

Chapitre 0 : Généralités sur le protocole TCP/IP

Chapitre 1 : Structure des PDU

Chapitre 2 : Routeur et configuration de base

Chapitre 3 : Généralités sur le routage

Chapitre 4 : Routage Statique

Chapitre 5 : Routage à vecteurs de distance

Chapitre 6 : VLSM et CIDR

Chapitre 7 : protocole RIP

Chapitre 8 : Routage à état de liens

Chapitre 9 : Protocole IGRP et EIGRP

Chapitre 10 : Protocole OSPF

Chapitre 11 : Routage externe : BGP

Chapitre 12 : IP V6

Chapitre 13 : translation d'adresse

Chapitre 0 : GENERALITES SUR LE PROTOCOLE TCP/IP

Le plus grand réseau qui est internet est basé sur le protocole TCP/IP. Il est pratiquement impossible de trouver aujourd’hui un ordinateur qui ne prenne pas en charge la suite de protocoles TCP/IP. Tout système d’exploitation Microsoft, Linux et UNIX la supporte. Les assistants personnels, les téléphones portables et même les systèmes d’exploitations des mainframes la gèrent. Nous allons au cours de ce chapitre rappeler quelques notions sur ce protocole, tout en rappelant le modèle OSI qui sert de base à tous les protocoles réseaux actuellement utilisés.

1. Le modèle OSI

La décomposition en couches des différentes fonctions ou tâches intervenant dans la communication en réseau permet de diviser un ensemble complexe de concepts et de protocoles en plusieurs parties facile à décrire, à implémenter et à dépanner. Cette décomposition et la définition d’interfaces standard entre ces couches présentent de nombreux avantages :

- Réduction de la complexité
- Standardisation des interfaces
- Facilité d’apprentissage
- Facilité de développement
- Interopérabilité entre fabricants
- Ingénierie modulaire

Le modèle OSI constitue un modèle de référence pour les communications en réseau. Elle n'a jamais eu de succès sur le marché à cause de son nombre de couche élevé. Elle est constitué de sept couches :

- Application (couche 7) : cette couche définit l'interface entre le logiciel de communication et n'importe quelle application ayant besoin de communiquer au-delà de l'ordinateur sur lequel elle réside. Elle définit également le processus pour l'authentification des utilisateurs.
- Présentation (couche 6) : Le rôle principal de cette couche est de définir des formats de données, tels que texte ASCII, texte EBCDIC, binaire, BCD ou JPEG. Le chiffrement est également défini comme un service de la couche présentation.
- Session (couche 5) : Cette couche précise comment initier, contrôler et terminer des conversations appelées session.
- Transport (couche 4) : Cette couche gère les aspects liés à la livraison de données à un autre ordinateur, tels que la correction d'erreur et le contrôle de flux. La donnée unitaire ou PDU(Packet Data Unit) de cette couche est appelé segment.
- Réseau (couche 3) : cette couche possède trois grandes fonctionnalités : adressage logique, routage et détermination des routes. La PDU de cette couche est appelée paquet.
- Liaisons de données (couche 2) : Cette couche définit les règles qui déterminent quand un équipement peut envoyer des données sur un support de transmission spécifique. La PDU de cette couche est appelée trame.
- Physique (couche 1) : Cette couche traite des caractéristiques physiques du support de transmission, telles que les connecteurs, les broches, les tensions électriques, le codage, la modulation , l'activation et la désactivation du support physique. La PDU de cette couche est le bit.

2. L'architecture des protocoles TCP-IP

L'architecture des protocoles TCP-IP est constituée de quatre couches :

- La couche application (couche 4) : cette couche englobe les trois dernières couches du modèle OSI, à savoir : application, présentation et session. On y trouve des protocoles tels que http, POP3, STMP, TELNET, SSH etc.
- La couche transport (couche 3) : cette couche est équivalente à la couche 4 du modèle OSI. On y trouve principalement deux protocoles : TCP et UDP, mais aussi le protocole ICMP pour le test de la connexion entre deux hôtes.
- La couche internet (couche2) : elle est équivalente à la couche 3(réseau) du modèle OSI. On y trouve des protocoles tels que IP, IPX, les protocoles de routages tels que RIP, OSPF etc.
- La couche accès réseau (couche 1) : cette couche englobe la couche 1 et la couche 2 du modèle OSI. On trouve des protocole comme Ethernet, Frame Relay, PPP etc.

3. Etude d'un protocole du LAN : Ethernet

Le protocole Ethernet est le plus utilisé actuellement dans les réseaux Locaux. L'IEEE sépare la fonction de la couche liaison de données en deux sous-couche :

- La sous-couche MAC (Media Access Control) :
 - ✓ Il délimite la trame
 - ✓ L'adressage
 - ✓ Détection d'erreurs
 - ✓ Contrôle d'entrée et de sortie de la trame sur le support
- La sous-couche LLC (Logical Link Control) :
 - ✓ Il réalise la connexion avec les couches supérieures
 - ✓ Il encapsule le paquet en provenance de la couche réseau
 - ✓ Identifie le protocole de la couche réseau
 - ✓ Indépendant de la couche physique

Nous allons étudier dans cette partie l'algorithme CSMA/CD(Carrier Sense Multiple Access/Collision Detection), les différentes normes d'Ethernet, les paires torsadées, l'adressage MAC et les équipements utilisés dans le protocole Ethernet principalement le hub, le pont et le switch.

3.1 Les normes du protocole Ethernet

Pour communiquer sur le LAN, les équipements Ethernet utilisent l'algorithme CSMA/CD. Le CSMA/CD est un protocole qui gère le partage de l'accès physique au réseau Ethernet, selon la norme IEEE 802.3. :

- Un équipement ayant une trame à envoyer écoute jusqu'à ce que le réseau soit libre.
- Une fois le réseau libre, le ou les expéditeurs commencent à envoyer la trame.
- Le ou les expéditeurs écoutent pour s'assurer qu'aucune collision n'a eu lieu
- En cas de collision, les équipements qui ont envoyé une trame envoient un signal de brouillage pour s'assurer que toutes les stations ont reconnu la collision.
- Une fois le brouillage terminé, chaque émetteur déclenche un temporisateur et attend pour renvoyer la trame.
- A l'expirateur du temporisateur, le processus redémarre.

CSMA/CD n'empêche pas les collisions : il garantit le bon fonctionnement du réseau même en cas de collision mais il a des conséquences sur la performance du réseau.

Tout d'abord le CSMA/CD contraint les équipements à attendre que le réseau soit silencieux avant d'envoyer les données, en conséquence tous ceux qui sont liés au même concentrateur partagent la même bande passante. La logique qui consiste à attendre que le réseau soit silencieux avant d'émettre s'appelle le **half-duplex**.

Quelques normes d'Ethernet :

Nom courant	débit	Autre nom	Nom de la norme IEEE	Type de câble, longueur maximale
Ethernet	10Mbit/s	10BASE2		Câble coaxial, 185m
Ethernet	10Mbit/s	10BASE5		Câble coaxial, 500m
Ethernet	10Mbit/s	10BASE-T	IEEE 802.3	Paire torsadée, 100m

Fast Ethernet	100Mbit/s	100BASE-TX	IEEE 802.3u	Paire torsadée, 100m
Gigabit Ethernet	1000Mbit/s	1000BASE-LX 1000BASE-SX	IEEE 802.3z	Fibre optique, 550m(SX), 5Km(LX)
Gigabit Ethernet	1000Mbit/s	1000BASE-T	IEEE 802.3ab	Cuivre, 100m

Tableau 1 : Types d'Ethernet

Pour construire un LAN moderne avec l'un des types d'éthernet basés sur les UTP listées, voici les composants dont on a besoin :

- Des ordinateurs dotés d'une carte réseau Ethernet ou carte NIC (Network Interface Card)
- Un concentrateur ou un commutateur Ethernet
- Des câbles UTP pour relier les ordinateurs au concentrateur ou au commutateur.

3.2 Paires torsadées et prise RJ45

Plusieurs types de câbles utilisés dans le réseau de nos jours : les paires torsadées, les câbles séries, le câble coaxial, la fibre optique etc. Dans le cadre de ce cours on va étudier les paires torsadées car ils sont les plus utilisés dans le réseau LAN de nos jours.

Une **paire torsadée** est une ligne de transmission formée de deux fils conducteurs enroulés en hélice l'un autour de l'autre. Cette configuration a pour but de maintenir précisément la distance entre les fils et de diminuer la diaphonie.

Les paires torsadées sont souvent blindées afin de limiter les interférences. Comme le blindage est fait de métal, celui-ci constitue également un référentiel de masse. Le blindage peut être appliqué individuellement aux paires ou à l'ensemble formé par celles-ci. Lorsque le blindage est appliqué à l'ensemble des paires, on parle d'écrantage.

Il existe plusieurs types de paires torsadées :

Paire torsadée non blindée

Unshielded twisted pair (UTP) - dénomination officielle U/UTP. La paire torsadée non blindée n'est entourée d'aucun blindage protecteur.

Paire torsadée écrantée

Foiled twisted pair (FTP) - dénomination officielle F/UTP. L'ensemble des paires torsadées a un blindage global assuré par une feuille d'aluminium. L'écran est disposé entre la gaine extérieure et les 4 paires torsadées. Les paires torsadées ne sont pas individuellement blindées.

Paire torsadée blindée

Shielded twisted pair (STP) - dénomination officielle U/FTP. Chaque paire torsadée blindée est entourée d'un écran en aluminium de façon similaire à un câble coaxial.

Paire torsadée doublement écrantée

Foiled foiled twisted pair (FFTP) - dénomination officielle F/FTP. Chaque paire torsadée est entourée d'une couche conductrice de blindage en aluminium. L'ensemble des paires torsadées a un écran collectif en aluminium.

Paire torsadée écrantée et blindée

Shielded foiled twisted pair (SFTP) - dénomination officielle SF/UTP. Câble doté d'un double écran (feuille métallisée et tresse) commun à l'ensemble des paires. Les paires torsadées ne sont pas individuellement blindées contrairement à ce que le terme Shielded foiled twisted pair pourrait faire croire.

Paire torsadée doublement blindée

Shielded shielded twisted pair (SSTP) - dénomination officielle S/FTP. Chacune des paires est blindée par un écran en aluminium, et en plus la gaine extérieure est blindée par une tresse en cuivre étamé. Le terme SSTP ne signifie pas Shielded shielded twisted pair puisque les paires ne sont pas individuellement blindée par une tresse.

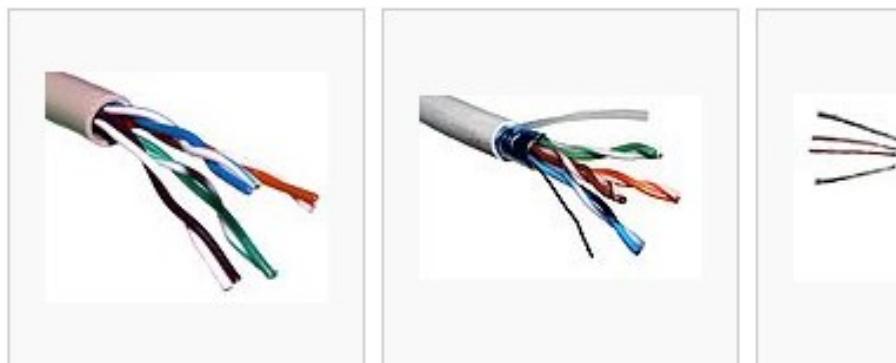


Figure 1 : Type de paires torsadées

Le RJ est une abréviation en anglais de **Registered Jack** qui veut dire en bon français **prise jack enregistrée**. Les prises RJ45 se trouvent aux extrémités d'un câble Ethernet. Pour être plus précis, il existe la prise RJ45 mâle qui se trouve aux extrémités d'un câble Ethernet et la prise RJ45 femelle que l'on trouve sur les hôtes ou sur le mur de votre salon.

Il existe des câbles droits et les câbles croisés. On sertir les câbles à l'aide d'une pince à sertir.

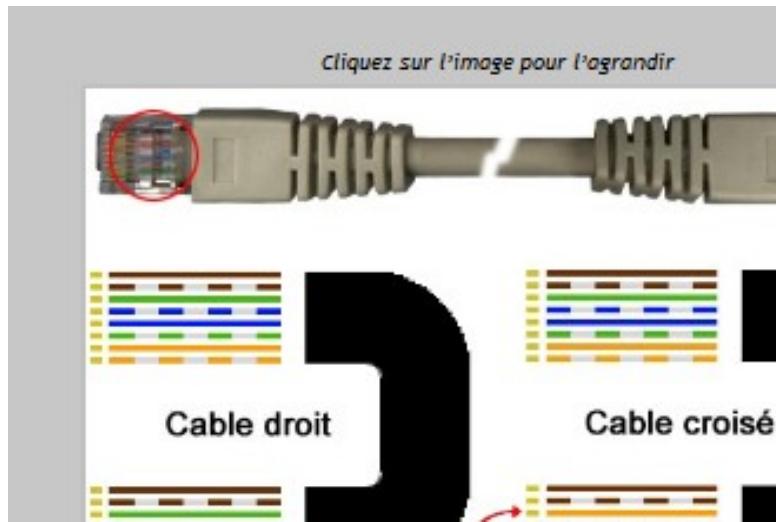


Figure 2 : différence entre câble droit et câble croisé

On utilise le câble droit entre le switch et le routeur, le switch et le PC, le switch et le HUB.

On utilise le câble croisé entre deux switch, entre deux PC, entre deux routeurs sur leur interface Ethernet, entre deux hub, entre un routeur et un PC, un routeur et un hub, et un PC et le HUB.

3.3 Equipements du protocole Ethernet

a) Etude d'un concentrateur : HUB

A ce niveau on trouve les répéteurs et le HUB. Le rôle du répéteur est de régénérer le signal après une certaine distance. Le HUB est un concentrateur qui permet de faire communiquer plusieurs terminaux. Il est constitué de plusieurs ports. Lorsque le hub reçoit un signal d'un port, il le transfert à tous les ports sauf le port par lequel il a reçu le signal. Donc tous les terminaux reçoivent le signal transmis sauf le terminal qui l'a transmis. Ceci augmente la probabilité de collision des paquets dans le HUB, ceci fait du HUB un domaine de collision.

b) Etude d'un Commutateur : le switch

Les équipements de niveau 2 de la couche OSI où le protocole Ethernet est implémenté sont : les ponts et le switch. Ces équipements séparent les domaines de collisions. Le switch est plus intelligent que le HUB. Il envoie le paquet reçu seulement au port de destination et non à tous les ports comme le HUB. Pour cela il utilise des adresses appelées adresse MAC pour définir à quel port envoyer le paquet.

- Adressage Ethernet :

L'adresse MAC identifie des équipements individuels ou des groupes d'équipements. Chaque adresse MAC est constitué de 6 octets en hexadécimal. Dans les équipements cisco un point sépare chaque groupe de quatre chiffres hexadécimaux. Exemple : 0000.0C12.3456 est une adresse valide. Pour garantir l'unicité de chaque adresse MAC par carte réseau, la première moitié de l'adresse désigne le fabricant de la carte. Ce code attribué par l'IEEE est appelé **OUI** (Organizationally Unique Identifier). On distingue :

- Les adresses de diffusion : FFFF.FFFF .FFFF
- Les adresses de multidiffusion : 0100.5Exx.xxxx (où les x peuvent être remplacés par n'importe quelle valeur).
- Les adresses de monodiffusion

- Full-Duplex :

Comme les commutateurs peuvent mettre les trames en mémoires tampon, ils éliminent complètement les collisions sur les ports reliés à un seul équipement, en conséquence les commutateurs LAN ayant un seul équipement relié à chaque port autorise la transmission en full-duplex c'est-à-dire une carte Ethernet peut envoyer et recevoir simultanément les données. Ceci désactive évidemment le CSMA/CD.

- Construction de la table de correspondance adresse MAC et port par le switch :

Lorsque le switch reçoit une trame, il regarde d'abord l'adresses MAC source dans sa table ; si cette adresse n'existe pas, il l'inscrit dans sa table avec le numéro du port par lequel il a reçu la trame. Ensuite il regarde l'adresse MAC de destination dans sa table.

S'il trouve cette adresse il envoie la trame au port correspondant sinon il diffuse la trame à tous les ports.

Pour acheminer une trame le switch a deux méthodes :

- Store-and-Forward : il attend recevoir toute la trame avant d'envoyer.
- Cut-throw : Dès qu'il reçoit une partie de la trame, il envoie. Le cut-throw a deux variantes :
 - ❖ Commutation Fast-Forward : ce mode de commutation offre le niveau de latence le plus faible. La commutation Fast-Forward transmet un paquet immédiatement après la lecture de l'adresse de destination.
 - ❖ Commutation Fragment-Free : en mode de commutation Fragment-Free, le commutateur stocke les 64 premiers octets de la trame avant la transmission.

- **Délimitation de la trame :**

Préambule	SFD	Destination	Source	Longueur/Type	Données	FCS
-----------	-----	-------------	--------	---------------	---------	-----

Tableau 2 : trame Ethernet IEEE 802.3 (revu en 1997)

Champ	Longueur en octet	Description
Préambule	7	Synchronisation
SFD(Start Frame Delimiter)	1	Signifie que le prochain octet entame le champ de l'adresse de destination
Adresse MAC de destination	6	
Adresse MAC source	6	
Longueur	2	Définit la longueur du champ de données
Type	2	Définit le type de protocole listé dans la trame
Données	46-1500	

FCS(Frame Check Sequence)	4	Permet à la carte réseau du destinataire de savoir si des erreurs sont survenus lors de la transmission
---------------------------	---	---

Tableau 3 : description de la trame Ethernet

- **Détection d'erreurs :**

Pour détecter les erreurs, l'équipement émetteur calcule une fonction mathématiques complexe sur la trame et place le résultat dans l'en-queue dans le champ FCS. L'équipement receiteur effectue la même opération mathématique sur la trame. Si le résultat correspond à la valeur du champ FCS, aucune erreur n'a lieu, sinon une erreur s'est produite et la trame est supprimée.

4. L'adressage IP

Dans la couche réseau, on retrouve les protocoles tels que :

- IP : open
- IPX propriétaires aux équipements NOVEL
- Apple Talk (Protocole propriétaire à apple)

Dans ce cours nous allons étudier le protocole IP version 4 sachant qu'il existe IP version 6.

Dans le protocole IP, la couche réseau utilise l'adresse IP pour la communication entre les machines d'un même réseau ou des réseaux différents. Dans cette partie nous allons étudier les adresses IP, les sous-réseau, et les fonctionnement de cette couche.

4.1 L'adresse IP

Une adresse IP dans IP-V4 est constitué de 32 bits regroupé en 4 octets en décimal séparé par des points. Exemple : 10.23.201.12 est une adresse IP valide. Cette adresse comprend deux parties : la partie réseau et la partie hôte. Le masque de sous-réseau permet d'identifier ces 2 parties. Le masque de sous-réseau est aussi constitué de 32 bits regroupés en 4 octets exprimés en décimal. Tous les bits de la partie réseau sont à 1 et le reste à 0. Exemple : 255.0.0.0 signifie que la partie réseau est les 8 premier bits c'est-à-dire le premier octet.

a) Les classes d'adresse

La RFC 791 spécifie le protocole IP et plusieurs classes de réseaux différentes. IP définit trois classes de réseaux, A, B, C d'où sont tirés les adresses destinées aux hôtes. TCP/IP définit également des adresses de classe D pour la multidiffusion et des adresses de classe E pour l'expérimentation.

- **Classe A :**

Dans cette classe la partie réseau est constitué du premier octet et la partie hôte sur le reste. Le premier bit est à 0. Le premier octet prend les valeurs de 1 à 126. Le masque réseau est 255.0.0.0 et le nombre d'hôtes par réseau est : $2^{24}-2$.

- **Classe B :**

La partie réseau est constitué des deux premiers octets. Le premier bit est à 1 et le deuxième bit à 0. Le premier octet prend les valeurs de 128 à 191. Le masque réseau est 255.255.0.0 et le nombre d'hôtes par réseau : $2^{16}-2$.

- **Classe C :**

La partie réseau est constitué des trois premiers octets. Les deux premiers bits sont à 1 et le deuxième bit à 0. Le premier octet prend les valeurs de 192 à 223. Le masque réseau est 255.255.255.0 et le nombre d'hôtes par réseau : 2^8-2 .

- **Classe D :**

Les adresses de cette classe sont utilisées pour la multidiffusion. Le premier octet est 224.

- **Classe E :**

Les adresses destinées aux expériences. Le premier octet prend les valeurs à partir de 225.

- **Les adresses réservés :**

0.0.0.0 définit n'importe quel hôte.

127.0.0.0 est l'adresse de bouclage

b) L'adressage public et privé

ICANN (Internet Cooperation for Assigned Numbers and Names) ancien IANA (Internet Assign numbers Authority) sont les régulateurs des normes sur Internet. L'IETF(Internet Engineering Task Force) est une communauté de travail qui travaille sous la tutelle de l'ICANN gère l'affectation des adresses IP et des numéros des ports.) La RFC(Request For common qui est la publication finale d'un résultat) 1918 définit un ensemble d'adresse IP Privées destinées aux interréseaux qui ne seront pas connectés sur internet.

Réseaux IP privés	Classe	Nombre de réseau
10.0.0.0 à 10.0.0.0	A	1
172.16.0.0 à 172.31.0.0	B	16
192.168.0.0 à 192.168.255.0	C	256

Tableau 4 : Adresses IP privés par classe

c) Sous-réseau

Comparée aux conventions des classes A, B, C la création de sous-réseaux génère un plus grand nombre de groupe d'adresse IP. Un réseau de classe A, B ou C peut être subdivisé en groupes plus petits. Chaque sous-réseau peut se comporter comme s'il était lui-même un réseau. Le problème posé ici est que pour un nombre de sous-réseau donné combien de bits faut-il emprunté à la partie hôte pour constituer le sous réseau ?

8	x	24-x	
réseau	Sous-réseau	hôtes	Classe A

16	x	16-x	
réseau	Sous-réseau	hôtes	Classe B

réseau	Sous-réseau	hôtes	Classe C
--------	-------------	-------	----------

Tableau 5 : Sous-réseau par classe

Exemple : nous voulons diviser une adresse réseau de classe C en 6 sous-réseau ; quel est le nombre de bits à emprunter à la partie hôte pour constituer les adresses de sous-réseau.

Définir le nombre d'adresses hôte par sous-réseau et : le masque de sous-réseau.

Si x est le nombre de bits à emprunter et y le nombre d'hôtes par sous-réseau

$$2^x = 6 \Rightarrow x = 3. \quad y = 2^{8-x} - 2 \quad y = 30 \text{ le masque de sous-réseau est } 255.255.255.11100000 \\ \text{c'est-à-dire } 255.255.255.224$$

4.2 fonctionnalités de la couche réseau

La couche réseau encapsule les données dans un paquet. Le paquet contient une en-tête. Les seuls éléments de l'en-tête vu dans le CCNA sont les adresses IP source et destination et le champ TTL(Time to Live) pour éviter les boucles dans le réseau.

a) Affectation des adresses IP et DHCP (Dynamic Host Configuration Protocol)

Pour pouvoir communiquer les équipements IP ont besoin des adresses IP. On peut faire des affectations manuelles ou statiques. Mais dans un parc de plusieurs machines, il serait difficile de faire des configurations manuelles d'où la mise sur pied d'un serveur DHCP pour une affectation automatique ou dynamique des adresses IP. Seulement, même avec la présence d'un serveur DHCP, certains PC, surtout les serveurs requièrent une configuration statique des adresses IP. Lors de la configuration du serveur DHCP, ces adresses ne doivent pas faire partie de la plage d'adresse pour l'affectation dynamique.

b) Le protocole ARP et RARP

Un ordinateur pour communiquer dans le réseau doit avoir une adresse IP. Deux façons de configurer une adresse IP : manuel ou automatique via un serveur DHCP. Lorsqu'il y'a un serveur DHCP sur le réseau l'ordinateur qui ne connaît pas son adresse IP utilise l'adresse 0.0.0.0 et lance une requête RARP(Reverse Adresse Resolution Protocole) afin de demander son adresse IP à partir de son adresse MAC. Pour cela il utilise l'adresse MAC de diffusion. Le serveur DHCP seul va répondre à cette requête, en lui fournissant son adresse IP son

masque ainsi que la passerelle par défaut. Lorsqu'un ordinateur veut communiquer avec un PC sur le même sous-réseau dont il connaît l'adresse IP il utilise le protocole ARP pour demander l'adresse MAC de ce dernier. Pour cela il utilise l'adresse MAC de diffusion. Seul le PC correspondant va répondre en envoyant son adresse MAC. Ce qui va permettre à l'ordinateur qui veut communiquer de remplir le champ adresse MAC destination de la trame. Les requêtes ARP sont peu fréquentes en effet tout équipement IP doit conserver les adresses apprises avec ARP dans son cache ARP. Commande pour afficher la cache ARP sur un PC ou un routeur : arp -a. Si un PC veut communiquer avec un autre PC se trouvant sur un autre sous-réseau, il va utiliser l'adresse MAC de destination de la passerelle mais l'adresse IP de destination du PC se trouvant sur un autre réseau. L'adresse MAC destination va changer de proche en proche jusqu'à ce que le paquet arrive au PC de destination mais l'adresse IP destination reste fixe.

c) Serveur DNS(Domain Name Resolution)

Pour pouvoir communiquer avec d'autres PC, les utilisateurs doivent connaître les adresses IP des PC qu'ils veulent contacter. Retenir les adresses IP c'est très difficile. Il est mis sur pied un mécanisme qui permet de convertir ces adresses IP en des noms. C'est ce que réalise les serveurs DNS. Par exemple pour se connecter à Yahoo, les internautes utilisent le nom www.yahoo.fr. Avant d'envoyer la requête au serveur de Yahoo, le PC envoie d'abord une requête DNS pour avoir l'adresse IP de Yahoo.

d) Test de la connectivité IP

Une fois un réseau implémenté, il faut un moyen de tester la connectivité IP sans dépendre d'une application. Le premier outil est une commande nommée **PING** (Packet Internet Groper) qui envoie un message de requête d'écho ICMP (Internet Control Message Protocol) vers une adresse IP. L'ordinateur ayant cet adresse IP doit répondre avec une réponse d'écho ICMP. Si le test réussi la connectivité IP fonctionne. Une autre commande pour le test de la connectivité IP est **TRACEROUTE**(**TRACERT** sur la plateforme WINDOWS). La réponse de cette commande montre les différents sauts parcourus par les paquets pour arriver à destination, ce qui permet en cas de problème de localiser où il se trouve.

5. TCP/IP : transport, applications

La couche transport du modèle OSI définit plusieurs fonctions dont les plus importantes sont la correction d'erreur et le contrôle de flux.

Fonction	description
Multiplexage par numéros de ports.	Fonction qui permet aux hôtes destinataires de choisir l'application appropriée aux données reçues en

	fonction du numéro de port.
Correction d'erreur (fiabilité)	Processus consistant à numérotter et à acquitter des données avec les champs Numéro de séquence et Numéro d'acquittement de l'en-tête.
Contrôle de flux par fenêtrage	Processus qui utilise une taille de fenêtre pour protéger l'espace du tampon et les équipements de routage.
Etablissement et libération des connexions	Processus utilisé pour initialiser des numéros de ports et les champs Numéro de séquence et numéro d'acquittement.
Transfert séquentiel de données et segmentation	Un flux continu d'octets provenant d'un processus d'une couche supérieure est segmenté en vue de la transmission et livré au processus de la couche supérieure de l'équipement receiteur, sans que l'ordre des octets ait été modifié.

Tableau 6 : Fonctions de la couche transport de TCP/IP

Port source (16)		Port destination (16)			
Numéro de séquence (32)					
Numéro d'acquittement (32)					
Longeur d'en-tête(4)	Reservé (6)	Bits de code (6)	Fenêtre (16)		
Somme de contrôle (16)		Urgent (16)			
Options (de 0 à 32)					
Données (longueur variable)					

Tableau 7 : champ de l'en-tête TC

5.1 le protocole TCP et le protocole UDP

Le protocole TCP est orienté connexion. La fiabilité est l'une de ses principales caractéristiques par rapport au protocole UDP(User Datagram Protocol). TCP garantit un

transfert fiable des données. Concernant la fiabilité, il numérote les octets de données au moyen des champs séquence et acquittement contenu dans l'en-tête TCP

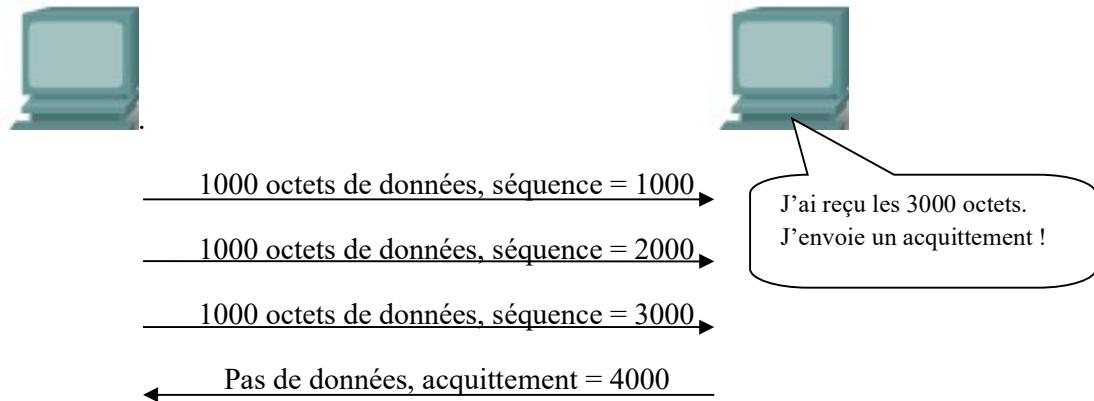


Figure 3 : Acquittement TCP sans erreur

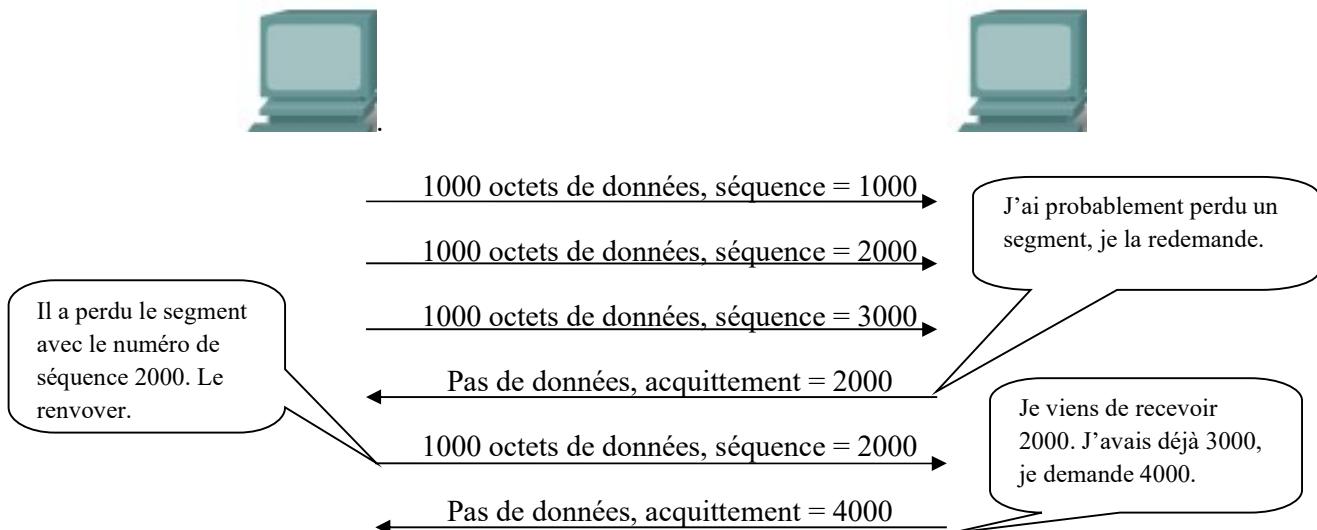
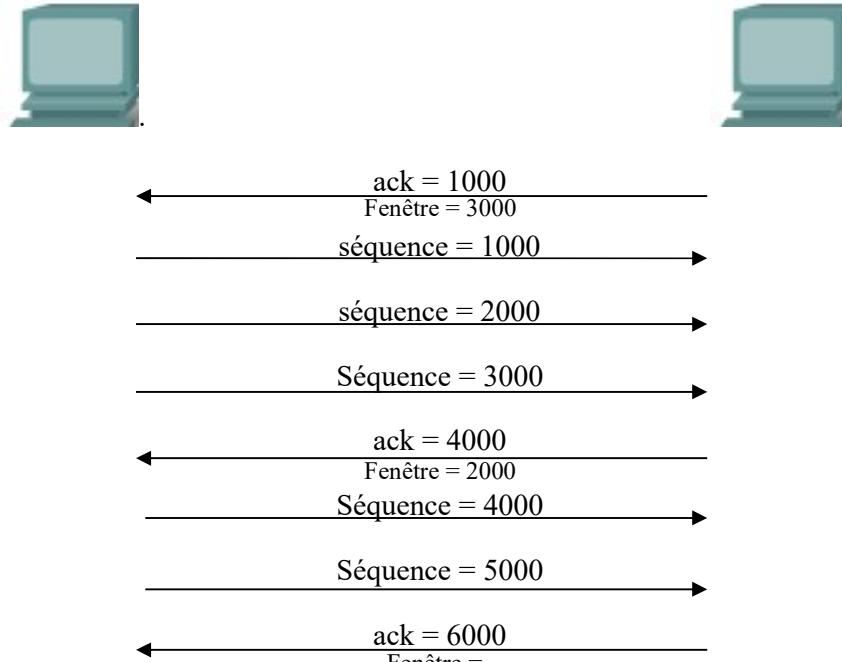


Figure 4 : Acquittement TCP avec erreur

TCP implémente le contrôle de flux en tirant parti des champs numéro de séquence et numéro d'acquittement de l'en-tête TCP, ainsi que d'un champ fenêtre. Ce dernier indique le nombre maximal d'octets non acquittés autorisés à tout moment.



PAR(Positive Acknowledge and Retransmission) décrit les processus de correction d'erreur et de fenêtrage TCP.

L'établissement d'une connexion TCP a lieu avant toutes les autres fonctions TCP. Il s'agit d'un processus qui consiste à initialiser les champs de séquence et d'acquittement et à déterminer les numéros de port à utiliser.

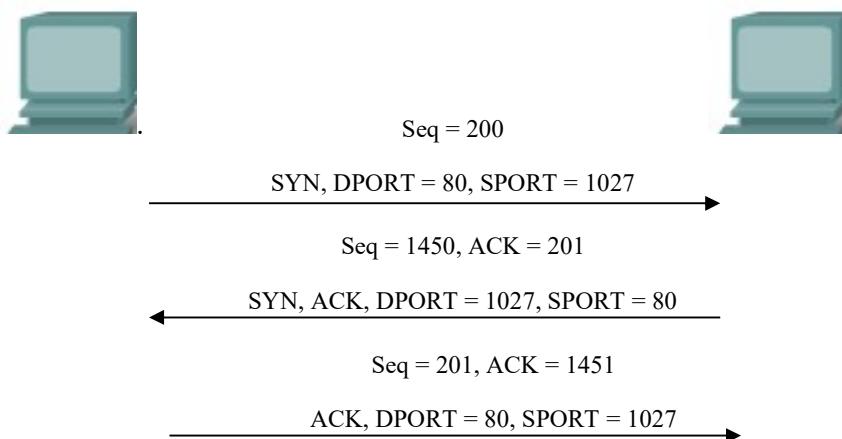


Figure 6 : établissement d'une connexion TCP

Le récepteur TCP doit procéder à un transfert séquentiel des données en réassemblant les données dans leur ordre d'origine.

UDP fournit aux applications un service leur permettant d'échanger des messages.

Contrairement à TCP, UDP opère en mode non connecté, et n'assure ni correction d'erreur, ni fenêtrage ou réordonnancement des données reçues, ni segmentation des données. La VoIP et le DNS utilisent UDP. Par rapport à TCP, UDP présente l'avantage de ne pas utiliser de champs de séquence et d'acquittement. Ses services requièrent donc moins d'octets de surcharge et il n'a pas non plus besoin d'attendre d'acquittement ou de maintenir des données en tampon dans l'attente d'un acquittement.

5.2 la couche application

Pour connaître à quelle application remettre les données reçues au niveau de la couche transport, TCP et UDP utilisent le numéro de port qui se trouve dans leur en-tête. Le numéro de port identifie donc l'application utilisée. Le multiplexage s'appuie sur le concept de socket. Un socket est composé de :

- Une adresse IP
- Un protocole de transport
- Un numéro de port

Il existe différents types de numéros de ports :

Ports réservés (numéros 0 à 1023). Ces numéros sont réservés à des services et applications. Ils sont généralement réservés à des applications de type HTTP (serveur Web), POP3/SMTP (serveur de messagerie) et Telnet. En définissant ces ports réservés pour une utilisation par des applications serveur, il est possible de programmer les applications clientes de façon à ce qu'elles demandent à être connectées à ce port précis et au service qui lui est associé.

Ports inscrits (numéros 1024 à 49151). Ces numéros de ports sont affectés à des processus ou applications d'utilisateurs. Ces processus sont essentiellement des applications particulières qu'un utilisateur a choisi d'installer plutôt que des applications courantes qui recevraient un port réservé. Un client peut également sélectionner dynamiquement ces ports en tant que ports source lorsqu'ils ne sont pas utilisés par une ressource serveur.

Ports privés ou dynamiques (numéros 49152 à 65535). Également appelés ports éphémères, ces ports sont généralement affectés de façon dynamique à des applications clientes lorsqu'une connexion est initiée. Il est relativement rare pour un client de se connecter à un service par le biais d'un port dynamique ou privé (bien que certains programmes de partage de fichiers peer to peer le fassent).

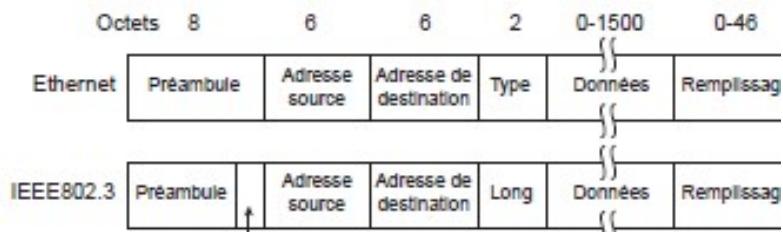
Numéro de port	protocole	Application
20	TCP	Données FTP
21	TCP	Contrôle FTP
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67,68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	HTTPS (SSL)
16, 384-32, 767	UDP	Voix(VoIP) et vidéo avec RTP

Tableau 8 : Applications courantes et numéro de port réservé

Chapitre 1 : Structure des PDU

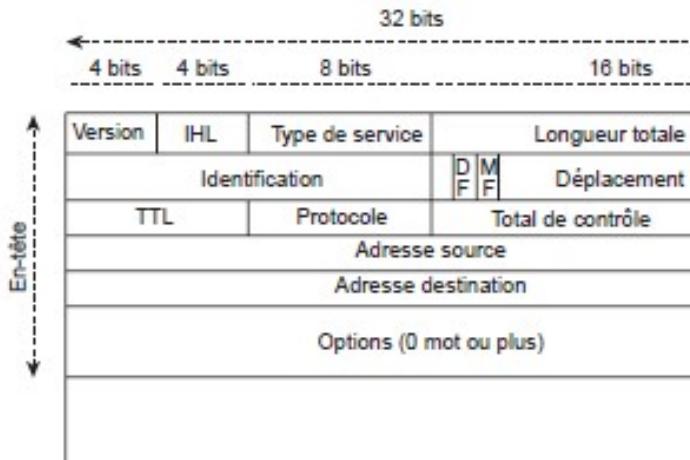
1. Structure de la trame Ethernet

La figure 5.9. illustre le format de la trame Ethernet de base. Il comprend un long préambule (101010...) provoquant l'émission d'un signal rectangulaire de fréquence 10 MHz si le débit de transmission est de 10 Mbit/s. L'ensemble des équipements du réseau se synchronise ainsi sur le message émis. Le champ SFD (*Start Frame Delimiter*) contient la séquence 10101011 qui marque le début de la trame. La trame contient dans son premier champ significatif l'adresse du destinataire DA (*Destination Address*) et celle de l'expéditeur SA (*Source Address*). Il s'agit des adresses MAC dont nous avons parlé à la section 1.2. Un champ sur deux octets précise la longueur (en nombre d'octets) des données de la couche LLC. La norme 802.3 ayant défini une longueur minimale de trame à 64 octets (qui représente à 10 Mbit/s un temps de transmission de 51,2 microsecondes), celle-ci est complétée par des octets de « bourrage » si la trame est plus courte. En fait, la taille de la trame doit être comprise entre 64 et 1 518 octets, ce qui laisse de 46 à 1 500 octets « utiles » dans le champ de données. La taille maximale est imposée pour assurer un rôle équitable entre les différents équipements (celui qui a réussi à prendre la parole ne peut pas la monopoliser...). La trame se termine par un champ FCS (*Frame Check Sequence*). Calculé par l'émetteur, le FCS permet au récepteur de vérifier la validité des trames reçues.



Initialement, dans la norme IEEE 802.3, le champ longueur devait indiquer la longueur réelle du contenu de la trame. Dans la pratique, le contenu de la trame définit implicitement sa propre longueur. Ce champ, rebaptisé *type*, s'utilise désormais pour indiquer à quel protocole appartiennent les données encapsulées dans la trame. Par exemple, il peut prendre (en hexadécimal) les valeurs suivantes : 0800 (protocole IP), 0806 (protocole ARP), 0835 (protocole RARP). Nous reverrons au chapitre 6 le rôle de ces trois protocoles.

2. Format du datagramme IP V4



Le datagramme IP comprend un en-tête et des données. L'en-tête contient principalement les adresses IP de la source et du destinataire, et des informations sur la nature des données transportées (voir figure 6.4). Classiquement, les différents champs sont décrits par des mots de 32 bits. La première ligne de la figure 6.4 contient quatre champs :

- *Version*. Il s'agit de la version du protocole IP qu'on utilise (actuellement, c'est la version 4 ou IPv4) afin de vérifier la validité du datagramme. La version est codée sur 4 bits.
- *Longueur de l'en-tête*. Le nombre de mots de 32 bits de l'en-tête (qui commence avec le champ version). La longueur est également codée sur 4 bits. De ce fait, un en-tête IP contient (en hexadécimal) au maximum F mots de 32 bits, soit 60 octets.
- *Type de services (ToS)*. Ce champ de 8 bits indique la façon dont le datagramme doit être traité. Historiquement, il était possible de demander que le datagramme soit traité sur la route la plus rapide, sur celle qui offrait le meilleur débit, la plus fiable, etc. Encore fallait-il être capable de mesurer l'état des routes et de gérer les options... Les premières implémentations du protocole IP ont vite abandonné cette idée de services différenciés. Le champ ToS est resté à 0, d'autant que plusieurs propositions incompatibles les unes avec les autres ont été faites pour modifier l'attribution de ce champ.
- Nous verrons à la section 5 que la version IPv6 reprend, sous une forme différente, l'idée de qualité de service.
- *Longueur totale*. Ce champ de 16 bits exprime en octets la taille totale du datagramme (en-tête + données). La longueur maximale d'un datagramme est donc 64 Ko, mais des raisons physiques imposent des tailles inférieures dans la plupart des réseaux.
- Le deuxième mot de 32 bits concerne la fragmentation. Le champ *Identification* est un numéro de 16 bits attribué à chaque datagramme. Chaque fragment d'un même datagramme reprend le même identifiant, pour permettre le râssemblage correct du datagramme initial chez le destinataire. Après un premier bit non utilisé, les deux bits suivants sont des *drapeaux* qui permettent le râssemblage :
 - *DF : Don't Fragment* (le deuxième bit). Autorise ou non la fragmentation du datagramme (si DF = 0 la fragmentation est autorisée, interdite si DF = 1). Par convention, toute machine doit pouvoir transmettre en un seul datagramme des données de 476 octets.
 - *MF : More Fragments* (le dernier bit). Indique si le fragment de données est suivi ou

non par d'autres fragments (si MF = 0, le fragment est le dernier du datagramme).

Le champ *Déplacement* permet de connaître la position du début du fragment par rapport au datagramme initial. Le fragment doit avoir une taille qui est un multiple entier de 8 octets. Le déplacement est codé sur les 13 derniers bits du mot.

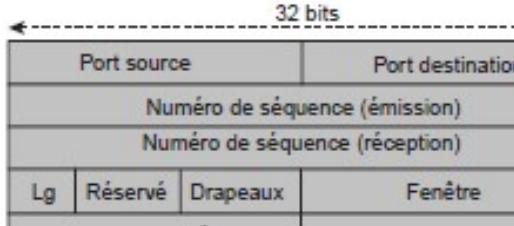
Le troisième mot de 32 bits contient trois champs :

- *Durée de vie (TTL, Time To Live)*. Indique sur 8 bits le nombre maximal de routeurs que le datagramme peut traverser. Ce champ était prévu à l'origine pour décompter un temps, d'où son nom. La durée de vie est choisie par l'émetteur ; elle est décrémentée chaque fois que le datagramme traverse un routeur. Lorsque la durée de vie atteint la valeur nulle, le datagramme est détruit.
 - *Protocole*. Champ de 8 bits indiquant à quel protocole sont destinées les données véhiculées dans le datagramme. Les valeurs décimales les plus courantes sont : 1 pour ICMP, 2 pour IGMP (*Internet Group Management Protocol*, ou protocole de gestion des groupes multicast), 6 pour TCP et 17 pour UDP.
 - *Header checksum*. Ces 16 bits suivants constituent un bloc de contrôle d'erreur pour l'en-tête : ce champ permet de contrôler l'intégrité de l'en-tête. Celui-ci, en effet, transporte toutes les informations fondamentales du datagramme. Si, par hasard, il était détecté en erreur, le datagramme serait directement écarté. Remarquons qu'il n'y a aucune protection concernant les données transportées dans le datagramme.
- Les deux derniers mots de 32 bits contiennent, dans cet ordre, l'*adresse IP source* et l'*adresse IP destination*. Ces cinq mots constituent l'en-tête minimal, commun à tous les datagrammes IP. En plus de ces informations, l'en-tête peut contenir en option des informations supplémentaires. C'est pourquoi il faut en indiquer la longueur.
- Les options doivent tenir sur un nombre entier de mots de 32 bits. Parmi elles, le *routage* et l'*horodatage* sont particulièrement intéressantes (l'horodatage demande à chaque routeur d'estampiller le datagramme avec la date et l'heure à laquelle il a été traité). Elles constituent un bon moyen de surveiller ou de contrôler la traversée des datagrammes dans le réseau. Une autre option, l'*enregistrement de route*, demande à chaque routeur traversé de placer sa propre adresse dans le datagramme. Le destinataire reçoit ainsi un datagramme contenant la liste des adresses des routeurs traversés. Le *routage défini par la source*, lui, permet à l'émetteur d'imposer le chemin par lequel doit passer un datagramme.

3. format du datagramme transport

3.1 Datagramme TCP

Il faut remarquer qu'il n'y a qu'un seul format de segment TCP, illustré à la figure 7.1, bien que le protocole soit complexe. Le segment contient un en-tête de 20 octets (sauf options) et un champ de données.



Signification des différents champs

- **Port Source** (16 bits). Numéro du port utilisé par l'application en cours sur la machine source.
- **Port Destination** (16 bits). Numéro du port relatif à l'application en cours sur la machine de destination.
- **Numéro d'ordre** (32 bits). La signification de ce numéro est à interpréter selon la valeur du drapeau SYN (*Synchronize*). Lorsque le bit SYN est à 0, le numéro d'ordre est celui du premier octet de données du segment en cours (par rapport à tous les octets du flot de données transportées). Lorsqu'il est à 1, le numéro d'ordre est le *numéro initial*, celui du premier octet du flux de données qui sera transmis (*Initial Sequence Number*). Celui-ci est tiré au sort, plutôt que de commencer systématiquement à 02.
- **Numéro d'accusé de réception** (32 bits). Numéro d'ordre du dernier octet reçu par le récepteur (par rapport à tous les octets du flot de données reçues).
- **Longueur en-tête** (4 bits). Il permet de repérer le début des données dans le segment. Ce décalage est essentiel, car il est possible que l'en-tête contienne un champ d'option de taille variable. Un en-tête sans option contient 20 octets, donc le champ longueur contient la valeur 5, l'unité étant le mot de 32 bits (soit 4 octets).
- **Réservé** (6 bits). Champ inutilisé (comme dans tous les formats normalisés, il reste une petite place, prévue en cas d'évolutions à venir ou en cas de bogue à corriger, par exemple).
- **Drapeaux ou flags** (6 bits). Ces bits sont à considérer individuellement :
 - **URG (Urgent)**. Si ce drapeau est à 1, le segment transporte des données urgentes dont la place est indiquée par le champ Pointeur d'urgence (voir ci-après).
 - **ACK (Acknowledgement)**. Si ce drapeau est à 1, le segment transporte un accusé de réception.
 - **PSH (Push)**. Si ce drapeau est à 1, le module TCP récepteur ne doit pas attendre que son tampon de réception soit plein pour délivrer les données à l'application. Au contraire, il doit délivrer le segment immédiatement, quel que soit l'état de son tampon (méthode Push).
 - **RST (Reset)**. Si ce drapeau est à 1, la connexion est interrompue.
 - **SYN (Synchronize)**. Si ce drapeau est à 1, les numéros d'ordre sont synchronisés (il s'agit de l'ouverture de connexion).
 - **FIN (Final)**. Si ce drapeau est à 1, la connexion se termine normalement.
- **Fenêtre** (16 bits). Champ permettant de connaître le nombre d'octets que le récepteur est capable de recevoir sans accusé de réception.
- **Total de contrôle ou checksum** (16 bits). Le total de contrôle est réalisé en faisant la somme des champs de données et de l'en-tête. Il est calculé par le module TCP émetteur

et permet au module TCP récepteur de vérifier l'intégrité du segment reçu.

- *Pointeur d'urgence* (16 bits). Indique le rang à partir duquel l'information est une donnée urgente.

- *Options* (taille variable). Options diverses, les plus fréquentes étant :

- *MSS (Maximum Segment Size)*. Elle sert à déterminer la taille maximale du segment que le module TCP accepte de recevoir. Au moment de l'établissement d'une connexion, le module émetteur annonce sa taille de MSS.

- *Timestamp (estampille temporelle)*. Sert à calculer la durée d'un aller et retour (RTT, Round Trip Time).

- *Wscale (Window Scale ou facteur d'échelle)*. Sert à augmenter la taille de la fenêtre au-delà des 16 bits du champ Fenêtre normal. Si la valeur proposée est n , alors la taille maximale de la fenêtre est de $65\ 535 \times 2^n$.

- *Remplissage*. Les options utilisent un nombre quelconque d'octets, or les segments TCP sont toujours alignés sur une taille multiple entier de 4 octets. Si l'en-tête sans option compte 5 mots de 32 bits, les options peuvent avoir une taille quelconque. Si besoin, on remplit l'espace qui suit les options avec des zéros pour aligner la taille du segment à une longueur multiple de 32 bits.

- *Données*. Ce champ transporte les données normales et éventuellement les données urgentes du segment.

3.2 Datagramme UDP

Les messages UDP sont généralement appelés *datagrammes UDP*. Ils contiennent deux parties, un en-tête et des données encapsulées dans les datagrammes IP, comme les segments TCP.



L'en-tête très simple compte quatre champs :

- *Port source* (16 bits). Il s'agit du numéro de port correspondant à l'application émettrice du paquet. Ce champ représente une adresse de réponse pour le destinataire.
- *Port destination* (16 bits). Contient le port correspondant à l'application de la machine à laquelle on s'adresse. Les ports source et destination ont évidemment la même signification que pour TCP.
- *Longueur* (16 bits). Précise la longueur totale du datagramme UDP, exprimée en octets. La longueur maximale des données transportées dans le datagramme UDP est de : $216 - 4 \times 16$, soit 65 472 octets.
- *Total de contrôle* ou *checksum* (16 bits). Bloc de contrôle d'erreur destiné à contrôler l'intégrité de l'en-tête du datagramme UDP, comme dans TCP.

Chapitre2 : Routeur et configuration de base

1. L'intérieur d'un routeur

1.1 Les routeurs sont des ordinateurs

Un routeur est un ordinateur comme un autre. Le processeur IMP (Interface Message Processor), utilisé pour l'ARPANET (Advanced Research Projects Agency Network), a été le tout premier routeur. Grâce au processeur IMP, un mini-ordinateur Honeywell 316, l'ARPANET a vu le jour le 30 août 1969.

Remarque : l'ARPANET a été développé par l'ARPA (Advanced Research Projects Agency), relevant du ministère américain de la Défense. L'ARPANET a été le premier réseau de commutation de paquets opérationnel du monde et le prédecesseur de l'Internet d'aujourd'hui. Les routeurs possèdent de nombreux composants matériels et logiciels communs avec d'autres ordinateurs :

Processeur

RAM

ROM

Système d'exploitation

a) Les routeurs se trouvent au centre du réseau

Les utilisateurs ne sont pas forcément conscients de la présence de nombreux routeurs sur leur propre réseau ou sur Internet. Les utilisateurs veulent pouvoir accéder aux pages Web, envoyer des courriels et télécharger de la musique, que le serveur auquel ils accèdent se trouve sur leur propre réseau ou sur un autre réseau situé à des milliers de kilomètres. Toutefois, les professionnels des réseaux savent que c'est le routeur qui est responsable du transfert de paquets d'un réseau à l'autre, de la source à la destination.

Un routeur relie plusieurs réseaux. Pour ce faire, il dispose de plusieurs interfaces, chacune appartenant à un réseau IP différent. Lorsqu'un routeur reçoit un paquet IP sur une interface, il détermine quelle interface utiliser pour transférer le paquet vers sa destination.

L'interface utilisée par le routeur pour transférer le paquet peut être le réseau de la destination finale du paquet (celui qui porte l'adresse IP de destination de ce paquet) ou il peut s'agir d'un réseau relié à un autre routeur utilisé pour accéder au réseau de destination.

Chaque réseau auquel un routeur se connecte nécessite généralement une interface séparée. Ces interfaces sont utilisées pour se connecter à une combinaison de réseaux locaux et réseaux étendus. Les réseaux locaux sont généralement des réseaux Ethernet comportant des périphériques tels que des PC, imprimantes et serveurs. Les réseaux étendus sont utilisés pour relier des réseaux dans une zone géographique vaste. Par exemple, une connexion WAN est généralement utilisée pour relier un réseau local au réseau du fournisseur de services Internet.

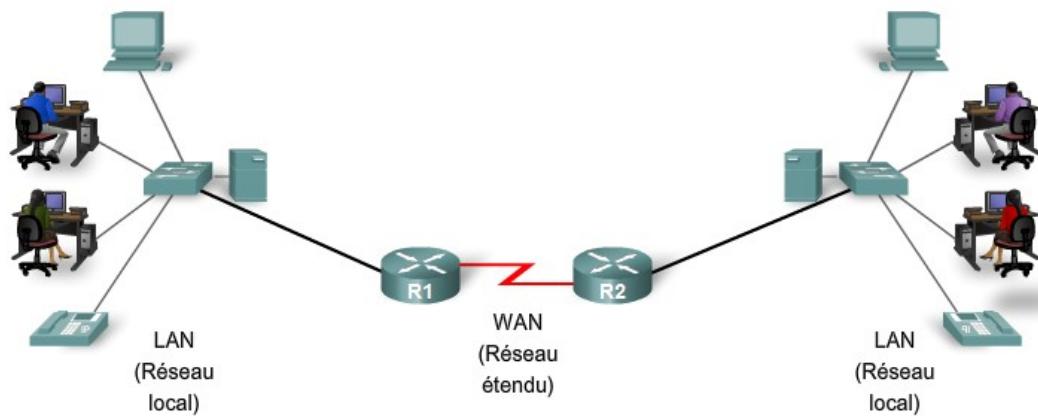


Figure 7 : Routeurs dans un réseau WAN

b) Les routeurs déterminent le meilleur chemin

La fonction principale d'un routeur consiste à diriger les paquets destinés à des réseaux locaux et distants en :

- déterminant le meilleur chemin pour l'envoi des paquets,
- transférant les paquets vers leur destination.

Le routeur utilise sa table de routage pour déterminer le meilleur chemin pour le transfert du paquet. Lorsque le routeur reçoit un paquet, il examine son adresse IP de destination et recherche, dans la table de routage, l'adresse réseau qui lui correspond le mieux. La table de routage contient également l'interface à utiliser pour le transfert du paquet. Une fois une correspondance trouvée, le routeur encapsule le paquet IP dans la trame de liaison de données de l'interface sortante ou de sortie, et le paquet est alors transféré vers sa destination.

Il est fort probable qu'un routeur recevra un paquet encapsulé dans un type de trame de liaison de données, comme une trame Ethernet, et lors du transfert du paquet, l'encapsule dans un autre type de trame de liaison de données, comme le protocole point-à-point (PPP). L'encapsulation de la liaison de données dépend du type d'interface présente sur le routeur et du type de support auquel celui-ci se connecte. Les différentes technologies de liaison de données auxquelles un routeur se connecte peuvent inclure des technologies LAN, comme Ethernet, et des connexions série WAN, comme une connexion T1 utilisant PPP, Frame Relay et le mode ATM.

Des routes statiques et protocoles de routage dynamique sont utilisés par les routeurs pour découvrir des réseaux distants et créer leurs tables de routage. Le cours se concentre essentiellement sur ces routes et protocoles, décrits en détail dans les chapitres suivants ainsi que le processus utilisé par les routeurs pour les recherches dans leurs tables de routage et le transfert des paquets.

1.2 Processeurs et mémoire de l'ordinateur

Bien qu'il existe plusieurs types et modèles de routeurs, chacun comporte, à la base, les mêmes composants matériels. Selon le modèle, ces composants se trouvent à différents emplacements dans le routeur. La figure présente l'intérieur d'un routeur 1841. Pour voir les composants internes du routeur, vous devez dévisser et retirer son couvercle métallique. En général, il n'est pas nécessaire d'ouvrir le routeur, sauf pour mettre à niveau la mémoire.



Figure 8 : carte mère d'un routeur

a) Composants du routeur et leurs fonctions

Comme un PC, un routeur comprend également les éléments suivants :

- Unité centrale (UC)
- Mémoire vive (RAM)
- Mémoire morte (ROM)

b) L' unité Centrale

L'UC exécute les instructions du système d'exploitation, telles que l'initialisation du système, des fonctions de routage et de commutation.

c) Mémoire vive

La mémoire vive stocke les instructions et données requises pour exécution par l'UC. La mémoire vive est utilisée pour enregistrer ces composants :

- Système d'exploitation : le système IOS (Internetwork Operating System) de Cisco est copié dans la mémoire vive pendant l'amorçage.
- Fichier de configuration en cours : il s'agit du fichier de configuration qui enregistre les commandes de configuration actuellement utilisées par l'IOS du routeur. À de rares exceptions près, toutes les commandes configurées sur le routeur sont enregistrées dans le fichier de configuration en cours, appelé running-config.
- Table de routage IP : ce fichier stocke des informations sur les réseaux directement connectés et les réseaux distants. Il permet de déterminer le meilleur chemin pour le transfert du paquet.
- Cache ARP : ce cache contient les mappages d'adresses IPv4 et MAC, de manière similaire au cache ARP d'un PC. Le cache ARP est utilisé sur les routeurs dotés d'interfaces de réseau local, telles que les interfaces Ethernet.
- Mémoire tampon de paquets : les paquets sont stockés temporairement dans une mémoire tampon lors de leur réception sur une interface ou avant de quitter une interface.

La mémoire vive est une mémoire volatile : elle perd donc son contenu lorsque le routeur est mis hors tension ou redémarré. Cependant, le routeur contient également des zones de stockage permanent, comme la mémoire morte, flash et NVRAM.

d) Mémoire morte

La mémoire morte est une forme de stockage permanent. Les périphériques Cisco utilisent la mémoire morte pour enregistrer les éléments suivants :

- Instructions d'amorçage
- Logiciel de diagnostic de base
- Version réduite d'IOS

La mémoire morte utilise un progiciel, qui est un logiciel incorporé dans le circuit intégré. Le progiciel inclut les logiciels qui n'ont habituellement pas besoin d'être modifiés ou mis à niveau, les instructions d'amorçage par exemple. Plusieurs de ces fonctions, notamment le moniteur ROM, sont étudiées dans un prochain cours. La mémoire morte ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

e) Mémoire flash

La mémoire flash est une mémoire non volatile pouvant être stockée et effacée électriquement. Elle sert de stockage permanent pour le système d'exploitation, Cisco IOS. Sur la plupart des modèles de routeurs Cisco, l'IOS est stocké de manière permanente dans la mémoire flash et copié dans la mémoire vive lors du processus d'amorçage, où il est ensuite exécuté par le processeur. Certains modèles plus anciens de routeurs Cisco exécutent l'IOS directement à partir de la mémoire flash. La mémoire flash se compose de barrettes SIMM ou de cartes PCMCIA, qui peuvent être mises à niveau pour en augmenter la capacité.

La mémoire flash ne perd pas son contenu lorsque le routeur est mis hors tension ou redémarré.

f) Mémoire vive non volatile

La mémoire vive non volatile ne perd pas les informations qu'elle contient lorsque le système est mis hors tension. Elle s'oppose aux formes les plus courantes de mémoire vive, telles que la mémoire vive dynamique (DRAM), qui nécessite une alimentation continue pour conserver les informations. La mémoire vive non volatile est utilisée par Cisco IOS comme stockage permanent pour le fichier de configuration initiale (startup-config). Toutes les modifications de configuration sont enregistrées dans le fichier de configuration en cours (running-config) dans la mémoire vive, et sont, à de rares exceptions près, immédiatement implémentées par l'IOS. Pour enregistrer ces modifications, au cas où le routeur serait redémarré ou mis hors tension, la configuration en cours doit être copiée dans la mémoire vive non volatile, où elle est enregistrée en tant que fichier de configuration initiale. La mémoire vive non volatile conserve son contenu, même si le routeur se recharge ou s'il est mis hors tension.

La mémoire morte, la mémoire vive, la mémoire vive non volatile et la mémoire flash sont étudiées dans la section suivante, portant sur l'IOS et le processus d'amorçage. Elles seront également traitées plus en détail dans un cours ultérieur relatif à la gestion de l'IOS.

Il est plus important pour un professionnel des réseaux de comprendre la fonction des principaux composants internes d'un routeur que de connaître l'emplacement exact de ces composants dans un routeur donné. L'architecture physique interne diffère d'un modèle à l'autre.

g) Processus de démarrage d'un routeur

- ✓ Le routeur exécute l'autotest POST(Power-On-Self-test) pour reconnaître les composants matériels et vérifier qu'ils fonctionnent correctement.
- ✓ Il copie en RAM un programme d'amorçage depuis la ROM et l'exécute
- ✓ Le programme d'amorçage décide quelle image d'IOS charger en RAM et la Charge, puis il lui transfère le contrôle du routeur. Les IOS se trouvent dans le Flash ou dans un serveur TFTP.
- ✓ Si le programme d'amorçage a chargé l'IOS, l'IOS localise le fichier de configuration (le fichier startup-config en NVRAM ou dans un serveur TFP) et le charge en RAM sous running-config.

2. Configuration de base d'un routeur

Pour configurer un routeur, on se connecte sur ce routeur avec un PC via le câble console si le routeur n'est pas encore configuré ou à l'aide du protocole TELNET ou SSH. La configuration se fait en ligne de commande sur une console du PC. Il existe plusieurs mode de configuration du routeur :

- Mode utilisateur **R>**
- Mode privilégié **R#**
- Mode configuration globale **R(Config)#**
- Mode interface **R(Config-int)#**

Lors de la configuration d'un routeur, certaines tâches de base sont effectuées :

- Attribution d'un nom au routeur
R(Config)#hostname « nom du routeur »
- Définition de mots de passe
- Mot de passe pour se connecter en mode console
R(Config) # line console 0
R(Config-line)#password « mot de passe »

R(Config-line)#login

- Mot de passe pour la connexion par TELNET

R(Config) # line vty 0 15

R(Config-line)#password « mot de passe »

R(Config-line)#login

- Mot de passe pour passer du mode utilisateur au mode privilégié

R(Config)#enable password « mot de passe » ‘mot de passe en clair’

R(Config)#enable password « mot de passe » ‘mot de passe crypté’

Pour que tous les mots de passe apparaissent cryptés, il faut utiliser la commande

R(Config)# service password-encryption

- Configuration d'interfaces

R(config)#interface fastethernet 0/1

R(Config-int)#ip address « adresse IP » « masque de sous-réseau »

R(Config-int)#description « description de l'interface »

- Configuration d'une bannière

Une bannière est une phrase de bienvenue et d'avertissement pour les utilisateurs du routeur.

- MOTD (Message of the day) affiché avant l'invite de connexion

R(Config)#banner MOTD « message »

- Login affiché avant l'invite de connexion mais après le bananière MOTD

R(Config)#banner login « message »

- Exec affiché après l'invite de connexion

R(Config)#banner exec « message »

- Désactivation de la recherche DNS

R(Config)#no ip domain-lookup

- Enregistrement des modifications apportées à un routeur

R#copy running-config startup-config

R#write memory

- Vérification de la configuration de base

R#show running-config

Configuration des paramètres de base d'un routeur

Syntaxe des commandes de configuration des paramètres de base d'un routeur	
Attribution d'un nom au routeur	Router(config)#hostname <i>name</i>
Définition des mots de passe	Router(config)#enable secret <i>password</i> Router(config)#line console 0 Router(config-line)#password <i>password</i> Router(config-line)#login Router(config)#line vty 0 4 Router(config-line)#password <i>password</i> Router(config-line)#login
Configuration d'une bannière de message du jour	Router(config)#banner motd # <i>message</i> #

Tableau 9 : configuration de base d'un routeur

Chapitre 3 : Généralités sur le Routage

1. Présentation de la table de routage

La fonction principale d'un routeur est de transférer un paquet à son réseau de destination, qui correspond à l'adresse IP du paquet. Pour ce faire, le routeur doit rechercher les informations de routage stockées dans sa table de routage.

Une table de routage est un fichier de données dans la mémoire vive servant à stocker les informations sur la route à emprunter sur les réseaux directement connectés et les réseaux distants. La table de routage contient des associations réseau/tronçon suivant. Celles-ci informent un routeur qu'une destination donnée peut être atteinte de manière optimale en envoyant le paquet à un routeur donné, lequel représente le « tronçon suivant » sur le chemin menant à la destination finale. L'association de tronçon suivant peut également être constituée de l'interface de sortie vers la destination finale.

L'association réseau/interface de sortie peut également représenter l'adresse réseau de destination du paquet IP. Cette association se produit sur les réseaux directement connectés au routeur. Un tel réseau est directement relié à l'une des interfaces du routeur. Lorsqu'une interface de routeur est configurée avec une adresse IP et un masque de sous-réseau, l'interface devient un hôte sur ce réseau connecté. L'adresse réseau et le masque de sous-réseau de l'interface, ainsi que le type et le numéro de l'interface, sont entrés dans la table de routage en tant que réseau directement connecté. Lorsqu'un routeur transfère un paquet à un hôte, un serveur Web par exemple, cet hôte se trouve sur le même réseau qu'un réseau directement connecté au routeur.

Un réseau distant n'est pas directement connecté au routeur. En d'autres termes, un réseau distant est un réseau qui peut être atteint uniquement en envoyant le paquet à un autre routeur. Les réseaux distants sont ajoutés à la table de routage grâce à un protocole de routage dynamique ou grâce à la configuration de routes statiques. Les routes dynamiques, qui mènent à des réseaux distants, sont apprises automatiquement par le routeur et utilisent un protocole de routage dynamique. Les routes statiques mènent à des réseaux configurés manuellement par l'administrateur réseau.

Remarque : La table de routage, avec ses réseaux directement connectés, ses routes statiques et dynamiques, est présentée dans les sections suivantes et décrite plus en détail tout au long du cours.

Pour consulter la table de routage, on utilise la commande en mode privilégié :

R#show ip route

Les analogies suivantes peuvent aider à clarifier le concept de routes connectées, statiques et dynamiques :

- Routes directement connectées : Pour rendre visite à un voisin, il vous suffit de descendre la rue dans laquelle vous habitez déjà. Ce chemin est similaire à une route directement connectée car la « destination » est directement disponible via votre « interface connectée », la rue.
- Routes statiques : Pour une route donnée, un train utilise toujours la même voie ferrée. Ce chemin est similaire à une route statique car la voie menant à la destination est toujours la même.
- Routes dynamiques : Lorsque vous conduisez une voiture, vous pouvez « dynamiquement » choisir une route différente, en fonction du trafic, des conditions météorologiques ou autres. Ce chemin est similaire à une route dynamique car, tout au long du trajet, vous pouvez choisir, à différents moments, de prendre une autre route.

Les routes directement connectées sont apprises automatiquement dès que les interfaces du routeur sont configurés d'une manière appropriée. Les routes statiques sont configurés par l'administrateur et les routes dynamiques sont apprises à travers les protocoles de routage dynamique.

Les informations qu'on trouve dans la table de routage sont :

- Le protocole de routage
- Le réseau de destination
- La métrique
- La distance administrative
- L'interface de sortie

On distingue les routages statiques et les routages dynamiques. Nous allons étudier le routage statique au prochain chapitre. Dans le cas des routages dynamiques, il existe des protocoles de routages dynamiques que nous allons classifier au prochain paragraphe.

Plusieurs caractéristiques permettent de comparer les protocoles de routage :

- Temps de convergence
- Évolutivité
- Sans classe (utilisation d'un masque VLSM) ou par classe
- Utilisation des ressources
- Implémentation et maintenance

2. Protocoles de routage dynamique

Les protocoles de routage dynamique sont utilisés dans les réseaux depuis le début des années 80. La première version du protocole RIP a vu le jour en 1982, mais certains de ses algorithmes de base étaient déjà utilisés dans ARPANET depuis 1969.

De nouveaux protocoles de routage ont émergé à mesure que les réseaux ont évolué et se sont complexifiés. RIP (Routing Information Protocol) est l'un des tous premiers protocoles de routage. Il a évolué pour donner naissance à la version RIPv2. Toutefois, cette nouvelle version n'est toujours pas adaptée aux grands réseaux. Aussi, deux protocoles de routage avancés ont été développés pour répondre aux besoins des réseaux plus importants : OSPF (Open Shortest Path First) et IS-IS (Intermediate System-to-Intermediate System). Cisco a développé les protocoles IGRP (Interior Gateway Routing Protocol) et EIGRP (Enhanced IGRP), qui présentent également une bonne évolutivité dans les réseaux plus importants. Il a fallu par ailleurs interconnecter des interréseaux différents et assurer un routage entre ces derniers. Le protocole BGP (Border Gateway Routing) est aujourd'hui utilisé entre FAI et entre des FAI et leurs clients privés plus importants pour échanger des informations de routage.

Le nombre de périphériques utilisant le protocole IP ne cessant de croître, l'espace d'adressage IPv4 est pratiquement épuisé, d'où l'émergence d'IPv6. De nouvelles versions des protocoles de routage IP ont été développées pour prendre en charge les communications reposant sur IPv6.

Ce chapitre présente une vue d'ensemble des différents protocoles de routage dynamique. Les protocoles de routage RIP, EIGRP et OSPF sont présentés en détail dans les chapitres suivants. Les protocoles de routage IS-IS et BGP sont quant à eux présentés dans le cursus CCNP. IGRP est le précurseur d'EIGRP et est désormais obsolète.

2.1 Maintenance de la table de routage

a) Fonction des protocoles de routage dynamique

Un protocole de routage est un ensemble de processus, d'algorithmes et de messages qui sont utilisés pour échanger des informations de routage et construire la table de routage en y indiquant les meilleurs chemins choisis par le protocole. Un protocole de routage permet d'effectuer les opérations suivantes :

- Découverte des réseaux distants

- Actualisation des informations de routage
- Choix du meilleur chemin vers des réseaux de destination
- Capacité à trouver un nouveau meilleur chemin si le chemin actuel n'est plus disponible

2.2 Quels sont les composants d'un protocole de routage ?

Structures des données - Pour fonctionner, certains protocoles de routage utilisent des tables et/ou des bases de données. Ces informations sont conservées dans la mémoire vive.

Algorithme - Un algorithme est une liste précise d'étapes permettant d'accomplir une tâche. Les protocoles de routage utilisent des algorithmes pour faciliter l'échange d'informations de routage et déterminer le meilleur chemin d'accès.

Messages de protocoles de routage - Les protocoles de routage utilisent différents types de messages pour découvrir les routeurs voisins, échanger des informations de routage et effectuer d'autres tâches afin de découvrir et de gérer des informations précises sur le réseau.#

2.3 Fonctionnement des protocoles de routage dynamique

Tous les protocoles de routage ont la même fonction qui consiste à découvrir des réseaux distants et à s'adapter rapidement en cas de modification de la topologie. La méthode adoptée à cette fin par un protocole de routage dépend de l'algorithme qu'il utilise et des caractéristiques de fonctionnement de ce protocole. Les opérations d'un protocole de routage dynamique dépendent du type de protocole de routage et du protocole de routage lui-même. D'une manière générale, le fonctionnement d'un protocole de routage dynamique peut être décrit de la manière suivante :

- Le routeur envoie et reçoit des messages de routage sur ses interfaces.
- Le routeur partage les messages et les informations de routage avec d'autres routeurs qui utilisent le même protocole de routage.
- Les routeurs échangent des informations de routage pour découvrir des réseaux distants.
- Lorsqu'un routeur détecte une modification topologique, le protocole de routage peut l'annoncer aux autres routeurs.

L'algorithme utilisé pour les protocoles de routage définit les processus suivants :

- Mécanisme d'envoi et de réception des informations de routage

- Mécanisme de calcul des meilleurs chemins et d'installation de routes dans la table de routage
- Mécanisme de détection des modifications topologiques et de réaction à celles-ci

2.4 Avantages et inconvénients du routage dynamique

Avantages du routage dynamique :

- Réduction pour l'administrateur des tâches de maintenance de la configuration lors de l'ajout et de la suppression de réseaux.
- Les protocoles réagissent automatiquement aux modifications topologiques.
- La configuration est moins sujette aux erreurs.
- Plus évolutif, l'expansion du réseau ne présente généralement pas de problème.

Inconvénients du routage dynamique :

- Utilisation des ressources du routeur (cycle de processeur, mémoire et bande passante de liaison).
- Les administrateurs doivent avoir des connaissances plus approfondies pour la configuration, la vérification et le dépannage.

2.5 Distance administrative

Bien que ce soit moins fréquent, il est possible de déployer plusieurs protocoles de routage dynamique sur le même réseau. La distance administrative (AD) définit la préférence d'une source de routage. Chaque source de routage (y compris les protocoles de routage spécifiques, les routes statiques et même les réseaux connectés directement) est classée par ordre de priorité, du plus préférable au moins préférable, à l'aide d'une valeur de distance administrative. La distance administrative est une valeur entière comprise entre 0 et 255. Plus la valeur est faible, plus la source de la route est privilégiée. Une distance administrative de 0 est idéale. Seul un réseau directement connecté à une distance administrative égale à 0, laquelle ne peut pas être modifiée.

Origine de la route	Distance administrative
Connecté	0
Statique	1
Résumé de routes EIGRP	5
BGP externe	20
EIGRP interne	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120

Tableau 10 : distance administrative par défaut

3. Classification des protocoles de routage dynamique

Voici trois principes de la table de routage :

Principe 1 : « Chaque routeur prend sa décision seul, en se basant sur les informations dont il dispose dans sa propre table de routage. »

Principe 2 : « Le fait qu'un routeur dispose de certaines informations dans sa table de routage ne signifie pas que d'autres routeurs ont les mêmes informations. »

Principe 3 : « Les informations de routage concernant un chemin d'un réseau à l'autre ne fournissent aucune information de routage sur le chemin inverse ou de retour. »

3.1 Protocoles IGP et EGP

Un système autonome (SA), également appelé domaine de routage, est un ensemble de routeurs dont l'administration est commune. Le réseau interne d'une société et le réseau d'un fournisseur de services Internet en sont des exemples. Dans la mesure où Internet repose sur le concept de système autonome, deux types de protocoles de routage sont nécessaires : des protocoles de routage intérieurs et extérieurs. Ces protocoles sont les suivants :

- Les protocoles IGP (Interior Gateway Protocols) sont utilisés pour le routage interne du système autonome. Les protocoles IGP pour IP sont : RIP, IGRP, EIGRP, OSPF et IS-IS.

- Les protocoles EGP (Exterior Gateway Protocol) sont utilisés pour le routage entre systèmes autonomes. BGP est le seul protocole de routage EGP actuellement viable utilisé par Internet.

3.2 Vecteurs de distance et état de lien

Les protocoles IGP (Interior Gateway Protocols) peuvent appartenir à deux types :

- Protocoles de routage à vecteur de distance : RIP, IGRP
- Protocoles de routage d'état des liaisons : EIGRP, OSPF, IS-IS

3.3 Protocoles de routage par classe et sans classe

Les protocoles de routage par classe n'envoient pas d'informations sur les masques de sous-réseau dans les mises à jour de routage. Les protocoles de routage par classe incluent RIPv1 et IGRP.

Les protocoles de routage sans classe incluent le masque de sous-réseau avec l'adresse réseau dans les mises à jour de routage. Les protocoles de routage sans classe sont RIPv2, EIGRP, OSPF, IS-IS et BGP.

Chapitre 4 : Routage Statique

Les réseaux distants sont ajoutés à la table de routage grâce à la configuration de routes statiques ou à l'activation d'un protocole de routage dynamique. Lorsque l'IOS doit atteindre un réseau distant et qu'il est informé de l'interface à utiliser, il ajoute cette route à la table de routage tant que l'interface de sortie est activée.

Une route statique inclut l'adresse réseau et le masque de sous-réseau du réseau distant, ainsi que l'adresse IP du routeur du tronçon suivant ou de l'interface de sortie. Les routes statiques sont indiquées par le code S dans la table de routage, comme illustré dans la figure. Elles sont abordées en détail au chapitre suivant.

1. Quand utiliser les routes statiques

Les routes statiques doivent être utilisées dans les cas suivants :

- Un réseau ne comporte que quelques routeurs. Dans ce cas, l'utilisation d'un protocole de routage dynamique ne présente aucun bénéfice substantiel. Par contre, le routage dynamique peut accroître la charge administrative.
- Un réseau est connecté à Internet via un seul FAI. Il n'est pas nécessaire d'utiliser un protocole de routage dynamique sur cette liaison car le FAI représente le seul point de sortie vers Internet.
- Un grand réseau est configuré dans une topologie Hub and Spoke. Une topologie Hub and Spoke est constituée d'un emplacement central (le concentrateur ou « Hub ») et de multiples terminaisons (les rayons ou « spokes »), chaque rayon ayant une seule connexion au concentrateur. L'utilisation du routage dynamique serait inutile car chaque terminaison n'est reliée à une destination donnée que par un chemin unique, qui passe par l'emplacement central.

Généralement, la plupart des tables de routage contiennent une combinaison de routes statiques et de routes dynamiques. Toutefois, comme indiqué précédemment, la table de routage doit d'abord contenir les réseaux directement connectés utilisés pour accéder aux réseaux distants, avant de pouvoir utiliser tout routage statique ou dynamique.

2. Commande ip route

La commande de configuration d'une route statique est ip route. La syntaxe complète pour configurer une route statique est :

```
Router(config)#ip route prefix mask {ip-address | interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]
```

La plupart de ces paramètres n'ont aucune importance pour ce chapitre. Nous allons utiliser une version simplifiée de la syntaxe :

Router(config)#ip route network-address subnet-mask {ip-address | exit-interface }

Les paramètres suivants sont utilisés :

network-address : adresse réseau de destination du réseau distant à ajouter à la table de routage.

subnet-mask : masque de sous-réseau du réseau distant à ajouter à la table de routage. Le masque de sous-réseau peut être modifié pour résumer un groupe de réseaux.

Un des paramètres suivants ou les deux doivent également être utilisés :

ip-address : communément considérée comme l'adresse IP du routeur de tronçon suivant.

exit-interface : interface sortante à utiliser pour le transfert de paquets vers le réseau de destination.

Remarque : le paramètre ip-address est communément considéré comme l'adresse IP du routeur du « tronçon suivant ». L'adresse IP du routeur du tronçon suivant réel est communément utilisée pour ce paramètre. Toutefois, le paramètre ip-address peut être n'importe quelle adresse IP, tant qu'elle peut être résolue dans la table de routage.

3. Configurations des routes statiques

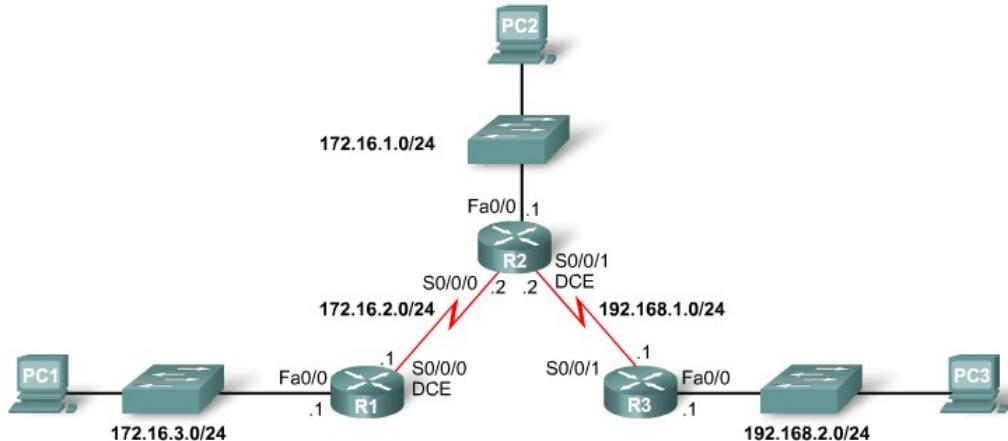


Figure 9 : Configuration d'une route statique

3.1 Installation d'une route statique dans la table de routage

N'oubliez pas que R1 connaît ses réseaux connectés directement. Il s'agit des routes actuellement présentes dans sa table de routage. Les réseaux distants que R1 ne connaît pas sont :

- 172.16.1.0/124 : le réseau local sur R2 ;
- 192.168.1.0/24 : le réseau série entre R2 et R3 ;
- 192.168.2.0/24 : le réseau local sur R3.

Tout d'abord, activez debug ip routing pour que l'IOS affiche un message lorsque la nouvelle route est ajoutée à la table de routage. Ensuite, utilisez la commande ip route pour configurer des routes statiques sur R1 pour chacun de ces réseaux. La figure représente la première route configurée.

```
R1#debug ip routing  
R1#conf t  
R1(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2
```

Analysons chaque élément dans cette sortie :

ip route - Commande de route statique
172.16.1.0 - Adresse réseau de réseau distant
255.255.255.0 - Masque de sous-réseau de réseau distant
172.16.2.2 - Adresse IP d'interface Serial 0/0/0 sur le routeur R2, qui représente le « saut suivant » vers ce réseau

Lorsque l'adresse IP constitue l'adresse IP du routeur de saut suivant réelle, cette adresse IP est joignable à partir de l'un des réseaux directement connectés de ce routeur. En d'autres termes, l'adresse IP du tronçon suivant 172.16.2.2 est sur le réseau 172.16.2.0/24 directement connecté au Serial 0/0/0 du routeur R1.

3.2 Vérification de la route statique

Les résultats de la commande debug ip routing indiquent que cette route a été ajoutée à la table de routage.

```
00:20:15: RT: add 172.16.1.0/24 via 172.16.2.2, static metric [1/0]
```

Notez dans la figure qu'en entrant show ip route sur le routeur R1, la nouvelle table de routage apparaît. L'entrée de la route statique est mise en surbrillance.

Examinons ce résultat :

S : code de la table de routage pour la route statique ;

172.16.1.0 : adresse réseau pour la route ;

/24 : masque de sous-réseau pour cette route. Il est affiché dans la ligne de dessus, appelée la route parent, et est traité plus en détail au chapitre 8 ;

[1/0] : distance administrative et mesure pour la route statique (expliquées dans un autre chapitre) ;

via 172.16.2.2 : adresse IP du prochain routeur de tronçon suivant, l'adresse IP de l'interface Serial 0/0/0 de R2.

Tout paquet dont les 24 bits les plus à gauche de l'adresse IP de destination correspondent à 172.16.1.0 utilisent cette route.

4. Listes de commandes du routage statique

Use ...	To ...
Router(config)#ip route <destination> <next_hop>	Identify a next hop router to receive packets sent to the specified destination network.
Router(config)#ip route <destination> <interface>	Identify the interface used to forward packets to the specified destination network.
Router(config)#ip default-network <network>	Identify a default network on which all packets sent to unknown networks are forwarded.
Router(config)#ip classless	Enables the router to match routes based on the number of bits in the mask and not the default subnet mask.

Tableau 11 : commandes du routage statique

5. Avantages et inconvénients du routage statiques

a. Avantages du routage statique

- Traitement processeur minimal.
- Plus facile à comprendre par l'administrateur.

- Facile à configurer

b. Inconvénients du routage statique

- La configuration et la maintenance prennent du temps.
- La configuration présente des risques d'erreurs, tout particulièrement dans les grands réseaux.
- L'intervention de l'administrateur est requise pour assurer la maintenance des informations changeantes relatives aux routes.
- N'évolue pas bien pour les réseaux en expansion ; la maintenance devient fastidieuse.

Exige une connaissance complète de l'ensemble du réseau pour une implémentation correcte.

Chapitre 5 : Routage à vecteur de distance

1. Présentation des protocoles de routage à vecteur de distance

Vecteur de distance signifie que les routes sont exprimées en tant que vecteurs de distance et de direction. La distance est définie en termes de mesure, comme le nombre de sauts, et la direction est simplement le routeur de tronçon suivant ou l'interface de sortie. Les protocoles à vecteur de distance utilisent généralement l'algorithme Bellman-Ford pour déterminer le meilleur chemin.

Certains protocoles à vecteur de distance envoient régulièrement des tables de routage entières à tous les voisins connectés. Dans le cas des grands réseaux, ces mises à jour de routage peuvent être gigantesques et générer un trafic important sur les liaisons.

a) Les caractéristiques des protocoles de routage à vecteur de distance

Les protocoles de routage à vecteur de distance comprennent : RIP, IGRP et EIGRP. Un routeur utilisant un protocole de routage à vecteur de distance ne connaît pas le chemin complet vers un réseau de destination. Le routeur ne connaît que les éléments suivants :

- la direction ou l'interface dans laquelle les paquets doivent être transmis ;
- la distance le séparant du réseau de destination.

Les protocoles de routage à vecteur de distance ont des caractéristiques en commun.

- Des mises à jour régulières sont envoyées à intervalles fixes (30 secondes pour le protocole RIP et 90 secondes pour le protocole IGRP).
- Les voisins sont des routeurs qui partagent une liaison et qui sont configurés de manière à utiliser le même protocole de routage. Les routeurs utilisant un routage à vecteur de distance ne connaissent pas la topologie du réseau.
- Des mises à jour de diffusion sont envoyées à 255.255.255.255.
- Des mises à jour de toute la table de routage sont envoyées régulièrement à tous les voisins.

b) Choix du protocole de routage à vecteur de distance

Les protocoles à vecteur de distance sont particulièrement adaptés aux situations suivantes :

- Le réseau est simple et linéaire et ne nécessite pas de conception hiérarchique particulière.
- Les administrateurs ne sont pas suffisamment expérimentés pour configurer et dépanner les protocoles d'état des liaisons.

- Des types de réseaux spécifiques, comme les réseaux hub-and-spoke sont implémentés.
- Des délais de convergence extrêmement longs sur un réseau ne posent pas problème.

c) Avantages et inconvénients

Les avantages sont :

- Implémentation et maintenance simples
- Faible ressource requise (mémoire, processeur, bande passante)

Les inconvénients des protocoles de routage à vecteur de distance sont:

- Les boucles de routage
- Le temps de convergence qui est long
- Evolutivité limitée

2. Maintenance de la table de routage

Plusieurs protocoles à vecteur de distance ont recours à des mises à jour régulières pour échanger des informations de routage avec leurs voisins et maintenir les informations de routage à jour dans la table de routage. On distingue :

- Les mises à jour régulières
- Les mises à jour limitées
- Les mises à jour déclenchées
- Les gigues aléatoires

2.1 Les mises à jour régulières : RIPv1 et IGRP

Pour les protocoles RIP, ces mises à jour sont envoyées toutes les 30 secondes sous forme de diffusion (255.255.255.255) que la topologie ait été ou non modifiée. L'intervalle de 30 secondes est un minuteur de mise à jour des routes qui permet également de connaître l'âge des informations de routage dans une table de routage.

Outre le minuteur de mise à jour, l'IOS implémente trois minuteurs supplémentaires pour le protocole RIP :

- Temporisation (Invalid Timer) (180 secondes par défaut) : après ce temps, si le routeur n'a pas reçu les mises à jour d'un réseau, le routeur met la valeur de 16 au niveau du nombre de saut de ce réseau.
- Annulation (Flush Timer) (240 secondes par défaut) : après ce temps, si le routeur n'a pas reçu les mises à jour d'un réseau, le routeur supprime ce réseau dans sa table de routage.
- Mise hors service (Hold-down Timer) (180 secondes par défaut) :
 - ❖ Un routeur reçoit une mise à jour d'un voisin lui indiquant qu'un réseau auparavant accessible est devenu inaccessible.
 - ❖ Le routeur marque la route comme étant éventuellement inactive et démarre le minuteur de mise hors service
 - ❖ Si une mise à jour avec une mesure inférieure pour ce réseau est reçue d'un voisin entre temps, le réseau est rétabli et le minuteur de mise hors service est arrêté.
 - ❖ Si une mise à jour d'un voisin a une mesure identique ou supérieure pour ce réseau, cette mise à jour est ignorée
 - ❖ Les routeurs continuent d'acheminer les paquets au réseau de destination qui sont marqués étant éventuellement inactif

2.2 Mises à jour limitées : EIGRP

À la différence des autres protocoles de routage à vecteur de distance, le protocole EIGRP n'envoie pas de mises à jour régulières. Au lieu de cela, le protocole EIGRP envoie des mises à jour limitées à propos d'une route en cas de modification d'un chemin ou de la mesure pour cette route. Lorsqu'une nouvelle route devient disponible ou qu'une route doit être supprimée, le protocole EIGRP envoie une mise à jour ne concernant que ce réseau et non la table entière. Ces informations sont envoyées uniquement aux routeurs qui en ont besoin.

Le protocole EIGRP utilise des mises à jour qui présentent les caractéristiques suivantes :

- Elles ne sont pas régulières car elles ne sont pas envoyées périodiquement.
- Des mises à jour partielles sont envoyées uniquement en cas de modification topologique influençant les informations de routage.
- Elles sont limitées, ce qui signifie que la propagation des mises à jour partielles est automatiquement limitée de sorte que seuls les routeurs ayant besoin de ces informations sont mis à jour.

2.3 Mises à jour déclenchées

Pour accélérer la convergence en cas de modification de la topologie, le protocole RIP utilise des mises à jour déclenchées. Une mise à jour déclenchée est une mise à jour de la table de routage qui est envoyée immédiatement en réponse à la modification d'un routage.

Des mises à jour déclenchées sont envoyées lorsque l'un des événements suivants se produit :

- Une interface change d'état (activée ou désactivée)
- Une route passe à l'état « inaccessible » (ou sort de cet état)
- Une route est installée dans la table de routage

Pour pouvoir utiliser uniquement des mises à jour déclenchées, il faudrait avoir la certitude que la vague de mises à jour atteigne immédiatement chaque routeur approprié. Toutefois, deux problèmes sont associés aux mises à jour déclenchées :

Les paquets contenant le message de mise à jour peut être abandonné ou endommagé par une liaison dans le réseau.

Les mises à jour déclenchées ne se produisent pas instantanément. Il est possible qu'un routeur qui n'a pas encore reçu la mise à jour déclenchée émette une mise à jour régulière au mauvais moment, provoquant ainsi la réinsertion de la route incorrecte dans un voisin ayant déjà reçu la mise à jour déclenchée.

2.4 Gigue aléatoire

Lorsque plusieurs routeurs transmettent simultanément des mises à jour de routage sur des segments LAN à accès multiples (comme illustré dans l'animation), les paquets de mise à jour peuvent entrer en collision et causer des délais ou consommer trop de bande passante.

Pour empêcher la synchronisation des mises à jour entre routeurs, le système IOS de Cisco utilise une variable aléatoire appelée RIP_JITTER qui soustrait un délai variable à l'intervalle de mise à jour pour chaque routeur dans le réseau. Cette gigue aléatoire, ou durée variable, correspond à une valeur comprise entre 0 % et 15 % de l'intervalle de mise à jour spécifié. Ainsi, l'intervalle de mise à jour varie aléatoirement de 25 à 30 secondes pour l'intervalle par défaut de 30 secondes.

3. Boucle de routage

Une boucle de routage est une condition dans laquelle un paquet est transmis en continu entre une série de routeurs sans jamais atteindre le réseau de destination souhaité. Une boucle de

routage peut se produire lorsque deux routeurs ou plus possèdent des informations de routage qui indiquent, à tort, qu'il existe un chemin valide vers une destination inaccessible.

La boucle peut être le résultat des problèmes suivants :

- Routes statiques configurées incorrectement
- Redistribution de routes configurées incorrectement (la redistribution, c.-à-d. le processus de transmission des informations de routage d'un protocole de routage à un autre)
- Tables de routage incohérentes qui ne sont pas mises à jour en raison d'une convergence lente dans un réseau changeant
- Routes de suppression configurées ou installées incorrectement

Les protocoles de routage à vecteur de distance sont d'un fonctionnement simple. Cette simplicité se traduit par des inconvénients, comme les boucles de routage. Les boucles de routage sont moins susceptibles de se produire avec les protocoles de routage d'état des liaisons, mais elles peuvent néanmoins survenir dans certaines circonstances.

Une boucle de routage peut créer les conditions suivantes :

La bande passante de la liaison est utilisée pour faire tourner le trafic en boucle entre les routeurs dans une boucle.

Le processeur d'un routeur est fortement sollicité en raison des paquets tournant en boucle.

Le processeur d'un routeur est surchargé en raison du réacheminement inutile de paquets, ce qui impacte négativement la convergence du réseau.

Les mises à jour de routage peuvent se perdre ou ne pas être traitées en temps voulu. Ces conditions introduisent des boucles de routage supplémentaires qui aggravent davantage la situation.

Les paquets peuvent se perdre dans des « trous noirs ».

Le comptage infini est une manifestation de la boucle de routage. Voici quelques éléments pour lutter contre les boucles infinis :

- Définition d'une valeur maximale de saut.
- Les minuteurs
- Découpage en horizon : un routeur ne doit pas annoncer de réseau par le biais de l'interface dont est issue la mise à jour.

- Découpage en horizon avec empoisonnement inverse et avec empoisonnement de route
- Le champ TTL (Time To Live): Le TTL est un champ dans l'en-tête d'un paquet IP et c'est une valeur comprise entre 0 et 255. Le routeur émetteur du paquet fixe la valeur du TTL. Lorsque le paquet traverse un saut dans le tronçon la valeur du TTL diminue. Lorsque le TTL atteint 0, le paquet est supprimé.

Chapitre 6 : VLSM et CIDR

1. Adressage VLSM

1.1 rappel sur l'adressage par classe

	Premier octet	Deuxième octet	Troisième octet	Quatrième octet	Masque de sous-réseau
Classe A	Réseau	Hôte	Hôte	Hôte	255.0.0.0 ou /8
Classe B	Réseau	Réseau	Hôte	Hôte	255.255.0.0 ou /16
Classe C	Réseau	Réseau	Réseau	Hôte	255.255.255.0 ou /24

Nombre de réseaux et d'hôtes par réseau pour chaque classe

Classe de l'adresse	Première plage d'octets	Nombre de réseaux possibles	Nombre d'hôtes par réseau
Classe A	De 0 à 127	128 (2 sont réservés)	16 777 214
Classe B	De 128 à 191	16 384	65 534
Classe C	De 192 à 223	2 097 152	254

Figure 10 : adressage par classe

Nous avons vu au chapitre 1 que pour une meilleure gestion des adresses IP, on pouvait découper une adresse réseau en sous-réseau. On avait alors plusieurs sous-réseaux avec la même longueur de masque de sous-réseau et donc avec le même nombre d'hôtes. Or dans la plupart des cas les sous-réseau n'ont pas nécessairement le même nombre d'hôtes. Pour un adressage plus efficace, on doit définir les masques de sous-réseau en fonction du nombre d'hôtes sur le sous-réseau. On définit ainsi un réseau VLSM(Variable Length Subnet Mask).

1.2 Calcul d'un réseau VLSM

Le problème posé ici est de déterminer le masque de chaque sous-réseau et les adresses de sous réseaux.

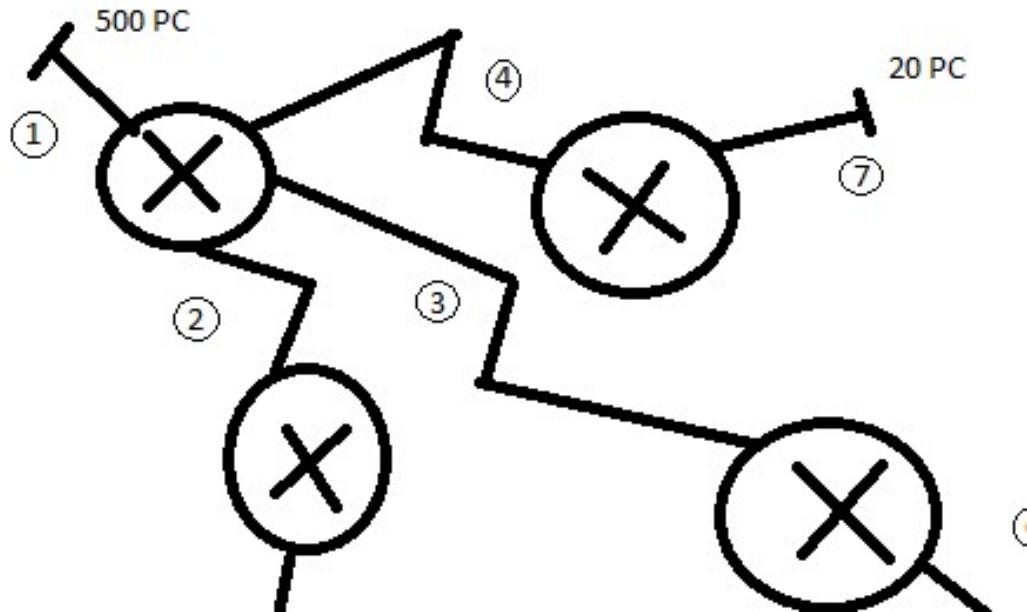


Figure 11 : réseau VLSM

Ce réseau contient 7 sous-réseau numéroté de 1 à 7. N est le nombre de bits de la partie réseau et H le nombre de bits de la partie hôte. Le nombre d'hôtes de ce réseau est $501 + 21 + 201 + 51 + 2 + 2 + 2 = 780$. $2^{10} = 1024$, d'où $H = 10$ et $N = 32 - H = 22$. Pour adresser ce réseau on va utiliser l'adresse réseau 172.16.0.0/22. Pour réaliser l'adressage de ce réseau, nous allons commencer par le sous-réseau qui a le plus d'hôtes.

- Sous-réseau 1

$$2^H - 2 = 501 \Rightarrow H = 9 \text{ et } N = 32 - H \Rightarrow N = 23$$

Masque sous-réseau : 255.255.254.0

Sous-réseau : 172.16.0.0/23

1^{er} hôte : 172.16.0.1

Dernier hôte : 172.16.1.254

Adresse de diffusion : 172.16.1.255

- Sous-réseau 6

$$2^H - 2 = 201 \Rightarrow H = 8 \text{ et } N = 32 - H \Rightarrow N = 24$$

Masque sous-réseau : 255.255.255.0

Sous-réseau : 172.16.2.0/24

1^{er} hôte : 172.16.2.1

Dernier hôte : 172.16.2.254

Adresse de diffusion : 172.16.2.255

- **Sous-réseau 5**

$$2^H - 2 = 51 \Rightarrow H = 6 \text{ et } N = 32 - H \Rightarrow N = 26$$

Masque sous-réseau : 255.255.255.192

Sous-réseau : 172.16.3.0/26

1^{er} hôte : 172.16.3.1

Dernier hôte : 172.16.3.62

Adresse de diffusion : 172.16.3.63

- **Sous-réseau 7**

$$2^H - 2 = 21 \Rightarrow H = 5 \text{ et } N = 32 - H \Rightarrow N = 27$$

Masque sous-réseau : 255.255.255.224

Sous-réseau : 172.16.3.64/27

1^{er} hôte : 172.16.3.65

Dernier hôte : 172.16.3.94

Adresse de diffusion : 172.16.3.95

- **Sous-réseau 2**

$$2^H - 2 = 2 \Rightarrow H = 2 \text{ et } N = 32 - H \Rightarrow N = 30$$

Masque sous-réseau : 255.255.255.252

Sous-réseau : 172.16.3.96/30

1^{er} hôte : 172.16.3.97

Dernier hôte : 172.16.3.98

Adresse de diffusion : 172.16.3.99

- **Sous-réseau 3**

$$2^H - 2 = 2 \Rightarrow H = 2 \text{ et } N = 32 - H \Rightarrow N = 30$$

Masque sous-réseau : 255.255.255.252

Sous-réseau : 172.16.3.100/30

1^{er} hôte : 172.16.3.101

Dernier hôte : 172.16.3.102

Adresse de diffusion : 172.16.3.103

- **Sous-réseau 4**

$$2^H - 2 = 2 \Rightarrow H = 2 \text{ et } N = 32 - H \Rightarrow N = 30$$

Masque sous-réseau : 255.255.255.252

Sous-réseau : 172.16.3.104/30

1^{er} hôte : 172.16.3.105

Dernier hôte : 172.16.3.106

Adresse de diffusion : 172.16.3.107

2. Protocole de routage compatible CIDR(*Classless Inter Domain Routing*)

a) Protocole de routage par classe

L'utilisation d'adresses IP par classe signifie que le masque de sous-réseau d'une adresse réseau peut être déterminé par la valeur du premier octet ou plus précisément, par les quatre premiers bits de l'adresse. Les protocoles de routage, tels que RIPv1, ont uniquement besoin de propager l'adresse réseau des routes connues mais n'ont pas besoin d'inclure le masque de sous-réseau à la mise à jour du routage. Ceci, parce que le routeur recevant la mise à jour de routage peut déterminer le masque de sous-réseau en examinant simplement la valeur du premier octet de l'adresse réseau, ou bien en appliquant le masque de son interface d'entrée dans le cas des routes découpées en sous-réseaux. Le masque du sous-réseau étant associé à l'adresse réseau de l'interface d'entrée.

b) Protocole de routage sans classe

En 1993, l'IETF introduit le routage interdomaine sans classe (CIDR) (RFC 1517). Le CIDR permet :

- Une utilisation plus efficace de l'espace d'adressage IPv4 ;

- Une agrégation du préfixe réduisant la taille des tables de routage.

CIDR utilise les masques de sous-réseau de longueur variable (VLSM) pour allouer les adresses IP aux sous-réseaux en fonction d'un besoin particulier, et non en fonction de la classe. Ce type d'allocation permet de positionner la coupure entre la partie réseau et la partie hôte à n'importe quel endroit (bit) dans l'adresse. La propagation de VLSM et des routes de super-réseau nécessite un protocole de routage sans classe car le masque de sous-réseau ne peut plus être déterminé par la valeur du premier octet de l'adresse IP. Le masque de sous-réseau doit maintenant accompagner l'adresse réseau. Les protocoles de routage sans classe incluent le masque de sous-réseau et l'adresse réseau dans la mise à jour du routage.

Les protocoles RIPv2, EIGRP, OSPF, IS-IS et BGP font partie des protocoles de routage sans classe. Ces protocoles de routage incluent le masque de sous-réseau et l'adresse réseau dans leurs mises à jour de routage. Les protocoles de routage sans classe sont nécessaires lorsque le masque ne peut pas être supposé ou déterminé par la valeur du premier octet.

Le CIDR ignore les limitations des classes et autorise le résumé avec les masques inférieurs à celui du masque par classe par défaut(c'est-à-dire le CIDR autorise les agrégations manuelles). Ce type de résumé permet de réduire le nombre d'entrées dans les mises à jour de routage et de diminuer le nombre d'entrées dans les tables de routage locales. Il permet également de réduire la bande passante utilisée pour les mises à jour de routage et d'effectuer des recherches plus rapidement dans les tables de routage.

Chapitre 7 : le protocole RIP

1. Etude du protocole RIP

1.1 Caractéristiques du protocole RIP

Comme évoqué dans le chapitre 4, « Protocoles de routage à vecteur de distance », le protocole RIP présente les principales caractéristiques suivantes :

- RIP est un protocole de routage à vecteur de distance.
- La seule mesure qu'il utilise pour le choix du chemin d'accès est le nombre de sauts.
- Les routes annoncées dont le nombre de sauts est supérieur à 15 sont inaccessibles.
- Les messages sont diffusés toutes les 30 secondes.
- RIP utilise le minuteur de mise hors service, minuteur d'annulation et le minuteur de temporisation pour éviter les boucles de routage.

1.2 Format des messages du protocole RIP : En-tête RIP

Trois champs sont spécifiés dans la partie en-tête à quatre octets apparaissant en orange dans la figure. Le champ Commande identifie le type de message (voir la section suivante pour plus de détails). Le champ Version est défini sur 1 pour Protocole RIP version 1. Le troisième champ est défini sur Must be zero. Les champs « Must be zero » fournissent de la place pour une extension future du protocole

1.3 Format de message RIP : Entrée de route

La partie entrée de route du message comprend trois champs avec le contenu suivant : Identificateur de famille d'adresses (de valeur 2 pour le protocole IP sauf si un routeur exige une table de routage complète, auquel cas ce champ doit avoir la valeur zéro), Adresse IP et Mesure. Cette partie du message relative à l'entrée de route représente une route de destination avec sa mesure associée. Une mise à jour RIP peut contenir jusqu'à 25 entrées de route. La taille maximale du datagramme est 512 octets, sans compter les en-têtes IP ou UDP.

1.4 Fonctionnement du protocole RIP

Le protocole RIP utilise deux types de messages spécifiés dans le champ Commande : un message de requête et un message de réponse. RIP est un protocole de routage par classe. Comme vous l'avez sans doute noté dans la discussion précédente sur le format des messages, le protocole RIPv1 n'envoie pas d'informations de masque de sous-réseau dans la mise à jour. Par conséquent, un routeur utilise le masque de sous-réseau configuré sur une interface locale ou applique le masque de sous-réseau par défaut de la classe de l'adresse. Du fait de cette

limite, les réseaux RIPv1 ne peuvent ni être discontinus, ni implémenter VLSM. La distance administrative par défaut du protocole RIP est 120. Par rapport aux autres protocoles IGP, RIP est le protocole de routage le moins apprécié. IS-IS, OSPF, IGRP et EIGRP ont tous des valeurs de distance administrative par défaut plus faibles.

2. Configuration du protocole RIP version 1

Pour configurer RIP version 1 il faut :

- Activer RIP au mode global avec la commande :

```
R(Config)#router rip
```

```
R(Config-router)#
```

- Spécifier les réseaux directement liés au routeur avec la commande

```
R(Config-router)#network << adresse réseau >>
```

Pour vérifier la configuration RIP, utiliser les commandes :

- **Show ip protocol**
- **Show ip route**
- **Debug ip rip**

Pour configurer une passerelle par défaut sur le routeur lié au FAI, utiliser la commande :

```
R(Config)#ip route 0.0.0.0 0.0.0.0 S0/0/0
```

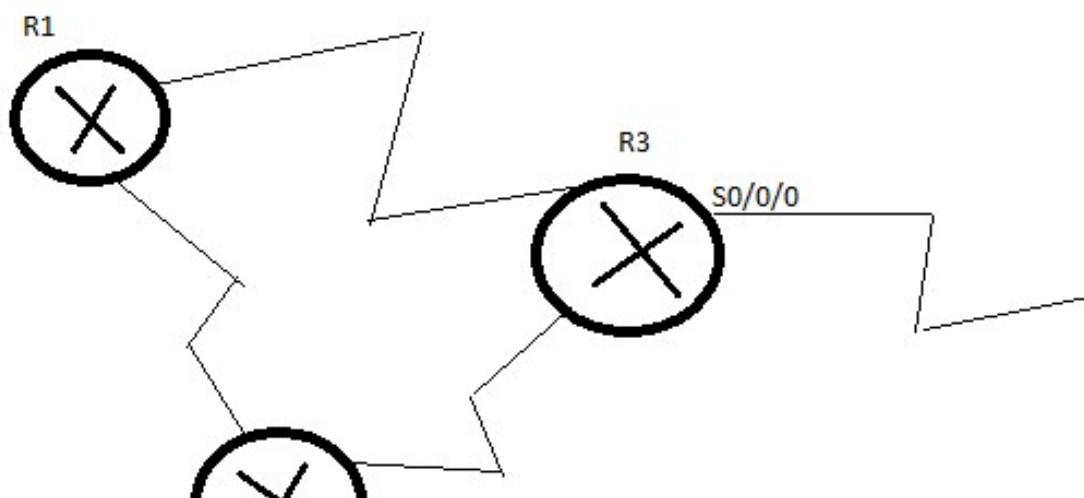


Figure 12 : passerelle par défaut

Il faut propager ensuite cette route par défaut sur les autres routeurs avec la commande :

R(Config-router)#default-information originate

Le routeur configuré en rip envoie les mises à jour sur toutes les interfaces qui ont été déclarées. Mais les mises à jour ne sont pas nécessaires sur toutes les interfaces, par exemple les interfaces qui sont reliées au PC. Pour éviter que les mises à jour soient envoyées sur ces interfaces il faut utiliser la commande :

- **R(Config-router)#passive-interface fastethernet0/0**

3. Limitations de RIP version 1

3.1 RIP version 1 et les réseaux discontinus

Un réseau discontinu est un réseau qui contient des sous-réseau ayant la même adresse réseau par classe et séparés par des sous-réseaux d'adresse réseau par classe différente.

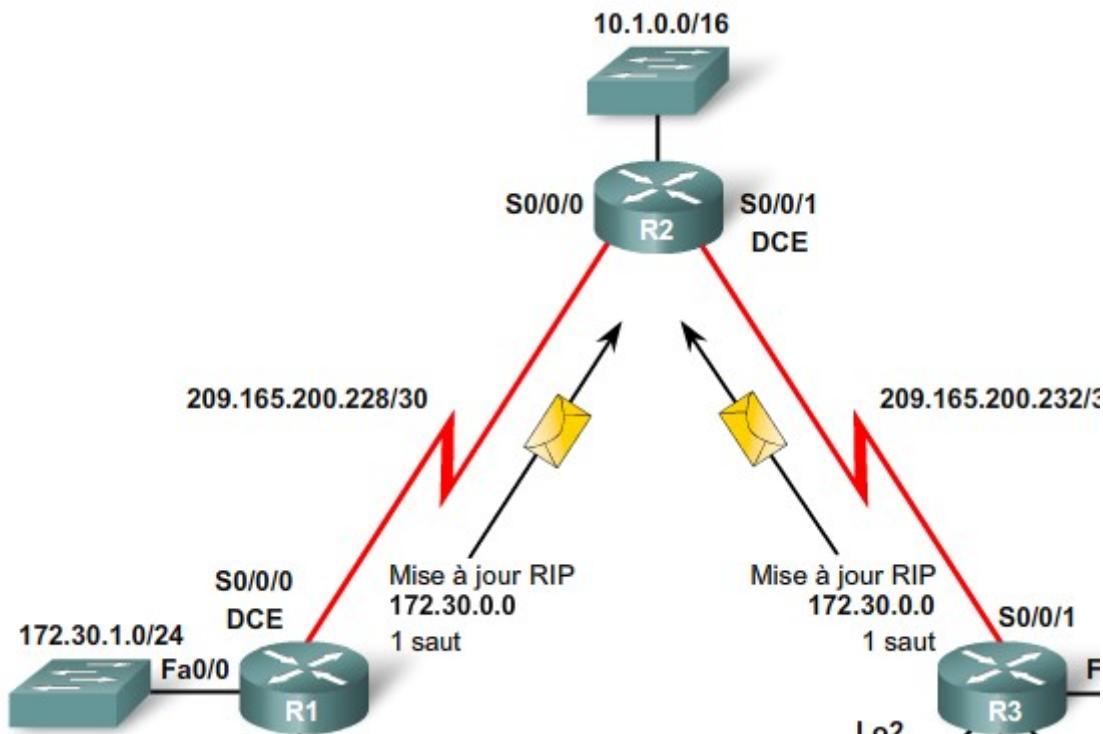


Figure 13 : réseau discontinu

Le masque de sous-réseau n'étant pas inclus dans la mise à jour, RIPv1 et d'autres protocoles de routage par classe peuvent résumer les réseaux au niveau des périphéries de réseau principal. Comme vous pouvez le constater dans la figure, RIPv1 résume les sous-réseaux 172.30.0.0 des routeurs R1 et R3 dans l'adresse réseau principal par classe de 172.30.0.0 lors de l'envoi de mises à jour de routage vers R2. Au niveau de R2, les deux mises à jour ont un coût égal d'un saut pour atteindre le réseau 172.30.0.0/16. Comme vous pouvez le constater,

R2 installe les deux chemins dans la table de routage. On conclut que RIP version 1 ne converge pas dans les réseaux discontinus.

3.2 RIP version 1 et VLSM

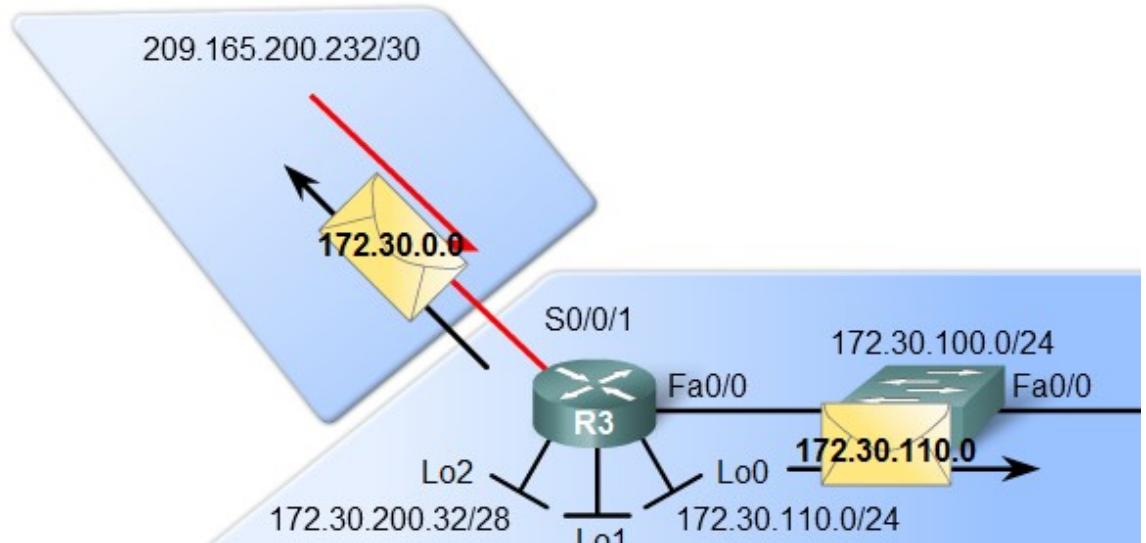


Figure 14 : VLSM et RIP version 1

R3 doit déterminer les sous-réseaux 172.30.0.0 à inclure dans les mises à jour qui définissent son interface FastEthernet 0/0 avec l'adresse IP 172.30.100.1/24. Il n'inclut dans sa table de routage que les routes 172.30.0.0 dont le masque est le même que celui de l'interface de sortie. S'agissant d'une interface 172.30.100.1 dotée d'un masque /24, il n'inclut que les sous-réseaux 172.30.0.0 dotés d'un masque /24. Le sous-réseau 172.30.110.0 est le seul à remplir cette condition.

Les autres sous-réseaux 172.30.0.0 (172.30.200.16/28 et 172.30.200.32/28) ne sont pas inclus car les masques /28 ne correspondent pas au masque /24 de l'interface sortante. Le routeur récepteur (R4) ne peut appliquer son propre masque d'interface /24 qu'aux annonces de route RIPv1 avec les sous-réseaux 172.30.0.0. R4 appliquerait le mauvais masque (/24) aux sous-réseaux dotés de masques /28. Conclusion : **RIP version 1 n'est pas compatible VLSM.**

3.3 RIP version 1 et CIDR

Nous avons vu qu'un protocole de routage est compatible CIDR lorsqu'il accepte les résumés de routes avec un masque inférieur au masque de la classe.

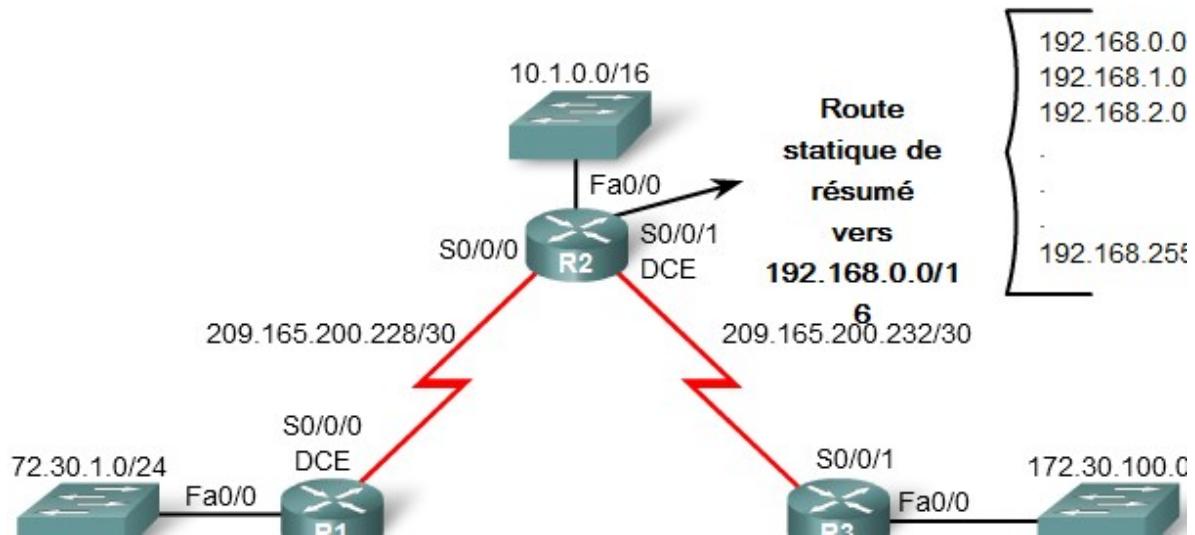


Figure 15 : résumé manuel de routes

La commande **redistribute static** est configuré sur R2 pour qu'il inclut ce réseau dans ses mises à jour avec RIP version 1. Nous avons configuré la route statique 192.168.0.0 avec un masque /16. Il compte moins de bits que le masque de classe C par classe /24. Le masque ne correspondant pas à la classe ni à un sous-réseau de la classe, RIPv1 n'inclut pas cette route dans ses mises à jour vers d'autres routeurs. D'où le protocole RIP version 1 n'est pas compatible CIDR.

3.4 RIP version 2

Pour répondre aux limitations de RIP version 1, une deuxième version de rip a été développée. C'est un protocole de routage par classe qui converge dans les réseaux discontinus et qui est compatible VLSM et CIDR. Pour le configurer il suffit d'ajouter la commande version 2 après l'activation de rip :

```
R(Config)# router rip
```

```
R(Config-router)#version 2
```

Pour éviter que rip version 2 ne fasse les résumés de route automatique comme le fait rip version 1 utiliser la commande :

```
R(Config-router)#no auto-summary
```

Chapitre 8: Protocole de routage à état de liens

Les protocoles de routage d'état des liaisons sont également appelés protocoles SPF (Shortest Path First), car ils sont conçus sur la base de l'algorithme SPF d'Edsger Dijkstra. L'algorithme SPF sera expliqué plus en détail dans une section ultérieure.

Les protocoles de routage d'état de liaisons IP sont:

- protocole OSPF (Open Shortest Path First) ;
- protocole de routage IS-IS.

Les protocoles de routage d'état de liaisons ont la réputation d'être beaucoup plus complexes que leurs équivalents à vecteur de distance. Cependant, la fonctionnalité et la configuration de base de ces protocoles de routage ne sont pas complexes du tout. Même l'algorithme lui-même est parfaitement compréhensible.

1. Routage d'état de liaisons

1.1 Algorithme SPF

L'algorithme de Dijkstra est en général désigné sous le nom d'algorithme SPF (shortest path first - chemin le plus court d'abord). Cet algorithme cumule les coûts de chaque chemin, depuis leur source jusqu'à leur destination. Bien que l'algorithme de Dijkstra soit connu sous le nom de l'algorithme du chemin le plus court, c'est en fait le but de chaque algorithme de routage.

1.2 Processus de routage d'état des liaisons

1. Chaque routeur prend connaissance de ses propres liaisons, de ses propres réseaux directement connectés. Il le fait en détectant qu'une interface est à l'état actif.
2. Chaque routeur est responsable de la détection de ses voisins sur les réseaux connectés directement. Comme avec le protocole EIGRP, les routeurs d'état de liaisons effectuent cette détection en échangeant des paquets Hello avec d'autres routeurs d'état de liaisons situés sur des réseaux directement connectés.
3. Chaque routeur crée un LSP (Link-State Packet) contenant l'état de chaque liaison directement connectée. Il procède en enregistrant toutes les informations pertinentes sur chaque voisin, notamment l'ID du voisin, le type de liaison et la bande passante.
4. Chaque routeur diffuse son LSP à l'ensemble de ses voisins, qui stockent tous les LSP qu'ils reçoivent dans une base de données. Les voisins diffusent ensuite le LSP à leurs voisins, jusqu'à ce que tous les routeurs de la zone aient reçu le LSP. Chaque routeur stocke une copie de chaque LSP reçu de ses voisins dans une base de données locale.

5. Chaque routeur utilise la base de données pour élaborer une carte complète de la topologie et calcule le meilleur chemin vers chaque réseau de destination. Le routeur possède ainsi une carte complète s'apparentant à une carte routière de l'ensemble des destinations de la topologie et des routes pour les atteindre. L'algorithme SPF sert à construire la carte de la topologie et à déterminer le meilleur chemin vers chaque réseau.

2. Mise en œuvre du protocole de routage d'état des liens

2.1 Avantages du protocole de routage d'état des liens

Les protocoles de routage d'état des liaisons présentent plusieurs avantages sur les protocoles de routage à vecteur de distance.

- Élaboration d'une carte topologique
- Convergence rapide
- Mises à jour pilotées par événement
- Conception hiérarchique

2.2 Eléments requis pour le protocole de routage d'état des liens

Configuration requise pour les protocoles de routage d'état des liaisons

- Mémoire requise pour la base de données d'état des liaisons
- Temps processeur requis pour l'exécution de l'algorithme SPF
- Bande passante requise pour l'inondation de paquets LSP

Contrairement à un routeur configuré avec un protocole de routage à vecteur de distance, un routeur configuré avec un protocole de routage d'état des liaisons peut créer une « vue complète » ou topologie du réseau en récupérant des informations provenant de tous les autres routeurs. Un routeur d'état des liaisons utilise les informations d'état des liaisons pour créer une topologie et sélectionner le meilleur chemin vers tous les réseaux de destination de la topologie.

Les protocoles d'état des liaisons sont tout particulièrement adaptés dans les situations suivantes :

- Réseau conçu de manière hiérarchique (il s'agit généralement de grands réseaux).

- Administrateurs ayant une bonne connaissance du protocole de routage d'état des liaisons implémenté.
- Réseaux pour lesquels une convergence rapide est primordiale.

Chapitre 9 : Le protocole de routage IGRP et EIGRP

Bien que le protocole EIGRP soit décrit comme un protocole de routage à vecteur de distance amélioré, il s'agit d'un protocole de routage à vecteur de distance à part entière. Cela peut quelquefois engendrer la confusion. Pour être en mesure d'en apprécier les améliorations et de dissiper toute confusion, commençons par étudier son prédecesseur, IGRP.

1. Caractéristique du protocole EIGRP

1.1 Les origines du protocole EIGRP : IGRP

Cisco a développé le protocole propriétaire IGRP en 1985, pour pallier certaines des limites du protocole RIPv1, notamment l'utilisation du nombre de sauts comme mesure et la taille maximale du réseau égale à 15 sauts.

Les protocoles IGRP et EIGRP n'utilisent pas le nombre de sauts, mais des mesures complexes comprenant la bande passante, le délai, la fiabilité et la charge. Par défaut, les deux protocoles de routage utilisent seulement la bande passante et le délai. Cependant, comme IGRP est un protocole de routage par classe utilisant l'algorithme Bellman-Ford et les mises à jour périodiques, son utilité est limitée sur bon nombre de réseaux actuels.

C'est pour cette raison que Cisco a amélioré IGRP en utilisant un nouvel algorithme, DUAL, ainsi que d'autres fonctions. Les commandes des protocoles IGRP et EIGRP sont similaires, et dans bien des cas, identiques. Cela permet une migration aisée d'IGRP vers EIGRP.



Résumé du fonctionnement

Protocoles traditionnels de routage à vecteur de distance

- Utilisent l'algorithme de Bellman-Ford ou Ford-Fulkerson ;
- Classent les entrées de routage par ancienneté et utilisent des mises à jour périodiques ;
- N'assurent le suivi que des meilleures routes ; le meilleur chemin vers un réseau de destination ;
- Lorsqu'une route n'est plus disponible, le routeur doit attendre une nouvelle mise à jour du routage ;
- Convergence plus lente en raison des minuteurs de mise hors service.

Protocole à vecteur de distance amélioré : EIGRP

- Utilise l'algorithme DUAL ;
- Ne classe pas les entrées de routage par ancienneté et n'utilise pas de mise à jour régulière ;
- Gère une table topologique séparée de la table de routage, qui comprend le meilleur chemin et les chemins de secours sans boucle ;
- Lorsqu'une route n'est plus disponible, l'algorithme DUAL utilise un chemin de secours de la table topologique ;
- Convergence plus rapide grâce à l'absence de minuteurs de mise hors service et à des calculs de routes coordonnés.

1.2 Format de message EIGRP

La partie donnée d'un message EIGRP est encapsulée dans un paquet. Ce champ de données est nommé Type/Longueur/Valeur ou TLV. Comme indiqué dans le schéma, les types de TLV concernant ce cours sont les paramètres EIGRP, des routes internes IP et les routes IP externes.

L'en-tête de paquet EIGRP est inclus dans chaque paquet EIGRP, quel que soit son type. L'en-tête de paquet EIGRP et TLV sont ensuite encapsulés dans un paquet IP. Dans l'en-tête de paquet IP, le champ protocole est défini à 88 pour indiquer EIGRP, et l'adresse de destination est définie à l'adresse multidiffusion 224.0.0.10. Si le paquet EIGRP est encapsulé dans une trame Ethernet, l'adresse MAC de destination est elle aussi une adresse multidiffusion : 01-00-5E-00-00-0A.



1.3 Modules dépendant d'un protocole

EIGRP a la capacité de router plusieurs protocoles différents, notamment IP, IPX et AppleTalk en utilisant des modules dépendant d'un protocole. Ces derniers ont pour charge d'effectuer des tâches de routage spécifiques pour chaque protocole de couche réseau.

1.4 EIGRP et RTP

RTP (Reliable Transport Protocol – Protocole de transport fiable) est le protocole utilisé par EIGRP pour la livraison et la réception des paquets EIGRP.

1.5 Protocole Hello

Avant que quelque paquet EIGRP que ce soit puisse être échangé entre routeurs, EIGRP doit détecter ses voisins. Les voisins EIGRP sont d'autres routeurs qui exécutent EIGRP sur des réseaux partagés directement connectés. Les routeurs EIGRP détectent les voisins et établissent des contiguïtés avec les routeurs voisins au moyen des paquets Hello.

1.6 Mises à jour

EIGRP utilise le terme partiel ou limité pour qualifier ses paquets de mise à jour. Contrairement au protocole RIP, EIGRP n'envoie pas de mises à jour périodiques. En revanche, EIGRP envoie ses mises à jour uniquement lorsque la mesure d'une route change. Le terme partiel signifie que la mise à jour ne contient que les informations concernant les modifications de route. Le terme limité désigne la propagation des mises à jour envoyées uniquement aux routeurs affectés par le changement.

1.7 L'algorithme DUAL

L'algorithme DUAL (Algorithme de diffusion de mise à jour) est l'algorithme de convergence qu'utilise le protocole EIGRP au lieu des algorithmes Bellman-Ford ou Ford Fulkerson utilisés par les autres protocoles de routage à vecteur de distance comme RIP.

1.8 Distance administrative

Par défaut, le protocole EIGRP a pour distance administrative 90 pour les routes internes, et 170 pour les routes importées depuis une source externe, par exemple, les routes par défaut.

1.9 Calcul de mesure EIGRP

EIGRP utilise les valeurs suivantes dans sa mesure composite pour calculer le chemin préféré vers un réseau :

- Bande passante
- Délai
- Fiabilité
- Charge

Mesure composite EIGRP

Formule par défaut :

$$\text{mesure} = [\text{K1} \cdot \text{bande passante} + \text{K3} \cdot \text{délai}]$$

Formule complète :

$$\text{mesure} = [\text{K1} \cdot \text{bande passante} + (\text{K2} \cdot \text{bande passante})/(256 - \text{charge}) + \text{K3} \cdot \text{délai}] * [\text{K5}/(\text{fiabilité} + \text{K4})]$$

(N'est pas utilisée si les valeurs « K » sont égales à 0)

Valeurs par défaut :
K1 (bande passante) = 1
K2 (charge) = 0
K3 (délai) = 1
K4 (fiabilité) = 0
K5 (fiabilité) = 0

Les valeurs « K » peuvent être modifiées à l'aide de la commande **metric weights**.

```
Router(config-router)#metric weights tos k1 k2 k3 k4 k5
```

Utilisez la commande d'interface bandwidth pour modifier la mesure de bande passante :

Router(config-if)#bandwidth kilobits

Utilisez la commande d'interface **no bandwidth** pour restaurer la valeur par défaut.

2. Configuration du protocole EIGRP

Pour activer le protocole eigrp sur un routeur, on utilise la commande en mode de configuration globale :

R(Config)#router eigrp id où id est le numéro de processus ;

Pour annoncer les réseaux, on utilise la commande :

R(Config-router)#network <adresse réseau> où <adresse réseau> est une adresse réseau par classe.

Par défaut, lorsqu'on utilise la commande network et une adresse de réseau par classe telle que 172.16.0.0, toutes les interfaces du routeur appartenant à cette adresse de réseau par classe sont activées pour EIGRP. Toutefois, l'administrateur réseau ne veut pas nécessairement inclure toutes les interfaces d'un réseau lorsqu'il active EIGRP. Pour configurer EIGRP afin d'annoncer des sous-réseaux spécifiques uniquement, utilisez l'option wildcard-mask de la commande network :

Router(config-router)#network network-address [wildcard-mask]

Considérez un masque générique (wildcard-mask) comme l'inverse d'un masque de sous-réseau. Le contraire du masque de sous-réseau 255.255.255.252 est 0.0.0.3. Pour calculer l'inverse du masque de sous-réseau, soustrayez le masque de sous-réseau à 255.255.255.255.

EIGRP inclut automatiquement un résumé de routage null0 comme route enfant lorsqu'une des deux conditions qui suivent est avérée :

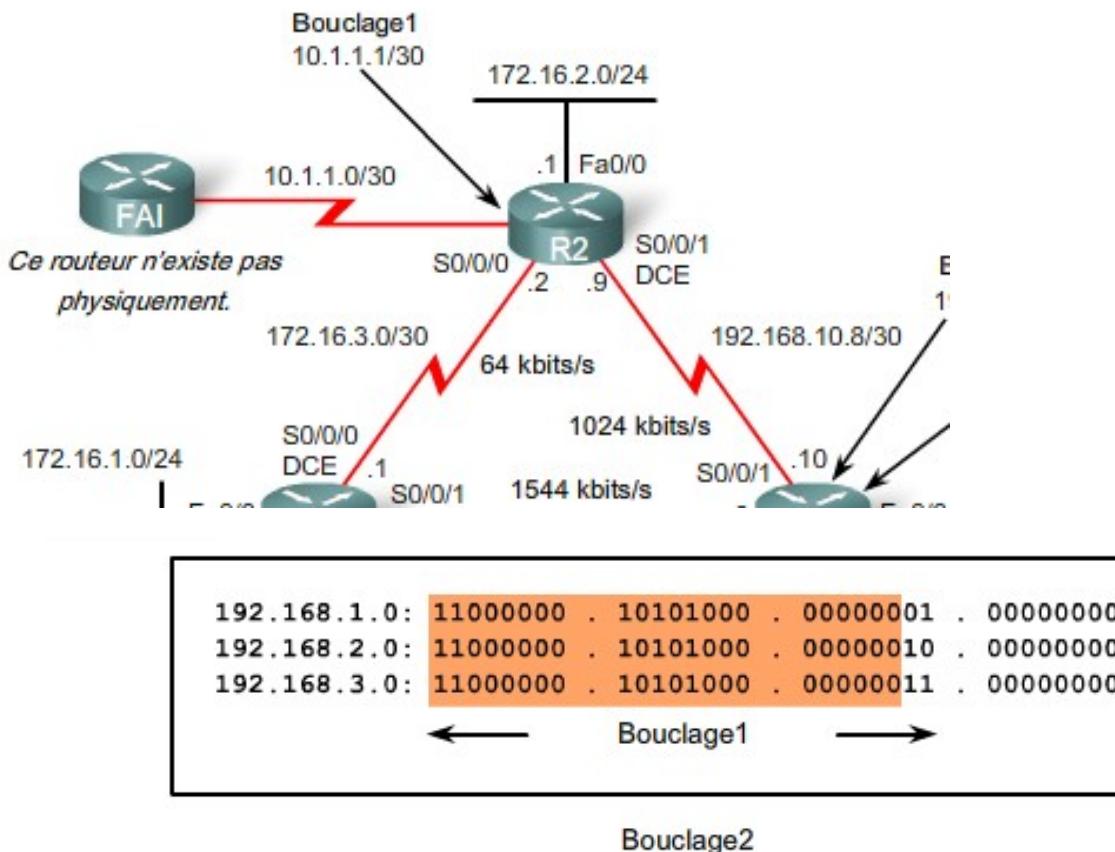
- Il existe au moins un sous-réseau qui a été acquis via EIGRP.
- Le résumé automatique est activé.

Le résumé automatique peut être désactivé avec la commande **no auto-summary**.

❖ résumé manuelle des routes

Pour établir le résumé manuel EIGRP sur toutes les interfaces qui envoient des paquets EIGRP, utilisez la commande d'interface suivante :

Router(config-if)#ip summary-address eigrp as-number network-address subnet-mask



```
R3(config)#interface serial 0/0/0
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
R3(config-if)#interface serial 0/0/1
R3(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.252.0
```

La configuration de la route par défaut se configure de la même manière que dans RIP. Seulement pour que le routeur inclut cette route dans ses mises à jour il faut utiliser la commande **redistribute static**.

Chapitre 10 : Le protocole OSPF

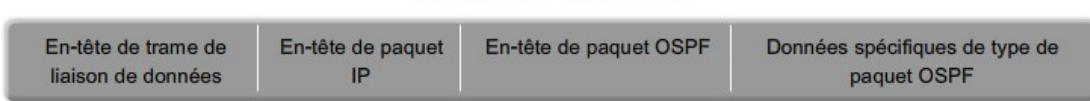
Le protocole de routage OSPF (Open Shortest Path First) est un protocole à état de lien qui a été développé pour remplacer le protocole de routage RIP. OSPF est un protocole de routage sans classe qui utilise le concept de zone. Pour son évolutivité, il est adapté aux grands réseaux. Il présente comme avantage sur RIP une convergence plus rapide ; en plus de son évolutivité, il fonctionne grâce à l'algorithme SPF lui-même basé sur l'algorithme de DIJKSTRA.

1. Fonctionnement du protocole OSPF

1.1 Encapsulation du packet OSPF

La partie donnée d'un message OSPF est encapsulée dans un paquet. Cette zone de données peut inclure un des 5 types de paquets OSPF. Chacun d'eux est brièvement présenté dans la rubrique qui suit.

L'en-tête de paquet OSPF est inclus dans chaque paquet OSPF, quel que soit son type. L'en-tête de paquet OSPF et les données spécifiques relatives à son type sont ensuite encapsulés dans le paquet IP. Dans l'en-tête de paquet IP, le champ protocole est défini à 89 pour indiquer OSPF, et l'adresse de destination a pour valeur une des deux adresses multidiffusion suivantes : 224.0.0.5 ou 224.0.0.6. Si le paquet OSPF est encapsulé dans une trame Ethernet, l'adresse MAC de destination est elle aussi une adresse multidiffusion : 01-00-5E-00-00-05 ou 01-00-5E-00-00-06.



1.2 Les types de paquets utilisés par OSPF

OSPF utilise 5 types de paquets pour construire 3 tables :

- Table des voisins (adjacency table)
- Base des données topologique (topologic database)
- Routing table (table de routage)

Les 5 paquets que OSPF utilisent sont :

- ❖ Paquet Hello : Découvrir ses voisins et les inscrire dans la table de voisins.

- ❖ Paquet Data base Description(DBD) : Ce paquet est émis par le routeur désigné (DR) pour synchroniser les bases de données des routeurs dans le système autonome.
- ❖ Paquet Link-state Request (LSR) : c'est une requête de mises à jour de la part d'un routeur qui n'est pas DR auprès du DR.
- ❖ Paquet Link-state Update (LSU) : c'est les mises à jour de la part d'un routeur qui n'est pas DR aux autres routeurs dans le système autonome.
- ❖ Paquet Link-state acknowledgment (LSAck) : Accusé de réception des autres 4 paquets.

1.3 Etude du protocole Hello

Le protocole Hello est responsable des paquets du même nom. Ces paquets sont les premiers à être utilisés par OSPF. Ils sont utilisés pour :

- Découvrir les voisins et établir les contiguïtés
- Annoncer les paramètres sur lesquels les deux routeurs doivent s'accorder pour devenir voisins.
- Il permet de définir le routeur désigné (DR : Designated Router) et les routeurs désignés de secours (BDR : Border Designated Router) sur les réseaux à accès multiples.

Avant que deux routeurs puissent former une contiguïté de voisinage, ils doivent s'entendre sur trois valeurs : l'intervalle Hello, l'intervalle DEAD et le type de réseau.

L'intervalle hello indique la fréquence à laquelle un routeur OSPF envoie des paquets hello. Par défaut, sa valeur est de 10s sur les segments à accès multiples et point à point, et de 30s sur les réseaux NBMA. Dans la plupart des cas, ces paquets sont envoyés à l'adresse de multidiffusion réservée 224.0.0.5.

L'intervalle Dead ou d'arrêt est la période pendant laquelle un routeur attendra de recevoir un paquet hello avant de déclarer son voisin hors service. Par défaut sa valeur est 4 fois celles des intervalles hello.

1.4 Sélection du routeur DR et BDR

Contrairement au protocole de routage à vecteur de distance, les protocoles de routage à état de lien constituent une base de données topologique du réseau afin de déterminer les

meilleurs chemins. Pour ce faire il utilise différents types de paquets de mises à jour appelés LSP. Le protocole OSPF a la particularité de définir 5 types différents de réseaux dans son mode de fonctionnement ;

- Les réseaux point à point
- Les réseaux à accès multiples avec diffusion
- Les réseaux à accès multiple sans diffusion (NBMA)
- Les réseaux point à multipoint
- Les liaisons virtuelles

Les réseaux NBMA et point à multipoint incluent les réseaux Frame Relay, ATM et X.25. Les réseaux point-à-multipoint sont traités dans le cours CCNP. Les liaisons virtuelles sont des liaisons de type spécial, qui peuvent être utilisées dans les OSPF à zones multiples. Les liaisons virtuelles OSPF sont traitées dans le cours CCNP.

Pour réduire le trafic OSPF sur les réseaux à accès multiple, OSPF choisit un DR et un BDR. Le DR est chargé de la mise à jour de tous les autres routeurs OSPF appelés DR other. Le BDR surveille le DR et prend sa place si ce dernier tombe en panne.

Le choix du routeur désigné se fait selon les critères suivants :

- Le routeur avec les priorités d'interface la plus élevée qui est choisi comme routeur désigné
- Si les priorités d'interface sont égales c'est le routeur dont l'Id est le plus élevé qui est choisi.

La priorité est un nombre sur 8 bits fixé par défaut à 1 sur tous les routeurs. Pour départager les routeurs ayant la même priorité, celui qui est élu a la plus grande adresse IP sur une interface de boucle locale (loopback interface) ou sur un autre type d'interface active. Afin de s'assurer que votre routeur préféré sera élu DR, il suffit de lui affecter une priorité supérieure à 1 avec la commande **ospf priority**. Vous devrez faire cela avant d'activer le processus de routage sur les routeurs car, une fois élu, le DR n'est jamais remis en cause même si un routeur avec une priorité plus grande apparaît dans la zone.

1.5 Mesure OSPF

Pour calculer un coût, l'IOS de Cisco cumule les bandes passantes des interfaces de sortie depuis le routeur vers le réseau de destination.

La formule de calcul est simplissime :

$$\text{coût} = \frac{10^8}{\text{débit de la liaison en kbps}}$$

La référence 10^8 correspond à un débit maximum de 100Mbps. Dans le cas où l'on utilise des interfaces avec un débit supérieur, il est possible de redéfinir la référence avec une commande du type **auto-cost reference-bandwidth 1000** pour la valeur 10^9 . Lorsque l'exécution de cette commande est nécessaire, il est conseillé de l'utiliser sur tous les routeurs, afin que la mesure de routage OSPF reste cohérente.

La commande bandwidth est utilisée pour modifier la valeur de la bande passante utilisée par l'IOS dans le calcul de la mesure de coût OSPF. La syntaxe de la commande d'interface est la même que celle indiquée pour le protocole EIGRP :

Router(config-if)#bandwidth bandwidth-kbps

Il existe une méthode alternative à l'utilisation de la commande bandwidth, utiliser la commande ip ospf cost, qui vous permet de spécifier directement le coût d'une interface. Par exemple, sur R1, nous pourrions configurer Serial 0/0/0 avec la commande suivante

R1(config)#interface serial 0/0/0

R1(config-if)#ip ospf cost 1562

2. Configuration du protocole OSPF

Pour activer le protocole ospf sur un routeur, on utilise la commande en mode config:

R(Config)#router ospf <process-id>

Le process-id (id de processus) est un nombre compris entre 1 et 65535 choisi par l'administrateur réseau. Le process-id n'a qu'une signification locale, ce qui veut dire qu'il n'a pas à correspondre à celui des autres routeurs OSPF pour établir des contiguïtés avec des voisins, contrairement à ce qui se passe dans le protocole EIGRP. Le numéro de système autonome ou l'ID de processus EIGRP doit correspondre pour que deux voisins EIGRP deviennent contigus.

Après avoir activé OSPF, il faut déclarer les réseaux des interfaces du routeur avec la commande :

R(Config-router)#network <network address> <wildcardmask> area <area-id>

<area-id> est la zone OSPF du routeur.

Pour vérifier le protocole OSPF on utilise les commandes :

Show ip route

Show ip ospf neighbor

Show ip protocol

Show ip ospf interface

Chapitre 11: Routage externe: BGP

I Configuration des système autonome

Un Autonomous System, abrégé en AS, ou Système Autonome, est un ensemble de réseaux informatiques IP intégrés à Internet et dont la politique de routage interne (routes à choisir en priorité, filtrage des annonces) est cohérente.

Un AS est généralement sous le contrôle d'une entité/organisation unique, typiquement un fournisseur d'accès à Internet. Au sein d'un AS, le protocole de routage est qualifié d'« interne » (par exemple, Open shortest path first, abrégé en OSPF). Entre deux systèmes autonomes, le routage est « externe » (par exemple Border Gateway Protocol, abrégé en BGP).

Chaque AS est identifié par un numéro de 16 bits (ou 32 depuis 2007, selon la [RFC 4893](#)) , appelé « Autonomous System Number » (ASN). Ce numéro est utilisé par le protocole de routage Border gateway protocol. Il est affecté par les organisations qui allouent les adresses IP, les [Registres Internet régionaux](#) (RIR). Les numéros entre 64512 et 65534 sont réservés pour un usage personnel, et ne doivent pas être utilisés pour un réseau relié à Internet.

En général, l'ASN n'apparaît pas dans les protocoles de routage internes puisque, par définition, ils sont limités à un seul AS. Cependant, certains protocoles de routage internes, tels que Enhanced Interior Gateway Routing Protocol (EIGRP), sont configurés pour n'établir d'adjacence qu'avec les routeurs qui annoncent le même système autonome.

Les ASN sont distribués de manière similaire aux adresses IP. En Europe, c'est le [RIPE-NCC](#) qui assume cette charge. Le nombre d'AS composant Internet dépassait 5000 en 1999, 30 000 fin 2008, 35 000 mi-2010¹, 36 000 début 2011².

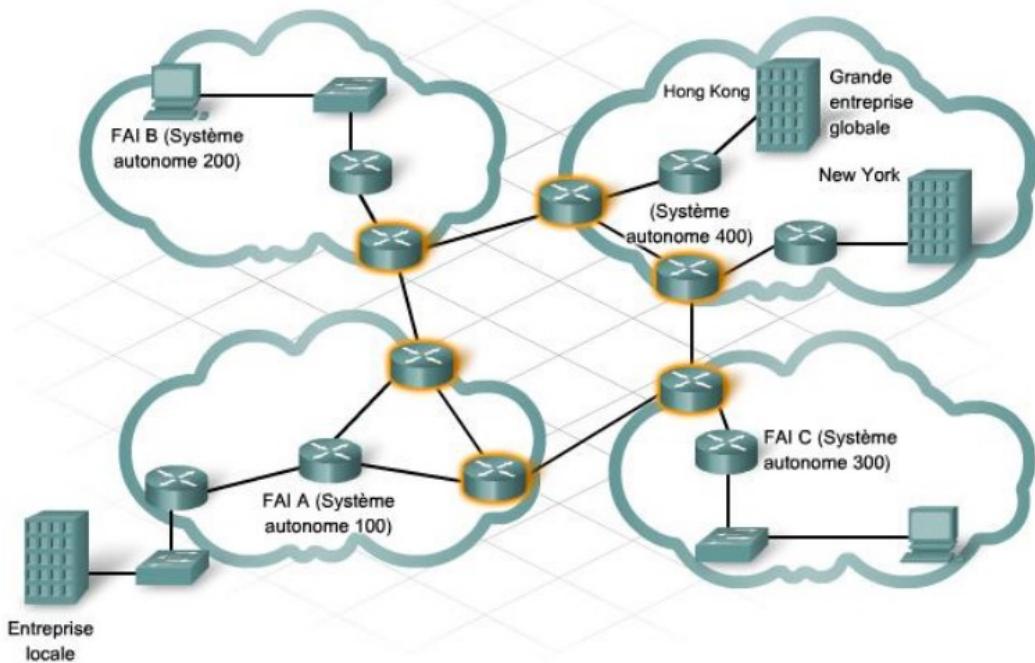
Le même numéro de système autonome s'applique à tous les périphériques réseau au sein du domaine de routage du système autonome.

Le FAI A est un système autonome dont le domaine de routage inclut une entreprise locale qui se connecte directement à ce FAI pour son accès à Internet. Cette entreprise ne possède pas son propre numéro de système autonome. Elle utilise le numéro de système autonome du FAI A (ASN 100) dans ses informations de routage.

On observe également une société de taille internationale dont le siège est basé à Hong Kong et à New-York. Étant situés dans des pays différents, les bureaux se connectent chacun à un FAI local différent pour leur accès à Internet. Cela signifie que l'entreprise est connectée à deux FAI. À quel système autonome appartient-elle et quel numéro de système autonome utilise-t-elle ?

Le fait que l'entreprise communique à la fois via le FAI B et le FAI C rend le routage confus en termes de connectivité. Le trafic provenant d'Internet ignore quel système autonome utiliser pour atteindre l'entreprise globale. Pour remédier à cette situation, l'entreprise

s'enregistre comme système autonome et se voit attribuer le numéro de système autonome 400.



II Routage entre les systèmes autonomes

Les protocoles IGP (Interior Gateway Protocols) permettent d'échanger des informations de routage au sein d'un système autonome ou d'une organisation individuelle. L'objectif d'un protocole de routage intérieur consiste à trouver le meilleur chemin possible sur le réseau interne. Les protocoles IGP sont exécutés sur les routeurs internes, c'est-à-dire les routeurs à l'intérieur d'une organisation. Les protocoles RIP, EIGRP et OSPF sont des exemples de protocoles IGP.

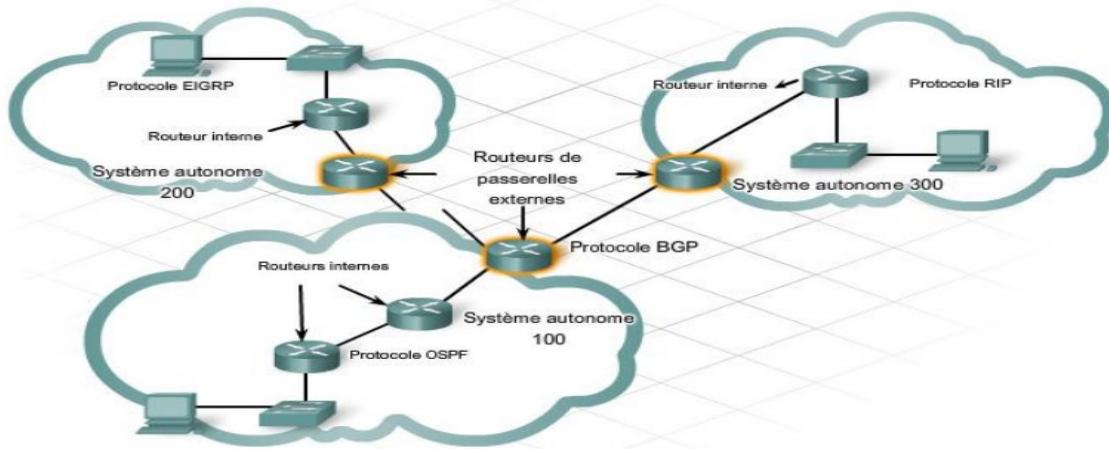
En revanche, les protocoles EGP (Exterior Gateway Protocols) sont conçus pour échanger des informations de routage entre différents systèmes autonomes. Étant donné que chaque système autonome est géré par une administration différente et qu'il peut utiliser différents protocoles intérieurs, les réseaux doivent utiliser un protocole capable de communiquer entre différents systèmes. Le protocole EGP sert de traducteur pour que les informations de routage externe soient correctement interprétées à l'intérieur de chaque réseau de système autonome.

Les protocoles EGP s'exécutent sur les routeurs externes, c'est-à-dire les routeurs qui sont situés à périphérie d'un système autonome. Les routeurs externes sont également appelés des passerelles externes.

Contrairement aux routeurs internes qui échangent des routes individuelles entre eux à l'aide de protocoles IGP, les routeurs externes échangent des informations concernant le

moyen d'atteindre différents réseaux à l'aide de protocoles extérieurs. Les protocoles de routage extérieurs cherchent à trouver le meilleur chemin via Internet sous forme de série de systèmes autonomes.

Le protocole de routage extérieur le plus courant sur Internet aujourd'hui est le protocole BGP (Border Gateway Protocol). On estime que 95 % des systèmes autonomes utilisent le protocole BGP. La version la plus courante du protocole BGP est la version 4 (BGP-4) dont la description la plus récente figure dans la spécification RFC 4271.



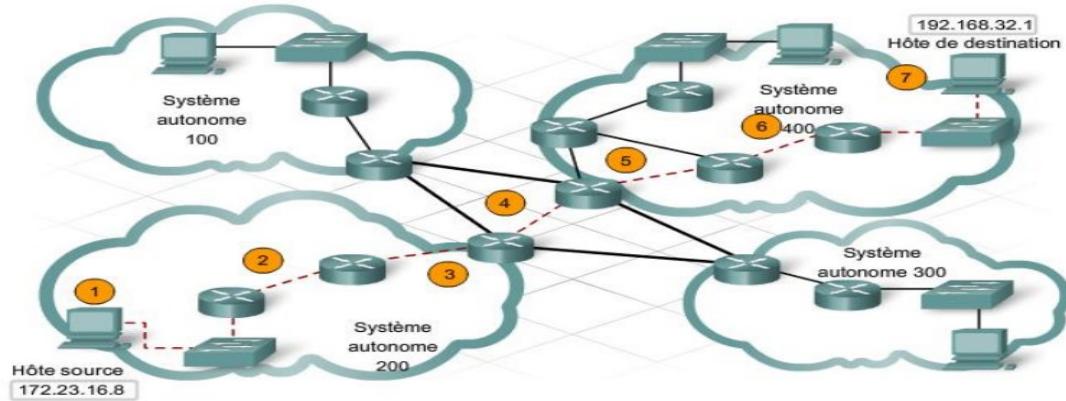
III Routage sur internet

Chaque système autonome est chargé d'informer les autres systèmes autonomes sur les réseaux qu'ils peuvent atteindre via ce système autonome. Les systèmes autonomes échangent entre eux ces informations d'accessibilité via des protocoles de routage extérieurs qui s'exécutent sur des routeurs dédiés, appelés passerelles externes.

Les paquets sont routés via Internet en plusieurs étapes :

1. L'hôte source envoie un paquet destiné à un hôte distant situé sur un autre système autonome.
2. Étant donné que l'adresse IP de destination du paquet ne désigne pas un réseau local, les routeurs internes continuent de faire transiter le paquet par leurs routes par défaut, jusqu'à ce qu'il parvienne à un routeur externe au bord du système autonome local.
3. Le routeur externe tient à jour une base de données pour tous les systèmes autonomes auxquels il est connecté. Cette base de données d'accessibilité indique au routeur que le chemin vers le réseau de destination passe par plusieurs systèmes autonomes et que le prochain saut sur le chemin transite par un routeur externe directement connecté sur un système autonome voisin.

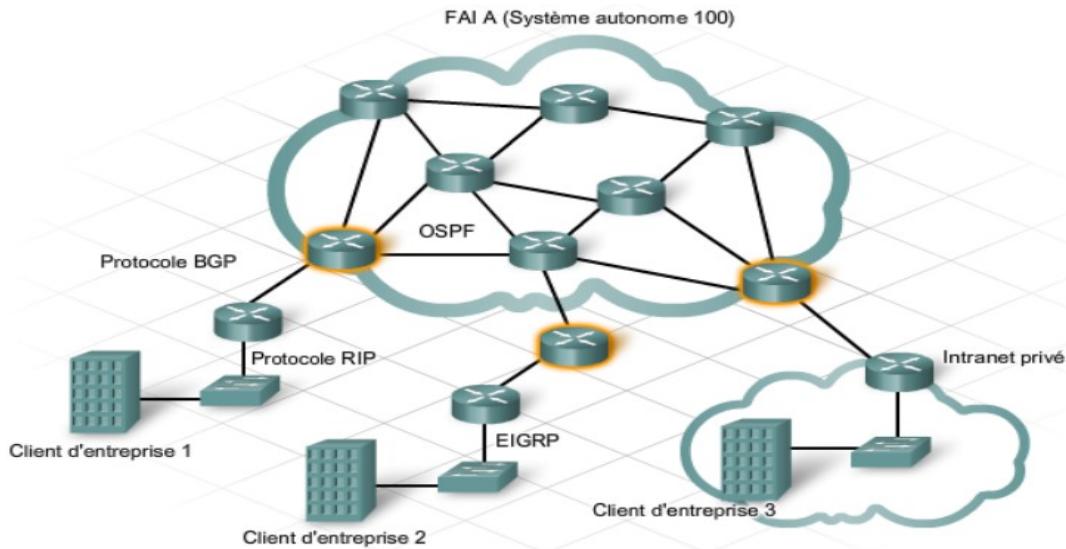
4. Le routeur externe dirige le paquet vers son prochain saut sur le chemin, qui est le routeur externe du système autonome voisin.
5. Le paquet atteint le système autonome voisin où le routeur externe vérifie sa propre base de données d'accessibilité et transfère le paquet au système autonome suivant sur le chemin.
6. Le processus est reproduit à chaque système autonome jusqu'à ce que le routeur externe, du côté du système autonome de destination, reconnaisse l'adresse IP de destination du paquet en tant que réseau interne de ce système autonome.
7. Le dernier routeur externe dirige ensuite le paquet vers le routeur interne suivant dans sa table de routage. Par la suite, le paquet est traité comme n'importe quel paquet local et dirigé par le biais de protocoles de routage internes saut après saut jusqu'à l'hôte de destination.



IV Protocoles de routage extérieurs et FAI

Les protocoles EGP (Exterior Gateway Protocol) proposent de nombreuses fonctionnalités utiles aux FAI. Ils permettent non seulement de router le trafic Internet vers des destinations distantes, mais ils fournissent en plus aux FAI le moyen de définir et d'appliquer des stratégies et des préférences locales de sorte que le flux du trafic via le FAI soit efficace et qu'aucune des routes internes ne soit surchargée par le trafic de transit.

Pour les clients professionnels, la fiabilité de leur service Internet est primordiale et les FAI doivent veiller à ce que la connexion Internet de ces clients soit toujours disponible. Ils le font en proposant des routes et des routeurs de secours en cas d'inaccessibilité des routes régulières. Dans des conditions normales, le FAI indique la route régulière aux autres systèmes autonomes. En cas d'échec de cette route régulière, le FAI envoie un message de mise à jour du protocole extérieur pour indiquer la route de secours.

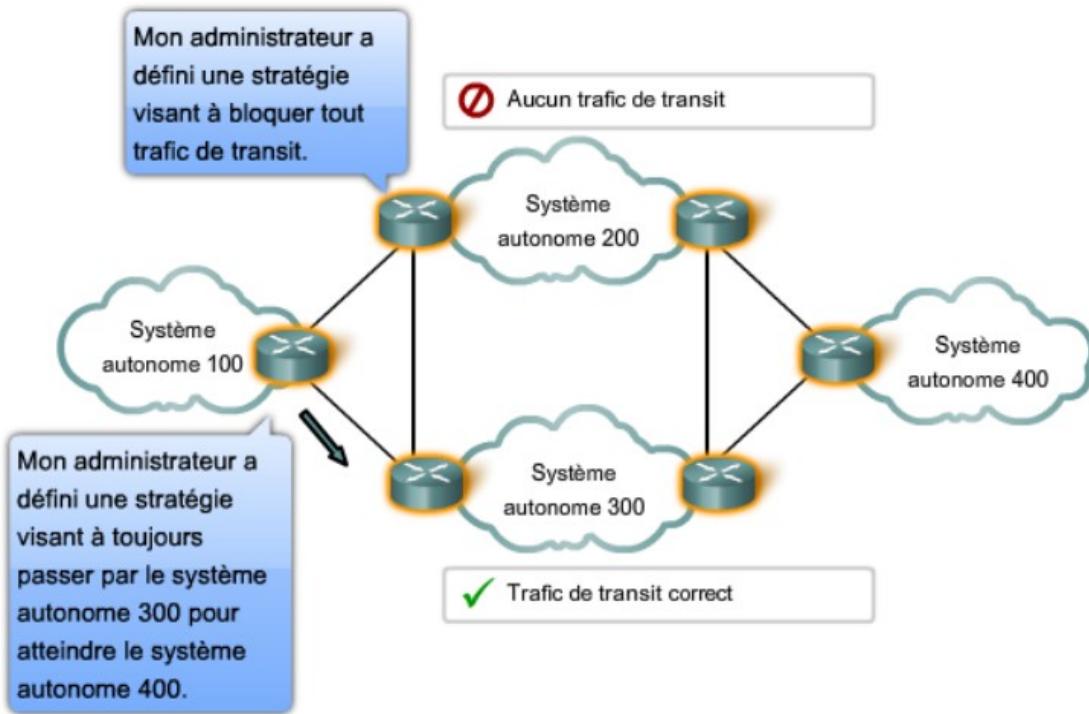


Le flux des messages sur Internet est dénommé trafic. Le trafic Internet peut être classé en deux catégories :

- Trafic local : trafic transporté à l'intérieur d'un système autonome, ayant démarré à l'intérieur de ce même système autonome ou devant être livré à l'intérieur de ce système autonome. Ce type de trafic s'apparente à la circulation locale dans une rue.
- Trafic de transit : trafic généré en dehors de ce système autonome et pouvant traverser le réseau interne du système autonome en direction de destinations extérieures au système autonome. Ce type de trafic s'apparente à la circulation de passage dans une rue.

Le flux du trafic entre systèmes autonomes est étroitement contrôlé. Il est important de pouvoir limiter, voire interdire le trafic de certains types de messages à destination ou en provenance d'un système autonome, pour des raisons de sécurité ou pour éviter les risques de surcharge.

De nombreux systèmes autonomes ne souhaitent pas assurer le trafic de transit. Le trafic de transit peut mettre les routeurs en état de surcharge et d'échec, s'ils n'ont pas la capacité de traiter de grandes quantités de trafic.



V Configuration et vérification du protocole BGP

Lorsqu'un FAI place un routeur périphérique chez un client, il le configure habituellement à l'aide d'une route statique par défaut vers le FAI. Il peut toutefois arriver qu'un FAI souhaite que le routeur soit inclus dans son système autonome et participe au protocole BGP. Le cas échéant, il est nécessaire de configurer le routeur installé sur le site du client en le dotant des commandes nécessaires à l'activation du protocole BGP.

La première étape de l'activation du protocole BGP sur un routeur consiste à configurer le numéro de système autonome. Cette opération s'effectue à l'aide de la commande suivante :

```
router bgp [numéro de système autonome]
```

L'étape suivante consiste à identifier le routeur du FAI qui est le voisin BGP avec lequel le routeur CPE (Customer Premise Equipment) échange des informations. La commande permettant d'identifier le routeur voisin est la suivante :

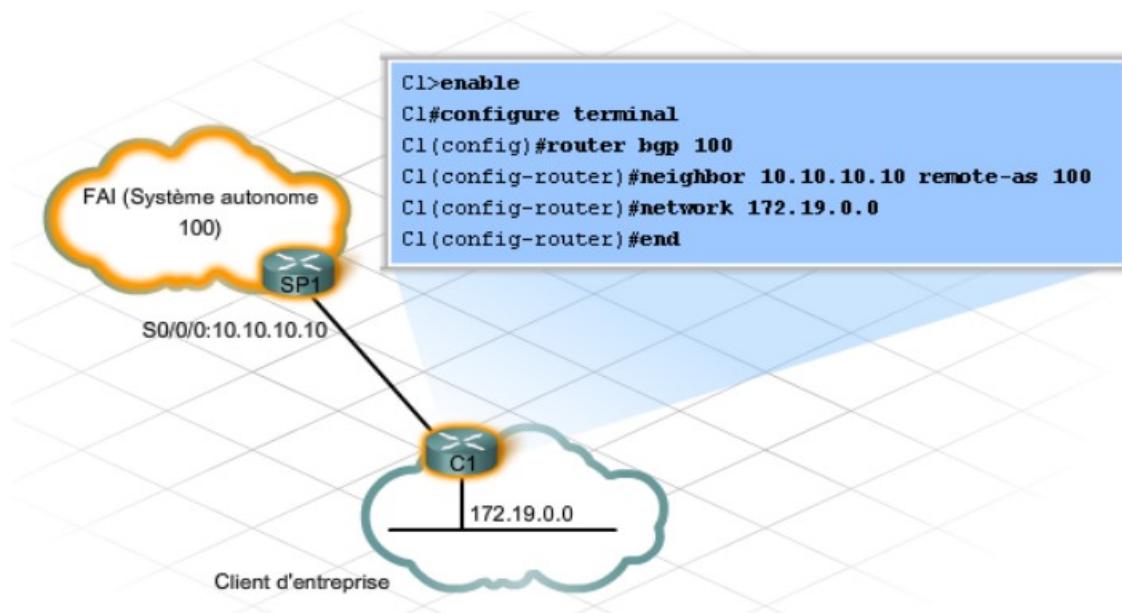
```
neighbor [adresse IP] remote-as [numéro de système autonome]
```

Lorsqu'un client de FAI possède son propre bloc d'adresses IP enregistrées, il peut souhaiter que les routes vers certains de ses réseaux internes soient connues sur Internet. Pour utiliser le protocole BGP afin d'annoncer une route interne, une commande réseau est nécessaire. Le format de la commande réseau est le suivant :

network [adresse réseau]

Une fois tout l'équipement du site client installé et les protocoles de routage configurés, le client dispose à la fois de la connectivité locale et de la connectivité Internet. Le client est maintenant capable de participer pleinement aux autres services offerts par le FAI.

Les adresses IP utilisées pour le protocole BGP sont des adresses routables normalement enregistrées qui identifient des organisations uniques. Dans les très grandes organisations, des adresses privées peuvent être utilisées dans le processus BGP, comme illustré. Sur Internet, le protocole BGP ne doit jamais être utilisé pour annoncer une adresse de réseau privé.



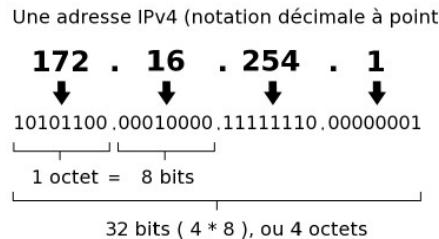
Chapitre 12 Le protocole IP V6

Introduction

Différentes versions des adresses IP

Il existe deux versions pour les adresses IP :

- **version 4** : les adresses sont codées sur **32 bits**
 - Elle est généralement notée avec quatre nombres compris entre 0 et 255, séparés par des points.



Historique

En quelques dates :

- Septembre 1981 : Internet Protocol (IP)
- Octobre 1984 : Création du concept de sous-réseau (*Internet Subnetting*)
- Septembre 1993 : Abandon de l'adressage par classes et CIDR (*Classless Inter-Domain Routing*)
- Février 1996 : Réservation d'adresses pour l'usage privé
- ~~Décembre 1998 : Spécification d'Internet Protocol Version 6 (IPv6)~~

Notation des adresses IPv6

La notation décimale pointée employée pour les adresses IPv4 (par exemple 172.31.128.1) est abandonnée au profit d'une **écriture hexadécimale**. Les groupes de 2 octets (soit 16 bits par groupe) sont séparés par un signe deux-points ' : ' :

Exemple : La notation complète comprend exactement 39 caractères :

2001:0db8:0000:85a3:0000:0000:ac1f:8001

Il est permis d'omettre de 1 à 3 chiffres zéros non significatifs dans chaque groupe de 4 chiffres hexadécimaux. Ainsi, l'adresse IPv6 ci-dessus est équivalente à :

2001:db8:0:85a3:0:0:ac1f:8001

De plus, une unique suite de un ou plusieurs groupes consécutifs de zéros nuls peut être omise, en conservant toutefois les signes deux-points :

Type d'adresses IPv6

Les bits de poids fort (à gauche) d'une adresse IPv6 détermine le type d'adresse. Ce champ de longueur variable est appelé « préfixe » ou simplement **préfixe** :

Préfixe	Description
::/8	Adresses réservées
2000::/3	Adresses unicast routables sur Internet
fc00::/7	Adresses locales uniques (utiliser fd00::/8 sur un réseau local)
fe80::/10	Adresses locales lien
ff00::/8	Adresses multicast

Décomposition

Les adresses IPv6 sur **128 bits** sont décomposées en :

- un **préfixe** de localisation public : 48 bits
- un champ **sous-réseau** de topologie locale du site (subnet) : 16 bits
- un identifiant de l'**interface** (basé sur l'adresse MAC ou aléatoire garantie l'unicité de l'adresse (équivalent à *hostid*) : 64 bits

Structure des adresses unicast globales			
champ	préfixe	sous-réseau	interface
bits	48	16	64
Structure des adresses link-local			
champ	préfixe	zéro	interface
bits	10	54	64
1111111010			
Format d'une adresse multicast			
champ	préfixe	drap.	scope
bits	8	A	A
			groupe
			111

Remarques IPv6

- Les adresses constituées entièrement de 0 ou de 1 ne jouent aucun rôle particulier en IPv6.
- Pour les cas où le ':' a un sens (par exemple dans une URL) l'adresse IPv6 entre [] pour éviter toute confusion. Exemple : [http://\[::1\]/](http://[::1]/)
- La notion historique de classes a totalement disparu, au profit de l'utilisation exclusive des préfixes et de la notation CIDR (masque / et le masque, déjà utilisés en IPv4). Les masques par défaut disparaissent aussi.
- En IPv6, les sous-réseaux ont une taille fixe de /64, c'est-à-dire que 64 des 128 bits de l'adresse IPv6 sont réservés pour les sous-réseaux.

Adresse IPv6 mappant IPv4

Une adresse IPv6 mappant une adresse IPv4 constitue un **cas spécial** d'adresse IPv6. Elles sont utilisées par la pile IP pour représenter des adresses IPv4 dans des applications IPv6 (mais ne doivent pas être envoyées dans le réseau). Une telle adresse IPv6 a une notation ::ffff:0000:0000:0000::ffff:0000:0000. Elle est constituée de la manière suivante :

- les premiers 80 bits fixés à zéro,
- les 16 suivants à un et
- **les 32 bits restants représentent une adresse IPv4.**

Remarque : Exception spéciale à la notation des adresses IPv6, correspondant à des adresses IPv4 qui sont communément représentées avec des masques de sous-réseau comme 255.255.255.0 ou 255.255.255.252.

Adresses obsolètes

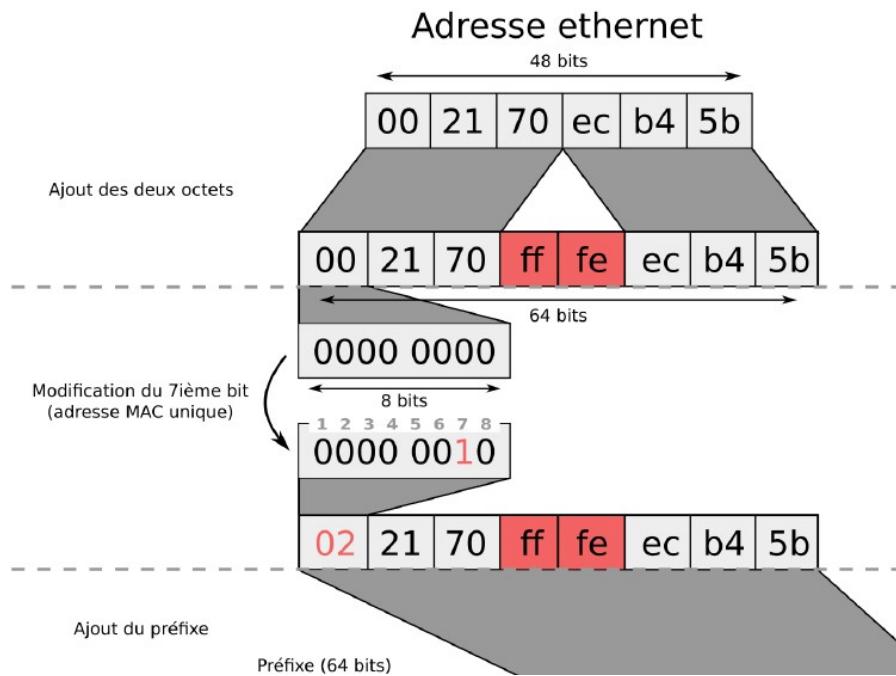
Adresses IPv6 obsolètes

Préfixe	Description
3ffe::/16 5f00::/8	Adresses utilisées par le réseau expérimental
fec0::/10	Adresse locale de site
::a.b.c.d/96	Adresse compatible IPv4 (a.b.c.d est une adresse IPv4)

Autoconfiguration basée sur l'adresse MAC I

La construction automatique de l'adresse IP basée sur l'adresse MAC suit le principe suivant :

- Ajouter les octets **ffff** au milieu de l'adresse MAC de l'appareil.
- Positionner le septième bit (U/L) de l'adresse MAC moins partant de la gauche à 1 si l'adresse est unique (ce qui est le cas pour toutes les adresses MAC par défaut) sinon 0.
- Récupération du préfixe si c'est une adresse globale, sinon



Chapitre 13 Translation d'adresse

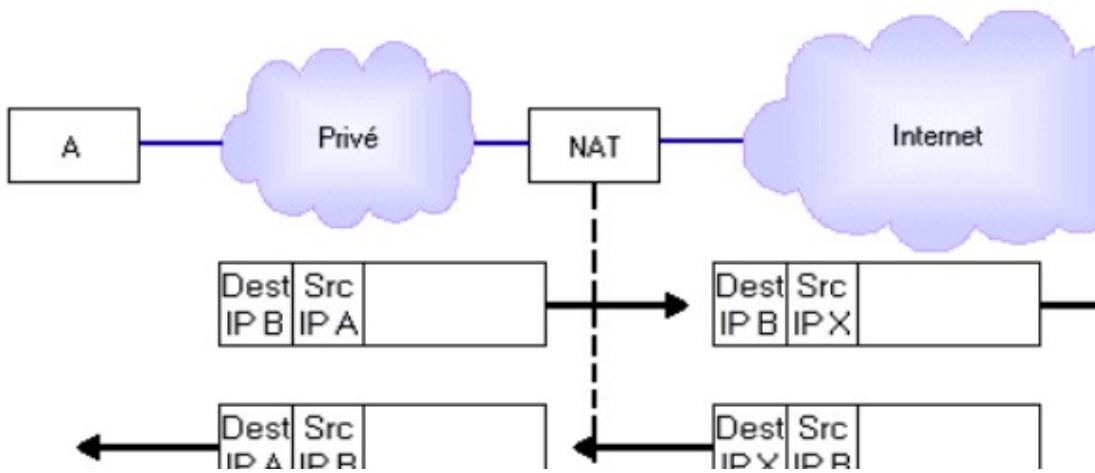
1. Qu'est-ce que le NAT ?

La technique de translation d'adresses (NAT en anglais, [RFC 3022](#)) est une pratique courante qui est apparue à l'origine pour pallier au manque croissant d'adresses IPv4 libres. En effet, ces adresses sont codées sur 4 octets et sont du type 0.0.0.0 à 255.255.255.255 (certaines valeurs étant réservées et par conséquence inutilisables) ; il y a donc peu d'adresses disponibles en comparaison du nombre croissant de machines sur Internet. Il fut donc décidé de réserver des intervalles d'adresses à des usages privés uniquement ([RFC 1918](#)). Ce sont les adresses :

10.0.0.0 - 10.255.255.255 (10/8 prefix)
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

En conséquence, ces adresses ne sont pas routables sur Internet et ne doivent pas être utilisées par des machines de ce réseau. Par contre, tous les réseaux privés peuvent utiliser ces adresses sans restriction.

Comme ces adresses ne sont pas routables sur le réseau public, la translation d'adresse est utilisée pour permettre aux machines du réseau privé d'accéder à Internet, et de façon générale à d'autres réseaux. Le principe de base est simple puisqu'il s'agit de remplacer à la volée les champs d'adresses dans les paquets qui sont destinés à un autre réseau (ce qui implique que le NAT soit effectué entre les 2 interfaces réseau, entre le réseau privé et les autres).



Comme le montre le schéma, le NAT va effectuer le remplacement de l'IP source de A par son IP X puis il va router le paquet vers le réseau extérieur. La réponse lui parviendra, et

suivant la technique utilisée que nous allons détailler plus loin, il va cette fois-ci modifier l'adresse de destination X pour celle de A sur son réseau privé.

2. Techniques de translation

Il existe plusieurs variantes de NAT suivant la topologie du réseau privé, le nombre de machines privées, le nombre d'adresses IP publiques et les besoins en termes de services, d'accessibilité et de visibilité de l'extérieur.

- Le NAT de base est statique et attribue de façon automatique une adresse IP à une autre. Aucune information liée à la connexion n'est nécessaire, il suffit de modifier le paquet suivant la règle prédefinie de translation. L'idéal dans ce cas-ci est d'avoir le même nombre d'IP extérieures que d'IP privées.
- Le NAT dynamique ne considère aucune association prédefinie entre l'IP publique et l'IP privée de la requête qu'il reçoit. Il peut d'ailleurs y avoir plusieurs IP extérieures tout comme il y a plusieurs IP privées. Cela entraîne nécessairement un suivi de la connexion car le NAT attribue l'IP extérieure lors de la requête initiale qui provient de son réseau privé; il doit ensuite pouvoir discriminer les paquets entrants de façon à pouvoir leur attribuer à chacun l'IP correspondante sur le réseau privé (celle de la connexion). Le but étant de rester transparent vis-à-vis de l'ordinateur source ou distant; un problème se pose si l'on ne dispose pas du même nombre d'adresses IP externes que d'adresses privées, car si toutes les adresses externes sont déjà en cours d'utilisation, aucune machine supplémentaire ne pourra accéder au réseau extérieur.
- Le NAPT MASQ (Network Address and Port Translation) permet de résoudre le problème cité précédemment et s'avère donc particulièrement utile si le nombre d'adresses externes est limité; c'est le cas typique d'une connexion Internet simple où plusieurs machines vont devoir partager la même adresse IP publique (externe). Le problème technique derrière cette méthode est bien de savoir à quelle machine privée les paquets entrants sont destinés, puisqu'ils ont tous -à priori- la même adresse IP de destination (celle de la passerelle). Pour permettre leur différenciation, le NAT va devoir conserver une trace plus complète des paramètres de chaque connexion de façon établir un véritable contexte pour chacune de ces dernières. Parmi ces critères de séparation, citons :
 - **l'adresse source** est le premier élément qui est regardé; chaque machine du réseau privé aura tendance dans la majorité des cas à communiquer avec une machine extérieure différente. Donc les paquets entrants seront porteurs de cette information et permettront au NAT d'identifier la machine à l'origine de chaque échange. Mais cela ne fonctionnera pas si les machines extérieures ne sont pas toutes différentes.
 - **le protocole supérieur** peut également être regardé par le NAT pour pouvoir identifier le contexte. Ce sera par exemple de l'UDP ou du TCP, et si une machine utilise le premier et une autre utilise TCP, alors le NAT saura retrouver la machine initiale de la connexion.
 - **le port** et d'autres informations liées aux protocoles supérieurs peuvent être utilisés pour identifier chaque contexte. Ainsi le NAT pourra faire la différence entre des paquets entrants qui présentent la même IP source, le même protocole de transport mais un port de destination différent.

Il reste un dernier cas dans lequel tout cela ne suffira pas, c'est celui où les 2 contextes basés sur ces informations sont identiques, c'est-à-dire quand les paquets entrants présentent la même IP source, le même protocole de transport et le même port de destination. Dans ce cas-là, le NAT effectue une translation de port en même temps que d'adresse pour pouvoir identifier les flux de façon certaine. Cela consiste à modifier les paramètres de connexion avec la machine distante de façon à utiliser le port voulu sur la passerelle où se situe le NAT. Cette opération reste transparente pour la machine locale (privée) puisque cela est effectué au niveau du NAT qui rétablit ensuite les paramètres initiaux pour cette machine.

Comme il existe 65535 ports disponibles (moins les 1024 réservés), cela laisse une grande marge de sécurité. La dénomination MASQ provient du fait que cette opération est comparable à une attaque du type [man-in-the-middle](#) sauf qu'elle ne vise pas à obtenir quelqu'information que ce soit (la législation à ce niveau est stricte, voir les recommandations de la [CNIL](#)).

- Le NAPT Redirect/Port Forwarding est identique au précédent sauf qu'il présente des services additionnels de redirection des flux entrants ou sortants. Ainsi, le Port Forwarding permet à l'extérieur d'accéder à un service (serveur WEB ou autre) qui est en fait basé sur une machine de réseau privé : la machine distante pense communiquer avec la machine hébergeant le NAT alors qu'en fait celui-ci redirige le flux vers la machine correspondant réellement à ce service. Le Redirect permet quant à lui de rediriger les flux sortants vers des services particuliers comme des proxies, firewalls, etc...
- Le Bi-directional NAT diffère des précédents puisqu'il permet à des machines distantes d'accéder à des machines du réseau privé, et ce directement contrairement au Port forwarding. Le principe fait appel au service DNS pour interpréter les requêtes; celles-ci sont initiées par la machine distante et reçues par le NAT. La passerelle répond par sa propre adresse IP tout en gardant en mémoire l'association entre l'IP distante et l'IP requise pour le service. Ainsi, les paquets provenant de la machine distante seront transférés vers la machine correspondante. Le problème de cette technique est l'utilisation du service DNS qui peut être coûteux dans le cas d'un utilisateur de base accédant au réseau public Internet. Par contre, cette solution pourra se révéler utile dans le cas d'une entreprise interconnectant plusieurs réseaux privés car les serveurs DNS sont alors mieux maîtrisés.
- Le Twice-NAT est, comme son nom l'indique, une technique de double translation d'adresses et de ports. A la fois les paramètres de destination et ceux de la source seront modifiés. Concrètement, on peut dire que le NAT cache les adresses internes vis-à-vis de l'extérieur ainsi que les adresses externes vis-à-vis du réseau privé. L'utilité de cette technique apparaît quand plusieurs réseaux privés sont interconnectés : comme nous l'avons expliqué précédemment, les machines doivent utiliser des plages d'adressage bien précises ce qui peut créer des conflits et des collisions entre plusieurs réseaux privés (c'est-à-dire plusieurs machines utilisant la même adresse IP privée). Le Twice-NAT permet de résoudre ces problèmes de collisions en modifiant les 2 adresses du paquet.
- Le NAT avec Serveurs Virtuels/Load Balancing est une évolution des techniques de NAT qui permet d'optimiser leurs implémentations. L'utilisation de serveurs virtuels est actuellement très répandue; cela correspond à une machine inexistante représentée

uniquement par son adresse IP et prise en charge par une ou plusieurs machines réelles qui ont également leurs propres adresses (différentes). Ainsi, les requêtes des machines distantes sont adressées à une ou plusieurs adresses virtuelles correspondant à la passerelle où est implanté le démon effectuant le NAT. Celui-ci remplace alors l'adresse virtuelle par une des adresses réelles appartenant aux machines implémentant le service NAT, puis leur transmet la requête et la connexion associée.

La sélection de l'adresse réelle peut se faire sur la base de la charge de travail de la machine correspondante: si le serveur NAT est surchargé, on choisira un autre serveur NAT moins chargé. Cette technique est à la base du load balancing et il existe de nombreux algorithmes de sélection et de répartition de la charge.

Enfin, comme le service NAT est habituellement placé sur la machine chargée du routage, une évolution possible est l'utilisation de routes virtuelles tout comme nous avons vu les adresses virtuelles. Dans ce dernier cas, la passerelle possède plusieurs interfaces vers le réseau externe et peut choisir laquelle utiliser en fonction de la charge de trafic sur chaque brin

3. Avantages et inconvénients

N'oublions pas que l'utilité principale du NAT est d'économiser les adresses IP nécessaires pour connecter un réseau à Internet par exemple. Cela s'avère particulièrement utile pour tout particulier possédant une connexion Internet simple (modem, ADSL, cable) avec allocation d'une adresse dynamique. Si ce particulier possède plusieurs machines sur son réseau privé, il pourra utiliser la fonctionnalité de NAT pour partager l'adresse IP de sa machine principale. D'autre part, les fonctionnalités avancées du NAT permettent d'interconnecter plusieurs réseaux privés de façon transparente même s'il existe des conflits d'adressage entre eux.

Par contre, dans la majorité des techniques citées précédemment, la connexion est nécessairement initiée à partir d'une machine locale. Les machines externes ne verront que l'adresse de la passerelle et ne pourront pas se connecter directement aux machines locales; cela est bien sûr résolu avec les techniques plus évoluées de translation, mais celles-ci restent couteuses et peu accessibles.

Enfin, l'opération même de translation peut poser certains nombres de problèmes que nous allons aborder dans le paragraphe suivant.

4. Sécurité et NAT

Le NAT présente à la fois des inconvénients et des avantages au niveau de la sécurité pour les machines du réseau privé.

Tout d'abord, comme nous l'avons vu précédemment, le NAT n'est pas une opération anodine et ce bien qu'il ait pour vocation d'être transparent. En effet, le NAT modifie les paquets IP et cela a pour conséquence directe de **casser tout contrôle d'intégrité** au niveau IP et même aux niveaux supérieurs puisque TCP par exemple inclut les adresses dans ses checksums!

Concrètement, on se rend compte qu'un protocole de sécurisation des datagrammes comme **IPSec est totalement incompatible avec le NAT**, que ce soit en mode tunneling ou transport (voir fiche IPSec).

Une autre raison simple est qu'un NAT évolué a tendance à remonter les couches pour étudier les protocoles de transport afin de rassembler assez d'informations pour chaque contexte. Tout chiffrement à ce niveau empêcherait donc le NAT de fonctionner, puisque les informations seraient alors cryptées.

Un des avantages du NAT est de protéger les machines du réseau privé d'attaques directes puiqu'elles ne sont en fait pas accessibles de l'extérieur. De plus dans la majorité des cas, les requêtes de connexion ne peuvent provenir que de ces machines privées. Cela permet également de se prémunir contre un monitoring du traffic qui viserait à scruter les communications entre 2 machines particulières, un serveur sur Internet par exemple et une machine du réseau privé. Comme cette dernière n'est plus identifiable, l'opération devient impossible à moins de remonter au niveau applicatif (d'où l'utilité d'utiliser une protection/chiffrement à ce niveau également).

5. Conclusion

Le NAT est aujourd'hui incontournable dans la plupart des topologies réseau, à partir du moment où l'on souhaite connecter le réseau à d'autres. Comme nous l'avons vu, les techniques correspondant au service NAT ont évolué pour répondre aux besoins croissants de transparence, connectivité, disponibilité, etc... Quoiqu'il en soit, l'utilisation d'une telle technique ne doit pas être prise à la légère car elle implique autant d'inconvénients que d'avantages. Enfin, on peut s'interroger sur la pérennité du NAT sachant que cette technique n'était à l'origine destinée qu'à palier les lacunes d'IPv4. Or, il y a fort à parier qu'elle sera toujours effective avec les nouvelles adresses IPv6, autant à cause de ses qualités de sécurisation que du fait de la lenteur prévisible de la migration des terminaux d'un système d'adressage à l'autre.