATM
 - AAL1 144
 - AAL2 144
 - AAL3/4 144
 - AAL5 144
 - de distribution 24, 37
 - OSI 23
 - physique ATM, sous-couche
 - de convergence 142
 - de média physique 141
- Coûts**
 - d'interconnexion, RNIS 349, 370
 - des réseaux
 - assistance 15
 - compromis sur les performances 15
 - équipements matériels et logiciels 15
 - expansion 15
 - improductivité 16

Coûts (suite)

- des réseaux (*suite*)
 - installation 15
 - irrécupérables 16
 - renonciation à une solution 16
- CPA (Channel Port Adapter)** 289
- Cryptage**
 - des données du réseau 758
 - des mots de passe Cisco 722
- CSNA (Cisco SNA)**
 - assignation d'adresse E/S 300
 - définition de LAN virtuel interne 301
 - support du serveur TN3270 303
 - DDDLU VTAM 304
 - définition de PU SNA 304

D**Data Link Switching Plus** *Voir DLSw+*

- DDR (Dial-on Demand Routing)** 315
 - adressage de nuage 323
 - analyse du trafic 319
 - authentification
 - CHAP 341
 - PAP 342
 - configuration
 - interface 638
 - listes d'accès 637, 639
 - paramètres et adresses IP 636
 - routage 637, 639
 - dynamique 642
 - site
 - central 635, 638, 640, 643, 645, 648
 - distant 637, 643, 645, 648, 651
 - sur RNIS 685
 - correspondances de numérotation 323
 - DLSw+** 285
 - encapsulation PPP 340
 - filtrage d'appel
 - informations SNMP 336
 - listes ACL 335
 - NBP d'AppleTalk 338
 - paquets
 - Banyan VINES, DECnet, et OSI 340
 - de répliques NDS 338
 - IPX 337
 - keepalive SPX 338
 - watchdog IPX 338

fonction de rappel 343

- interfaces
 - de connexion
 - groupes de rotation 322
 - modems asynchrones 321
 - RNIS 321
 - série synchrones 320
 - de secours 332
 - liaisons de secours 331
 - numérotation
 - DTR 657
 - V.25 bis 658
 - méthodes d'encapsulation 323
 - nuage de numérotation 316
 - profils de numérotation 322
 - RNIS 346, 349
 - routage
 - connexion dynamique 328
 - dynamique 327
 - horizon éclaté (split horizon) 328
 - interfaces passives 328
 - Snapshot 329
 - statique 326
 - routes statiques
 - flottantes 333, 654
 - mises à jour SAP 333
 - scripts de dialogue 660
 - secours de liaisons louées 653
 - sécurité RNIS 343
 - topologies
 - hub and spoke 318
 - point à point 317
 - totalemaillée 318
 - zones AppleTalk statiques 334
- Découverte de routeurs** 49
- Délimitation de trames PPP** 360
- Dependent Logical Unit (DLU)** 209
- Dial-on Demand Routing** *Voir DDR*
- Distances administratives, BGP** 125
- Distribution stratégique** 39
- DLCI (Data Link Connection Identifier), Frame Relay** 178
- DLSw Lite, encapsulation** 281
- DLSw** *Voir DLSw+*

DLSw+ (Data Link Switching Plus) 257, 265
 acquittement local 257
 commutation locale 287
 configuration
 avec APPN 236
 avec CIP 297
 minimale requise 266
 connexions d'homologues 259, 273
 contrôle de flux 260
 disponibilité 262
 échange entre routeurs 259
 encapsulation
 de SNA 206
 DLSw Lite 281
 FST 279
 HDLC directe 280
 TCP 278
 équilibrage de charge 263, 273
 établissement d'un circuit 259
 évolutivité 261
 homologues
 actifs multiples 278
 contrôle de la sélection 276
 de secours 276
 dynamiques 284
 groupes 261, 283
 inter-zones 261, 283
 intégration avec
 Ethernet 268
 QLLC 270
 SDLC 268
 Token Ring 267
 listes de ports 282
 pare-feu d'exploration 262
 redondance 273
 réduction de noeuds APPN 216
 routage
 DDR 285
 ODR 286
 snapshot 286
 standard DLSw 258
 surcharge de service d'encapsulation 281
 tolérance aux pannes 263
DLU (Dependent Logical Unit) *Voir* Unités logiques IBM, dépendantes

Données de référence, administration 467
DSL (Digital Subscriber Line) 9
DUAL (Diffusing Update Algorithm) 77

E

EARL (Enhanced Address Recognition Logic), circuit 454
EIGRP (Enhanced IGRP)
 adressage 75
 conception de réseaux 75
 convergence 77
 évolutivité du réseau 81
 intégration avec AppleTalk 583
 métriques 584
 redistribution de routes 585
 sélection de route 584
 intégration avec IPX 572
 métriques 576
 redistribution de routes 576
 réduction du trafic SAP 579
 sélection de route 576
 masques VLSM 75
 mises à jour
 partielles 81
 SAP incrémentielles 835
 redistribution de routes 561
 sécurité 81
 sélection de route 76
 synthèse de routes 76
 topologie 75
ELAN (Emulated LAN) 154, 156
 arbre recouvrant (Spanning-Tree) 164
 configuration
 de la base LECS 157
 des noms de LEC 157
 connexions VCC
 Configure Direct 157
 Control Direct 158
 Control Distribute 158
 Multicast Forward 159
 Multicast Send 159
 enregistrement LEC/LES 158
 interface ILMI 157
 interrogation du LECS 157
 recherche du serveur BUS 159

- Emulation LAN** 152
- EN (End Node), nœud APPN** 201
- Encapsulation**
- datagrammes RNIS 349
 - DDR 323
 - DLSw Lite 281
 - fonctions des routeurs Cisco 32
 - FST de DLSw+ 279
 - HDLC directe de DSLw+ 280
 - PPP 360
 - STUN, mise en œuvre 32
 - surcharge de services 281
 - TCP/IP de DSLw+ 278
 - techniques IBM 33
- End Node (nœud APPN)** 201
- End System-to-Intermediate System (ES-IS)** 49
- Enhanced IGRP** *Voir EIGRP*
- Epine dorsale**
- monoprotocole 59
 - multiprotocole 59
 - options de routage 59
 - OSPF 83
 - services de réseau 25
- Equilibrage de charge** 30
- commutation
 - CEF 556
 - par processus 540
 - rapide 550
 - DLSw+ 263, 273
 - HSRP 787
 - modèle multicouche LAN 404
 - OSPF 91
- Equipements de réseau** 20
- commutateurs 20, 58
 - hubs 20
 - ponts 20
 - routeurs 20, 58
- Erreurs**
- administration 466
 - CRC 499
 - d'alignement des trames 498
 - de routeur 511
 - trames runts 499
- ESCON, configuration avec CIP** 294
- ES-IS (End System-to-Intermediate System)** 49
- ETCD (Equipement Terminal de Circuit de Données), modes duplex et semi-duplex** 808
- Ethernet**
- commutation LAN 7
 - configuration de DLSw+ 268
- Événements**
- administration SNMP 460
 - modèle Cisco 462
 - moteur de corrélation 462
 - plates-formes SNMP 461
 - traitement 461
- Evolutivité**
- APPN 210
 - d'un réseau 72
 - DLSw+ 261
 - EIGRP 81
 - Frame Relay 178
 - modèle multicouche 415
 - OSPF 91
 - PIM-SM 444
 - plates-formes de commutation 390
 - réseaux hiérarchiques 173
 - RNIS 365
 - routage DDR 663
- Exigences de conception de réseaux** 12
- F**
- FECN (Forward Explicit Congestion Notification)** 186
- FEP (Front End Processor), NCP, génération** 811, 822
- Files**
- broadcast, Frame Relay 185
 - d'attente
 - de priorité 26
 - équitables pondérées 29
 - personnalisées 28
- Filtrage**
- BGP 125
 - DDR 334
 - NBP d'AppleTalk 338
 - paquets
 - de répliques NDS 338
 - IPX 337
 - keepalive SPX 338
 - watchdog IPX 338, 340
 - de l'identifiant d'appelant, RNIS 364
 - de zone et de service, couche de distribution 38
 - SAP 837

Fonction de rappel

DDR 343
RNIS 692

Formats

d'adresses ATM 146
de trames
 encapsulation 281
 traduction *Voir Trames*

Forward Explicit Congestion Notification (FECN)

186

Frame Relay

adaptation de trafic 190
bande passante consommée 74
BECN 186
bit DE 187
BNN/BAN (Border Network Node/Border Access Node) 205
CIR 178
commutation APPN via FRAS BNN/BAN 217
conception hiérarchique 178
connexions virtuelles permanentes 178
diffusions broadcast 184
DLCI 178
évolutivité 178
FECN 186
files broadcast 185
FRAS BNN et APPN 252
gestion
 de trafic multiprotocole 188
 des performances 186
interfaces virtuelles 183
métriques de coût 186
technologie WAN 9
topologies
 en étoile 182
 maillées
 hiérarchiques 179
 hybrides 181
 partiellement maillées 182
 totalement maillées 182
Voir aussi Voix sur Frame Relay

Frame Relay Access Support Boundary Network Node *Voir Frame Relay***FST (Fast Sequenced Transport), encapsulation de DLSw+ 279****G****Generic Routing Encapsulation (GRE) 34****Gestion du trafic**

accès commuté 31
adressage de soutien 44
alimentation redondante 53
broadcast 45
chemins alternatifs 31
contrôle
 de congestion 225
 de flux DLSw 260
découverte de routeur 49
distribution stratégique 39
encapsulation 32
équilibrage de charge 30
files d'attente
 de priorité 26
 équitables pondérées 29
 personnalisées 28
filtrage de zone et de service 38
Frame Relay 188
gestion de la bande passante 38
inter-zones OSPF 90
liens redondants 51
limitation du trafic
 mises à jour 286
 SAP 579, 835
listes d'accès 765
microsegmentation 58, 388
multicast 45
noms, proxy et cache 46
optimisation de l'acheminement 26
pare-feu d'exploration 262
redistribution de route 42
réseau APPN
 gestion de la bande passante 225
 mémoire consommée 228
RNIS 370
sécurité
 accès au média 48
 IP 764
segmentation de réseau 45
services de passerelle 40
techniques intraprotocole 27
temps de latence 225
tolérance aux pannes 55
traduction de format de trame 42
vitesse d'accès au média 225

-
- Gigabit Ethernet, technologie de LAN** 7
 - GRE (Generic Routing Encapsulation)** 34
 - Groupes**
 - d'homologues
 - BGP 131
 - DLSw+ 261
 - de recherche de ligne 664
 - de rotation de numérotation 322
 - de secours Hot Standby 783
 - de travail, commutateurs ATM 150
 - H**
 - HDLC (High-level Data Link Control)** 280
 - High Performance Routing, routage APPN** 208
 - Homologues**
 - actifs multiples 278
 - BGP
 - groupes 131
 - routeurs 104
 - de secours 276
 - DLSw+ 258
 - dynamiques 284
 - groupes 261, 283
 - interzones 261, 283
 - Hot Standby Routing Protocol** *Voir HSRP*
 - HSRP (Hot Standby Routing Protocol)** 57, 169, 777
 - configuration 781
 - équilibrage de charge 787
 - groupes de secours Hot Standby 783
 - interaction avec protocoles routés 789
 - messages multicast 780
 - MHSRP 783
 - proxy ARP 780
 - routeurs
 - LANE redondants 165
 - virtuels 778
 - schéma de priorité 780
 - suivi d'interface 785
 - Hub-and-Spoke (topologie)** 696
 - Hubs** 20
 - I**
 - IARP (Inverse Address Resolution Protocol)** 189
 - IBM**
 - techniques d'encapsulation 33
 - unités logiques 27
 - ICMP Router Discovery Protocol** *Voir IRDP*
 - Identifiants de chemins virtuels** 154
 - IGRP (Interior Gateway Routing Protocol)**
 - configuration du routage 637
 - solution propriétaire 14
 - ILMI (Interim Local Management Interface)** 157
 - Intégration de réseaux**
 - ATM 148
 - DLSw+ 266
 - LAN/WAN 10
 - RNIS 345
 - tendances 11
 - Interceptions SNMP**
 - de routeurs 513
 - événements 460
 - mise en œuvre 467
 - Interconnexion de réseaux** 3
 - Interfaces**
 - ATM
 - UNI et NNI 152
 - CLI, administration
 - bases de données de transmission de pont 492
 - châssis et environnement 488
 - erreurs de pont 494
 - modules de commutateur 489
 - ressources processeur 482
 - statistiques mémoire 518
 - taux d'utilisation des ports 496
 - topologie Spanning-Tree 491
 - utilisation des ressources processeur et mémoire 518
 - de bouclage, BGP 106
 - de connexion DDR
 - groupes de rotation 322
 - modems asynchrones 321
 - RNIS 321
 - série synchrones 320
 - de numérotation DDR 315
 - passives DDR 328
 - RNIS
 - d'accès de base BRI 350
 - d'accès primaire PRI 355
 - série synchrones 320
 - virtuelles 183
 - Interim Local Management Interface (ILMI)** 157
 - Interior Gateway Routing Protocol** *Voir IGRP*
 - Intermediate System-to-Intermediate System (IS-IS)** 15

- Internet Protocol Security Option (IPSO)** 48
Internet Protocol *Voir IP*
Interréseaux DLSw+ 257
Inverse Address Resolution Protocol *Voir IARP*
IP (Internet Protocol)
 - broadcast 828
 - configuration DDR 636
 - HSPR 777
 - sécurité *Voir Sécurité IP*
 - segmentation d'un espace d'adresse IP 793**IPSO (Internet Protocol Security Option)** 48
IPX (Internetwork Packet Exchange)
 - configuration
 - d'un réseau 572
 - sur RNIS 705
 - filtrage DDR 337
 - intégration de EIGRP 571
 - réduction du trafic SAP 835
 - filtrage par listes d'accès 837
 - mises à jour incrémentielles 838**IRDP (ICMP Router Discovery Protocol), découverte de routeurs** 49, 778
IS-IS (Intermediate System-to-IS) 15
ISR (Intermediate Session Routing), routage APPN 208
- K**
- Keepalive (messages)** 286
- L**
- L2F (Level 2 Forwarding)** 368
LAN (Local Area Network)
 - campus 4
 - commutateurs 60, 391
 - commutés, modèle multicouche 401
 - connexion à des services PSDN 171
 - CSNA et LAN interne pour SNA *via* CIP 301
 - émulation (LANE) 152
 - émulé (ELAN) *Voir ELAN*
 - intégration avec les réseaux étendus 10
 - interconnectés, APPN 200
 - technologies de réseau de campus 6**LANE (LAN Emulation)** 152
 - client (LEC) 155, 611
 - composants 154
 - conception 161**connexions**
 - LEC-BUS 619
 - LEC-LEC 621
 - LEC-LECS 616
 - LEC-LES 618**épine dorsale LANE ATM** 411
fonctionnement *Voir ELAN*
HSRP 165
implémentation, commutateurs et routeurs 161
PNNI 162
redondance 164
 - adresse LECS connue 168
 - emploi
 - de HSRP 169
 - de SSRP 168
 - partitions de réseau 169
 - réseaux LANE 1.0 165**résolution d'adresse** 160
serveur (LES) 155, 612
serveur de configuration (LECS) 155, 611
SSRP 165
sur ATM 609
Latence 225
LCN (Logical Channel Number) 178
LCP (Link Control Protocol) 361
LDN (Local Directory Number) 353
LEC (LAN Emulation Client), composant LANE 155
LECS (LAN Emulation Configuration Server), composant LANE 155
LEN (Low Entry Node), nœud APPN 201
LES (LAN Emulation Server), composant LANE 155
Level 2 Forwarding (L2F) 368
Liaisons
 - à la demande 31
 - asynchrones 807
 - de secours
 - DDR 331
 - RNIS 347
 - DLSw+ 257
 - louées 9
 - appuyées par DDR 653
 - WAN *Voir WAN***Lignes** *Voir Liaisons*
Link Control Protocol (LCP) 361

Listes de contrôle d'accès (ACL) 736

- application sur un routeur 738
- de pare-feu 765
- dynamiques (Lock-and-Key) 749
- étendues 741
- exemple de configuration DDR 637
- filtrage DDR 335
- fonctionnement 736
- masque générique 739
- réflexives 743
- services de distribution 38
- standards 740

Listes de ports 282**LLC2 (Logical Link Control-Type 2), encapsulation DLSw Lite** 281**Local Area Network** *Voir LAN***Local Directory Number, RNIS** 353**Logical Channel Number, X.25** 178**Low Entry Node (nœud APPN)** 201**LU** *Voir Unités logiques IBM***M****MAC (Media Access Control)**

- adresses 21
- commutation 21

Masque générique, listes ACL 739**Matériel de secours** 56**Media Access Control** *Voir MAC***Médias**

- ATM 147
- pour réseaux étendus 10
- sécurité d'accès 48

Mémoire

- CAM, pont/commutateur 454
- exigences APPN 228
- protocoles 72

Messages

- BIND 208
- Join 422
- keepalive 286
- LOCATE 207
- LSA 95
- Prune 422
- quench 38
- Register 435
- Register-Stop 436
- Syslog, administration 460

Métriques

- de coût, Frame Relay 186
- de routage
 - EIGRP 76
 - OSPF 90

MHSRP (Multigroup HSRP) *Voir HSRP***MIB (Management Information Base)**

- base de données de transmission de pont 492
- châssis et environnement 486
- documentation 473
- erreurs de pont 493
- états de l'environnement 516
- EtherChannel 506
- groupes système et châssis 502
- instances, chaînes de communauté 478
- interceptions SNMP de routeurs 513
- interfaces réseau 522
- interrogation SNMP 473, 474
- modules 489
- cartes de lignes 503

objets

- à surveiller 473

- divers 507

- MIB-II 500

- performances d'ensemble 497

- ports 504

- de tronçons 497

- ressources

- commutateur 482

- processeur 518

- RSM 506

- statistiques mémoire 518

- tampons 520

- taux d'utilisation des ports 495

- topologie Spanning-Tree 491

- tronçons 505

- VLAN 505

Microcode CIP, chargement 298**Microsegmentation** 58, 388**Migration**

- de sous-zone SNA vers APPN 239
- stratégies pour réseaux commutés 417

MIP (MultiChannel Interface Processor) 355**Mise en cache, commutation rapide** 543**Mises à jour**

- complètes 73
- EIGRP 81

- IGRP 73
- IPX 337
- OSPF 92
- par inondation 73
- partielles 73
- réduction 286
- SAP
 - filtrage par listes d'accès 837
 - incrémentielles 835, 838
 - réduction 835
- MLP** *Voir Multilink PPP*
- MMP** *Voir Multichassis Multilink PPP*
- Modèles**
 - d'adhésion explicite, PIM-SM 422
 - d'événements Cisco
 - administration 460
 - composants 462
 - Voir aussi* Événements
 - de référence OSI 23
 - hiérarchiques
 - avantages 173
 - conception 172
 - couche
 - centrale ou épine dorsale 24
 - d'accès 25
 - de distribution 24
- Modélisation de la charge de travail** 16
- Modems**
 - agrégation 348
 - analogique 9
- Modes**
 - duplex
 - ETCD 808
 - liaisons asynchrones 807
 - SNA 808
 - multipoint 809
 - semi-duplex
 - ETCD 808
 - liaisons asynchrones 807
 - SNA 808
- Modules ATM**
 - PLIM 161
 - redondants 170
- Mots clés**
 - accept 693
 - b8zs 688
 - bias 263
- broadcast 673, 699
- cost 275
- demand 678
- dialer 693, 697
- dynamic 284
- eigrp 581
- esf 688
- established 766
- first-call 701
- ip 673
- keepalive 285
- linger 277
- local 676
- modem-script 673
- name 673, 697
- no-lc 284
- passive 273
- pass-thru 280
- password 703, 755
- predictor 363
- primary 269
- promiscuous 266
- request 693
- RO 732
- route-map 674
- rsup-only 581, 838
- RW 732
- secondary 269
- speed 689
- stac 363
- static 110
- subnets 674
- succeed 755
- suppress-statechange-update 698
- suppress-statechange-updates 695
- system-script 673
- timeout 286
- timeslots 689
- xid-passthru 269
- MPC (Multipath Channel), configuration avec CIP** 294
- MPOA (Multiprotocol over ATM)** 400
 - Classical IP sur ATM (RFC 1577) 603
 - conception 604
 - configuration 604
 - dépannage 605
 - topologie 604

- MPOA (Multiprotocol over ATM) (*suite*)**
- client MPC 623
 - conception 623
 - configuration 624
 - découverte du MPS 627
 - dépannage 626
 - imposition de cache 629
 - LANE sur ATM 609
 - conception 610
 - configuration 611
 - dépannage 614
 - topologie 611
 - processus de résolution MPOA 628
 - serveur MPS 623
 - sur une configuration AAL5 (RFC 1483) 588
 - topologie 624
- Multicast**
- connexions VCC 156
 - HSRP 780
 - IP 413, 827
 - adressage 867
 - avantages 865
 - enregistrement dynamique 868
 - exigences 870
 - livraison 868
 - Microsoft NetShow 872
 - notions de base 867
 - processus 869
 - routage 868
 - multicast, PIM-SM 421
 - services d'accès local 45
 - MultiChannel Interface Processor (MIP)** 355
 - Multichassis MultiLink PPP (MMP)**
 - groupes de numérotation Stack Group 368
 - L2F 368
 - RNIS 367
 - Multilink PPP (MLP)** 361
 - Multiprotocole sur ATM** *Voir* MPOA
- N**
- Name Binding Protocol (NBP)** 833
- NAS (Network Access Server)** 346
- NAT (Network Address Translation)** 365
- NBP (Name Binding Protocol)** 833
- filtrage DDR 338
 - fonctions proxy 46
- NCP (Network Control Program)**
- processus de génération 811
 - support de QLLC 270
- NCP (Network Control Protocols)** 361
- NetBIOS**
- DLSw+ 257
 - établissement d'un circuit DLSw 260
- Network Access Server** 346
- Network Address Translation (NAT)** 365
- Network Control Protocols (NCP)** 361
- Network Node (nœud APPN)** 201
- NMS, station d'interrogation SNMP** 473
- NN (Network Node) (nœud APPN)** 201
- NNI (Network-to-Network Interface), ATM** 597
- Nœuds**
- APPN 206
 - EN (End Node) 201
 - établissement d'une session 207
 - identificateurs 207
 - LEN (Low Entry Node) 201
 - lignes de secours 220
 - NN (Network Node) 201
 - nœud de routage virtuel (VRN) 213
 - paquets LOCATE
 - annuaire central 219
 - cache d'annuaire sécurisé 218
 - enregistrement central des ressources 219
 - entrées d'annuaire partielles 218
 - réduction des diffusions 217
 - paquets TDU
 - APPN sur DLSW+ 216
 - APPN sur FRAS BNN/BAN 217
 - APPN sur RSRB 217
 - réduction des mises à jour 211
 - réduction des sessions CP-CP 214
 - réduction du nombre de liens 211
 - réduction du nombre de noeuds 216
 - point de contrôle (CP) 201
 - routage intermédiaire de session 208
 - commutés par VTAM 815
 - de routage virtuel 213
 - distant virtuels, RNIS 365
- NUAGE DE NUMÉROTATION DDR** 316

O

- ODC (On Demand Circuit)** 96
- ODR (On-Demand Routing)** 101, 286
- On Demand Circuit (ODC)** 96
- On-Demand Routing (ODR)** 286
- Open Shortest Path First** *Voir OSPF*
- Optimisation du routage** 26
- OSPF (Open Shortest Path First)**
 - adressage
 - de zone 85
 - privé 87
 - conception de réseaux 81
 - convergence 91
 - épine dorsale 83
 - équilibrage de charge 91
 - évolutivité du réseau 91
 - masques VLSM 86
 - mises à jour 92
- ODC (On Demand Circuit)**
 - configuration 97
 - fonctionnement 96
 - utilisation 96
- redistribution de routes 561
- réseau non broadcast, mode
 - NBMA 98
 - point-multipoint 98
- sécurité 92
- élection de route 90
- synthèse de routes 84
 - annonces
 - épine dorsale-zone 88
 - zone-épine dorsale 88
 - techniques 87
- topologie 82
- trafic inter-zones 90
- zones 84
 - NSSA 92
 - annonces LSA Type 7 94
 - configuration 94

P

- Packet Switched Data Network** *Voir PSDN*
- Pannes**
 - chemins alternatifs 31
 - de LECS LANE 165
 - de LES/BUS LANE 165

PAP (Password Authentication Protocol) 342

- Paquets**
 - commutation 455, 537
 - de type voix 841
 - services de commutation 171
- Pare-feu**
 - d'exploration 262
 - sécurité IP 763
- Passerelles 40**
- PCA (Parallel Channel Adapter), configuration avec CIP 294**
- Performances**
 - commutation de niveau 2 6
 - Frame Relay 186
 - PSDN 177
 - SMDS 9
- PIM-SM (Protocol Independent Multicast Sparse Mode)**
 - actualisation d'état 434
 - arbres
 - de plus court chemin (SPT) 428
 - adhésion 429
 - basculement 439
 - élagage 430
 - partagés 422
 - adhésion 423
 - élagage de branche 426
 - élagage de source 441
 - enregistrement de source 434
 - évolutivité 444
 - messages
 - Join 422, 433
 - Prune 422, 433
 - Register 435
 - Register-Stop 436
 - modèle d'adhésion explicite 422
 - point de rendez-vous (RP) 422
 - routeur désigné (DR) 443
 - découverte 444
 - reprise de fonction 443
- Ping, administration 466**
- Plates-formes de commutation évolutives 390**
- PNNI (Private Network to Network Interface), spécification ATM 162, 594**

- Point de contrôle (CP), nœud APPN** 201
- Point-to-Point Protocol** *Voir PPP*
- Ponts** 20
 RSRB, réduction de nœuds APPN 217
 table de transmission 454
- Ports**
 analyseur SPAN 457
 de commutateurs, administration des éléments critiques 465
 listes DLSw+ 282
 Telnet VTY 731
- PPP (Point-to-Point Protocol)**
 authentification 361, 364
 CCP 363
 délimitation de trames 360
 encapsulation de RNIS 360
 LCP 361
 Multilink PPP (MLP) 361
 NCP 361
- Priorité de trafic, services de l'épine dorsale** 26
- Problèmes de conception d'un réseau** 12
- Processeur et protocoles** 72
- Profils**
 numérotation DDR 322
 virtuels, RNIS 367
- Protocoles**
 BECN (Backward Explicit Congestion Notification) 186
 CCP (Compression Control Protocol) 363
 CDP (Cisco Discovery Protocol) 457
 CGMP (Cisco Group Management Protocol) 64
 CHAP(Challenge Handshake Authentification Protocol) 49
 de routage DDR 327
 ES-IS (End System-to-Intermediate System) 49
 FECN (Forward Explicit Congestion Notification) 186
 HSRP (Hot Standby Routing Protocol) 57
 HSRP (Hot Standby Routing rProtocol) 165
 IARP (Inverse Address Resolution Protocol) 189
 IP (Internet Protocol) 715
 IRDP (ICMP Router Discovery Protocol) 49
 L2F (Level 2 Forwarding) 368
 LCP (Link Control Protocol) 361
 MLP (Multilink PPP) 361
 MMP (Multichassis MultiLink PPP) 367
 MPOA (Multiprotocol over ATM) 587
- NBP (Name Binding Protocol) 833
 NCP (Network Control Protocols) 361
 niveaux de trafic broadcast 176
 NNI (Network-to-Network Interface) 152
 OSPF (Open Shortest Path First) 81
 OSPF ODC (On Demand Circuit) 95
 PIM-SM (Protocol Independent Multicast Sparse Mode) 421
 PPP (Point-to-Point Protocol) 360
 Proxy ARP (Proxy Address Resolution Protocol) 49
 Q.931 379
 RDP (Router Discovery Protocol) 833
 ressources consommées
 bande passante 73
 mémoire 72
 processeur 72
 routage
 par EIGRP 73
 par état de lien 73
 par vecteur de distance 73
 RIP (Routing Information Protocol) 50
 SAP (Service Advertisement Protocol) 835
 SGBP (Stack Group Bidding Protocol) 368
 SNA (Systems Network Architecture) 200
 SSP (Switch-to-Switch Protocol) 258
 SSRP (Simple Server Replication Protocol) 165
 STP (Spanning-Tree Protocol) 456
 topologie de réseau 68
 UNI (User-to-Network Interface) 152
Voir aussi Routage
- Proxy ARP (Address Resolution Protocol)** 49
- Proxy, résolution**
 ARP 46
 NBP 46
- PSDN (Packet Switched Data Network)**
 circuits virtuels 177
 conception hiérarchique 172
 diffusions broadcast 173, 176
 Frame Relay 178
 topologies
 en étoile 174, 182
 partiellement maillées 175, 182
 totalement maillées 175, 182
- PVC (Permanent Virtual Circuit), sur ATM** 588

Q

Q.931, RNIS 379
QLLC (Qualified Logical Link Control), configuration de DLSw+ 270

R

Rappel (callback)
 DDR 343
 RNIS 364

RDP (Router Discovery Protocol) 833
Redistribution de routes 42

BGP
 dynamiques 111
 statiques 110

EIGRP et OSPF 561
 ajout dans une liste de distribution 568
 configuration 561
 états de liens 566
 vérification 565

Redondance
 APPN 220, 221
DDR
 interfaces de secours 332
 lignes de secours 331, 653
 routes statiques flottantes 333
 LANE 164
 liaisons WAN 51
 modèle multicouche LAN 404
 OSPF 83
 routeurs DLSw+ 273
 SSRP 168
 systèmes d'alimentation 53
 topologies
 partiellement maillées 53
 totalement maillées 53

Réflecteurs de route, BGP 136

Relais de trames *Voir* Frame Relay

Réseau de connexion, réduction de liens APPN 211

Réseau Numérique à Intégration de Services *Voir*

RNIS

Réseaux

à commutation de paquets *Voir* PSDN
 AppleTalk 832
 APPN 199
 ATM 139

commutés
 broadcast 827
 de campus 63

conception
 choix d'un modèle 23
 évaluation
 des besoins utilisateur 13
 des coûts 15
 exigences 12
 modèle hiérarchique 24
 modélisation de la charge de travail 16
 problèmes 12
 solutions propriétaires ouvertes 14
 test de sensibilité du réseau 17

d'entreprise commutés 681

DDR 315
 évolutifs 663
 adresses de prochain saut 667
 adresses de sous-réseau 666
 authentification 666
 choix du média 664
 configuration des routeurs 670, 676
 convergence 669
 matériel 665
 protocoles requis 664
 schémas de trafic 664
 stratégie de routage 668

de campus 4, 388

de FAI commutés 683

EIGRP 75

équipements 20

étendus *Voir* WAN

fédérateurs *Voir* Epine dorsale

Frame Relay 178

guerre de l'information 720

hiérarchiques
 Frame Relay 178
 PSDN 172

intégration 11

interconnexion 3

IP 68
 broadcast 828
 évaluation de l'état de sécurité 717
 sécurité 715

Réseaux (*suite*)

LAN commutés
 augmentation de la bande passante 408
 avantages du modèle multicouche 419
 composants 390
 conception 385, 396
 épine dorsale LANE ATM 411
 modèle
 de VLAN de campus 398
 hub et routeur 397
 multicouche 401
 multicast IP 413, 827
 organisation de la couche centrale 409
 plates-formes de routage 393
 portage dans le modèle multicouche 418
 positionnement des serveurs 410
 problèmes d'évolutivité 415
 sécurité du modèle multicouche 418
 solutions 389
 stratégies de migration 417
 technologies de conception 387
 LANE 157
 locaux *Voir* LAN (Local Area Network)
 multiservices 148
 Novell 831
 Novell IPX et Snapshot 698
 OSPF 81
 protocoles d'administration 459
 RNIS 345
 segmentation 45, 388
 services
 d'accès local 44
 de distribution 37
 de l'épine dorsale 25
 SNA 200
 Token Ring 7
 topologies 174
 VLAN 394, 455
 voix
 en paquets 841
 sur Frame Relay 190
 vulnérabilités 721

RIP (Routing Information Protocol) 50
 découverte de routeurs 778

RMON
 Cisco TrafficDirector 473
 contraintes de mémoire 477

couches OSI 459
 documentations MIB 473
 fonctions d'administration 458
 gestion de seuils 476
 groupes de base RMON-1 476
 instance MIB 478
 objets MIB à surveiller 473
 seuils de référence
 adaptation 470
 configuration 470
 types 469
 surveillance de routeurs 514
 version réduite sur Catalyst 476

RNIS (Réseau Numérique à Intégration de Services) 345
 accès
 de base 686
 primaire 686
 agrégation de modems 348
 configuration
 AppleTalk 701
 commutateur 687
 DDR 685
 fonction de rappel 692
 interface en natif 687
 IPX 705
 numéros d'identification de lignes appelantes 691
 routage Snapshot 694

connectivité
 RNIS 348
 ROBO 345
 SOHO 345, 347

de bout en bout
 réseau RNIS données sur voix 359
 signalisation SS7 358
 vitesse des chemins de données 359

dépannage 373
 authentification PPP 383
 commande debug bri 374
 de la couche
 liaison de données 376
 physique 374
 réseau 378
 interface PRI 375
 message RELEASE_COMP 381
 négociation LCP 381

- dépannage
 - processus TEI 376
 - protocoles NCP 384
 - Q.931 379
 - SPID 380
- encapsulation
 - de datagrammes 349
 - PPP 360
- évolutivité 365
- fonctions NAT 365
- interface
 - BRI
 - configuration 351
 - contrôle du fonctionnement 353
 - équipements de communication 350
 - identifiant SPID 352
 - implémentation 350
 - LDN 353
 - types de commutateurs 351
 - DDR 321
 - PRI
 - cartes MIP 355
 - configuration 355
 - contrôle du fonctionnement 356
- limitation des coûts 349, 370
 - analyse du trafic 370
 - application CEA 373
 - comptabilité AAA 373
 - exploitation de SNMP 371
 - formation des utilisateurs 371
 - structure de tarification 371
- Multichassis Multilink PPP (MMP) 367
- NAS (Network Access Server) 346
- noeuds distants virtuels 365
- profils virtuels 367
- routage DDR 346, 349
 - secours par ligne commutée 347
 - sécurité
 - authentification PPP 364
 - DDR 343
 - filtrage de l'identifiant d'appelant 364
 - modèle 349
 - rappel de l'appelant 364
 - vérification du numéro appelé 365
- technologie WAN 9
- Routage** 387
 - algorithmes 26
- APPN 202
 - connexion *via* FRAS BNN/BAN 217
 - intermédiaire de session 208
 - pont RSRB 217
 - Sysplex 247
 - via* DLSW+ 216
 - CIDR 133
 - classe de service APPN 204
 - contrôle d'instabilité de route 138
 - DDR 315
 - connexion dynamique 328
 - dynamique 327
 - évolutivité 663
 - horizon éclaté (split horizon) 328
 - interfaces passives 328
 - RNIS 346, 349
 - Snapshot 329
 - statique 326
 - via* DLSW+ 285
 - DLSW+ 259
 - entre succursales, APPN 204
 - et commutation 21
 - évolutivité du réseau 72
 - métriques
 - EIGRP 76
 - OSPF 90
 - monoprotocole 59
 - multicast IP 868
 - multiprotocole 59
 - ODR 101, 286
 - options de l'épine dorsale 59
 - par ouverture de ligne à la demande *Voir* DDR
 - redistribution de routes, BGP 110, 111
 - réduction des mises à jour 286
 - réseaux commutés 393
 - sécurité 74
 - sélection de route 70
 - snapshot 286
 - sous-zone et Sysplex 245
 - sous-zone/APPN et Sysplex 246
 - synthèse de routes 68
 - EIGRP 76
 - OSPF 84, 87
 - technologie de LAN 7
 - trafic inter-zones 90
 - Voir aussi* Commutation
 - Voir aussi* Convergence
 - Voir aussi* Gestion du trafic

Router Discovery Protocol (RDP) 833
Routes statiques DDR 333
Routeurs 20
 APPN
 CIP et Sysplex 244
 configuration DLUS 249
 avantages 58
 CIP et Sysplex 248
 commutateurs de liaisons DLSw+ 258
 contrôle d'accès 729
 conversion de médias 287
 de VLAN 62
 découverte 49
 ARP 778
 IRDP 49
 RIP 778
 désignés (DR), PIM-SM 443
 DLSw+
 configuration 266
 échange d'informations de services 259
 protocoles de transport supportés 264
 fonctions RMON 458
 gestion des erreurs 511
 homologues BGP 104
 LANE ATM 161
 recommandations, administration 511
 RNIS, interface
 BRI 350
 PRI 355
 secours HSPR 777
 stub 101
 sur réseaux commutés 393
 virtuels 778
Routing Information Protocol (RIP) 50
RSRB (Remote Source Routing Bridge)
 cohabitation avec DLSw+ 265
 configuration avec CIP 295
 réduction de nœuds APPN 217

S

SAP (Service Advertisement Protocol) 835
 Novell IPX
 filtrage des mises à jour 837
 mises à jour incrémentielles 838

Scénarios de corrélation d'événements
 changements de topologie STP 528
 cohérence des ports 510
 défaillance de routeur/commutateur 532
 environnement 535
 erreurs mineures d'alimentation 509
 flux des ports 510
 interceptions d'alarmes 509
 lien actif/inactif 528
 modules
 de commutateurs 508
 superviseurs 509
 performances 533
 ports
 de cartes de superviseurs 509
 de VLAN 510
 redémarrage d'équipement 527
SDLC (Synchronous Data Link Control), configuration
 d'hôtes SNA 821
 de DLSw+ 268
Sécurité
 approche Cisco 726
 authentification
 de voisin OSPF 760
 en texte clair 761
 MD5 762
 contrôle et rétablissement après incident 719
 cryptage des données du réseau 758
 d'accès au média 48
 EIGRP 81
 évaluation
 de l'état de sécurité 717
 des besoins 723
 fonctions de protocoles 74
 guerre de l'information 720
 menaces 720
 motivations des cyber-pirates 721
 listes de contrôle d'accès 736
 modèle RNIS 349
 OSPF 92
 pare-feu 763
 réseaux IP *Voir Sécurité IP*
 RNIS pour DDR 343
 services Cisco 717

- stratégies 723
 - création 725
 - documentation et analyse 726
- vulnérabilités
 - attaques par déni de service 722
 - authentification CHAP de Cisco 722
- Voir aussi* Administration réseau
- Sécurité IP**
 - accès
 - aux routeurs 729
 - par console 730
 - cryptage des mots de passe 733
 - délais d'expiration de session 733
 - mode non privilégié 730
 - mode privilégié 730
 - SNMP 731
 - mode non privilégié 732
 - mode privilégié 732
 - Telnet 731
 - adresses IP 733
 - mode non privilégié 731
 - mode privilégié 731
 - ports TCP 734
 - TACACS 755
 - architecture pare-feu 763
 - application de listes d'accès 768
 - contrôle du flux de trafic 764
 - listes d'accès de pare-feu 765
 - routeur pare-feu 765
 - serveur de communication pare-feu 769
 - assignation de numéros de ports 771
 - contrôle d'accès aux serveurs 756
 - niveaux de privilège Cisco 757
 - notifications d'utilisation non autorisée 757
 - sécurisation des services non standard 757
 - suggestions de lecture 774
 - usurpation d'adresse (spoofing) 770
- Segmentation** 45, 388
 - d'un espace d'adresse IP 793
 - gestion du trafic 45
 - LAN 388
 - tolérance aux pannes 55
- Sélection de route** 70, 76, 90
- Serveur TN3270**
 - avec DLUR/DLUS 306
- support avec CSNA 303
 - définition de PU SNA 304
 - fonction DDDLU VTAM 304
 - support CIP 297
- Service Advertisement Protocol (SAP)** 835
- Service Profile Identifier (SPID)** 352
- Services**
 - d'accès local 44
 - de cache 46
 - de commutation de paquets
 - Frame Relay 186
 - PSDN 171
 - de distribution 37
 - de l'épine dorsale 25
 - de nom 46
 - de proxy 46
 - de sécurité Cisco 717
 - Frame Relay 178
- Sessions APPN**
 - établissement 207
 - routage intermédiaire 208
 - unités logiques dépendantes (DLU) 209
- SGBP (Stack Group Bidding Protocol)** 368
- Signalisation**
 - système SS7 358
 - voix en paquets 852
- Simple Server Replication Protocol (SSRP)** 165
- Small Office/Home Office (SOHO)** 347
- SMDS (Switched Multimegabit Data Service)** 9
- SNA (Systems Network Architecture)**
 - classe de service 200
 - combinaison avec un CIP 292
 - configuration
 - avec Cisco SNA 301
 - support de TN3270 303
 - d'hôtes 811, 821
 - DLSw+ 257
 - encapsulation avec DLSw+ (Data Link Switching Plus) 206
 - équilibrage de charge 263
 - établissement d'un circuit DLSw 259
 - interréseau multiprotocole et Sysplex 248
 - modes duplex et semi-duplex 808
 - routage DDR 285
 - sous-zone et ACF/VTAM 200
 - transport natif 205
 - VTAM et CMPC 307

- SNAP (Subnetwork Access Protocol)** 458
- Snapshot**
- activation du routage 330
 - configuration sur RNIS 694
 - modèle de conception 329
 - protocoles
 - à vecteur de distance 329
 - non supporté 330
 - réseau Novell IPX 698
 - routage 286
 - topologie Hub-and-Spoke 696
- SNMP (Simple Network Management Protocol)**
- administration réseau 459
 - bases MIB
 - base de données de transmission de pont 492
 - châssis et environnement 486
 - erreurs de pont 493
 - états de l'environnement 516
 - EtherChannel 506
 - groupes système et châssis 502
 - interceptions de routeurs 513
 - interfaces réseau 522
 - modules 503
 - de commutateur 489
 - objets
 - divers 507
 - MIB-II 500
 - performances d'ensemble 497
 - ports 504
 - de tronçons 497
 - ressources
 - de commutateur 482
 - processeur 518
 - RSM 506
 - statistiques mémoire 518
 - tampons 520
 - taux d'utilisation des ports 495
 - topologie Spanning-Tree 491
 - tronçons 505
 - VLAN 505
 - configuration IOS 480
 - filtrage pour DDR 336
 - gestion des performances 517
 - indexation par chaîne de communauté 478
 - interceptions
 - d'événements 460
 - pour RMON 476
- interrogations 472
 - de performances 475
 - de seuils 474
 - de surveillance 474
 - MIB RNIS 371
 - plate-forme NMS 472
 - routeurs 512
 - scénarios de corrélation d'événements 524
 - sécurité IP 731
- SOHO (Small Office/Home Office)** 345, 347
- Sous-zone SNA**
- ACF/VTAM 200
 - migration vers APPN 239
- Soutien d'adressage** 44
- SPAN (Switched Port Analyzer), analyseur de port** 457
- Spanning Tree** *Voir Arbre recouvrant*
- SPID (Service Profile Identifier)** 352
- Split Horizon, fonction de routage** 328
- SRB (Source Routing Bridge), configuration d'hôtes SNA** 811
- SS7 (Signaling System 7)** 358
- SSCP (System Services Control Point), redondance APPN** 223
- SSP (Switch-to-Switch Protocol)** 258
- SSRP (Simple Server Replication Protocol)**
- emploi et configuration 168
 - partitions de réseau 169
 - services LANE redondants 165
- Stack Group Bidding Protocol** *Voir SGBP*
- Standard DLSw** 258
- Store-and-forward (commutation en mode différé)** 21
- Stratégies de sécurité** 723
- Structure**
- d'adresse ATM 146
 - de réseau ATM 152
- Stub**
- routeur 101
 - zones 89
- Switched Multimegabit Data Service (SMDS)** 9
- Switch-to-Switch Protocol (SSP)** 258
- Synthèse de routes**
- EIGRP 76
 - OSPF 85

-
- Syslog**
 administration réseau 460
 contraintes de mémoire 478
 filtrage des messages 526
 journalisation 460
 messages
 de routeurs 512
 liés à l'environnement 516
 mise en place de la journalisation 466
- Sysplex (System Complex)**
 APPN et routeurs CIP 244
 CMOS 9672 245
 routage
 APPN 247
 de sous-zone 245
 de sous-zone/APPN 246
 SNA et interréseau multiprocole 248
- System Services Control Point (SSCP) 223**
- Systèmes**
 autonomes, OSPF 81
 d'alimentation redondants 53
 de Signalisation 7 (SS7) 358
- T**
- Tables**
 CEF, commutation CEF 554
 de commutation 21
 de hachage, commutation rapide 545
 de routage 21
 de voisinage, commutation CEF 554
- TACACS (Terminal Access Controller Access Control System) 48, 755**
 accès
 non privilégié 755
 privilégié 755
 cartes d'accès à jeton 756
- TCP/IP (Transmission Control Protocol/Internet Protocol), encapsulation 278**
- TDM (Time Division Multiplexing), file d'attente équitable pondérée 29**
- TDU (Topology Database Update) Voir Nœuds APPN**
- Technologies**
 LAN 6
 WAN 8
- Telnet**
 administration 459
 ports
 TCP 734, 736
 VTY 731
 sécurité d'accès 731
- Temporiseurs, linger 277**
- Temps de latence 225**
- Terminaison numérique de réseau, RNIS 350**
- Terminal Access Controller Access Control System** *Voir TACACS*
- Test de sensibilité du réseau 17**
- Token Ring**
 commutation LAN 7
 configuration de DLSw+ 267
- Tolérance aux pannes**
 DLSw+ 263
 fonctions intraprotocoles 56
 HSPR 777
 matériel de secours et chemins alternatifs 56
 problèmes de média 55
 réseaux LANE
 protocole par arbre recouvrant 165
 routeurs redondants (protocole HSRP) 165
 services redondants (protocole SSRP) 165
 segmentation 55
- Topologies**
 DDR 317
 EIGRP 75
 en étoile
 Frame Relay 182
 PSDN 174
 maillées
 hiérarchiques, Frame Relay 179
 hybrides, Frame Relay 181
 OSPF 82
 partiellement maillées
 Frame Relay 182
 interfaces virtuelles 183
 PSDN 175
 redondance 53
 réduction des mises à jour APPN 211
 routage 68
 totalement maillées
 Frame Relay 182
 PSDN 175
 redondance 53

ToS (Type of Service) 27
Traduction de format de trame 42
Trafic *Voir Gestion du trafic*
Trames
CANUREACH 259
d'exploration 259
délimitation de trames, PPP 360
erreurs
 CRC 499
 d'alignement 498
ICANREACH 259
runts 499
traduction de format 42
Tunnel *Voir Encapsulation*
Type de service IP (ToS) 27

U

UIT-T (Union Internationale des Télécommunications, secteur normalisation) 633
UNI (User-Network Interface) 152
 ATM 597
Unicast, trafic ATM 160
Unités logiques IBM
 avec CIP 297
 dépendantes 209
 configuration
 de DLUR 249
 de DLUS 249
 interréseau multiprotocole et SNA 248
 gestion de priorité 27
 serveur TN3270 306

V

Variable Length Subnet Mask *Voir VLSM*
VCC (Virtual Channel Connection), ATM 592
Virtual LAN *Voir VLAN*
Virtual Routing Node (VRN) 213
Vitesse d'accès au média 225
VLAN (Virtual LAN)
 commutateurs et routeurs 62
 composition 394
 réseau et services 455
VLSM (Variable Length Subnet Mask), adresse
 EIGRP 75
 OSPF 86

VoFR *Voir Voix sur Frame Relay*
Voix en paquets 841-842
 codage de la voix 843
 contextes d'utilisation 856
 délai 846
 options de transport 848
 réseaux
 de données privés 851
 de paquets X.25 850
 de trames/cellules 849
 en mode non connectés 850
 synchrônes commutés 849
 qualité de compression 846
 signalisation
 établissement de la connexion 852
 externe 853
 interne 854
 standards de codage 844
Voix sur Frame Relay 190
 algorithmes de compression de la voix 192
 caractéristiques des communications humaines 191
 délai et gigue 194
 écho et annulation d'écho 193
 fragmentation de trame 196
 interpolation de la parole numérique (DSI) 196
 optimisation de la bande passante 197
 pertes de trames 195
 priorité de trafic 196
 support pour fax et données 195
VPI (Virtual Path Identifier), ATM 589
VRN (Virtual Routing Node), réseau de connexion APPN 213
VTAM (Virtual Telecommunication Access Method)
 adaptateur XCA pour CIP 302
 CMPC
 groupe de transmission CMPC 309
 nœud principal
 SNA local 308
 VTAM TRL 307
 sous-canaux CMPC 308
 configuration avec CIP 297
 exemple 309
 configuration avec CIP CMPC 307
 fonction DDDLU pour serveur TN3270 304

nœuds interzones 254
SNA, interréseau multiprotocole et Sysplex 248

W

WAN (Wide Area Network)

accès commuté 31
ADSL 9
ATM 9
bande passante 73
conception et tendances 8
connexions
 à des services PSDN 171
 distantes 9
Frame Relay 9
intégration avec les réseaux locaux 10
liaisons
 avec commutateurs 7
 louées 9
 redondantes 51
 secondaires, APPN 220
médias 10

modems analogiques 9
RNIS 9
SMDS 9
technologies 8
topologies 174
X.25 9

Wide Area Network *Voir WAN*

X

X.25

LCN 178
QLLC 270
technologie WAN 9

Z

Zones AppleTalk statiques 334

Zones OSPF 84
NSSA (Not-So-Stubby-Area) 92
annonces LSA Type 7 94
configuration 94

