

CCNA 4 - Essentiel

Réseaux et technologies WAN

www.tri.on.ma

Table des matières

1. NAT et PAT	4
1.1. Adressage privé et public	4
1.2. Translation d'adresses	4
1.2.1. Principe du NAT	4
1.2.2. Principe du PAT	6
1.3. Configuration	6
1.3.1. Commandes	6
1.3.2. Procédure de configuration	7
1.3.3. Vérification	7
2. Protocole DHCP	8
2.1. Introduction	8
2.1.1. Comparatif entre BOOTP et DHCP	8
2.1.2. Opération DHCP	9
2.1.3. Relais DHCP	10
2.2. Configuration	11
2.2.1. Commandes	11
2.2.2. Procédure de configuration	12
2.2.3. Vérification	12
3. Réseaux WAN	13
3.1. Définitions	13
3.2. Equipements et dispositifs	14
3.3. Normes WAN	15
3.4. Classement des différents types de liaison WAN	17
4. Conception WAN	19
4.1. Communication dans un WAN	19
4.2. Premières étapes de la conception WAN	19
4.3. Modèle de réseau hiérarchique	20
4.3.1. Modèle à 3 couche	21
4.3.2. Modèle à 2 couche	22
4.3.3. Modèle à 1 couche	23
5. Protocole PPP	24
5.1. Etude du protocole	24
5.2. Etablissement d'une session	25
5.3. Authentification/Configuration	25
5.3.1. Procédure de configuration du protocole PAP	27
5.3.2. Procédure de configuration du protocole CHAP	27
6. Technologies RNIS	29
6.1. Technologie	29
6.2. Termes et équipements	30
6.3. Normes	31
6.4. Utilisation/Implémentation	32
6.5. Routage à établissement de la connexion à la demande (DDR)	33
6.6. Commandes	34
6.7. Configuration	36

7. Technologies Frame Relay	37
7.1. Technologie	37
7.2. Interface LMI & DLCI	38
7.3. Fonctionnement, table de commutation et processus de transmission.....	39
7.4. Les sous interfaces Frame Relay.....	41
7.5. Commandes	42
7.6. Configuration.....	44
8. Initiation à l'administration réseau	45
8.1. Stations de travail et serveurs	45
8.1.1. Stations de travail	45
8.1.2. Serveurs.....	45
8.2. Systèmes d'exploitation réseau.....	45
8.2.1. Systèmes d'exploitation réseau Microsoft Windows	46
8.2.2. Systèmes d'exploitation réseau UNIX et Linux.....	46
8.2.3. Système d'exploitation réseau Apple	47
8.3. Gestion du réseau.....	47
8.3.1. Introduction à la gestion réseau.....	47
8.3.2. Modèle de gestion réseau et OSI.....	48
8.4. Protocole SNMP	49
8.4.1. Introduction	49
8.4.2. Fonctionnement.....	49
8.4.3. MIB	52
8.4.4. Configuration	53
8.4.5. RMON.....	54
8.5. Syslog	57
8.5.1. Fonctionnement.....	57
8.5.2. Configuration	58

1. NAT et PAT

1.1. Adressage privé et public

La très forte croissance et popularité d'Internet dans le début des années 90 ont menée très rapidement à la saturation des adresses pouvant être fournies par le protocole IP version 4. C'est entre autres pourquoi le système d'adressage privé a été élaboré, de manière à ralentir l'inévitable, à savoir l'épuisement de toutes les adresses IPv4.

Les plages d'adresses privées définies par la RFC 1918 sont les suivantes :

Classe d'adresses	Plage d'adresses privées	CIDR correspondant
A	De 10.0.0.0 à 10.255.255.255	10.0.0.0/8
B	De 172.16.0.0 à 172.31.255.255	172.16.0.0/12
C	De 192.168.0.0 à 192.168.255.255	192.168.0.0/16

Ces plages d'adresses privées utilisées conjointement à la translation d'adresses, permettent à plusieurs réseaux d'utiliser les mêmes adresses. La translation d'adresse prend alors tout son intérêt en traduisant, ou remplaçant, les adresses privées en une ou plusieurs adresses publiques afin de transiter sur Internet.

Ceci crée donc plusieurs « cellules » d'adresses privées pouvant être identiques pour différents réseaux, sachant que chaque cellule ne serait accessible depuis Internet que par la ou les adresses publiques attribuées à chaque entreprise.

Les adresses privées étant réservée à un usage interne, ces adresses ne peuvent pas être utilisées directement sur Internet. C'est pourquoi les routeurs de bordure des FAI sont configurés pour empêcher le routage de ces adresses.

1.2. Translation d'adresses

La translation d'adresse est un processus générique permettant la substitution d'une adresse par une autre, et permet ainsi de masquer les adresses privées des réseaux locaux derrière une adresse publique.

Ce processus existe sous deux variantes :

- **NAT** (Network Address Translation)
 - Statique
 - Dynamique
- **PAT** (Port Address Translation)

1.2.1. Principe du NAT

Le NAT a été fait pour économiser des adresses IP en permettant la translation d'adresses IP privées (RFC1918), internes à une entité (une entreprise, une école etc.) en une ou plusieurs adresses IP publiques routable sur Internet.

Remarque : l'adresse IP utilisée pour la translation n'est pas forcément une adresse IP public et peut être à nouveau une adresse IP privée qui, à son tour, pourra être traduite.

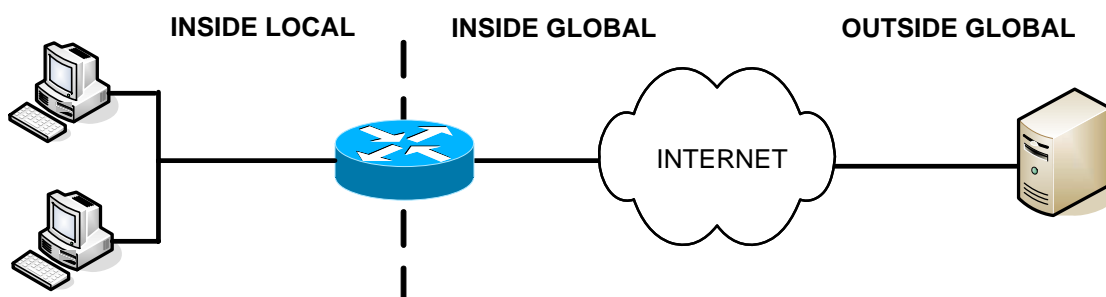
Cette translation d'adresse est effectuée principalement sur les routeurs de bordure d'une entreprise connectée à Internet. Le réseau utilisant les adresses IP privées est ainsi appelé le réseau interne (**inside**), tandis que la partie du réseau utilisant des adresses IP publiques (Internet) est appelé le réseau externe (**outside**).

Quand un utilisateur du réseau interne (inside) souhaite communiquer avec un hôte du réseau externe (outside), le routeur reçoit le paquet avec l'adresse IP privée et réécrit le paquet en changeant l'adresse IP source avec l'adresse IP public du routeur (c'est l'opération de translation).

Le routeur consulte ensuite sa table de routage pour acheminer le paquet jusqu'à la bonne destination. Le destinataire recevra le paquet avec comme source l'adresse IP public du routeur et non l'adresse IP privée de l'hôte qui envoie le paquet dans le réseau interne.

Au-delà des appellations « inside » et « outside », Cisco définit 4 types d'adresses pour le NAT :

- **Inside local address**
 - Adresse IP attribuée à un hôte dans le LAN.
- **Inside global address**
 - Adresse(s) IP attribuée(s) par le FAI reconnue(s) par l'Internet pour représenter le LAN.
- **Outside local address**
 - Adresse IP d'un hôte du réseau externe telle qu'elle est connue par les utilisateurs du réseau interne. La plupart du temps, celle-ci est identique à l'« outside global address ».
- **Outside global address**
 - Adresse IP attribuée à un hôte dans le réseau externe.



Le NAT peut être utilisé dans plusieurs cas, cependant il peut être configuré de deux manières différentes statiquement ou dynamiquement.

- **Le NAT statique** traduit une adresse IP privée avec toujours la même adresse IP publique. S'il y a 4 utilisateurs nécessitant une traduction d'adresse, il faudra donc utiliser 4 adresses IP publiques.
- **Le NAT dynamique** traduit une adresse privée avec une adresse IP publique appartenant à un pool d'adresses. L'adresse IP publique utilisée pour la traduction n'est donc pas toujours la même. S'il n'y a pas assez d'adresses IP publiques disponibles les utilisateurs devront attendre qu'une adresse se libère pour pouvoir être traduite.

L'avantage du NAT, en plus de la grande économie d'adresses IP, est de ne pas avoir à refaire tout l'adressage IP lorsque l'on change de fournisseur d'accès internet.

Cette technologie apporte également de la sécurité au sein du réseau interne puisque les machines qui s'y trouvent ne sont pas accessibles depuis l'extérieur.

1.2.2. Principe du PAT

Le **PAT** (Port Address Translation) ou Overloading permet d'attribuer une seule adresse IP publique pour la translation de plusieurs adresses IP privées. Chaque utilisateur est différencié grâce à un numéro de port unique qui lui est attribué lorsqu'il souhaite communiquer.

Etant donné qu'il existe 65536 ports différents, un routeur pourrait traduire jusqu'à 65536 adresses IP privées différentes. Cependant en réalité, un équipement ne peut gérer en moyenne que la translation d'environ 4000 ports par adresse IP publique.

1.3. Configuration

1.3.1. Commandes

- **ip nat inside**
 - Mode de configuration d'interface
 - Spécifie l'interface inside.
 - Complémentaire des autres commandes NAT
- **ip nat outside**
 - Mode de configuration d'interface
 - Spécifie l'interface outside
 - Complémentaire des autres commandes NAT
- **ip nat inside source static {local-ip} {global -ip}**
 - Mode de configuration globale
 - Etablit une translation statique entre une 'Inside local address' et une 'Inside global address'
- **access-list {numéro} permit {prefix} {wildcard_mask}**
 - Mode de configuration globale
 - Spécifie le ou les réseaux autorisés à être traduits
- **ip nat inside source list {numéro} pool {nom_du_pool}**
 - Mode de configuration globale
 - Définit le pool qui va être traduit
- **ip nat pool {nom_du_pool} {première-ip} {dernière-ip} netmask {masque_de_sous-reseau}**
 - Mode de configuration globale
 - Spécifie le pool d'adresses IP : toutes les adresses IP entre première-ip et dernière-ip
- **ip nat inside source list {numéro} interface type {numéro} overload**
 - Mode de configuration globale
 - Configuration du PAT sur l'interface outside
- **clear ip nat translation**
 - Mode privilégié
 - Configuration du PAT sur l'interface outside

1.3.2. Procédure de configuration

- Spécifier les interfaces outside et inside (ip nat outside / inside)
 - NAT statique :
 - Spécifier chaque adresse une par une (ip nat inside source static ip1 ip2)
 - NAT dynamique :
 - Spécifier le bloc privé
 - Spécifier le pool public
 - Activer le NAT avec le bloc privé et le pool public en argument.
 - PAT :
 - Spécifier le bloc privé
 - Activer le NAT sur l'interface outside avec le bloc privé en argument.

1.3.3. Vérification

- show ip nat translations
 - Mode privilégié
 - Affiche des informations sur chaque translation en cours en particulier le temps depuis lequel elle est active.
- show ip nat statistics
 - Mode privilégié
 - Configuration du PAT sur l'interface outside
- show running-config
 - Mode privilégié
 - Affiche la configuration du routeur.
- debug ip nat
 - Mode privilégié
 - Affiche en temps réel toute les paquets traduits.

2. Protocole DHCP

2.1. Introduction

DHCP (Dynamic Host Configuration Protocol) est un protocole fonctionnant en mode Client – Serveur. Il fournit aux clients une configuration de couche 3 : principalement une adresse (IP), mais aussi des adresses de passerelle ou de serveur DNS, NETBIOS, noms de domaines, ...

Ce protocole permet une gestion dynamique de l'adressage de niveau 3. Il allège ainsi grandement les tâches de l'administrateur réseau.

Les **clients DHCP** sont fournis aux utilisateurs sur la plupart des systèmes d'exploitation. Grâce à l'envoi d'une requête au serveur, ceux-ci peuvent se voir attribuer une adresse de couche 3. Seuls les équipements utilisateurs doivent bénéficier de ce service, les serveurs et équipements réseaux devant être adressés de façon statique.

Le DHCP fonctionne sur un principe de location ou bail. Le serveur attribue une adresse à un client pour une durée prédéterminée (en jours, minutes, secondes). Le client doit donc effectuer à nouveau une demande pour voir son bail reconduit.

Il existe trois types d'allocation d'adresse :

- **Automatique** : une adresse IP permanente est attribuée automatiquement au client. Un mappage statique (mac – IP) permet de retrouver la même adresse lors d'une déconnexion / reconnexion.
- **Manuelle** : l'attribution est faite manuellement par l'administrateur réseau (mappage statique). Le protocole DHCP se charge d'envoyer ces informations au client lors d'une demande.
- **Dynamique** : l'attribution se fait à la volée. Une IP libre est attribuée à un client en faisant la demande, pour une durée déterminée.

Les **serveurs DHCP** sont généralement gérés par des serveurs d'entreprise (service généralement assuré par l'OS), mais ils peuvent également être configurés sur les routeurs.

2.1.1. Comparatif entre BOOTP et DHCP

BOOTP (Bootstrap Protocol) est l'ancêtre du protocole DHCP. Son but était d'attribuer une configuration de couche 3 aux stations de travail fonctionnant sans disque dur. DHCP reprend plusieurs de ses caractéristiques :

- Fonctionne en mode client - serveur
- Utilise les ports UDP 67 (serveur) et 68 (client), appelés ports BOOTP
- Attribue une adresse IP
- Attribue un masque de sous-réseau
- Attribue une adresse de passerelle
- Attribue une adresse de serveur DNS

Le protocole BOOTP alloue les adresses de façon statique : le serveur BOOTP doit posséder au préalable une table de correspondance mac – IP pour attribuer une IP. BOOTP n'a pas de notion de bail et fait donc une liaison permanente entre un hôte et l'adresse IP qu'il lui donnera.

Enfin, le protocole DHCP peut fournir jusqu'à 30 options de configuration, contre 4 seulement pour BOOTP (IP, masque, adresse de passerelle, adresse du DNS).

Laboratoire SUPINFO des Technologies Cisco

Site Web : www.labo-cisco.com – E-mail : labo-cisco@supinfo.com

Ce document est la propriété de SUPINFO et est soumis aux règles de droits d'auteurs

2.1.2. Opération DHCP

La configuration d'un client avec le protocole DHCP se fait en 4 étapes :

1) **DHCP DISCOVER :**

- Lorsqu'une configuration DHCP cliente est présente sur un poste utilisateur, celui-ci envoie une requête en broadcast aux serveurs DHCP, appelée DHCP DISCOVER.

2) **DHCP OFFER :**

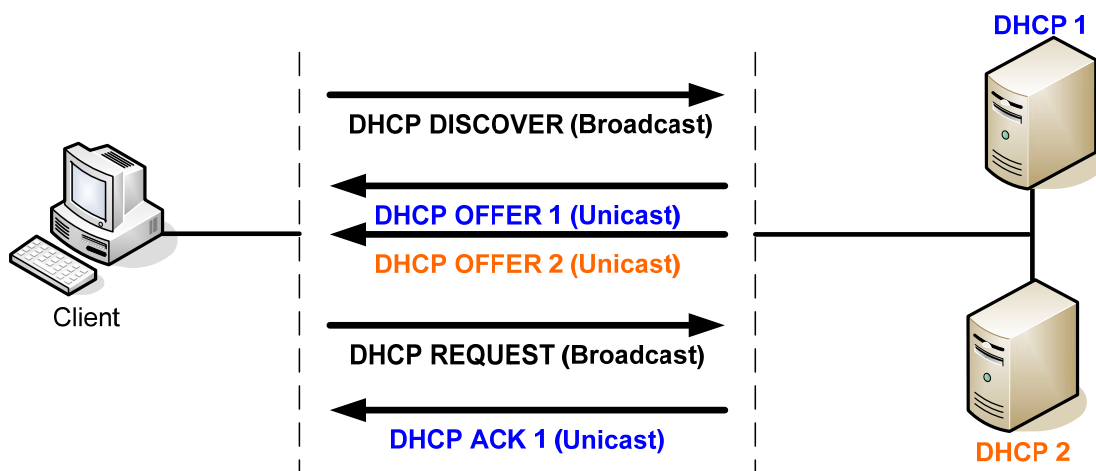
- Les serveurs DHCP recevant le broadcast et pouvant répondre à la demande, envoient une requête en unicast au client. Ce DHCP OFFER contient toutes les informations nécessaires au client (IP, adresse de passerelle, durée du bail, serveur DNS, WINS, etc.).

3) **DHCP REQUEST :**

- Le client émet ensuite une requête en broadcast afin de confirmer l'offre qu'il a sélectionnée (celle qui lui est arrivée en premier).
- S'il y avait plusieurs serveurs DHCP, tous sont alors au courant et peuvent libérer leur offre en conséquence.
- S'il s'agit d'un renouvellement de bail, le client propose au serveur l'IP qu'il veut se voir réattribuer.

4) **DHCP ACK :**

- Cette confirmation est envoyée en unicast par le serveur DHCP au client. Une fois le DHCP ACK reçu, le client peut alors utiliser l'adresse IP ainsi que le reste de la configuration attribuée.



Il existe trois autres requêtes DHCP :

- **DHCP DECLINE :** Si le client détecte l'IP qu'on lui a proposée sur le même segment réseau, il envoie cette requête au serveur. Le processus redémarre alors.
- **DHCP NACK :** Lorsqu'un serveur détecte que l'IP pour laquelle il doit renvoyer un ACK est déjà présente sur le réseau, il envoie un DHCP NACK. Le processus doit alors redémarrer pour le client concerné.
- **DHCP RELEASE :** Lorsqu'un client veut annuler le bail (arrêt du système, commande `ipconfig /release` sous Windows), cette requête est envoyée au serveur afin qu'il libère la réservation d'adresse.

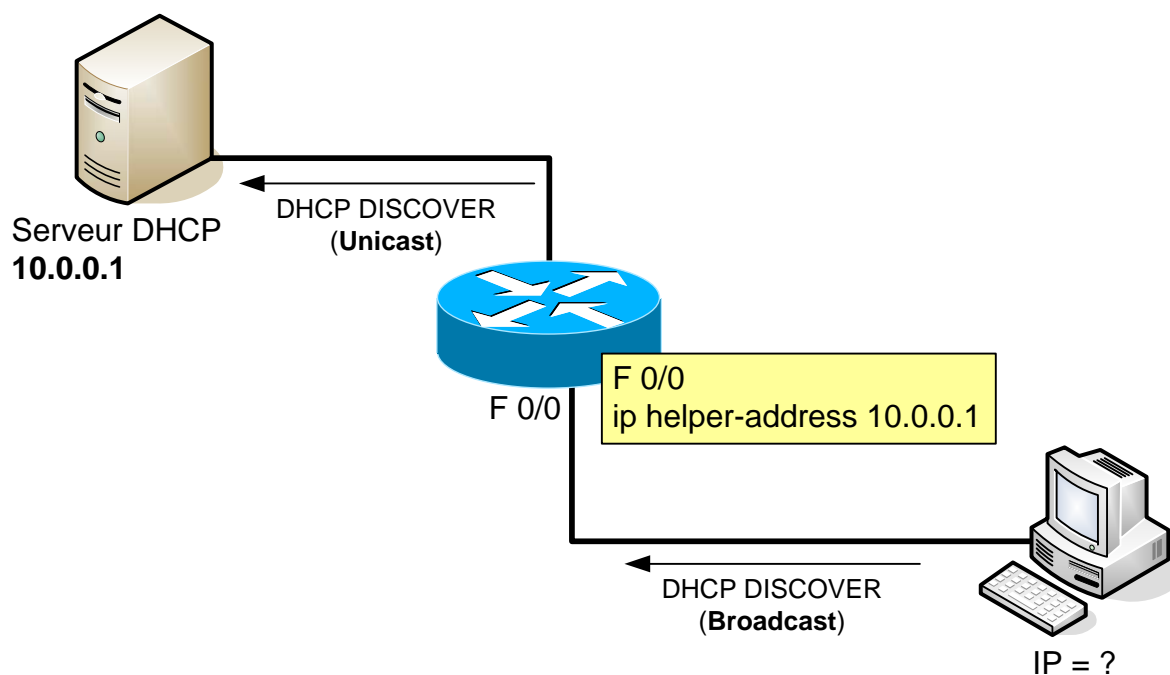
2.1.3. Relais DHCP

Les serveurs DHCP font partie des serveurs d'entreprise. Il est très courant que ces serveurs soient placés sur un sous-réseau différent de celui des utilisateurs.

Un problème se pose donc : les requêtes clientes étant envoyées au serveur DHCP en broadcast, un routeur segmentant le réseau arrêtera également ces broadcast. Il en va de même pour les services DNS, TFTP, TACACS (service d'authentification), etc.

Il est possible d'éviter ce problème en appliquant la commande `ip helper-address` sur l'interface d'un routeur. Celle-ci permet de relayer les broadcast UDP vers une adresse unicast définie. Ce relais se fait au niveau des services UDP suivants :

- Protocole Time
- TACACS
- Le protocole DNS
- Le service BOOTP/DHCP
- TFTP
- Le service NetBIOS



2.2. Configuration

Comme pour le NAT, la configuration DHCP nécessite la définition de groupe(s) de plages d'adresses attribuables.

2.2.1. Commandes

- **ip dhcp pool {nom_groupe}**
 - Mode de configuration globale
 - Passe en mode de configuration DHCP
 - Spécifie et nomme un groupe d'adresses
- **ip dhcp excluded-address {prefix} [prefix2]**
 - Mode de configuration globale
 - Spécifie l'adresse ou la plage d'adresses à exclure du DHCP
- **[no] service dhcp**
 - Mode de configuration globale
 - Active/désactive le service DHCP
 - Actif par défaut
- **network {prefix} {masque}**
 - Mode de configuration DHCP
 - Spécifie la plage d'adresses attribuables
- **default-router {prefix}**
 - Mode de configuration DHCP
 - Spécifie la passerelle par défaut
- **dns-server {prefix} [prefix2, prefix3, ...]**
 - Mode de configuration DHCP
 - Spécifie le(s) serveur(s) DNS
- **netbios-name-server {prefix}**
 - Mode de configuration DHCP
 - Spécifie l'adresse du serveur NETBIOS WINS
- **domain-name {nom}**
 - Mode de configuration DHCP
 - Spécifie le nom du domaine
- **lease {infinite | jours [heures] [minutes]}**
 - Mode de configuration DHCP
 - Spécifie la durée du bail
 - Valeur par défaut : 1 jour
- **ip helper-address {prefix}**
 - Mode de configuration d'interface
 - Relaye les broadcast UDP (reçus sur l'interface) vers l'adresse unicast spécifiée.

2.2.2. Procédure de configuration

Voici la procédure permettant de configurer le service DHCP sur un routeur Cisco :

- Définir le nom du groupe d'adresses (commande ip dhcp pool)
- Définir les plages d'adresses attribuables (commande network)
- Spécifier la passerelle par défaut (commande default-router)
- Exclure les adresses IP statiques (commande ip dhcp excluded-address)

Commandes optionnelles :

- Spécifier l'adresse du serveur DNS (commande dns-server)
- Spécifier la durée du bail (commande lease)
- Spécifier l'adresse du serveur NETBIOS (commande netbios-name-server)
- Spécifier le nom de domaine (commande domain-name)
- Relayer les broadcast vers le serveur concerné (commande ip helper-address)

2.2.3. Vérification

Deux commandes show permettent de vérifier le bon fonctionnement du protocole DHCP :

- show ip dhcp binding
 - Mode privilégié
 - Affiche les liaisons créées par DHCP (mac – IP)
 - Affiche la date de fin du bail
 - Affiche le type d'allocation d'adresse (Automatique, Manuel, Dynamique)
- show ip dhcp server statistics
 - Mode privilégié
 - Affiche les requêtes DHCP envoyées et reçues

3. Réseaux WAN

3.1. Définitions

Caractéristiques principales des réseaux WAN :

- Fonctionnent sur de vastes étendues géographiques.
- Utilisent les services d'un opérateur Télécom.
- Transportent différents types de trafic (Voix, données, vidéo).
- Axés sur les couches physique et liaison de données du modèle OSI.

La boucle locale est la partie située entre le POP du client et le central téléphonique de l'opérateur.

Un réseau WAN, d'un point de vue général, est un ensemble de liaisons reliées aux différents opérateurs, qui sont interconnectés.

Le rôle des opérateurs Télécom est de fournir une communication bout à bout, en utilisant diverses méthodes de commutation (circuits, paquets, cellules), tout en fournissant des services.

Les trois grands types de services fournis par un opérateur Télécom sont :

Établissement de la communication :

- Aussi appelé signalisation, ce service permet d'établir ou de mettre fin à la communication entre les utilisateurs du système téléphonique.

Transit des données :

- **Multiplexage temporel** : Principe simple qui permet d'allouer l'intégralité de la bande passante disponible d'une liaison par tranche de temps fixe, affectée à chaque utilisateur.
- **Partage de bande passante** : Il existe une bande passante totale disponible sur le backbone, et les clients qui y sont rattachés se la partagent.

Le chemin de réseau WAN reliant les ETDD est appelé :

- Liaison.
- Circuit.
- Canal.
- Ligne.

Le but principal de l'ETCD est de servir d'interface entre l'ETDD et la liaison de communication WAN de l'opérateur :

L'ETDD fournit les données de l'utilisateur (Exemple : routeur).

L'ETCD convertit le format des données de l'utilisateur en un format acceptable par les unités du service réseau WAN (Exemple : modem, unité CSU/DSU, TA, NT1).

Il existe deux types de circuits :

- **Circuit point-à-point** : Circuit physique dédié aux deux extrémités (Exemple : Circuit POTS ou RNIS une fois la commutation de circuits effectuée).
- **Circuit virtuel** : Circuit logique passant au travers d'un nuage (Exemple : Frame Relay, X.25).

Les circuits virtuels se découpent en deux catégories :

- **SVC :**

Établi dynamiquement sur demande et fermé en fin de transmission.

Communication en trois phases : Etablissement du circuit, transfert des données et fermeture du circuit.

Consomme de la bande passante à cause des différentes phases de la communication.

Coûts liés à la disponibilité (Temps) du circuit réduit.

- **PVC :**

Établi en permanence.

Est utilisé pour transmettre des débits de données constantes.

Communication en une phase : Transfert des données.







Consommation en bande passante réduite par rapport à un SVC.

Coûts supérieurs en raison de la continuité de service.

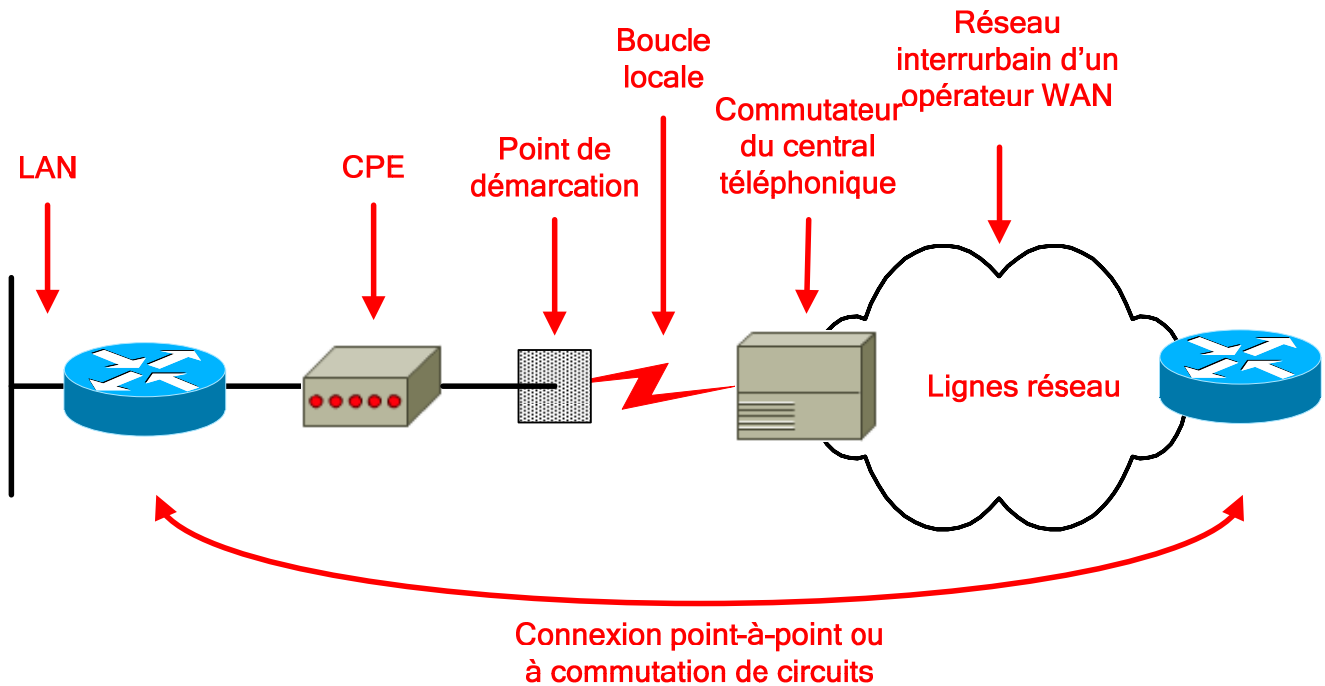
Exemples de lignes WAN et bande passante associée :

Type de ligne	Bande passante
T1	1.544 Mbits/s
E1	2.048 Mbits/s
E3	34.064 Mbits/s
T3	44.736 Mbits/s

3.2. Equipements et dispositifs

	Routeur
	Serveur de communication
  	Commutateurs WAN (ATM, RNIS, etc.)
	Modem (Unité CSU/DSU, TA, NT1, etc.)

- **Routeur** : Dispositif de routage, offrant différents services dont des ports d'interface de réseau LAN et WAN.
- **Serveur de communication** : Concentrateur de communications utilisateur entrantes et sortantes.
- **Commutateur WAN** : Unité multiport qui assure les commutations du trafic WAN.
- **Modem** : Equipement de conversion d'un signal numérique en un signal analogique par l'intermédiaire du principe de modulation/démodulation.
- **Unité CSU/DSU** : Interface numérique (ou deux interfaces séparées, si les parties CSU et DSU sont séparées) qui adapte l'interface ETTD à celle d'un ETCD. Cette unité est généralement intégrée au routeur.



- **CPE** : Equipement placé dans les locaux du client, lui appartenant ou étant loué à l'opérateur (Exemple : modem).
- **Point de démarcation de service** : Démarcation entre la partie client et la partie opérateur (boucle locale). C'est à ce point que la responsabilité de chaque partie (Client et opérateur) s'arrête.
- **Boucle locale** : Partie reliant le point de démarcation de service au central téléphonique de l'opérateur.
- **Commutateur du central téléphonique** : Point de commutation le plus proche du client.
- **Réseau interurbain** : Unités et commutateur (appelés lignes réseau) situés dans le nuage de l'opérateur.

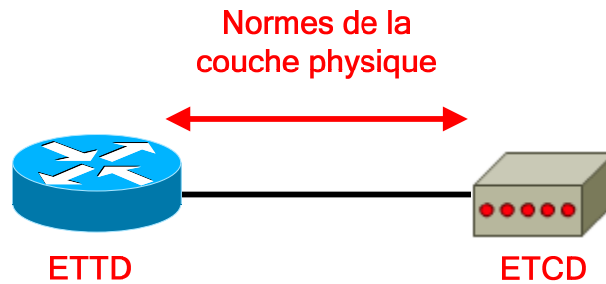
3.3. Normes WAN

Les normes des réseaux WAN décrivent généralement les méthodes d'acheminement de la couche physique ainsi que la configuration exigée pour la couche liaison de donnée, notamment :

- L'adressage.
- Le contrôle de flux.
- L'encapsulation.

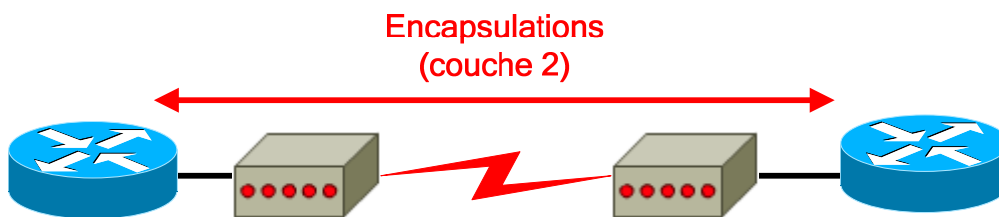
Les principaux organismes définissant et gérant les normes WAN sont :

- **UIT-T** (Union Internationale des Télécommunications - secteur de normalisation des Télécommunications), anciennement appelée CCITT (Comité Consultatif International Télégraphique et Téléphonique).
- **ISO** (International Standards Organization).
- **IETF** (Internet Engineering Task Force).
- **EIA** (Electrical Industries Association).
- **TIA** (Telecommunications Industry Association).



La couche physique d'un réseau WAN décrit principalement l'interface entre l'ETTD (unité connectée) et l'ETCD (fournisseur) :

- **EIA/TIA-232** : Similaire à la norme V.24 et anciennement appelée RS-232. Prévue pour les circuits asymétriques dont la bande passante peut atteindre 64 Kbits/s.
- **EIA/TIA-449** : Version plus rapide que l'EIA/TIA-232 (2 Mbits/s).
- **EIA/TIA-612/613** : Décrit l'interface HSSI (pour T3, E3, SDH STM-0, etc.).
- **V.24**.
- **V.35** : Décrit un protocole synchrone, utilisé pour la communication dans un réseau de paquets.
- **X.21** : Pour les lignes numériques synchrones.
- **G.703** : Connexions utilisant des connecteurs BNC et fonctionnant à des débits E1.
- **EIA-530** : Deux mises en œuvres électriques des normes EIA/TIA-449 :
 - **RS-422** : Transmissions symétriques.
 - **RS-423** : Transmissions asymétriques.



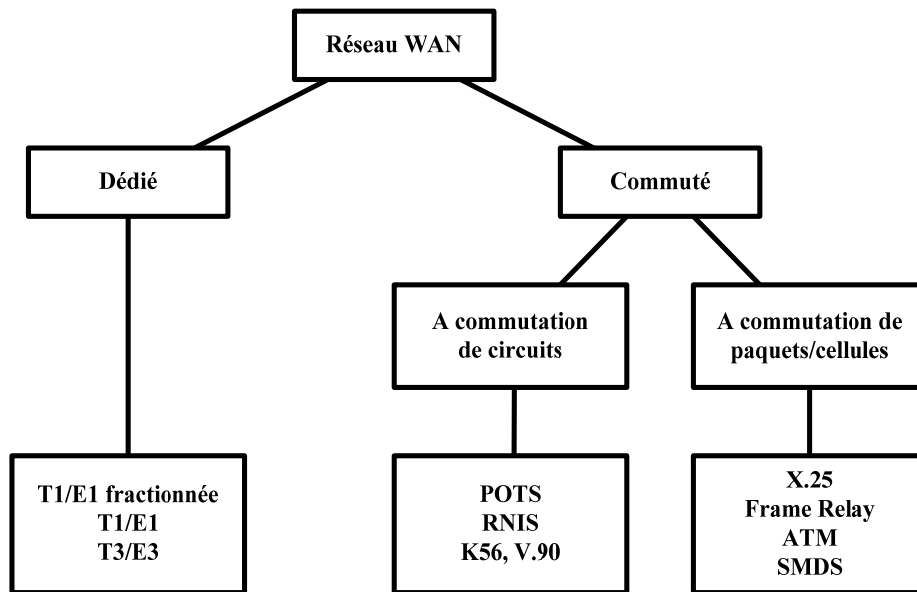
La couche liaison de données définit le mode d'encapsulation des données sur les réseaux WAN :

- **Frame Relay** :
 - Encapsulation simplifiée.
 - Dépourvue de mécanismes de correction des erreurs.
 - Prévu pour des unités numériques haut de gamme.
 - Transmet les données très rapidement par rapport aux autres encapsulations WAN.
 - Il existe deux variantes pour cette encapsulation, à savoir Cisco et IETF.
- **PPP** :
 - Comprend un champ identifiant le protocole de couche réseau.
 - Vérifie la qualité de la liaison au moment de l'établissement d'une connexion.
 - Gère l'authentification grâce aux protocoles PAP et CHAP.
- **RNIS** : Ensemble de services numériques pour la voix et les données sur le réseau commuté classique.
- **LAPB** :
 - Encapsulation des paquets à la couche 2 de la pile X.25 sur des réseaux à commutation de paquets.
 - Egalement sur des liaisons point-à-point, si elles ne sont pas fiables ou possèdent un délai inhérent (Exemple : liaison par satellite).
 - Apporte la fiabilité et le contrôle de flux sur une base point-à-point.
- **HDLC** :
 - Peut être incompatible entre fournisseurs car chacun a sa propre mise en œuvre.
 - Prend en charge les configurations point-à-point et multipoints.
 - Dérivé du protocole SDLC.
 - Protocole par défaut pour les interfaces série d'un routeur Cisco.

- Extrêmement simplifié : Pas de fonctions de fenêtrage ni de contrôle de flux.
- Champ d'adresse contenant uniquement des 1, avec un code propriétaire à 2 octets indiquant le type de verrouillage de trame du fournisseur.

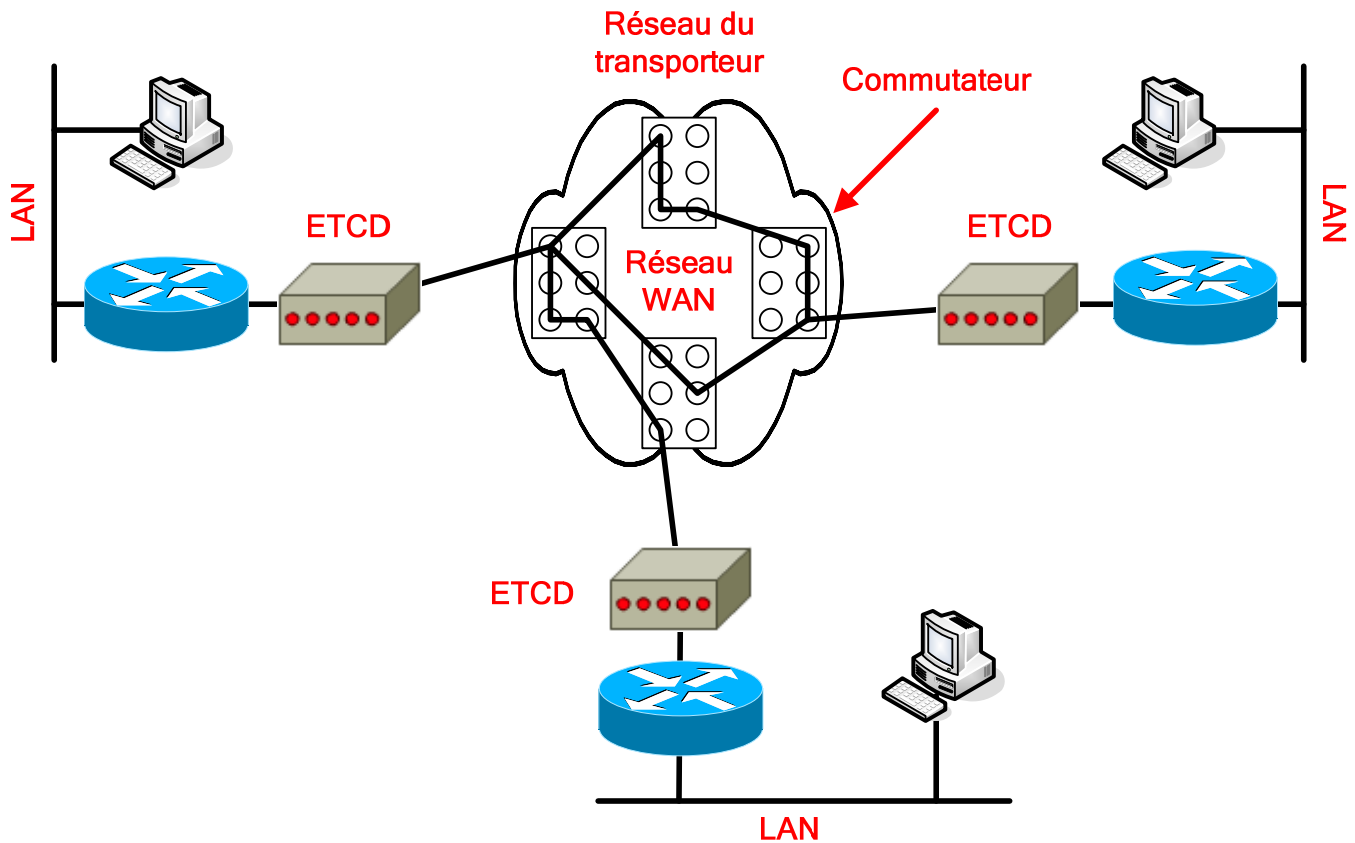
Le protocole HDLC est recommandé sur une liaison reliant deux équipements utilisant IOS. Dans le cas contraire, il est recommandé d'utiliser le protocole PPP.

3.4. Classement des différents types de liaison WAN



Les différents types de liaison WAN habituellement disponibles sont :

- **Liaisons dédiées** (aussi appelées liaisons spécialisées ou lignes louées) :
 - Fournissent un service continu.
 - Il s'agit d'un lien physique dédié qui va directement d'un port du routeur client à un port du routeur de l'opérateur, sans passer par un environnement commuté.
 - Il est nécessaire d'avoir un port par liaison client sur le routeur de l'opérateur.
 - Fournies par des liaisons série synchrone point-à-point.
 - Cette liaison point-à-point est utilisée pour :
 - Une liaison physique directe.
 - Des liaisons virtuelles constituées de plusieurs liaisons physiques.
 - Conviennent aux grands volumes d'information et aux trafics constants.
- **Connexions commutées** :
 - **A commutation de circuits** :
 - Commutation physique des centraux téléphoniques afin d'obtenir la liaison point-à-point.
 - **A commutation de paquets/cellules** :
 - Commutation « logique » effectuée au niveau de la couche 2 du modèle OSI.



Les deux grands types de liaison à commutation sont :

- **Commutation de circuits :**
 - Circuit physique dédié par commutation des centraux téléphoniques.
 - Établi, maintenu et fermé à chaque session.
 - Établi à la demande.
 - Sert aussi de ligne de secours aux circuits haut débit.
 - Offre une bande passante dédiée.
- **Commutation de paquets/cellules :**
 - Utilisation d'un PVC similaire à une liaison point-à-point.
 - Possibilité d'acheminer des trames de taille variable (paquets) ou de taille fixe (cellules).
 - Les unités du réseau partagent une liaison point-à-point unique.
 - Plus souple et utilise mieux la bande passante que les services à commutation de circuits.

4. Conception WAN

4.1. Communication dans un WAN

La communication WAN est généralement appelée « service », car elle a un coût par rapport au temps d'utilisation (Facture forfaitaire ou basée sur la consommation) contrairement à la communication LAN (Uniquement les frais d'installation du matériel), et se caractérise habituellement par :

- Un débit relativement faible (par rapport aux réseaux LAN).
- Des délais importants (liés aux distances).
- Un taux d'erreurs généralement élevé (Réseaux WAN plus soumis aux interférences extérieures).

Le choix d'un service WAN dépend principalement des critères suivants :

- Optimisation de la bande passante.
- Réduction des coûts.
- Optimisation de l'efficacité du service.

Les besoins liés aux services WAN sont parmi les facteurs suivants :

- Augmentation de l'utilisation des réseaux (Applications client/serveur, multimédia, etc.).
- Évolution permanente des exigences relatives aux logiciels (Qualité, etc.).
- Nombre de connexions à distance en constante augmentation (Utilisateurs éloignés ou mobiles, sites répartis dans le monde, communication avec les clients et les fournisseurs, etc.).
- Croissance des intranets et extranets d'entreprise (bande passante).
- Utilisation de plus en plus importante des serveurs d'entreprise.

4.2. Premières étapes de la conception WAN

Les deux principaux objectifs de la conception et de la mise en œuvre d'un WAN sont :

- Disponibilité des applications (Accès aux applications = efficacité du réseau).
- Coût (Utilisation rentable des ressources).

Ces deux critères sont fondamentalement contradictoires. Il est donc nécessaire d'observer une pondération entre la relative importance de la disponibilité des ressources et les prix de revient globaux.

La première étape de la conception d'un réseau WAN est de recueillir des informations :

- Données sur la structure et les processus de l'entreprise.
- Déterminer les personnes susceptibles de nous aider à concevoir le réseau.
- Identifier les besoins des utilisateurs (concernant la disponibilité des applications) :
 - Temps de réponse.
 - Débit.
 - Fiabilité.

Les différentes méthodes d'évaluation des besoins des utilisateurs sont :

- **Les profils des utilisateurs** : Définition des besoins des divers groupes d'utilisateurs.
- **Des entretiens, groupes de discussion et sondages** : Etablissement d'une base de référence.
- **Des entretiens aux groupes d'utilisateurs clés** : Méthode de collecte de renseignements par échantillonnage.
- **Tests du facteur humain** : Test en laboratoire avec un groupe représentatif d'utilisateurs. C'est la méthode d'évaluation la plus coûteuse et significative.

Cette analyse des besoins des utilisateurs a pour but de déterminer :

- Le type de trafic passé.
- Le niveau du trafic.
- Le temps de réponse des systèmes hôtes.
- La durée d'exécution des transferts de fichiers.
- L'utilisation de l'équipement réseau existant.

Les besoins ne sont pas statiques, il faut donc prendre en compte :

- L'accès au réseau changeant en fonction du temps (Période de pointe).
- Les différences liées au type de trafic (Sensibilité aux paquets abandonnés, exigence en bande passante).
- La nature aléatoire du trafic réseau (les heures d'utilisation peuvent changer).

Ensuite, il reste à effectuer un test de sensibilité en brisant des liaisons stables et à observer le résultat. On peut utiliser une de ces deux méthodes :

- **Supprimer une interface active** : Observation de la redirection du trafic, d'une probable perte de connectivité.
- **Modifier la charge réseau** : Observation du comportement du réseau lors de la saturation du réseau.

4.3. Modèle de réseau hiérarchique

Il existe deux structures de modèle de réseau :

- **Hiérarchique** :
 - Réseau divisé en couches.
 - Fonction(s) précise(s) associée(s) à chaque couche.
- **Maillée** :
 - Topologie linéaire.
 - Tous les dispositifs ont les mêmes fonctions.

L'intérêt d'utiliser un modèle de réseau hiérarchique lors de la conception est de :

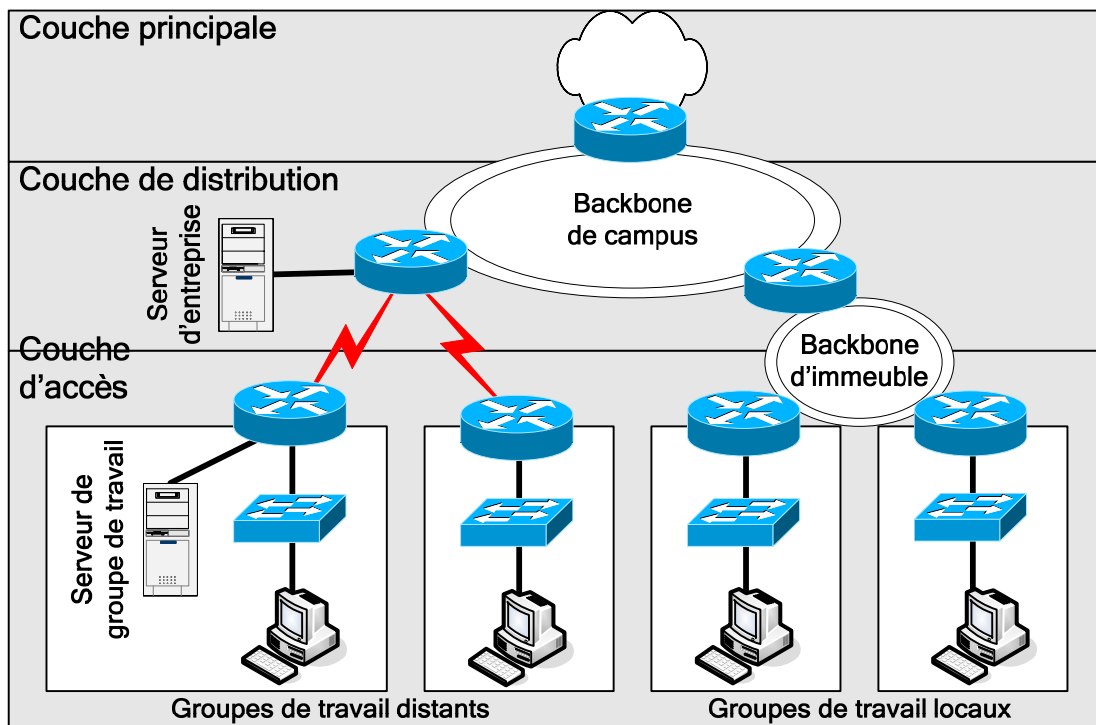
- Faciliter les modifications et la compréhension du réseau (Réseau modulaire).
- Limiter les coûts et la complexité des mises à niveau du réseau (appliquées à un sous-ensemble uniquement).
- Limiter les coûts de construction et d'élaboration du réseau.
- Faciliter l'identification des points de défaillance.

L'utilisation d'un modèle hiérarchique procure des avantages tels que :

- Évolutivité.
- Facilité de mise en œuvre.
- Facilité de dépannage.
- Prévisibilité.
- Prise en charge de protocoles.
- Facilité de gestion.

Les couches, dans un modèle de conception, sont séparées par des dispositifs de couche 3 du modèle OSI, qui séparent le réseau en domaines de broadcast.

4.3.1. Modèle à 3 couche



Les couches de ce modèle sont :

- **Couche principale** (Centrale) : Assure l'optimisation du transport entre les sites.
- **Couche de distribution** : Assure une connectivité fondée sur les politiques.
- **Couche d'accès** : Permet aux utilisateurs et aux groupes de travail d'accéder au réseau.

La couche principale :

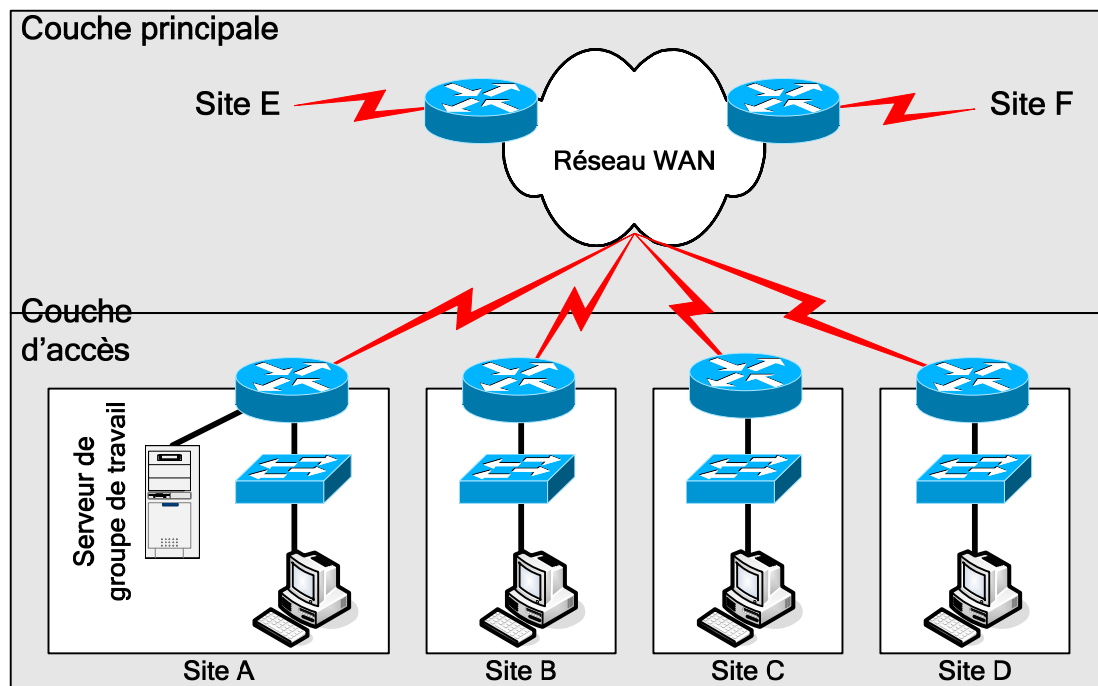
- Assure la communication (la plus rapide possible) entre les sites éloignés.
- Comporte habituellement des liaisons point-à-point.
- Aucun hôte présent, que des unités de communication.
- Services présents (Frame Relay, T1/E1, SMDS) loués auprès d'un fournisseur de services.
- Ne s'occupe pas du filtrage ou de la sécurité.
- Exigence de chemins redondants pour la continuité de service en cas de panne.
- Fonctionnalités des protocoles de routage très importantes (Partage de charge, convergence rapide).
- Utilisation efficace de la bande passante reste une préoccupation principale.

La couche distribution :

- Fournit des services à plusieurs LAN au sein d'un WAN (Backbone de campus).
- C'est l'emplacement du backbone du WAN (de type Fast Ethernet).
- Sert à interconnecter des immeubles.
- Emplacement des serveurs d'entreprise (DNS, messagerie centralisée).
- A pour rôle de définir les frontières (sous la forme de politiques).
- Prend en charge le filtrage (ACL), le routage des VLAN.

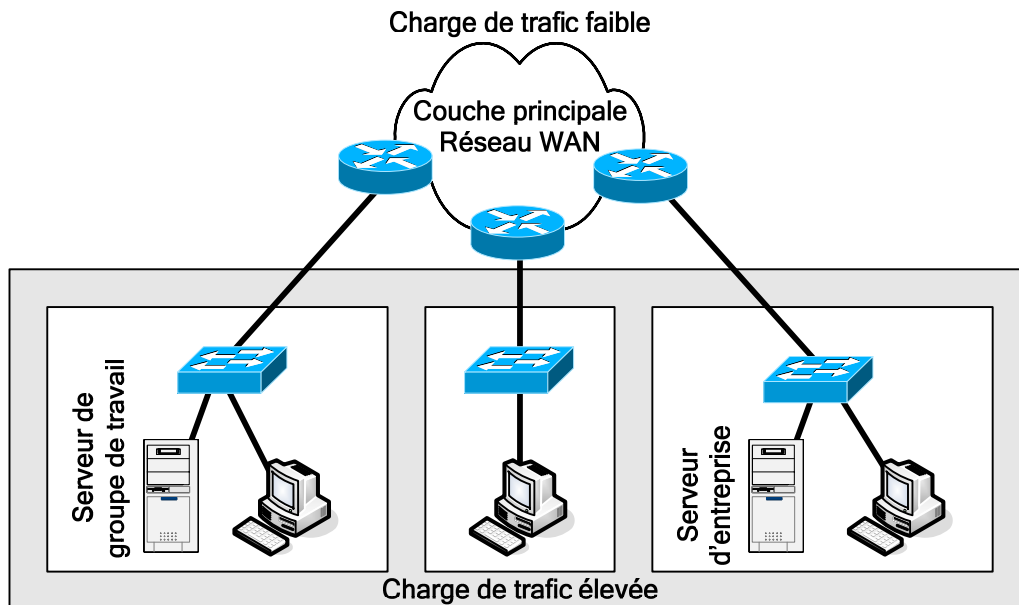
La couche d'accès :

- Partie LAN du réseau.
- Emplacement des hôtes (Utilisateurs).
- Emplacement des serveurs de groupe de travail (Stockage des fichiers, impression).
- Possibilité d'utiliser des ACL afin de déterminer les besoins précis d'un groupe d'utilisateur.
- Partage et/ou commutation de la bande passante, micro segmentation et VLAN.
- Regroupement des utilisateurs selon leur fonction, leurs besoins.
- Isolation du trafic de broadcast destiné à un groupe de travail ou à un LAN.

4.3.2. Modèle à 2 couche

Dans un modèle à 2 couches, les sites distincts sont interconnectés directement par l'intermédiaire de liaisons WAN, représentant la couche principale. Chaque site peut contenir plusieurs LAN.

4.3.3. Modèle à 1 couche



Un réseau à une couche (Modèle linéaire) est mis en œuvre si l'entreprise n'a pas beaucoup d'emplacements éloignés, et si l'accès aux applications se fait principalement à l'intérieur du LAN.

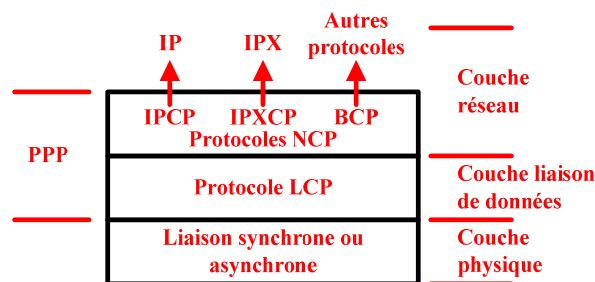
5. Protocole PPP

5.1. Etude du protocole

C'est le protocole de réseau WAN le plus répandu, successeur du protocole SLIP, permettant :

- Connexion entre routeurs ou entre un hôte et un routeur.
- Gestion des circuits synchrones et asynchrones.
- Contrôle de la configuration des liaisons.
- Possibilité d'attribution dynamique des adresses de couche 3.
- Multiplexage des protocoles réseau (Possibilité de faire passer plusieurs paquets de protocoles différents sur la même connexion).
- Configuration des liaisons et vérification de leur qualité.
- Détection des erreurs.
- Négociation d'options (Adresses de couche 3, Compression, etc.).

Le protocole PPP est composé de trois parties distinctes indispensables :



- **Un mode d'encapsulation :** La trame PPP est une trame générique HDLC modifiée.
- **Le protocole LCP (Link Control Protocol) :** Etablissement et contrôle d'une session.
 - Trame LCP d'établissement de liaison.
 - Trame LCP de fermeture de liaison.
 - Trame LCP de maintenance de liaison.
- **Une famille de protocoles NCP (Network Control Protocol) :** Gestion des protocoles de couche 3.
 - **IPCP (Internet Protocol Control Protocol).**
 - **IPXCP (Internetwork Packet eXchange Control Protocol).**
 - **BCP (Bridge Control Protocol).**
 - Une trame PPP est de la forme :

Drapeau (1 octet)	Adresse (1 octet)	Contrôle (1 octet)	Protocole (2 octets)	Données (Taille variable)	FCS (2 ou 4 octets)
----------------------	----------------------	-----------------------	-------------------------	------------------------------	------------------------

- **Drapeau :** Indicateur de début ou fin de trame (Valeur = 01111110).
- **Adresse :** Adresse de broadcast standard (Valeur = 11111111), car PPP n'attribue pas d'adresse d'hôte (Couche 2).
- **Contrôle :** Fourniture d'un service non orienté connexion (semblable au LLC) (Valeur = 00000011).
- **Protocole :** Identification du protocole encapsulé (IP, IPX, etc.).
- **Données :** Contient soit la valeur zéro, soit des données (1500 octets maximum).
- **FCS :** Séquence de contrôle de trame pour une vérification des erreurs.

5.2. Etablissement d'une session

Les quatre phases d'une session PPP, pour l'établissement des communications sur une liaison point-à-point, sont :

- **Établissement de la liaison.**
- **Détermination de la qualité de la liaison.**
- **Configuration du ou des protocoles de couche réseau.**
- **Fermeture de la liaison.**

Ce sont les trames LCP qui se chargent du bon déroulement de ces quatre phases.

Phase 1 - Etablissement de la liaison :

- Le nœud d'origine envoie des trames LCP pour configurer et établir la liaison.
- Négociation des paramètres de configuration grâce au champ d'option des trames LCP (MTU, compression, authentification, etc.). Ces options peuvent donc être explicite (indiquées dans les trames LCP) ou implicites (Utilisation des valeurs par défaut).
- Fin de cette phase par l'émission et la réception d'une trame LCP d'accusé de réception de la configuration.

Phase 2 - Détermination de la qualité de la liaison :

- Cette phase est facultative.
- Vérification de la qualité suffisante pour activer les protocoles de couche 3.
- Une fois la liaison établie, le processus d'authentification est lancé, si nécessaire.

Phase 3 - Configuration du ou des protocoles de couche réseau :

- Émission de paquets NCP pour configurer les protocoles de couche 3 choisis.
- Configuration individuelle des protocoles de couche 3 grâce au protocole NCP approprié.
- Activation et fermeture à tout moment des protocoles de couche 3.
- Les paquets des protocoles de couche 3 sont émis une fois configuré par son NCP correspondant.

Phase 4 - Fermeture de la liaison :

- Fermeture par le biais de trames LCP ou de paquets NCP spécifiques (Si LCP ferme la liaison, il informe les protocoles de couche 3 par l'intermédiaire du NCP correspondant).
- Fermeture à cause d'un événement extérieur (délai d'attente, perte de signaux, etc.).
- Fermeture en cas de demande d'un utilisateur.

On peut vérifier l'état des protocoles LCP et NCP grâce à la commande **show interfaces**.

5.3. Authentification/Configuration

Le protocole PPP peut prendre en charge plusieurs modes d'authentification :

- Aucune authentification.
- Utilisation du protocole PAP.
- Utilisation du protocole CHAP.

Les caractéristiques du protocole PAP sont :

- **Échange en deux étapes** (après la demande d'authentification) :
 - Envoie des informations d'authentification.
 - Acceptation ou refus.
- **Méthode simple d'authentification** : Emission de la combinaison utilisateur/password de façon répétée jusqu'à :

- Confirmation de l'authentification.
 - Interruption de la connexion.
- **PAP n'est pas très efficace :**
 - Mots de passe envoyés en clair.
 - Aucune protection (Lecture répétée des informations, attaques répétées par essais et erreurs).
- Le nœud s'authentifiant contrôle la fréquence et la durée des tentatives d'authentification.

Pour le protocole PAP, on a le choix entre une authentification :

- **Unidirectionnelle :** Seul le client est authentifié sur le serveur de compte.
- **Bidirectionnelle :** Chaque hôte authentifie l'autre.

Celles du protocole CHAP sont :

- **Échange en trois étapes** (après la demande d'authentification) :
 - Confirmation.
 - Réponse.
 - Acceptation ou refus.
- **Méthode d'authentification plus évoluée :**
 - Vérification régulière de l'identité du nœud distant (A l'établissement puis à tout moment).
 - Authentification dans les deux sens.
 - Impossibilité de tenter une authentification sans avoir reçu une demande de confirmation.
 - Authentification cryptée via l'algorithme MD5 lors du transit sur la liaison.
- **Efficacité contre le piratage :**
 - Utilisation d'une valeur de confirmation variable, unique et imprévisible.
 - Répétition des demandes de confirmation visant à limiter la durée d'exposition aux attaques.
 - Chaque côté contrôle la fréquence et la durée des tentatives d'authentification.

Les commandes permettant de configurer tous les différents aspects du protocole PPP sont les suivantes :

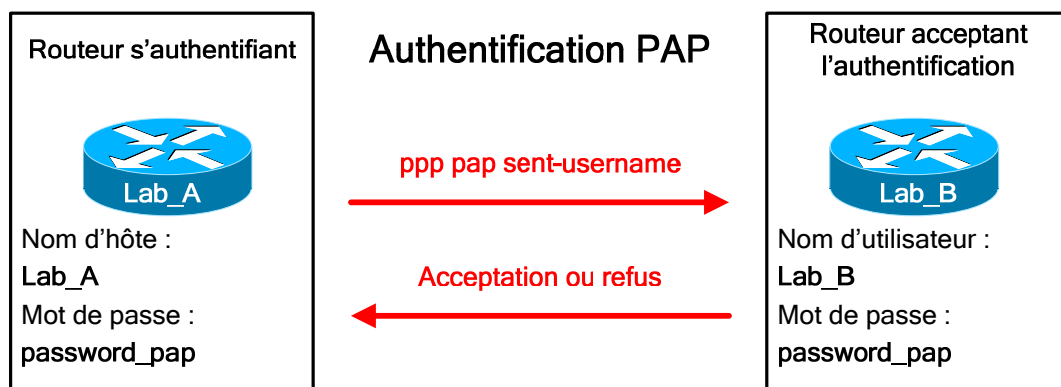
- **username {nom} password {mot_de_passe} :**
 - Mode de configuration globale.
 - Paramètre nom : Nom d'hôte qu'on souhaite accepter.
 - Paramètre mot_de_passe : Mot de passe à utiliser pour l'authentification. Celui-ci doit correspondre au mot de passe du mode privilégié crypté du routeur distant si on utilise CHAP. Ce mot de passe doit être le même sur les deux routeurs.
 - Définir un compte d'utilisateur localement, afin de permettre l'authentification d'un hôte distant.
- **encapsulation PPP :**
 - Mode de configuration d'interface.
 - Spécifier le mode d'encapsulation pour l'interface courante.
- **ppp authentication {chap | chap pap | pap chap | pap} [callin] :**
 - Mode de configuration d'interface.
 - Définir la méthode d'authentification voulue. On a la possibilité de définir deux méthodes différentes. Dans ce cas, la première est utilisée, et en cas de refus ou de suggestion de la deuxième, la deuxième méthode sera utilisée.
 - Le paramètre callin est utilisé pour différencier l'authentification unidirectionnelle de la bidirectionnelle.
- **ppp pap sent-username {nom} password {mot_de_passe} :**
 - Mode de configuration d'interface.
 - Indique les informations qui seront envoyées lors d'une demande d'authentification PAP. Les informations doivent correspondre au compte utilisateur défini sur le routeur distant.
- **ppp chap hostname {nom} :**
 - Mode de configuration d'interface.
 - Permettre l'authentification sur plusieurs routeurs en donnant toujours le même nom d'hôte.
- **ppp chap password {mot_de_passe} :**
 - Mode de configuration d'interface.

- Idem que pour le hostname, mais pour le mot de passe. Ceci permet de limiter le nombre d'entrées utilisateur/password.
- **ppp quality {pourcentage} :**
 - Mode de configuration d'interface.
 - Permet de configurer le LQM (Link Quality Monitor) sur la liaison PPP courante. Si la qualité de la liaison tombe en dessous du pourcentage spécifié, le routeur coupera la liaison.

Pour tout problème concernant l'authentification et la négociation de liaison par rapport au protocole PPP, nous avons à notre disposition les commandes suivantes :

- debug ppp authentication
- debug ppp negotiation

5.3.1. Procédure de configuration du protocole PAP



Nous allons d'abord étudier la configuration qu'il faut utiliser pour une authentification unidirectionnelle.

```
Lab_A (config-if)# encapsulation ppp
Lab_A (config-if)# ppp authentication pap callin
Lab_A (config-if)# ppp pap sent-username Lab_A password password_pap
```

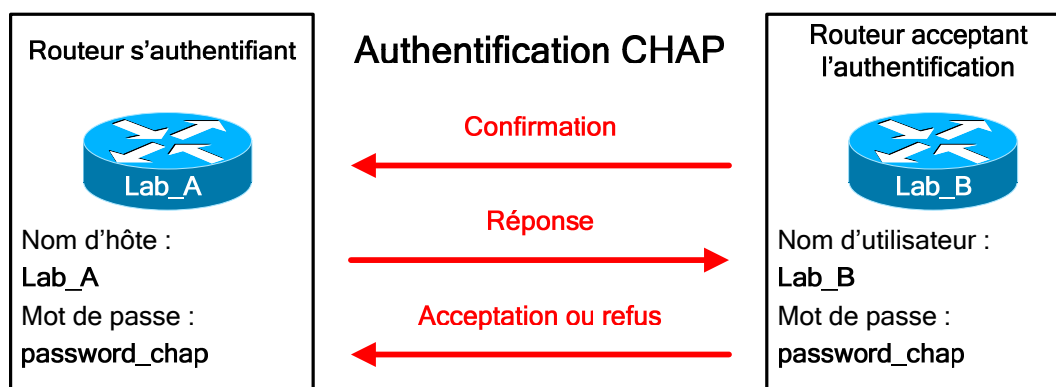
```
Lab_B (config)# username Lab_A password password_pap
Lab_B (config-if)# encapsulation ppp
Lab_B (config-if)# ppp authentication pap
```

Pour une authentification bidirectionnelle, il suffit de procéder comme suit :

```
Lab_A (config)# username Lab_B password password_pap
Lab_A (config-if)# encapsulation ppp
Lab_A (config-if)# ppp authentication pap
Lab_A (config-if)# ppp pap sent-username Lab_A password password_pap
```

```
Lab_B (config)# username Lab_A password password_pap
Lab_B (config-if)# encapsulation ppp
Lab_B (config-if)# ppp authentication pap
Lab_B (config-if)# ppp pap sent-username Lab_B password password_pap
```

5.3.2. Procédure de configuration du protocole CHAP



Le schéma d'authentification ci-dessus représente l'authentification dans un seul sens, il va donc falloir répéter ce schéma dans les deux sens de l'authentification CHAP.

Pour cela, nous allons effectuer les tâches de configuration suivantes sur le routeur Lab_A :

```
Lab_A (config)# username Lab_B password password_chap
Lab_A (config-if)# encapsulation ppp
Lab_A (config-if)# ppp authentication chap
```

Les commandes à utiliser sur le routeur Lab_B sont :

```
Lab_B (config)# username Lab_A password password_chap
Lab_B (config-if)# encapsulation ppp
Lab_B (config-if)# ppp authentication chap
```

6. Technologies RNIS

6.1. Technologie

Il existe deux types de services RNIS :

- **BRI** : Accès de base.
 - Aussi appelé canal 2B+D.
 - 2 canaux B à 64 Kbits/s (8 bits).
 - 1 canal D à 16 Kbits/s (2 bits).
 - Débit binaire de 192 Kbits/s (8000 trames de 24 bits).
 - Débit réel de 144 Kbits/s (2 canaux B + 1 canal D).
- **PRI** : Accès primaire (fonctionnant sur des lignes dédiées).
 - **T1** (Débit de 1.544 Mbits/s) :
 - 23 canaux B à 64 Kbits/s (8 bits).
 - 1 canal D à 64 Kbits/s (8 bits).
 - 1 bit de verrouillage de trame.
 - 8000 trames par seconde.
 - **E1** (Débit de 2.048 Mbits/s) :
 - 30 canaux B à 64 Kbits/s (8 bits).
 - 1 canal D à 64 Kbits/s (8 bits).
 - 1 canal à 8 bits pour le verrouillage de trame.

La vitesse de transmission est toujours de 8000 trames par seconde et par canal.

Ces deux services utilisent plusieurs canaux, qui sont répartis en deux types :

- **Canal B (Bearer) :**
 - Acheminement du trafic de voix et de données.
 - Le RNIS offre une grande souplesse d'utilisation, car il est possible d'utiliser chaque canal B séparément, pour transmettre à la fois la voix (Téléphone) et les données (Informatique).
 - Le protocole PPP multi liaison s'occupe du regroupement de la bande passante lorsque plusieurs canaux B sont utilisés pour le trafic de données.
 - Utilisation éventuelle d'un SPID par canal B. Cet identificateur permet de déterminer la configuration de ligne, et ressemble à un numéro de téléphone. Le commutateur peut ainsi relier les services demandés à la connexion.
- **Canal D (Delta) :**
 - Canal de signalisation des instructions de traitement des données des canaux B.
 - Le protocole de signalisation de ce canal s'exécute au niveau des couches 1 à 3 du modèle OSI.

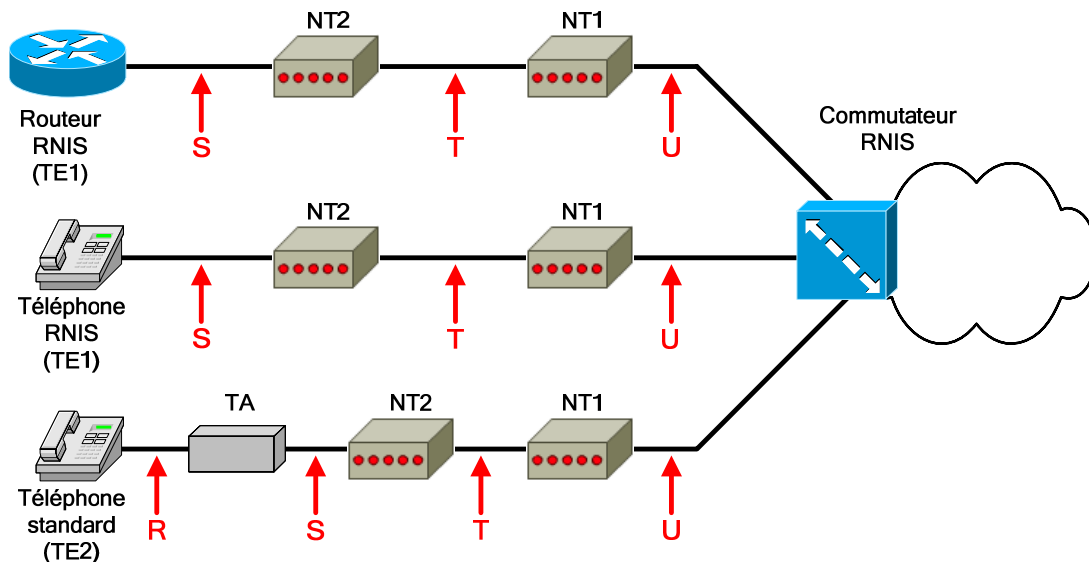
Le protocole LAPD (Couche 2) est utilisé sur le canal D et permet une circulation et une réception adéquate des flux d'information de contrôle et de signalisation. Ce protocole est similaire à HDLC et à LAPB (X.25).

Il est possible de connecter plusieurs unités utilisateur sur un même circuit RNIS. Dans ce cas, des collisions peuvent apparaître. Le canal D prend en charge des fonctions permettant de déterminer des conflits sur la liaison. Il a été mis en place un principe simple afin de permettre à chaque terminal de transmettre :

- Un terminal ne peut transmettre sur le canal D que lorsqu'il détecte un nombre précis de 1 (indiquant l'absence de signal), ce qui correspond à un niveau de priorité prédéterminé.
- Si le terminal détecte un bit E (Voir normes RNIS) qui est différent de ses bits du canal D, il doit cesser immédiatement la transmission.

- Dès que le message du canal D a été transmis, le niveau de priorité du terminal est réduit.
- Un terminal ne peut passer à un niveau de priorité supérieur que si tous les autres terminaux sur la même ligne n'ont pas eu la possibilité d'émettre un message de canal D.
- La connexion téléphonique est prioritaire aux autres services (Données, etc.).
- L'information de signalisation est prioritaire aux autres types d'informations.

6.2. Termes et équipements



Les différents équipements que l'on peut trouver sur un réseau RNIS sont :

Commutateur RNIS : Dispositif de couche 2 permettant la commutation entre les différentes liaisons RNIS.

- **NT1 (Terminaison réseau 1) :**
 - Unité reliant le câblage à quatre fils de l'utilisateur à la boucle locale à deux fils classique.
- **NT2 (Terminaison réseau 2) :**
 - Unité dirigeant le trafic des différentes unités terminales (TE1 et TE2) vers le NT1.
 - Assure les fonctions de commutation et de concentration (Permet de connecter plusieurs TE sur un NT1).
 - Généralement présent dans les autocommutateurs numériques (PABX).
- **TA (Adaptateur de terminal) :**
 - Unité convertissant des signaux standard (provenant d'un TE2) au format RNIS.
 - Raccordée en amont sur une unité NT 1 ou 2.
- **TE1 (Equipement terminal 1) :**
 - Unité compatible RNIS.
 - Raccordée sur une unité NT 1 ou 2.
 - Reliée au réseau au moyen d'une liaison numérique à paires torsadées de quatre fils.
- **TE2 (Equipement terminal 2) :**
 - Unité non compatible RNIS.
 - Raccordée sur une unité TA.

Les points de référence RNIS sont regroupés sous quatre désignations :

- **R** : Interface entre une unité TE2 et un TA.
- **S** : Interface entre un NT2 et un TE1 ou TA. C'est la partie qui active les appels entre les différentes parties du CPE.
- **T** : Idem électriquement que S mais correspond à la connexion entre un NT2 et un NT1 ou le réseau RNIS.
- **S/T** : Interface entre un TE1 ou un TA et directement un NT1 (car le NT2 est optionnel).
- **U** : Interface entre un NT1 et le réseau RNIS (uniquement aux USA, car NT1 n'est pas pris en charge par l'opérateur).

6.3. Normes

La technologie RNIS a été mise au point en vue d'uniformiser les services proposés par les opérateurs aux abonnés. Cette uniformisation comprend l'**interface UNI** (Correspond aux informations génériques de base ainsi qu'à des fonctions réseau). En plus de cette interface UNI, une pile complète de protocoles (Couches 1 à 3) a été définie.

Les différents protocoles définis pour le RNIS sont classés dans trois catégories :

- **E** : Normes de réseau téléphonique RNIS.
 - E.164 : Adressage international RNIS.
- **I** : Concepts, terminologie et méthodes générales.
 - Série I.100 : Concepts généraux.
 - Série I.200 : Aspects des services RNIS.
 - Série I.300 : Aspects réseau.
 - Série I.400 : Comment est fournie l'interface UNI.
- **Q** : Fonctionnement de la commutation et de la signalisation.
 - Q.921 : Décrit les processus du protocole LAPD (Canal D).
 - Q.931 : Précise les fonctions de couche 3 (entre le point d'extrémité et le commutateur RNIS).

La norme Q.931 n'impose pas de recommandation de bout en bout. Cette norme a donc pu être mise en œuvre de diverses façons en fonction du fournisseur et du type de commutateur. Ce point est à préciser lors de la configuration.

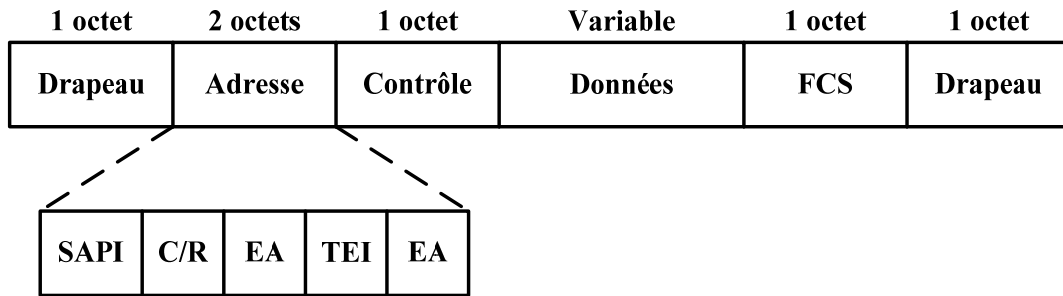
Les différentes normes que nous étudierons en fonction des couches du modèle OSI sont :

- **Couche physique** :
 - I.430 : Spécification de couche physique du BRI.
 - I.431 : Spécification de couche physique du PRI.
- **Couche liaison de données** :
 - Q.920 à Q.923 : Spécification fondée sur LAPD.
- **Couche réseau** :
 - Q.930 (I.450) et Q.931 (I.451) : Définition des connexions entre utilisateurs, à commutation de circuits ou de paquets. La signalisation d'établissement, maintien et fermeture des connexions réseau RNIS est le principal objectif de ces deux normes. Elles s'occupent aussi de fournir une variété de messages (Configuration, connexion, libération, information sur les utilisateurs, annulation, état et déconnexion).

Il existe deux formats de trames pour le RNIS :

- **Trame TE** : Trame sortante (Terminal au réseau).
- **Trame NT** : Trame entrante (Réseau au terminal).

Elles ont une taille de 48 bits, dont 36 de données. Il s'agit en réalité de deux trames successives de 24 bits (deux canaux B à 8 bits + un canal D à 2 bits + 6 bits de verrouillage de trame) :

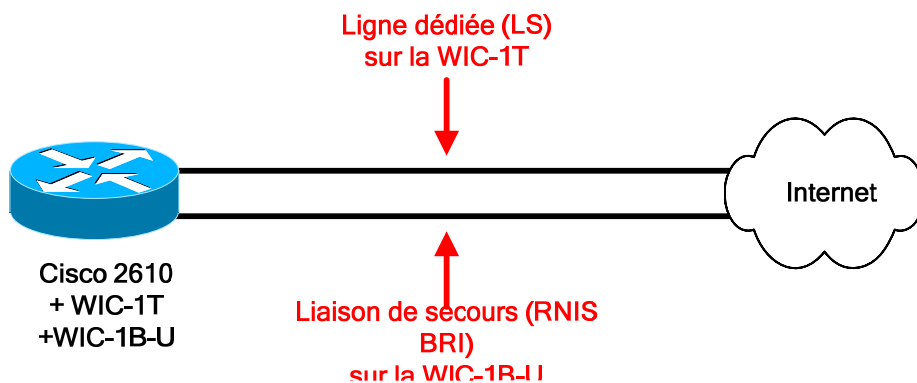


- **Drapeau** : Similaire au champ HDLC.
- **Adresse** : Peut comporter 1 ou 2 octets (Dépend de la valeur des bits EA).
 - **SAPI** : Bits d'identification du point d'accès (6 bits). Indique le portail où les services LAPD sont fournis à la couche 3.
 - **C/R** : Bit de commande/réponse.
 - **EA** : Bit d'adressage étendu. Si le premier EA est défini, alors l'adresse comporte 1 octet, sinon elle en comporte 2.
 - **TEI** : Identificateur de point d'extrémité de terminal. Ce champ précise le nombre de terminaux, ou s'il s'agit d'un broadcast.
- **Contrôle** : Similaire au champ HDLC.
- **Données** : Données fournies par l'intermédiaire des canaux B.
- **FCS** : Séquence de contrôle de trame (Contrôle d'erreurs).

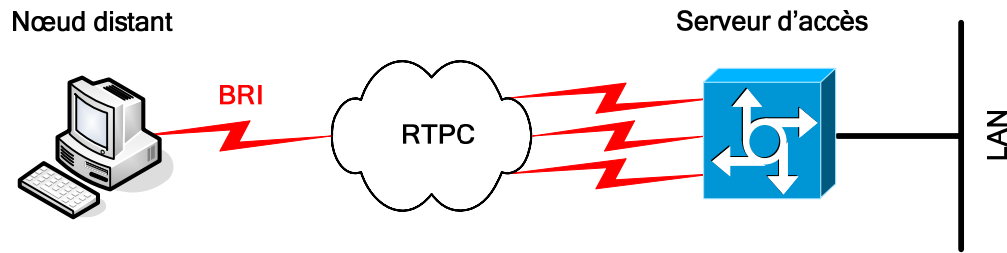
6.4. Utilisation/Implémentation

La technologie RNIS a de nombreuses applications :

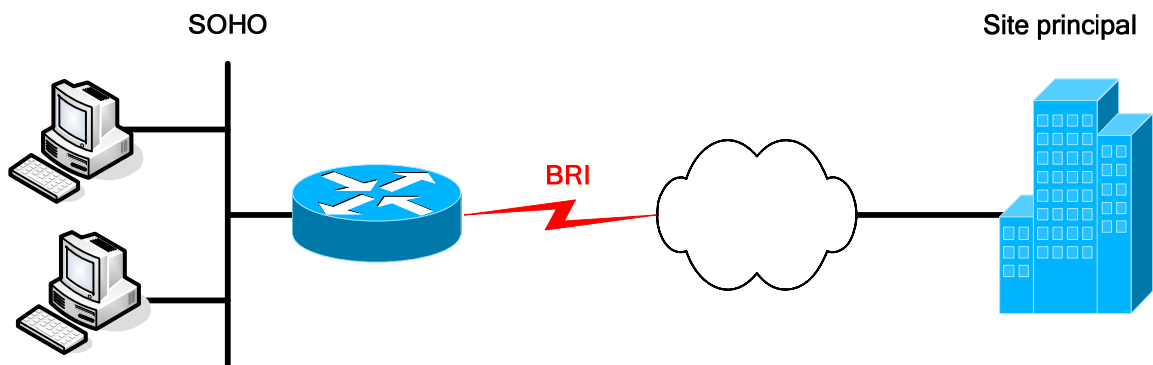
- Solution alternative aux lignes dédiées.
- Accès à distance :
 - Nœuds distants.
 - Connectivité des petits bureaux et bureaux à domicile (SOHO – Small Office / Home Office).



L'utilisation du RNIS en tant qu'alternative aux lignes dédiées permet d'avoir une continuité de service en cas de défaillance de la liaison principale. L'utilisation de la liaison de secours se fait automatiquement, car la route ayant une meilleure métrique passant par la liaison principale sera désactivée, laissant ainsi comme seul choix le passage par la liaison de secours.



L'accès à distance pour un nœud isolé (Employés itinérants, etc.) permet une connectivité éphémère. L'environnement présenté à l'utilisateur est identique à celui qu'il verrait s'il était en local (Utilisation du VPN). La seule différence pour le nœud distant est que la liaison est relativement lente comparée à celle d'un LAN, et passe par l'intermédiaire d'un serveur d'accès, qui fournit les services LAN.



L'accès à distance pour une SOHO (Succursale de l'entreprise, etc.) permet à un petit groupe d'utilisateurs d'avoir un accès aux ressources du site principal. C'est le routeur de la SOHO qui s'occupe de la translation d'adresse, afin de fournir des services à plusieurs travailleurs en utilisant une seule connexion WAN (Une seule IP).

6.5. Routage à établissement de la connexion à la demande (DDR)

Le principe du DDR est d'ouvrir ou de fermer dynamiquement une session de communication, et ce sur une liaison WAN de type commutation de circuits (Exemples : POTS, RNIS).

La notion de trafic intéressant pour le DDR est un trafic, ou ensemble de paquets, que le routeur doit acheminer par le biais de la liaison WAN. Ceci peut être basé :

- Sur les adresses de couche 3.
- Sur les services réseaux spécifiques, en se basant sur les numéros de port des protocoles de couche 4.

Principe de fonctionnement du DDR :

- Lorsque le routeur reçoit un trafic intéressant, il va ouvrir une session, afin de transmettre ce trafic.
- Cette session sera fermée après expiration du délai du compteur d'inactivité.
- Ce compteur d'inactivité est réinitialisé uniquement si un trafic intéressant est reçu.

Les avantages du DDR sont nombreux :

- Plus économique que des liaisons spécialisées ou multipoints, lorsque le trafic devant être émis ne nécessite pas un circuit continu.
- Partage de charges, lorsque l'on a par exemple plusieurs liaisons séries, ce qui permet d'utiliser le nombre de liaison nécessaire uniquement. Dans ce cas, il faudrait configurer le DDR afin d'ouvrir la session uniquement lorsque la liaison précédente est surchargée.
- Liaison de secours pour une liaison spécialisée. Le DDR permet d'offrir un moyen de communication de secours en cas de défaillance de la liaison principale (liaison spécialisée).

Le trafic empruntant une liaison utilisant le DDR est moins important et plus intermittent que le trafic passant au travers d'un réseau LAN ou par une liaison spécialisée.

Les étapes de la configuration du DDR sur un routeur sont les suivantes :

- **Utilisation des ACL** : Permet de préciser les adresses de couche 3 (source et destination), ainsi que les protocoles de couche 4 et numéro de port associés. Cela définit ce que nous voulons considérer comme trafic intéressant.
- **Définition des interfaces utilisant le DDR** : Indique le groupe de numérotations qui associe l'interface WAN voulue avec les ACL pour le DDR..

6.6. Commandes

Les commandes qu'il est nécessaire de connaître en vue de pouvoir configurer un routeur branché sur une liaison RNIS sont :

- **interface bri {numéro} :**
 - Mode de configuration globale.
 - Permet de passer dans le mode de configuration d'une interface BRI.
- **interface dialer {numéro} :**
 - Mode de configuration globale.
 - Permet de passer dans le mode de configuration d'une interface de connexion à la demande.
- **isdn switch-type {isdn_swith_type} :**
 - Mode de configuration globale.
 - Permet de spécifier le type de commutateur RNIS sur lequel on est raccordé.
 - Le paramètre `isdn_switch_type` peut prendre les valeurs `basic-1tr6` (Allemagne), `basic-5ess` (USA), `basic-dms100` (Angleterre), `basic-net3` (Angleterre et Europe), `basic-ni`, `basic-qsig`, `basic-ts013` (Australie), `ntt` (Japon), `vn3` (France).
- **isdn spid1 {valeur_spid_1} :**
 - Mode de configuration d'interface BRI.
 - Configure le SPID pour le canal B1.
- **isdn spid2 {valeur_spid_2} :**
 - Mode de configuration d'interface BRI.
 - Configure le SPID pour le canal B2.
- **dialer-list {numéro_groupe} protocol {proto} {permit | deny | list {numéro_acl}} :**
 - Mode de configuration globale.
 - Cette commande permet de définir le trafic intéressant pour le DDR.
 - Le paramètre **numéro_groupe** indique le groupe pour lequel on attribut le trafic intéressant.
 - **proto** permet de spécifier le protocole de couche 3 dont fera partie le trafic intéressant.
 - Le dernier paramètre permet de rendre intéressant tout le protocole spécifié (**permit**), tout sauf le protocole spécifié (**deny**), ou bien de limiter le trafic intéressant à tout ce qui correspond à l'ACL indiquée (**list**).
- **dialer-group {numéro_groupe} :**
 - Mode de configuration d'interface BRI ou Dialer.
 - Permet d'affecter un trafic intéressant spécifique (**dialer-list correspondant**) sur l'interface actuelle.
- **dialer pool {numéro} :**
 - Mode de configuration d'interface Dialer.
 - Permet le regroupement d'interfaces Dialer sur une interface BRI spécifique (**dialer pool-member**).
- **dialer pool-member {numéro} :**
 - Mode de configuration d'interface BRI.

- Permet de spécifier l'interface BRI qui sera la source des interfaces Dialer (**dialer pool**).
- **dialer string {numéro} :**
 - Mode de configuration d'interface Dialer.
 - Permet de configurer le numéro de téléphone de la destination à appeler.
- **dialer wait-for-carrier-time {temps} :**
 - Mode de configuration d'interface BRI ou Dialer.
 - Configuration du temps pendant lequel le routeur attendra le signal de porteuse.
- **dialer idle-timeout {temps} :**
 - Mode de configuration d'interface BRI ou Dialer.
 - Configuration du temps de déconnexion après inactivité.
- **dialer remote-name {nom_distant} :**
 - Mode de configuration d'interface Dialer.
 - Permet de spécifier le nom d'hôte du nœud distant.
- **dialer in-band :**
 - Mode de configuration d'interface BRI ou Dialer.
 - Indique que l'on va faire passer le flux de signalisation dans le canal de données
- **dialer map {protocole} {adresse} name {nom} {numéro} :**
 - Mode de configuration d'interface BRI ou Dialer.
 - Précise le numéro de téléphone à appeler pour atteindre l'adresse de destination indiquée.
 - Ne pas utiliser cette commande avec la commande **dialer string** en même temps.
- **dialer load-threshold {charge} [inbound | outbound | either] :**
 - Mode de configuration d'interface.
 - Spécifie à quel pourcentage de charge de la liaison un nouveau canal B sera utilisé (Uniquement avec PPP), que ce soit en entrée (**inbound**), sortie (**outbound**) ou les deux (**either**).
 - Charge doit être un nombre entre 1 et 255 (255 = 100 %).
- **PPP multilink :**
 - Mode de configuration d'interface.
 - Indique que le protocole PPP sur l'interface courante pourra prendre en charge la gestion de liaisons multiples.

Afin de permettre une résolution des problèmes éventuels ainsi qu'une surveillance de l'état des protocoles et des connexions, IOS fournit différentes commandes :

- **show interfaces bri {numéro}:{bearer} :** Permet de visualiser l'état d'un canal B particulier de l'interface BRI voulue.
- **show isdn status :** Etat de la liaison RNIS. Cette commande indique le type de commutateur RNIS configuré, les statuts au niveau des couches 1 et 2, ainsi que le nombre de connexions actives sur la liaison.
- **show isdn active :** Affichage des connexions actives.
- **show dialer :** Affichage des paramètres et des statistiques concernant l'interface DDR (Dialer).
- **debug isdn events :** Permet d'obtenir des informations sur les événements RNIS.
- **debug isdn q921 :** Permet la vérification d'une connexion au commutateur RNIS (Problèmes liés aux SPID).
- **debug isdn q931 :** Permet d'identifier les problèmes entre le routeur et le commutateur (Problème lié à une mauvaise configuration du type de commutateur RNIS).
- **debug dialer [events | packets] :** Permet une visualisation sur l'état du DDR.

6.7. Configuration

On peut choisir entre plusieurs types d'encapsulation lors de la configuration d'une liaison RNIS :

- HDLC (Par défaut).
- PPP (Généralement utilisé).

Les tâches à accomplir sont :

- Détermination du type de commutateur RNIS sur lequel on est relié.
- Choix de l'encapsulation pour notre liaison (HDLC, ou PPP avec ou sans authentification).
- Définir les SPID pour les canaux B (Si nécessaire).
- Configurer une ou plusieurs interfaces Dialer, en fonction des besoins :
 - Indiquer le numéro à appeler.
 - Indiquer le rattachement de l'interface Dialer courante à une interface BRI.
 - Préciser le type de trafic qui devra être transmis (DDR).
 - Créer une route statique pour diriger le trafic sur la bonne interface.

7. Technologies Frame Relay

7.1. Technologie

La technologie Frame Relay dispose des caractéristiques suivantes :

- Destinée pour des équipements numériques haut de gamme et à haut débit.
- Fonctionne au niveau des couches 1 et 2 du modèle OSI.
- Utilise des circuits virtuels dans un environnement commuté.
- Technologie à commutation de paquets, et à accès multiples.
- L'ETTD et l'ETCD sont respectivement généralement le routeur client et le commutateur de l'opérateur.
- Remplace des réseaux point-à-point, trop coûteux.
- Se base sur l'encapsulation HDLC.
- Utilise le multiplexage pour partager la bande passante totale du nuage Frame Relay.

Cette technologie comporte quelques inconvénients, dont :

- Capacité de vérification des erreurs et fiabilité minimale (laissées aux protocoles de couches supérieures).
- Affecte le fonctionnement de certains aspects (Split Horizon, broadcasts, etc.).
- Ne diffuse pas les broadcasts. Pour en effectuer, il faut envoyer un paquet à chaque destination du réseau.

Un réseau Frame Relay peut être conçu suivant deux topologies :

- **Maillage global** : Chaque extrémité est reliée par l'intermédiaire d'un PVC distinct vers chaque autre destination.
- **Maillage partiel** : Egalement appelé topologie en étoile ou "hub-and-spokes". Chaque extrémité n'est pas reliée à toutes les autres.

Définitions :

- **Tarif d'accès** : Vitesse d'horloge de la connexion.
- **DLCI (Identificateur de connexion de liaison de données)** : C'est un numéro désignant un point d'extrémité. Le commutateur Frame Relay mappe deux DLCI (Source et destination) afin de créer un PVC. Il a une portée locale.
- **PVC (Circuit virtuel permanent)** : Circuit virtuel agissant comme une liaison point-à-point dédiée pour relier deux extrémités dans un environnement commuté.
- **LMI (Interface de supervision locale)** : Norme de signalisation entre le point d'extrémité et le commutateur Frame Relay chargé de la gestion et maintenance de l'état entre les unités.
- **CIR (Débit de données garanti)** : Débit de données que le fournisseur s'engage à fournir.
- **Bc (Débit garanti en rafale)** : Nombre maximum de bits que le commutateur accepte de transférer sur une période donnée.
- **Be (Débit garanti en excès)** : Nombre maximum de bits non garantis que le commutateur tentera de transférer au-delà du CIR. Il est généralement limité par la vitesse du port de la boucle locale. Les trames émises en excès ont leur bit d'éligibilité à la suppression mis à 1.
- **FECN (Notification explicite de congestion au destinataire)** : Bit défini dans une trame qui signale à l'unité réceptrice de lancer des procédures de prévention de congestion.
- **BECN (Notification explicite de congestion à la source)** : Idem mais pour l'unité source. Un routeur recevant cette notification réduira le débit de transmission de 25%.
- **Bit d'éligibilité à la suppression** : Bit qui indique que la trame peut être supprimée en priorité en cas de congestion.

Le format des trames Frame Relay est le suivant :

1 octet	2 octets	Variable	2 octets	1 octet
Drapeau	Adresse	Données	FCS	Drapeau

- **Drapeau** : Indique le début et la fin de la trame.
- **Adresse** : Contient l'adresse d'extrémité (10 premiers bits), ainsi que les mécanismes de notification de congestion (3 derniers bits).
 - DLCI.
 - FECN.
 - BECN.
 - Bit d'éligibilité à la suppression.
- **Données** : Informations encapsulées de couche supérieure.
- **FCS** : Séquence de contrôle de trame.

7.2. Interface LMI & DLCI

La mise en œuvre et le fonctionnement de la technologie Frame Relay repose essentiellement sur les interfaces LMI, dont les fonctions de base sont :

- Déterminer la fonctionnalité des PVC connus du routeur.
- Transmettre des messages de veille, pour éviter que le PVC ne se ferme pour cause d'inactivité.
- Indiquer au routeur les PVC disponibles.

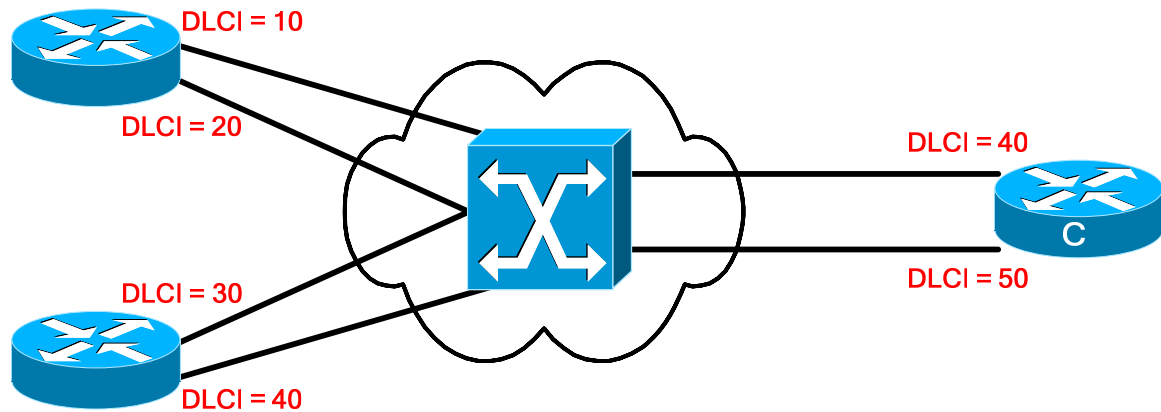
Il existe des extensions LMI, qui sont optionnelles :

- **Messages d'état des circuits virtuels (Extension universelle)** : Signalisation périodique sur les PVC (Nouveaux, supprimés, leur intégrité, etc.).
- **Diffusion multicast (Extension facultative)** : Permet la diffusion des messages de protocole de routage et ARP, qui doivent être normalement transmis à plusieurs destinataires. Cela utilise les DLCI 1019 à 1022.
- **Adressage global (Extension facultative)** : Portée globale des DLCI au lieu d'être locale. Permet d'avoir un DLCI unique sur le réseau Frame Relay.
- **Contrôle de flux simple (Extension facultative)** : Contrôle de flux de type XON/XOFF, destiné aux unités dont les couches supérieures ne peuvent pas utiliser les bits de notification de congestion, mais nécessitant un niveau de contrôle de flux.

1 octet	2 octets	1 octet	1 octet	1 octet	1 octet	Variable	2 octets	1 octet
Drapeau	DLCI LMI	Indicateur d'informations non numéroté	Indicateur de protocole	Référence d'appel	Type de message	Éléments d'information	FCS	Drapeau

Le schéma ci-dessus représente une trame Frame Relay spécifique aux messages LMI.

- **DLCI LMI** : DLCI pour les messages LMI. Il est fixé à 1023.
- **Indicateur de protocole** : Défini sur une valeur précisant l'interface LMI.
- **Type de message** : Deux types ont été définis, qui permettent de vérifier l'intégrité des liaisons logiques et physiques.
 - **Message d'état** : Emis en réponse à un message de demande d'état. Message de veille ou message d'état sur chaque DLCI défini pour la liaison.
 - **Message de demande d'état**.
- **Éléments d'information (IE)** : Contient un ou plusieurs éléments d'information d'1 octet chacun, et un ou plusieurs octets de données.



Les identificateurs DLCI sont reconnus localement, ce qui implique qu'ils ne sont pas forcément uniques dans le nuage Frame Relay (Exception faite si on utilise l'extension LMI d'adressage global). Deux unités ETDD peuvent utiliser une valeur DLCI identique ou différente pour désigner le PVC les reliant.

L'espace d'adressage DLCI est limité à 10 bits. Une partie de la plage d'adresse (0 à 1023) est utilisable pour les adresses d'extrémité (Transport des données utilisateur), et le reste est réservé à des fins d'implémentation par le constructeur (Messages LMI, adresses de multicast, etc.).

La portion exploitable de la plage d'adresse DLCI est définie par le type LMI utilisé :

- **ansi** : La plage de DLCI hôte va de 16 à 992.
- **cisco** : Les DLCI hôte vont de 16 à 1007.
- **q933a** : Même plage DLCI que la version **ansi**.

7.3. Fonctionnement, table de commutation et processus de transmission

La norme Frame Relay de base ne supporte que des PVC reconnus localement. Il n'y a pas d'adresses pour désigner les nœuds distants. Il est donc impossible d'utiliser un processus classique de résolution d'adresses. Pour palier à ce problème, il y a deux possibilités :

- Créer manuellement des cartes statiques avec la commande **frame-relay map**.
- Opter pour l'extension LMI sur l'adressage global. Ainsi, chaque nœud aura un DLCI unique.

La carte Frame Relay comporte trois champs :

- DLCI local par lequel passer pour atteindre la destination.
- L'adresse de couche 3 du nœud distant correspondant.
- L'état de la connexion :
 - **Active state** : Connexion active. Les routeurs peuvent échanger des données.
 - **Inactive state** : La connexion locale au commutateur est en service, mais la connexion du routeur distant au commutateur ne l'est pas.
 - **Deleted state** : Soit aucun LMI n'est reçu du commutateur, soit aucun service n'est assuré entre le routeur local et le commutateur.

Il existe un mécanisme de résolution d'adresse inverse (Inverse-ARP), qui permet à un routeur d'élaborer automatiquement la carte Frame Relay :

- Le routeur prend connaissance des DLCI au moment de l'échange LMI initiale avec le commutateur.
- Il envoie alors une requête Inverse-ARP à chaque DLCI pour chaque protocole de couche 3 configurés localement.

- Les informations renvoyées sont utilisées pour remplir la carte Frame Relay.

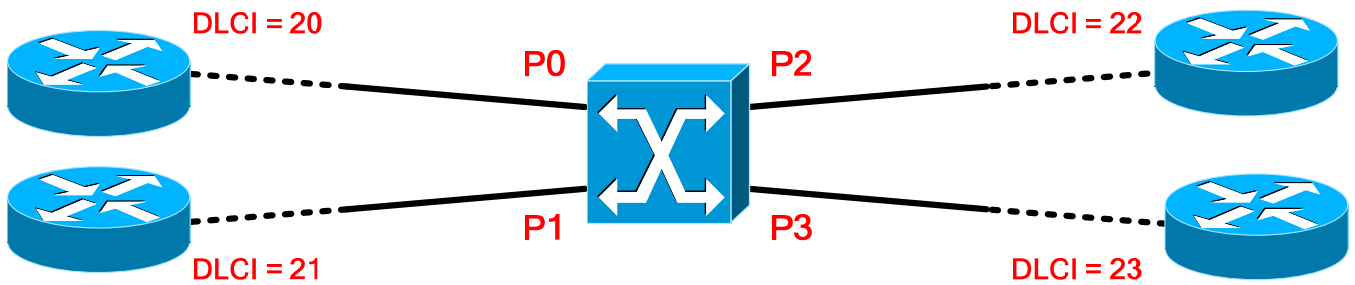


Table de commutation du port P0

IN_Port	IN_DLCI	OUT_Port	OUT_DLCI
P0	20	P1	21
		P2	22
		P3	23

La table de commutation Frame Relay dispose de quatre colonnes :

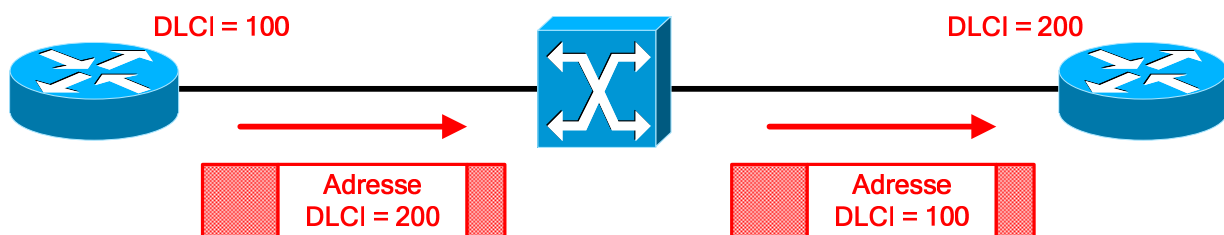
- Port d'entrée.
- DLCI d'entrée.
- Port de sortie.
- DLCI de sortie.

Cette table de commutation est basée sur un port du commutateur, il y a donc autant de tables qu'il y a de ports fonctionnels. De plus, elle est administrée, ce qui signifie que c'est l'opérateur qui décide du contenu de chaque table. Elle sert :

- Au moment du premier échange LMI, afin d'informer le routeur des DLCI des nœuds distants qui lui sont accessibles.
- Durant la transmission des données, où elle fonctionne comme une table de commutateur LAN.

Le processus de découverte est le suivant :

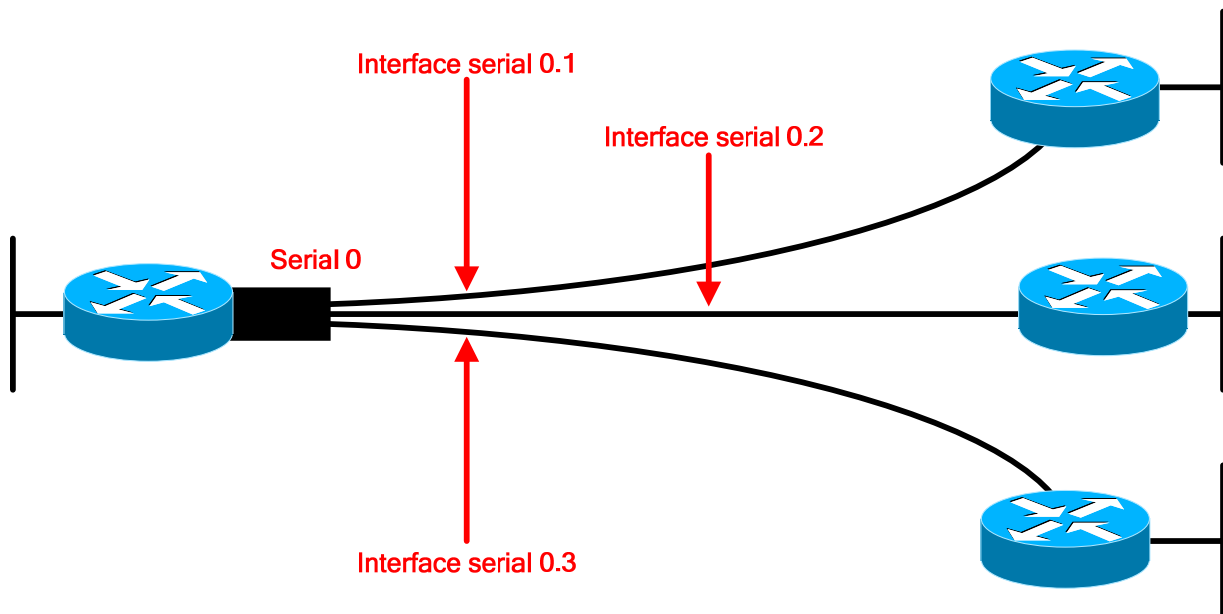
- Émission d'un message de demande d'état au commutateur Frame Relay (donne l'état du routeur local et demande celui des connexions des routeurs distants).
- Le commutateur répond avec un message d'état, contenant les DLCI des routeurs distants qui sont accessibles au routeur local.
- Pour chaque DLCI actif, le routeur envoie un paquet Inverse-ARP afin de se présenter et de demander aux routeurs distants de s'identifier (Adresse de couche 3).
- Le routeur mappe dans sa carte chaque adresse de nœud distant qu'il reçoit par le biais d'un message de résolution d'adresse inverse.
- Les messages de résolution d'adresse inverse sont ensuite échangés toutes les 60 secondes.
- Les messages de vieille sont envoyés toutes les 10 secondes au commutateur.



Le processus de transmission de données au travers d'un réseau Frame Relay est :

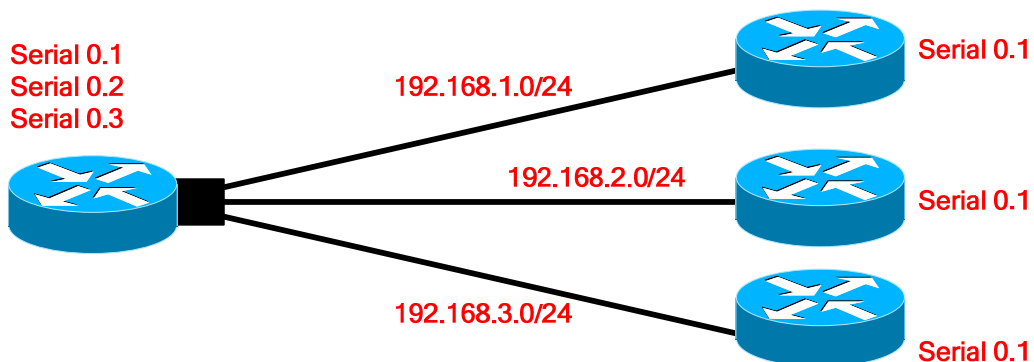
- Le routeur source encapsule les données à transmettre dans une trame Frame Relay, dont la valeur du champ Adresse correspond au DLCI du destinataire, puis l'envoie.
- Le commutateur reçoit cette trame, et utilise la table de commutation du port d'entrée afin de déterminer le port de sortie, et donc le DLCI de sortie.
- Le commutateur modifie la trame en plaçant le DLCI de la source, afin que la destination puisse savoir quelle est cette source.
- Le routeur de destination reçoit la trame émise par le commutateur. Il répondra, si besoin est, en émettant une trame vers le DLCI indiqué dans la trame reçue.

7.4. Les sous interfaces Frame Relay



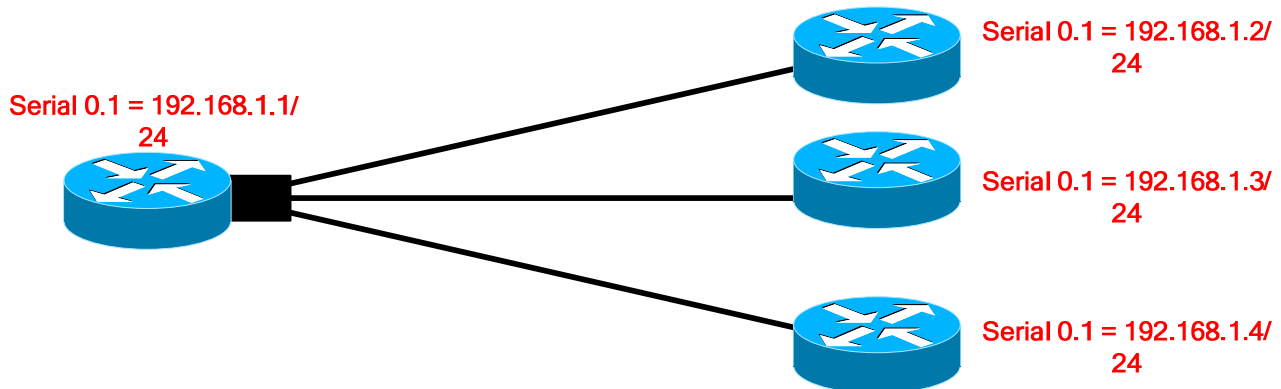
Les sous-interfaces sont des subdivisions logiques d'une interface physique et peuvent être de deux types :

- Point-à-point.
- Multipoint.



Les caractéristiques des sous-interfaces point-à-point sont :

- Une sous-interface par PVC.
- Une attribution statique de DLCI par sous-interface.
- Chaque connexion point-à-point est son propre sous-réseau.
- Chaque interface possède un seul DLCI.
- Split horizon ne fonctionne pas comme on voudrait qu'il fonctionne dans le principe, car il ne connaît pas le principe de sous-interface, ce qui veut dire que les mises à jour de routage ne seront pas propagées vers les autres sous-interfaces.



Les caractéristiques des sous-interfaces multipoints sont :

- Une seule sous-interface pour établir plusieurs PVC.
- Autant d'attributions statiques de DLCI qu'il y a de PVC (Destinataires).
- Toutes les interfaces font partie du même sous-réseau.
- Chaque interface possède son DLCI local.
- Split horizon fonctionne avec ce type de sous-interface.

7.5. Commandes

Les commandes concernant Frame Relay sont les suivantes :

- **interface serial {numéro} :**
 - Mode de configuration globale.
 - Permet de passer dans le mode de configuration de l'interface souhaitée.
- **interface serial {numéro.sous-numéro} {multipoint | point-to-point} :**
 - Mode de configuration globale.
 - Permet de passer dans le mode de configuration de la sous-interface souhaitée.
 - Le paramètre multipoint ou point-to-point définit le type de sous-interface utilisée.
 - Il faut utiliser multipoint si on veut que le routeur envoie les broadcast et les mises à jour de routage qu'il reçoit.
- **encapsulation frame-relay [ietf] :**
 - Mode de configuration d'interface.
 - Précise l'encapsulation des trames pour l'interface courante.
 - Le paramètre cisco est la valeur par défaut, et est à utiliser si on est raccordée à un autre équipement Cisco.
 - Le paramètre ietf est utile pour se connecter à un dispositif non Cisco.
- **frame-relay interface-dlci {dlci} :**
 - Mode de configuration de sous-interface.
 - Affecte un DLCI pour la sous-interface courante.

- **frame-relay local-dlci {dlci} :**
 - Mode de configuration d'interface.
 - Permet d'affecter manuellement le DLCI pour l'interface courante (normalement attribué automatiquement par le LMI).
 - Il faut utiliser cette commande dans les environnements ne supportant pas les interfaces LMI.
- **frame-relay lmi-type {ansi | cisco | q933a} :**
 - Mode de configuration d'interface.
 - La valeur cisco est par défaut.
 - Cette commande est à utiliser uniquement pour une version d'IOS ancienne car, avec les versions 11.2 et ultérieure, le type de LMI est détecté automatiquement.
- **bandwidth {bp} :**
 - Mode de configuration d'interface.
 - Permet de spécifier la bande passante de la liaison sur un ETTD, à titre d'information (Pour un protocole de routage).
- **frame-relay inverse-arp {protocole} {dlci} :**
 - Mode de configuration d'interface.
 - Active la résolution d'adresse inverse pour le protocole de couche 3 indiqué en paramètre.
 - Cette résolution est active par défaut.
- **frame-relay map {protocole} {adresse} {dlci} [broadcast] :**
 - Mode de configuration d'interface.
 - Permet de mapper localement une adresse de couche 3 distante avec le DLCI local par lequel passer pour atteindre cette destination.
- **frame-relay intf-type {dte | dce | nni} :**
 - Mode de configuration d'interface.
 - Permet d'explicitier le type d'interface Frame Relay locale.
 - La valeur par défaut est **dte**.
 - **dce** est à utiliser pour l'interface du commutateur Frame Relay reliée au DTE (ETTD), et **nni** est pour les interfaces reliant les commutateurs Frame Relay.
- **frame-relay switching :**
 - Mode de configuration globale. Permet d'activer la commutation de PVC sur une unité ETCD (Commutateur Frame Relay).
 - Active l'interface LMI.
- **frame-relay route {dlci_src} interface {type} {numéro} {dlci_dest} :**
 - Mode de configuration d'interface.
 - Permet de créer une entrée dans la table de commutation Frame Relay.
 - Il faut indiquer le DLCI source, l'interface locale de sortie et celui de la destination.
 - Cette commande est à utiliser sur un commutateur Frame Relay uniquement.

IOS met à notre disposition des commandes de visualisation d'état et de débogage afin de pouvoir vérifier le bon fonctionnement des points spécifiques à Frame Relay, ainsi que d'identifier les problèmes éventuels :

- **show interfaces serial {numéro} :** Affichage des informations sur les DLCI utilisés et sur l'indicateur de connexion de liaison de données LMI utilisé.
- **show frame-relay pvc :** Affichage de l'état de chaque connexion configurée ainsi que les statistiques sur le trafic. Cette commande permet aussi de savoir le nombre de paquets BECN et FECN reçus par le routeur.
- **show frame-relay map :** Affichage de l'adresse de couche 3 ainsi que le DLCI associé à chaque destination distante connectée au routeur local.
- **show frame-relay lmi :** Affichage des statistiques sur le trafic LMI.
- **show frame-relay route :** Affichage des routes Frame Relay configurées avec leur statut.
- **show frame-relay traffic :** Affichage des statistiques Frame Relay globales (Requêtes ARP, etc.).
- **debug frame-relay events :** Affichage des réponses aux requêtes ARP.
- **debug frame-relay lmi :** Affichage des échanges de paquets LMI entre le routeur et le commutateur.
- **debug frame-relay packet :** Analyse des paquets Frame Relay envoyés.

7.6. Configuration

La procédure de configuration d'une interface (DTE) en Frame Relay passe par les étapes suivantes :

- Passer dans le mode de configuration de l'interface voulue (**Commande interface serial {numéro}**).
- Définir une adresse de couche 3 (**Commande ip address {IP} {SM}**).
- Définir le type d'encapsulation (**Commande encapsulation frame-relay**).
- Définir le DLCI local en cas de non support de l'interface LMI (**Commande frame-relay local-dlci {dlci}**).
- Définir optionnellement la bande passante de la liaison (**Commande bandwidth {bp}**).
- Activer l'interface (**Commande no shutdown**).

Cette même procédure change un peu lorsqu'il s'agit de sous-interfaces :

- Passer dans le mode de configuration de l'interface voulue.
- Enlever toute adresse de couche 3 (**Commande no ip address**).
- Définir le type d'encapsulation.
- Passer dans le mode de configuration de la sous-interface voulue (**Commande interface serial {if.subif} {point-to-point | multipoint}**).
- Définir une adresse de couche 3.
- Définir le ou les DLCI locaux, car le LMI ne supporte pas les sous-interfaces (**Commande frame-relay interface-dlci {dlci}**).
- Définir optionnellement la bande passante de la liaison.
- Activer la sous-interface.

Il est possible de simuler un commutateur Frame Relay à l'aide d'un routeur. Les interfaces utilisées sont alors obligatoirement de type DCE. Pour ce faire, il faut utiliser une configuration distincte, et ce pour chaque interface :

- Activer la commutation Frame Relay sur le routeur (**Commande frame-relay switching**).
- Passer dans le mode de configuration de chaque interface utilisée.
- Enlever toute adresse de couche 3.
- Définir le type d'encapsulation.
- Définir la vitesse de fonctionnement de la liaison (**Commande clock rate {valeur}**).
- Définir le type d'interface Frame Relay.
- Définir une route pour chaque destinations accessibles depuis la source raccordée sur l'interface courante (**Commande frame-relay route {dlci_src} interface serial {numéro} {dlci_dest}**).
- Activer l'interface.

8. Initiation à l'administration réseau

8.1. Stations de travail et serveurs

Les premiers ordinateurs personnels (PC) furent conçus pour fonctionner de manière autonome. Le système d'exploitation utilisé sur ces machines autorisait l'accès au fichier et aux ressources du système à un utilisateur à la fois. Peu à peu, les PC ont envahis les espaces de travail, nécessitant de la part des systèmes d'exploitation des fonctions de réseau, permettant le partage de ressource.

Ces systèmes d'exploitation réseaux classifient les ordinateurs en 2 grandes familles :

- Les stations de travail
- Les serveurs

8.1.1. Stations de travail

Une station de travail est un poste utilisateur qui exécute une application et qui est connecté à un serveur à partir duquel il obtient des données partagées. La plupart d'entre elles dispose de connexions réseaux et supporte les accès multi-utilisateurs. Une station de travail peut être de type :

- Ordinateur de bureau.
- Ordinateur portable.
- Ordinateur sans disque dur.

8.1.2. Serveurs

Un serveur est un ordinateur exécutant un système d'exploitation réseau auquel des stations de travail viendront se connecter. De manière générale, les serveurs sont des machines plus puissantes et plus robustes que les stations de travail.

8.2. Systèmes d'exploitation réseau

Un système d'exploitation est un environnement au travers duquel les applications et les services sont exécutés sur une machine. Un système d'exploitation réseau aussi appelé NOS¹, permet la communication entre plusieurs équipements et ressources à travers le réseau. C'est un système multi-tâches et Multi-Utilisateurs capable d'exécuter plusieurs programmes à la fois. Les caractéristiques d'un tel système sont :

- Performance
- Gestion et supervision
- Sécurité
- Evolutivité
- Robustesse/tolérance de panne

Il existe plusieurs familles de système d'exploitation réseau (Windows, Unix, Linux, Apple). Les plus connus sont détaillés ci-dessous.

¹ Network Operating System

8.2.1. Systèmes d'exploitation réseau Microsoft Windows

Microsoft dispose, dans son offre commerciale, de plusieurs NOS :

- Windows NT4 Server

Sortie en Juillet 1996, Windows NT4 peut s'exécuter à la fois en tant que station de travail (NT4 Workstation) ou en tant que serveur (NT4 Server). Windows NT utilise une structure de domaine afin de contrôler les accès utilisateurs et les accès aux ressources. Chaque domaine NT nécessite la présence d'un contrôleur de domaine contenant la base SAM². Lorsqu'un utilisateur se connecte au domaine NT, les informations du compte de l'utilisateur sont envoyées à la base de données SAM. Si le compte est valide, l'utilisateur est authentifié sur le domaine et a accès à la station de travail.

- Windows2000 Server

Sortie en février 2000, Windows 2000 existe en version « Professional » et « Server »

Basé sur le noyau de Windows NT4, Windows2000 Server intègre également la technologie « Plug and Play ». La gestion des utilisateurs et des ressources d'un domaine peut maintenant se faire en tant qu'objets. Ceux-ci peuvent être placés dans des conteneurs, dont la gestion peut être déléguée à un utilisateur ou un groupe. Tout cela est possible via la technologie Active Directory.

- Windows2003 Server

Sortie en Avril 2003, Windows 2003 Server reprend les points forts de Windows2000 Server. Il accroît les fonctionnalités de migration depuis Windows NT4, tout en étant compatible avec un domaine NT4. Divers services réseaux ont été améliorés tel que « IIS Web Server ». De plus, la technologie .NET a été directement intégrée au système.

8.2.2. Systèmes d'exploitation réseau UNIX et Linux

- UNIX

Unix est un nom donné à un groupe de systèmes d'exploitations issu des laboratoires Bell de 1969. C'est un système multi-utilisateurs et multitâches qui prend en compte les protocoles réseau d'Internet. Au fil du temps plusieurs entreprises ont contribué au développement d'Unix, ce qui entraîna dans les années 1980 sa commercialisation sous diverses appellations :

- Hewlett Packard UNIX (HP-UX)
- Santa Cruz Operation (SCO) UNIX
- Sun Solaris
- IBM UNIX (AIX)

Berkeley Software Design, Inc. (BSD UNIX) distribuera également sa version d'Unix qui produira des dérivés tels que :

- FreeBSD
- OpenBSD
- NetBSD

Unix sous ses diverses formes compose et consolide aujourd'hui sa position de système d'exploitation fiable et sécurisé. Cependant Unix est souvent associé à du matériel coûteux et propriétaire, mais la création de Linux est en train de changer cette image.

- Linux

En 1991, frustré par l'état des systèmes d'exploitation de bureau, mais aussi par les coûts et les problèmes de licence, un étudiant Finlandais du nom de Linus Torvald se mit à travailler sur un système d'exploitation destiné

² Sécurité Accounts Management Database

Laboratoire SUPINFO des Technologies Cisco

Site Web : www.labo-cisco.com – E-mail : labo-cisco@supinfo.com

Ce document est la propriété de SUPINFO et est soumis aux règles de droits d'auteurs

aux ordinateurs à base de processeur 80386. Son système était semblable à Unix et, particularité de ce dernier, le code était ouvert et gratuit pour tous les utilisateurs. Son travail mena à une collaboration Internationale entre la communauté des développeurs et dès la fin des années 1990, Linux était devenue une alternative aux serveurs Unix et aux systèmes de bureau Windows.

A l'instar d'Unix il existe plusieurs versions de Linux dont :

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

Linux est doté de composants réseaux intégrés permettant de se connecter à un réseau local, établir une connexion réseau commutée vers l'Internet ou faire du tunnelling. La pile de protocole TCP/IP est d'ailleurs directement intégrée au noyau Linux.

8.2.3. Système d'exploitation réseau Apple

Apple dispose également d'une version Serveur de son fameux système d'exploitation Mac OS X. Ce dernier dénommé Mac OS X Server est capable de gérer des ordinateurs sous divers systèmes d'exploitation Apple et concurrents (Mac OS 9, Microsoft Windows, Unix et Linux etc..). Le noyau de Mac OS X qui a pour nom de code « Darwin » est dérivé de la technologie BSD4.5 et 5.0. Il en résulte une combinaison de la technologie serveur open source la plus populaire, combinée à l'installation et l'utilisation aisée des systèmes Apple. Les applications réseaux classiques sont toutes supportées (NTP, SMTP, DNS, LDAP, etc..) et le partage des données avec des clients Unix et Windows est également supporté (Nfs, Samba).

8.3. Gestion du réseau

8.3.1. Introduction à la gestion réseau

Un réseau évolue. A mesure que ce dernier s'étend, il devient une ressource de plus en plus cruciale pour l'organisation. Sa gestion se complique et conséquence de tout cela, le réseau devient de plus en plus complexe. Dans ce cas de figure, la tâche de l'administrateur devient ardue : la non constatation de la défaillance d'un service peut avoir des conséquences graves en environnement de production.

L'administrateur doit gérer le réseau de manière active, diagnostiquer les problèmes, prévoir les pannes, et les empêcher de survenir. Les mauvaises performances et la perte de ressources réseaux ne sont pas acceptables pour les utilisateurs. Il devient très difficile pour un administrateur, voire impossible, d'assurer toutes ces tâches sans aide logicielle ni outils de gestion automatique du réseau.

Les facteurs qui régissent l'administration réseau sont les suivants :

- **Contrôle des ressources de l'entreprise** – Gestion efficace des ressources réseaux. Le cas échéant, les résultats fournis ne seront pas à la hauteur d'une administration efficace.
- **Contrôle de la complexité** – Contrôler l'évolution du réseau afin d'éviter que trop de complexité n'entraîne la perte de contrôle de ce dernier.
- **Amélioration du service** – S'assurer que l'utilisateur bénéficie d'un meilleur service, sinon égal à l'ancien, à mesure que le réseau évolue.
- **Équilibrage des divers besoins** – Les applications mises à la disposition des utilisateurs doivent l'être avec un niveau donné de support, de disponibilité et de sécurité.
- **Réduction des temps d'arrêt** – Assurer la redondance des services en environnement haute disponibilité.

- **Contrôle des coûts** – Surveiller et contrôler l'utilisation des ressources, de cette manière les utilisateurs peuvent être satisfaits à coût raisonnable.

L'administration réseau implique les tâches ci-dessous:

- La surveillance de la disponibilité du réseau
- L'amélioration de l'automatisation
- La surveillance des temps de réponse
- La mise en place de fonctionnalités de sécurité
- Le réacheminement du trafic
- Le rétablissement de la fonctionnalité
- L'enregistrement d'utilisateurs

8.3.2. Modèle de gestion réseau et OSI

Afin d'avoir un modèle commun à tout les constructeurs, l'ISO s'est occupé de créer un standard pour la gestion du réseau. La tâche de produire un modèle d'administration réseau commun fut assignée à un comité dirigé par le groupe OSI.

Le comité en charge de cette modélisation en est arrivé à un modèle d'administration découpé en quatre parties :

- **Le modèle d'organisation** Il définit les différents composant de l'administration réseau, Administrateur, NMS, agent SNMP etc., ainsi que leurs relations.
- **Le modèle d'information** Il définit la structure de stockage des informations d'administration appelé SMI. Cette structure définit la syntaxe des informations d'administration. Le contenu de la SMI est appelé MIB.
- **Le modèle de communication** Il définit la manière dont les données sont acheminées depuis la NMS jusqu'aux agents SNMP. Il traite du protocole de communication (SNMP).
- **Le modèle fonctionnel** Il traite des applications d'administration réseau qui s'exécutent sur la NMS.

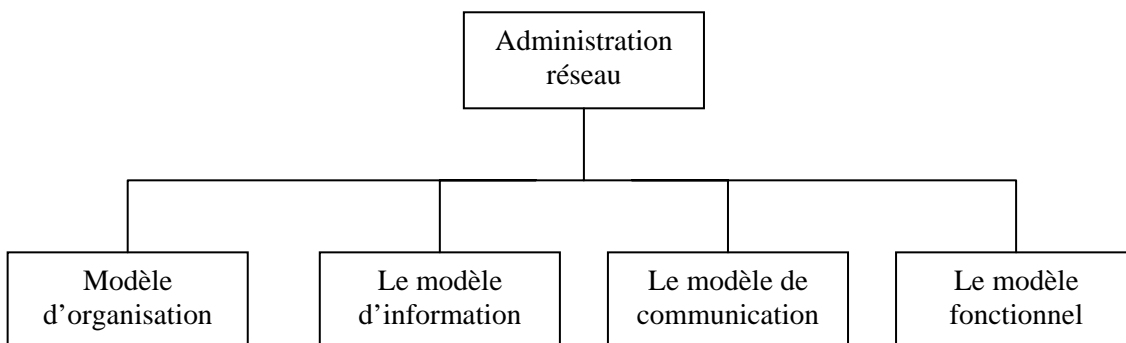


Figure 1- Modèle de gestion réseau de l'ISO

8.4. Protocole SNMP

8.4.1. Introduction

SNMP (Simple Network Management Protocol) a été adopté comme norme pour les réseaux TCP/IP en 1989. Ce protocole désigne un ensemble de normes d'administration, notamment :

- Un protocole de communication
- Une spécification de structure de base de données
- Un ensemble d'objets de données

Très populaire et présent dans la plupart des réseaux d'entreprise, SNMP connu une mise à niveau (SNMPv2c) en 1993, améliorant entre autre la structure des informations d'administration, l'authentification ainsi que le protocole lui-même. SNMP évolue pour en arriver à la version 3 (SNMPv3) qui prend en charge l'authentification et le cryptage des communications tout en restant rétro compatible.

8.4.2. Fonctionnement

SNMP est un protocole de la couche application conçu pour faciliter l'échange d'informations d'administration entre les équipements réseaux. On peut par exemple l'utiliser pour accéder à des données d'informations d'administrations tels que le nombre de paquets en sortie sur l'interface WAN d'un routeur, le nombre de connexions TCP ouvertes ou même la quantité d'erreur détectées sur cette même interface.

La quantité d'informations accessibles et récupérables est très nombreuse et détaillée. SNMP est un protocole simple, mais ses fonctions sont suffisamment efficaces pour gérer les problèmes liés à l'administration des réseaux hétérogènes. Le modèle organisationnel de l'administration réseau SNMP comporte quatre éléments :

- La station de gestion du réseau (NMS : Network Management System)
- Les agents de supervision (Agent SNMP)
- La base d'information de management (MIB : Management Information Base)
- Le protocole de gestion réseau.

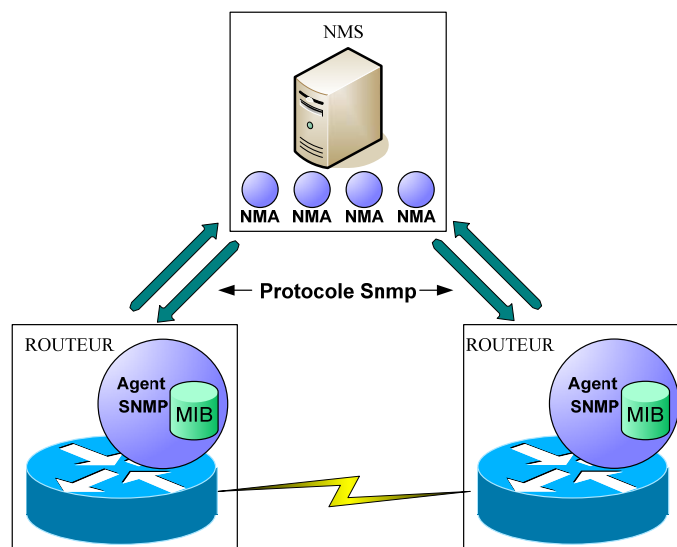


Figure 2-Fonctionnement de SNMP

La NMS est généralement une station de travail autonome. Elle se compose d'un ensemble de logiciels appelé NMA.

Ceux-ci intègrent une interface utilisateur permettant aux administrateurs de superviser le réseau en récupérant des informations sur les agents SNMP. Ceux-ci sont situés sur les différents équipements réseaux (routeur, pont, commutateur, répéteur, serveur d'application).

Un agent SNMP peut répondre à une requête d'exécution d'action de la part de la NMS. Il peut également remonter des informations utiles, non sollicitées par la NMS, telles que la perte de connectivité entre deux routeurs, ou un dysfonctionnement du service de messagerie de l'entreprise.

Un agent SNMP peut effectuer un suivi de ces éléments :

- 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 inter réseaux.
- Les messages de broadcast envoyés et reçus.
- L'état d'activation des interfaces réseau.

Afin de permettre à une NMS de dialoguer avec un agent SNMP, le protocole définit une chaîne de caractère : « l'identifiant de communauté ». Les échanges ne sont possibles qu'entre agents et NMA d'une même communauté SNMP.

Cette forme très basique de vérification reste une simple identification implémentée dans le protocole SNMP (SNMPv1).

Ceci représentant une faille de sécurité de taille (cet identifiant transitant en clair), la version 2 de SNMP a bénéficié de l'implémentation de mécanismes d'authentification et d'intégrité (chiffrement symétrique à clé privée utilisant l'algorithme HMAC-MD5-96).

Celle-ci posant des problèmes de rétro compatibilité, la version 3 a été conçue pour parer à ces problèmes. SNMPv3 permet donc une sécurité accrue ainsi qu'une rétro compatibilité.

A un identifiant de communauté, peut être affecté des permissions en lecture seulement ou en lecture/écriture sur les objets.

La communauté par défaut pour la lecture seule est « public », et « private » pour l'accès en lecture et écriture.

Version	Authentification	Confidentialité	Cryptage	Fonctionnement
SNMPv1	Non	Non	Non	Identification assurée par l'appartenance à la communauté SNMP
SNMPv2c	Oui	Oui	Oui	Authentification par chiffrement symétrique Problème de rétro compatibilité
SNMPv3	Oui	Oui	Oui	Authentification par chiffrement symétrique Rétro compatible

Tableau 1-Différences SNMPv1SNMPv2c, SNMPv3

SNMP est un protocole de la couche application qui utilise les ports UDP 161 (NMS) et 162 (Agent). Il fonctionne selon un système d'échange de messages.

Ces derniers peuvent être de types :

- **Get** : Récupération de la valeur d'un objet de la MIB à partir de l'agent, nécessite au moins les droits en lecture.
- **Set** : Affecter une valeur à l'un des objets MIB grâce à l'agent, nécessite les droits en lecture et écriture.
- **Trap** : Utilisé par l'agent afin de signaler des informations jugées «importantes» à la NMS.

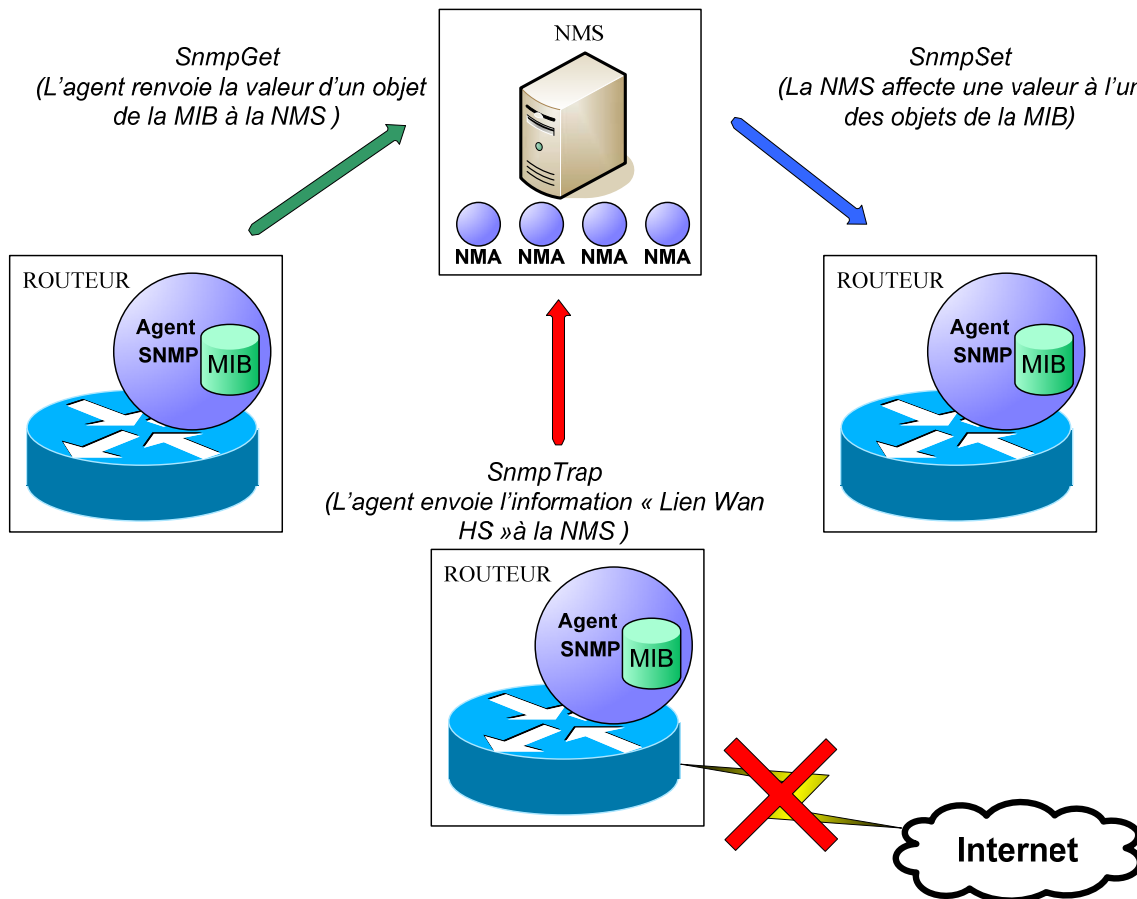


Figure 3 - Les types de messages SNMP

8.4.3. MIB

La MIB est organisée en arborescence définie par la norme SMI³. SMI spécifie également les types de données utilisés pour stocker un objet (entier, chaîne de caractère), la manière dont ces objets sont nommés etc. Chaque élément final de la MIB représente un attribut de l'équipement réseau concerné.

C'est un référentiel contenant une somme considérable d'informations concernant l'équipement. Il existe des MIB standards et propriétaires :

La MIB SMI d'origine est composée de 8 groupes et de 114 objets. Nous en sommes actuellement à la version 2 de la MIB aussi appelée MIB-II.

Les MIB propriétaires sont propres aux équipements du constructeur.

Ci-dessous, un exemple de MIB-II :

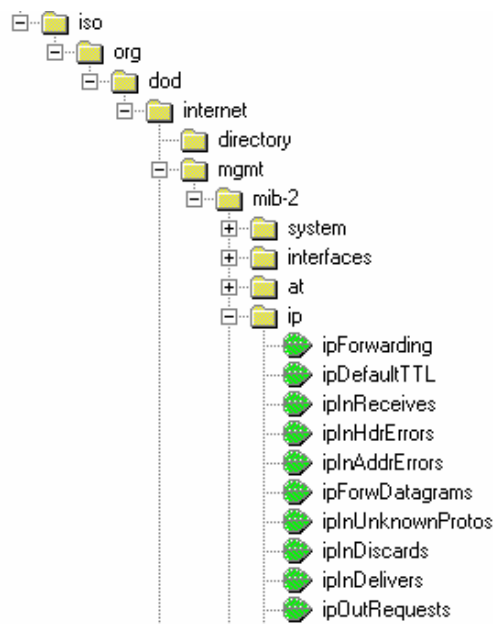


Figure 4 - Représentation logicielle d'une MIB

Chaque feuille de la MIB est identifiée par une OID⁴.

Une OID est une information constituée de valeurs décimales pointées. (Exemple : 1.3.6.1.2.1.4.3).

Chaque valeur décimale de l'OID identifie l'une des branches de la MIB.

Exemple pour l'objet « **ipInReceives** »:

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).ip(4).ipInReceives(3)

Le schéma ci dessous présente les différents groupes de la MIB ainsi que leurs OID:

³ Structure of Management Information

⁴ Object Identifier

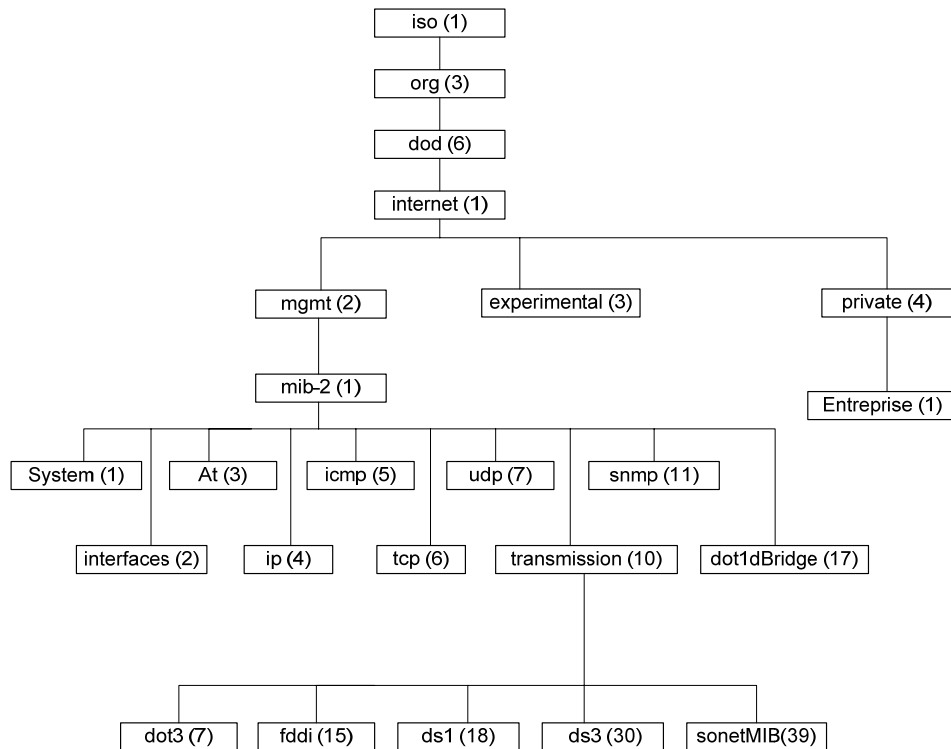


Figure 5 - Représentation des groupes de la MIB et de leur OID

8.4.4. Configuration

Voici les commandes de configuration nécessaires à la communication entre les équipements réseaux et la NMS :

- **snmp-server community {communauté} ro**
 - Mode de configuration globale
 - Autorise l'accès en lecture seule à la communauté spécifiée
- **snmp-server community {communauté} rw**
 - Mode de configuration globale
 - Autorise l'accès en lecture et écriture à la communauté spécifiée
- **snmp-server location {emplacement}**
 - Mode de configuration globale
 - Configure la description de l'emplacement du routeur
- **snmp-server contact {chaîne de caractère}**
 - Mode de configuration globale
 - Configure les informations relatives aux personnes à contacter si besoin est
- **snmp-server host {IP de la NMS} {communauté}**
 - Mode de configuration globale
 - Spécifie une NMS qui recevra les Traps SNMP
- **snmp-server enable traps snmp [authentication][linkup][linkdown][coldstart] [warmstart]**
 - Mode de configuration globale
 - Spécifie le(s) événement(s) qui déclencheront l'envoi des traps

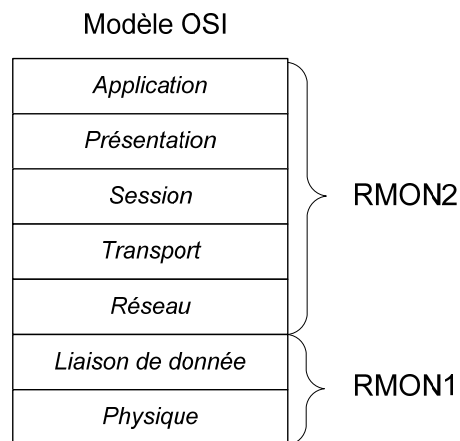
8.4.5. RMON

RMON définit une MIB de surveillance qui complète MIB-II. Cette MIB contient des informations de statistiques obtenues en analysant chaque trame d'un segment du réseau. Pour se faire, des dispositifs de surveillance matérielle (sonde RMON) sont placés sur les segments à surveiller. Ces dispositifs permettent de créer des alarmes définies par l'utilisateur, mais surtout de rassembler une multitude de statistiques vitales grâce à l'analyse approfondie de chaque trame d'un segment.

Avec RMON, l'administrateur peut obtenir des informations relatives à la globalité d'un segment LAN (pourcentage de collisions sur le segment, stations émettant le plus de broadcast etc...). L'administrateur n'a plus pour limite la vision d'information locale et propre à une station exécutant un agent SNMP classique. RMON n'a pas nécessité la modification du protocole SNMP, il n'a suffi pour intégrer RMON que de rajouter des entités dans la MIB. Il existe en deux versions :

RMON1 – Fonctionnant au niveau des couches 1 et 2 du modèle OSI.

RMON2 – Fonctionnant au niveau des couche 3 à 7 du modèle OSI.



- **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**

Définit un ensemble de filtres afin d'identifier et capturer un flux de paquets correspondant à un schéma distinct.

- **Groupe d'interception des paquets**

Définit la méthode de mise en tampon interne des paquets qui répondent aux critères de filtrage.

- **Groupe des événements**

Consigne des événements à l'intention de l'administrateur. Il s'agit par exemple de rapports personnalisés s'appuyant sur le type d'alarme.

- **Groupe de répertoire des protocoles**

Contient une liste de protocoles supportés par la sonde RMON2, ce groupe est essentiel lorsqu'un agent RMON2 désire savoir quel protocole de communication utilise la sonde RMON2, surtout lorsque les constructeurs des agents et des sondes diffèrent.

- **Groupe de distribution des protocoles**

Contient les données collectées par la sonde, regroupées par protocoles.

- **Groupe de mappage des adresses IP**

Conserve les informations de mappages des adresses mac avec leurs adresses IP.

- **Groupe des hôtes réseaux**

Conserve les statistiques de la couche réseau relatives à une adresse IP.

- **Groupe des matrices de la couche réseau**

Contient des statistiques de la couche réseau concernant les échanges entre deux adresses IP.

- **Groupe des hôtes applicatifs**

Contient des statistiques concernant les protocoles de la couche application d'un hôte.

- **Groupe des matrices de trafic applicatif**

Stocke des statistiques de la couche application relative aux échanges entre deux hôtes.

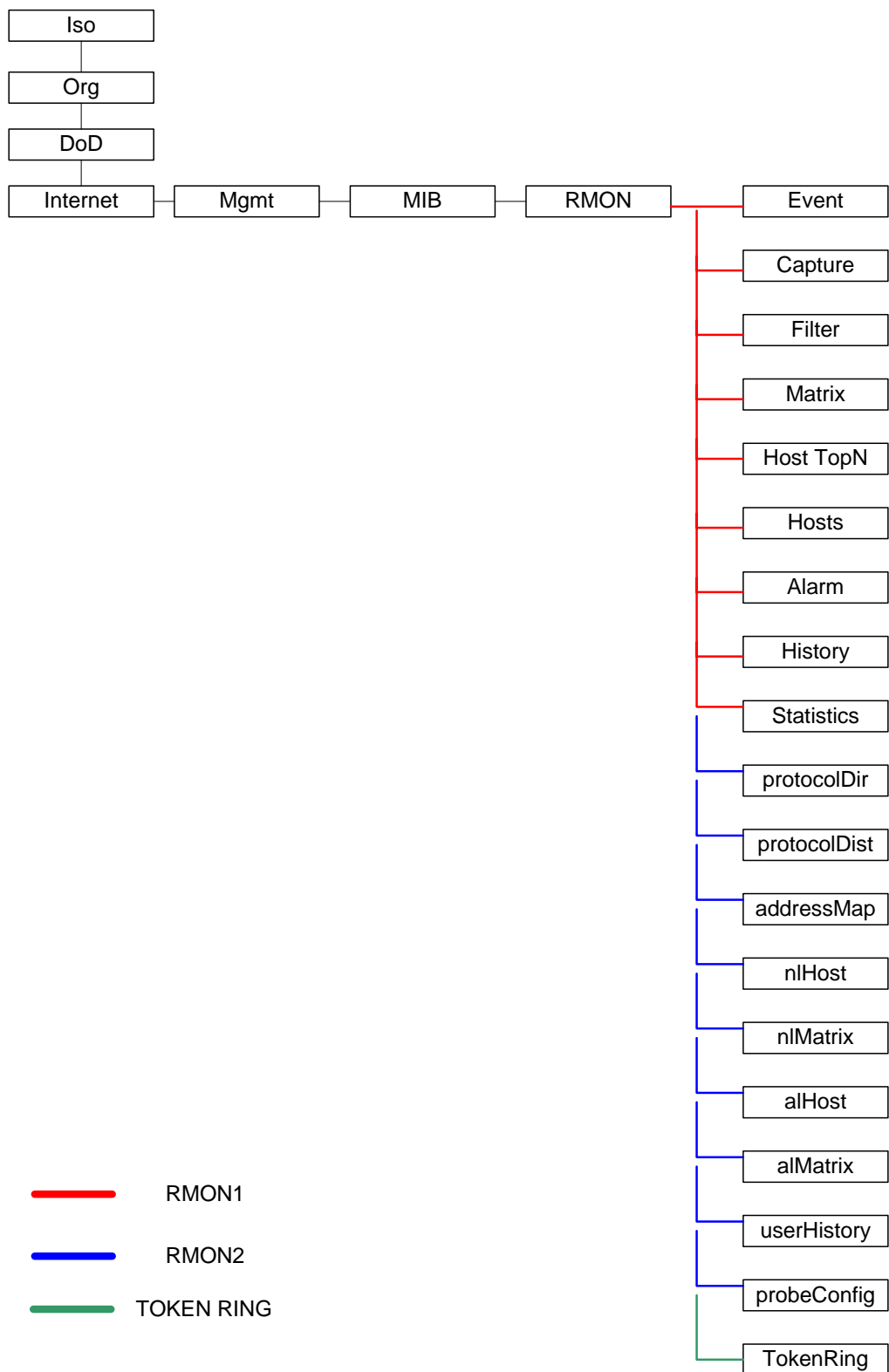
- **Groupe de l'historique des utilisateurs**

Permet à l'administrateur réseau d'archiver les données relatives à n'importe quel hôte du segment, un serveur web ou autres, ...

- **Groupe de configuration de la sonde**

Permet à une application d'un constructeur de configurer à distance la sonde RMON2 d'un autre constructeur.

Ci-dessous, les groupes : RMON1, RMON2, et Token Ring :



8.5. Syslog

8.5.1. Fonctionnement

Syslog est un utilitaire de consignation d'évènements Cisco basé sur l'utilitaire Syslog d'Unix. A l'origine, Syslog avait été développé pour le logiciel Sendmail uniquement. Mais l'utilité de ce dernier était telle que beaucoup d'autres applications se sont mises à l'utiliser. Syslog fonctionne sur un modèle client - serveur.

Le port utilisé sur le serveur est le port UDP/514 et la taille des messages ne peut excéder 1024 octets. En 2001, les spécifications de Syslog ont été définies dans la RFC 3164.

Sur un routeur ou commutateur Cisco, les évènements Syslog peuvent être envoyés sur une NMS. Les messages envoyés seront alors de type « non sollicités » (Traps).

Chaque message syslog est horodaté, contient un niveau de gravité ainsi qu'un message de consignation. Ces messages sont parfois la seule manière de résoudre un problème sur les équipements. Il existe 8 niveaux de gravité dans les Traps Syslog (0 à 7). Le niveau 0 étant le plus critique (7 le moins).

Un équipement réseau n'envoiera au serveur Syslog que des messages dont la gravité est supérieure (inférieure en chiffre) au seuil défini.

Par défaut, le niveau de gravité est à 6 sur les IOS Cisco. On aura donc tous les messages disponibles excepté ceux de débogage.

Niveau de gravité	Description
0	Urgences
1	Alertes
2	Critique
3	Erreurs
4	Avertissements
5	Notifications
6	Informatifs
7	Déboguages

Niveau par défaut de Cisco IOS →

Par défaut, Cisco IOS adopte le niveau de gravité 6. Ce paramètre est configurable.

8.5.2. Configuration

Pour que la NMS puissent recevoir les traps Syslog d'un équipement, il faut qu'une application serveur Syslog (CiscoWorks2000, Kiwi Syslog...) soit configurée sur celle-ci.

Il faut également configurer le routeur pour l'envoi des événements sur la NMS. Ci-dessous, les différentes commandes de configurations nécessaires sur un routeur 2620xm :

- **logging on**
 - Mode de configuration globale
 - Active la consignation des événements
- **logging {nom d'hôte} | {adresse IP de la station}**
 - Mode de configuration globale
 - Spécifie au routeur la station NMS recevant les traps Syslog
- **logging trap {debugging | informational | notification | warnings | errors | critical | alerts | emergencies}**
 - Mode de configuration globale
 - Configure le niveau de gravité (optionnel)
- **service timestamps log datetime**
 - Mode de configuration globale
 - Horodate les messages syslog (optionnel)