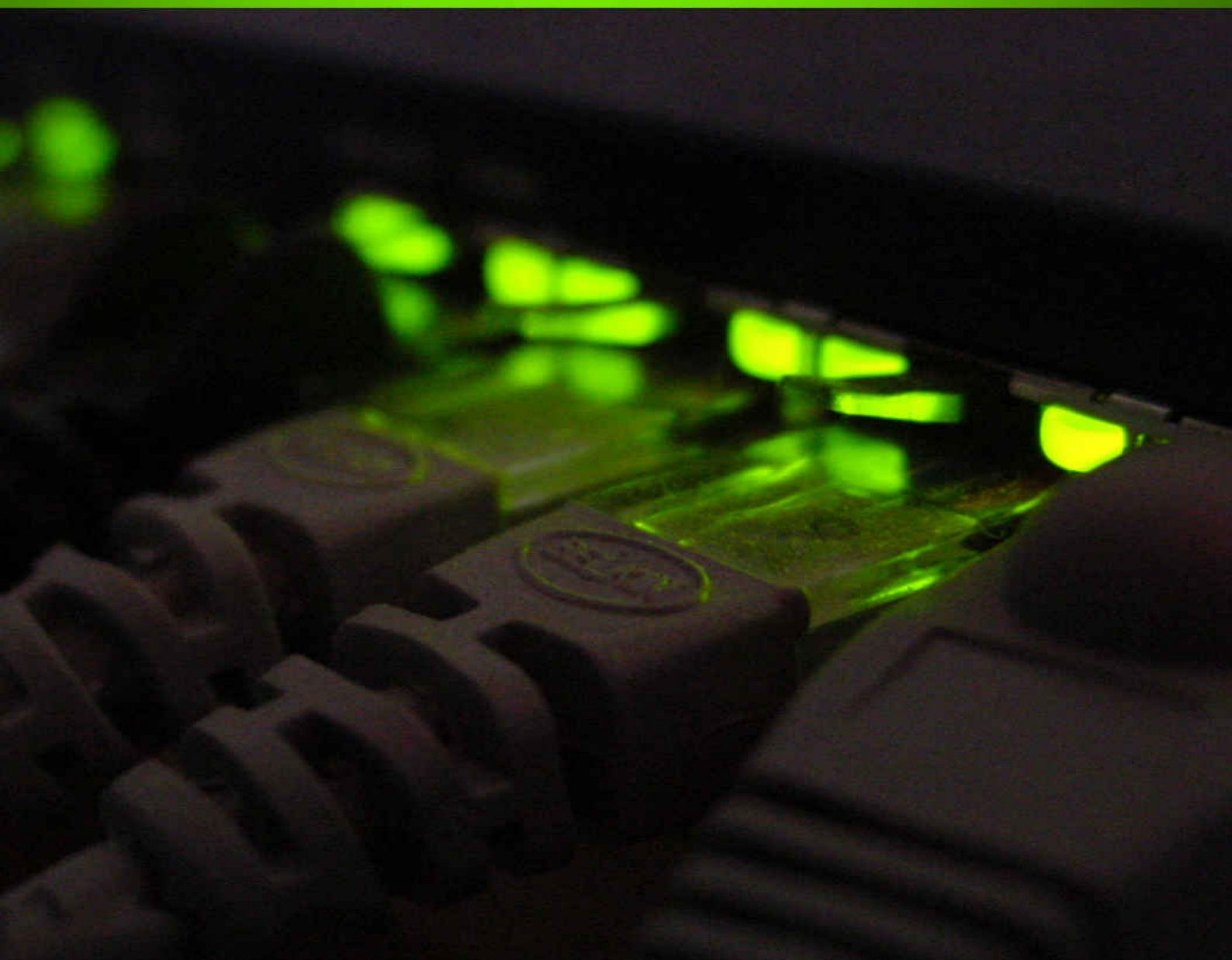
ADMINISTRATION SYSTÈME RÉSEAUX

bases de l'administration

Alain MOUHLI



Bases Du système D’administration

Alain MOUHLI

Contenu

Chapitre 1 : Réseaux WAN Chapitre 2 Conception WAN Chapitre 3 PPP Chapitre 4 RNIS Chapitre 5 VLAN Chapitre 6 Administration Réseaux

Réseaux WAN

1. DEFINITIONS

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 la couche 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 :

Etablissement 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 fixes, 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 ETTD est appelé :

Liaison. Circuit. Canal. Ligne.

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

o Etabli dynamiquement sur demande et fermé en fin de transmission. o Communication en trois phases : Etablissement du circuit, transfert des données et

fermeture du circuit.

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

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

PVC :

o Etabli en permanence.

o Est utilisé pour transmettre des débits de données constantes.

o Communication en une phase : Transfert des données.

o Consommation en bande passante réduite par rapport à un SVC.

o Coûts supérieurs en raison de la continuité de service.

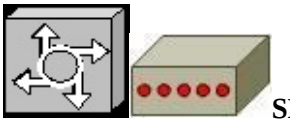
Exemples de lignes WAN et bande passante associée :

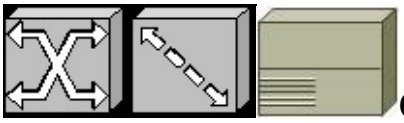
Type de ligne T1
E1
E3
T3

Bande passante
1.544 Mbits/s
2.048 Mbits/s 34.064 Mbits/s 44.736 Mbits/s

2. EQUIPEMENTS & DISPOSITIFS


ROUTEUR


SERVEUR DE COMMUNICATION MODEM (Unité CSU/DSU, TA, NT1, etc.)


Commutateurs WAN (ATM, RNIS, etc.)

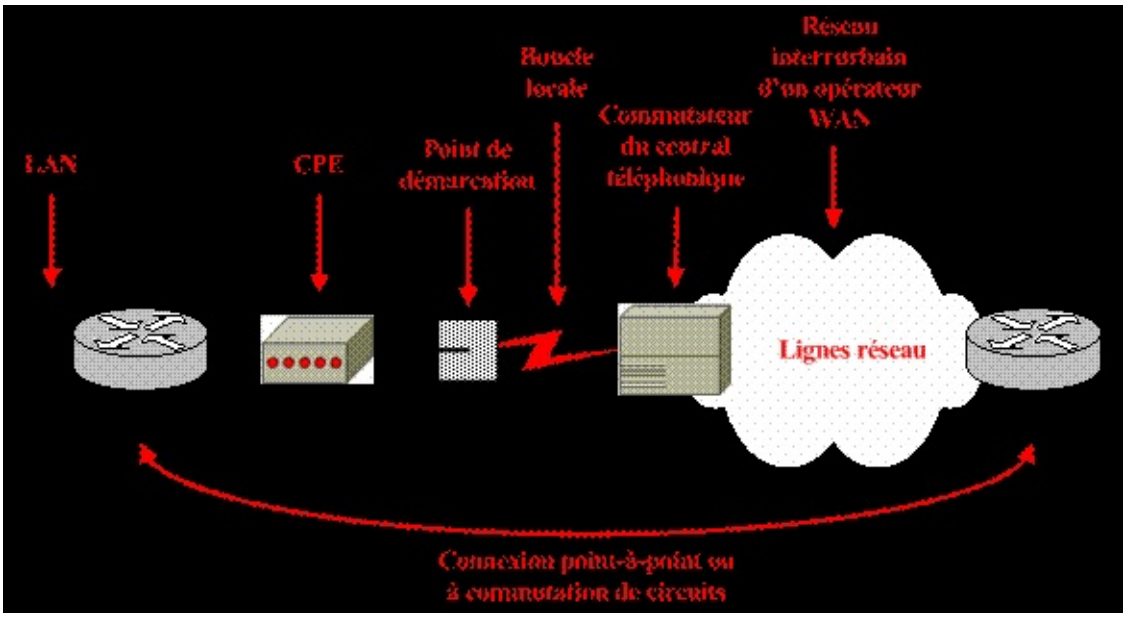
Routeur : Dispositif de routage, offrant différents services dont des ports d'interface de réseau LAN et WAN.

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. LES NORMES WAN

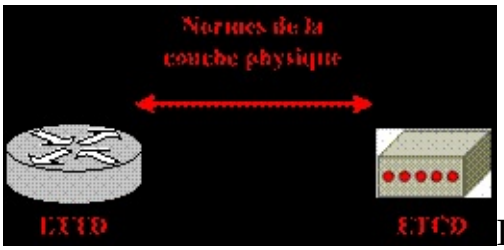
Les normes des réseaux WAN décrivent généralement les méthodes d'acheminement de la couche physique ainsi que la configuration exigée pour la couche liaison de donnée, notamment :

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

Les principaux organismes définissant et gérant les normes WAN sont :

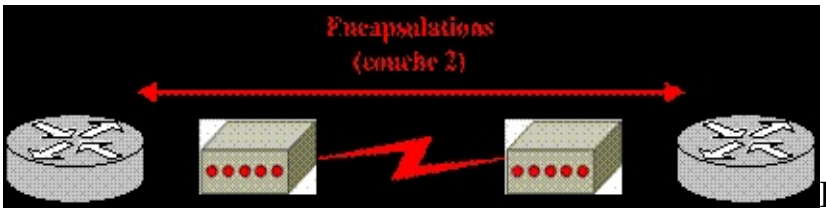
UIT-T (Union Internationale des Télécommunications - secteur de normalisation des Télécommunications), anciennement appelée CCITT (Comité Consultatif International Télégraphique et Téléphonique).

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 œuvre 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**.

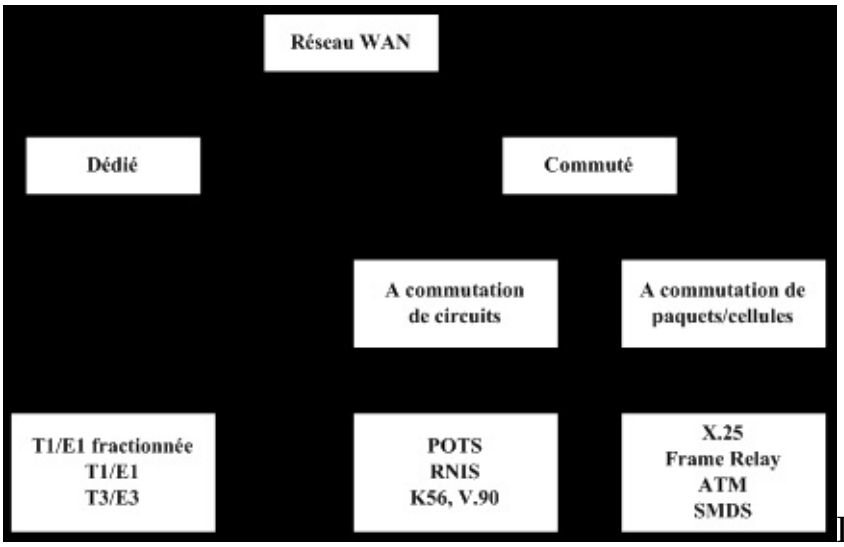
PPP :
○ Comprend un champ identifiant le protocole de couche réseau.
○ Vérifie la qualité de la liaison au moment de l’établissement d’une connexion. ○ Gère l’authentification grâce aux protocoles PAP et CHAP.

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 elle n’est pas fiable ou possède un délai inhérent (Exemple : liaison par satellite).
○ Apporte la fiabilité et le contrôle de flux sur une base point-à-point.
HDLC :

o Peut être incompatible entre fournisseurs car chacun a sa propre mise en œuvre. o Prend en charge les configurations point-à-point et multipoints.
o Dérivé du protocole SDLC.
o Protocole par défaut pour les interfaces série d'un routeur Cisco.
o Extrêmement simplifié : Pas de fonctions de fenêtrage ni de contrôle de flux. o 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.

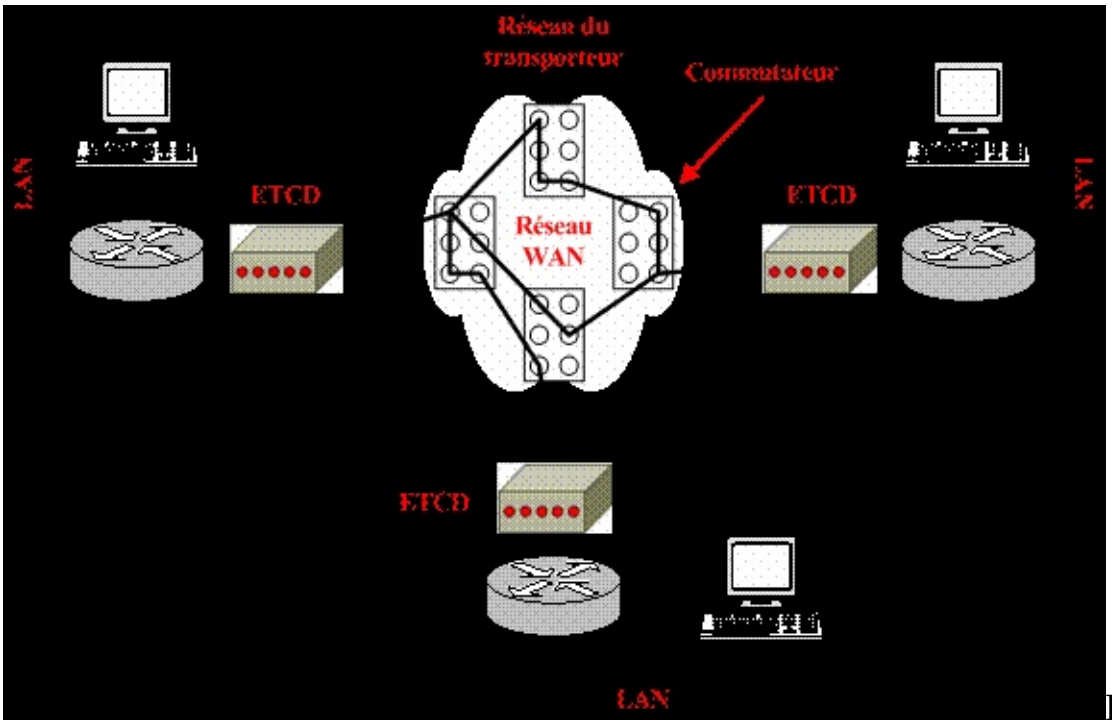
4. CLASSEMENT DES DIFFERENTS TYPES DE LIAISONS WAN



Les différents types de liaison WAN habituellement disponibles sont :

Liaisons dédiées (aussi appelées **liaisons spécialisées** ou **lignes louées**) : o Fournissent un service continu.
o 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. o Il est nécessaire d'avoir un port par liaison client sur le routeur de l'opérateur. o Fournies par des liaisons série synchrone point-à-point.
o Cette liaison point-à-point est utilisée pour :

Une liaison physique directe.
Des liaisons virtuelles constituées de plusieurs liaisons physiques. o Conviennent aux grands volumes d'information et aux trafics constants. **Connexions commutées** :
o **A commutation de circuits** :
Commutation physique des centraux téléphoniques afin d'obtenir la liaison point-à-point.
o **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 :

o Circuit physique dédié par commutation des centraux téléphoniques. o Etabli, maintenu et fermé à chaque session.

o Etabli à la demande.

o Sert aussi de ligne de secours aux circuits haut débit.

o Offre une bande passante dédiée.

Commutation de paquets/cellules :

o Utilisation d'un PVC similaire à une liaison point-à-point.

o Possibilité d'acheminer des trames de taille variable (paquets) ou de taille fixe (cellules).

o Les unités du réseau partagent une liaison point-à-point unique. o Plus souple et utilise mieux la bande passante que les services à commutation de circuits.

Conception WAN

1. COMMUNICATION DANS UN WAN

La communication WAN est généralement appelée “service” car elle à 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.).
Evolution 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.

2. PREMIERES ETAPES 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’utilisateur. **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.

3. MODELES DE RESEAU HIERARCHIQUES
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 sousensemble uniquement).
Limiter les coûts de construction et d'élaboration du réseau.
Faciliter l'identification des points de défaillance.

Il existe deux structures de modèle de réseau :

Hiérarchique :
- Réseau divisé en couches.
- Fonction(s) précise(s) associée(s) à chaque couche.

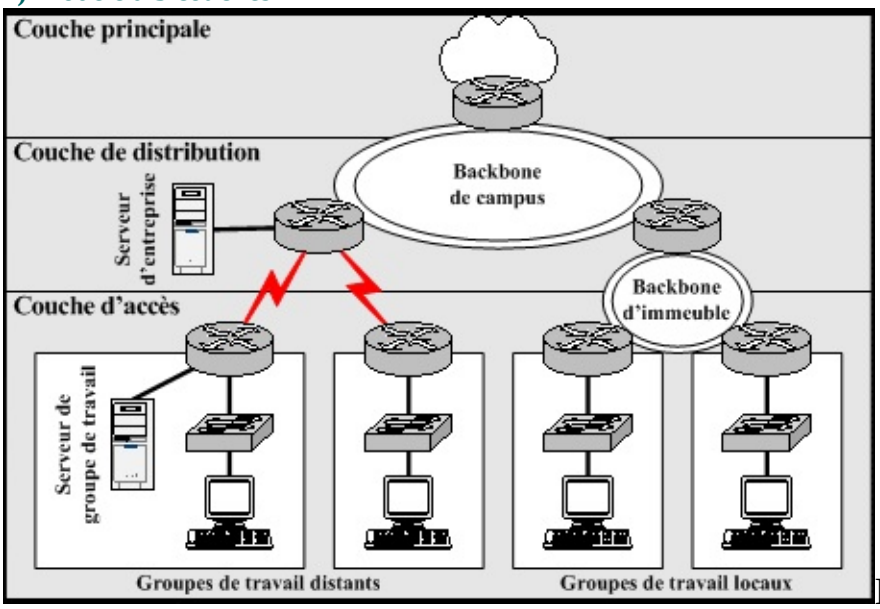
Maillée :
- Topologie linéaire.
- Tous les dispositifs ont les mêmes fonctions.

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

Evolutivité.
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.

1) Modèle à 3 couches



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 :

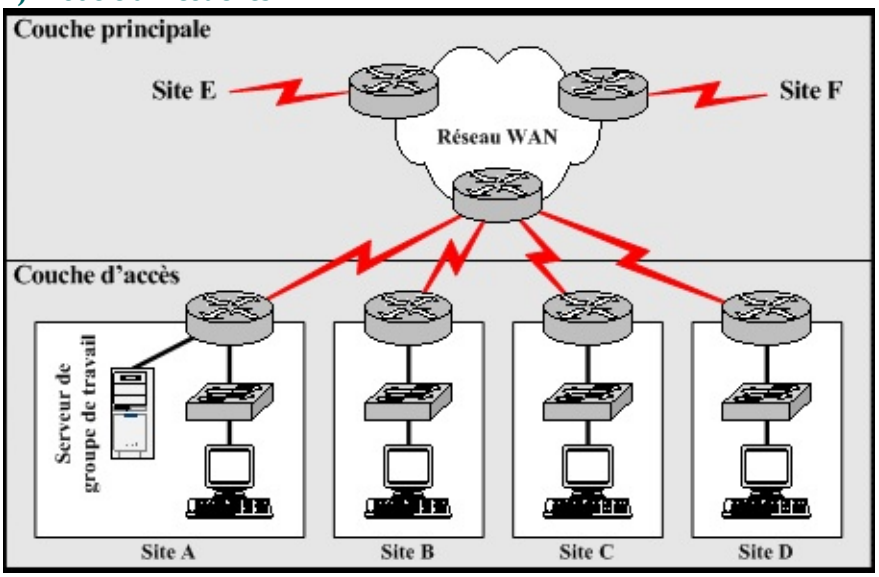
Fournit des services à plusieurs LAN au sein d'un WAN (Backbone de campus). C'est l'emplacement du backbone du WAN (de type Fast Ethernet).
Sert à interconnecter des immeubles.
Emplacement des serveurs d'entreprise (DNS, messagerie centralisée).
A pour rôle de définir les frontières (Sous la forme de 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, microsegmentation et VLAN. Regroupement des utilisateurs selon leur fonction, leurs besoins. Isolation du

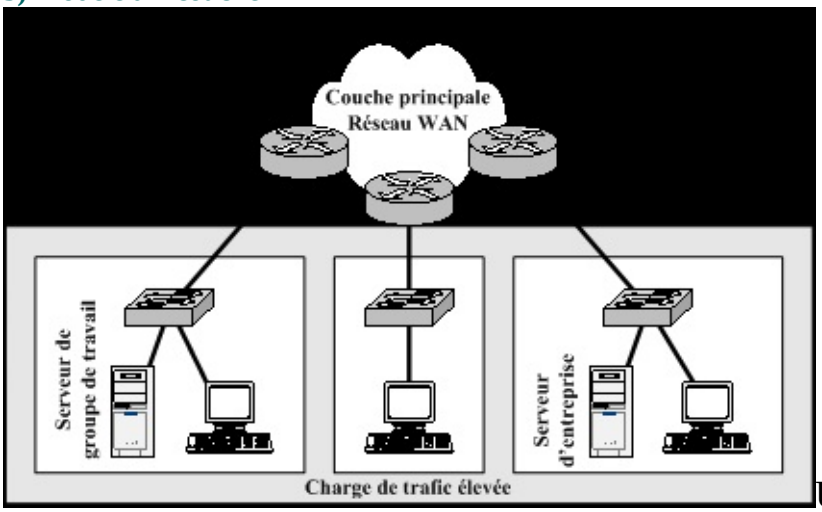
trafic de broadcast destiné à un groupe de travail ou à un LAN.

2) Modèle à 2 couches



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.

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.

PPP

Présentation de PPP

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.).

Les développeurs ont conçu PPP pour établir les connexions sur des liaisons point à point. PPP, à l'origine décrit dans les RFC 1661 et 1332, encapsule des informations de protocoles de la couche réseau sur des liaisons point à point. Le RFC 1661 a été mis à jour par le RFC 2153, *" PPP Vendor Extensions "*.

Il est possible de configurer PPP sur les types d'interfaces physiques suivants :

Série asynchrone
HSSI (High speed serial Interface, interface série à haute vitesse) RNIS
Série synchrone

PPP utilise son composant NCP (*Network Control Program, programme de contrôle de réseau*) pour encapsuler plusieurs protocoles, cf. fig1. Cet emploi de NCP dépasse les limites du prédécesseur de PPP, SLIP (*Serial Line IP*), qui ne pouvait permettre que le transport de paquets IP.

PPP utilise un autre de ses composants principaux, le protocole LCP (*Link Control Protocol*), pour négocier et définir des options de contrôle sur la liaison de données WAN.

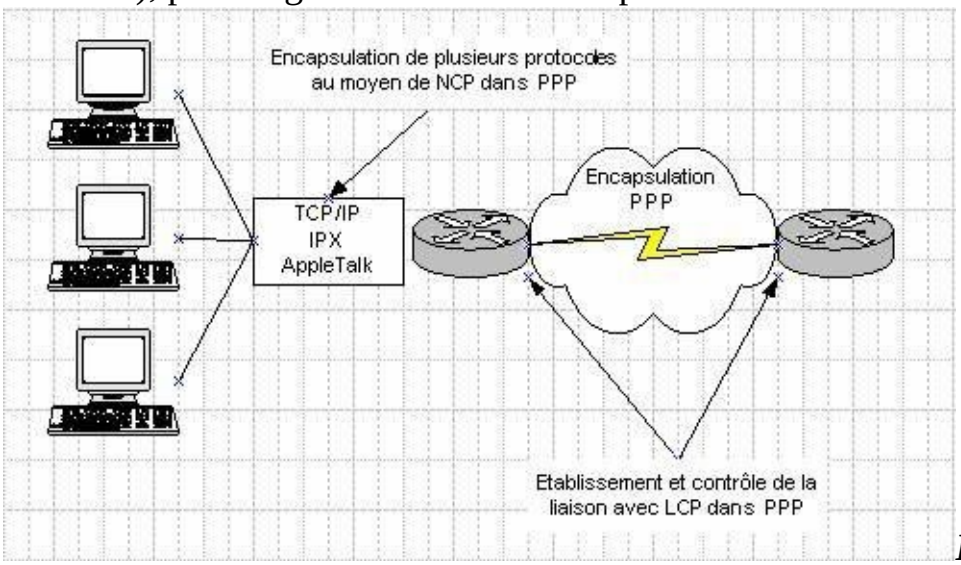


Figure 1

COMPOSANTS DE PPP EN COUCHES

PPP utilise une architecture en couches, comme illustré Fig.2. Avec ses fonctions les plus

basses, PPP peut employer :
Un média physique synchrone comme ceux qui connectent RNIS, Un média physique asynchrone comme ceux qui utilisent les services téléphoniques de base pour les connexions par modems commutés.

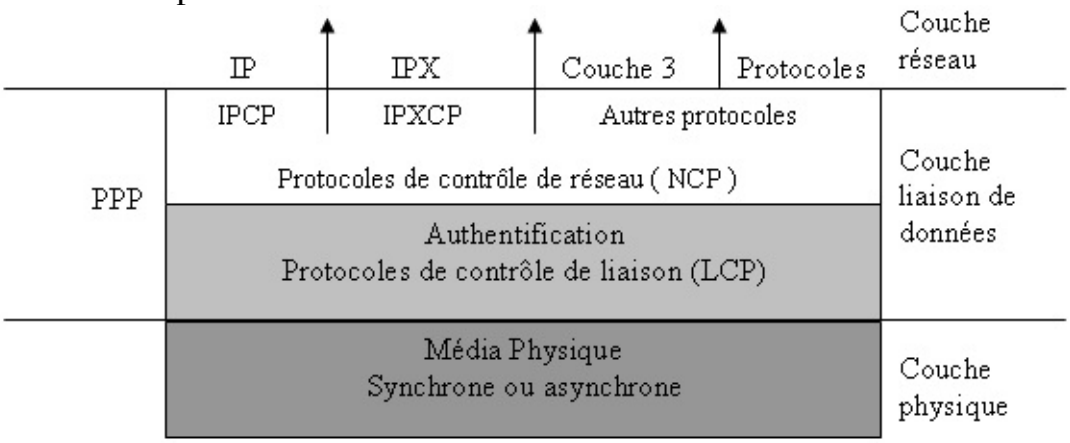


Figure 2

Architecture PPP

PPP offre un riche ensemble de services qui contrôle l'établissement d'une liaison de données. Ces services sont des options dans LCP et sont principalement des trames de négociation et de vérification pour implémenter les contrôles point à point qu'un administrateur définit pou l'appel.

Avec ses fonctions de niveaux supérieurs, PPP transporte dans NCP des paquets de plusieurs protocoles de couche réseau. Il s'agit de champs fonctionnels contenant des codes standardisés pour indiquer le type de protocole de couche réseau que PPP encapsule.

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. o Trame LCP d'établissement de liaison.
o Trame LCP de fermeture de liaison.
o Trame LCP de maintenance de liaison.
Une famille de protocoles NCP (Network Control Protocol) : Gestion des protocoles de couche 3.
o IPCP (Internet Protocol Control Protocol).
o IPXCP (Internetwork Packet eXchange Control Protocol).
o 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.

OPTION DE CONFIGURATION DE PPP LCP

Le RFC 1548 décrit l'exploitation de PPP et des options de configuration de LCP. Il a été mis à jour par le RFC 1570 " *PPP LCP Extensions* ".

Fonction Authentification
Compression
Détection d'erreur Multilink

Mode opératoire
Nécessite un mot de passe
Effectue la négociation par tests
Compresse les données sur la source ; Reproduit les données sur la destination Surveille les données supprimées sur la liaison Evite le bouclage de trame
Equilibrage de charge sur plusieurs Liaisons

Protocole PAP
CHAP
Stacker ou Predictor
Quality Magic Number
MultiLink Protocole (MP)

Les routeurs Cisco qui utilisent l'encapsulation PPP, incluent les options LCP décrit par le tableau ci-dessus.

Les options d'authentification nécessitent que le côté appelant de la liaison spécifie des informations qui permettent de vérifier que l'appelant a la permission de l'administrateur d'établir la connexion. Les routeurs homologues échangent des messages d'authentification.

Les deux solutions possibles sont :

PAP (*Password Authentication Protocol*, Protocole d'authentification de mot de passe),
CHAP (*Challenge Handshake Authentication Protocol*, Protocole d'authentification par tests).

Pour améliorer la sécurité, à partir de la version 11.1 du système Cisco IOS, une fonction de rappel sur PPP est disponible. Avec cette option LCP, un routeur Cisco peut agir comme client de rappel ou serveur de rappel.

Le client envoie la requête d'appel DDR initiale en demandant d'être rappelé et met fin à la connexion. Le serveur de rappel répond à la requête et appelle en retour le client en se basant sur ses instructions de configuration. Cette option est décrite dans le RFC 1570.

Les options de compression augmentent le débit effectif sur les connexions PPP en réduisant la quantité de données dans la trame qui doivent transiter sur la liaison.
Le protocole décompresse la trame sur sa destination.
Les deux protocoles de compression disponibles sur les routeurs Cisco sont Stacker et Predictor.
Les mécanismes de détection d'erreurs avec PPP permettent à un processus d'identifier les conditions de faute.

Les solutions Quality et Magic Number apportent une aide au maintien d'une liaison de

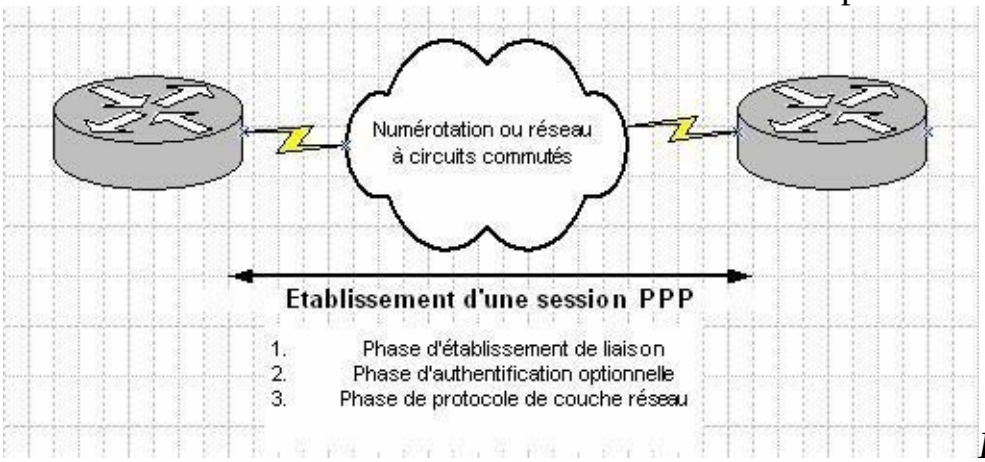
données exempte de boucles.
Depuis la version 11.1 de Cisco IOS, Multilink PPP est supporté. Cette solution apporte l'équilibrage de charge sur les interfaces du routeur que PPP utilise.

La fragmentation et le séquencement de paquets, comme spécifié dans le RFC 1717, scindent la charge de PPP et envoient des fragments sur des circuits parallèles. Dans certains cas, ce « faisceau » de tubes Multilink PPP fonctionne comme une seule liaison logique, améliorant le débit et réduisant la latence entre routeur homologues.

Le RFC 1990 , " *The PPP Multilink Protocol (MP)* " rend obsolète le RFC 1717.

ETABLISSEMENT D'UNE SESSION PPP

L'établissement d'une session PPP fait intervenir trois phases :



Phase1 : Etablissement de liaison

Dans cette phase, chaque équipement PPP envoie des paquets LCP pour configurer et tester la liaison de données. Les paquets LCP contiennent un champ d'option de configuration qui permet aux équipements de négocier l'utilisation d'options telles que l'unité maximale de réception, la compression de certains champs PPP et le protocole d'authentification de liaison. Si une option de configuration n'est pas incluse dans un paquet LCP, la valeur par défaut pour cette option sera utilisée.

Phase2 : Authentification optionnelle

Après que la liaison a été établie et que le protocole d'authentification a été choisi, le routeur homologue peut être authentifié. L'authentification, si elle est utilisée, a lieu avant d'entrer dans la phase de protocole de la couche réseau.

PPP supporte deux protocoles d'authentification, PAP, et CHAP. Ces deux protocoles sont détaillés dans le RFC 1334, " *PPP Authentication Protocols* ". Toutefois, le RFC 1994, " *PPP Challenge Handshake Authentication Protocol* " le rend obsolète.

Phase3 : Protocole de couche réseau

Dans cette phase, les équipements PPP envoient des paquets NCP pour choisir et configurer un ou plusieurs protocoles de la couche réseau (tel que IP). Après que chacun des protocoles choisis a été configuré, des datagrammes de chaque protocole peuvent être envoyés sur la liaison. PPP supporte plusieurs protocoles dont IP, IPX, AppleTalk, etc …

SELECTION D'UN PROTOCOLE D'AUTHENTIFICATION PPP

Lors de la configuration de l'authentification PPP, vous pouvez choisir entre les protocoles PAP ou CHAP. En général, ce dernier est le protocole préféré.

PAP :

PAP fournit une méthode simple pour qu'un nœud distant puisse décliner son identité au moyen d'une négociation en deux temps. L'authentification n'est réalisée qu'au moment de l'établissement de la liaison initiale.

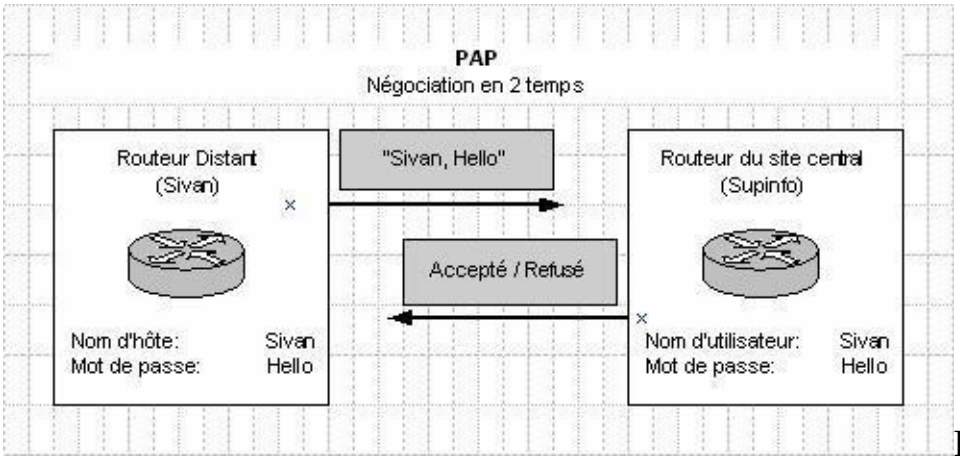


Figure 4

Après que la phase d'établissement de liaison PPP a été accompli, un ensemble nom d'utilisateur / mot de passe est envoyé de façon répétée pour le nœud distant vers le routeur jusqu'à ce que l'authentification soit acquittée ou que la connexion soit terminée.

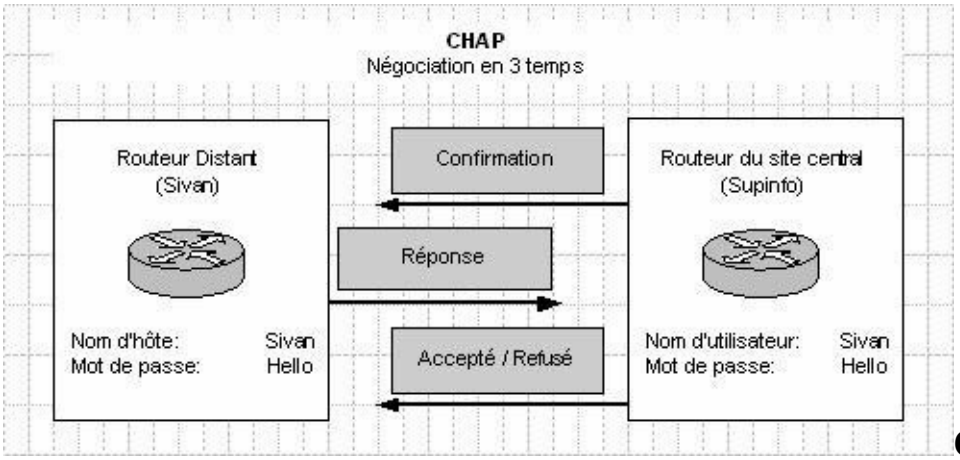
PAP n'est pas un protocole d'authentification puissant. Les mots de passe sont envoyés sur la liaison en texte clair et il n'existe aucune protection contre un risque d'attaques par copie ou itération de cycles tentative-échec. Une attaque par copie se produit lorsqu'un analyseur de trafic capture les paquets et les reproduit sur le réseau à partir d'un autre équipement. Le nœud distant est maître de la fréquence et de la synchronisation des tentatives de connexion.

CHAP :
CHAP est utilisé au démarrage d'une liaison et périodiquement pour vérifier l'identité d'un nœud distant au moyen d'une négociation en trois temps.

Après l'établissement de la liaison PPP, le routeur local envoie un message de test vers le nœud distant. Celui-ci répond avec un numéro d'identifiant crypté, un mot de passe secret et un nombre aléatoire. Le routeur local compare la valeur de réponse avec le résultat de ses propres calculs. Si les valeurs correspondent, l'authentification est acquittée ; autrement, la connexion est immédiatement terminée.

CHAP offre une protection contre les attaques par copie par l'intermédiaire d'une valeur de défi variable qui est unique et imprévisible. L'utilisation de tests répétés permet de limiter le temps d'exposition à une seule attaque. Le routeur local (ou serveur d'authentification) est maître de la fréquence et de la synchronisation des messages de test.

Pour afficher la séquence d'échanges au moment où elle se produit il faut utiliser la commande " **debug ppp authentication** "



CONFIGURATION DE L'AUTHENTIFICATION PPP

Les routeurs de chaque côté de la liaison doivent être configurés pour l'authentification PPP.

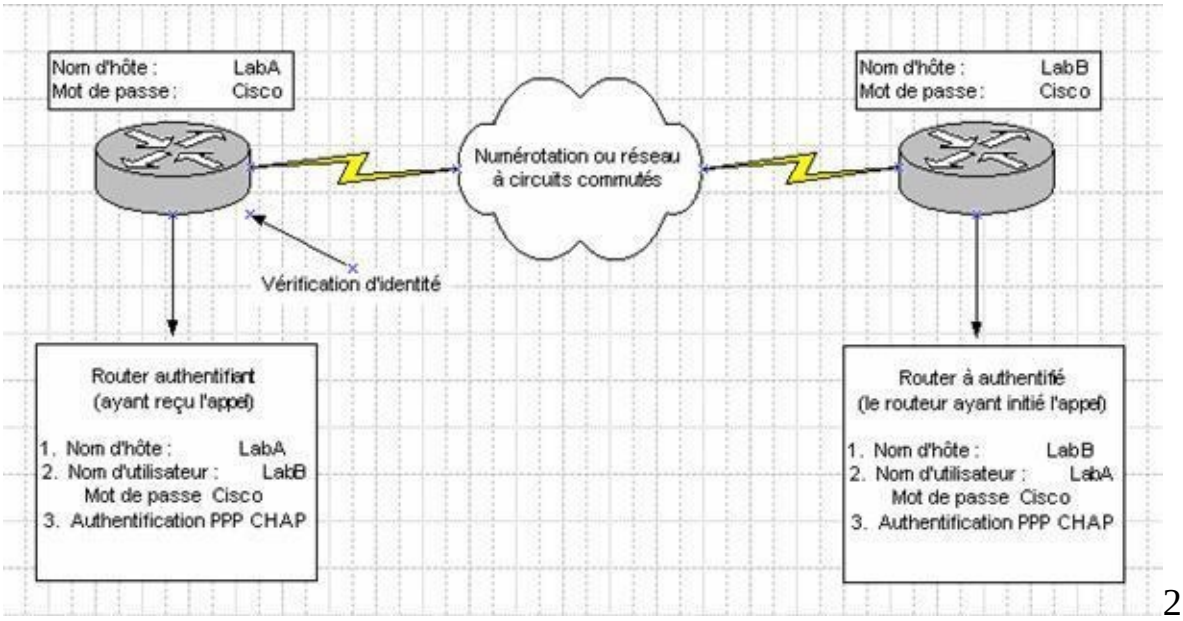
Pour configurer l'authentification PPP, il faut procéder comme suit :

1. Sur chaque routeur, il faut définir de nom d'utilisateur et le mot de passe attendus de la part du routeur distant. Voici la syntaxe de la commande :

*Router(config)# **username** nom **password** secret*

Les paramètres de la commande sont les suivants :

- Nom : c'est le nom d'hôte du routeur distant,
- Secret : Sur les routeurs Cisco, le mot de passe secret doit être le même pour les deux routeurs.



2. Il faut ensuite entrer en mode de configuration d'interface pour l'interface appropriée.

3. Il faut ensuite configurer l'interface pour l'encapsulation PPP.

Router (config)# encapsulation PPP

4. Puis configurer l'authentification PPP.

Router (config)# PPP authentication {CHAP | CHAP PAP | PAP CHAP}

Il existe quatre options disponibles pour l'authentification PPP :

Si PAP et CHAP sont tous les deux activés, la première méthode spécifiée sera demandée durant la négociation de liaison. Si l'homologue suggère l'emploi de la deuxième méthode ou refuse simplement la première, la deuxième méthode sera utilisée.

VERIFICATION PPP

Lorsque PPP est configuré, vous pouvez vérifier ses états LCP et NCP au moyen de la commande **show interfaces**

Frame Relay

Introduction

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.

Les réseaux Frame Relay sont multi accès, dans ce type de réseaux plusieurs équipements peuvent s'interconnecter et communiquer simultanément, de plus contrairement au LAN, les broadcast de couche liaison de données ne sont pas diffusés à travers un réseau Frame relay.

Les réseaux Frame Relay sont appelés Non-Broadcast Multiaccess (NBMA).

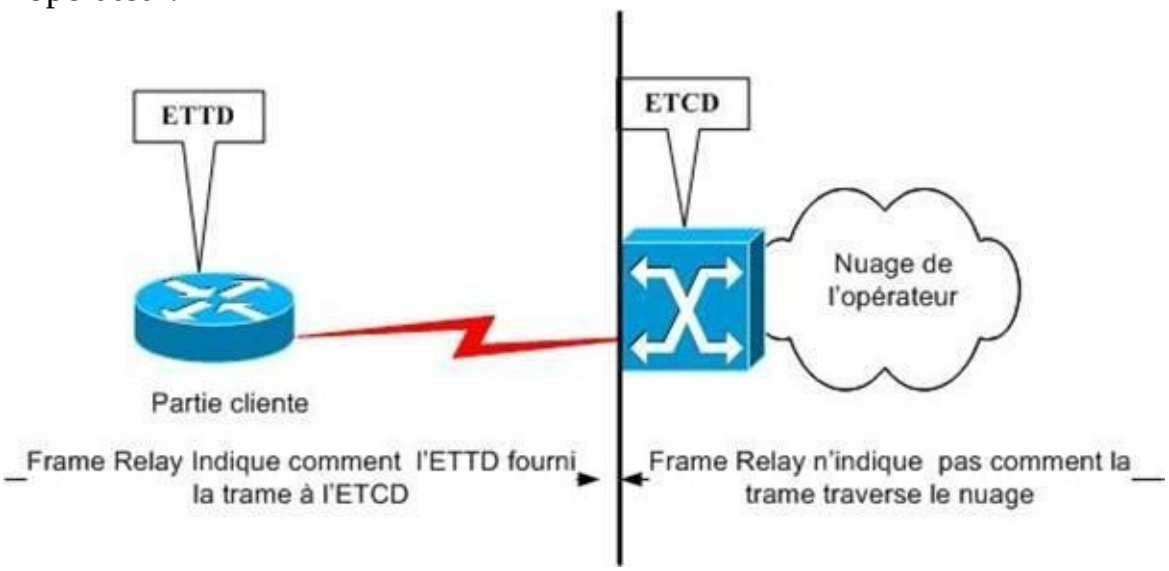
1. Présentation de Frame Relay

1.1- Les équipements d'un réseau Frame Relay

Frame Relay se charge de transporter les données entre l'ETTD (DTE : Equipement Terminal de Traitement des Données) et L'ETCD (DCE : Equipement Terminal de Circuit des Données);

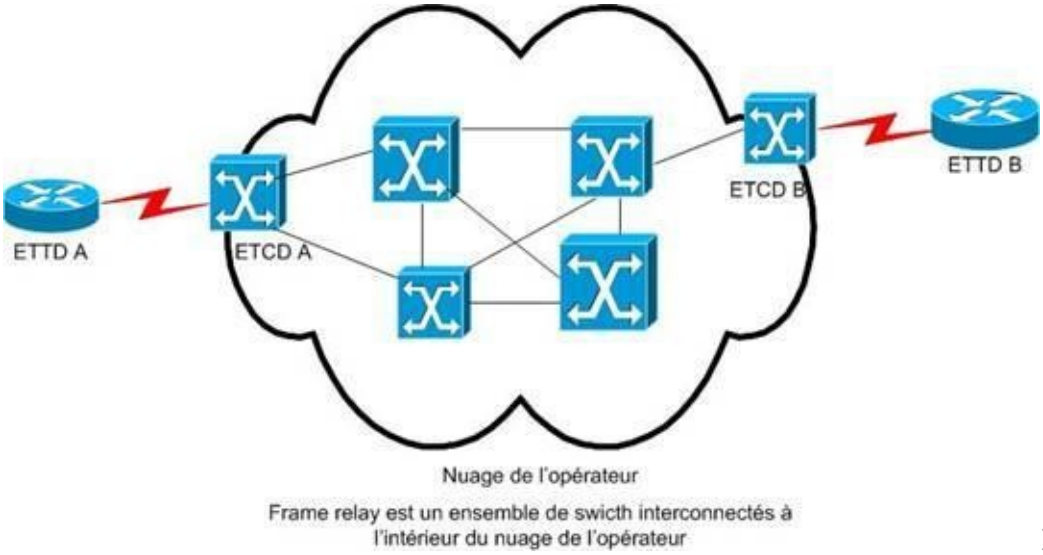
L'ETTD correspond à la partie « client » de la communication c'est lui qui fournit les données, c'est généralement un routeur. L'ETCD est la partie fournisseur c'est généralement un commutateur, il se charge de délivrer les données fournies par l'ETTD à l'opérateur.

Frame Relay ne se charge pas de spécifier comment les données traverse le nuage de l'opérateur.



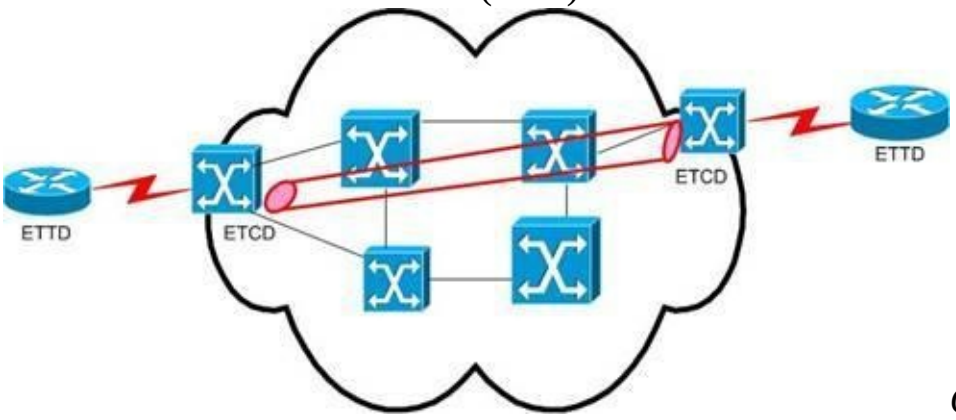
Il faut savoir q'un réseau Frame Relay correspond à un ensemble de switch interconnectés. Comme nous l'avons vu dans l'introduction, Frame Relay est souvent utilisé pour interconnecter des réseaux LAN.
Considérons par exemple un LAN A connecté au routeur A (ETTD A) et un LAN B connecté au routeur B (ETTD B); lorsque que l'ETTD A souhaite communiquer avec l'ETTD B la communication se passe de la façon suivante :

1. L'ETTD A envoie la trame à l'ETCD A.
2. La trame est transmise à l'intérieur du nuage et passe de switch en switch jusqu'à ce qu'elle arrive à L'ETCD B.
3. L'ETCD B transmet la trame à l'ETTD B.



1.2. Les circuits virtuels

Frame Relay relie deux DTE ou plus via une connexion appelée circuits virtuels. Les circuits virtuels permettent une connexion point à point et point à multipoint.
Les circuits virtuels permettent d'avoir une connectivité vers chaque destination à partir d'une connexion physique. Il existe deux types de circuits virtuels :
les circuits virtuels permanents (PVC)
les circuits virtuels commutés (SVC)



Circuit virtuel au travers d'un réseau commuté

1.2.1. Les SVC (Switched Virtual Circuit)

Les SVC sont dynamiquement établis à la demande par l'envoi de messages de signalisation dans le réseau et sont supprimés lorsque la transmission est terminée.
Les SVC ne sont pas très utilisés, les PVC sont préférés.

1.2.2. Les PVC (Permanent Virtual Circuit)

Un PVC est un circuit virtuel établi de manière permanente. Les PVC sont plus utilisés, ils économisent de la bande passante associée à l'établissement du circuit et à son arrêt.

1.2.3 Bande passante et congestion dans un réseau Frame Relay

Généralement il existe plusieurs VC qui opèrent sur la ligne dédiée, les circuits virtuels partagent la bande passante et chaque VC à un débit garanti pour l'acheminement des données appelé **CIR (Commited Information Rate)**. Lorsque des trames arrivent dans un switch elles sont stockées dans un tampon en attendant d'être commutées. Si le réseau est congestionné le commutateur place dans le champ adresse de la trame un bit **ECN (Explicit Congestion notification)** afin de réduire le flux de trame jusqu'à ce le la congestion soit terminée.

Il existe 2 types de bit ECN :
FECN (Forward Explicit Congestion Notification) : le bit ECN est placé sur une trame qui se dirige vers l'équipement de destination, pour indiquer l'origine de la congestion.

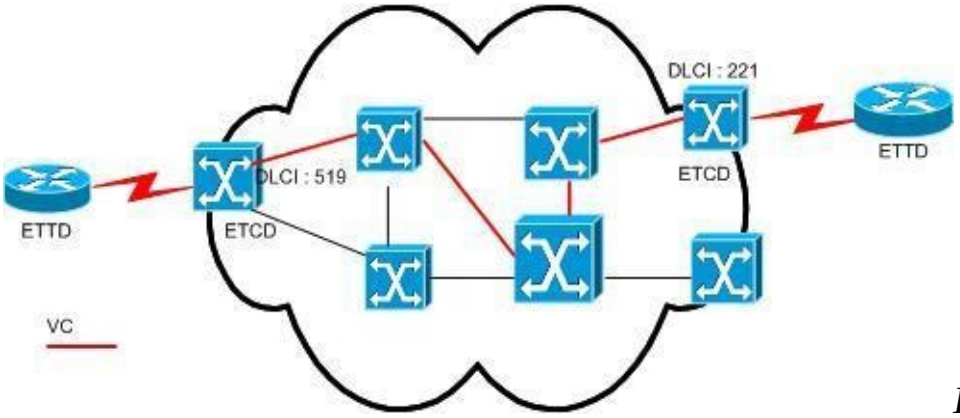
BECN (Backward Explicit Congestion Notification) : le bit ECN est placé sur une trame qui se dirige vers l'équipement source, afin de lui demander de réduire son débit d'envoi pour ne pas aggraver la congestion.

1.3. L'adressage Frame Relay

1.3.1. Les DLCI

Pour pouvoir distinguer chaque circuit virtuel entre le routeur (ETTD) et le commutateur Frame Relay (ETCD) un identifiant est attribué à chaque VC appelé **DLCI** (Data Link Channel Identifier).

Les DLCI ont une portée locale puisque l'identifiant renvoie au point situé entre le routeur local et le commutateur auquel il est connecté. Les équipements placés à la fin de la connexion peuvent identifier un même circuit virtuel par un DLCI différent.



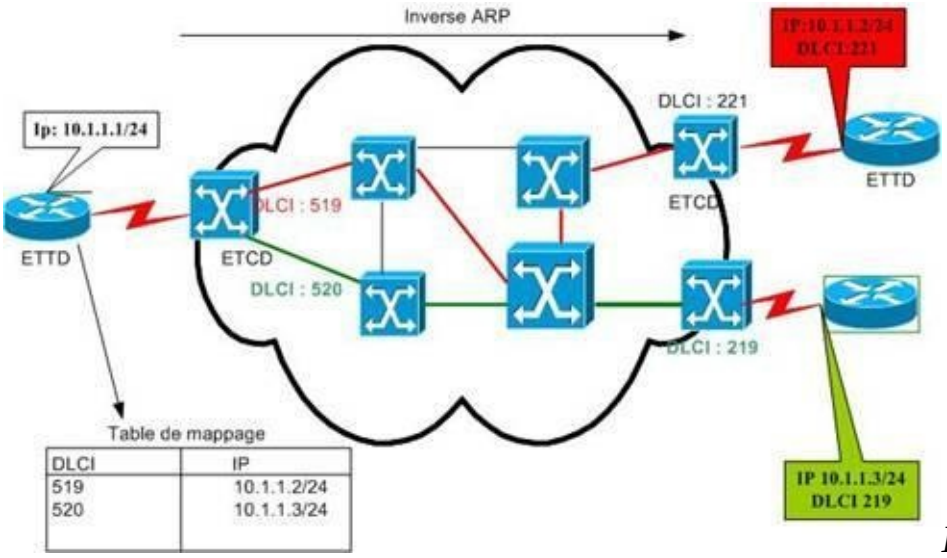
Les DLCI identifient le Circuit virtuel en rouge

1.3.2. Le mappage des adresses

Comme nous l'avons vu précédemment les circuits virtuels permettent à un même équipement d'être connecté via une seule interface physique à plusieurs équipements distants.

Chaque VC est identifié par un DLCI, or les routeurs basent leur décision d'acheminement de paquets sur une adresse IP. Pour connaître l'adresse IP de chaque VC il faut faire un mappage entre le DLCI d'un VC et son adresse IP.
Les adresses sont mappées dynamiquement avec Inverse ARP qui associe un DLCI donné à l'adresse logique du prochain saut pour une connexion spécifique. Le routeur constitue

une table de mappage qu'il met à jour; c'est sur cette table que le routeur base ces décisions de routage.



Le mappage dynamique des adresses avec Inverse ARP

Lorsque l'inverse ARP n'est pas supporté, l'administrateur à la possibilité de configurer un mappage statique entre les DLCI et l'adresse IP. Nous verrons ceci dans la partie 2.2.

1.3.3. La signalisation LMI

La signalisation LMI (Local Management Interface) est un standard qui gère la connexion et le maintien du statut entre l'ETTD et l'ETCD. Il existe trois types de LMI .
Le tableau suivant les présentes:

LMI Standard Lmi-type sur le routeur cisco Cisco cisco
ansi Ansi T1.617 ansi
ietf ITU-T Q933 a

LMI informe sur l'état des VC grâce à des " message status". Les VC peuvent avoir trois états: **Etat actif** (active state) indique que la connexion est active et que les équipements peuvent échanger des données.
Etat inactif (inactive state) indique que la connexion locale au commutateur frame relay fonctionne mais que la connexion du routeur distant au commutateur Frame-Relay ne fonctionne pas.
Etat supprimé (deleted) state indique qu'aucun LMI n'est reçu du commutateur Frame Relay

La signalisation LMI fournit aussi une fonction de maintien en vie (Keepalive), si une liaison entre le retour et l'ETCD à un problème, l'absence de keepalive signifie que le lien est "mort".
Le format des trames Frame Relay est le suivant :

Drapeau : Indique le début et la fin de la trame.

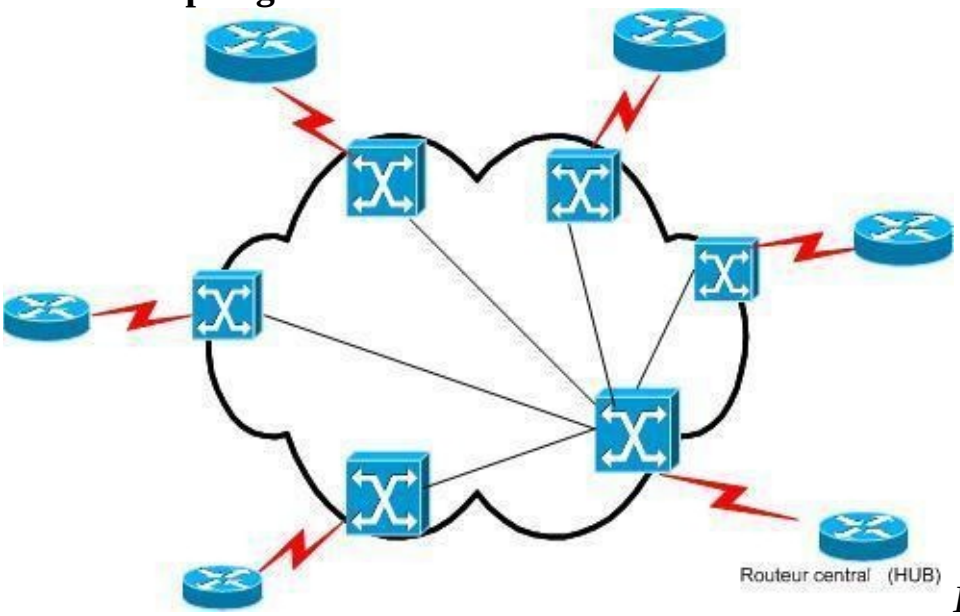
Adresse : Contient l'adresse d'extrémité (10 premiers bits), ainsi que les mécanismes de notification de congestion (3 derniers bits).
DLCI.
FECN.
BECN.

Bit d’éligibilité à la suppression.

Données : Informations encapsulées de couche supérieure.
FCS : Séquence de contrôle de trame.

1.4- Les topologies Frame Relay

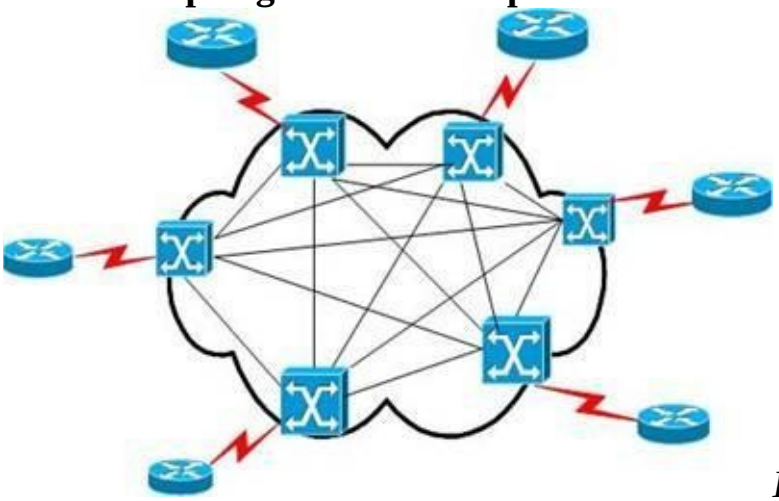
1.4.1. La topologie en étoile



La topologie en étoile (Hub and spoke) frame Relay

La topologie en étoile encore appelée Hub and spoke est configurée de manière à ce que les sites distants soient reliés à un site central. Le site central fourni une connexion multipoint car il y a autant de PVC que de sites distants tandis que les sites distants ont un seul PVC vers le site central la connexion est donc point à point ; Il s’agit de la topologie la plus répandue dans l’architecture WAN car est la moins onéreuse, le nombre de PVC nécessaires est réduit, donc un coût moindre pour la ligne louée.
Le coût n’étant pas lié à la distance, le routeur central n’a pas besoin d’être situé au centre de la topologie géographiquement.

1.4.2. La topologie maillée complète

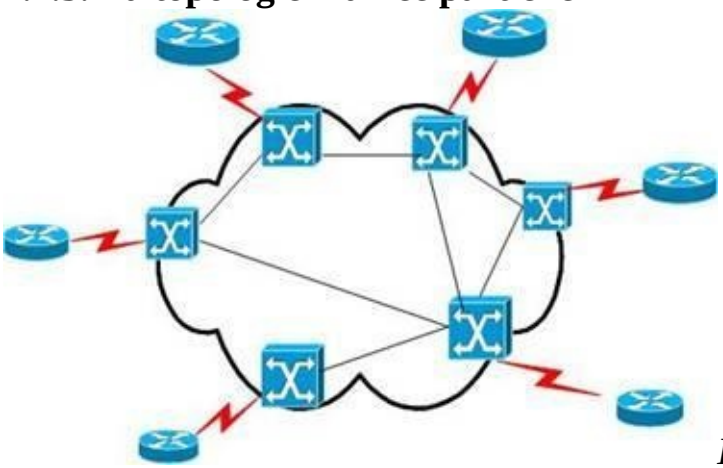


La topologie maillée complète

La topologie maillée est utilisée lorsque les sites distants sont très dispersés et une qu’une fiabilité maximum est requise. Chaque site dispose d’un circuit virtuel pour chaque destination. Dans cette topologie si un réseau WAN dispose de 6 sites distants chaque DTE doit avoir 5 circuits virtuels.

Cette topologie est très onéreuse en cas de croissance les coûts augmenteront vite. Toutefois ce type de topologie a l'avantage de fournir des chemins redondants en cas de défaillance d'une liaison.

1.4.3. La topologie maillée partielle



La topologie maillée partielle

Dans la topologie maillée partielle, tous les sites ne disposent pas de VC pour toutes les destinations. Dans cette topologie il y a plus d'interconnexion qu'une topologie étoile et moins qu'une topologie maillée complète. Ce type de topologie est utilisé pour les très grands réseaux. Il faut savoir qu'au maximum 1000 VC peuvent être créés à partir d'une liaison physique.

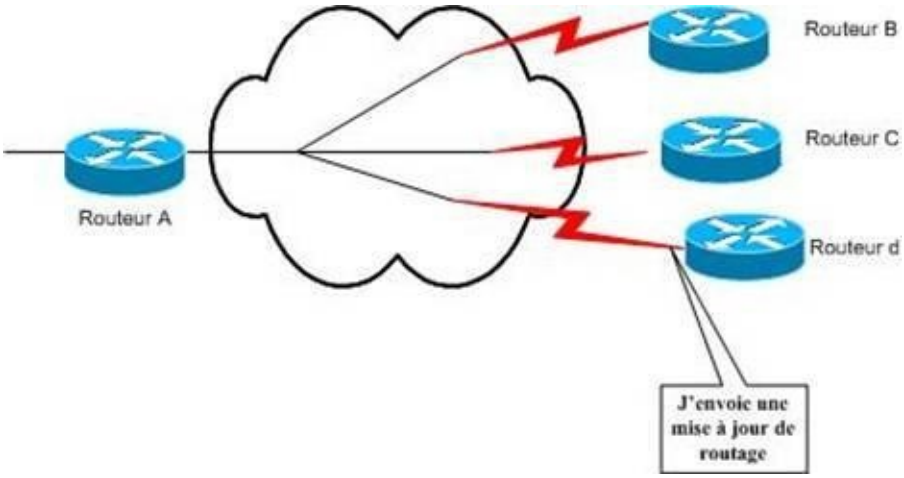
1.5. L'accessibilité dans un réseau NBMA

Frame Relay est une technologie Non broadcast Multiacccess. Dans ce type de réseau une même interface est connectée à plusieurs sites grâce à l'utilisation de circuits virtuels c'est l'aspect « Multiaccès ». De plus les diffusions générales ne sont pas susceptibles d'être transmises aux sites distants, c'est l'aspect «non broadcast ». Les réseaux NBMA sont sources de 2 problèmes :

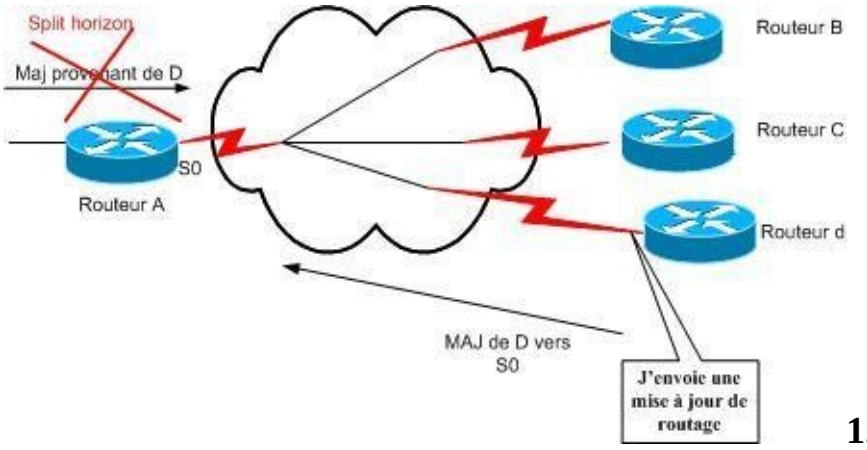
La non diffusion des mises à jour de routage à cause du Split horizon
La réplication des mises à jour sur chaque PVC.

1.5.1 La non diffusion des mises à jour de routage à cause du Split horizon

Les Réseaux NBMA sont sources de problèmes dans un réseau en étoile, plusieurs PVC sont connectés une seule interface physique du routeur central. Lorsqu'une mise à jour est diffusée par un routeur connecté à l'interface centrale les autres routeurs connectés à cette même interface risquent de ne pas recevoir cette mise à jour.
Pour mieux comprendre utilisons un exemple, le routeur D envoie une mise à jour de routage à l'interface S0 du routeur A



Le routeur A ne pourra pas transmettre la mise à jour de routage aux routeurs C et D à cause du mécanisme de Split Horizon utilisé par le routeur Frame Relay pour empêcher la formation de boucle de routage. Le Split horizon empêche à un paquet d'être renvoyé à l'interface d'origine de ce même paquet dans notre exemple les routeurs C et D se trouvent sur l'interface S0.



1.5.2 La réplication des mises à jour sur chaque PVC.

Le second problème lié aux routeurs qui supportent plusieurs VC sur une seule interface physique est que les routeurs doivent répliquer les paquets de broadcast sur chaque VC pour qu'ils soient reçus par les sites distants. La réplication consomme beaucoup de bande passante et provoque de la latence.

1.5.3 Une solution pour résoudre les problèmes des réseaux NBMA

Nous l'avons vu Split horizon est une des problématiques des réseaux NBMA, il est donc logique de penser qu'il suffit de désactiver ce mécanisme pour résoudre le problème mais premièrement certains protocoles réseaux ne permettent pas sa désactivation et de plus désactiver split horizon entraînerait une augmentation des boucles de routage.

Une des solutions plus efficace pour résoudre le problème serait de configurer des sous interfaces logiques, Split horizon n'empêche pas des mises à jour de routage provenant d'une sous- interface d'être renvoyé à une autre sous interface.

Les sous interfaces sont des subdivisions logiques d'une interface physique.
Les sous interfaces sont de deux 2 types :

Point à point : Les sous interfaces point-à-point une seule sous interface sert à établir un PVC vers une autre interface ou sous-interface sur un routeur distant. Dans ce cas les deux

sous interfaces doivent être dans le même sous-réseau, de plus chaque sous interface à un DLCI unique. Les sous-interfaces point à point permettent de résoudre le problème de Split horizon.

Multipoints: Une sous interface est connectée à plusieurs sous interfaces sur des routeurs distants. Dans ce cas toutes les interfaces participantes doivent être dans le même sous réseau. Malheureusement ce type d'interface fonctionne comme les réseaux NBMA et le problème de split horizon est le même, une solution existe transformé les liaisons multipoint en liaison point à point, je vous invite à lire l'article intitulé **Split horizon sur frame relay** présent sur le site du laboratoire (www.labo-cisco.com) pour avoir plus d'informations.

Nous verrons dans la partie 2.3 comment configurer les sous interfaces.

2. Configuration de Frame Relay

2.1. Etapes de la configuration de base de Frame Relay

La configuration de Frame Relay est simple, elle suit les étapes suivantes :

· **Définir l'encapsulation**

Par défaut l'encapsulation sur les routeurs Cisco est HDLC ;
L'encapsulation Frame Relay est définie avec la commande :
- - > **routeur(config-if)#Encapsulation frame relay [ietf|cisco]**
La commande est à entrer au mode de configuration d'interface
Le paramètre Cisco (par défaut) est utilisé entre deux routeurs Cisco
Le paramètre ietf est utilisé entre un routeur Cisco et un routeur d'une autre marque.

· **Définir la signalisation Lmi :**

Cette commande n'est plus nécessaire à partir de la version d'IOS 11.2 car le lmi type est automatiquement géré (autosense)
- - > routeur(config-if)# Frame-relay lmi-type [ansi | cisco | q933a]
Par défaut le LMI type est cisco; La commande est à entrer au mode de configuration d'interface.

· **Définir la bande passante**

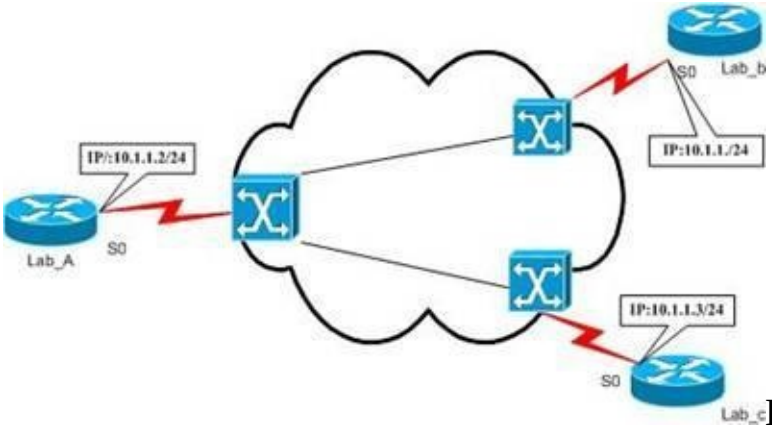
La bande passante est utilisée par certains protocoles de routage comme métrique (IGRP, EIGRP).Il est donc nécessaire de la configurer et non garder les paramètres par défaut.
La commande à utiliser est :
- - > **routeur(config-if)# bandwith *valeur***
La commande est à entrer au mode de configuration d'interface.
La valeur de la bande passante est exprimée en kbps.

· **Activer Inverse Arp**

Par défaut inverse Arp est activé sur les routeurs cisco. Toutefois la commande pour activer/désactiver Inverse ARP est la suivante :
La commande est à entrer au mode de configuration d'interface.
- -> **routeur(config-if)# [No] frame-relay inverse Arp**

Exemples de configuration de Frame Relay

Pour mieux illustrer la configuration nous allons prendre des exemples,
Example1:



La figure suivante montre la configuration de Frame Relay sur Lab_A :
La version d'IOS du routeur Lab_A est 12.2 :

```
interface Serial0/0
 bandwidth 64
 ip address 10.1.1.2 255.255.255.0
 encapsulation frame-relay
```

Lab_B a une version antérieure à la 11.2 et les valeurs par défaut ne sont pas utilisées:

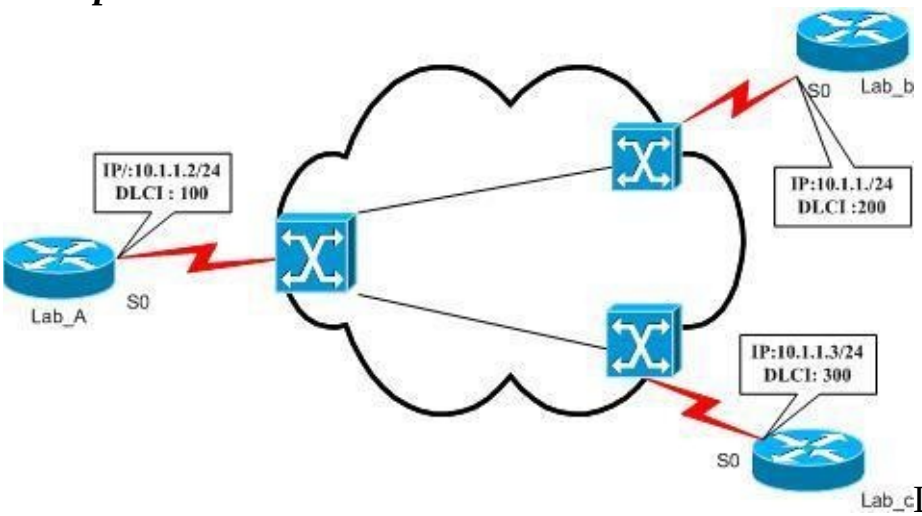
2.2. Configurer le mappage statique

Pour configurer le mappage statique il faut utiliser au mode de configuration des interfaces la commande :

— > Routeur(config)# frame-relay map *protocole prochain saut dlci* **[broadcast]**

Protocole : identifie le protocole supporté (ip, ipx…).
Prochain saut : Correspond à l'adresse du prochain saut
dlci : Correspond au DLCI
Broadcast : option qui autorise les broadcast sur le VC.

Exemple2:



Le mappage statique est configuré lorsque l'inverse ARP n'est pas supporté ou désactivé.

```
Lab_A(config-if)#no frame-relay inverse-arp
Lab_A(config-if)#frame-relay map ip 10.1.1.1 200 broadcast
Lab_A(config-if)#frame-relay map ip 10.1.1.3 300 broadcast
```

2.3. Configuration des sous-interfaces

La topologie suivante comporte des liaisons point à points et multipoints. Pour créer une sous interface il faut être dans le mode de configuration de l'interface et taper la commande suivante :

— > routeur(config)# Interface {numéro.sous-interface} [point-to-point|multipoint]
Il faut configurer l'adresse IP de la sous interface
— > routeur(config)# Ip address {adresse_ip}{masque de sous-réseau}
Ensuite il faut faire correspondre la sous interface à un DLCI en tapant la commande :
— > routeur(config)# Frame-relay interfaces-dlci {dlci} [ietf|cisco]
Au niveau de l'interface physique il ne faut pas configurer d'adresse IP par contre il faut activer l'encapsulation Frame Relay.
Pour mieux comprendre nous allons monter comment configurer les sous interfaces du routeur du Lab_A (Gamme Cisco 2600).
Le tableau suivant contient les informations nécessaires pour la configuration :

Routeur Sous interface Sous réseau Adresse IP Type de la sous interface Lab_A 0.1 10.1.1.0/24 10.1.1.1 Point à point Lab_A 0.2 10.1.2.0/24 10.1.2.1 Multipoint Lab_A 0.3 10.1. 2.0/24 10.1.2.2 Multipoint

Voici les commandes utilisées pour configurer les sous interfaces sur le routeur Lab_A :
1. Activation de l'encapsulation Frame Relay dans l'interface serial 0/0

```
Lab_A(config)#interface serial 0/0
Lab_A(config-if)#encapsulation frame-relay
```

2. Configuration de l'interface 0/0.1
3. Configuration de l'interface 0/0.2

```
Lab_A(config-if)#interface serial 0/0.2 multipoint
Lab_A(config-subif)#ip address 10.1.2.1 255.255.255.0
Lab_A(config-subif)#frame-relay interface-dlci 300
```

4. Configuration de l'interface 0/0.3

```
Lab_A(config)#interface serial 0/0.3 multipoint
Lab_A(config-subif)#ip address 10.1.2.2 255.255.255.0
Lab_A(config-subif)#frame-relay interface-dlci 400
Lab_A(config-fr-dlci)#_
```

3.

Inconvénients de Frame Relay
Cette technologie comporte quelques inconvénients, dont :

- Capacité de vérification des erreurs et fiabilité minime (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.

RNIS

1. TECHNOLOGIE

Il existe deux types de services RNIS :

BRI : Accès de base.
○ Aussi appelé canal 2B+D.
○ 2 canaux B à 64 Kbps/s (8 bits).
○ 1 canal D à 16 Kbps/s (2 bits).
○ Débit binaire de 192 Kbps/s (8000 trames de 24 bits). ○ Débit réel de 144 Kbps/s (2 canaux B + 1 canal D).

PRI : Accès primaire (Fonctionnant sur des lignes dédiées). ○ **T1** (Débit de 1.544 Mbps/s) :
23 canaux B à 64 Kbps/s (8 bits).
1 canal D à 64 Kbps/s (8 bits).
1 bit de verrouillage de trame.
8000 trames par seconde.

○ **E1** (Débit de 2.048 Mbps/s) :
30 canaux B à 64 Kbps/s (8 bits).
1 canal D à 64 Kbps/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 multiliaison 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.

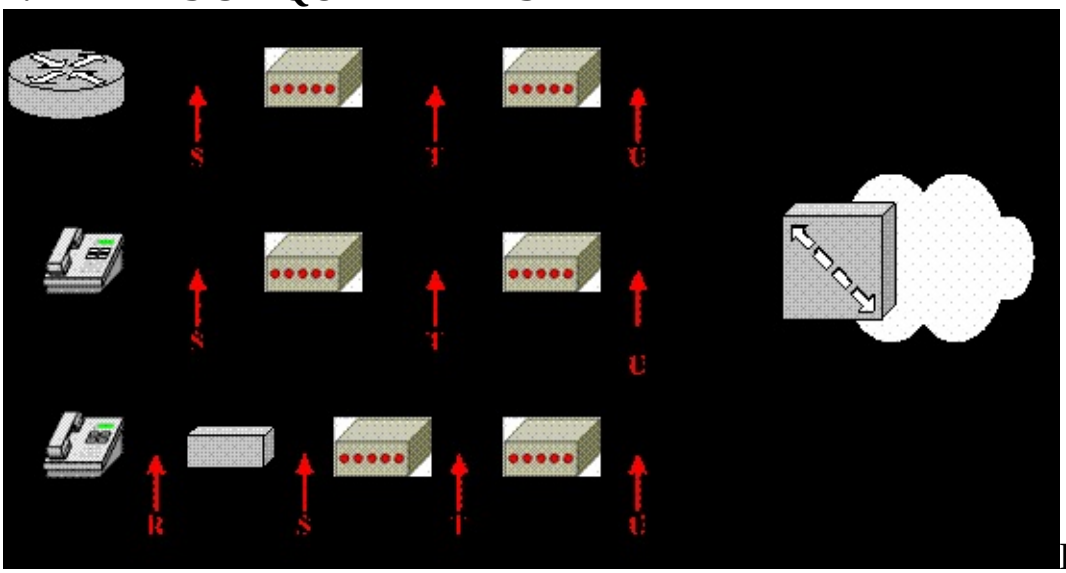
Le protocole LAPD (Couche 2) est utilisé sur le canal D et permet une circulation et une réception adéquate des flux d'information de contrôle et de signalisation. Ce protocole est similaire à HDLC et à LAPB (X.25).

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.

2. TERMES & EQUIPEMENTS



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

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 définit.

Les différents protocoles définit 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.

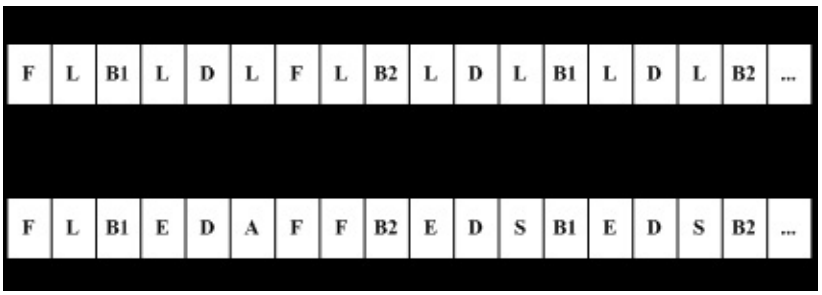
Couche liaison de données :
- **Q.920 à Q.923** : Spécification fondée sur LAPD.

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).

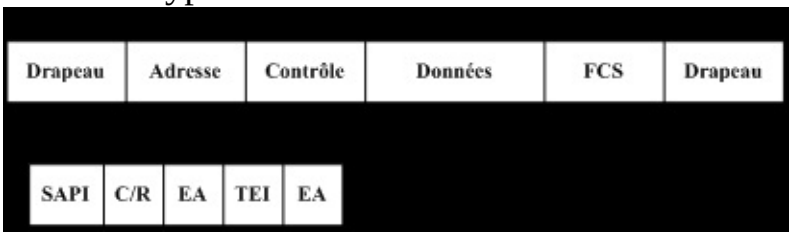
Il existe deux formats de trames pour le RNIS :
Trame TE : Trame sortante (Terminal au réseau). **Trame NT** : Trame entrante (Réseau au terminal).

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) :



A : Bit d'activation (Activation d'unités).
B1 : Bits de canal B1.
B2 : Bits de canal B2.
D : Bit de canal D.
E : Echo du bit D précédent (Résolution de conflits pouvant survenir lorsque plusieurs terminaux sur un bus passif rivalisent pour un canal).
F : Bit de verrouillage de trame (Synchronisation).
L : Bit d'équilibrage de charge (Ajustement de la valeur moyenne de bit). **S** : Bit de réserve (Non affecté).

Ces deux types de trame sont sous la forme d'une trame LAPD générique :

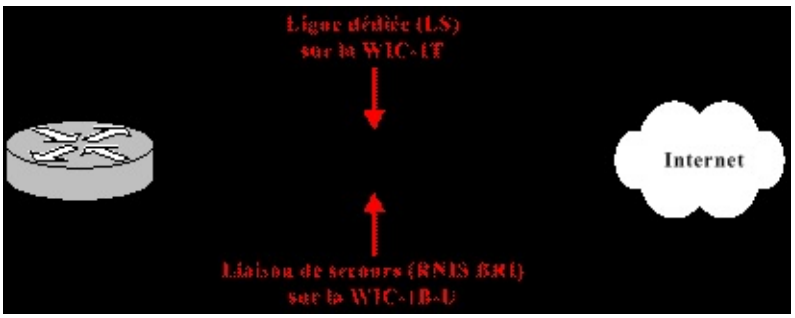


Drapeau : Similaire au champ HDLC.
Adresse : Peut comporter 1 ou 2 octets (Dépend de la valeur des bits EA). ○ **SAPI** : Bits d'identification du point d'accès (6 bits). Indique le portail où les services LAPD sont fournis à la couche 3.
○ **C/R** : Bit de commande/réponse.
○ **EA** : Bit d'adressage étendu. Si le premier EA est définit, alors l'adresse comporte 1 octet, sinon elle en comporte 2.

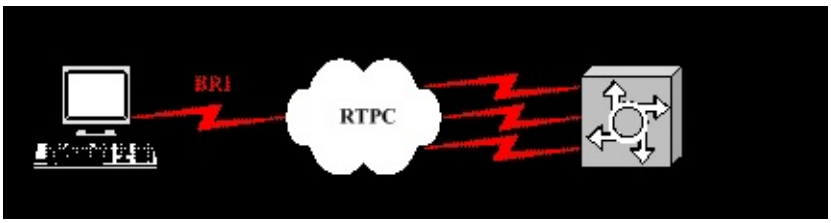
○ **TEI** : Identificateur de point d'extrémité de terminal. Ce champ précise le nombre de terminaux, ou s'il s'agit d'un broadcast.
Contrôle : Similaire au champ HDLC.
Données : Données fournies par l'intermédiaire des canaux B.
FCS : Séquence de contrôle de trame (Contrôle d'erreurs).

4. UTILISATION / IMPLEMENTATION
La technologie RNIS a de nombreuses applications :

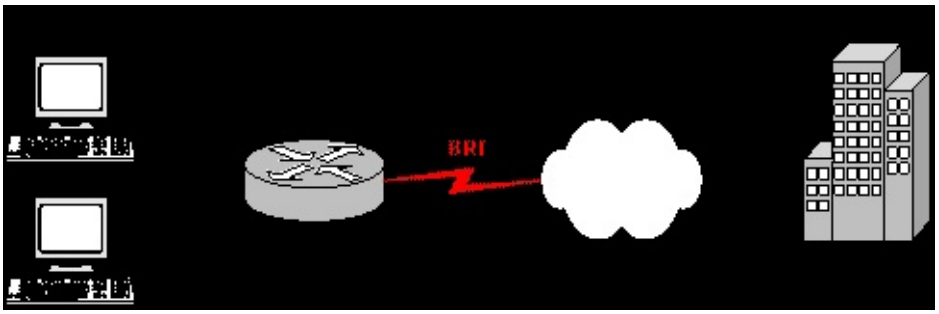
Solution alternative aux lignes dédiées.
Accès à distance :
o Nœuds distants.
o Connectivité des petits bureaux et bureaux à domicile (SOHO – Small Office / Home Office).



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).

5. ROUTAGE A ETABLISSEMENT DE CONNEXION A 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. COMMANDES IOS

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

o Le paramètre (Allemagne), (Angleterre et

interface bri {numéro} :
o Mode de configuration globale.
o Permet de passer dans le mode de con figuration d'une interface BRI.

interface dialer {numéro} :
o Mode de configuration globale.
o Permet de passer dans le mode de configuration d'une interface de connexion à la

demande.
isdn switch-type {isdn_swith_type} :
o Mode de configuration globale.
o Permet de spécifier le type de commutateur RNIS sur lequel on est raccordé.

isdn_switch_type peut prendre les valeurs **basic-1tr6**
basic-5ess (USA), **basic-dms100** (Angleterre), **basic-net3**
Europe), **basic-ni**, **basic-qsig**, **basic-ts013** (Australie), **ntt** (Japon), **vn3** (France).

isdn spid1 {valeur_spid_1} :
o Mode de configuration d'interface BRI.
o Configure le SPID pour le canal B1.

isdn spid2 {valeur_spid_2} :
o Mode de configuration d'interface BRI.
o Configure le SPID pour le canal B2.

dialer-list {numéro_groupe} protocol {proto} {permit | deny | list {numéro_acl}} :
o Mode de configuration globale.
o Cette commande permet de définir le trafic intéressant pour le DDR. o Le paramètre **numéro_groupe** indique le groupe pour lequel on attribut le trafic

intéressant.
o **proto** permet de spécifier le protocole de couche 3 dont fera partie le trafic intéressant.
o Le dernier paramètre permet de rentre 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} :
o Mode de configuration d'interface BRI ou Dialer.
o Permet d'affecter un trafic intéressant spécifique (**dialer-list** correspondant) sur l'interface actuelle.

dialer pool {numéro} :
o Mode de configuration d'interface Dialer.
o Permet le regroupement d'interfaces Dialer sur une interface BRI spécifique (**dialer pool-member**).

dialer pool-member {numéro} :
o Mode de configuration d'interface BRI.
o Permet de spécifier l'interface BRI qui sera la source des interfaces Dialer (**dialer pool**).

dialer string {numéro} :
o Mode de configuration d'interface Dialer.
o Permet de configurer le numéro de téléphone de la destination à appeler. **dialer wait-for-carrier-time {temps}** :
o Mode de configuration d'interface BRI ou Dialer.
o Configuration du temps pendant lequel le routeur attendra le signal de porteuse. **dialer idle-timeout {temps}** :
o Mode de configuration d'interface BRI ou Dialer.
o Configuration du temps de déconnexion après inactivité.

dialer remote-name {nom_distant} :
o Mode de configuration d'interface Dialer.

o Permet de spécifier le nom d'hôte du nœud distant.

dialer in-band :

o Mode de configuration d'interface BRI ou Dialer.

o Indique que l'on va faire passer le flux de signalisation dans le canal de données **dialer map {protocole} {adresse} name {nom} {numéro}** :

o Mode de configuration d'interface BRI ou Dialer.

o Précise le numéro de téléphone à appeler pour atteindre l'adresse de destination indiquée.

o Ne pas utiliser cette commande avec la commande **dialer string** en même temps.

dialer load-threshold {charge} [inbound | outbound | either] :

o Mode de configuration d'interface.

o 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**).

ppp multilink :

o Mode de configuration d'interface.

o 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 évènements 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.

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).

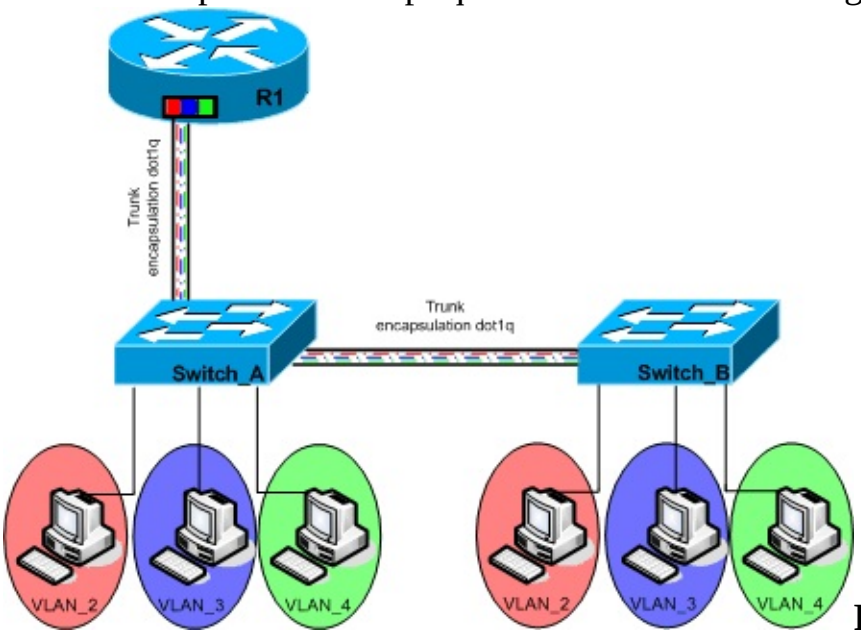
Configurer une ou plusieurs interfaces Dialer, en fonction des besoins :

- 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.

VLAN

Introduction

Cet article a pour but d'expliquer et d'établir une configuration de routage inter-VLAN.



Rappel sur les VLANs et le VTP:

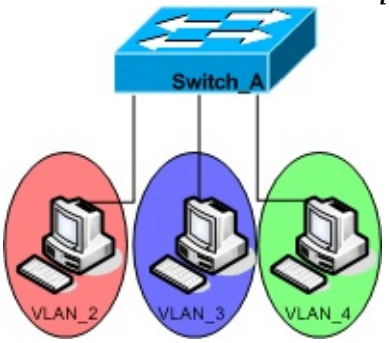
Un VLAN peut être assimilé à un domaine de broadcast. Typiquement, dans une configuration de VLAN, chaque VLAN comprend son propre sous-réseau. Sans équipement de couche 3, il est donc impossible pour les terminaux d'un VLAN de communiquer avec les terminaux d'un autre VLAN.

Le VLAN Trunking Protocol (VTP) est nécessaire si l'on veut étendre une configuration de VLAN sur plusieurs commutateurs. Pour cela, on crée un " trunk " entre les commutateurs. Ce trunk représente un canal par lequel transitent les trames des différents VLANs d'un commutateur à un autre. Pour que les commutateurs "sachent" à quel VLAN appartient une trame, un étiquetage est nécessaire. C'est pourquoi le VTP utilise deux protocoles d'étiquetage : ISL (Cisco) ou 802.1q (IEEE). Nous utiliserons ici le 802.1q qui est le protocole utilisé par défaut.

1. Configuration des VLANs

Dans notre cas on va utiliser des VLANs statiques, chaque port de chaque commutateur va donc être attribué à un VLAN.

N.B: Les accolades indiquent un paramètre obligatoire, les crochets une option.



1.1 Création des VLANs

Pour créer un VLAN, il faut se trouver dans le mode de configuration correspondant, accessible par la commande :

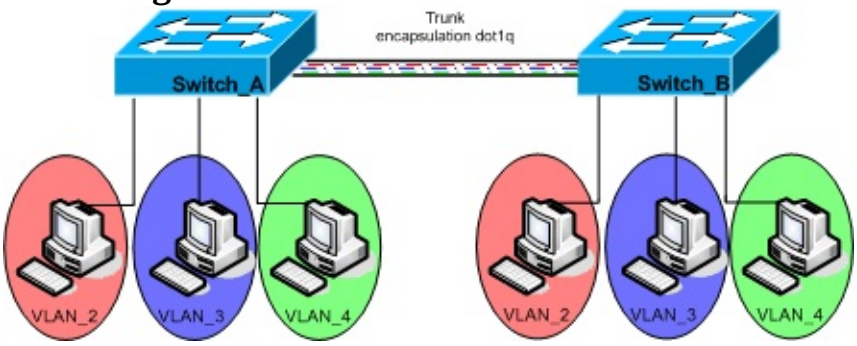
Switch_A# **vlan database**
A partir de ce mode, la création d'un VLAN se fait par la commande :
Switch_A(vlan)# **vlan {numéro} [name {nom}]** Switch_A(vlan)# **exit**

Cette dernière commande permet d'enregistrer la configuration des VLANs, qui se trouve dans le fichier vlan.dat dans la mémoire Flash.
Dans une configuration de VLAN statique, les ports du commutateur doivent être attribués à un VLAN. Ceci se fait dans le mode de configuration de l'interface spécifiée :

Switch_A(config)# **interface fastEthernet {numéro_interface}** *on passe dans le mode de configuration de l'interface spécifiée* Switch_A(config-if)#**switchport mode access** *spécification du mode de l'interface*
Switch_A(config-if)#**switchport access vlan {numéro}** *attribution du vlan spécifié à l'interface*

La configuration est maintenant faite sur le commutateur Switch_A.

1.2 Configuration d'un domaine VTP



Pour propager cette configuration à un deuxième commutateur, ceux-ci doivent appartenir à un domaine commun : le domaine VTP. Ce domaine est organisé hiérarchiquement : le serveur VTP diffuse ses configurations VLAN, tandis que le client VTP met à jour sa configuration VLAN en fonction des informations reçues du serveur.
Considérons le commutateur Switch_A comme le serveur du domaine VTP, et le commutateur Switch_B comme le client. Les commandes nécessaires sont :

Switch_A# **vlan database**
Switch_A(vlan)# **vtp domain {nom_domaine}**
Switch_A(vlan)# **vtp server**
Switch_A(vlan)# **exit**

Switch_B# **vlan database**
Switch_B(vlan)# **vtp domain {nom_domaine}**
Switch_B(vlan)# **vtp client**
Switch_B(vlan)# **exit**

Enfin, un trunk est nécessaire entre ces deux équipements. C'est en effet par celui-ci que les trames étiquetées transitent. Entre deux commutateurs, un câble croisé doit être utilisé.
Un trunk est une connexion physique regroupant plusieurs connexions logiques.
Dans le schéma, un câble physique laisse transiter 3 trafics logiques différents. Ceux-ci représentent les trafics propres à chaque VLAN.
L'encapsulation utilisée doit également être spécifiée, à moins que le commutateur utilisé n'accepte qu'un seul protocole. Chaque commutateur doit donc configurer une des ses

interfaces pour accueillir un trunk :

Switch_A(config)# **interface fastEthernet {numéro_interface}** Switch_A(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation {dot1q | isl}**

Switch_B(config)# **interface fastEthernet {numéro_interface}** Switch_B(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation {dot1q | isl}**

A ce stade, la configuration VLAN du commutateur serveur est transmise au client. Il faut cependant assigner les ports du commutateur client aux VLANs spécifiés (la configuration transmise énumère seulement les VLANs crées et leurs noms) :

Switch_B(config)# **interface fastEthernet {numéro_interface}** Switch_B(config-if)# **switchport mode access**
Switch_B(config-if)# **switchport access vlan {numéro}**

Désormais, chaque hôte peut communiquer avec un hôte du même VLAN, connecté sur un commutateur différent.

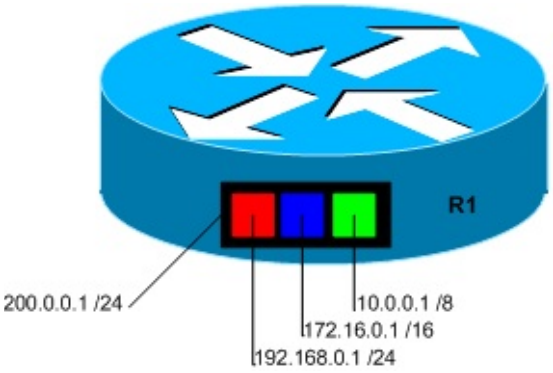
2. Configuration spécifique au routage inter VLAN

2.1 Sur le commutateur

Lorsque deux utilisateurs se trouvent sur des VLANS différents, ils se trouvent - en général - sur des sous-réseaux différents. Pour communiquer, ils doivent donc passer par une passerelle commune : l'interface du routeur connectée au commutateur. Pour spécifier au commutateur la passerelle utilisée pour "passer" d'un VLAN à un autre (ou plus généralement d'un sous-réseau à un autre), on utilise la commande :

Switch_A(config)# **ip default-gateway {adresse_ip}**

2.2 Sur le routeur La liaison routeur-commutateur constitue également un trunk. Cette connexion regroupe en effet plusieurs liens logiques : un trafic VLAN par sous-interface, sur une liaison physique : un câble droit connectant une interface du routeur à une interface d'un commutateur.



Chaque trafic de VLAN est supporté par une sous-interface du routeur. Il faut donc, pour chaque sous-interface, attribuer une adresse IP appartenant au sous-réseau du VLAN et spécifier l'encapsulation (étiquetage) utilisée:

R1(config)# **interface fastEthernet {sous-interface}**
R1(config-sub)# **encapsulation {dot1q | isl} {numéro_vlan}** R1(config-sub)# **ip address {adresse_ip} {masque_sous_réseau}**

L’interface doit également avoir une adresse IP afin de constituer la passerelle:
R1(config)# **interface fastEthernet {interface}**
R1(config-if)# **ip address {adresse_ip} {masque_sous_réseau}**

Chaque hôte peut désormais communiquer avec un hôte sur un VLAN différent. Lorsque le premier envoi une trame avec pour destination un sous-réseau différent du sous-réseau source, le commutateur l’encapsule et l’envoi à la passerelle par défaut. Après avoir traversé le trunk, la trame est traitée au niveau du routeur. Celui-ci la désencapsule, la réencapsule pour le VLAN de destination avant de l’envoyer sur la sous-interface correspondante.

3. Configuration complète

3.1 Configuration du switch_A

Création des VLANs
Switch_A# **vlan database**
Switch_A(vlan)# **vlan 2 name VLAN_2** Switch_A(vlan)# **vlan 3 name VLAN_3**
Switch_A(vlan)# **vlan 4 name VLAN_4** Switch_A(vlan)# **vtp domain cisco**
Switch_A(vlan)# **vtp server**
Switch_A(vlan)# **exit**

Création des trunk
Switch_A(config)# **interface fastEthernet 0/1**
Switch_A(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation dot1q** Switch_A(config-if)# **exit**

Switch_A(config)# **interface fastEthernet 0/8**
Switch_A(config-if)# **switchport mode trunk**
Switch_A(config-if)# **switchport trunk encapsulation dot1q** Switch_A(config-if)# **exit**

Attribution des VLANs aux ports
Switch_A(config)# **interface fastEthernet 0/2** Switch_A(config-if)# **switchport mode access** Switch_A(config-if)# **switchport access vlan 2** Switch_A(config-if)# **exit**
Switch_A(config)# **interface fastEthernet 0/3** Switch_A(config-if)# **switchport mode access** Switch_A(config-if)# **switchport access vlan 3** Switch_A(config-if)# **exit**
Switch_A(config)# **interface fastEthernet 0/4** Switch_A(config-if)# **switchport mode access** Switch_A(config-if)# **switchport access vlan 4** Switch_A(config-if)# **exit**

Définition de la passerelle par défaut Switch_A(config)# **ip default-gateway 200.0.0.1**

3.2 Configuration du switch_B Adhésion au domaine cisco

Switch_B# **vlan database**
Switch_B(vlan)# **vtp domain cisco** Switch_B(vlan)# **vtp client**
Switch_B(vlan)# **exit**

Création du trunk
Switch_B(config)# **interface fastEthernet 0/1**
Switch_B(config-if)# **switchport mode trunk**
Switch_B(config-if)# **switchport trunk encapsulation dot1q** Switch_B(config-if)# **exit**

Attribution des VLANs aux ports
Switch_B(config)# **interface fastEthernet 0/2** Switch_B(config-if)# **switchport mode access** Switch_B(config-if)# **switchport access vlan 2** Switch_B(config-if)# **exit**

Switch_B(config)# **interface fastEthernet 0/3** Switch_B(config-if)# **switchport mode access** Switch_B(config-if)# **switchport access vlan 3** Switch_B(config-if)# **exit**
Switch_B(config)# **interface fastEthernet 0/4** Switch_B(config-if)# **switchport mode access** Switch_B(config-if)# **switchport access vlan 4** Switch_B(config-if)# **exit**

Définition de la passerelle par défaut Switch_B(config)# **ip default-gateway 200.0.0.1**
3.3 Configuration du Routeur R1

R1(config)# **interface fastEthernet 0/0**
R1(config-if)# **ip address 200.0.0.1 255.255.255.0** R1(config-if)# **exit**

R1(config)# **interface fastEthernet 0/0.2**
R1(config-subif)# **encapsulation dot1q 2**
R1(config-subif)# **ip address 10.0.0.1 255.255.255.0** R1(config-subif)# **exit**

R1(config)# **interface fastEthernet 0/0.3**
R1(config-subif)# **encapsulation dot1q 3**
R1(config-subif)# **ip address 172.16.0.1 255.255.255.0** R1(config-subif)# **exit**

R1(config)# **interface fastEthernet 0/0.4**
R1(config-subif)# **encapsulation dot1q 4**
R1(config-subif)# **ip address 192.168.0.1 255.255.255.0** R1(config-subif)# **exit**

Conclusion
Vous avez pu voir que pour réaliser un routage entre VLANs, il ne suffit pas de brancher un routeur sur un commutateur, il est nécessaire de configurer le routeur.

Administration Réseaux

1. ASPECT ADMINISTRATIF

L'administration réseau ne comporte pas seulement les aspects de design, de configuration et de déploiement. Il est en effet important d'avoir une vue du réseau, afin de permettre une maintenance efficace et appropriée. Les caractéristiques liées à cette vue sont les suivantes :

Il faut avoir une vue d'ensemble, et non pas une vue unitaire de chaque dispositif, car chaque unité du réseau influe sur les autres.
Il faut bien définir et répartir les responsabilités de l'administration réseau au personnel concerné. Il faut éviter que les responsabilités par service soient trop vastes (Surcharge de travail et des ressources du service), mais aussi qu'elles soient trop limitées (Résolution des problèmes moins efficace).

L'analyse des coûts est l'une des plus grandes responsabilités de l'administration réseau, dont voici quelques exemples :

Conception.
Mise en œuvre.
Frais de maintenance :

- Réparations.
- Main d'œuvre.
- Equipement de réserve, pour la continuité des services importants.

Mise à niveau :
- Croissance du réseau.
- Formation technique du personnel.
- Formation des utilisateurs.

Installation :
- Déploiement de logiciels.

L'administration réseau efficace passe toujours par une documentation complète. A ce niveau, l'utilisation de relevés d'erreurs est très conseillée. Ce type de document sert à :

Recueillir des éléments d'information (Pour l'identification d'un problème). Assurer le suivi du traitement.
La résolution du problème (Inconnu ou déjà rencontré).
Justifier des frais supplémentaires :

- Embauche de personnel.
- Achat de matériel.
- Formation supplémentaire.

2. SURVEILLANCE DU RESEAU

i) Surveillance avec SNMP

La surveillance réseau est un point important de l'administration réseau, car elle sert à :

Prévoir les changements liés à la croissance.

Détecter des modifications imprévues dans l'état du réseau, qui peuvent être : ○ Une panne sur un équipement.
○ Une tentative de piratage.
○ La défaillance d'une liaison.

La surveillance du réseau à l'aide du protocole SNMP est un choix judicieux, car il permet :

La surveillance du trafic. La détection de défaillance d'un équipement.
La détection de la surcharge ou de la mauvaise configuration d'une unité.

Afin d'envoyer, de recueillir et d'analyser les informations de surveillance, deux types d'unités sont utilisées :
Agent SNMP (Fournisseur et transmetteur d'information d'un segment à un autre).
Console de gestion SNMP (Logiciel d'analyse).
Il existe différents logiciels permettant cette surveillance, comme :
Surveillance réseau de Windows NT (2000 & XP). Network Analyser de Fluke.
Ces logiciels ne peuvent pas recueillir les informations provenant d'autres segments du réseau sans l'aide d'agents SNMP.
L'architecture de gestion de réseaux se compose de quatre éléments principaux :

Station d'administration réseau (Console de gestion) :
○ Interface entre l'administrateur et le système réseau.
○ Dispose de programmes traitant les données recueillies avec SNMP. ○ Tient à jour une MIB contenant les informations de toutes les unités gérées.

Agent de supervision :
○ Elément contenu dans les unités à gérer (Emettrices d'informations). ○ Remplit la base MIB locale et transmet les informations au moment opportun.

MIB (Base d'informations de management) :
○ Réside sur chaque unité gérée.
○ Base de données contenant toutes les informations de surveillance.

Protocole de gestion de réseau :
○ Il s'agit du protocole SNMP (Simple Network Management Protocol). ○ Fonctionne au niveau de la couche 7 du modèle OSI.
○ Il comporte trois fonctions principales :

GET : La console de gestion peut récupérer des données de l'agent. **PUT** : Définir les valeurs pour les objets se trouvant sur l'agent. **TRAP** : Permet à l'agent d'informer la console de gestion.

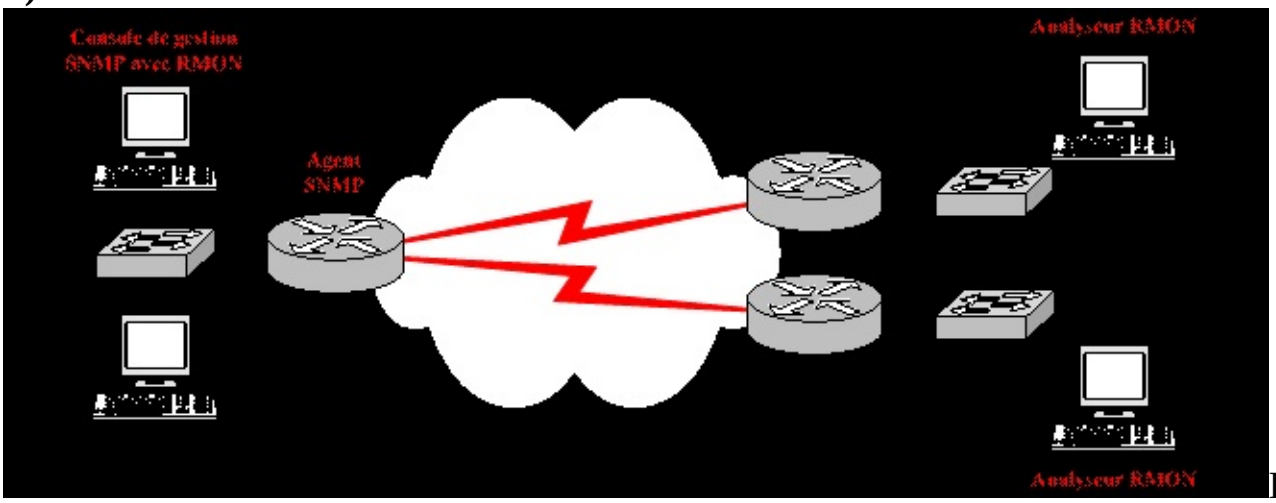
Le processus de transmission et de recueil des informations peut être fait par l'intermédiaire de deux méthodes :

Récupération :
○ Demande de la console de gestion aux unités gérées.
○ Régulière dans le temps.

Interception :

o L’agent de supervision recueille ses informations dans sa MIB locale. o Définition de seuils (Limites maximales ou minimales).
o En cas de dépassement de seuil, l’agent envoie un message d’alerte à la console de gestion, qui récupérera les informations.
o Emission uniquement lorsque c’est nécessaire (Définit par des seuils).

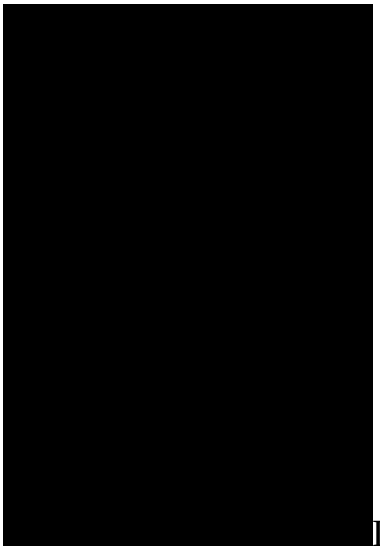
ii) Extensions RMON



L’une des améliorations les plus efficaces à SNMP est la fonction RMON :
Elle fait appel à des analyseurs RMON.

Un analyseur RMON a les mêmes fonctions qu’un agent, avec des fonctionnalités RMON supplémentaires.
Un analyseur RMON est placé sur chaque segment du réseau contrôlé.
Les analyseurs RMON recueillent les données de leur segment et les acheminent vers la console de gestion.

De plus, le principe de consoles de gestion redondantes existe dans le but de fournir deux avantages importants :
Possibilité de contrôle et de gestion du même réseau sur plusieurs sites distants.
Redondance de la base MIB (En cas de panne d’une station d’administration).



L’extension RMON enrichie la base MIB de SNMP en créant de nouvelles catégories de données :

Groupe de statistiques Ethernet :
o Statistiques sur chaque sous-réseau contrôlé.

o Contient des compteurs incrémentaux (Pour les octets, paquets, erreurs, taille de trames, etc.).
o Contient aussi une table d'index (Référencement de chaque unité Ethernet contrôlée, regroupant leurs compteurs respectifs).
o Donne une vue d'ensemble sur la charge et l'état de fonctionnement d'un sousréseau.

Groupe de contrôle de l'historique :
o Enregistrement d'échantillons des compteurs du groupe de statistiques Ethernet. o Prélèvement par défaut toutes les 30 minutes.
o Taille par défaut de la table à 50 entrées (Nouvelles remplaçant les anciennes). o Constitue une base de référence du réseau.

Groupe des alarmes :
o Utilisation des seuils, qui sont définis par l'utilisateur.
o Message d'alarme envoyé aux personnes concernées en cas de dépassement d'un seuil (Processus appelé interception d'erreurs).
o Elément essentiel au dépannage préemptif.

Groupe des systèmes hôtes :
o Compteurs pour chaque hôte sur le segment de réseau (Paquets émis ou reçus, broadcasts, etc.).

Groupe des systèmes hôtes TOPN :
o Production de rapports sur un groupe d'hôtes en tête d'une liste statistique. o Identification des hôtes qui ont les plus grandes valeurs de compteurs.

Groupe des matrices :
o Enregistrement de la communication entre deux hôtes.
o Données stockées dans une matrice.

Groupe des filtres :
o Utilisation d'un filtre de données et d'un filtre d'état.
o Délégation à un analyseur RMON de recueillir les paquets provenant d'une certaine interface et correspondant à une combinaison logique (ET, OU, etc.) de ces deux filtres.
o Le filtre de données permet de déterminer si les données des paquets correspondent à un modèle précis.
o Le filtre d'état se base sur un type de paquet recherché.

Groupe d'interception des paquets :
o Permet de préciser une méthode d'interception des paquets qui ont été choisis par le groupe des filtres.
o Précise aussi la quantité de données dans chaque paquet capturé ainsi que le nombre total de paquets capturés.

Groupe des évènements :
o Contient les évènements générés par d'autres groupes dans la MIB. o Chaque opération de comparaison dans une extension RMON de la base MIB crée un évènement.

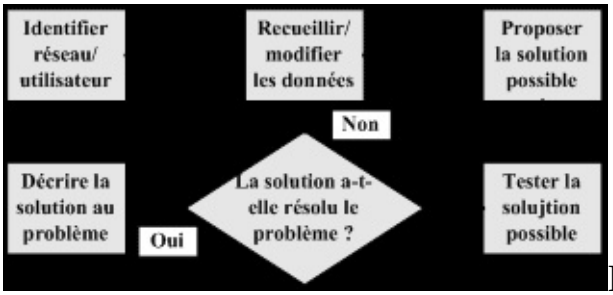
Groupe Token Ring :

- Compteurs concernant le protocole Token Ring.
- Identique sur le principe au groupe des statistiques.

3. DEPANNAGE DE RESEAUX

Il faut utiliser un journal technique et prendre des notes. Ces notes serviront à résoudre un problème éventuel en cataloguant toutes les actions. Cela concerne aussi le référencement des différents problèmes rencontrés ainsi que les solutions appliquées.

Un autre élément essentiel du dépannage préemptif est l'étiquetage :
Les câbles, avec emplacement des extrémités, fonction, etc. Les ports des dispositifs d'interconnexion.



Les étapes du dépannage réseau sont les suivantes :

Définir le problème.
Recueillir un maximum d'informations sur le problème.
Utiliser une technique de résolution de problème.
Référencer le problème ainsi que sa solution.

i) Différentes techniques

Les deux techniques de dépannage réseau les plus efficaces sont :
Le processus d'élimination.
La méthode "diviser pour mieux régner".

Le processus d'élimination consiste à partir du point où l'on a observé la défaillance, puis à vérifier tous les points plausibles de ce point vers le reste du réseau. Cette technique est utilisée pour résoudre des problèmes liés à un utilisateur.

La méthode "diviser pour mieux régner" consiste plutôt à découper le réseau en plusieurs parties et à déterminer quelle est la partie qui pose problème. Il suffira de vérifier chaque cause probable en réduisant au fur et à mesure la taille de la partie du réseau qui pose problème. Cette technique est utilisée pour résoudre des problèmes survenant en reliant deux réseaux fonctionnels pour obtenir un réseau à problème.

ii) Outils logiciels

La plupart des systèmes d'exploitation mettent à notre disposition différents outils de tests réseaux. Le listing suivant concerne essentiellement ceux du système Microsoft Windows, sachant qu'ils ont pour la plupart des équivalents sur les autres systèmes :

Ping
Tracert
Telnet
Netstat
ARP

IPconfig/WinIPcfg

La commande Ping permet de vérifier la connectivité à un hôte distant. Pour cela, elle utilise des paquets Echo du protocole ICMP. Le résultat donne le nombre de paquets envoyés, reçus ainsi que le temps de réponse.

Il faut utiliser la commande **ping [-t] [-a] [-n {valeur}] [-l {taille}] [-f] [-i {ttl}] [-r {valeur}] {IP | nom}**.

Paramètre
-t
-a
-n {valeur}
-l {taille}
-f
-i {ttl}

Description
Envoie des requêtes tant que l'utilisateur n'arrête pas le processus (Ctrl-C). Résolution inverse de l'adresse demandée.
Spécifie ne nombre de requêtes qui seront effectuées.
Spécifie la taille du paquet d'écho.
Demande aux passerelles de na pas fragmenter les paquets.
Précise la valeur du TTL du paquet.

-r {valeur} Enregistre l'itinéraire pour le nombre de saut.
{IP | nom} Indique l'adresse IP ou le nom d'hôte associé (NetBios, DNS, etc.).

La commande Tracert (pour traceroute) est le mécanisme de test à utiliser après avoir rencontré une erreur avec la commande Ping. Elle utilise aussi le protocole ICMP, afin de nous indiquer le chemin qu'a pris le paquet pour atteindre la destination. Le résultat indique chaque saut sur le chemin entre la source et la destination, leur adresse (Voir aussi le nom DNS), ainsi que les résultats de trois analyseurs par saut. Cette commande est utile pour :

Déterminer l'emplacement du problème sur le chemin. Visualiser une éventuelle boucle de routage.
Il faut utiliser la commande **tracert [-d] [-h {nombre}] [-j {liste}] [-w {délai}] {IP | nom}**.

Paramètre
-d
-h {nombre}
-j {liste}

Description
Ne pas convertir les adresses en noms d'hôtes. Nombre maximum de sauts pour rechercher la cible. Indique la route source libre.

-w {délai} Attente d'un délai (millisecondes) pour chaque réponse. {IP | nom} Adresse ou nom de la cible.

La commande Telnet est le mécanisme de test de connectivité le plus complet, car il permet de vérifier le bon fonctionnement de toutes les couches du modèle OSI de la destination. Cette commande est au départ un outil d'accès à distance, mais elle est très performante pour ce qui est du test de fonctionnalité d'un service réseau.

La commande à utiliser est **telnet {IP | nom} [tcp_port_number]**.

Paramètre Description
{IP | nom} Destination à tester.
Tcp_port_number Service réseau utilisant TCP à tester.

Netstat affiche les statistiques relatives au protocole et les connexions TCP/IP actuelles.
La commande à utiliser est **netstat [-a] [-e] [-n] [-s] [-p {proto}] [-r] [intervalle]**.

Paramètre Description
-a Affiche toutes les connexions et les ports en écoute.
-e Affiche les statistiques Ethernet. Cette option peut être combinée avec -s.
-n Affiche les adresses et les numéros de port en format numérique.
-s Affiche les statistiques par protocole, pour IP, TCP & UDP.
-p {proto} Affiche les statistiques pour un protocole précis (TCP ou UDP).
-r Affiche la table de routage.
intervalle Affiche les statistiques demandées à intervalle régulier.

ARP sert à afficher et à modifier les tables de traduction d'adresses IP en adresses physiques. Il existe trois commandes :

arp -a [IP] [-N {interface}] : Affichage de la table de traduction. **arp -d {IP} [interface]** : Suppression d'une entrée dans la table de traduction. **arp -s {IP} {MAC} [interface]** : Ajout d'une entrée dans la table de traduction.

Paramètre
-a | -g
-d
-s
-N {interface} IP
MAC
interface

Description
Affichage du contenu de la table de traduction. Suppression d'une entrée.
Ajout d'une entrée.
Affichage des entrées pour une interface uniquement. Adresse IP à mettre en correspondance.
Adresse MAC qui sera associée à une adresse IP. Précise l'interface où la modification doit être effectuée.

IPconfig (Windows NT, 2000 et XP) et WinIPcfg (Windows 9x et Millenium) affichent les informations d'adressage IP pour chaque adaptateur réseau.
La commande à utiliser est **ipconfig [/all] [/renew {carte} | /release {carte}]**.

Paramètre Description
/all Affichage de l'intégralité des informations sur toutes les cartes. /renew {carte}

Renouvellement d’un bail DHCP pour une carte spécifique. /release {carte} Libération du bail DHCP pour la carte spécifiée.