OFPPT

ISTA HAY HASSANI

CISCO

CCNA 4

WAN Technologies

Résumé

Réalisé par : **BOUTAHIR Mounir**

Keep Connection to Share Information ★ NAMIRO ★ Keep Connection to Share Information

SOMMAIRE

Module 1

Evolutivité des adresses IP

Evolutivité des réseaux avec NAT & PAT :

Adresses privées :

La ***RFC 1918*** réserve les trois blocs d'adresses IP privées ci-dessous :

Classe	Plage d'adresses internes RFC 1918	Préfixe CIDR
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

- 1 adresse de classe A
- 16 adresses de classe B
- 256 adresses de classe C

Ces adresses sont exclusivement *destinées aux réseaux internes privés*. Les paquets qui les contiennent *ne sont pas routés sur Internet*.

Les adresses Internet publiques doivent être enregistrées par une société faisant autorité sur Internet, par exemple l'ARIN (*American Registry for Internet Numbers*) ou le RIPE (*Réseaux IP Européens*).

Généralement, les FAI configurent généralement les routeurs périphériques de façon à empêcher le transfert du trafic privé.

Avec NAT, les sociétés individuelles peuvent attribuer des adresses privées à certains ou tous leurs hôtes, et utiliser NAT pour leur procurer un accès à Internet.

Présentation des fonctions NAT et PAT

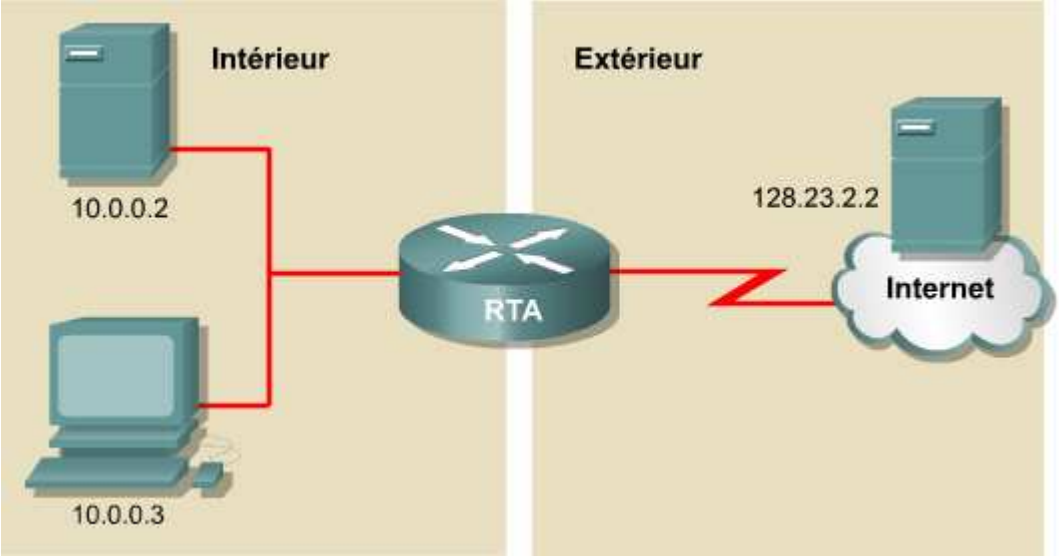
NAT est conçu pour conserver des adresses IP et permettre aux réseaux d'utiliser des adresses IP privées sur les réseaux internes. Ces adresses internes privées sont traduites en adresses publiques routables.

Un matériel compatible NAT fonctionne généralement à la périphérie d'un réseau d'extrémité. *Quand un hôte situé à l'intérieur du réseau d'extrémité souhaite émettre vers un hôte de l'extérieur*, il transfère le paquet au routeur périphérique frontière. Ce routeur périphérique frontière effectue le processus NAT et traduit l'adresse privée interne d'un hôte en une adresse publique externe routable.

Les termes ci-dessous, liés à NAT, ont été définis par Cisco :

- ***Adresse locale interne*** – L'adresse IP attribuée à un hôte du réseau interne. Il s'agit généralement d'une adresse privée RFC 1918.

- ***Adresse globale interne*** – Une adresse IP légitime attribuée par InterNIC ou par le fournisseur d'accès, et qui représente une ou plusieurs adresses IP locales internes pour le monde extérieur.
- ***Adresse locale externe*** – L'adresse IP d'un hôte externe telle que la connaissent les hôtes du réseau interne.
- ***Adresse globale externe*** – L'adresse IP attribuée à un hôte du réseau externe. C'est le propriétaire de l'hôte qui attribue cette adresse.



Un hôte interne (10.0.0.3) veut communiquer avec un hôte externe (128.23.2.2). L'hôte interne envoie un paquet à la passerelle, RTA.

RTA détermine que le paquet doit être routé en externe, vers Internet. Le processus NAT choisit une adresse IP globalement unique (179.9.8.80) et remplace l'adresse locale du champ source du paquet par l'adresse globale. Il stocke ce mappage de l'adresse locale sur l'adresse globale dans la table NAT.

Le paquet est routé vers sa destination. Dans cet environnement client-serveur, le serveur peut répondre par un paquet, qui revient à RTA, adressé à l'adresse globale 179.9.8.80.

Le processus NAT détermine qu'un paquet est routé de l'extérieur vers l'intérieur et consulte la table NAT pour y trouver le mappage de cette adresse globale en une adresse locale. S'il trouve un mappage, l'adresse globale du champ de destination du paquet est remplacée par l'adresse locale et le paquet est transféré en interne.

Principales fonctionnalités NAT et PAT

Les traductions NAT peuvent avoir de nombreuses utilisations et peuvent indifféremment être attribuées de façon statique ou dynamique.

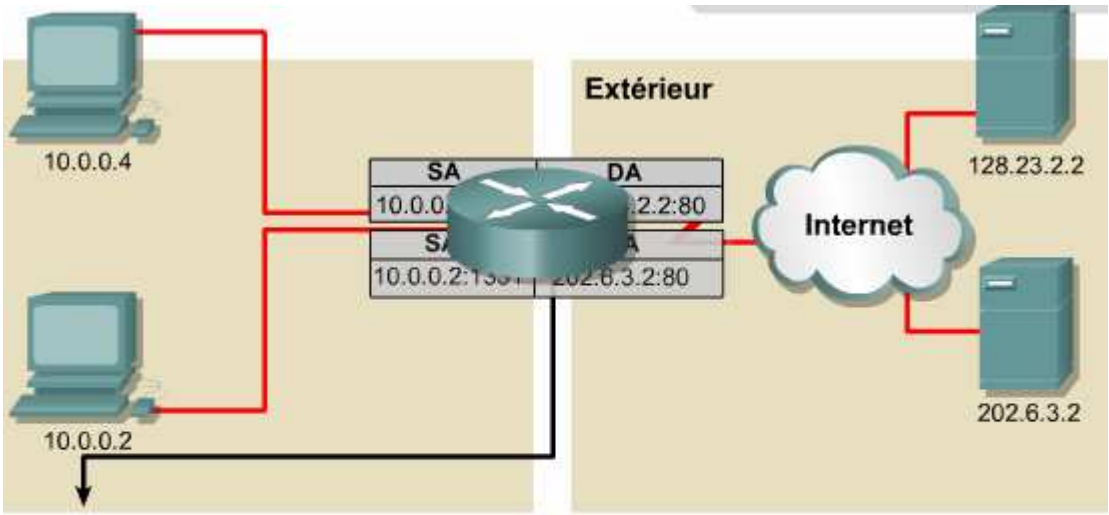


Table NAT avec surcharge

Adresse IP locale interne	Adresse IP globale interne	Adresse IP locale externe	Adresse globale externe
10.0.0.2:1331	179.9.8.80:1331	202.6.3.2:80	202.6.3.2:80
10.0.0.4:1555	179.9.8.80:1555	128.23.2.2:80	128.23.2.2:80

La fonction ***NAT statique*** est conçue pour permettre le mappage bi-univoque d'adresses locales et globales. Ceci s'avère particulièrement utile pour les hôtes qui doivent disposer d'une adresse permanente, accessible depuis Internet. Ces hôtes internes peuvent être des serveurs d'entreprise ou des équipements de réseau.

La fonction ***NAT dynamique*** est conçue pour mapper une adresse IP privée sur une adresse publique. Une adresse IP quelconque prise dans un groupe d'adresses IP publiques est attribuée à un hôte du réseau.

Avec la traduction d'adresses de ports (*Port Address Translation* - **PAT**), plusieurs adresses IP privées peuvent être mappées sur une adresse IP publique unique.

La fonction PAT utilise des numéros de port source uniques sur l'adresse IP globale interne, de façon à assurer une distinction entre les traductions.

Le *numéro de port* est encodé sur 16 bits. Le nombre total d'adresses internes pouvant être traduites en une adresse externe peut théoriquement atteindre les 65 536 par adresse IP.

De façon plus réaliste, le nombre de port pouvant être attribués à une adresse IP unique avoisine les 4000.

→ La fonction PAT tente de conserver le port source d'origine. Si ce port source est déjà utilisé, PAT attribue le premier numéro de port disponible en commençant au début du groupe de ports approprié.

→ Quand il n'y a plus de ports disponibles et que plusieurs adresses IP externes sont configurées, PAT sélectionne l'adresse IP suivante pour tenter d'allouer de nouveau le numéro du port source initial.

Avantages de NAT :

- Elle économise du temps et de l'argent. Elle élimine le besoin de réattribuer une nouvelle adresse IP à chaque hôte lors du passage à un nouveau FAI.
- Elle économise les adresses au moyen d'un multiplexage au niveau du port de l'application.
- Elle protège le réseau. En effet, comme les réseaux privés ne divulguent pas leurs adresses ou leur topologie interne, ils restent raisonnablement sécurisés.

Configuration des fonctions NAT et PAT

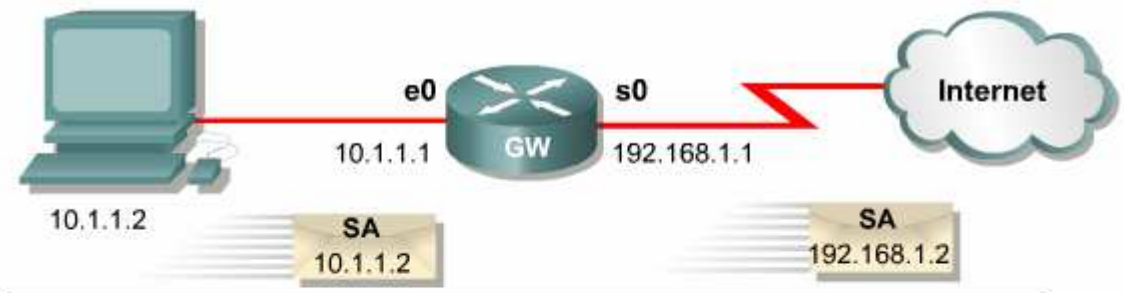
Traduction statique :

1 → Etablir le mappage statique :

Router(config)#**ip nat inside source static {@ IP locale} {@ IP globale}**

2 → Définir les interfaces :

Router(config-if)#**ip nat inside** → l'interface connectée à l'intérieur
Router(config-if)#**ip nat outside** → l'interface connectée à l'extérieur




```
hostname GW
!
ip nat inside source static 10.1.1.2 192.168.1.2
!
interface ethernet 0
  ip address 10.1.1.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
```

Traduction dynamique :

1 → Définir une liste d'@IP globales à allouer :

Router(config)#**ip nat pool {nom_pool} {@ IP début} {@ IP fin} netmask {masque de SR}**

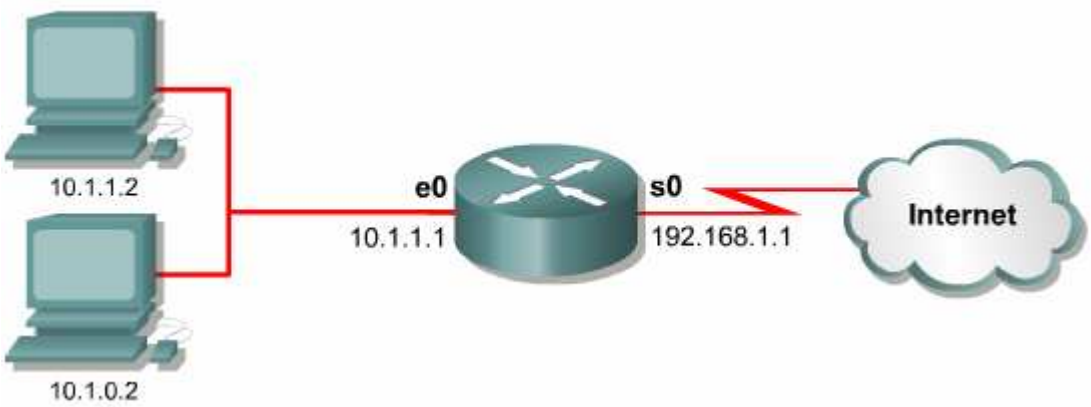
2 → Définir une ACL standard autorisant les @ qui doivent être traduites.

3- Etablir la traduction dynamique

Router(config)#**ip nat inside source list {n° ACL} pool {nom_pool}**

4 → Définir les interfaces :

Router(config-if)#**ip nat inside** → l'interface connectée à l'intérieur
Router(config-if)#**ip nat outside** → l'interface connectée à l'extérieur




```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface ethernet 0
  ip address 10.1.1.1 255.255.0.0
  ip nat inside
!
interface serial 0
  ip address 192.168.1.1 255.255.255.0
  ip nat outside
!
access-list 1 permit 10.1.0.0 0.0.0.255
```

Remarque : Cisco recommande de ne pas configurer les listes d'accès référencées par des commandes NAT à l'aide de la commande **permit any**. En effet, **permit any** peut mener la fonction NAT à consommer trop de ressources routeur, ce qui peut occasionner des problèmes

Surcharge :

Il existe deux façons de configurer la surcharge, en fonction de la manière dont les adresses IP publiques ont été allouées.

1 → Un FAI ne peut allouer qu'une adresse IP publique à un réseau.

→ Définir une ACL standard autorisant les @ qui doivent être traduites.

→ Spécifier l'@ globale, en tant que groupe à utiliser par la surcharge :

Router(config)#**ip nat pool {nom_pool} {@ IP début} {@ IP fin} netmask {masque de SR}**

→ Etablir la traduction dynamique :

Router(config)#**ip nat inside source list {n° ACL} interface {interface} overload**

4 → Définir les interfaces :

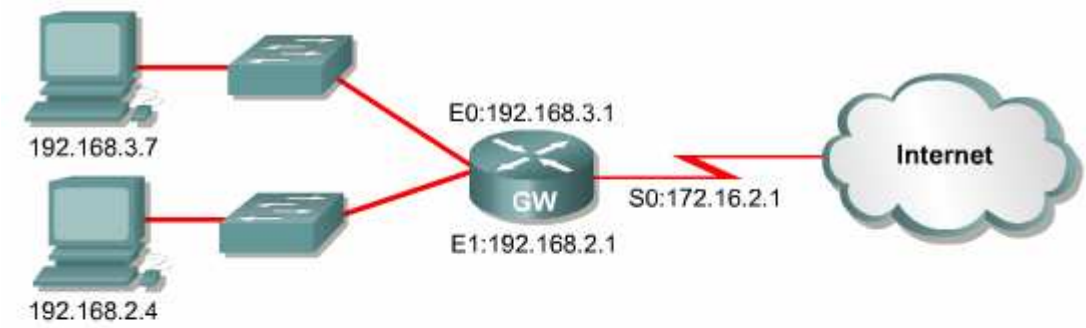
Router(config-if)#**ip nat inside** → l'interface connectée à l'intérieur
Router(config-if)#**ip nat outside** → l'interface connectée à l'extérieur

2 → Si le FAI a fourni une ou plusieurs adresses IP publiques à titre de groupe NAT.

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255

Router(config)#ip nat pool nat-pool2 179.9.8.20 netmask
255.255.255.240

Router(config)#ip nat inside source list 1 pool nat-pool2
overload
```




```
interface ethernet 0
  ip address 192.168.3.1 255.255.255.0
  ip nat inside
!
interface ethernet 1
  ip address 192.168.2.1 255.255.255.0
  ip nat inside
!
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
!
ip nat inside source list 1 interface serial 0 overload
!
access-list 1 permit 192.168.2.0 0.0.0.255
access-list 1 permit 192.168.3.0 0.0.0.255
```

Vérification de la configuration PAT

Par défaut, les traductions d'adresse dynamiques deviennent inactives dans la table de traduction NAT au terme d'une période de non-utilisation de 24 heures, sauf si les temporisations ont été reconfigurées par la commande

Router(config)#**ip nat translation timeout {timeout_seconds}**

Commande	Description
clear ip nat translation *	Efface toutes les entrées de traduction dynamique d'adresses de la table de traduction NAT
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Efface une entrée de traduction dynamique simple contenant une traduction interne ou une traduction à la fois interne et externe
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Efface une entrée étendue de traduction dynamique

```
Router#show ip nat translations [verbose]
```

* verbose (facultatif) Affiche des informations complémentaires pour chaque entrée de la table de traduction, notamment le temps écoulé depuis la création et l'utilisation de l'entrée

```
Router#show ip nat translations
Pro Inside global     Inside local       Outside local      Outside global
172.16.131.1          10.10.10.1               ---                ---
```

```
Router#show ip nat statistics
```

• Affiche les statistiques de traduction

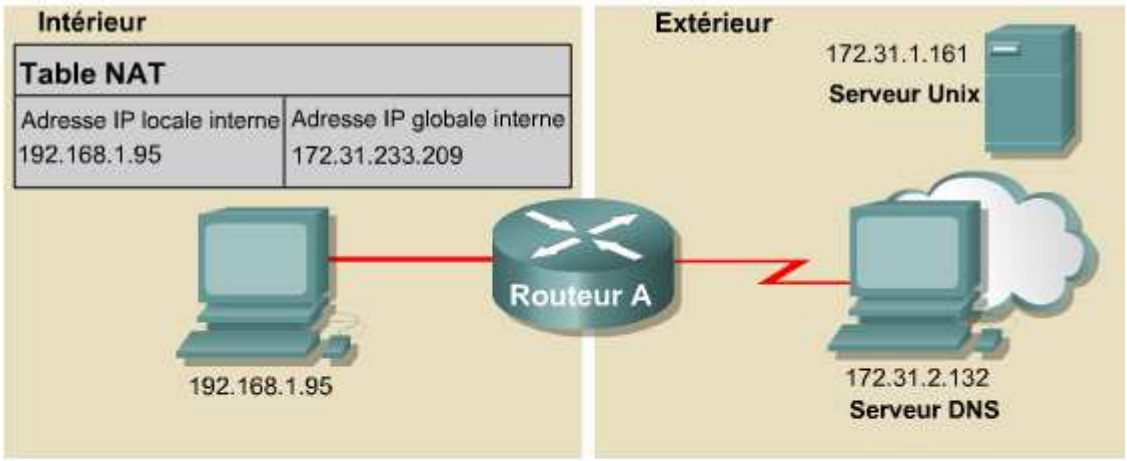
```
Router#show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0
Inside interfaces:
Ethernet0, Ethernet1
Hits: 5 Misses:0
```

Dépannage de la configuration des fonctions NAT et PAT

Procédez comme suit pour déterminer si NAT fonctionne correctement:

1. Définissez clairement ce que la fonction NAT est censée faire.
2. Vérifier que les traductions appropriées sont présentes dans la table de traduction.
3. Assurez-vous que la traduction s'effectue en exécutant les commandes **show** et **debug**.
4. Vérifiez de façon détaillée ce qui arrive au paquet et assurez-vous que les routeurs disposent des informations correctes pour l'acheminer.

Debug ip nat → afficher des informations sur chacun des paquets traduits par le Routeur
Debug ip nat detailed → générer une description individuelle les paquets + erreurs …




```
RouteurA#debug ip nat
NAT:   s= 192.168.1.95   ->172.31.233.209,        d=172.31.2.132 [6825]
NAT:   s= 172.31.2.132,    d=172.31.233.209,    ->192.168.1.95 [21852]
NAT:   s= 192.168.1.95   ->172.31.233.209,        d=172.31.1.161 [6826]
NAT*:  s= 172.31.1.161,    d=172.31.233.209,    ->192.168.1.95 [23311]
NAT*:  s= 192.168.1.95   ->172.31.233.209,        d=172.31.1.161 [6827]
NAT*:  s= 192.168.1.95   ->172.31.233.209,        d=172.31.1.161 [6828]
NAT*:  s= 172.31.1.161     d=172.31.233.209,    ->192.168.1.95 [23313]
NAT*:  s= 172.31.1.161,    d=172.31.233.209,    ->192.168.1.95 [23313]
```

Décodez les résultats à l'aide des points clés suivants :

- **L'astérisque** indique que la traduction s'effectue sur le chemin à commutation rapide (mémoire cache)
- **s** = a.b.c.d est l'adresse source.
- → L'adresse source a.b.c.d est traduite en w.x.y.z.
- **d** = e.f.g.h est l'adresse de destination.
- **La valeur entre parenthèses** représente le numéro d'identification IP.

Problèmes liés à la fonction NAT

La fonction NAT offre plusieurs ***avantages***, notamment :

- Elle ménage le système d'adressage enregistré légalement en autorisant la privatisation des intranets.
- Elle augmente la souplesse des connexions vers le réseau public.

Toutefois, NAT présente certains ***inconvénients***.

- Une perte de fonctionnalité, en particulier avec les protocoles ou les applications qui impliquent l'envoi d'adresses IP à l'intérieur des données utiles du paquet IP.
- NAT augmente les délais. Des délais de commutation de chemin sont introduits par la traduction de chaque adresse IP à l'intérieur des en-têtes de paquet.
- Le processeur examine chaque paquet pour déterminer s'il doit être ou non traduit.
- La perte de traçabilité IP de bout en bout. Il devient bien plus difficile de suivre les paquets qui subissent de nombreux changements d'adresse sur plusieurs sauts NAT.

Cisco IOS NAT prend en charge les types de trafic ci-dessous, bien qu'ils transportent les adresses IP dans le flux de données de l'application :

- ICMP
- Le protocole FTP (File Transfer Protocol), et notamment les commandes PORT et PASV
- Les services NetBIOS sur TCP/IP, de datagramme, de nom et de session
- Real Audio de Progressive Networks
- CUSeeMe de White Pines
- Les requêtes DNS " A " et " PTR "
- H.323/NetMeeting, versions 12.0(1)/12.0(1)T et ultérieures
- VDOLive, versions 11.3(4)/11.3(4)T et ultérieures
- Vxtreme, versions 11.3(4)/11.3(4)T et ultérieures
- IP Multicast, version 12.0(1)T, traduction d'adresses sources seulement

Cisco IOS NAT ne prend pas en charge les types de trafic ci-dessous :

- Les mises à jour de la table de routage
- Les transferts de zone DNS
- Le protocole BOOTP
- talk, ntalk
- Le protocole SNMP (Simple Network Management Protocol)

Protocole DHCP :

Présentation du protocole DHCP

Le protocole DHCP (*Dynamic Host Configuration Protocol*) permet aux clients DHCP d'un réseau IP d'obtenir leurs configurations à partir d'un serveur DHCP. Le protocole DHCP est décrit dans la ***RFC 2131***.

Un client DHCP est fourni avec la plupart des systèmes d'exploitation récents, notamment les divers systèmes Windows, Novell Netware, Sun Solaris, Linux et MAC OS.

Le protocole DHCP n'est pas destiné à configurer les routeurs, les commutateurs et les serveurs. Ces types d'hôtes nécessitent des adresses IP statiques.

Les routeurs Cisco peuvent utiliser un jeu de fonctions Cisco IOS, Easy IP, pour offrir en option un serveur DHCP complet.

Le protocole DHCP s'appuie sur le protocole de transport UDP (*User Datagram Protocol*). Le client envoie des messages au serveur sur le port **67**. Le serveur envoie des messages au client sur le port **68**.

Différences entre les protocoles BOOTP et DHCP

La communauté Internet a tout d'abord développé le protocole BOOTP pour assurer la configuration des stations de travail sans disque. Le protocole BOOTP a été défini à l'origine dans la ***RFC 951*** de 1985

Les deux protocoles sont de type client/serveur et utilisent les ports UDP 67 et 68. Ces ports continuent à s'appeler les ports BOOTP.

Les quatre paramètres IP de base sont:

- L'adresse IP
- L'adresse de passerelle
- Le masque de sous-réseau
- L'adresse du serveur DNS

BOOTP	DHCP
Mappages statiques	Mappages dynamiques
Assignation permanente	Bail
Ne prend en charge que quatre paramètres de configuration	Prend en charge plus de 30 paramètres de configuration

Principales fonctions DHCP

Trois mécanismes permettent d'attribuer une adresse IP au client :

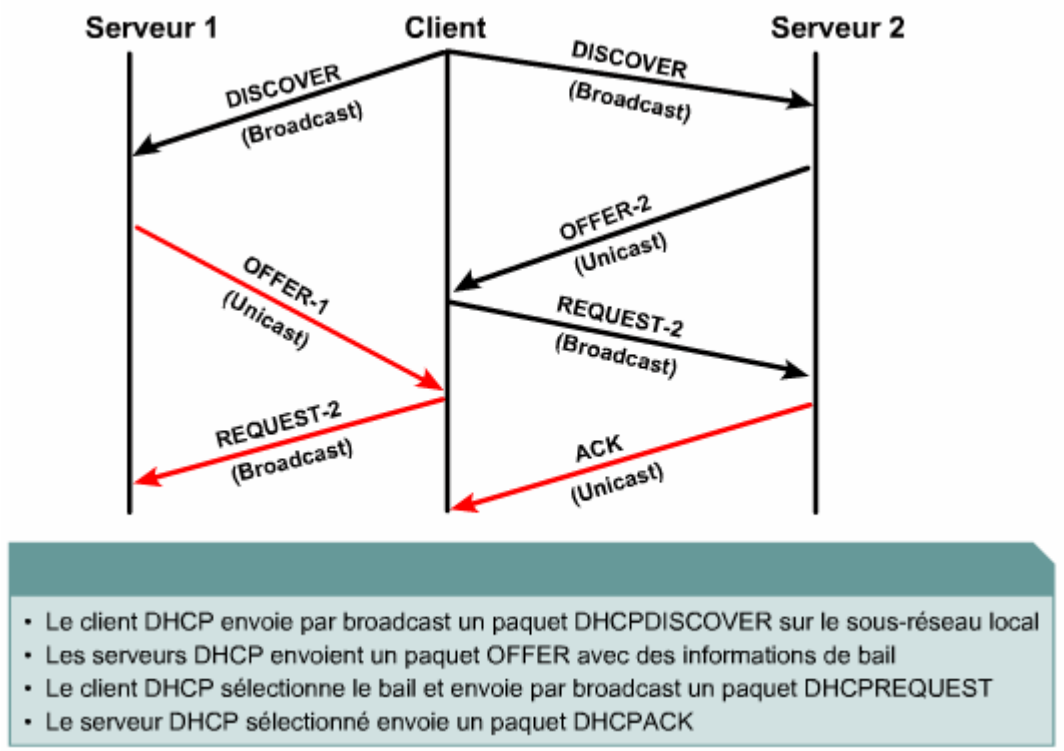
- **L'allocation automatique** – Le protocole DHCP attribue une adresse IP permanente à un client.
- **L'allocation manuelle** – C'est l'administrateur qui attribue l'adresse IP au client. DHCP transfère l'adresse au client.
- **L'allocation dynamique** – DHCP attribue une adresse IP au client pendant une durée limitée.

La présente section concerne principalement le mécanisme d'allocation dynamique. Certains des paramètres de configuration disponibles sont énumérés dans l'IETF ***RFC 1533***:

- Le masque de sous-réseau
- Le routeur (la passerelle par défaut)
- Le nom de domaine
- Le(s) serveur(s) de noms de domaine
- Le(s) serveur(s) WINS

Fonctionnement du protocole DHCP

Le processus de configuration du client DHCP se déroule comme suit :



- Le client DHCP envoie par broadcast un paquet DHCPDISCOVER sur le sous-réseau local
- Les serveurs DHCP envoient un paquet OFFER avec des informations de bail
- Le client DHCP sélectionne le bail et envoie par broadcast un paquet DHCPREQUEST
- Le serveur DHCP sélectionné envoie un paquet DHCPACK

1. Le client envoie une requête de configuration IP « un broadcast dénommé DHCPDISCOVER » à un serveur. Il peut arriver que le client suggère l'adresse IP dont il a besoin, par exemple pour demander l'extension d'une période d'utilisation.
2. Quand le serveur reçoit le broadcast, il détermine s'il peut desservir la requête à partir de sa propre base de données. Quand il n'y parvient pas, le serveur peut transférer la requête à un autre serveur DHCP. S'il y parvient, le serveur DHCP offre au client les informations de configuration IP sous la forme d'un DHCPOFFER unicast. Le DHCPOFFER est une configuration proposée qui peut inclure une adresse IP, une adresse de serveur DNS et la durée d'utilisation.
3. Si l'offre convient au client, celui-ci envoie un autre broadcast, DHCPREQUEST, pour demander spécifiquement ces paramètres IP.
4. Le serveur qui reçoit la demande DHCPREQUEST officialise la configuration en envoyant un accusé de réception en unicast, le DHCPACK. Il est possible, mais hautement improbable, que le serveur n'envoie pas le DHCPACK. Ceci peut se produire si le serveur a concédé ces informations à un autre client entre temps.

Si le client détecte que l'adresse est en cours d'utilisation sur le segment local, il envoie un message DHCPDECLINE et le processus recommence. Si le client a reçu un DHCPNACK du serveur après avoir envoyé le DHCPREQUEST, il recommence tout le processus.

Si le client n'a plus besoin de l'adresse IP, il envoie un message DHCPRELEASE au serveur.

Remarque : Le serveur émet une requête d'écho ICMP ou un ping vers une adresse du groupe avant d'envoyer le message DHCPOFFER à un client. Bien qu'il puisse être configuré, le nombre par défaut de pings utilisés pour vérifier une adresse IP potentielle s'élève à deux.

Configuration de DHCP

Router(config)#**ip dhcp pool {nom}** → spécifier le groupe DHCP

Router(dhcp-config)#**network {@ réseau} {masque}** → spécifier la plage d'@ du groupe

Router(config)#ip **dhcp excluded-address {@début} {@fin}** → exclure une plage d'@

Exemple :

```
Router(config)#ip dhcp pool subnet12
Router(dhcp-config)#network 172.16.12.0 255.255.255.0
Router(dhcp-config)#default-router 172.16.12.254
Router(dhcp-config)#dns-server 172.16.1.2
Router(dhcp-config)#netbios-name-server 172.16.1.3
Router(dhcp-config)#domain-name foo.com
```

Router(dhcp-config)#**lease infinite** → définir la durée de bail (par défaut : une journée)

Remarque : Le service DHCP est activé par défaut sur les versions de Cisco IOS qui le prennent en charge. Pour désactiver le service, utilisez la commande **no service dhcp**

Vérification du fonctionnement du protocole DHCP

Show ip dhcp binding → afficher la liste de toutes les liaisons créées par le service DHCP

Show ip dhcp server statistics → fournir les nombres de messages DHCP envoyés et reçus

```
Router#show ip dhcp binding
IP address     Hardware address   Lease expiration      Type
172.16.12.11   0100.10a4.97f4.6d  Mar 02 1993 12:38 AM  Automatic
```

Dépannage du protocole DHCP

Debug ip dhcp server events → vérifier régulièrement si les périodes d'utilisation ont expiré. S'affichent également les processus des adresses renvoyées et des adresses allouées

```
Router#debug ip dhcp server events
Router#
00:22:53: DHCPD:checking for expired leases.
00:22:23: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a4.97f4.6d
00:22:49: DHCPD:retured 172.16.13.11 to address pool remote.
00:22:59: DHCPD: assigned IP address 172.16.13.11 to client
0100.10a497f4.6d.
```

Relais DHCP

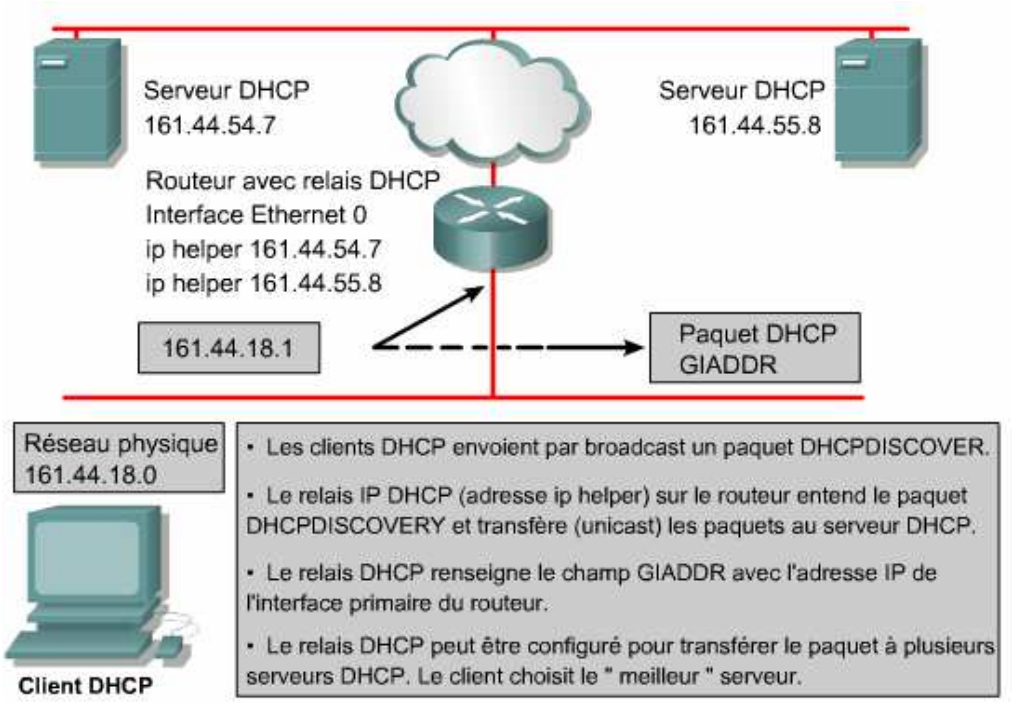
Les clients DHCP utilisent des broadcasts IP pour retrouver le serveur DHCP sur le segment. *Que se passe-t-il quand le serveur et le client ne résident pas sur le même segment et sont séparés par un routeur ?* Les routeurs ne transmettent pas les broadcasts.

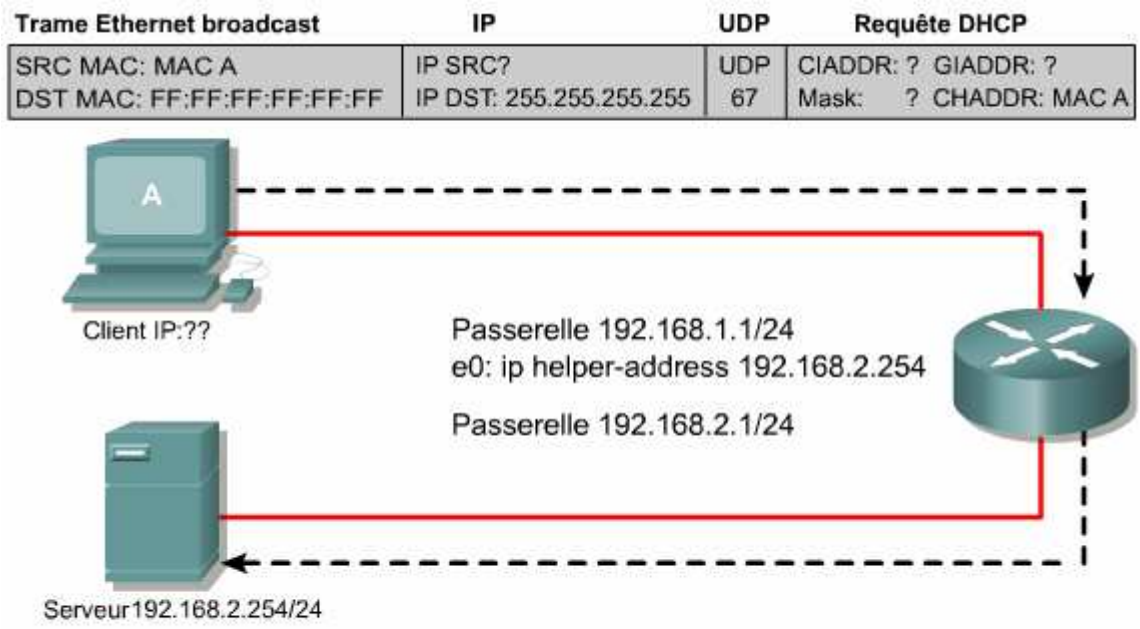
L'administrateur doit choisir entre les deux options suivantes : placer des serveurs sur tous les sous-réseaux ou utiliser la fonction adresse de diffusion de Cisco IOS. Utiliser la commande **ip helper-address** pour relayer les requêtes de broadcast.

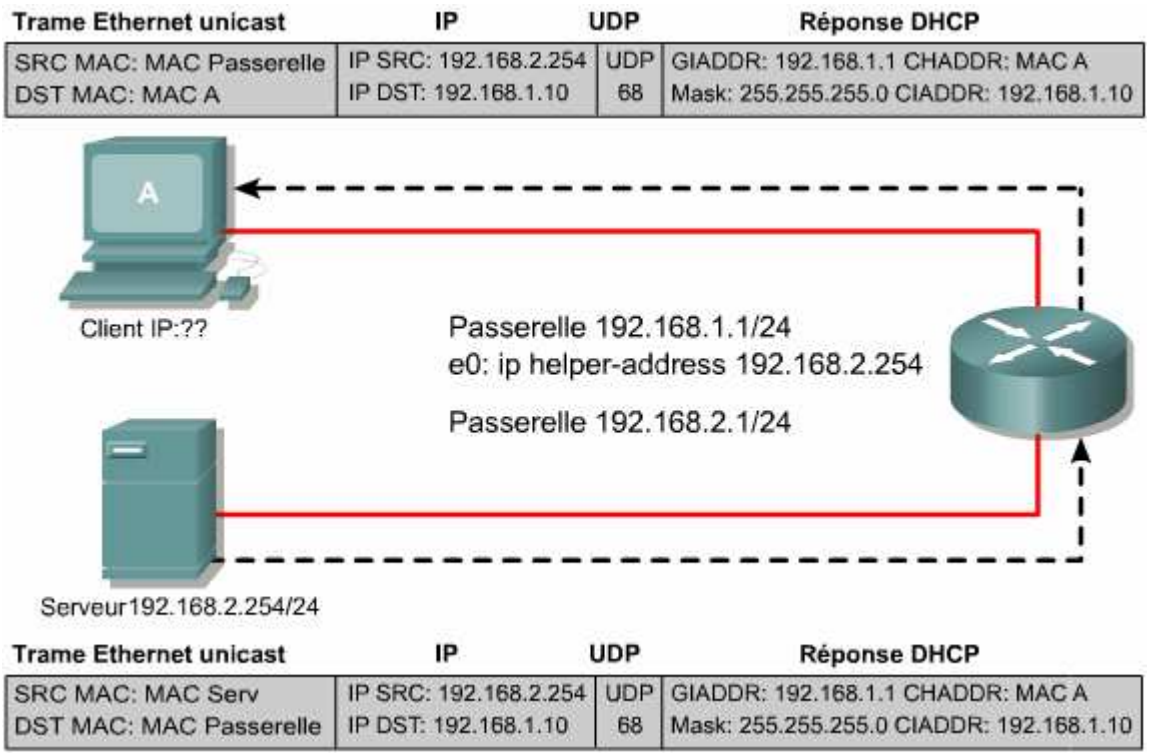
Par défaut, la commande **ip helper-address** transfère les huit services UDP suivants :

Protocole Time + TACACS + Le protocole DNS + Le serveur BOOTP/DHCP + Le client BOOTP/DHCP + TFTP + Le service de nom NetBIOS + Le service de datagramme NetBIOS

Code OP - 1 octet	Type de matériel - 1 octet	Longueur matériel - 1 octet	Sauts - 1 octet
ID transaction ID (XID) - 4 octets			
Secondes - 2 octets		Indicateurs - 2 octets	
Adresse IP client (CIADDR) - 4 octets			
Votre adresse IP (YIADDR) - 4 octets			
Adresse IP serveur (SIADDR) - 4 octets			
Adresse IP passerelle (GIADDR) - 4 octets			
Adresse matérielle client (CHADDR) -16 octets			
Nom serveur (SNAME) - 64 octets			
Nom de fichier - 128 octets			
Options DHCP - 312 octets			




Trame Ethernet broadcast
IP
UDP
Requête DHCP
SRC MAC: MAC A
DST MAC: FF:FF:FF:FF:FF:FF
IP SRC?
IP DST: 255.255.255.255
UDP
67
CIADDR: ? GIADDR: ?
Mask: ? CHADDR: MAC A
A
Client IP:??
Passerelle 192.168.1.1/24
e0: ip helper-address 192.168.2.254
Passerelle 192.168.2.1/24
Serveur192.168.2.254/24
Trame Ethernet unicast
IP
UDP
Requête DHCP
SRC MAC: MAC Passerelle
DST MAC: MAC Serv
IP SRC: 192.168.2.1
IP DST: 192.168.2.254
UDP
67
CIADDR: ? GIADDR: 192.168.1.1
Mask: ? CHADDR: MAC A


Trame Ethernet unicast
IP
UDP
Réponse DHCP
SRC MAC: MAC Passerelle
DST MAC: MAC A
IP SRC: 192.168.2.254
IP DST: 192.168.1.10
UDP
68
GIADDR: 192.168.1.1 CHADDR: MAC A
Mask: 255.255.255.0 CIADDR: 192.168.1.10
A
Client IP:??
Passerelle 192.168.1.1/24
e0: ip helper-address 192.168.2.254
Passerelle 192.168.2.1/24
Serveur192.168.2.254/24
Trame Ethernet unicast
IP
UDP
Réponse DHCP
SRC MAC: MAC Serv
DST MAC: MAC Passerelle
IP SRC: 192.168.2.254
IP DST: 192.168.1.10
UDP
68
GIADDR: 192.168.1.1 CHADDR: MAC A
Mask: 255.255.255.0 CIADDR: 192.168.1.10

Module 2

Technologies WAN

Aperçu des technologies WAN :

Technologie WAN :

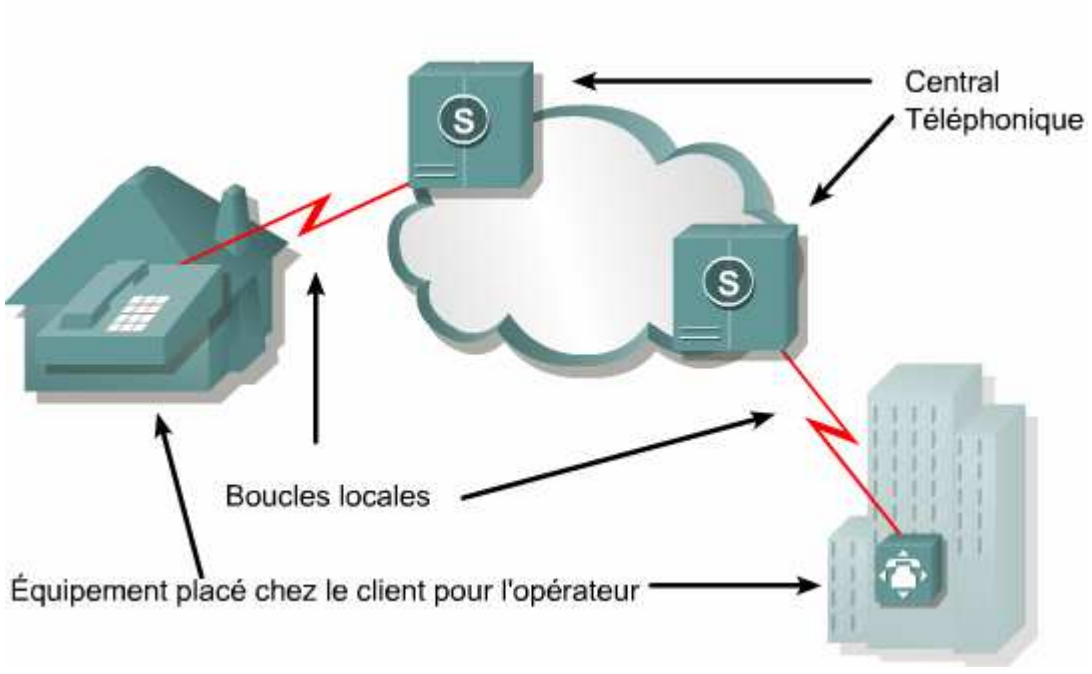
Un réseau WAN est un réseau de communication de données qui fonctionne au-delà de la portée géographique d'un réseau LAN. Les réseaux WAN et LAN ont pour différence principale qu'une société ou une entreprise doit s'abonner à un fournisseur d'accès WAN. Un réseau WAN utilise les liaisons de données fournies par un opérateur pour *accéder à Internet* et *connecter les sites d'une entreprise entre eux*, à des sites d'autres entreprises, à des *services externes* et à des *utilisateurs distants*.

Les WAN transportent généralement divers types de trafic, tels que la *voix*, des *données* et des *images vidéo*. Les services de réseau WAN les plus couramment utilisés sont les services téléphoniques et de données.

L'équipement situé dans les locaux de l'abonné est désigné par l'acronyme ***CPE*** (*Customer Premises Equipment* – équipement placé chez le client pour l'opérateur). L'abonné est propriétaire du CPE ou le loue à son fournisseur d'accès.

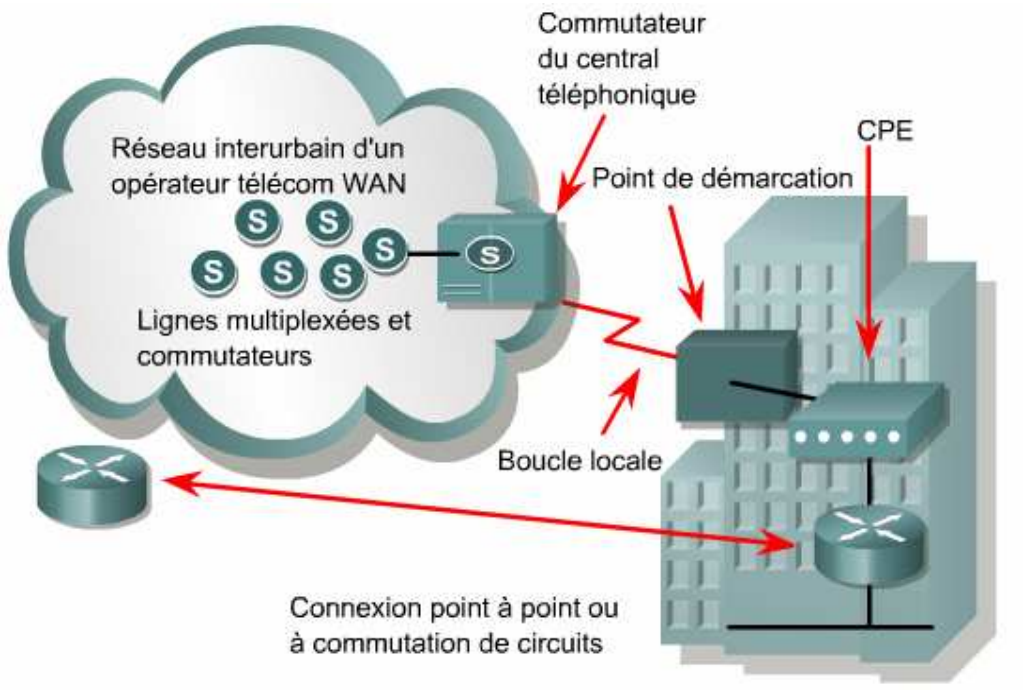
Un câble en cuivre ou en fibres connecte le CPE au central d'échange ou téléphonique (***CO*** – *central office*) le plus proche du fournisseur d'accès. Ce câblage est souvent désigné par le nom ***boucle locale***.

Un appel est connecté localement à d'autres boucles locales, ou non localement par l'intermédiaire d'une ligne multiplexée vers un central primaire. Il passe ensuite sur un central de section, puis un central d'opérateur régional ou international à mesure qu'il est mené à sa destination.



Pour que la boucle locale puisse transporter des données, un équipement tel qu'un modem s'avère nécessaire pour préparer la transmission. Les équipements qui mettent les données sur la boucle locale sont dénommées équipements de terminaison de circuit de données (***ETCD***) ou équipements de communication de données. Les équipements qui transmettent les données à l'ETCD sont appelés les équipements terminaux de traitement de données (***ETTD***).

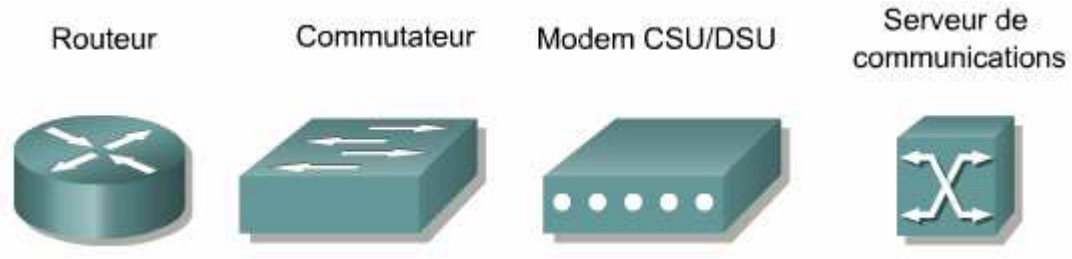
L'ETCD sert essentiellement d'interface entre l'ETTD et la liaison de communication située dans le nuage du réseau WAN.



Les liaisons WAN existent à diverses *vitesses* :

Type de ligne	Norme de signal	Débit binaire
56	DS0	56 Kbits/s
64	DS0	64 Kbits/s
T1	DS1	1.544 Mbits/s
E1	ZM	2.048 Mbits/s
E3	M3	34.064 Mbits/s
J1	Y1	2.048 Mbits/s
T3	DS3	44.736 Mbits/s
OC-1	SONET	51.84 Mbits/s
OC-3	SONET	155.54 Mbits/s
OC-9	SONET	466.56 Mbits/s
OC-12	SONET	622.08 Mbits/s
OC-18	SONET	933.12 Mbits/s
OC-24	SONET	1244.16 Mbits/s
OC-36	SONET	1866.24 Mbits/s
OC-48	SONET	2488.32 Mbits/s

Équipements WAN



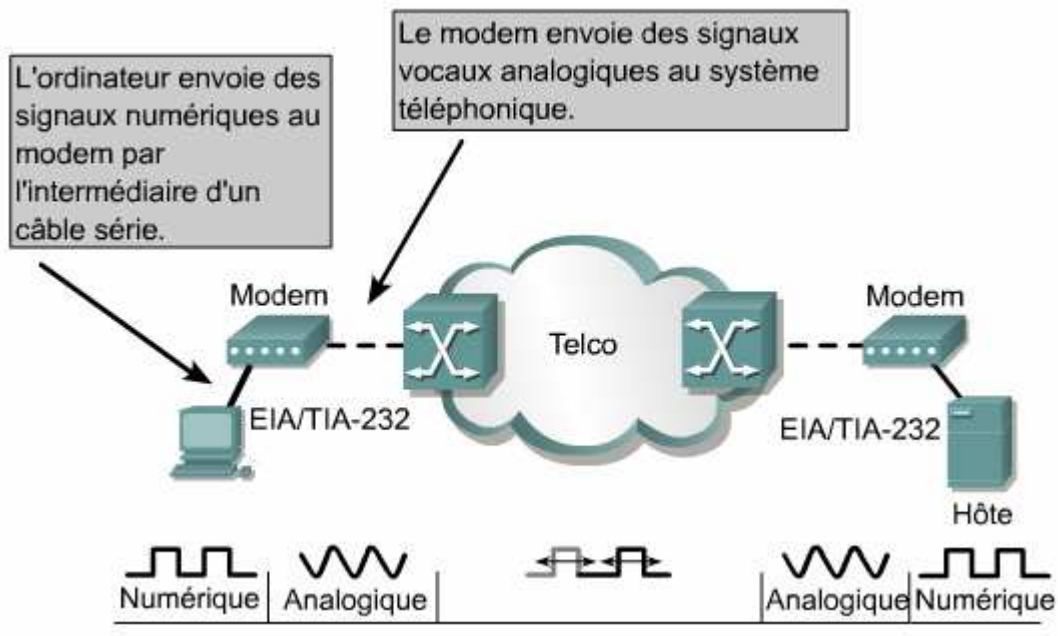
Les ordinateurs d'un réseau local ayant des données à transmettre les envoient sur un routeur qui contient à la fois des interfaces LAN et des interfaces WAN.

Le routeur utilise les informations d'adresse de couche 3 pour remettre les données sur l'interface WAN appropriée.

Les liaisons de communication nécessitent des signaux au format approprié. Sur les lignes numériques, une unité CSU (*channel service unit*) et une unité DSU (*data service unit*) sont nécessaires. Ces deux unités sont souvent combinées en une seule ***CSU/DSU***.

Un modem s'avère nécessaire si la boucle locale est analogique et non numérique. Les modems transmettent des données sur les lignes téléphoniques vocales en modulant et en démodulant le signal.

Les serveurs de communication concentrent les communications entrantes des utilisateurs et les accès à distance à un réseau local. Ils peuvent comporter un mélange d'interfaces analogiques et numériques (RNIS) et prendre en charge des centaines d'utilisateurs simultanés.



Normes WAN

Les WAN utilisent le modèle de référence OSI, mais se concentrent principalement sur la couche 1 et la couche 2.

Les normes WAN décrivent généralement les méthodes de livraison sur la couche physique et les caractéristiques requises pour la couche de liaison de données.

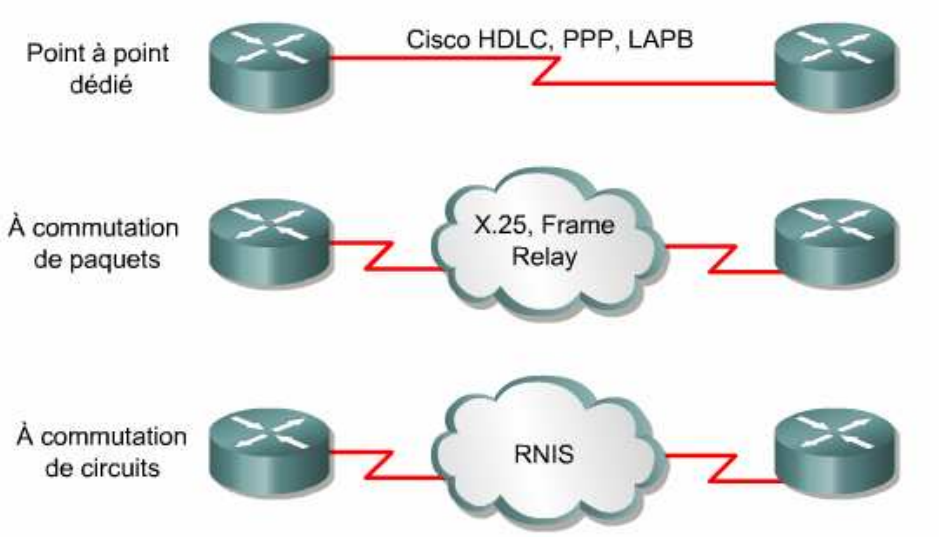
Les normes WAN sont définies et gérées par plusieurs autorités reconnues.

ITU-T + ISO + IETF + EIA + TIA

Les protocoles de couche physique décrivent comment fournir les connexions électriques, mécaniques, opérationnelles et fonctionnelles aux services fournis par un FA.

Norme	Description
EIA/TIA-232	Autorise des débits jusqu'à 64 kbits/s sur un connecteur D 25 broches sur de courtes distances. Anciennement désigné par RS-232. La spécification ITU-T V.24 est effectivement identique.
EIA/TIA-449/530	Version plus rapide (pouvant atteindre 2 Mbits/s) de la norme EIA/TIA-232. Elle utilise un connecteur D de 36 broches et est capable de prendre en charge des câbles plus longs. Il en existe plusieurs versions. Également appelée RS-422 et RS-423.
EIA/TIA-612/613	L'interface HSSI (High Speed Serial Interface), qui offre un accès aux services à des vitesses atteignant 52 Mbits/s sur un connecteur D à 60 broches.
V.35	Norme de l'ITU-T relative aux communications synchrones entre un équipement d'accès réseau et un réseau de transmission de paquets à des débits pouvant atteindre 48 kbits/s. Elle s'appuie sur un connecteur rectangulaire à 34 broches.
X.21	Norme de l'ITU-T relative aux communications numériques synchrones. Elle s'appuie sur un connecteur à 15 broches.

Les protocoles de la couche de liaison de données définissent la manière dont les données sont encapsulées en vue de leur transmission vers des sites distants, ainsi que les mécanismes de transfert des trames obtenues.

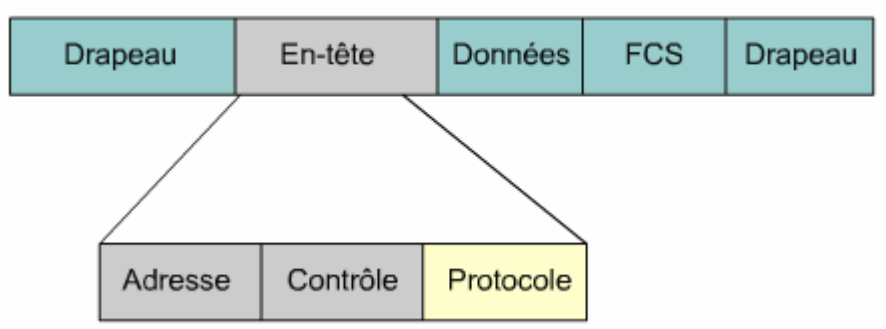


Encapsulation WAN

La couche de liaison de données établit une trame autour des données de la couche réseau, de telle sorte que les vérifications et contrôles nécessaires puissent être appliqués. Chaque type de connexion WAN utilise un protocole de couche 2 pour encapsuler le trafic pendant qu'il traverse la liaison longue distance.

Le choix du protocole d'encapsulation est fonction de la technologie WAN et de l'équipement. Le tramage s'appuie essentiellement sur la norme ***HDLC***.

Le tramage **HDLC** offre une livraison fiable des données sur des lignes qui ne sont pas fiables et inclut des mécanismes de contrôle de flux et d'erreur.



La trame commence et se termine toujours par un champ indicateur sur 8 bits, selon le motif 01111110. Comme ce motif est susceptible de survenir dans les données mêmes, le système HDLC émetteur insère toujours un bit 0 tous les cinq 1 du champ de données. Quand les trames sont transmises de façon consécutive, l'indicateur de fin de la première trame sert d'indicateur de début de la suivante.

Le champ **adresse** n'est pas requis pour les liaisons WAN, qui sont presque toujours point-à-point. Le champ adresse est toujours présent et peut avoir une longueur d'un ou deux octets.

Le champ de **contrôle** (généralement un octet, mais sera de deux octets pour les systèmes à fenêtres glissantes) indique le type de trame, qui peut être de type :

- Les trames non-numérotées transportent des messages de configuration de ligne.
- Les trames d'informations transportent les données de couche de réseau.
- Les trames de supervision contrôlent le flux de trames d'informations et demandent la retransmission des données en cas d'erreur.

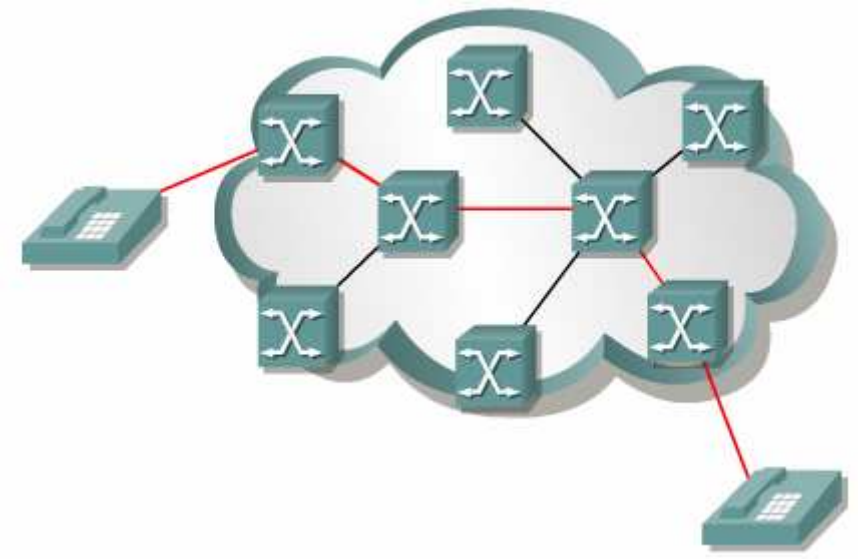
Une séquence de vérification de trame (**FCS**) utilise le mécanisme de code de redondance cyclique (CRC) pour établir un champ de deux ou quatre octets.

Plusieurs protocoles de liaison de données sont utilisés, notamment des sous-ensembles et des versions propriétaires de HDLC. PPP et la version Cisco de HDLC disposent d'un champ supplémentaire dans l'en-tête afin d'identifier le **protocole** de couche réseau des données encapsulées.

Commutation de paquets et de circuits

Les réseaux à commutation de paquets ont été développés pour éviter les dépenses entraînées par les réseaux à commutation de circuits publics et pour offrir une technologie WAN plus économique.

Lorsqu'un abonné passe un appel téléphonique, le numéro appelé sert à définir des commutations dans les échanges effectués sur la route de l'appel, de telle sorte qu'il existe un **circuit continu** entre l'appelant et l'appelé.

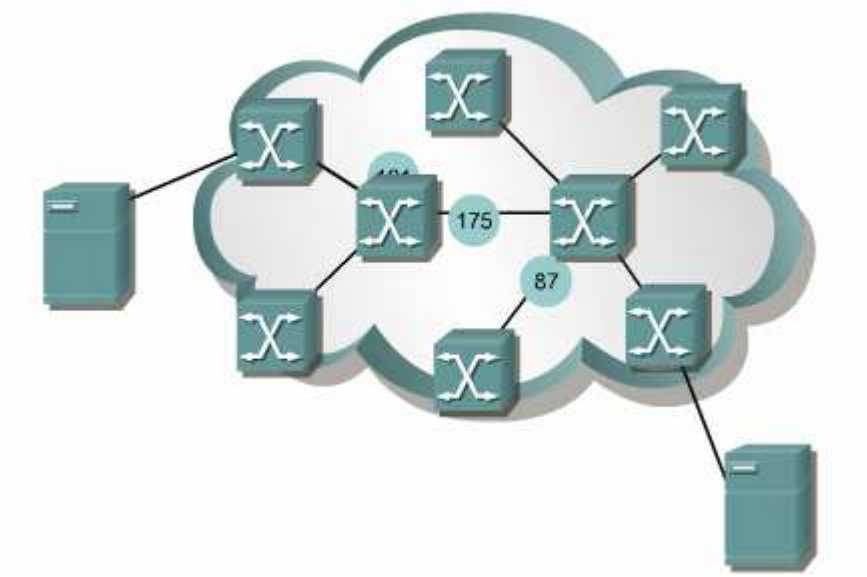


Le chemin interne emprunté par le circuit entre les échanges est partagé par un certain nombre de conversations. Le ***multiplexage temporel*** (TDM - *Time division multiplexing*) permet de partager la connexion à tour de rôle entre chaque conversation. Le TDM assure qu'une connexion de capacité fixe soit mise à la disposition de l'abonné.

Si le circuit transporte des données informatiques, l'utilisation de cette capacité fixe risque de ne pas être efficace. Les circuits commutés constituent généralement une méthode coûteuse de déplacement des données.

Une autre possibilité consiste à seulement allouer la capacité au trafic quand celui-ci s'avère nécessaire et partager la capacité disponible entre de nombreux utilisateurs. Avec une connexion à commutation de circuits, les bits de données placés sur le circuit sont automatiquement remis à l'extrémité distante, car le circuit est déjà établi.

Si le circuit doit être partagé, un mécanisme doit identifier les bits, de manière à ce que le système sache où les remettre. Il est difficile d'étiqueter des bits individuels et ceux-ci sont donc rassemblés dans des groupes appelés cellules, trames ou paquets. **Commutation de paquets**.



Les liaisons qui connectent les commutateurs du réseau du fournisseur d'accès appartiennent à un abonné en particulier au cours du transfert des données, ce qui permet à de nombreux abonnés de partager la liaison. Les coûts peuvent être considérablement moins élevés que ceux d'une connexion dédiée à commutation de circuits.

Les données des réseaux à commutation de paquets sont soumises à des retards imprévisibles lorsque des paquets individuels attendent que les paquets d'autres abonnés soient transmis par un commutateur.

À partir des informations d'adresse fournies dans chaque paquet, les commutateurs d'un réseau à commutation de paquets déterminent le lien vers lequel le paquet doit ensuite être envoyé. Il existe deux approches à cette détermination des liaisons :

→ **Non-orienté connexion** (Internet) transportent des données d'adressage complètes dans chaque paquet. Chaque commutateur doit évaluer l'adresse pour déterminer où envoyer le paquet.

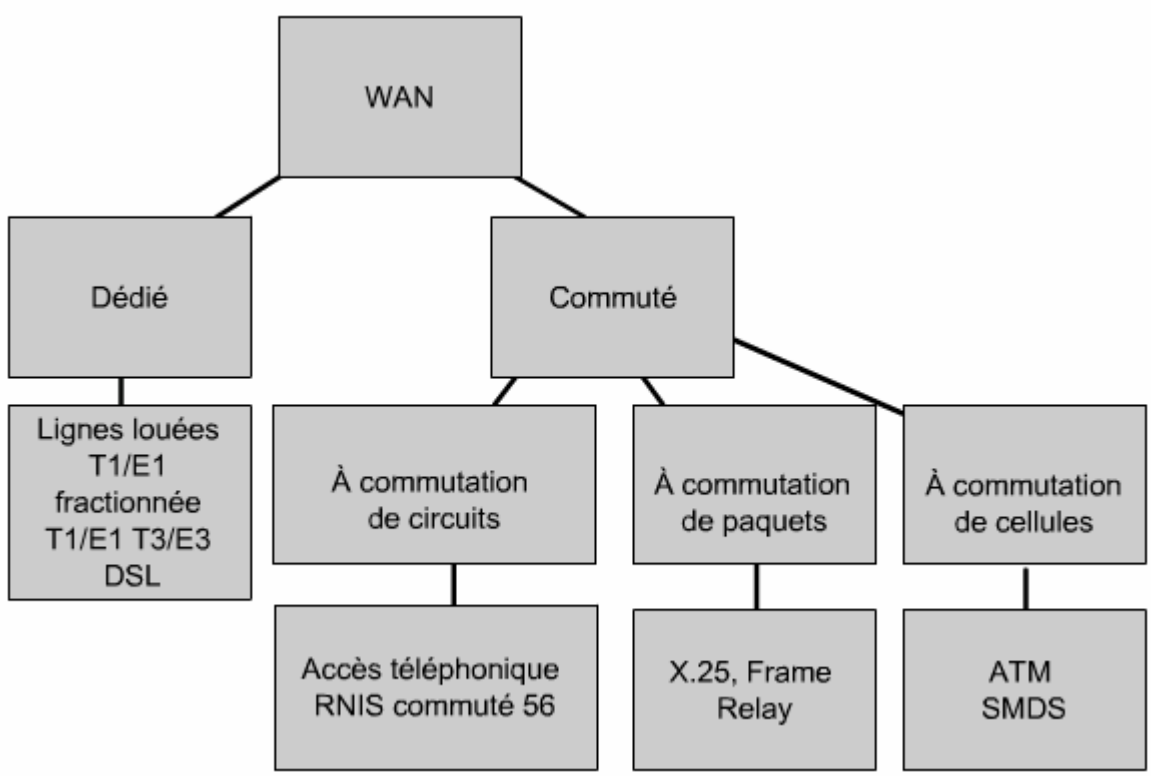
→ **Orientés connexion** prédéterminent la route de chaque paquet, qui n'a alors besoin que d'un identificateur.

Si un circuit n'existe physiquement que lorsqu'un paquet se déplace dessus, il prend le nom de ***circuit virtuel*** (VC – *Virtual Circuit*).

➔ Circuit virtuel commuté (***SVC***) : Les entrées qui constituent un circuit virtuel peuvent être établies par une requête de connexion envoyée sur le réseau.

➔ Circuit virtuel permanent (***PVC***) : Les entrées de la table sont chargées par les commutateurs au démarrage, de telle sorte que le circuit virtuel permanent soit toujours disponible.

Options de liaison WAN



Technologies WAN :

Connexions commutées analogiques

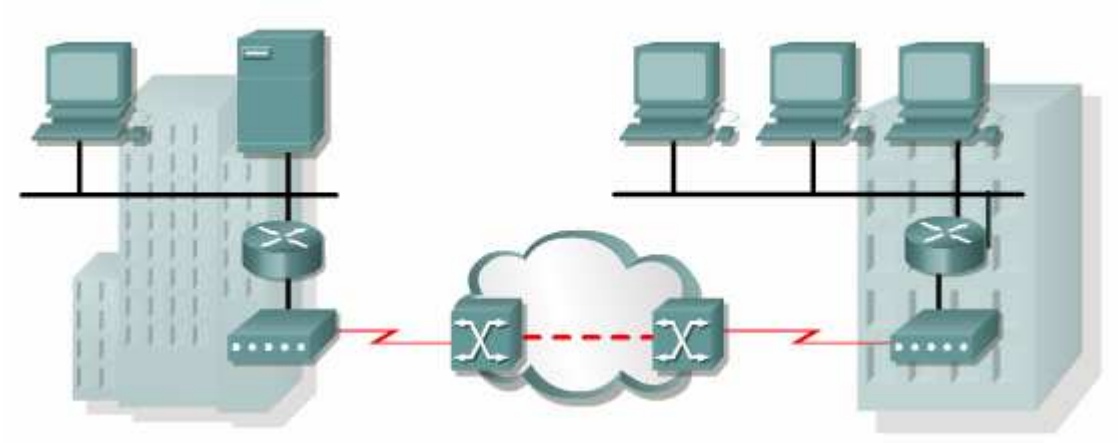
Lorsque des transferts de données intermittents de faible volume sont nécessaires, les modems et les lignes téléphoniques commutées analogiques fournissent des connexions ***commutées*** de faible capacité et dédiées.

La téléphonie traditionnelle utilise un câble de cuivre, appelé la boucle locale, pour connecter le combiné téléphonique situé dans les locaux de l'abonné au réseau téléphonique commuté public (RTCP).

La boucle locale n'est pas adaptée au transport direct de données informatiques binaires, mais un *modem permet d'envoyer des données informatiques* par le réseau téléphonique vocal.

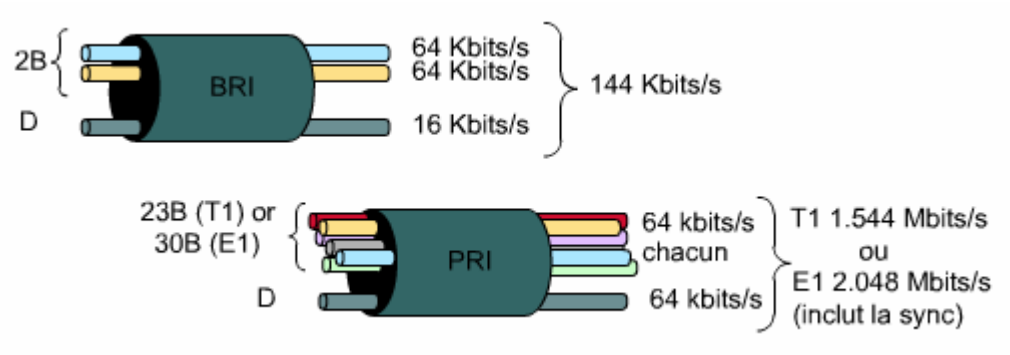
La limite supérieure du débit se situe aux environs de 33 Kbits/s. Le débit peut être augmenté à environ 56 Kbits/s si le signal passe directement par une connexion numérique.

Les **avantages** du modem et des lignes analogiques sont la simplicité, la disponibilité et le faible coût de mise en œuvre. Les **inconvénients** en sont les faibles débits et un temps de connexion relativement long. Le trafic vocal ou vidéo ne fonctionne pas de façon adéquate à des débits relativement faibles.



RNIS

Le réseau RNIS transforme la boucle locale en une connexion numérique TDM. La connexion utilise des canaux Bearer à 64 kbits/s (B) pour transporter la voix ou les données et un canal delta de signal (D) destiné à la configuration de la communication et à d'autres fonctions.



Le réseau ***RNIS BRI*** accès de base est destiné aux utilisateurs individuels et aux petites entreprises et offre deux canaux B à 64 kbits/s et un canal D à 16 kbits/s.

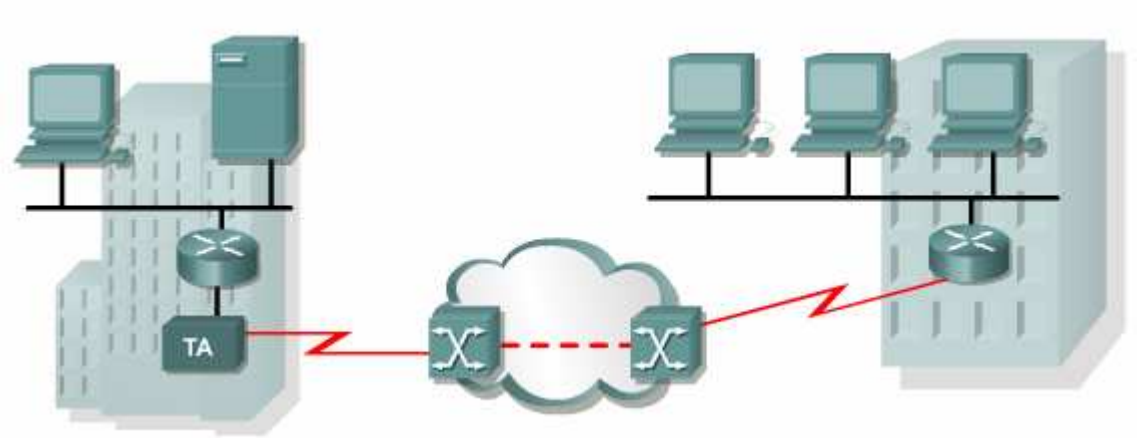
Pour les installations de plus grande taille, il existe une version de ***RNIS PRI*** accès primaire. L'accès PRI offre plusieurs canaux B (ça dépend des normes E1 ou T1).

Remarque : Le débit du PRI international correspond à une connexion E1.

Remarque : Avec l'utilisation de BRI, Certains fournisseurs laissent le canal D transporter des données à bas débit, telles que les connexions X.25 à 9.6 kbits/s.

Pour les petits réseaux WAN, le RNIS BRI peut offrir un mécanisme de connexion idéal. La durée de mise en fonction du BRI est inférieure à une seconde et son canal B à 64 kbits/s offre une capacité plus importante que celle d'une liaison par modem analogique.

Une autre application courante du RNIS consiste à fournir des capacités supplémentaires en fonction des besoins à une connexion par ligne louée. La ligne louée est dimensionnée pour transporter des charges de trafic moyennes et le RNIS vient s'y ajouter lors des périodes de pointe. Le RNIS sert également de ligne de secours en cas de défaillance de la ligne louée. Les tarifs RNIS sont calculés par canal B et sont similaires à ceux des connexions analogiques vocales.



Ligne Louée

Lorsque des connexions dédiées permanentes sont nécessaires, des lignes louées, dont le débit peut s'élever à 2,5 Gbits/s sont utilisées.

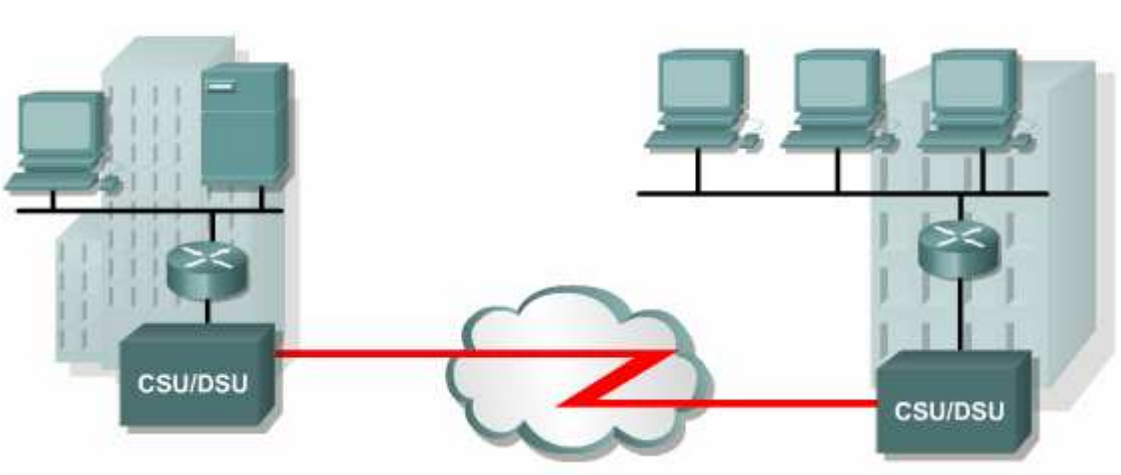
Une liaison point-à-point fournit un chemin de communication WAN préétabli entre les locaux du client et une destination distante. Il existe différentes capacités de lignes louées.

Type de ligne	Norme de signal	Débit binaire
56	DS0	56 Kbits/s
64	DS0	64 Kbits/s
T1	DS1	1.544 Mbits/s
E1	ZM	2.048 Mbits/s
E3	M3	34.064 Mbits/s
J1	Y1	2.048 Mbits/s
T3	DS3	44.736 Mbits/s
OC-1	SONET	51.84 Mbits/s
OC-3	SONET	155.54 Mbits/s
OC-9	SONET	466.56 Mbits/s
OC-12	SONET	622.08 Mbits/s
OC-18	SONET	933.12 Mbits/s
OC-24	SONET	1244.16 Mbits/s
OC-36	SONET	1866.24 Mbits/s
OC-48	SONET	2488.32 Mbits/s

Le prix de ces circuits dédiés est généralement fondé sur le débit, ainsi que sur la distance entre les deux points connectés.

Les liaisons point-à-point sont généralement plus coûteuses que les services partagés tels que Frame Relay. L'aspect dédié de la ligne permet d'éviter la latence ou la gigue entre les points d'extrémité. Une disponibilité constante est essentielle à certaines applications, telles que le commerce électronique.

Le port série d'un routeur est requis pour chaque connexion sur ligne louée. Une unité CSU/DSU et le circuit provenant du fournisseur d'accès sont également requis.



Inconvénients : Le trafic des WAN est souvent variable et les lignes louées offrent une capacité fixe. Par ailleurs, chaque point d'extrémité nécessite une interface sur le routeur, ce qui entraîne une augmentation des coûts en équipement.

Avantage : Plusieurs connexions peuvent être multiplexées sur une ligne louée, de façon à fournir des liaisons plus courtes et un nombre moins important d'interfaces requises.

X.25

En réaction aux coûts des lignes louées, les fournisseurs d'accès ont introduit des réseaux à commutation de paquets sur des lignes partagées, en vue de réduire les coûts. Le premier de ces réseaux à commutation de paquets a été normalisé sous le groupe de protocoles X.25. Il fournit une capacité variable de faible débit, qui peut être commutée ou permanente.

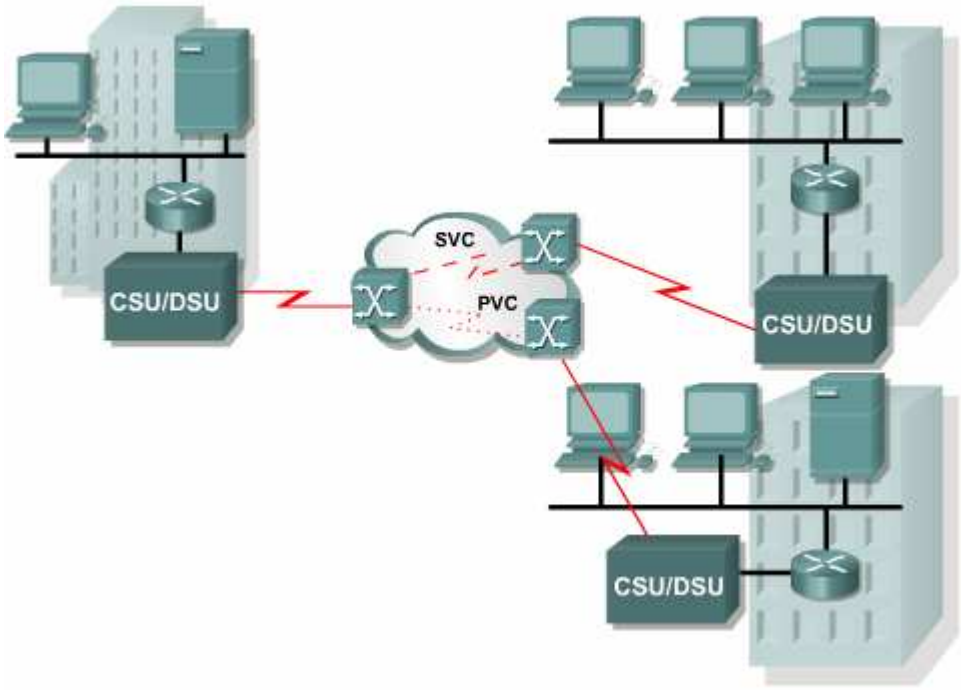
X.25 est un protocole de couche de réseau avec lequel les abonnés reçoivent une adresse réseau. Des circuits virtuels peuvent être établis sur le réseau, avec des paquets de requête d'appel vers l'adresse de destination. Le circuit virtuel commuté obtenu est identifié par un numéro de canal. Des paquets de données identifiés par le numéro de canal sont remis à l'adresse correspondante. *Plusieurs canaux peuvent être actifs sur une seule connexion.*

X.25 peut s'avérer très économique, car les tarifs sont fondés sur la quantité de données remises, et non sur la durée ou la distance de connexion. Les données peuvent être remises à n'importe quel débit, dans les limites de la capacité de la connexion. Ceci procure

une certaine souplesse. Les réseaux X.25 offrent généralement un débit faible, à un maximum de 48 kbits/s. Par ailleurs, les paquets de données sont soumis aux délais typiques des réseaux partagés.

Remarque : Les réseaux Frame Relay ont remplacé le X.25 chez de nombreux fournisseurs.

Parmi les applications X.25 typiques, on trouve les *lecteurs de carte sur point de vente* pour valider les transactions sur un ordinateur central. Certaines entreprises font également appel à des réseaux X.25 à valeur ajoutée pour *transférer des factures EDI* (*Electronic Data Interchange*), des *notes de chargement* et d'autres *documents commerciaux*. Pour ces applications, le bas débit et la latence élevée ne constituent pas une préoccupation, car son coût peu élevé rend le X.25 très économique.



Frame Relay

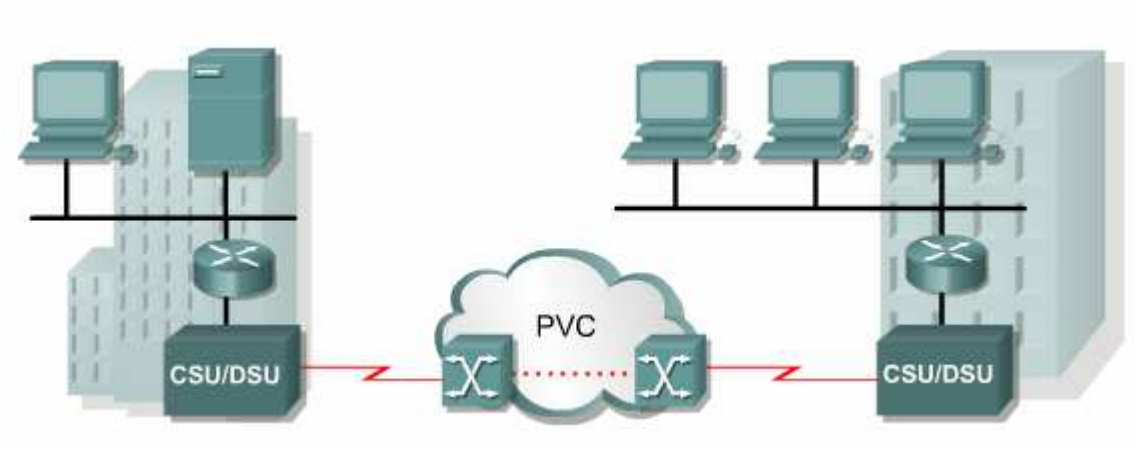
Avec l'augmentation de la demande d'une commutation de paquets au débit plus élevé et à la latence moins importante, les fournisseurs d'accès ont introduit les réseaux ***Frame Relay***. Bien que la configuration réseau semble similaire à celle de la technologie X.25, les débits peuvent couramment atteindre 4 Mbits/s, certains fournisseurs proposant même des débits plus élevés.

Plusieurs aspects différencient les technologies Frame Relay et X.25. Avant tout, il s'agit d'un protocole bien plus simple, qui fonctionne au niveau de la couche de liaison de données au lieu de la couche réseau.

Frame Relay ne met en œuvre aucun contrôle d'erreur ou de flux. L'accumulation des trames sur les commutateurs intermédiaires permettent de réduire les phénomènes de gigue.

La plupart des connexions Frame Relay sont des circuits virtuels permanents et non des circuits virtuels commutés (via une ligne louée), mais des connexions commutées sont disponibles auprès de certains fournisseurs utilisant des lignes RNIS. Le canal RNIS D sert à configurer un circuit virtuel commuté sur un ou plusieurs canaux B. Les tarifs Frame Relay sont fondés sur la capacité du port de connexion, à la périphérie du réseau.

Le Frame Relay fournit un débit partagé moyen pouvant transporter du trafic vocal et de données. La technologie Frame Relay s'avère idéale pour connecter les réseaux locaux d'entreprise. Le routeur du réseau local ne nécessite qu'une interface, même avec plusieurs circuits virtuels.



ATM

Les fournisseurs de communications ont déterminé qu'il existait un besoin de technologie réseau partagée permanente présentant peu de latence et de gigue à des débits bien plus élevés. La solution s'est présentée sous la forme du mode de transfert asynchrone ATM (*Asynchronous Transfer Mode*). ***ATM*** offre des débits supérieurs à 155 Mbits/s.

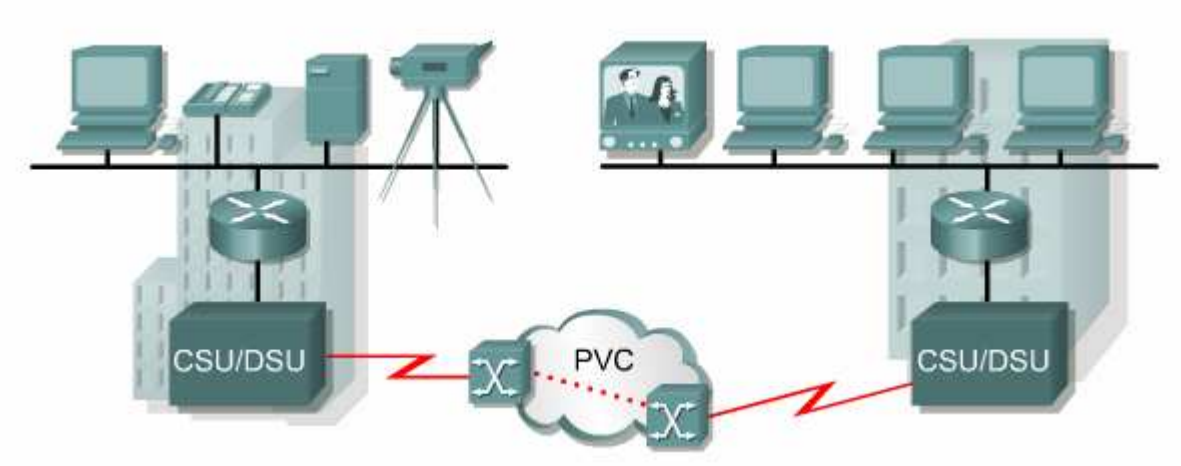
ATM est une technologie capable de transférer la voix, la vidéo et les données par des réseaux privés et publiques. Elle est fondée sur une architecture à cellules, et non une architecture à trames. Les cellules ATM présentent toujours une longueur fixe de 53 octets. La cellule ATM de 53 octets contient un en-tête ATM de 5 octet, suivie de 48 octets de données utiles ATM.

Les petites cellules de longueur fixe sont bien adaptées au transport du trafic vocal et vidéo, car ce trafic ne tolère pas les délais. En effet, le trafic vidéo et vocal n'a pas à attendre la fin de transmission d'un paquet de données de plus grande taille.

La cellule ATM de 53 octets est moins efficace que les trames et paquets de plus grande taille de Frame Relay et de X.25. Par ailleurs, quand la cellule transporte des paquets de couche réseau segmentée, la surcharge est plus importante, car le commutateur ATM doit être en mesure de regrouper les paquets au niveau de la destination.

ATM offre des circuits virtuels permanents et des circuits virtuels *commutés*, mais ces derniers sont plus courants avec les WAN.

Tout comme les autres technologies partagées, ATM accepte plusieurs circuits virtuels sur une seule connexion par ligne louée vers la périphérie du réseau.



DSL

Le ***DSL*** (*Digital Subscriber Line*) est une technologie à large bande qui utilise les lignes téléphoniques à paire torsadée existantes pour transporter des données à large bande aux abonnés du service.

Large bande désigne une technique utilisant plusieurs fréquences au sein d'un même support physique pour transmettre des données.

- ADSL (*Asymmetric DSL*)
- SDSL (*Symmetric DSL*)
- HDSL (*High Bit Rate DSL*)
- IDSL (*DSL RNIS*)
- CDSL *(Consumer DSL)*, également appelé DSL-lite ou G.lite

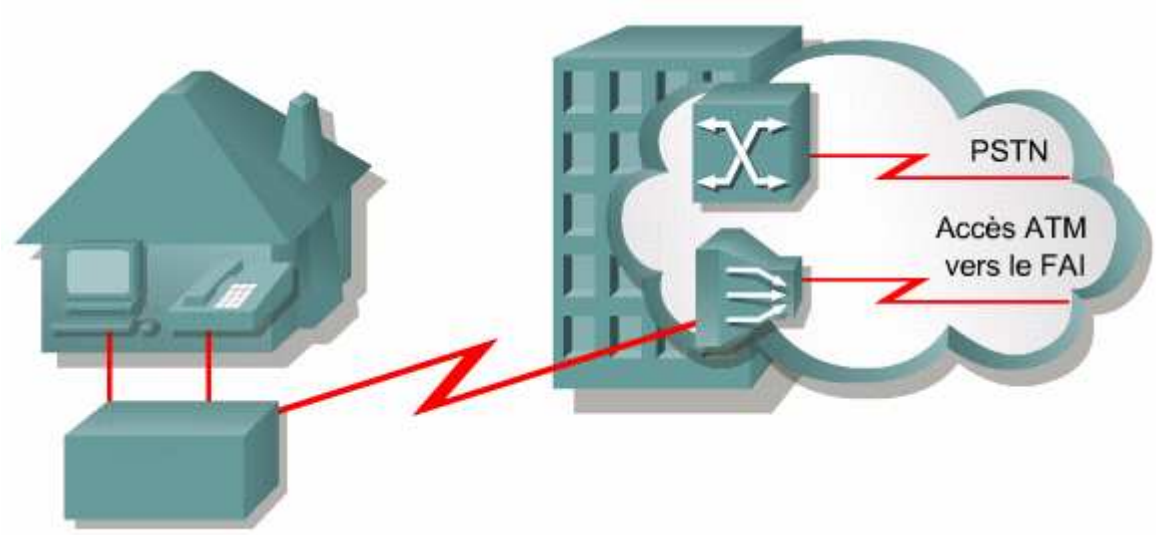
Service	Télédéchargement	Téléchargement
ADSL	64 Kbits/s - 8.192 Mbits/s	16 Kbits/s - 640 Kbits/s
SDSL	1.544 Mbits/s - 2.048 Mbits/s	1.544 Mbits/s - 2.048 Mbits/s
HDSL	1.544 Mbits/s - 2.048 Mbits/s	1.544 Mbits/s - 2.048 Mbits/s
IDSL	144 Kbits/s	144 Kbits/s
CDSL	1 Mbits/s	16 Kbits/s - 160 Kbits/s

La technologie ***DSL*** permet au fournisseur d'accès de proposer des services de réseau haut débit à ses clients, au moyen de boucles locales de cuivre existantes. La technologie DSL permet d'utiliser la ligne de boucle locale pour les connexions téléphoniques normales, ainsi que pour une connexion toujours active offrant une connectivité instantanée au réseau.

Plusieurs lignes d'abonnés DSL sont multiplexées en un lien unique à haute capacité au moyen d'un multiplexeur d'accès DSL (DSLAM) dans les locaux du fournisseur d'accès.

Les technologies DSL actuelles utilisent des techniques complexes de codage et de modulation pour obtenir des débits pouvant s'élever à 8 192 Mbits/s.

Les technologies DSL effectuent les transmissions de données en aval et en amont à des fréquences supérieures à cette plage de 4 KHz (minimum requis pour n'importe quelle transmission vocale sur la boucle locale). C'est cette technique qui permet aux transmissions vocales et de données de s'effectuer simultanément sur un service DSL.



Les deux types de technologies DSL de base sont le DSL *asymétrique* (ADSL) et le DSL *symétrique* (SDSL). Le service asymétrique offre à l'utilisateur une bande passante supérieure pour le téléchargement vers l'utilisateur à celle du transfert d'information dans la direction opposée. Le service symétrique fournit la même capacité dans les deux sens.

Certaines technologies DSL n'acceptent pas l'utilisation d'un téléphone. Le SDSL est appelé « ***dry copper*** » (cuivre sec), parce qu'il n'a pas de tonalité et n'offre pas de service téléphonique sur la même ligne.

Les différentes variétés de DSL fournissent des bandes passantes différentes, avec des capacités supérieures à celles d'une ligne louée T1 ou E1. Les taux de transfert dépendent de la longueur effective de la boucle locale, ainsi que du type et de la condition de ses câbles.

Remarque : Pour fournir un service satisfaisant, la boucle doit être inférieure à 5,5 kilomètres.

En général, une connexion IP vers l'entreprise est effectuée par Internet. Ceci occasionne donc des risques. Pour répondre à ces préoccupations de sécurité, les services DSL offrent la possibilité d'utiliser des connexions de réseau privé virtuel (VPN).

Modem câble

Les modems câble permettent d'effectuer des transmissions de données bidirectionnelles à haute vitesse sur les lignes coaxiales qui transmettent la télévision câblée. Certains fournisseurs d'accès câblé promettent des débits pouvant s'élever à 6,5 fois ceux de

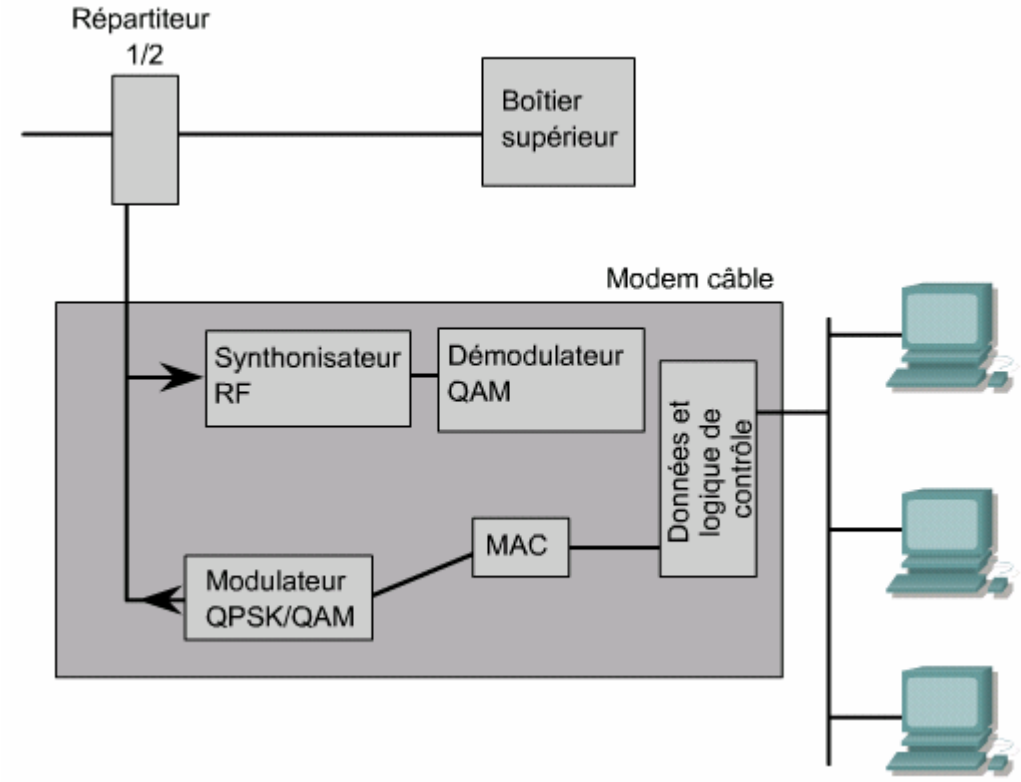
lignes louées T1. Cette vitesse fait du câble un support attrayant pour le transfert rapide de grandes quantités d'informations numériques, notamment des séquences vidéo, des fichiers audio ou des données en masse.

Exemple : Des informations dont le téléchargement prendrait deux minutes avec la technologie RNIS BRI peuvent être téléchargées en deux secondes par une connexion à modem câble.

Les modems câbles offrent une connexion permanente et sont faciles à installer. La connexion permanente implique que les ordinateurs connectés peuvent être sujets à des intrusions à tout moment et qu'ils doivent donc être sécurisés par des pare-feu → (VPN).

Un modem câble peut transférer jusqu'à 30 ou 40 Mbits/s de données sur un canal câblé à 6 MHz. Cela est pratiquement 500 fois plus rapide qu'un modem à 56 Kbits/s.

Avec un modem câble, *un abonné peut continuer à recevoir son service de télévision câblée, tout en recevant des données sur un ordinateur personnel*. Pour ce faire, il utilise un simple répartiteur à deux voies.



Tous les abonnés locaux partagent la même bande passante. À mesure que des utilisateurs se joignent au service, la bande passante disponible peut être inférieure au débit attendu.

Conception d'un WAN

Communication dans un réseau WAN :

Les WAN sont considérés comme un jeu de liaison de données connectant des routeurs de réseaux locaux.

Les frais de mise en œuvre des liaisons constituent l'élément de coût le plus important d'un WAN et l'objet de la conception doit être de fournir une bande passante maximale à un prix acceptable.

Les WAN transportent divers types de trafic. La conception sélectionnée doit fournir la capacité et les temps de transfert correspondant aux besoins de l'entreprise. Il faut tenir compte de la *topologie* des connexions entre les différents sites, de la *nature* de ces *connexions* et de la *bande passante*.

Les WAN fonctionnent au niveau des trois couches inférieures du modèle OSI.

Étapes de conception d'un WAN :

Pour concevoir un WAN il est nécessaire de savoir quel trafic de données va être transporté, son origine et sa destination. Les WAN transportent une grande diversité de types de trafic, avec différents besoins relatifs à la bande passante, la latence et la gigue.

Trafic	Latence	Gigue	Bande passante
Voix	Basses	Basses	Moyen
Transactions (par exemple SNA)	Moyen	Moyen	Moyen
Courrier électronique	Hautes	Hautes	Hautes
Transfert de fichiers	Hautes	Hautes	Hautes
Données en lots	Hautes	Hautes	Hautes
Administration réseau	Hautes	Hautes	Basses
Vidéoconférence	Basses	Basses	Hautes

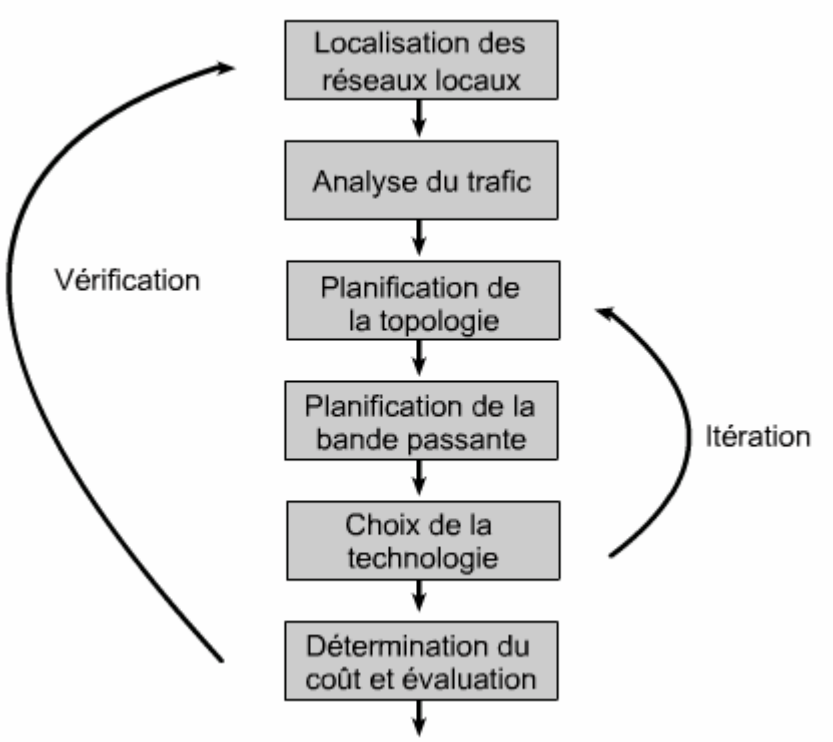
Pour chaque paire de points d'extrémité et pour chaque type de trafic, il est nécessaire d'obtenir des informations sur les diverses caractéristiques de trafic. Ceci implique des analyses approfondies, ainsi que la consultation des utilisateurs du réseau.

La connaissance des divers points d'extrémité permet de sélectionner une topologie ou une configuration pour le réseau. La topologie est influencée par des considérations géographiques, mais également par d'autres besoins, tels que la disponibilité.

Lorsque les points d'extrémité et les liaisons ont été choisis, la bande passante nécessaire peut être estimée. Le trafic sur les liaisons peut présenter divers besoins en matière de latence et de gigue. Une fois la disponibilité de la bande passante déterminée, des technologies de liaison appropriées doivent être sélectionnées.

Enfin, les coûts d'installation et d'exploitation du WAN peuvent être déterminés et comparés aux besoins de l'entreprise ayant nécessité l'installation du WAN.

Remarque : Il est également nécessaire d'effectuer une surveillance et une réévaluation constantes après l'installation du WAN, afin de maintenir des performances optimales.



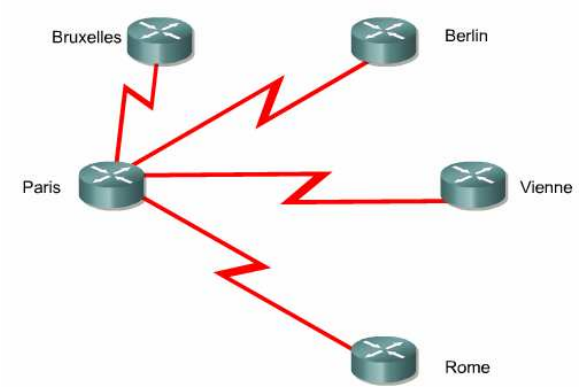
Identification et sélection des fonctionnalités du réseau :

De nombreux WAN s'appuient sur une topologie en étoile. Les points d'extrémité de l'étoile sont parfois interconnectés, en une topologie maillée ou à maillage partiel.

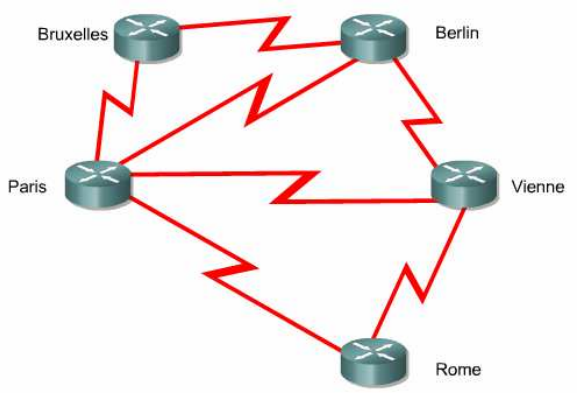
Pour la sélection d'une configuration, plusieurs facteurs doivent être pris en compte. *Un nombre plus important de liaisons augmente le coût des services de réseau*, alors que *plusieurs chemins entre les destinations augmentent la fiabilité*. En revanche, *l'ajout d'équipements de réseau sur le chemin des données augmente la latence et réduit la fiabilité.*

Les technologies qui demandent l'établissement d'une connexion avant que les données ne puissent être transmises, tels que le téléphone analogique, RNIS ou X.25 ne sont pas adaptées aux WAN qui nécessitent des temps de réponse rapides ou une faible latence.

Remarque : Un WAN typique utilise une combinaison de technologies généralement choisies en fonction du type et du volume de trafic.



Topologie en étoile



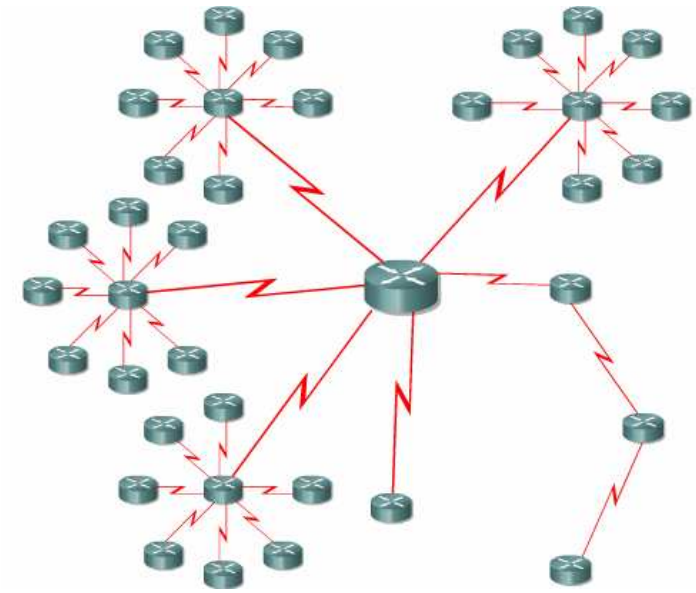
Topologie à maillage partiel

Modèle de conception à trois couches :

Une approche systématique s'avère nécessaire quand un grand nombre de sites doivent être contactés. Une solution hiérarchique à trois couches offre de nombreux avantages.

Imaginons une entreprise opérationnelle dans chaque pays de l'Union Européenne et disposant d'une filiale dans chaque ville de plus de 10 000 habitants. Chaque filiale a un réseau et il a été décidé d'interconnecter les filiales. Un réseau maillé n'est évidemment pas réalisable, car un nombre de liaisons proche de 500 000 serait nécessaire pour les 900 centres. Une étoile simple sera difficile à mettre en œuvre, car elle nécessite un routeur disposant de 900 interfaces au niveau du concentrateur ou d'une interface unique transportant 900 circuits virtuels vers un réseau à commutation de paquets.

Au lieu de cela, envisagez plutôt un modèle de conception hiérarchique. Les réseaux regroupés dans une zone sont interconnectés, plusieurs zones sont interconnectées pour constituer une région et les diverses régions sont interconnectées pour former le noyau du WAN.



La zone peut être fondée sur le nombre de sites à connecter, avec une limite supérieure d'entre 30 et 50. La zone peut adopter une topologie en étoile, les concentrateurs des étoiles étant reliés pour former la région.

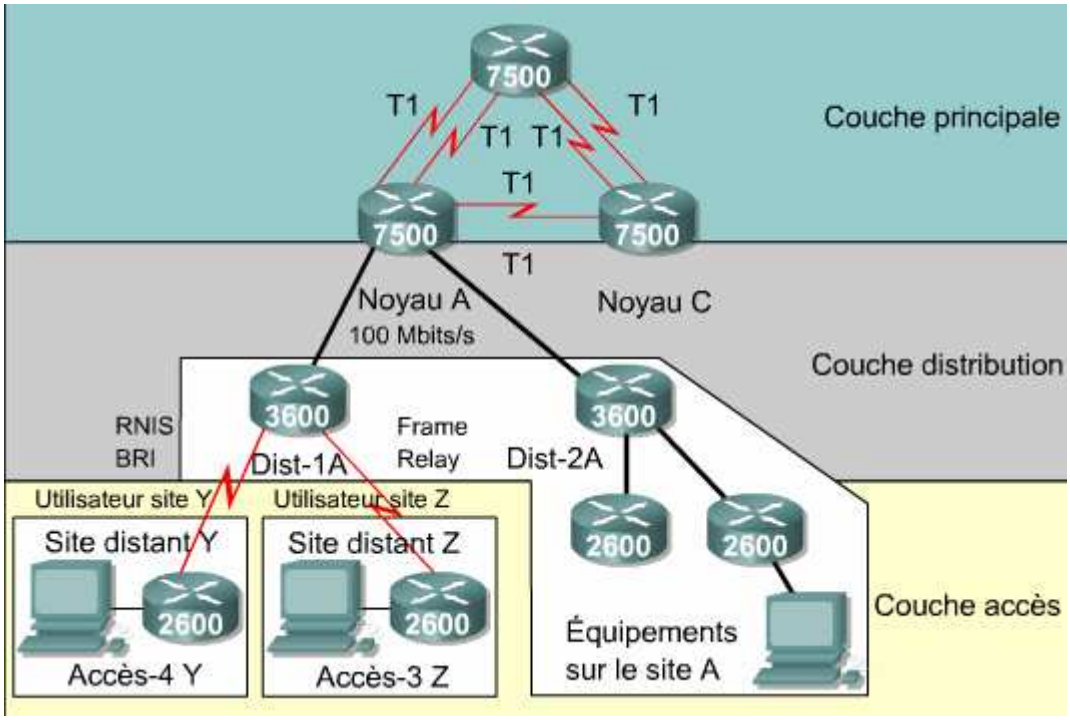
Remarque : Frame Relay facilite le maillage pour la redondance, sans demander l'ajout de connexions physiques supplémentaires. Les liaisons de distribution peuvent être de technologie Frame Relay ou ATM et le noyau du réseau peut être une ligne ATM ou louée.

Autres modèles à conception en couches :

De nombreux réseaux ne nécessitent pas la complexité d'une hiérarchie à trois couches complète. Il est possible d'utiliser des hiérarchies plus simples.

S'il existe un besoin de concentration géographique, une conception a deux niveaux s'avère appropriée. Ceci produit un motif en «étoile des étoiles». Ici encore, ce modèle, fondé sur la technologie des lignes louées, est considérablement différent de celui fondé sur la technologie Frame Relay.

Remarque : Lors de la planification de réseaux plus simples, le modèle à trois couches doit toujours être envisagé, car il offre une meilleure évolutivité au réseau.



Autres considérations liées à la conception de WAN :

De nombreux WAN d'entreprise ont des connexions à ***Internet***. Ceci pose des problèmes de sécurité, mais offre également d'autres possibilités pour le trafic inter-filiales.

Lorsque les volumes de trafic sont relativement faibles, Internet peut servir de WAN d'entreprise et transporter tout le trafic inter-filiales.

Module 3

PPP


Keep Connection to Share Information
NAMIRO
Keep Connection to Share Information

Liaisons série point à point :

Présentation des communications série :

Les technologies des réseaux WAN s'appuient sur une transmission série au niveau de la couche physique. Cela signifie que les bits d'une trame sont transmis un par un sur le support physique.

Les méthodes de signalisation sont notamment ***NRZ-L*** (*Nonreturn to Zero Level*), ***HDB3*** (*High Density Binary 3*) et ***AMI*** (Alternative Mark Inversion). Il ne s'agit que d'exemples de normes de codage de la couche physique.

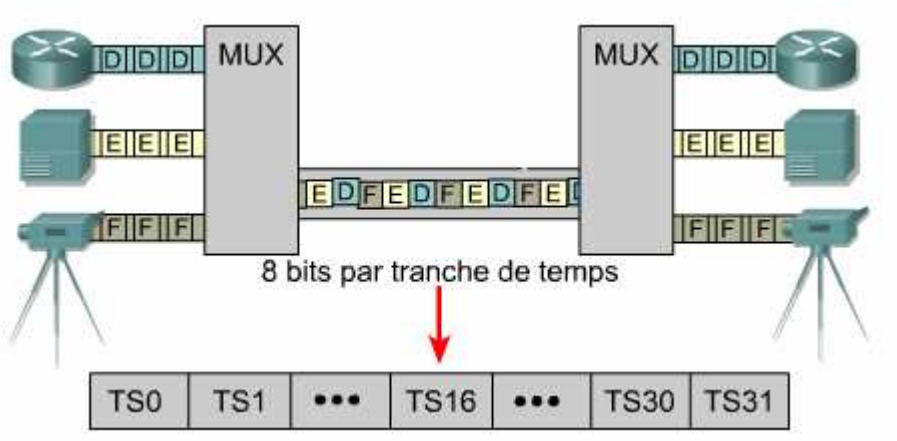
Parmi les nombreuses normes de communication série, on trouve les suivantes:

- RS-232-E
- V.35
- HSSI (High Speed Serial Interface)

Multiplexage temporel

Le ***multiplexage temporel*** (***TDM*** – *Time-division multiplexing*) désigne la *transmission de plusieurs sources d'informations sur un canal, ou signal, commun*, puis la reconstruction des flux d'origine à l'extrémité distante.

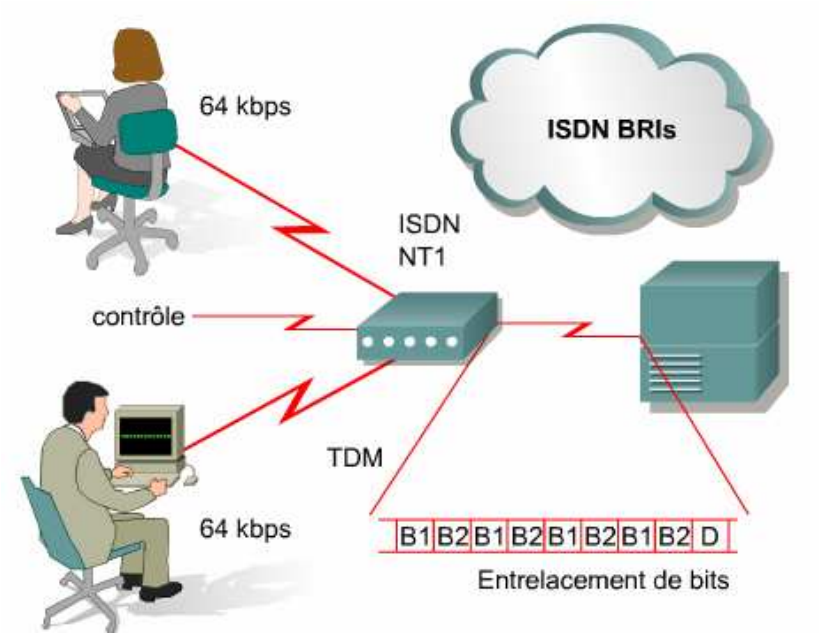
Tout d'abord, un bloc d'informations est prélevé de chaque canal d'entrée. La taille de ce bloc peut varier, mais il s'agit généralement d'un bit ou d'un octet. Selon que des bits ou des octets sont utilisés, ce type de TDM est appelé ***entrelacement*** de *bits* ou entrelacement d'*octets*.



Chacun des trois canaux d'entrée a sa propre capacité. Pour que le canal de sortie puisse accepter les informations provenant des trois entrées, sa capacité ne doit pas être inférieure au total de ces entrées.

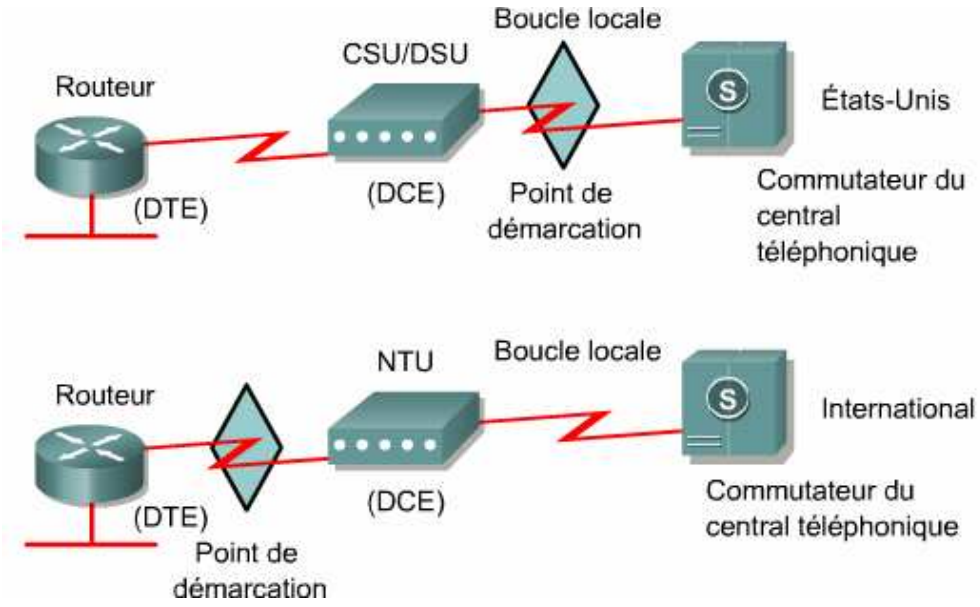
TDM agit au niveau de la couche physique, Il est indépendant du protocole de couche 2 qui a été utilisé par les canaux d'entrée.

Le réseau RNIS (*Réseau numérique à intégration de services*) est un exemple de TDM. RNIS accès de base (BRI) comporte trois canaux, à savoir deux canaux B à 64 kbits/s (B1 et B2) et un canal D à 16 kbits/s. Le TDM comporte neuf intervalles de temps, qui se répètent. Dans les autres pays du monde, l'unité de terminaison de réseau (***NTU***) est fournie et gérée par l'opérateur téléphonique.



Point de démarcation :

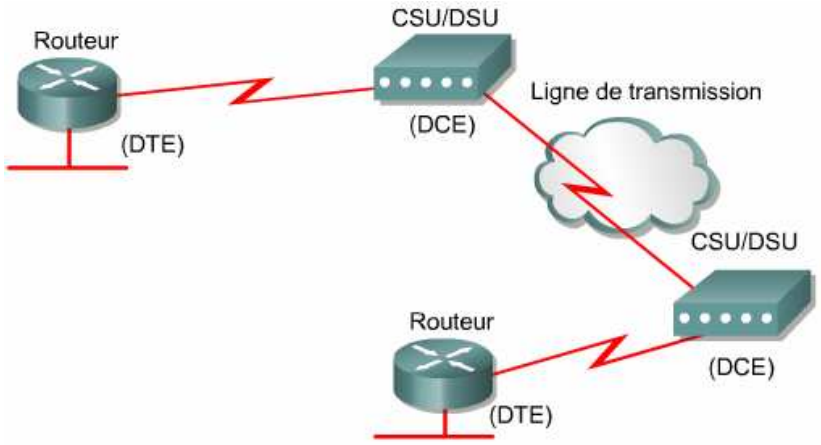
Le point de démarcation de service est le point du réseau où la responsabilité du fournisseur d'accès, ou opérateur téléphonique, prend fin.



ETCD/ETTD

Une ***connexion série comporte*** un équipement terminal de traitement de données (*ETTD*) à une extrémité de la connexion et un équipement de communication de données (*ETCD*) à l'autre extrémité.

Le CPE, généralement un routeur, constitue l'ETTD. L'ETCD, généralement un modem ou une unité CSU/DSU, est l'équipement servant à convertir les données utilisateur de l'ETTD en une forme compatible avec la liaison de transmission du fournisseur d'accès au WAN.



De nombreuses normes ont été développées pour permettre aux ETTD de communiquer avec les ETCD.

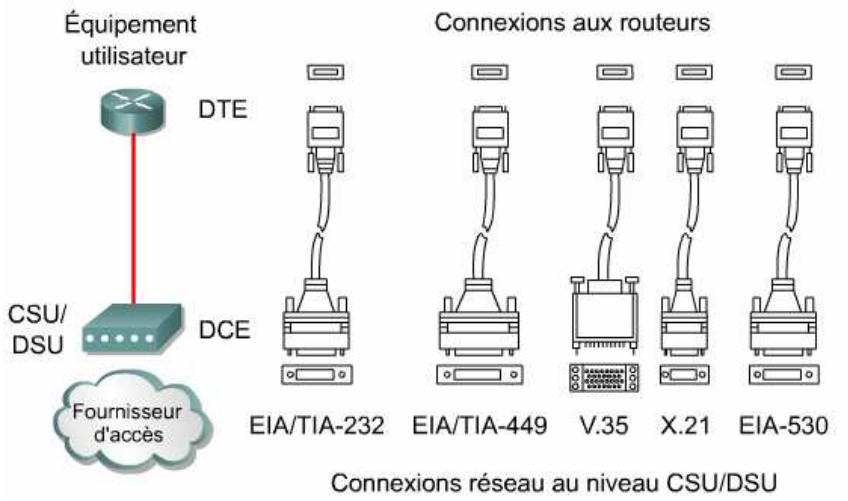
→ *L'ITU-T* : désigne l'ETCD comme l'équipement terminal de circuit de données.
→ *L'EIA* : désigne l'ETCD comme l'équipement de communication de données

L'interface ETCD/ETTD d'une norme particulière définit les *spécifications* :

- ***Mécanique/physique*** – Nombre de broches et type de connecteur
- ***Électrique*** – Définit les niveaux de tension pour 0 et 1
- ***Fonctionnelle*** – Spécifie les fonctions des lignes de signalement de l'interface
- ***Procédurale*** – Spécifie la séquence d'événements pour la transmission des données

Si deux ETTD doivent être interconnectés, comme deux ordinateurs ou deux routeurs, un câble spécial, appelé «***null-modem***», s'avère nécessaire pour se dispenser d'un ETCD.

Le fournisseur du WAN ou l'unité CSU/DSU dicte généralement le type de câble requis. Les équipements Cisco prennent en charge les normes série EIA/TIA-232, EIA/TIA-449, V.35, X.21 et EIA/TIA-530.



Pour prendre en charge des densités plus élevées avec un encombrement réduit → Cisco a créé le câble série intelligent (Smart Serial cable) « un connecteur 26 broches »

Encapsulation HDLC

À l'origine, les communications série étaient fondées sur des protocoles orientés caractères. Les protocoles orientés Bits étaient plus efficaces, mais étaient également *propriétaires*.

En 1979, l'ISO accepta HDLC, qui est un protocole de couche liaison de données, comme une norme orientée bits qui encapsule les données sur des liaisons série synchrones. Depuis 1981, ITU-T a développé une série de protocoles dérivés de HDLC.

- ***LAPB*** (*Link Access Procedure*), for X.25
- ***LAPD*** (*Link Access Procedure – D channel*) pour RNIS
- ***LAPM*** (Link Access Procedure for Modems) et ***PPP*** pour les modems
- ***LAPF*** (*Link Access Procedure for Frame Relay*) pour Frame Relay

HDLC utilise une transmission série synchrone offrant des communications sans erreurs entre deux points. HDLC définit une structure de tramage de couche 2 permettant un contrôle de flux et d'erreurs au moyen d'accusés de réception et d'un schéma de fenêtrage.

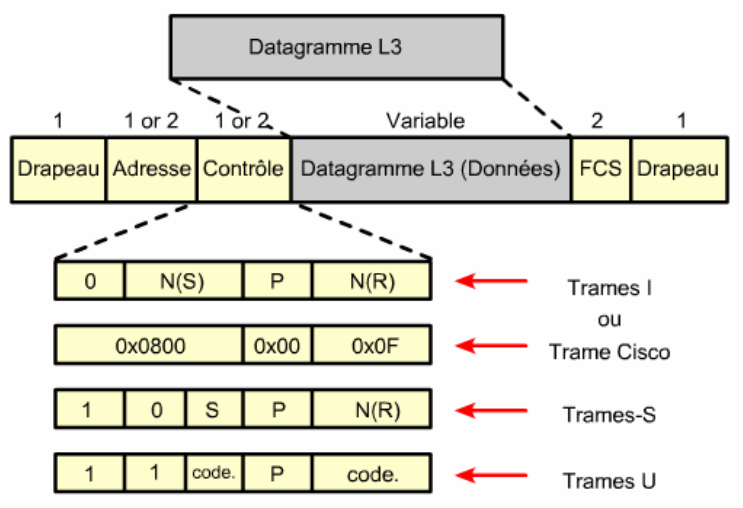
Le protocole HDLC ne prend pas en charge plusieurs protocoles sur une seule liaison, → Cisco offre une version propriétaire de HDLC. La trame HDLC de Cisco utilise un champ « ***type*** » propriétaire servant de champ de protocole. Ce champ permet à plusieurs protocoles de couche réseau de partager la même liaison série.

HDLC définit les trois types de trame, chacune présentant un format de champ de contrôle différent:

- **Les trames d'information (Trames I)** – Transportent les données à transmettre pour la station. Elles offrent un contrôle de flux et d'erreurs supplémentaire et les données peuvent être superposées sur une trame d'informations.

- **Les trames de supervision (Trames S)** – Fournissent des mécanismes de requête/réponse quand la superposition n'est pas utilisée.
- **Trames non-numérotées (Trames U)** – Fournissent des fonctions supplémentaires de contrôle des liaisons, telles que la configuration de connexion. Le champ de code définit le type de trame U.

Les un ou deux premiers bits du champ de contrôle servent à identifier le type de trame.



Configuration de l'encapsulation HDLC

Cisco HDLC est la méthode d'encapsulation par défaut utilisée par les équipements Cisco sur des lignes série synchrones.

Router(config-if)#**encapsulation hdlc** → Utiliser HDLC comme protocole sur l'interface serial

Dépannage d'une interface série

Show interfaces serial → présentent des informations spécifiques aux interfaces série.

```
Router#show interfaces s0/0
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.108.156.98, subnet mask is
255.255.255.240
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set
(10 sec)
```

Show controllers → indique l'état des canaux de l'interface et signalent la présence ou l'absence d'un câble.

```
Router#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x81414E2C, driver data structure at 0x8141753C
SCC Registers:
```

Si la sortie de l'interface électrique apparaît comme *UNKNOWN*, au lieu de V.35, EIA/TIA-449, ou un autre type d'interface électrique, c'est probablement un câble mal connecté qui est à l'origine du problème.

Debug serial interface → Vérifie si les paquets de veille HDLC s'incrémentent. S'ils ne s'incrémentent pas, il existe probablement un problème de synchronisation sur la carte d'interface ou le réseau.

Debug frame-relay lmi → Récupère des informations sur l'interface LMI, afin de déterminer si un commutateur Frame Relay et un routeur envoient et reçoivent des paquets LMI.

Debug frame-relay events → Détermine si des échanges se produisent entre un routeur et un commutateur Frame Relay.

Debug ppp negotiation → Montre les paquets PPP transmis au démarrage de PPP, au moment où les options PPP sont négociées.

Debug ppp packet → Montre les paquets PPP envoyés et reçus. Transferts de paquets à bas niveau

Debug ppp → Montre les erreurs PPP, telles que les trames illégales ou déformées, associées à la négociation et à l'utilisation de la connexion PPP.

Debug ppp authentication → Montre les échanges de paquets PPP CHAP et PAP.

Authentification PPP

Architecture multicouche PPP

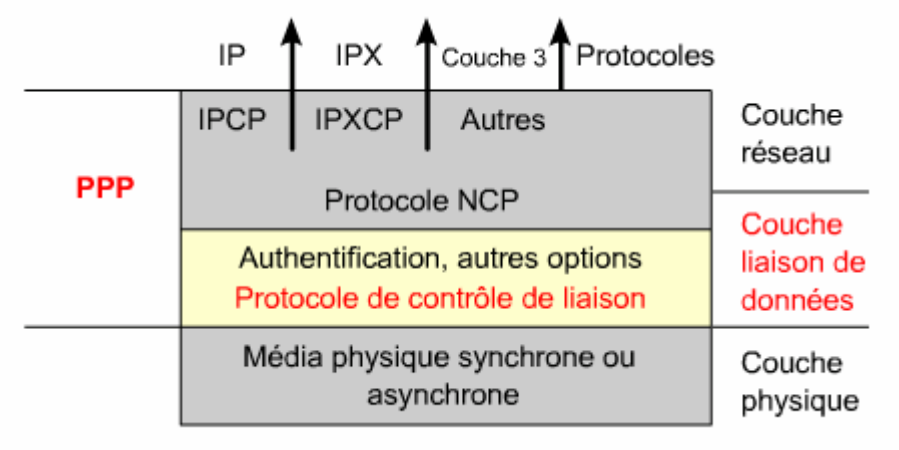
PPP utilise une architecture multicouche facilitant la communication entre des couches interconnectées.

PPP fournit une *méthode d'encapsulation des datagrammes multiprotocoles* sur une liaison point-à-point et utilise la couche de liaison de données pour tester la connexion.

PPP est constitué de deux sous-protocoles :

- Le protocole de contrôle de liaison **(*LCP* *Link Control Protocol*)** – Utilisé pour établir la liaison point-à-point.

- Le protocole de contrôle réseau **(*NCP* *Network Control Protocol*)** – Utilisé pour configurer les divers protocoles de couche réseau.



PPP peut être configuré sur les types suivants d'interfaces physiques:

- *Série asynchrone*
- *Série synchrone*
- *HSSI* (*High Speed Serial Interface*)
- *RNIS* (*Réseau Numérique à Intégration de Services*)

PPP utilise également ***LCP*** pour accepter automatiquement des options de format d'encapsulation, telles que:

Caractéristiques	Fonctionnement	Protocole
Authentification	Demandez un mot de passe et effectuez les échanges confirmés	PAP CHAP
Compression	Compressez les données à la source et reproduisez-les à la destination	Stacker, Predictor, en-tête TCP ou MPPC
Détection d'erreurs	Surveillez les données placées sur la liaison, évitez les boucles de trame	Quality Magic Number
Multiliaison	Équilibrage de charge sur plusieurs liaisons	Protocole multiliaisons (MP)

LCP effectue également les opérations suivantes:

- Il gère les limites variables de taille de paquets
- Il détecte les erreurs de configuration courantes
- Il met fin à la liaison
- Il détermine si une liaison fonctionne correctement ou présente des défaillances

Avec PPP, plusieurs protocoles de couche réseau peuvent fonctionner sur la même liaison de communications. Pour chaque protocole de couche réseau utilisé, un protocole de

contrôle réseau (***NCP***) est fourni. Par exemple, le protocole IP (Internet Protocol) utilise le protocole de contrôle IP (IPCP).

Une trame de l'interface PPP comporte les champs suivants:

- **Drapeau** – Indique le début ou la fin d'une trame et comprend la séquence binaire 01111110.
- **Adresse** – Comprend l'adresse de broadcast standard composée de la séquence binaire 11111111. Le protocole PPP n'attribue pas d'adresse de station individuelle.
- **Contrôle** – Comprend un octet composé de la séquence binaire 00000011, qui appelle la transmission des données utilisateur dans une trame non séquencée.
- **Protocole** – Comprend deux octets qui identifient le protocole encapsulé dans le champ de données de la trame.
- **Données** – Comprend zéro ou plusieurs octets contenant le datagramme du protocole précisé dans le champ de protocole. La longueur maximale par défaut du champ de données est de 1500 octets.
- **FCS** – Normalement, 16 bits ou 2 octets faisant référence aux caractères supplémentaires ajoutés à une trame à des fins de contrôle d'erreur.

Établissement d'une session PPP

- Phase d'établissement de la liaison
- Phase d'authentification facultative
- Phase de configuration du protocole de couche réseau

Les trois catégories de trames LCP ci-dessous sont utilisées au cours d'une session PPP :

- *Les trames d'établissement de liaison* permettent d'établir et de configurer une liaison.
- *Les trames de fermeture de liaison* permettent de fermer une liaison.
- *Les trames de maintenance de liaison* permettent de gérer et de déboguer une liaison.

Phase d'établissement de liaison – Au cours de cette phase, chaque équipement PPP envoie des trames LCP pour configurer et tester la liaison de données. Les trames LCP comprennent un champ d'option de configuration qui permet aux unités de négocier l'utilisation des options, telles que l'unité de transfert d'information maximale (MTU), la compression de certains champs PPP et le protocole d'authentification de la liaison. Cette phase se termine par l'envoi et la réception d'une trame d'accusé de réception de la configuration.

Phase d'authentification (facultative) – Une fois la liaison établie et le protocole d'authentification sélectionné, l'homologue peut être authentifié. Dans le cadre de cette phase, LCP permet également d'effectuer un test facultatif de détermination de qualité de la liaison.

Phase de protocole de couche réseau – Pendant cette phase, les équipements PPP envoient des paquets NCP pour choisir et configurer un ou plusieurs protocoles de couche réseau, par exemple : IP.

Si le protocole LCP ferme la liaison, il en informe les protocoles de couche réseau afin qu'ils prennent les mesures qui s'imposent.

Show interfaces → montre les états des trames LCP et NCP sous la configuration PPP.

La liaison PPP reste configurée pour les communications jusqu'à ce que l'un des événements ci-dessous survienne:

- Les trames LCP ou NCP ferment la liaison.
- Une horloge d'inactivité expire.
- Un utilisateur intervient.

Protocoles d'authentification PPP

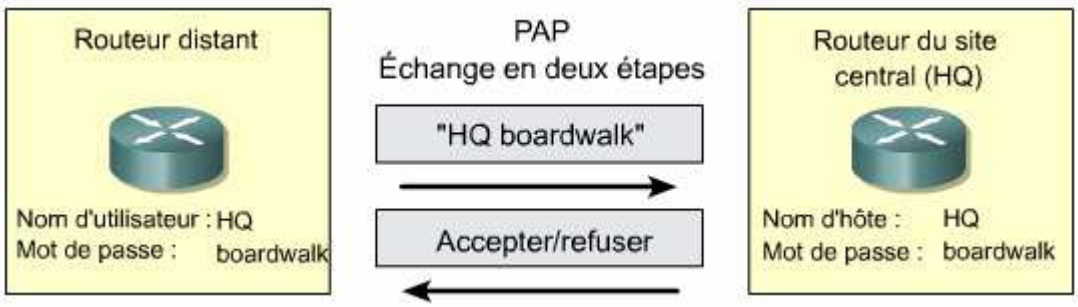
Lors de la configuration de l'authentification PPP, l'administrateur réseau peut sélectionner le protocole d'authentification de mot de passe (PAP) ou le protocole d'authentification à échanges confirmés (CHAP). « CHAP est préférable ».

Protocole d'authentification du mot de passe (PAP)

PAP procure une méthode simple permettant à un nœud distant d'établir son identité à l'aide d'un échange en deux étapes.

Une fois la phase d'établissement de la liaison PPP terminée, la combinaison nom d'utilisateur/mot de passe est envoyée de façon répétée par le nœud distant sur la liaison, jusqu'à ce que l'authentification soit confirmée ou que la connexion soit interrompue.

En effet, les mots de passe sont transmis en clair sur la liaison et il n'offre aucune protection contre la lecture répétée des informations ou les attaques répétées par essais et erreurs.

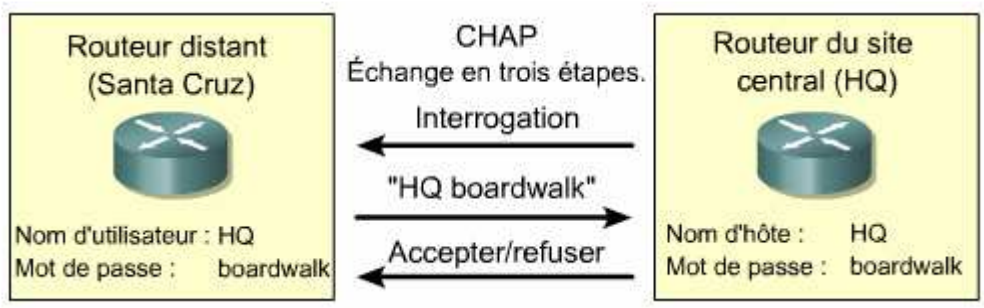


Protocole d'authentification à échanges confirmés (CHAP)

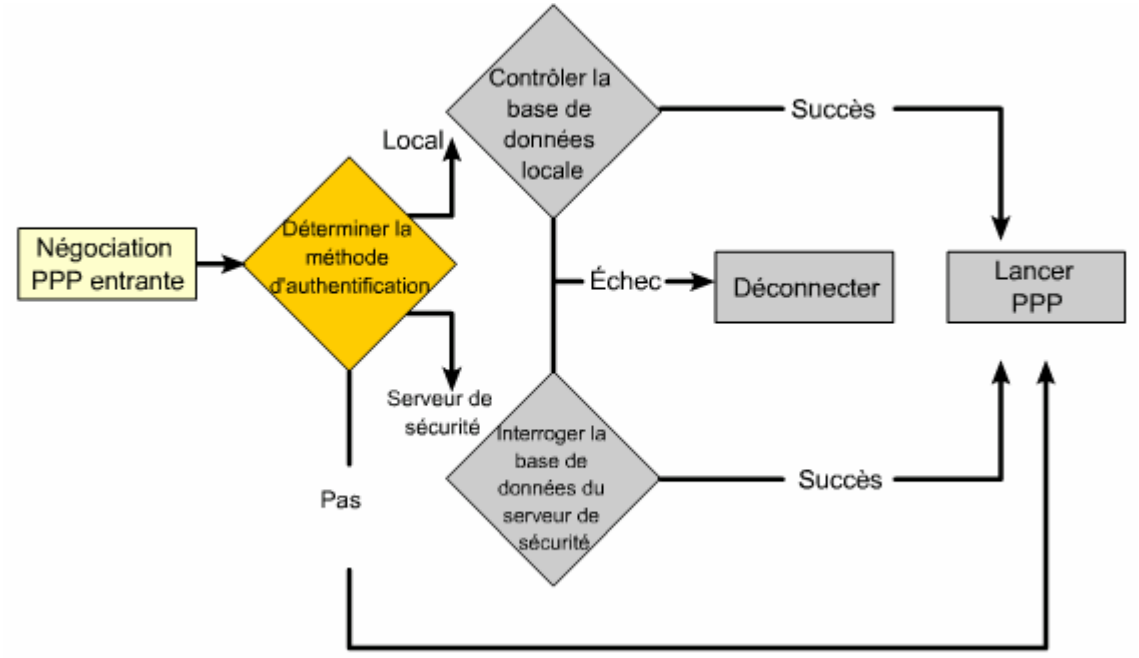
CHAP s'utilise au démarrage d'une liaison et vérifie régulièrement l'identité du nœud distant au moyen d'un échange en trois étapes. CHAP s'effectue à l'établissement initial de la liaison et se répète pendant la durée de cette liaison.

Une fois la phase d'établissement de la liaison PPP terminée, le routeur local envoie un message de demande de confirmation au nœud distant. Le nœud distant répond par une valeur calculée au moyen d'une fonction de hachage unidirectionnelle, généralement l'algorithme MD5.

Le protocole CHAP protège contre les attaques de lecture répétée des informations passant par le modem en utilisant une valeur de confirmation variable, unique et imprévisible. Les demandes de confirmation répétées visent à limiter la durée d'exposition à toute attaque. Le routeur local ou un serveur d'authentification externe contrôle la fréquence et la durée des demandes de confirmation.



Processus d'authentification et d'encapsulation PPP



Configuration PPP :

Configuration de PPP

Encapsulation ppp → Configurer PPP sur une interface serial (mode d'interface)

Compress [predictor | stac] → Configurer la compression désiré (mode d'interface)

Remarque : La compression n'est pas recommandée si le trafic est essentiellement constitué de fichiers compressés.

Ppp quality percentage → Surveiller les données reçues sur la liaison et éviter que la trame ne tourne en boucle (mode d'interface).

Ppp multilink → Procéder à un équilibrage de la charge sur plusieurs liaisons (interface)

Configuration de l'authentification PPP

Username {nom du routeur de l'autre extrémité} password {secret} → définir le nom d'utilisateur et le mot de passe sur chaque routeur (mode de configuration globale).

Ppp authentication {chap | chap pap | pap chap | pap} → définir le type d'authentification désiré (mode d'interface).

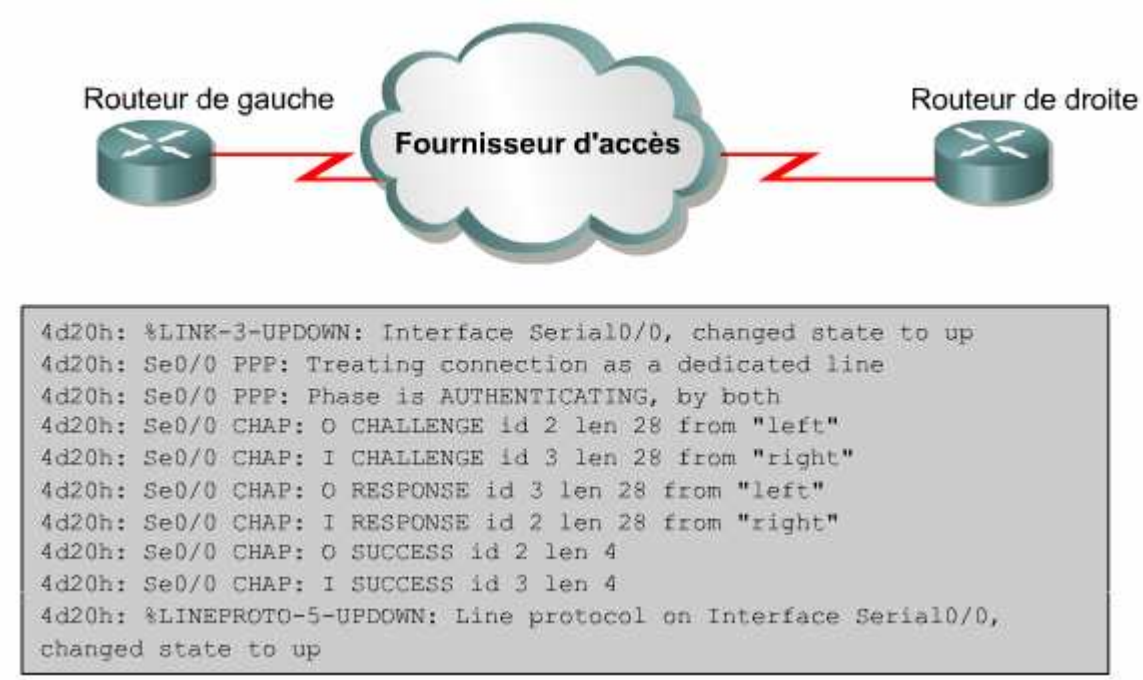
Ppp pap sent-username {nom} password {mdp} → Activer PAP sur l'interface.

Vérification de la configuration de l'encapsulation PPP série

Show interfaces → affiche des statistiques sur toutes les interfaces.

Dépannage de la configuration de l'encapsulation série

Debug ppp authentication → Déboguer le processus d'authentification PAP ou CHAP.




```
4d20h: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
4d20h: Se0/0 PPP: Treating connection as a dedicated line
4d20h: Se0/0 PPP: Phase is AUTHENTICATING, by both
4d20h: Se0/0 CHAP: O CHALLENGE id 2 len 28 from "left"
4d20h: Se0/0 CHAP: I CHALLENGE id 3 len 28 from "right"
4d20h: Se0/0 CHAP: O RESPONSE id 3 len 28 from "left"
4d20h: Se0/0 CHAP: I RESPONSE id 2 len 28 from "right"
4d20h: Se0/0 CHAP: O SUCCESS id 2 len 4
4d20h: Se0/0 CHAP: I SUCCESS id 3 len 4
4d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0,
changed state to up
```

Affichage	Description
Se0/0 PPP : Phase is AUTHENTICATING, by both	Authentification bidirectionnelle
Se0/0 PPP : O AUTH-REQ id 4 len 18 from "left"	Requête d'identification sortante
Se0/0 PPP : O AUTH-REQ id 1 len 18 from "right"	Requête d'authentification entrante
Se0/0 PPP : Authenticating peer right	Authentification entrante
Se0/0 PPP : O AUTH-ACK id 1 len 5	Accusé de réception sortant
Se0/0 PPP : O AUTH-ACK id 4 len 5	Accusé de réception entrant

Debug ppp {authentication | packet | negotiation | error | chap}

Commande	Description
packet	S'utilise avec la commande **debug ppp** pour afficher les paquets PPP envoyés et reçus
negotiation	S'utilise avec la commande **debug ppp** pour afficher les paquets PPP transmis au démarrage de PPP, où les options PPP sont négociées
error	S'utilise avec la commande **debug ppp** pour afficher les erreurs de protocole et les statistiques d'erreur associées à la négociation et à l'utilisation de la connexion PPP
chap	S'utilise avec la commande **debug ppp** pour afficher les échanges de paquets CHAP (Challenge Authentication

Module 4

RNIS & DDR

Concepts RNIS :

Présentation de RNIS :

Le RTPC traditionnel s'appuyait sur une connexion analogique entre les locaux du client et l'échange local, également appelée boucle locale.
→ Les circuits analogiques limitent la BP qui peut être obtenue sur la boucle locale.

Les restrictions des circuits ne permettent pas d'accepter les bandes passantes supérieures à environ 3000 Hz.

La technologie ***RNIS*** permet d'utiliser des données numériques sur la boucle locale, et ainsi d'offrir de meilleurs débits aux utilisateurs distants.

La technologie RNIS s'utilise généralement pour le télétravail et pour connecter les petits bureaux distants au réseau local de l'entreprise.

Les ***normes RNIS*** définissent le matériel et les méthodes d'établissement des appels assurant une connectivité numérique de bout en bout.

Avantages de RNIS :

- L'acheminement d'une grande diversité de signaux de trafic utilisateur, notamment données, voix et vidéo
- L'établissement des appels beaucoup plus rapide qu'avec une connexion modem grâce au canal D.
- Un meilleur taux de transfert que les modems grâce aux canaux B
- L'adaptation des canaux B aux liaisons PPP (*Point-to-Point Protocol*) négociées

Normes et méthodes d'accès

L'établissement des premières normes RNIS date de la fin des années 1960. Une série complète de recommandations relatives aux réseaux RNIS a été publiée en 1984 par l'UIT-T :

Objet	Protocole	Exemples clés
Réseau téléphonique et RNIS	Série E	E.164 – Plan de numérotation téléphonique international
Concepts, aspects et interfaces RNIS	Série I	I.100 Série - Concepts, Structures, Terminologie I.400 – Interfaces utilisateur-réseau
Commutation et signalisation	Série Q	Q.921 – Protocole de liaison LAPD Q.931 – Couche réseau RNIS entre le terminal et le commutateur

Les normes RNIS définissent deux principaux types de ***canaux*** :

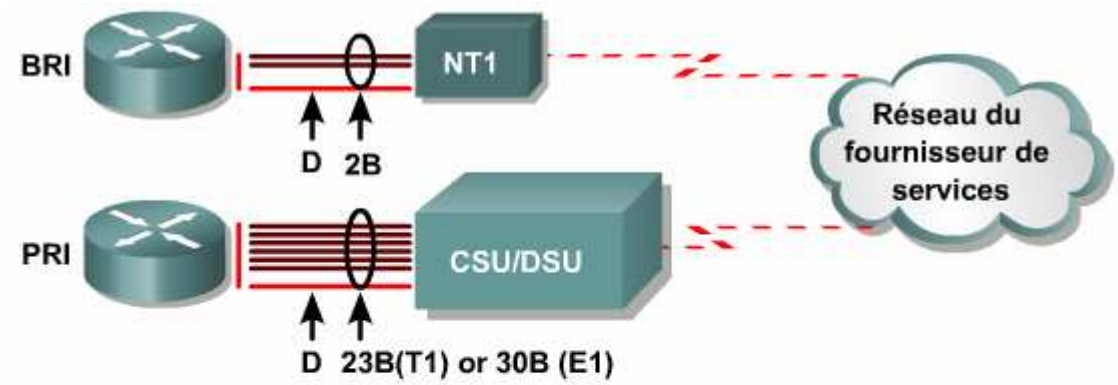
➔ Le canal Bearer (B), est défini comme un chemin numérique entièrement dégagé de 64 Kbits/s (il peut servir à *transmettre n'importe quel type de données numériques* en mode full-duplex)

➔ Le canal delta (D) peut y avoir 16 kbits/s pour l'accès de base BRI ou 64 kbits/s pour l'accès primaire PRI. Il sert à *acheminer des informations de contrôle* pour le canal B.

Remarque : La technologie RNIS fait appel à un canal séparé pour les informations de contrôle, le canal D. C'est ce que l'on appelle la signalisation hors bande.

La norme RNIS spécifie deux ***méthodes d'accès*** standard, à savoir BRI et PRI :

➔ BRI utilise deux canaux B à 64 kbits/s, plus un canal D à 16 kbits/s (2B+D).



Canal	Capacité	Utilisé principalement pour
B	64 kbps	Les données à commutation de circuits (HDLC, PPP)
D	16/64 kbps	Les informations de signalisation (LAPD)

Remarque : Le trafic sur le canal D utilise le protocole LAPD (*Link Access Procedure on the D Channel*). LAPD est un protocole de couche de liaison de données fondé sur HDLC.

Modèle en 3 couches et protocoles de la technologie RNIS

La technologie RNIS utilise un ensemble de normes de l'UIT-T portant sur la couche physique, la couche de liaison de données et la couche réseau du modèle de référence OSI.

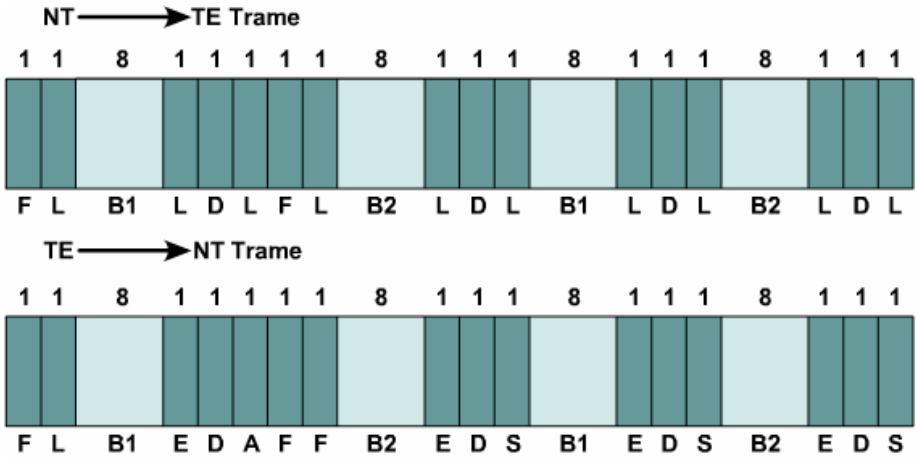
Couche OS	Canal D	Canal B
3	Q.931 – ISDNCouche réseau entre le terminal et le commutateur	IP
2	Q.921 – LAPD (Protocole de liaison LAPD)	PPP HDLC
1	I.430/I.431 - Interface de couche physique RNIS : = I.430 pour l'interface de base = I.431 pour l'interface primaire	

Les informations des trois canaux 2B+D sont multiplexées en un seul chemin physique.

Le format de trame de la couche RNIS physique diffère selon que la trame est entrante ou sortante.

➔ S'il s'agit d'une trame sortante, elle est envoyée du terminal au réseau. Format trame *TE*

➔ Si la trame est entrante, elle est envoyée du réseau au terminal. Format de trame *NT*



Chaque trame contient deux sous-trames, chacune contenant les éléments suivants:

- 8 bits du canal B1
- 8 bits du canal B2
- 2 bits du canal D
- 6 bits de surcharge

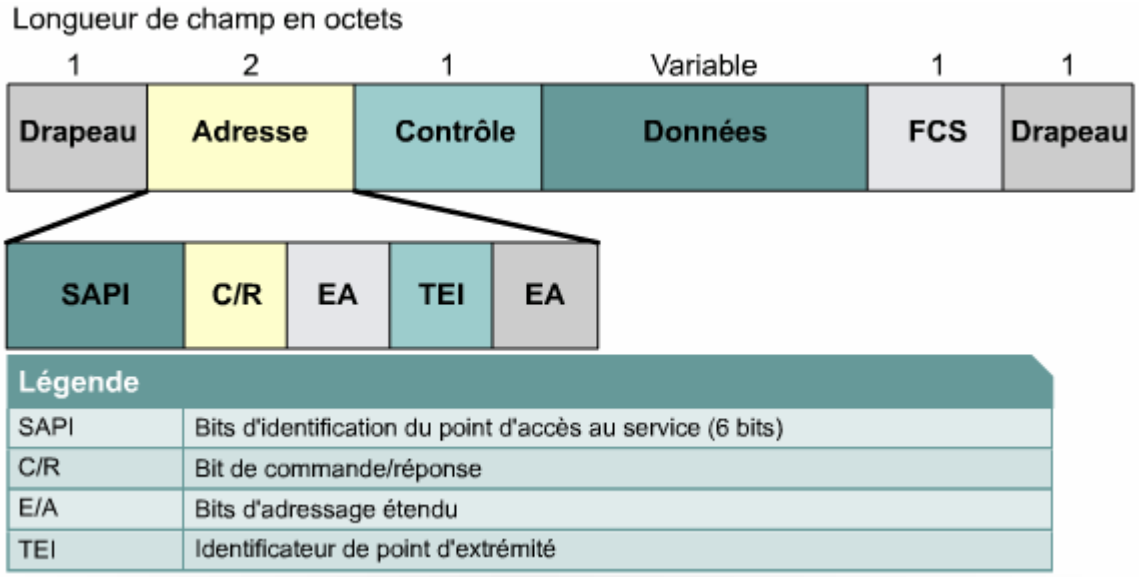
Les trames RNIS BRI contiennent donc 48 bits. Quatre mille de ces trames sont transmises chaque seconde. Chaque canal B, B1 et B2 offre une capacité de 8 * 4000 * 2 = 64 kbits/s. Le canal D a une capacité de 2 * 4000 * 2 = 16 kbits/s. Ceci représente 144 Kbits/s (B2+B1+D) pour un débit binaire total de l'interface physique RNIS BRI de 192 Kbits/s. Le reste du débit est constitué des bits de surcharge requis pour la transmission: 6 * 4000 * 2 = 48 kbits/s.

Les bits de surcharge d'une sous-trame RNIS sont utilisés de la façon suivante:

- **Bit de verrouillage de trame** – Synchronisation

- **Bit d'équilibrage de charge** – Ajustement de la valeur moyenne de bit
- **Écho des bits de canal D précédents** – Résolution des conflits pouvant survenir lorsque plusieurs terminaux sur un bus passif rivalisent pour un canal
- **Bit d'activation** – Activation des équipements
- **Bit de réserve** – Non affecté

Voici la **structure de trame LAPD** :



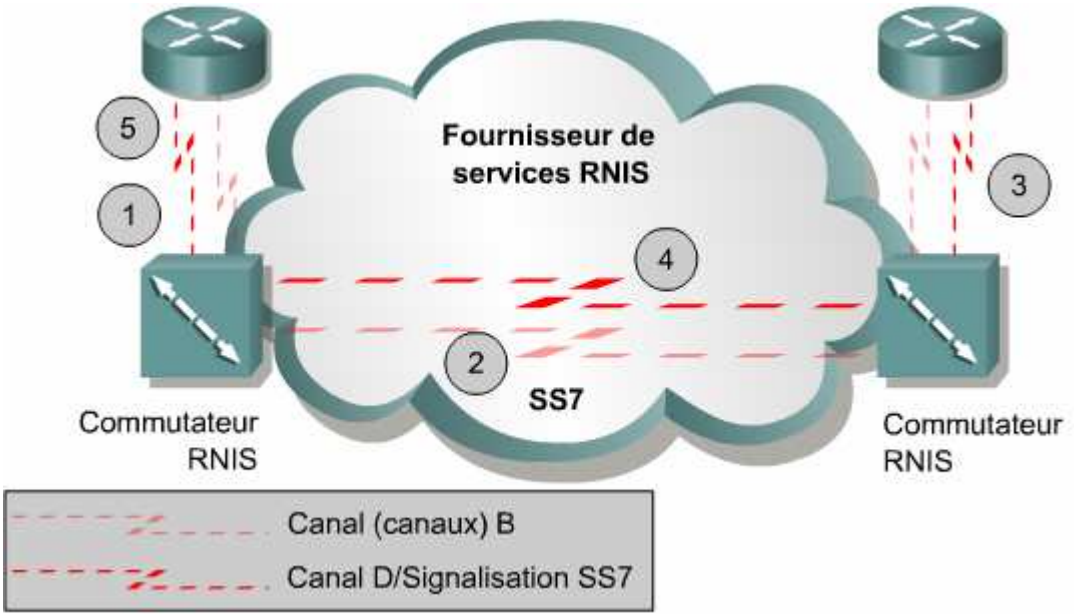
Légende	
SAPI	Bits d'identification du point d'accès au service (6 bits)
C/R	Bit de commande/réponse
E/A	Bits d'adressage étendu
TEI	Identificateur de point d'extrémité

Fonctions RNIS

Plusieurs échanges doivent s'effectuer pour qu'un routeur se connecte à un autre par RNIS. Pour établir une connexion RNIS, c'est le canal D qui est utilisé entre le routeur et le commutateur RNIS. La signalisation SS7 (*Signal System 7*) est utilisée entre les commutateurs du réseau du fournisseur d'accès.

La séquence d'événements ci-dessous s'effectue lors de l'établissement d'une communication BRI ou PRI :

1. Le canal D est utilisé pour envoyer le numéro appelé au commutateur RNIS local.
2. Le commutateur local utilise le protocole de signalisation SS7 pour définir un chemin et transmettre le numéro appelé au commutateur RNIS distant.
3. Le commutateur RNIS distant signale l'appel à la destination sur le canal D.
4. L'équipement RNIS NT-1 de destination envoie un message de connexion d'appel au commutateur RNIS distant.
5. Le commutateur RNIS distant utilise SS7 pour envoyer un message de connexion d'appel au commutateur local.
6. Le commutateur RNIS local connecte un canal B de bout en bout et laisse le deuxième canal B disponible pour une nouvelle conversation ou un transfert de données. Les deux canaux B peuvent être utilisés simultanément.

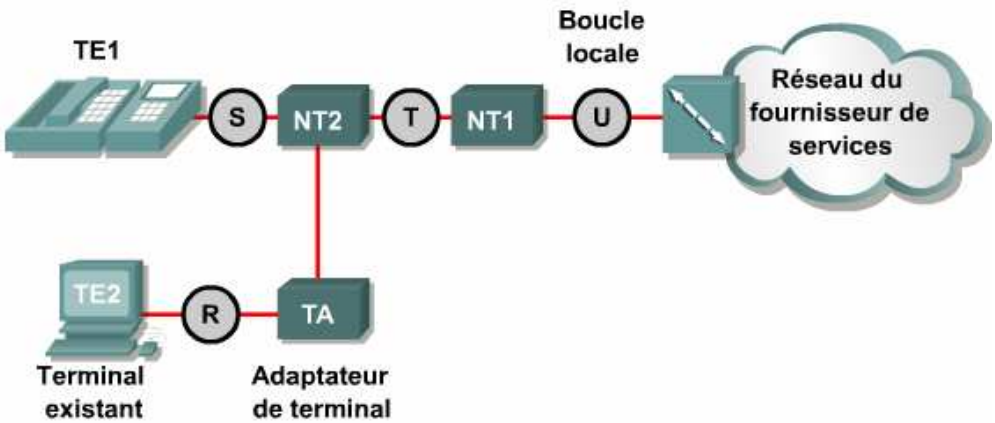


Points de référence RNIS

Les spécifications RNIS définissent quatre points de référence qui connectent un équipement RNIS à un autre. Chaque unité d'un réseau RNIS effectue une tâche spécifique :

- ***R*** – Désigne la connexion entre un équipement terminal de type 2 non compatible RNIS (TE2) et un adaptateur de terminal (TA), par exemple une interface série RS-232.
- ***S*** – Désigne les points qui se connectent dans l'équipement de commutation du client aux terminaisons de réseau de type 2 (NT2) et permettent les appels entre les divers types d'équipements placés chez le client.
- ***T*** – Électriquement identique à l'interface S; désigne la connexion sortante entre la NT2 et le réseau RNIS ou la terminaison de réseau de type 1 (NT1).
- ***U*** – Désigne les connexions entre l'unité de terminaison de réseau de type 1 (NT1) et le réseau RNIS appartenant à la compagnie de téléphone.

Remarque : Comme les références S et T sont similaires, certaines interfaces sont désignées par le sigle ***S/T***.



Détermination de l'interface RNIS du routeur

Aux États-Unis, c'est au client qu'il incombe de fournir la NT1. En Europe et dans d'autres pays, la compagnie téléphonique fournit la fonction NT1 et présente une interface S/T au client. Avec ces configurations, Les équipements tels que les modules et interfaces RNIS d'un routeur doivent être commandés.

Pour sélectionner un routeur Cisco avec l'interface RNIS appropriée :

1. *Déterminez si le routeur prend en charge RNIS BRI*. Recherchez un connecteur BRI ou une carte d'interface BRI WAN (WIC) à l'arrière du routeur.
2. *Déterminez le fournisseur de la NT1*. Une NT1 termine la boucle locale vers le central téléphonique (CO) du fournisseur d'accès RNIS.
3. Si la NT1 est intégrée au CPE, le routeur doit avoir une *interface U*. Si le routeur est équipé d'une interface S/T, il nécessite alors une NT1 externe pour se connecter au fournisseur RNIS.

Si le routeur est doté d'un connecteur libellé BRI, il est déjà compatible RNIS. Avec une interface RNIS native déjà intégrée, le routeur est un TE1 et doit se connecter à une NT1. Si le routeur a une interface U, il dispose également d'une NT1 intégrée.

Si le routeur ne comporte aucun connecteur BRI et qu'il s'agit d'un routeur à configuration fixe ou non modulaire, il doit alors utiliser une interface série existante avec un adaptateur de terminal externe pour fournir la connectivité BRI.

Types de commutateurs RNIS

Les types de commutateurs RNIS varient, partiellement en fonction du pays dans lequel le commutateur est utilisé.

Avant que le routeur ne puisse être connecté à un service RNIS, il doit être configuré pour le type de commutateur utilisé au central téléphonique.

Pays	Type de commutateur
États-Unis et Canada	AT&T 5ESS et 4ESS ; Northern Telecom DMS-100
France	VN2, VN3
Japon	NTT
Royaume-Uni	Net3 et Net5
Europe	Net3

Outre le type de commutateur utilisé par le fournisseur d'accès, il peut également s'avérer nécessaire de connaître les identificateurs de profil de service (SPID – *service profile identifiers*) attribués par l'opérateur téléphonique. Les SPID sont utilisés en Amérique du Nord et au Japon uniquement. L'opérateur RNIS fournit cet identificateur afin de *déterminer la configuration de ligne du service RNIS*. Dans de nombreux cas, les SPID doivent être entrés pendant la configuration d'un routeur.

Configuration RNIS :

Configuration de RNIS BRI

lsdn switch-type {switch-type} → peut être configurée dans le mode de commande global ou d'interface afin de spécifier le commutateur RNIS du fournisseur.

lsdn spid1 {numéro spid} {ldn} et **isdn spid2 {numéro spid} {ldn}** pour spécifier le SPID requis (pour B1 & B2) par le réseau RNIS quand le routeur établit une connexion vers l'échange RNIS local (mode de configuration d'interface)

→ L'argument facultatif **ldn** définit un numéro d'annuaire local

`Router(config)#`**interface bri slot/port** → Pour passer en mode d'interface Bri

Configuration de RNIS PRI

Comme les routeurs se connectent à PRI au moyen d'une ligne T1/E1, aucune commande « **interface pri** » ne s'avère nécessaire. Au lieu de cela, l'interface physique du routeur qui se connecte à la ligne louée est appelée contrôleur T1, ou contrôleur E1. Ce contrôleur doit être configuré correctement pour communiquer avec le réseau de l'opérateur. Les canaux RNIS PRI D et PRI B se configurent séparément à partir du contrôleur, au moyen de la commande **interface serial**

lsdn switch-type {switch-type} → peut être configurée dans le mode de commande global afin de spécifier le commutateur RNIS du fournisseur.

Type de commutateur	Description
primaire-5ess	Commutateurs d'accès de base AT&T (États-Unis)
primaire-dms100	Northern Telecom DMS-100 (Amérique du Nord)
primaire-ni	National ISDN (Amérique du Nord)
primaire-net5	Type de commutateur pour Net5 au Royaume-Uni, en Europe et en Australie
primaire-ntt	Commutateur RNIS NTT (Japon)

La configuration d'un contrôleur T1 ou E1 s'effectue comme suite:

1. indiquez le contrôleur dans lequel la carte PRI réside:

Router(config)#**controller {t1 | e1} {slot/port}**
Router(config-controller)#

2. Configurez le tramage selon les spécifications de l'opérateur.

➔ Pour des lignes T1 :
Router(config-controller)#**framing {sf | esf}**
➔ Pour des lignes E1 :
Router(config-controller)#**framing {crc4 | no-crc4}**

3. Identifier la méthode de signalisation de couche physique :
Router(config-controller)#**linecode {ami | b8zs| hdb3}**

4. Configurez l'interface spécifiée pour l'accès PRI et le nombre de tranches de temps fixes allouées sur l'installation numérique du fournisseur :
Router(config-controller)#**pri-group [time range]**

5. Spécifiez une interface pour le fonctionnement du canal D de l'accès PRI.:
Router(config)#**interface serial {slot/port: | unit:}{23 | 15}**

Exemples :

T1 - Exemple de configuration

```
Router(config)#controller t1 1/0
Router(config-controller)#framing esf
Router(config-controller)#linecode b8zs
Router(config-controller)#pri-group timeslots 1-24

Router(config-controller)#interface serial1/0:23
Router(config-if)#isdn switch-type primary-5ess
Router(config-if)#no cdp enable
```

E1 - Exemple de configuration

```
Router(config)#controller e1 1/0
Router(config-controller)#framing crc4
Router(config-controller)#linecode hdb3
Router(config-controller)#pri-group timeslots 1-31

Router(config-controller)#interface serial1/0:15
Router(config-if)#isdn switch-type primary-net5
Router(config-if)#no cdp enable
```

Vérification de la configuration RNIS

Show isdn status → Pour confirmer le fonctionnement de l'accès BRI, vérifier que l'équipement terminal TE1, ou le routeur, communique correctement avec le commutateur RNIS.

Assurez-vous que la couche 1 présente l'état ACTIVE, et la couche 2, l'état MULTIPLE_FRAME_ESTABLISHED. Cette commande présente également le nombre de communications actives.

```
Cork#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
ACTIVE
    Layer 2 Status:
TEI = 64, Ces = 1, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
TEI = 65, Ces = 2, SAPI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
TEI 64, ces = 1, state = 5(init)
    spid1 configured, no LDN, spid1 sent, spid1 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 1
```

Show isdn active → affiche des informations sur l'appel en cours, notamment les suivantes :

- Le numéro appelé
- La durée de l'appel avant déconnexion
- L'indication du coût
- Les unités de facturation utilisées pendant l'appel
- les informations d'indication du coût fournies pendant ou à la fin des appels

Show dialer → présente des informations sur l'interface de numérotation :

- L'état de la communication en cours
- Les valeurs de l'horloge de ligne téléphonique
- La raison de l'appel
- L'équipement distant connecté

Show interface bri 0/0:1 → renvoie les informations suivantes :

- Le canal B utilise l'encapsulation PPP.
- La trame LCP a été négociée et est ouverte.
- Il y a deux protocoles de contrôle NCP actifs, à savoir IPCP et CDPCP

```
BranchF#show interface bri0/0:1
BRI0:1 is up, line protocol is up
  Hardware is BRI
  MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation PPP, loopback not set, keepalive set
(10 sec)
  LCP Open
  Open: IPCP, CDPCP
  Last input 00:00:01, output 00:00:01, output hang
never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output
drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max
```

Dépannage de la configuration RNIS

```
Router#debug isdn q921
```

Affiche les messages de la couche 2 RNIS

```
Router#debug isdn q931
```

Affiche l'activité d'établissement et d'interruption de communication RNIS de la couche 3

```
Router#debug ppp authentication
```

Affiche les messages du protocole d'authentification PPP

```
Router#debug ppp negotiation
```

Affiche les informations relatives à l'établissement de la liaison PPP

```
Router#debug ppp error
```

Affiche des erreurs de protocole associées au protocole PPP

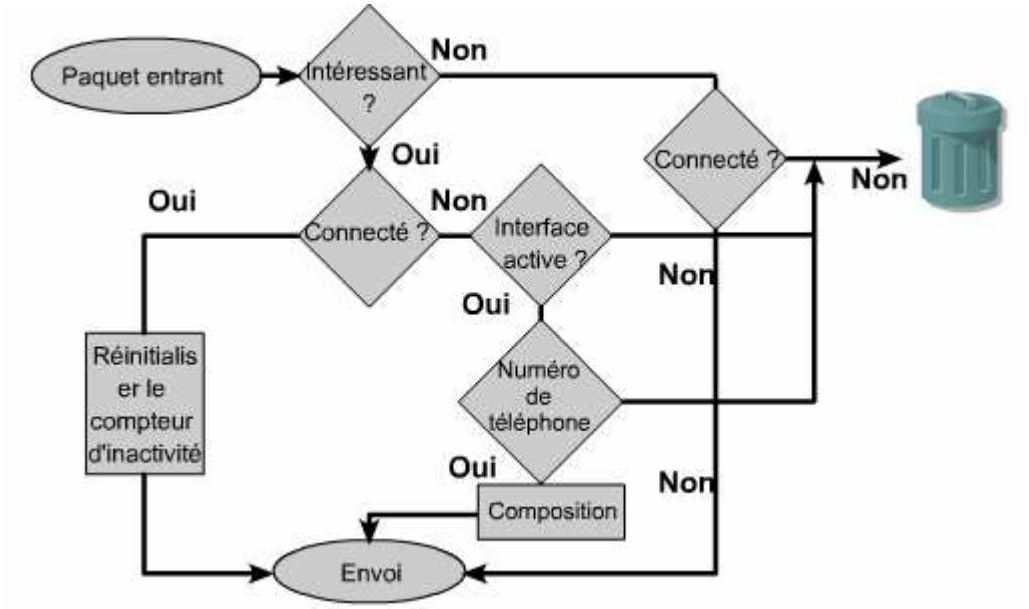
Configuration DDR :

Fonctionnement de DDR

Le *routage à établissement de connexion à la demande* (**DDR** – *Dial-on-demand routing*) se déclenche quand du trafic concordant avec un ensemble de critères prédéfini est mis en file d'attente pour être envoyé sur une interface compatible DDR. Le trafic qui occasionne un appel DDR est appelé ***trafic intéressant***

La procédure ci-dessous permet de mettre en œuvre DDR sur les routeurs Cisco :

1. Définition de la route vers la destination
2. Les paquets intéressants spécifient l'appel DDR
3. Recherche d'informations de numérotation
4. Transmission du trafic
5. La communication prend fin à l'expiration du délai



Configuration du DDR traditionnel

DDR traditionnel est un terme utilisé pour définir une configuration DDR élémentaire, avec laquelle un seul ensemble de paramètres de numérotation est appliqué à une interface.

Pour configurer le DDR traditionnel, procédez comme suit :

- Définissez des routes statiques.
- Spécifiez le trafic intéressant.

- Configurez les informations de numérotation.

Définition de routes statiques pour DDR

Lorsque vous configurez des routes statiques, tenez compte des facteurs ci-dessous:

- Par défaut, une route statique prend la priorité sur une route dynamique, du fait de sa distance administrative plus réduite. Sans configuration complémentaire, une route dynamique vers un réseau est ignorée s'il existe une route statique dans la table de routage pour le même réseau.
- Pour réduire le nombre d'entrées de routes statiques, définissez une route statique résumée ou par défaut.

Spécification du trafic intéressant pour DDR

Le trafic peut correspondre à l'une des définitions ci-dessous :

- Le trafic IP d'un type de protocole particulier
- Les paquets avec une adresse source ou de destination particulière
- Les autres critères définis par l'administrateur réseau

```
Router(config)#dialer-list {dialer-group-num} protocol {protocol-name} {permit | deny | list access-list-number}
```

→ Le paramètre **dialer-group-num** est un nombre entier entre 1 et 10 qui identifie la liste de numérotation pour le routeur.

Exemple :

Avec listes d'accès (pour un contrôle accru)

```
dialer-list 2 protocol ip list 101

access-list 101 deny tcp any any eq ftp      ← Refuser FTP
access-list 101 deny tcp any any eq telnet   ← Refuser Telnet
access-list 101 permit ip any any
```

Tout trafic IP active la liaison, à l'exception de FTP et Telnet

Remarque : La commande **dialer-list 1 protocol ip permit** permet à tout le trafic IP de déclencher un appel.

Configuration des informations de numérotation DDR

→ Configurer l'encapsulation PP sur l'interface appropriée.

→ Une liste de numérotation spécifiant le trafic intéressant pour cette interface DDR doit être associée à cette dernière. Pour ce faire, utilisez la commande **dialer-group {group-number}**

```
interface BRI0
 ip address 10.1.0.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 180
 dialer map ip 10.1.0.2 name Central 5552000
 dialer-group 1
 no fair-queue
 ppp authentication chap
!
router rip
network 10.0.0.0
no ip classless
ip route 10.10.0.0 255.255.0.0 10.1.0.2
ip route 10.20.0.0 255.255.0.0 10.1.0.2
dialer-list 1 protocol ip permit
```

Les deux valeurs doivent correspondre

→ Mapper l'adresse du protocole distant sur un numéro de téléphone.

`Router(config-if)#`**dialer map** **{protocol} {next-hop-address}** `[`**name** *hostname*`] [`**speed 56 | 64**`] [`**broadcast**`]` **{dial-string}**

Dialer idle-timeout {seconds} → Spécifier le nombre de secondes d'inactivité avant la déconnexion d'une communication (par défaut 120 s)

```
hostname Home
!
isdn switch-type basic-5ess
!
username Central password cisco
interface BRI0
 ip address 10.1.0.1 255.255.255.0
 encapsulation ppp
 dialer idle-timeout 180
 dialer map ip 10.1.0.2 name Central 5552000
 dialer-group 1
 no fair-queue
 ppp authentication chap
!
router rip
```

Remarque : Si vous n'appelez qu'un site, utilisez une commande **dialer string** inconditionnelle qui appelle toujours ce numéro de téléphone unique, quelle que soit la destination du trafic.

Profils de numérotation

Le DDR traditionnel est limité, car la configuration est appliquée directement à l'interface physique. Comme l'adresse IP est appliquée directement à l'interface, seules les interfaces DDR configurées dans ce sous-réseau spécifique peuvent établir une connexion DDR avec cette interface.

Les ***profils de numérotation*** suppriment la configuration de l'interface qui reçoit ou effectue des appels et peuvent uniquement lier la configuration à l'interface appel par appel.

Les profils de numérotation peuvent effectuer les opérations suivantes :

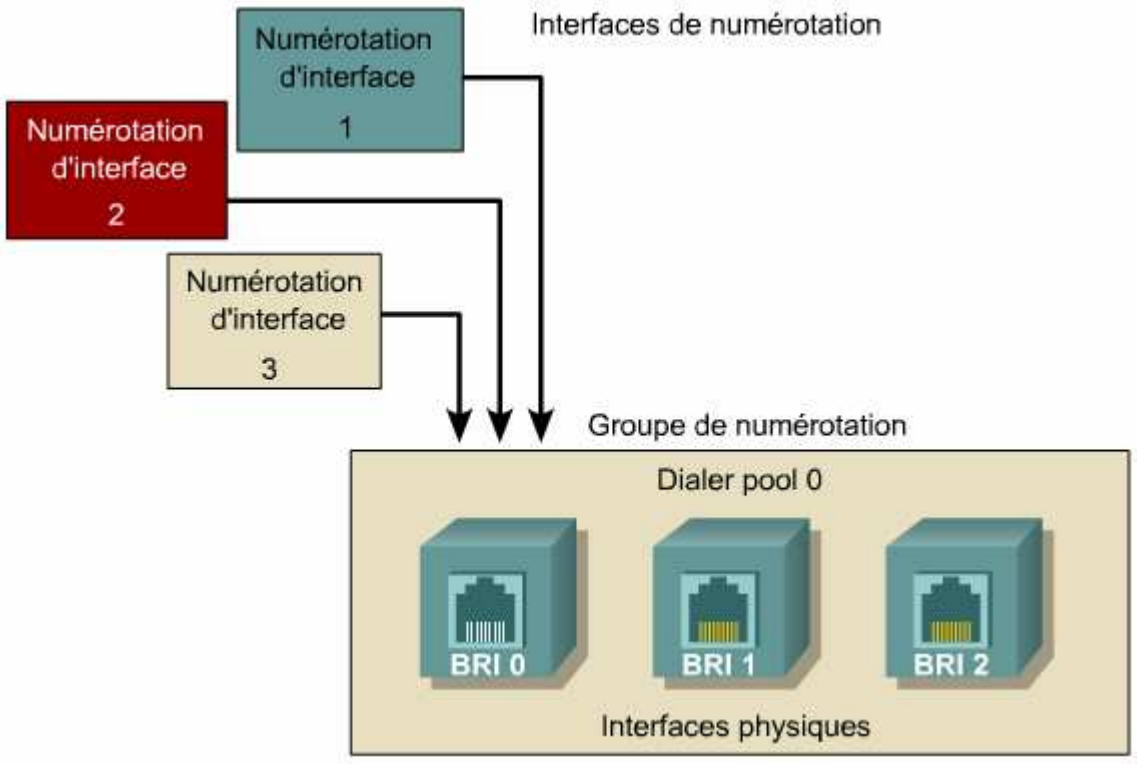
- Définir l'encapsulation et les listes de contrôle d'accès
- Déterminer le nombre minimum ou maximum d'appels
- Activer ou désactiver les fonctions

Les profils de numérotation permettent d'effectuer les activités ci-dessous :

- Configurer les canaux B d'une interface RNIS avec différents sous-réseaux IP
- Utiliser différentes encapsulations sur les canaux B d'une interface RNIS
- Définir différents paramètres DDR pour les canaux B d'une interface RNIS
- Éliminer le gaspillage de canaux B RNIS en permettant aux accès RNIS BRI d'appartenir à plusieurs groupes de numérotation

Un profil de numérotation comporte les éléments suivants:

- ***Interface de numérotation*** – Entité logique qui utilise un profil de numérotation par destination.
- ***Groupe de numérotation*** – Chaque interface de numérotation désigne un groupe de numérotation, c'est-à-dire un groupe d'une ou plusieurs interfaces physiques associées à un profil de numérotation.
- ***Interfaces physiques*** – Les interfaces d'un groupe de numérotation sont configurées pour des paramètres d'encapsulation et pour identifier les groupes de numérotation auxquels l'interface appartient. L'authentification PPP, le type d'encapsulation et le PPP multiliaison sont tous configurés sur l'interface physique.



Tout d'abord, un paquet intéressant est routé vers une adresse IP DDR distante. Le routeur consulte ensuite les interfaces de numérotation configurées pour trouver celle qui partage le même sous-réseau que l'adresse IP DDR distante. S'il en existe une, le routeur recherche une interface DDR physique non utilisée dans le groupe de numérotation. La configuration du profil de numérotation est ensuite appliquée à l'interface, et le routeur tente de créer la connexion DDR. À la fin de la connexion, l'interface revient au groupe de numérotation pour l'appel suivant.

Configuration de profils de numérotation

Il est possible de configurer plusieurs interfaces de numérotation sur un routeur. La commande **interface dialer** crée une interface de numérotation et passe en mode de configuration d'interface.

```
interface dialer1
 ip address 10.1.1.1 255.255.255.0
 encapsulation ppp
 dialer remote-name Smalluser
 dialer string 5554540
 dialer idle-timer 240
 dialer pool 1
 dialer-group 1
 ppp authentication chap
!
interface dialer2
 ip address 10.2.2.1 255.255.255.0
 encapsulation ppp
 dialer remote-name Mediumuser
 dialer string 5551234
```

Pour configurer l'interface de numérotation, procédez comme suit:

1. Configurez une ou plusieurs interfaces de numérotation :
   - L'adresse IP
   - Le type d'encapsulation et l'authentification
   - Le compteur d'inactivité
   - Le groupe de numérotation pour le trafic intéressant
2. Configurez une **dialer string** et un **dialer remote-name** pour spécifier le nom du routeur distant et le numéro de téléphone permettant d'y accéder. La commande **dialer pool** associe cette interface logique avec un groupe d'interfaces physiques.
3. Configurez les interfaces physiques et assignez-les à un groupe de numérotation à l'aide de la commande **dialer pool-member**

Plusieurs groupes de numérotation peuvent être attribués à une interface au moyen de plusieurs commandes **dialer pool-member**. S'il existe plusieurs interfaces physiques dans le groupe, utilisez l'option **priority** de la commande **dialer pool-member** pour définir la priorité de l'interface au sein d'un groupe de numérotation. Si plusieurs appels doivent être effectués et qu'une seule interface est disponible, c'est le groupe qui a la priorité la plus élevée qui effectue l'appel.

```
interface BRI0/0
 encapsulation ppp
 dialer pool-member 0 priority 100
 ppp authentication chap
!
interface BRI0/1
 encapsulation ppp
 dialer pool-member 1 priority 150
 ppp authentication chap
!
interface BRI0/2
 encapsulation ppp
 dialer pool-member 0 priority 50
 dialer pool-member 1 priority 50
 dialer pool-member 2 priority 50
 ppp authentication chap
!
```

Vérification de la configuration DDR

Show dialer interface [BRI] → affiche des informations sur les appels entrants et sortants.

Le message «*Dialer state is data link layer up*» suggère que le numéroteur s'est activé correctement et que l'interface BRI 0/0:1 est liée au profil dialer1.

```
sydney#show dialer

BRI0/0 - dialer type = ISDN

Dial String      Successes   Failures    Last DNIS   Last
status
0 incoming call(s) have been screened.
0 incoming call(s) rejected for callback.

BRI0/0:1 - dialer type = ISDN
Idle timer (120 secs), Fast idle timer (20 secs)
Wait for carrier (30 secs), Re-enable (15 secs)
Dialer state is data link layer up
Interface bound to profile Dialer1
Time until disconnect 83 secs
Current call connected never
Connected to 5552000 (perth)
```

Show isdn active → présente des informations sur les communications RNIS actives en cours.

```
Phoenix#show isdn active
-------------------------------------------------------------------------
-------------
                                ISDN ACTIVE CALLS
-------------------------------------------------------------------------
-------------
History table has a maximum of 100 entries.
History table data is retained for a maximum of 15 Minutes.
-------------------------------------------------------------------------
-------------
Call Calling Called  Remote Seconds Seconds Seconds Charges
Type Number  Number  Name   Used    Left    Idle    Units/Currency
-------------------------------------------------------------------------
Out          5551000 Seattle       87      41      78      0
-------------------------------------------------------------------------
```

Show isdn status → présente des informations sur les trois couches de l'interface BRI.

```
Phoenix#show isdn status
Global ISDN Switchtype = basic-ni
ISDN BRI0/0 interface
dsl 0, interface ISDN Switchtype = basic-ni
    Layer 1 Status:
ACTIVE
    Layer 2 Status:
TEI = 64, Ces = 1, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
TEI = 65, Ces = 2, SAPI = 0, State = MULTIPLE_FRAME_ESTABLISHED
    Spid Status:
TEI 64, ces = 1, state = 8(established)
    spid1 configured, no LDN, spid1 sent, spid1 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 1
TEI 65, ces = 2, state = 8(established)
    spid2 configured, no LDN, spid2 sent, spid2 valid
    Endpoint ID Info: epsf = 0, usid = 70, tid = 2
    Layer 3 Status:
1 Active Layer 3 Call(s)
    Activated dsl 0 CCBs = 1
CCB:callid=8001, sapi=0, ces=1, B-chan=1, calltype=DATA
```

Dans cet écran, la couche 1 RNIS est active, la couche 2 RNIS est établie avec SPID1 et SPID2 validés, et il y a une connexion active sur la couche 3.

Dépannage de la configuration DDR

Il existe *deux grandes catégories de problèmes DDR*. Soit un routeur ne numérote pas quand il le devrait, soit il numérote constamment quand il ne le devrait pas.

Debug isdn q931 → pour observer les échanges lors de l'établissement d'appels sortants et entrants.

```
remote#debug isdn q931
1d11h: ISDN BR0/0: RX <-  SETUP pd = 8  callref = 0x02
1d11h:         Bearer Capability i = 0x8890
1d11h:         Channel ID i = 0x89
1d11h:         Signal i = 0x40 - Alerting on - pattern 0
1d11h:         Called Party Number i = 0xC1, '5552000'
1d11h: ISDN BR0/0: Event: Received a DATA call from <unknown> on B1
at 64 Kb/s
1d11h: ISDN BR0/0: TX ->  CALL_PROC pd = 8  callref = 0x82
1d11h:         Channel ID i = 0x89
1d11h: ISDN BR0/0: TX ->  CONNECT pd = 8  callref = 0x82
1d11h:         Channel ID i = 0x89
1d11h: ISDN BR0/0: RX <-  CONNECT_ACK pd = 8  callref = 0x02
1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
```

On dit d'une interface qui s'active et se désactive en permanence qu'elle est *en battement*.

Debug dialer packet → envoie un message à la console à chaque fois qu'un paquet est envoyé d'une interface DDR. « Déterminer exactement le trafic responsable du battement d'une interface DDR »

Debug dialer events → envoie à la console un message lui indiquant quand une liaison DDR s'est établie et le trafic à l'origine de la connexion « détecter les problèmes de connectivité »

```
central#debug dialer events
Dial on demand events debugging is on

central#ping 192.168.1.2
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
192.168.1.2, timeout is 2 seconds:

1d11h: BR0/0 DDR: rotor dialout [priority]
1d11h: BR0/0 DDR: Dialing cause ip (s=192.168.1.1, d=192.168.1.2)
1d11h: BR0/0 DDR: Attempting to dial 5554000
1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
1d11h: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to
5552000 ..!!!
```

Isdn call interface → force le routeur local à accéder au routeur distant « détecter s'il s'agit d'un problème DDR ou RNIS »

Remarque : Dans certains cas, il est préférable de réinitialiser la connexion entre le routeur et le commutateur RNIS local. La commande **clear interface bri** annule les connexions actives sur l'interface et réinitialise celle-ci avec le commutateur RNIS.

```
central#isdn call interface bri0/0 5552000

1d11h: %LINK-3-UPDOWN: Interface BRI0/0:1, changed state to up
1d11h: %ISDN-6-CONNECT: Interface BRI0/0:1 is now connected to
5552000
```

Module 5

Frame Relay

Concepts Frame Relay :

Présentation de Frame Relay :

Frame Relay est une norme de l'UIT-T et de l'ANSI. Frame Relay est un service WAN *à commutation de paquets orienté connexion*. Il fonctionne au niveau de la couche liaison de données du modèle OSI.

Frame Relay utilise un sous-ensemble du protocole HDLC dénommé ***LAPF*** (*Link Access Procedure for Frame Relay*).

À l'origine, Frame Relay a été conçu pour permettre à l'équipement RNIS de disposer d'un accès vers un service à commutation de paquets sur un canal B. Toutefois, *Frame Relay est aujourd'hui une technologie autonome*.

Remarque : L'équipement informatique qui n'est pas sur un réseau local peut également envoyer des données sur un réseau Frame Relay. Cet équipement utilise une unité d'accès Frame Relay (***FRAD*** – *Frame Relay access device*) en tant qu'ETTD.

Terminologie Frame Relay

On appelle ***circuit virtuel*** (VC) la connexion entre deux ETTD par le réseau Frame Relay. SVC ou PVC.

Un circuit virtuel est créé par le stockage d'un mappage entre port d'entrée et port de sortie dans la mémoire de chaque commutateur, afin de les lier jusqu'à ce qu'un chemin continu d'une extrémité à l'autre du circuit ait été identifié.

Comme Frame Relay a été conçu pour fonctionner sur des lignes numériques de haute qualité, aucun mécanisme de récupération après erreur n'est fourni. Si un nœud détecte une erreur dans une trame, il la rejette sans notification.

Le *FRAD* (le routeur connecté au réseau) peut être connecté à divers points d'extrémité par plusieurs circuits virtuels → chaque point d'extrémité ne nécessite qu'une ligne d'accès et une interface + la capacité de la ligne d'accès est fondée sur la bande passante moyenne requise par les circuits virtuels et non sur la bande passante maximale requise.

Les divers circuits virtuels d'une seule ligne d'accès peuvent être distingués, chaque VC disposant de son propre identificateur de canal de liaison de données (*Data Link Connection Identifier ou* ***DLCI***).

Remarque : L'identificateur DLCI est stocké dans le champ d'adresse de chaque trame transmise. Le DLCI n'a généralement qu'une signification locale et peut différer à chaque extrémité d'un circuit virtuel.

Couches support de la pile Frame Relay

Frame Relay fonctionne comme suit:

- Prélèvement de paquets de données d'un protocole de couche réseau, tel qu'IP ou IPX
- Encapsulation de ces paquets comme partie données d'une trame Frame Relay
- Transfert de ces trames vers la couche physique pour les délivrer sur la ligne

La séquence de contrôle de trame (FCS) sert à déterminer si des erreurs se sont produites dans le champ d'adresse de couche 2 au cours de la transmission.

Bande passante et contrôle de flux Frame Relay

La connexion série ou le lien d'accès au réseau Frame Relay est généralement une ligne louée. La vitesse de la ligne est assujettie au débit d'accès ou du port.

Le ***CIR*** « débit de données garanti » est le débit auquel le fournisseur d'accès accepte de recevoir des bits sur le circuit virtuel.

Les CIR individuels sont généralement inférieurs au débit du port. Toutefois, la somme des CIR est normalement supérieure au débit des ports.

Le commutateur accepte les trames de l'ETTD à des débits dépassant le CIR. Ceci fournit effectivement à chaque canal une bande passante à la demande jusqu'à un maximum défini par la vitesse du port.

La différence entre le CIR et le maximum, que celui-ci soit inférieur ou égal à la vitesse du port, est appelée ***EIR*** (*Excess Information Rate*).

L'intervalle de temps sur lequel les débits sont calculés est appelé la durée garantie (T_c). Le nombre de bits garantis dans T_c constitue le débit garanti en rafale (B_c). Le nombre de bits supplémentaires au-dessus du débit garanti en rafale, jusqu'à la vitesse maximale de la liaison d'accès est le débit garanti en excès (B_e).

Bien que le commutateur accepte les trames excédant le CIR, chaque *trame en excès* est signalée au niveau du commutateur par le positionnement du bit d'éligibilité à la suppression (***DE*** - *Discard Eligible*) sur «1» dans le champ d'adresse.

Le commutateur gère un compteur de bits pour chaque circuit virtuel. Une trame entrante est signalée comme DE si elle met le compteur au-delà de B_c. Une trame entrante est éliminée si elle pousse le compteur au-delà de $B_c + B_e$. À la fin de chaque T_c secondes, le compteur est réinitialisé

Les trames qui arrivent au commutateur sont mises en file d'attente avant d'être transférées. Pour éviter le problème de congestion, les commutateurs Frame Relay appliquent une politique de rejet des trames en files d'attente. Les trames dont le bit DE est défini sont supprimées en premier.

Quand un commutateur détermine que sa file d'attente augmente, il essaie de réduire le flux de trames y parvenant. Pour ce faire, il avertit les ETTD du problème en positionnant les bits de notification explicite de congestion (***ECN*** – *Explicit Congestion Notification*) dans le champ d'adresse de la trame.

Le bit de notification explicite de congestion au destinataire (***FECN*** – *Forward ECN*) est positionné sur chaque trame reçue par le commutateur sur la liaison encombrée. Le bit de notification explicite de congestion à la source (***BECN*** - *Backward ECN*) est positionné sur chaque trame placée par le commutateur sur la liaison encombrée.

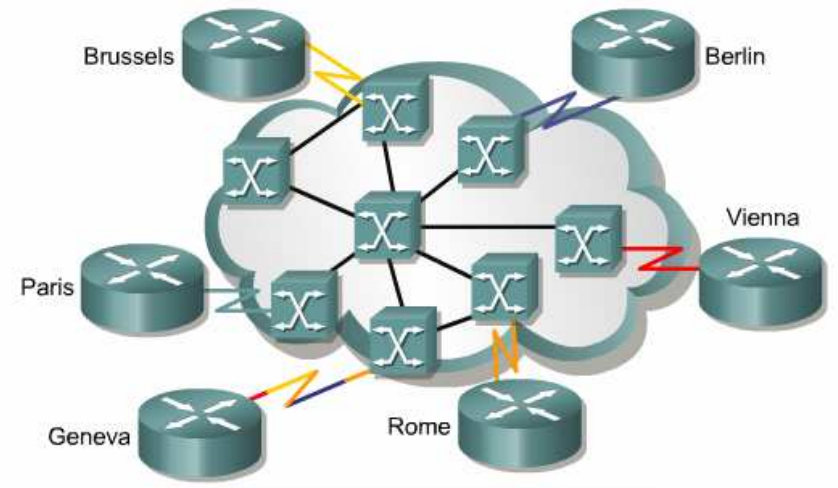
→ Les ETTD qui reçoivent des trames dans lesquelles les bits ECN sont définis sont censés réduire le flux de trames jusqu'à ce que l'encombrement se dissipe.

Remarque : Les bits DE, FECN et BECN font partie du ***champ d'adresse*** de la trame LAPF.

Mappage d'adresse et topologie Frame Relay

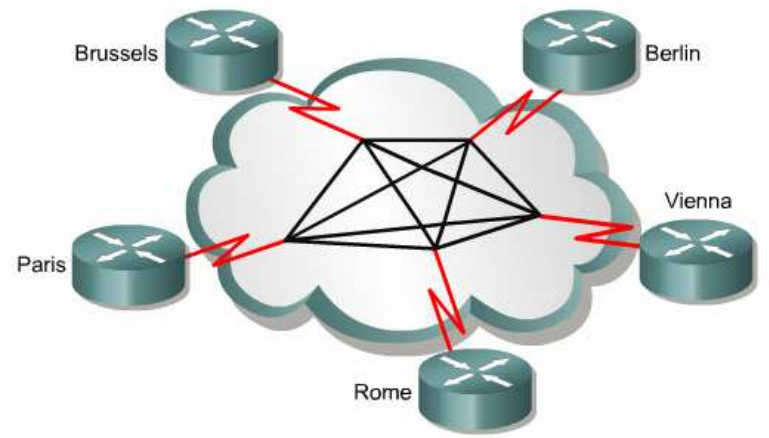
Frame Relay est plus rentable quand plusieurs sites doivent être interconnectés.

Avec une topologie « ***hub and spoke*** », le concentrateur est mis à l'emplacement permettant de réduire au maximum les coûts de la ligne louée. Avec une topologie en étoile pour Frame Relay, chaque site distant dispose d'une liaison d'accès au nuage Frame Relay avec un seul circuit virtuel. Le concentrateur a une liaison d'accès avec plusieurs circuits virtuels, un pour chaque site distant.



On choisit une topologie en ***maillage global*** quand les services à joindre sont dispersés géographiquement et qu'un accès très fiable est nécessaire. Avec le maillage global, chaque site est connecté à tous les autres sites. Contrairement aux interconnexions de lignes louées, Frame Relay ne nécessite aucun matériel supplémentaire.

Plusieurs circuits virtuels sur une liaison d'accès exploitent généralement mieux Frame Relay que des VC isolés. En effet, ils profitent du multiplexage statistique intégré.



Dans n'importe quelle topologie Frame Relay, quand une seule interface sert à interconnecter plusieurs sites, des *problèmes d'accessibilité* peuvent survenir. Ceci est dû à la nature d'accès multiple sans diffusion (***NBMA*** - *nonbroadcast multiaccess*) de Frame Relay (problème de Split Horizon par exemple).

→ Il est nécessaire d'effectuer un mappage au niveau de chaque FRAD ou routeur entre une adresse Frame Relay de la couche de liaison de données et une adresse de la couche réseau.

Fondamentalement, le routeur doit savoir quels réseaux sont accessibles au-delà d'une interface en particulier. Les informations DLCI peuvent être configurées manuellement à l'aide de commandes de mappage. Le DLCI peut également être configuré automatiquement, au moyen de la résolution d'adresse inverse.

LMI Frame Relay

L'interface de supervision locale (***LMI*** – *Local Management Interface*) → pour que les ETTD puissent acquérir de façon dynamique des informations sur l'état du réseau.

L'ETTD et l'ETCD s'échangent des messages LMI à l'aide de ces *identificateurs DLCI réservés*.

Identificateurs de circuit virtuel	Types de circuits virtuels
0	LMI (ANSI, ITU)
1..15	Réservé pour une utilisation ultérieure
992..1007	CLLM
1008..1022	Réservé pour une utilisation ultérieure (ANSI, ITU)
1019..1020	Diffusion multicast (Cisco)
1023	LMI (Cisco)

Les extensions LMI incluent les éléments suivants :

- Le mécanisme de test d'activité, qui vérifie qu'un circuit virtuel est opérationnel
- Le mécanisme multicast
- Le contrôle de flux
- La possibilité de donner une signification globale aux identificateurs DLCI
- Le mécanisme d'état du circuit virtuel

Il existe plusieurs types d'interfaces LMI, toutes mutuellement incompatibles. Le type de LMI configuré sur le routeur doit *correspondre* au type utilisé par l'opérateur. Trois types d'interfaces LMI sont pris en charge par les routeurs Cisco :

- **Cisco** – Les extensions LMI d'origine
- **Ansi** – Correspondant à la norme ANSI T1.617 annexe D
- **q933a** – Correspondant à la norme de l'ITU Q933 annexe A

Les messages LMI sont acheminés dans une variante des trames LAPF. Cette variante inclut quatre champs d'en-tête supplémentaires la rendant compatible avec les trames LAPD utilisées pour le RNIS.

Un ou plusieurs éléments d'informations (***IE***) suivent l'en-tête. Chaque IE contient les éléments suivants:

- Un identificateur d'IE sur un octet
- Un champ de longueur d'IE
- Un ou plusieurs octets contenant des données concrètes, qui incluent généralement l'état d'un identificateur DLCI

Étapes des protocoles de résolution d'adresse inverse et LMI

Quand un routeur connecté à un réseau Frame Relay démarre, il envoie au réseau un message d'interrogation de l'état LMI. Le réseau répond par un message d'état LMI contenant des informations sur chaque circuit virtuel configuré sur la liaison d'accès.

Remarque : Le routeur répète régulièrement cette interrogation de l'état, mais les réponses ultérieures n'incluent que les changements d'état. Après un nombre prédéfini de ces réponses abrégées, le réseau envoie un message d'état complet.

DLCI	Etat
101	Actif
102	Actif
103	Actif
104	Actif

Si le routeur doit mapper les circuits virtuels à des adresses de la couche réseau, il envoie un message de résolution d'adresse ***inverse*** sur chaque circuit virtuel. Ce message contient l'adresse de couche réseau du routeur, afin que l'ETTD ou le routeur distant puisse également procéder au mappage.

Configuration de Frame Relay :

Configuration de base de Frame Relay

Encapsulation frame-relay **[cisco | ietf]** → Pour passer à l'encapsulation Frame Relay.

L'encapsulation Frame Relay propriétaire de Cisco fait appel à un en-tête sur 4 octets, dont 2 désignent l'identificateur de connexion de liaisons de données (DLCI) et 2 le type de paquet.

Frame-relay lmi-type **[ansi | cisco | q933a]** → établir et configurer la connexion LMI.

Cette commande est seulement nécessaire avec la plate-forme logicielle Cisco IOS 11.1 ou une version précédente. À partir de l'IOS version 11.2, aucune configuration n'est nécessaire, car le type de LMI est détecté automatiquement.

Configuration d'une carte Frame Relay statique

Frame-relay map **{Protocol} {@ de destination} {dlci} [broadcast]** → pour mapper de façon statique l'adresse de couche réseau à l'identificateur DLCI local.

[Broadcast] : Permet de diffuser les Broadcast et les multicast sur le circuit virtuel

Problèmes d'accessibilité relatifs aux mises à jour de routage :

Une topologie NBMA Frame Relay peut être à l'origine de deux problèmes :

- Problèmes d'accessibilité relatifs aux mises à jour de routage
- Le besoin de répliquer les broadcasts sur chaque circuit virtuel permanent lorsqu'une interface physique en contient plusieurs

Pour résoudre le problème de «split-horizon», une méthode consiste à utiliser une topologie de maillage global. En revanche, cela augmente le coût, car un plus grand nombre de circuits virtuels permanents est alors nécessaire. La meilleure solution consiste à utiliser des sous-interfaces.

Sous-interfaces Frame Relay

Point-à-point
- Les sous-interfaces font office de lignes louées
- Chaque sous-interface point-à-point a besoin de son propre sous-réseau
- Applicable aux topologies de type " hub-and-spoke "

Multipoint
- Les sous-interfaces font office de réseaux NMBA. Elles ne résolvent donc pas le problème de " split-horizon "
- L'utilisation d'un seul sous-réseau permet d'économiser de l'espace d'adressage
- Applicable aux topologies à maillage partiel et à maillage global

Configuration de sous-interfaces Frame Relay

Pour configurer les sous-interfaces d'une interface physique, procédez comme suit :

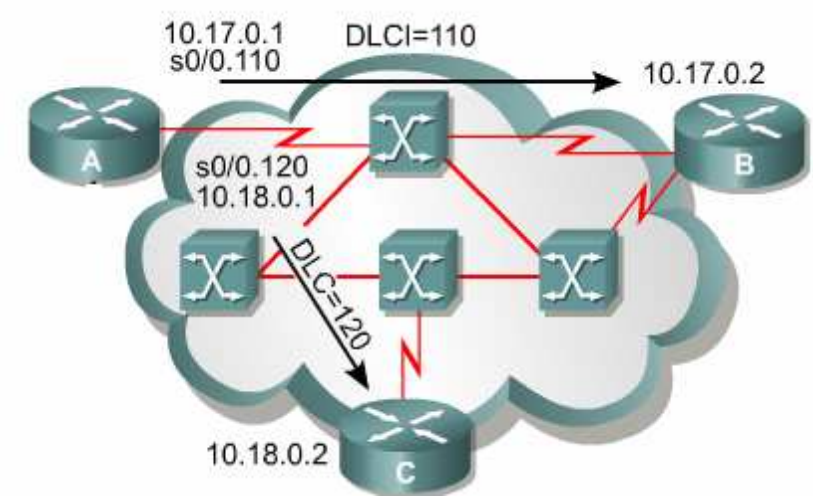
- Configurez l'encapsulation Frame Relay sur l'interface physique au moyen de la commande **encapsulation frame-relay**
- Pour chacun des circuits virtuels permanents définis, créez une sous-interface logique

Router(config-if)#**interface serial {port/numéro.numéroSI} [multipoint | point-to-point]**

Remarque : En général, le numéro de sous-interface est celui de l'identificateur DLCI. Ceci facilite le dépannage.

Router(config-subif)#**frame-relay interface-dlci {dlci-number}** → configurer l'identificateur DLCI local sur la sous-interface.

Remarque : On configure DLCI, si la sous-interface est configurée en point-to-point, ou Le pour les sous-interfaces **multipoint** pour lesquelles la résolution d'adresse inverse a été activée.



Vérification de la configuration Frame Relay

Show interfaces → affiche des informations sur l'encapsulation et l'état des couches 1 et 2. Elle affiche également les informations ci-dessous :

- Le type d'interface LMI
- L'identificateur DLCI de l'interface LMI
- Le type d'équipement (ETTD/ETCD)

```
Router#show interface s0/0
Serial0/0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 10.140.1.2/24
  MTU 150 bytes, BW 1544 Kbit, DLY 20000 usec, relay
  255/255, load 1/255
  Encapsulation FRAME-RELAY, loopback not set, keepalive
  set (10 sec)
  LMI enq sent 19, LMI stat recvd 20, LMI upd recvd 0,
  DTE LMI up
  LMI enq recvd 0, LMI stat sent 0, LMI upd sent 0
  LMI DLCI 1023 LMI type is CISCO frame relay DTE
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 8/0,
  interface broadcasts 5
```

Show frame-relay lmi → pour afficher les statistiques relatives au trafic sur l'interface LMI.

```
Router#show frame-relay lmi

LMI Statistics for interface Serial0/0 (Frame Relay DTE)
LMI TYPE = CISCO
  Invalid Unnumbered info 0 Invalid Prot Disc 0
  Invalid dummy Call Ref 0 Invalid Msg Type 0
  Invalid Status Message 0 Invalid Lock Shift 0
  Invalid Information ID 0 Invalid Report IE Len 0
  Invalid Report Request 0 Invalid Keep IE Len 0
  Num Status Enq. Sent 113100 Num Status msgs Rcvd
  113100
  Num Update Status Revd 0 Num Status Timeouts 0
```

Show frame-relay pvc [interface] [dlci] → pour afficher l'état de chaque circuit virtuel permanent configuré, ainsi que des statistiques sur le trafic.

```
Router#show frame-relay pvc 100

PVC Statistics for interface Serial0/0 (Frame Relay DTE)

DLCI = 100, DLCI USAGE = LOCAL, PVC STATUS = ACTIVE,
INTERFACE = Serial0/0

  input pkts 28      output pkts 10      in bytes 8398
  out bytes 1198     dropped pkts 0      in FECN pkts 0
  in BECN pkts 0     out FECN pkts 0     out BECN pkts 0
  in DE pkts 0       out DE pkts 0
  out bcast pkts 10  out bcast bytes 1198
  pvc create time 00:03:46, last time pvc status changed
  00:03:47
```

Show frame-relay map → pour afficher les entrées actuelles de la carte, ainsi que des informations sur les connexions.

```
Router#show frame-relay map
Serial0/0 (up) : ip 10.140.1.1 dlci 100 (0x64,0x1840),
                 dynamic, broadcast, status defined, active
```

Clear frame-relay-inarp → Pour supprimer les cartes Frame Relay créées de façon dynamique à l'aide de la résolution d'adresse inverse.

Dépannage de la configuration Frame Relay

Debug frame-relay lmi → pour déterminer si le routeur et le commutateur Frame Relay envoient et reçoivent correctement les paquets LMI.

```
Router#debug frame-relay lmi
Frame Relay LMI debugging is on
Displaying all Frame Relay LMI data
Router#
1w2d: Serial0/0(out):StENq,myseq 140, yourseen 139, DTE up
1w2d: datagramstart = 0xE008SEC, datagramsize = 13
1w2d: FR encap = 0xFCF10309
1w2d: 00 75 01 01 03 02 8C 8B
1w2d:
1w2d: Serial0/0 (in): Status, myseq 140
1w2d: RT IE 1, length 1, type 1
1w2d: KA IE 3, length 2, yourseg 140, myseq 140

  1w2d: Serial0/0 (in): Status, myseq 142
  1w2d: RT IE 1, length 1 type 0
  1w2d: KA IE 3, length 2 yourseg 142, myseq 142
  1w2d: PVC IE 0x7, length 0x6, dlci 100, status 0x2, bw0
```

→ «**Out**» est un message d'état de l'interface LMI envoyé par le routeur.
→ «**In**» est un message reçu du commutateur Frame Relay.
→ Un message d'état LMI complet est un «**type 0**». Un échange LMI est un «**type 1**».
→ Les valeurs possibles du champ d'état sont les suivantes :

- **0x0** – Ajouté/inactif signifie qu'un identificateur DLCI a été programmé pour le commutateur, mais qu'il n'est pas utilisable. La raison peut en être que l'autre extrémité du circuit virtuel permanent ne fonctionne pas.
- **0x2** – Ajouté/actif signifie que le commutateur Frame Relay dispose de l'identificateur DLCI et que tout est opérationnel.
- **0x4** – Supprimé signifie que le commutateur Frame Relay n'a programmé aucun identificateur DLCI pour le routeur, mais qu'il en a existé un dans le passé. Ceci est peut-être causé par l'inversion des DLCI sur le routeur ou parce que le circuit virtuel permanent a été supprimé par l'opérateur dans le nuage Frame Relay.

Module 6

Introduction à l'administration réseau

Stations de travail et serveurs :

Stations de travail :

Une ***station de travail*** est un ordinateur client utilisé pour exécuter des applications. Elle est connectée à un serveur sur lequel elle obtient des données partagées avec d'autres utilisateurs.

Une station de travail utilise des logiciels spéciaux, par exemple un Shell de réseau, pour effectuer les activités suivantes:

- Intercepter les données utilisateurs et les commandes des applications
- Décider si la commande est destinée au système d'exploitation local ou au système d'exploitation de réseau
- Diriger la commande vers le système d'exploitation local ou vers la carte réseau (NIC) pour traitement et transmission sur le réseau
- Acheminer les transmissions du réseau vers l'application exécutée sur la station de travail.

Remarque : UNIX ou Linux peuvent servir de systèmes d'exploitation de bureau, mais on les trouve généralement sur les ordinateurs haut de gamme.

Les stations de travail sans disque dur local constituent une catégorie spéciale d'ordinateurs, conçus pour fonctionner en réseau. Comme leur nom l'implique, elles n'ont pas de disques durs, mais possèdent un moniteur, un clavier, de la mémoire, des instructions de démarrage en ROM, ainsi qu'une carte réseau. Le logiciel servant à établir une connexion réseau se charge à partir de la ROM amorçable située sur la carte réseau.

Une station de travail sans disque dur local ne peut pas transmettre de virus au réseau, ni servir à prendre des données sur le réseau en les copiant sur un disque dur → *Sécurité*

Il est possible d'utiliser des ordinateurs portables comme stations de travail d'un réseau local en les connectant par une station d'accueil.

Serveurs

Les ***systèmes serveurs*** doivent être équipés pour prendre en charge de nombreux utilisateurs simultanés et de nombreuses tâches à mesure que les clients exigent du serveur des ressources à distance.

Avant qu'un client ne puisse accéder aux ressources du serveur, il doit être identifié, puis autorisé à utiliser ces ressources (Compte d'utilisateur + MDP).

Les serveurs sont généralement de plus ***grande capacité*** que les stations de travail et disposent de mémoire supplémentaire pour traiter simultanément les nombreuses tâches actives ou résidant en mémoire. Les serveurs ont également besoin d'espace disque supplémentaire pour stocker les fichiers partagés et pour servir d'extension à la mémoire

interne du système. Les cartes système des serveurs nécessitent des connecteurs d'extension supplémentaires pour y connecter des périphériques partagés, tels que des imprimantes et plusieurs interfaces réseau.

Les serveurs doivent être efficaces et *robustes*. Le terme robuste indique que les systèmes serveurs sont capables de fonctionner efficacement sous de lourdes charges. Il signifie également que les systèmes peuvent survivre à la défaillance d'un ou plusieurs processus ou composants sans qu'une défaillance générale du système se produise.

Les applications et fonctions du serveur incluent notamment les HTTP, FTP, DNS, SMTP, POP3 et IMAP. Les protocoles de partage de fichiers incluent NFS et SMB

Relation client-serveur

Le modèle d'architecture client-serveur distribue le traitement sur plusieurs ordinateurs. ***Le traitement distribué*** permet d'accéder à des systèmes distants dans l'objectif de partager des informations et des ressources réseau.

Les autres termes couramment utilisés sont:

- *Hôte local* – Machine sur laquelle l'utilisateur travaille habituellement.
- *Hôte distant* – Système auquel un utilisateur accède à partir d'un autre système.
- *Serveur* – Fournit des ressources à un ou plusieurs clients par le biais d'un réseau.
- *Client* – Machine utilisant les services d'un ou plusieurs serveurs réseau.

Exemple :

Client : en utilisant un navigateur, le client demande des pages Internet.
Serveur : en utilisant le service http, le serveur envoi les pages au client.

Remarque : La distribution des fonctions dans un réseau client-serveur offre des avantages substantiels, mais implique également des coûts.

Introduction aux systèmes d'exploitation de réseau

Le système d'exploitation d'un ordinateur constitue la fondation logicielle sur laquelle les applications et les services s'exécutent. De même, un système d'exploitation de réseau autorise la communication entre plusieurs équipements et le partage de ressources sur l'ensemble d'un réseau.

Novell	UNIX	Windows	Linux
NetWare	HP-UX	NT	Red Hat
IntraNetWare	Sun Solaris	Server 2000	Caldera
GroupWise	BSD	.NET Server	SuSE
	SCO	Server 2003	Debian
	AIX		Slackware

Le système d'exploitation de réseau amélioré la portée de la station de travail cliente en mettant à disposition les services distants en tant qu'extensions du système d'exploitation local.

Les principales caractéristiques à prendre en compte pour la sélection d'un système d'exploitation de réseau sont les performances, les outils d'administration et de surveillance, la sécurité, l'évolutivité et la robustesse ou tolérance d'erreurs.

Considérations relatives au système d'exploitation de réseau		
Sécurité	Cryptage	Authentification des utilisateurs
Robustesse	Charges de travail symétriques	Redondance
Performances	Constance lorsque la charge augmente	
Évolutivité	Évolutivité	
Gestion	Administration du système	

Microsoft NT, 2000 et .NET

Système d'exploitation	Versions	Utilisations
Windows NT	• Workstation • Server	• Utilisateurs en entreprise • Serveur départemental
Windows 2000	• Professional • Server • Advanced server • .NET	• Utilisateurs en entreprise ou petites entreprises • Serveur d'accès à distance ou Internet • Serveur départemental • Serveur d'entreprise • Serveur Internet d'entreprise

NT 4 a été conçu pour les opérations d'une importance capitale, dans le but de fournir un environnement plus stable que les systèmes d'exploitation grand public de Microsoft.

Il est disponible dans des versions de bureau (NT 4.0 Workstation) et serveur (NT 4.0 Server). Pour NT Les défaillances du programme sont isolées et ne demandent aucun redémarrage du système.

Windows NT fournit une structure de domaine permettant de contrôler l'accès des utilisateurs et des clients aux ressources du serveur. Elle est administrée par l'application User Manager for Domains sur le contrôleur de domaine. Chaque domaine NT nécessite un seul contrôleur de domaine primaire, qui contient la base de données ***SAM*** (*Security Accounts Management Database*)

S'appuyant sur le noyau NT, la version 2000 de Windows, plus récente, existe également dans des versions de bureau et serveur. Windows 2000 prend en charge la technologie «plug-and-play» + Active Directory.

Remarque : Windows 2000 Server ajoute de nombreuses fonctions serveur spécifiques aux fonctionnalités de Windows 2000 Professional.

UNIX, Sun, HP et LINUX

Origines d'UNIX

Depuis sa création, UNIX a été conçu pour prendre en charge les multi-utilisateurs et le multitâche. UNIX a également été l'un des premiers systèmes d'exploitation à prendre en charge les protocoles réseau d'Internet.

UNIX a tout d'abord été écrit en langage assembleur, un jeu d'instructions élémentaires qui contrôle les instructions internes d'un ordinateur. Toutefois, UNIX pouvait seulement fonctionner sur un type d'ordinateur spécifique.

En 1973, Ritchie et son collègue programmeur des laboratoires Bell Ken Thompson ont réécrit les programmes du système UNIX en langage C. Le fait que C soit un langage de plus haut niveau a permis de faire migrer UNIX vers d'autres ordinateurs sans trop d'efforts en matière de programmation

Avantages d'UNIX :

- Systèmes d'exploitation standard
- Puissant, souple, évolutif et sécurisé
- Pris en charge par plusieurs équipementiers
- Système d'exploitation stable, arrivé à maturité
- Intégration étroite avec les protocoles TCP/IP
- Très répandu pour les applications critiques

Aujourd'hui, il existe des dizaines de versions différentes d'UNIX, dont notamment les suivantes:

- Hewlett Packard UNIX (HP-UX)
- Berkeley Software Design, Inc. (BSD UNIX), qui a produit des dérivés tels que FreeBSD
- Santa Cruz Operation (SCO) UNIX
- Sun Solaris
- IBM UNIX (AIX)

L'environnement d'exploitation *Solaris de Sun Microsystems* et son système d'exploitation central, ***SunOS***, est une mise en oeuvre d'UNIX sur 64 bits. Solaris est actuellement la version d'UNIX la plus utilisée dans le monde pour les réseaux de grande taille et les sites Web d'Internet.

Origines de Linux

En 1991, un étudiant finlandais du nom de Linus Torvalds commença à travailler sur un système d'exploitation destiné à un ordinateur à processeur Intel 80386. « Semblable à UNIX dans son fonctionnement, mais utilisa un code logiciel ouvert et totalement gratuit pour tous les utilisateurs ».

Les versions de Linux peuvent aujourd'hui fonctionner sur pratiquement n'importe quel processeur 32 bits, dont notamment les puces Intel 80386, Motorola 68000, Alpha et PowerPC.

Les versions les plus populaires de Linux sont :

- Red Hat Linux – distribué par Red Hat Software
- OpenLinux – distribué par Caldera
- Corel Linux
- Slackware
- Debian GNU/Linux
- SuSE Linux

Certains constructeurs fournissent des logiciels d'émulation Windows, tels que WABI et WINE, qui permettent d'exécuter de nombreuses applications Windows sous Linux.

Les distributions récentes de Linux sont dotées de composants réseau intégrés pour se connecter à un réseau local, établir une connexion commutée vers Internet …

Avantages de LINUX :

- C'est un véritable système d'exploitation sur 32 bits.
- Il prend en charge le multitâche préemptif et la mémoire virtuelle.
- Son code est ouvert (Open Source) et par conséquent à la disposition de quiconque souhaite l'enrichir ou l'améliorer

Apple

Les ordinateurs ***Apple Macintosh*** ont été conçus pour une mise en réseau facile dans une situation de groupe de travail d'égal à égal. Les interfaces réseau sont intégrées au matériel, de même que des composants réseau le sont au système d'exploitation Macintosh. Il existe des adaptateurs réseau Ethernet et Token Ring pour le Macintosh.

Les Mac peuvent également être connectés à des réseaux locaux de PC contenant des serveurs Microsoft, NetWare ou UNIX.

Mac OS X (10)

Le système d'exploitation du Macintosh, Mac OS X, est parfois appelé Apple System 10.

Certaines des fonctions de Mac OS X se trouvent dans l'interface graphique appelée *Aqua*

Une nouvelle fonction de Mac OS X autorise la connectivité entre AppleTalk et Windows. Le système d'exploitation Mac OS X central est appelé *Darwin*. Darwin est un système fondé sur UNIX et offrant stabilité et performances élevées. Ces améliorations permettent à Mac OS X de gérer la mémoire protégée, le multitâche préemptif, la gestion avancée de la mémoire et le multitraitement symétrique. ➔ Avantages.

Concept de service sur les serveurs

Les systèmes d'exploitation de réseau sont conçus pour fournir des processus de réseau aux clients.

- Services Web (HTTP)
- Transfert de fichiers (FTP)
- Système de noms de domaine (DNS)
- Messagerie électronique (POP3, SMTP et IMAP)
- Partage de fichiers (NFS, SMB)
- Services d'impression (LPD)
- Protocole DHCP (Dynamic Host Configuration Protocol)

Tous ces processus réseau sont appelés des *services* sous Windows 2000 et des *démons* sous UNIX et Linux.

Administration réseau :

Présentation de l'administration réseau

Taches d'administration du réseau :

- Facilité d'utilisation
- Capacité de rétablissement
- Contrôle de la disponibilité du réseau
- Automatisation améliorée
- Contrôle des temps de réponse
- Fonctions de sécurité
- Possibilité d'ajouter et de supprimer des utilisateurs
- Réacheminement du trafic
- Enregistrement des utilisateurs

Les facteurs qui rendent nécessaire l'administration réseau :

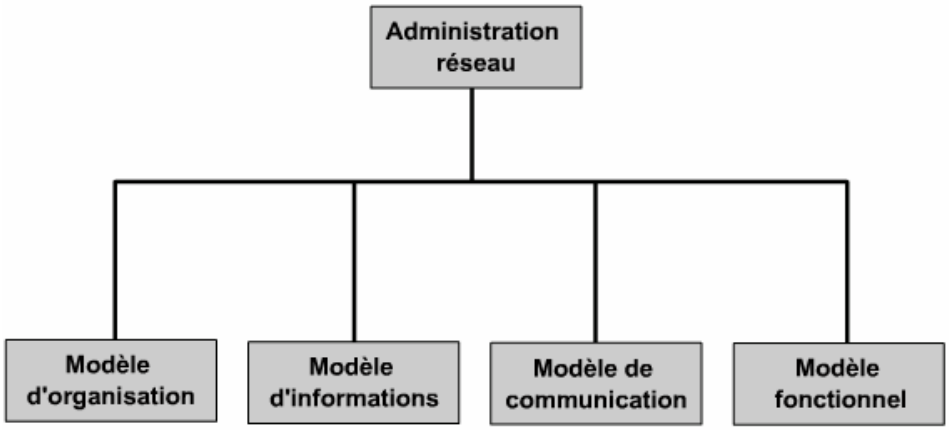
- Contrôle des actifs de l'entreprise
- Contrôle de la complexité
- Amélioration du service
- Amélioration de l'automatisation
- Équilibrage des divers besoins
- Réduction des périodes d'indisponibilité
- Contrôle des coûts

Terminologie basique de l'administration réseau :

SNMP	SNMP (Simple Network Management Protocol) est une norme universelle définie par l'IETF, destinée à la gestion des ressources réseau.
MIB	La base d'informations de management (MIB - Management Information Base) est la structure/la définition des données d'un objet géré.
RMON	RMON (Remote Monitoring) est une spécification d'agent/MIB définissant les fonctions de surveillance des équipements distants.
RFC	Les requêtes pour commentaires (Request For Comments ou RFC) sont des documents émis par l'IETF. Certaines ont été adoptées en tant que normes Internet.
NMS	La station d'administration réseau (Network Management Station) est une station SNMP conçue pour l'administration des équipements réseau. Il s'agit généralement d'une " boîte " UNIX ou NT qui exécute HP Openview, SunNET Mgr ou NetView pour AIX.

OSI et le modèle d'administration réseau

Le modèle d'administration se décline en quatre parties :



Le modèle d'organisation décrit les composants de l'administration réseau, par exemple administrateur, agent, et ainsi de suite, avec leurs relations.

Le modèle d'informations est relatif à la structure et au stockage des informations d'administration réseau. Ces informations sont stockées dans une base de données, appelée base d'informations de management (MIB).

Le modèle de communication traite de la manière dont les données d'administration sont transmises entre les processus agent et administrateur. Il est relatif au protocole d'acheminement, au protocole d'application et aux commandes et réponses entre égaux.

Le modèle fonctionnel concerne les applications d'administration réseau qui résident sur la station d'administration réseau (NMS).

Le modèle d'administration OSI compte *cinq domaines fonctionnels*, parfois appelés le modèle ***FCAPS***:

- Les erreurs
- La configuration
- La comptabilité
- Les performances
- La sécurité

Normes SNMP et CMIP

- Le protocole ***SNMP*** (*Simple Network Management Protocol*) – Communauté IETF
- Le protocole ***CMIP*** (*Common Management Information Protocol*) – Communauté des télécommunications

Le protocole *SNMP* (1989) désigne un ensemble de normes d'administration, notamment un protocole, une spécification de structure de base de données et un ensemble d'objets de données. Une mise à niveau, le protocole SNMP version 2c a été adoptée en 1993. ***SNMPv2c*** permet de prendre en charge les stratégies d'administration réseau centralisées et distribuées et offre des améliorations au niveau de la structure des informations d'administration (SMI), des opérations de protocole, de l'architecture d'administration et de la sécurité. Depuis, ***SNMPv3*** a été mis en circulation. Pour résoudre les défauts de sécurité de SNMPv1 et SNMPv2c, SNMPv3 fournit un accès sécurisé aux MIB en authentifiant et en cryptant les paquets acheminés sur le réseau.

CMIP est un protocole de gestion de réseaux OSI créé et normalisé par l'ISO pour la surveillance et le contrôle de réseaux hétérogènes.

Fonctionnement du protocole SNMP

Le modèle organisationnel de l'administration réseau SNMP comporte quatre éléments:

- La *station d'administration*
- *L'agent de supervision*
- *La base d'informations* de management
- *Le protocole de gestion* de réseau

La ***NMS*** est généralement une station de travail autonome, mais elle peut être mise en œuvre sur plusieurs systèmes. Elle contient un ensemble de logiciels appelés l'application d'administration réseau (*NMA*). La NMA comporte une interface utilisateur permettant aux administrateurs autorisés de gérer le réseau.

Les ***agents de supervision*** sont des logiciels modulaires résidant dans des équipements de réseau clés tels que d'autres hôtes, routeurs, ponts et concentrateurs. Ils répondent à des requêtes d'informations et des requêtes d'action émises par la NMS.

Toutes les informations de supervision d'un agent en particulier sont stockées dans la base d'informations de management de cet agent.

Un agent peut effectuer un suivi des éléments suivants:

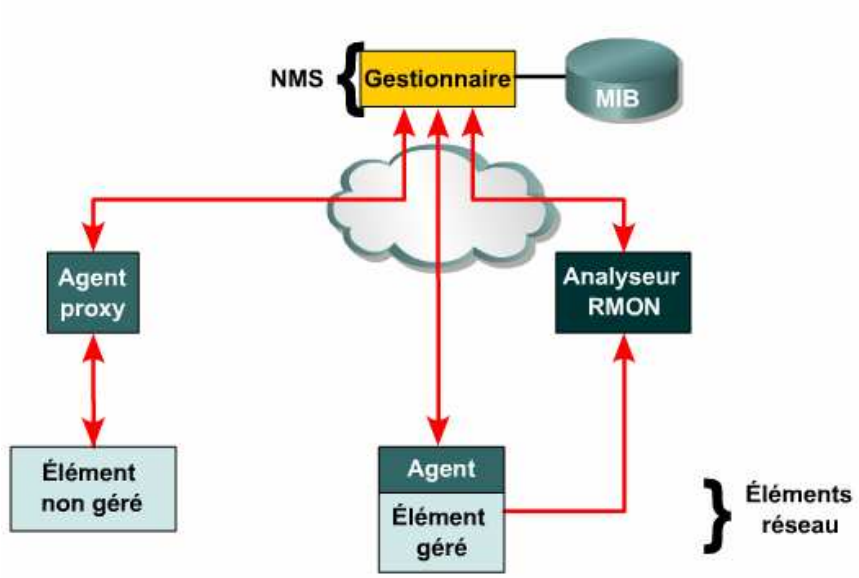
- Le nombre et l'état de ses circuits virtuels
- Le nombre de certains types de messages d'erreur reçus
- Le nombre d'octets et de paquets entrant et sortant de l'équipement
- La longueur maximale de la file d'attente de sortie pour les routeurs et autres équipements interréseaux
- Les messages de broadcast envoyés et reçus
- Les interfaces réseau qui se désactivent et s'activent

Le protocole SNMP utilise le protocole UDP et communique sur les ports 161 et 162. Il est fondé sur un échange de messages. Il existe trois types de message courants:

- ***Get*** – Permet à la station d'administration de récupérer la valeur des objets MIB à partir de l'agent.
- ***Set*** – Permet à la station d'administration de définir la valeur des objets MIB au niveau de l'agent.
- ***Trap*** – Permet à l'agent d'avertir la station d'administration lors d'événements significatifs.

Une station d'administration réseau qui souhaite obtenir des informations ou contrôler ce nœud propriétaire communique avec un ***agent proxy***. L'agent proxy traduit alors la requête SNMP de la station d'administration en un formulaire approprié au système cible, puis utilise le protocole d'administration propriétaire approprié pour communiquer avec ce système cible. Les réponses entre la cible et le proxy sont traduites en messages SNMP et renvoyées à la station d'administration.

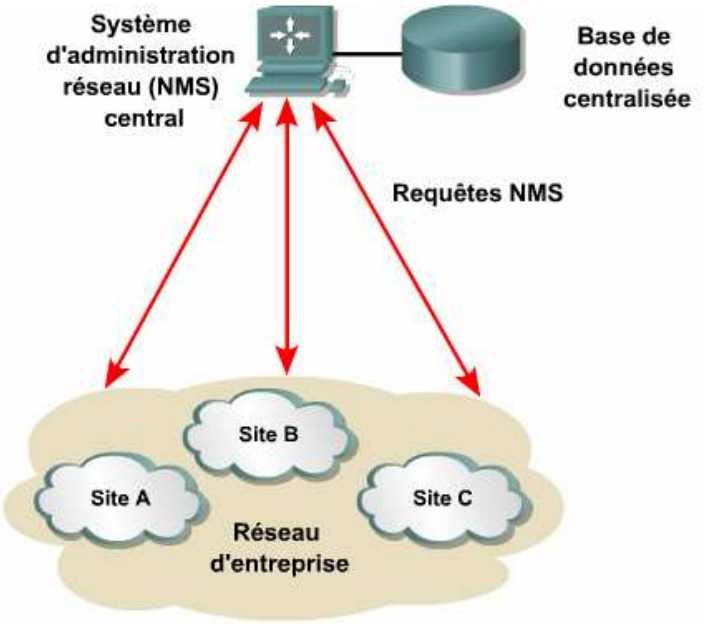
Les applications d'administration réseau déchargent souvent des fonctionnalités de gestion réseau à un analyseur distant (***RMON***). Cet analyseur RMON recueille localement des informations d'administration, puis la station d'administration réseau récupère régulièrement un résumé de ces données.



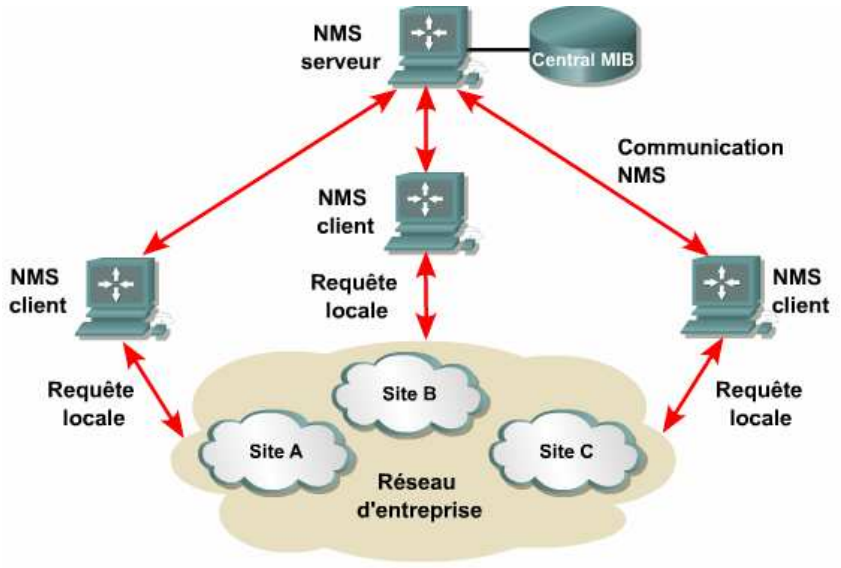
La NMS est une station de travail ordinaire, utilisant un système d'exploitation classique. Les applications d'administration réseau peuvent, par exemple, être *Ciscoworks2000*, *HP Openview* et *IBM NetView*

Architectures d'administration réseau :

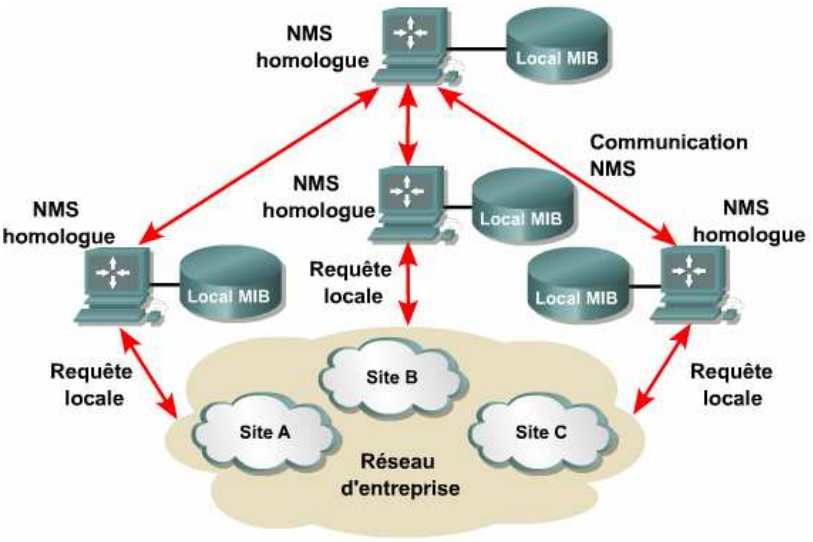
➔ Architecture centralisée :



➔ Architecture hiérarchique :



➔ Architecture distribuée :



Structure des informations d'administration et des MIB

Une base d'informations de management (MIB) définit les variables qui résident dans un nœud géré

- Définition conforme aux règles de gestion des informations d'administration (SMI)
- Chaque objet géré est décrit à l'aide d'un identificateur d'objet défini dans la structure SMI

MIB I

- 114 objets standard
- Les objets inclus sont considérés comme essentiels dans le cadre de la gestion des pannes ou de la configuration

MIB II

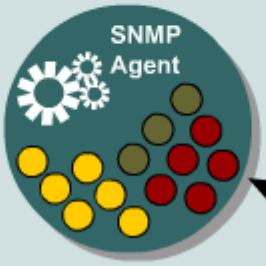
- Extension de MIB I
- 185 objets définis

Autres MIB standard

- RMON, hôte, routeur

MIB propriétaires

- Extensions des MIB standard



Des milliers d'objets administrables définis selon les règles exposées dans les normes SMI

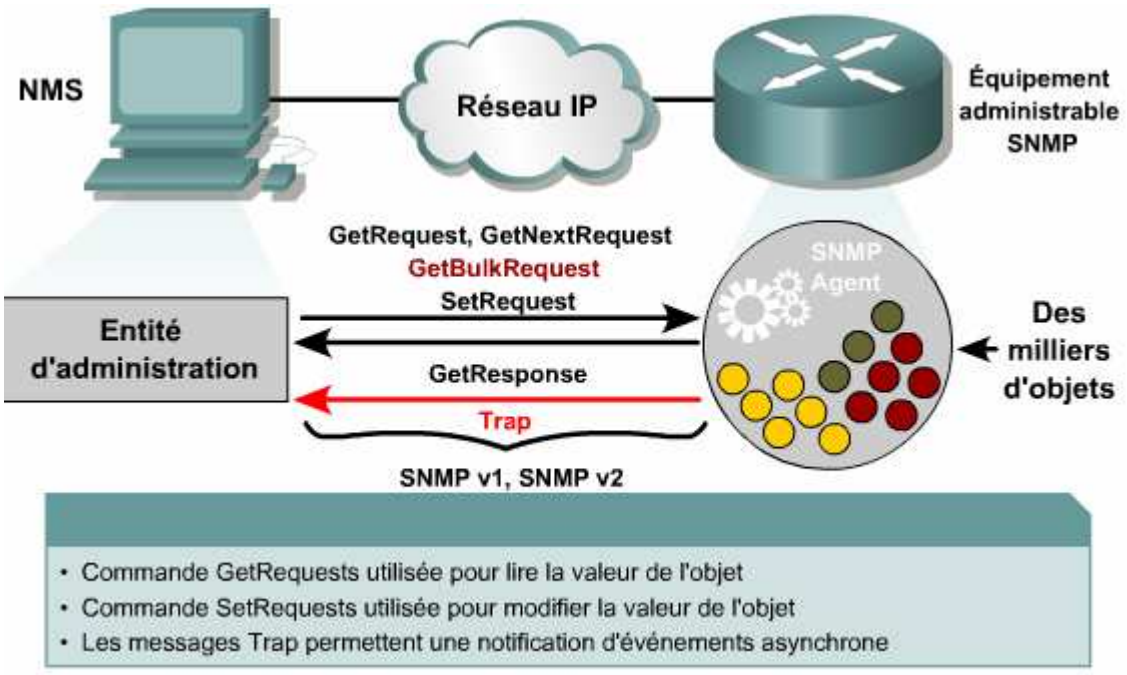
Le protocole SNMP utilise ces *identificateurs d'objet* pour identifier les variables MIB à récupérer ou à modifier

Tous les objets administrés de l'environnement SNMP sont organisés en une structure hiérarchique ou arborescente. Les objets feuille de l'arborescence, c'est-à-dire les éléments qui apparaissent dans le bas du diagramme, sont les *objets administrés*. Chaque objet administré représente une ressource, une activité ou une information associée à gérer.

Protocole SNMP

L'agent est responsable du traitement des requêtes SNMP provenant de la station d'administration. Il est également responsable de l'exécution de routines de gestion de variables définies dans les diverses bases MIB prises en charge.

Trois types de *messages SNMP sont émis pour une NMS*. Il s'agit des messages *GetRequest*, *GetNextRequest* et *SetRequest*. Ces trois messages sont reconnus par l'agent sous la forme d'un message *GetResponse*. Un agent peut émettre un message de *Trap* en réponse à un événement agissant sur la MIB et sur les ressources sous-jacentes.



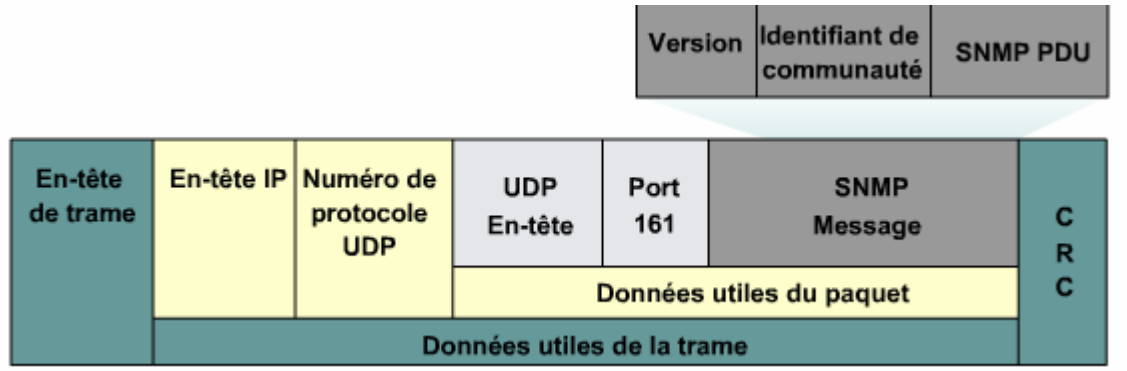
Le développement de SNMPv2c a permis de résoudre certaines limitations de SNMPv1. L'amélioration la plus remarquable a été l'introduction du type de message *GetBulkRequest* et l'ajout de *compteurs sur 64 bits* à la MIB.

- L'entité d'administration recueille des données en générant des requêtes. Cela entraîne la coexistence du trafic in-band et du trafic de production.
- L'entité d'administration reçoit des notifications d'alarmes réseau ou d'événements. Ces notifications peuvent être retransmises au gestionnaire par courrier électronique ou par SMS.
- L'entité d'administration exécute des applications afin d'analyser ou d'interpréter les données de gestion.

Remarque : La station d'administration ne sert pas seulement à récupérer des données. Elle comporte également une fonction permettant de modifier une valeur sur l'équipement administré.

Le protocole SNMP utilise le protocole d'acheminement *UDP*. Étant donné qu'UDP fonctionne sans connexion et n'est pas fiable, il se peut que le protocole SNMP perde des messages.

Chaque message SNMP contient une chaîne en texte clair, que l'on appelle ***identifiant de communauté***. L'identifiant de communauté s'utilise comme un mot de passe pour limiter l'accès aux équipements administrés.



Évitez d'attribuer à l'identifiant de communauté des valeurs par défaut bien connues :

- Accès à l'agent en lecture seule : public
- Accès à l'agent en lecture/écriture : privé

Les efforts de sécurité étaient présentés au groupe de travail *SNMPv3*. SNMPv3 accepte l'existence simultanée de plusieurs modèles de sécurité.

	Niveau	Auth	Cryptage	Que se passe-t-il ?
SNMPv1	noAuthNoPriv	Identifiant de communauté		Utilise la correspondance des identifiants de communauté pour l'authentification
SNMPv2c	noAuthNoPriv	Identifiant de communauté		Utilise la correspondance des identifiants de communauté pour l'authentification
SNMPv3	noAuthNoPriv	Nom d'utilisateur		Utilise la correspondance des identifiants de nom d'utilisateur pour l'authentification
SNMPv3	authNoPriv	MD5 or SHA		Authentification basée sur les algorithmes HMAC-MD5 ou HMAC-SHA
SNMPv3	authPriv	MD5 or SHA	DES	Cryptage DES 56 bits en plus de l'authentification basée sur DES-56

Configuration du protocole SNMP

Pour que la NMS puisse communiquer avec les équipements en réseau, SNMP doit être activé et les identificateurs de communauté SNMP doivent être configurés sur ces équipements.

Plusieurs chaînes en lecture seule sont prises en charge. Sur la plupart des systèmes, la valeur par défaut de cet identificateur de communauté est « *public* ». Il est déconseillé d'utiliser la valeur par défaut dans un réseau d'entreprise.

Router(config)#**snmp-server community string ro** → Pour configurer l'identificateur de communauté en lecture seule utilisé par l'agent

- **String** – Identificateur de communauté servant de mot de passe et autorisant l'accès.

Plusieurs chaînes en lecture-écriture sont prises en charge. Sur la plupart des systèmes, la valeur par défaut de cet identificateur de communauté est « *private* ». Il est déconseillé d'utiliser cette valeur dans un réseau d'entreprise., utilisez la commande ci-dessous :

Router(config)#**snmp-server community string rw** → Pour configurer l'identificateur de communauté en lecture-écriture utilisé par l'agent

Plusieurs chaînes peuvent être utilisées pour indiquer l'emplacement de l'équipement administré et le contact du système principal pour cet équipement.

Router(config)#**snmp-server location text**
Router(config)#**snmp-server contact text**

- **Text** – Chaîne décrivant les informations d'emplacement du système

Ces valeurs sont stockées dans les objets MIB *sysLocation* et *sysContact*

RMON

- RMON est une MIB
- RMON est basé sur les RFC de l'IETF
- Rassemblement de statistiques en analysant chaque trame sur un segment
- RMON1 est destiné à la couche liaison de données
- RMON2 est adapté pour les couches 3 (réseau) à 7 (application)
- Compatibilité avec un analyseur externe ou un module d'analyse réseau sur Catalyst

La norme RMON répertorie les fonctions de surveillance dans *neuf groupes* correspondant aux topologies Ethernet + un dixième dans pour Token Ring :

- ***Groupe de statistiques*** – Tient à jour les statistiques d'erreur et d'utilisation du sous-réseau ou du segment en cours de supervision. Il s'agit, par exemple, de l'utilisation de la bande passante, du broadcast, du multicast, de l'alignement CRC, des fragments, et ainsi de suite.
- ***Groupe de l'historique*** – Conserve des échantillons statistiques périodiques du groupe des statistiques et les stocke en vue d'une extraction ultérieure. Il s'agit, par exemple, de l'utilisation, du nombre d'erreurs et du nombre de paquets.
- ***Groupe des alarmes*** – Permet à l'administrateur de configurer l'intervalle et le seuil d'échantillonnage pour tout élément enregistré par l'agent. Il s'agit, par exemple, des valeurs absolues et relatives, ou des seuils en augmentation ou en diminution.

- ***Groupe des systèmes hôtes*** – Définit la mesure des différents types de trafic en provenance et à destination des systèmes hôtes connectés au réseau. Il s'agit, par exemple, des paquets envoyés ou reçus, des octets envoyés ou reçus, des erreurs et des paquets de broadcast et de multicast.
- ***Groupe des systèmes hôtes TopN*** – Génère un rapport des systèmes hôtes TOPN en s'appuyant sur les statistiques du groupe des systèmes hôtes.
- ***Groupe des matrices de trafic*** – Stocke les erreurs et les statistiques d'utilisation relatives aux paires de nœuds qui communiquent sur le réseau. Il s'agit, par exemple, des erreurs, des octets et des paquets.
- ***Groupe des filtres*** – Moteur de filtrage qui génère un flux de paquets à partir de trames correspondant au schéma défini par l'utilisateur.
- ***Groupe d'interception des paquets*** – Définit la méthode de mise en tampon interne des paquets qui répondent aux critères de filtrage.
- ***Groupe des événements*** – Permet de consigner des événements, également appelés pièges générés, à l'intention de l'administrateur, avec date et heure. Il s'agit par exemple de rapports personnalisés s'appuyant sur le type d'alarme

Syslog

Le protocole ***syslog*** s'utilise pour permettre aux équipements Cisco d'envoyer des messages non sollicités (activités et des conditions d'erreur) à une station d'administration réseau.

Chaque message syslog consigné est associé à un horodatage, une installation, une gravité et un message de consignation en texte.

Le niveau de gravité indique la nature cruciale du message d'erreur. Il existe huit niveaux :

0 Urgences
1 Alertes
2 Critique
3 Erreurs
4 Avertissements
5 Notifications
6 Informations (par défaut)
7 Débogage

Pour que la NMS puisse recevoir et consigner les messages système d'un équipement, syslog doit être configuré sur ce dernier.

Router(config)#**logging on** → Pour activer la consignation sur toutes les destinations

Router(config)#**logging hostname | ip address** → Pour envoyer des messages de consignation du journal vers un hôte du serveur syslog, tel que CiscoWorks2000

Router(config)#**logging trap informational** → Pour définir le niveau de gravité sur 6
Router(config)#**service timestamps log datetime** → Pour inclure l'horodatage avec le message.