المدرسة العليا للتكنولوجيا - الداخلة
ⵜⵉⵎⵙⵙⵓⵔⵉⵜ ⵜⴰⵏⴰⵎⵓⵔⵜ ⵏ ⵜⵙⵙⵏⵉⵡⵉⵏ - ⴰⴷⴰⵅⵍⴰ
ÉCOLE SUPÉRIEURE DE TECHNOLOGIE - DAKHLA

Module : Réseaux Informatique

Pr. Elahmadi Cheikh Année : 2022

Table des matières

1. Introduction aux réseaux

A l'origine, un réseau était un rassemblement de personnes ou d'objets. De nos jours on entend par réseau, les réseaux d'entreprises, qui connectent différentes machines afin de pouvoir les faire communiquer entre elles. Que ce soit pour le partage de fichiers ou l'envoi de messages, la plupart des entreprises sont aujourd'hui dotées d'un réseau afin d'être plus efficientes (il est quand même plus simple de transférer un fichier par Internet que de l'envoyer sur CD par la poste).

Au cours de cet essentiel nous allons étudier comment les informations (fichier, données, etc.) circulant sur des réseaux de petite taille (PAN, LAN) ou plus grande taille (MAN, WAN), ainsi que la connectique utilisée.

1.1. Connexion à un réseau

1.1.1. Matériel

Un ordinateur est composé de divers éléments. Avant de connecter votre ordinateur sur un réseau, il est nécessaire que vous connaissiez ce qui le compose, afin qu'en cas de panne vous sachiez identifier si cela provient du réseau ou non. De plus, cela vous permettra d'être plus familier avec une machine et pourra sûrement vous aider en cas de panne d'un ordinateur.

Voici la liste des différents composants de votre pc, ainsi que leurs descriptions :

Liste des composants	Description
Carte mère	La carte électronique principale dans un ordinateur. La carte mère contient les bus, le microprocesseur, et des circuits intégrés utilisés pour commander tous les périphériques extérieurs tels que le clavier, l'affichage graphique, les ports série et les ports parallèles, ou encore les ports USB ou Firewire.
Processeur	Puce de silicium effectuant tous les calculs arithmétiques et logiques dans un ordinateur. Il gère aussi les flux d'informations dans un ordinateur.
RAM (Random Access Memory)	Mémoire vive permettant de stocker les instructions en attente de traitement, autant que les données temporaires. Une fois l'ordinateur éteint cette mémoire se vide, contrairement au disque dur.
Disque Dur	Aussi appelé HDD (Hard Disk Drive en Anglais). Disque de stockage de données. C'est sur le disque dur que vous enregistrez vos données. Contrairement à la RAM, le disque dur conserve vos données même si l'ordinateur est éteint.
Bus	Canal de communication interne à un ordinateur par lequel transitent les données entre les différents composants.
Alimentation	Composant fournissant l'alimentation nécessaire à votre ordinateur.
ROM (Read Only Memory)	Mémoire accessible uniquement en lecture une fois la mémoire écrite. Ce genre de composant sert à stocker des informations qui ne doivent pas être effacées.
Lecteur de CD-ROM	Dispositif permettant de lire des CD-ROM

Il existe aussi des composants de fond de panier (backplane en Anglais) qui permettent d'ajouter des extensions à votre carte mère.

Liste des composants	Descriptions
Carte Vidéo	Carte d'extension permettant d'afficher un visuel sur un moniteur
Carte Son	Carte d'extension permettant de manipuler et de produire des sons via des hauts parleurs ou tout autre périphérique de sortie sonore (casque, etc.)
Carte Réseau (NIC/ Network Interface Card)	Carte d'extension permettant de relier physiquement un ordinateur à un réseau (LAN, WAN, etc.)
USB (Universal Serial Bus)	Port de connexion à chaud, vous permettant de brancher votre périphérique même si votre ordinateur est allumé. A noter que les transferts s'effectuent à haute vitesse.
Firewire	Norme concurrente de l'USB permettant aussi de connecter à chaud divers appareils et permettant des transferts à hautes vitesses.

1.2. Systèmes de numération

Lorsque les ordinateurs ont été créés, ils étaient fort coûteux du fait du nombre de composants qu'ils nécessitaient, en plus de leurs tailles impressionnantes.

Un ordinateur pourrait donc se résumer à un ensemble de commutateurs électriques pouvant prendre deux états :

- En fonction (le courant passe)
- Hors fonction (le courant ne passe pas)

Pour les différentes tâches qu'ils effectuent de nos jours, les ordinateurs utilisent le système de numérotation binaire.

1.2.1. Représentation des données informatiques

Du fait que les humains fonctionnent avec le système décimal, l'ordinateur doit pouvoir effectuer cette traduction afin de pouvoir traiter les informations des utilisateurs. Ces nombres binaires sont exprimés en « bits », qui constituent la plus petite unité d'information d'un ordinateur.

Un groupe de 8 bits correspond à un octet (bytes en anglais), qui représente un caractère de données. Pour un ordinateur, un octet représente également un emplacement de mémoire adressable.

Par exemple, la représentation binaire des caractères du clavier et des caractères de contrôle est donnée dans le tableau des codes ASCII (American Standard Code for Information Interchange) dont voici un extrait :

Décimal	Hexadécimal	Octal	Binaire	Char
0	0	000	00000000	NUL
1	1	001	00000001	SOH
2	2	002	00000010	STX
3	3	003	00000011	ETX
4	4	004	00000100	EOT
7	7	007	00000111	BEL

Ce tableau nous présente les équivalences entre différents systèmes de numérotation que nous allons étudier par la suite. Si nous regardons la colonne « binaire », nous voyons que tous les caractères sont exprimés grâce à une combinaison de 8 bits pouvant prendre la valeur 0 ou la valeur 1.

Du fait de la taille des informations contenues dans les ordinateurs actuels, différentes unités de mesure ont été mises en place :

Unité	Définition	Octets	Bits	Exemples
Bit (b)	Chiffre binaire 1 ou 0	1 bit	1 bit	+5 volts ou 0 volts
Octet (o)	8 bits	1 octet	8 bits	01001100 correspond à la lettre L en ASCII
Kilo-octet (Ko)	1 kilo-octet =1024 octets	1024 octets	8192 bits	mail type : 2ko premiers PC : 64Ko de Ram
Méga-octet (Mo)	1 méga-octet =1024 kilo-octets	1 048 576 octets	8 388 608 bits	disquette = 1,44 Mo CD-ROM = 650 Mo
Giga-octet (Go)	1 gigaoctet =1024 méga-octets	1 048 576 kilo-octets	Env. 8 milliards de bits	disque dur type = 4 Go
Téraoctet (To)	1 téraoctet =1024 giga-octets	1 048 576 méga- octets	Env. 8 trillions de bits	quantité théorique de données transmissibles par une fibre optique en 1 seconde

1.2.2. Systèmes de numération

L'homme est habitué dès le plus jeune âge à utiliser un système de numération pour représenter des valeurs. Ce système comporte 10 symboles : 0 1 2 3 4 5 6 7 8 9 et se nomme « système de numération décimal ».

Ce système constitue la base du calcul pour les hommes, principalement parce que ces derniers ont 10 doigts. Nous utiliserons d'ailleurs ce système comme système de référence dans la suite du cours. Cependant, il existe d'autres systèmes de numérotation pouvant représenter des valeurs.

Une valeur est de ce fait une notion abstraite pouvant être exprimée selon différents systèmes :

Un ordinateur, lui, utilise un système de numération basé sur la représentation du passage de courant, 0 (fermé) ou 1 (ouvert), dans un circuit électrique. Il faut se rappeler qu'à l'époque de l'expansion des ordinateurs, les composants à deux états ont participé à simplifier le traitement pour un ordinateur.

Autre système, le système hexadécimal, comportant 16 symboles 0 1 2 3 4 5 6 7 8 9 A B C D E F. Les 6 lettres correspondent en décimal à 10 11 12 13 14 15.Ce système est utilisé pour simplifier les valeurs décimales trop grandes.

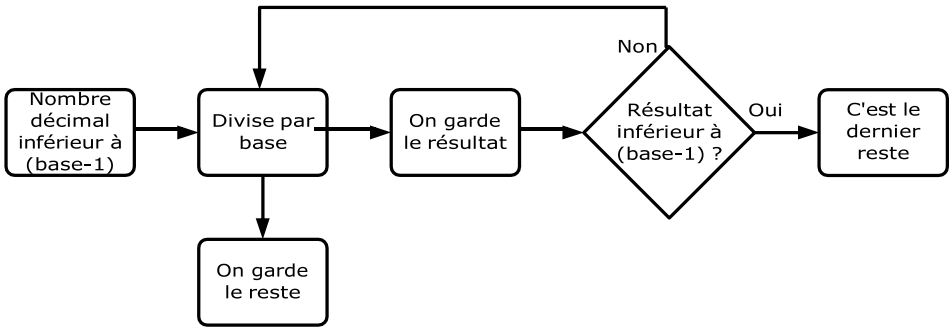
Il est évident ici de l'utilité de disposer de plusieurs systèmes d'informations. Une fois que l'on est familiarisé avec ces différents systèmes, la valeur A2F54B est plus facile à manipuler ou à mémoriser que son équivalent décimal.

1.2.3. Conversions

Entre ces bases il existe des méthodes de conversions :

- Décimal > Binaire
- Décimal > Hexadécimal
- Binaire > Décimal
- Hexadécimal > Décimal
- Binaire > Hexadécimal
- Hexadécimal > Binaire

Pour convertir du décimal vers une autre base, on utilise cette formule :



On divise notre nombre par la base à laquelle on veut le convertir et on continue tant que ce nombre n'est pas inférieur à la base. Il suffit ensuite de prend les différents restes et de les concaténer du dernier vers le premier (de droite à gauche).

La conversion vers une base décimale se fait en décomposant le nombre en digit (chaque élément de la valeur). Et ensuite on multiplie chaque digit par la puissance de la base en commençant par celui le plus à droite avec une puissance zéro (si le nombre est une valeur hexadécimale alors on multipliera les digits par 16^0, 16^1, 16^2, etc.). C'est donc l'ensemble des valeurs des différents digits ainsi multipliés qui forme la valeur en décimal, comme le montre cette formule

$$\sum_{0}^{i=n-1} (base^i \times \textit{valeur du digit})$$

Enfin, pour convertir du binaire vers l'hexadécimal, on prend un groupe de 4 bits et on les convertit en hexadécimal via les puissances de 2. Pour l'inverse, il suffit de faire exactement la même chose en utilisant la première formule comme si l'on convertissait en base 2, en utilisant des groupes de 4 bits ici aussi.

Hexadécimal	Binaire	Hexadécimal	Binaire
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

Tableau de conversion binaire/hexadécimale

1.3. Terminologie de base des réseaux

Un réseau est par définition un ensemble d'entités communicant entre elles. Nous allons nous intéresser dans le cadre de ce cours à ce que l'on nomme des réseaux de données ou réseauxinformatiques. Ces réseaux sont apparus suite à une demande des entreprises qui recherchaient une méthode pour éviter la duplication des imprimantes et une simplification des communications de données entre des équipements informatiques.

La première classification de réseau que nous allons faire s'établit sur la base des distances entre les communicants.

- Les réseaux LAN :
    - Couvrent une région géographique limitée
    - Permettent un accès multiple aux médias à large bande
    - Ils assurent une connectivité continue aux services locaux (Internet, messagerie, etc.)
    - Ils relient physiquement des unités adjacentes
        - Exemple : Une salle de classe

- Les réseaux WAN :
    - Couvrent une vaste zone géographique
    - Permettent l'accès par des interfaces séries plus lentes
    - Assurent une connectivité pouvant être continue ou intermittente
    - Relient des unités dispersées à une échelle planétaire
        - Exemple : Internet

Ces types de réseaux sont les plus courants, néanmoins il en existe d'autres, à l'instar des MAN (Metropolitan Area Network), qui connectent un ou plusieurs LANs dans une même région géographique. Ce type de réseau est en émergence du fait du développement des réseaux Wireless. On les trouve souvent en ville, situés dans les endroits publics.

Un autre type de réseau est le SAN (Storage Area Network) qui est une zone de stockage et de transfert de données.

Les SANs :

- Utilisent un réseau différent des hôtes afin de ne pas encombrer le trafic (ce type de réseau génère un important trafic).
- Permettent un taux de transfert nettement plus élevé entre serveurs, afin de permettre une réplication ou un mouvement des données plus aisé.
- Permettent de dupliquer des données entre serveurs jusqu'à une distance de 10 km.
- Utilisent diverses technologies qui permettent de ne pas tenir compte du système utilisé.

Un VPN (Virtual Private Network) est un réseau privé qui est construit dans une infrastructure de réseau public tel qu'Internet. Par Internet, un tunnel sécurisé peut être mis en place entre le PC de l'utilisateur et d'un routeur VPN se trouvant au siège social de l'entreprise, afin que celui-ci accède de chez lui au réseau de son entreprise.

1.4. Unités de mesure

La bande passante d'un réseau représente sa capacité, c'est-à-dire la quantité de données pouvant circuler en une période donnée sur de réseau. Celle-ci se mesure en bits par seconde. Du fait de la capacité des supports réseau actuels, les différentes conventions suivantes sont utilisées :

Unité de bande passante	**Abréviation**	**Équivalence**
Bits par seconde	bits/s	1 bit/s = unité fondamentale
Kilobits par seconde	Kbits/s	1kbit/s = 1000 bits/s
Mégabits par seconde	Mbits/s	1Mbit/s = 1 000 000 bits/s
Gigabits par seconde	Gbits/s	1Gbit/s = 1 000 000 000 bits/s

À cette notion de bande s'ajoute celle de débit. Le débit est la bande passante réelle, mesurée à un instant précis de la journée. Ce débit est souvent inférieur à la bande passante, cette dernière représentant le débit maximal du média. Cette différence peut avoir pour raisons :

- des unités d'interconnexion de réseaux et de leur charge
- du type de données transmises
- de la topologie du réseau
- du nombre d'utilisateurs
- de l'ordinateur, de l'utilisateur et du serveur
- des coupures d'électricité et autres pannes

De ce fait, le temps de téléchargement d'un fichier peut se mesurer de la manière suivante :

- Temps de téléchargement théorique(s)=Taille du fichier/bande passante
- Temps de téléchargement réel (s) = Taille du fichier (b) / débit

2. Modèles OSI et TCP/IP

2.1. Modèle OSI

La première évolution des réseaux informatiques a été des plus anarchiques, chaque constructeur développant sa propre technologie. Le résultat fut une quasi-impossibilité de connecter différents réseaux entre eux.

Pour palier à ce problème d'interconnections, l'ISO (International Standards Organisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseaux.

Ainsi fût créé le modèle OSI, à partir des structures réseau prédominantes de l'époque : DECNet (Digital Equipment Corporation's Networking développé par digital) et SNA (System Network Architecture développé par IBM).Ce modèle a permis aux différents constructeurs de concevoir des réseaux interconnectables.

Le modèle OSI est un modèle conceptuel. Il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique :

- Quelles sont les informations qui circulent ?
- Sous quelle forme circulent-elles ?
- Quels chemins empruntent-elles ?
- Quelles règles s'appliquent aux flux d'informations ?

Les 7 couches du modèle OSI sont les suivantes :

- **Couche 1 : Couche physique**
  La couche physique définit les spécifications du média (câblage, connecteur, voltage, bande passante…).
- **Couche 2 : Couche liaison de donnée**
  La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches :
  - La sous-couche MAC (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de donnée (MAC, DLCI).
  - La sous-couche LLC (Layer Link Control) s'occupe de la gestion des communications entre les stations et interagit avec la couche réseau.
- **Couche 3 : Couche réseau**
  Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.
- **Couche 4 : Couche transport**
  La couche transport assure la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission. Elle assure également le contrôle du flux d'envoi des données.
- **Couche 5 : Couche session**
  La couche session établit, gère et ferme les sessions de communications entre les applications.
- **Couche 6 : Couche présentation**
  La couche présentation spécifie les formats des données des applications (encodage MIME, compression, encryptions).

- **Couche 7 : Couche application**

Cette couche assure l'interface avec les applications, c'est la couche la plus proche de l'utilisateur.

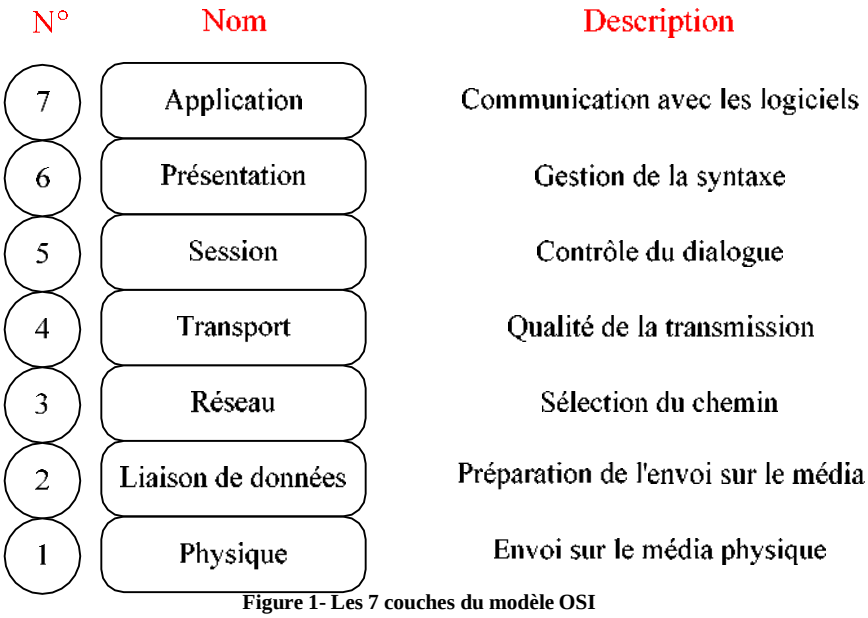


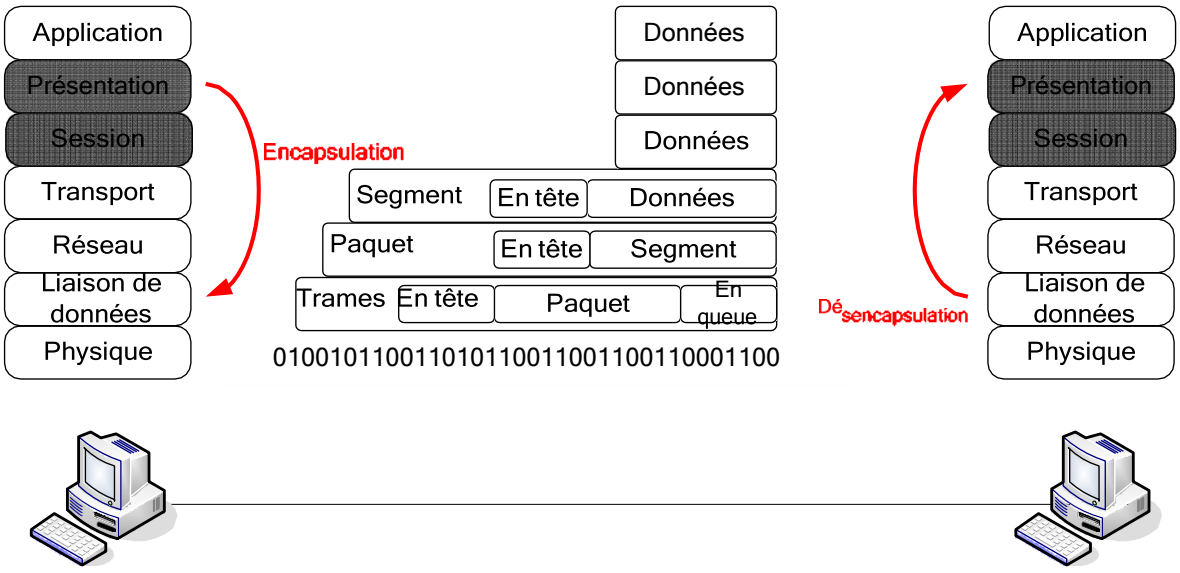
Figure 1- Les 7 couches du modèle OSI

Les avantages de ce modèle sont :

- Une division de la communication réseau en éléments plus petits et plus simples pour une meilleure compréhension
- L'uniformisation des éléments afin de permettre le développement multi constructeur
- La possibilité de modifier un aspect de la communication réseau sans modifier le reste (Exemple : un nouveau média)

Pour communiquer entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation.

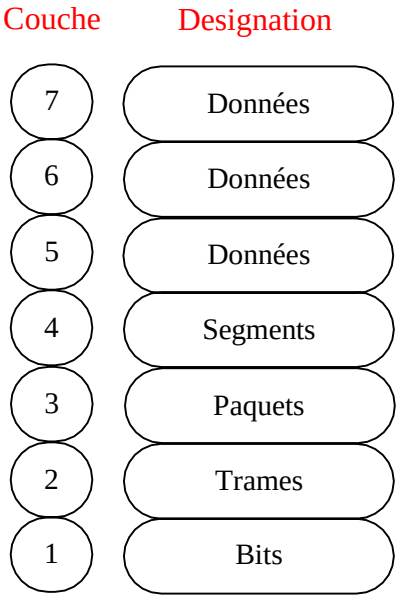
Encapsulation : processus de conditionnement des données consistant à ajouter un en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure :



Lorsque 2 hôtes communiquent, on parle de communication d'égal à égal, c'est-à-dire que la couche N de la source communique avec la couche N du destinataire.

Lorsqu'une couche de l'émetteur construit des données, elle encapsule ces dernières avec ses informations puis les passe à la couche inférieure. Le mécanisme inverse a lieu au niveau du destinataire ou une couche réceptionne les données de la couche inférieure, enlève les informations la concernant, puis transmet les informations restantes à la couche supérieure. Les données transitant à la couche N de la source sont donc les mêmes que les données transitant à la couche N du destinataire.

Pour identifier les données lors de leur passage au travers d'une couche, l'appellation PDU (Unité de données de protocole) est utilisée.



2.2. Modèle TCP/IP

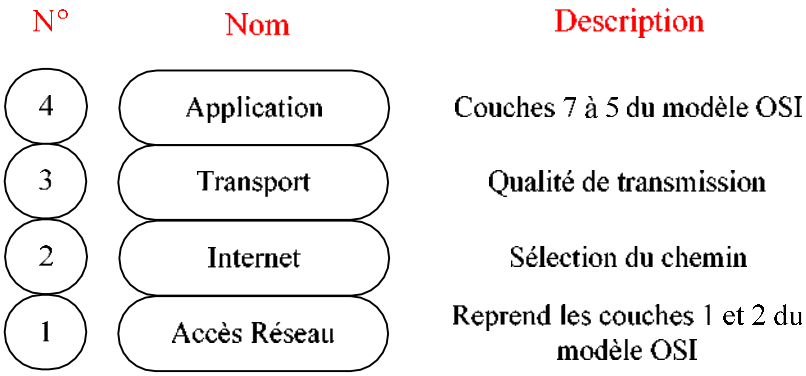
La forme actuelle de TCP/IP résulte du rôle historique que ce système de protocoles a joué dans le parachèvement de ce qui allait devenir Internet. À l'instar des nombreux développements de ces dernières années, Internet est issu des recherches lancées par le DOD (Department Of Defense), département de la défense américaine.

À la fin des années 60, les officiels du DOD se rendirent compte que les militaires du département de la défense possédaient une grande quantité de matériel informatique très divers, mais ces machines travaillaient pour la plupart de manière isolée ou encore en réseaux de taille très modeste avec des protocoles incompatibles entre eux, ceci rendant une interconnexion impossible.

Les autorités militaires se sont alors demandées s'il était possible, pour ces machines aux profils très différents, de traiter des informations mises en commun. Habitués aux problèmes de sécurité, les responsables de la défense ont immédiatement réalisés qu'un réseau de grande ampleur deviendrait une cible idéale en cas de conflit. La caractéristique principale de ce réseau, s'il devait exister, était d'être non centralisée.

Ses fonctions essentielles ne devaient en aucun cas se trouver en un seul point, ce qui le rendrait trop vulnérable. C'est alors que fut mis en place le projet ARPANet (Advanced Research Projects Agency Network du DOD), qui allait devenir par la suite le système d'interconnexion de réseau qui régit ce que l'on appelle aujourd'hui Internet : TCP/IP.

TCP/IP est un modèle comprenant 4 couches :



2.3. Comparaison entre le modèle TCP/IP et le modèle OSI

Ces deux modèles sont très similaires, dans la mesure où les 2 sont des modèles de communication à couche et utilisent l'encapsulation de données.

On remarque cependant deux différences majeures :

- TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales
- TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau Internet actuel

Modèle OSI

Couche	Désignation
Application	Couche Application
Présentation	
Session	
Transport	Couches flux de données
Réseau	
Liaison de données	
Physique	

Modèle TCP/IP

Couche	Désignation
Application	Protocoles
Transport	
Internet	Réseaux
Accès Réseau	

Les modèles OSI et TCP/IP

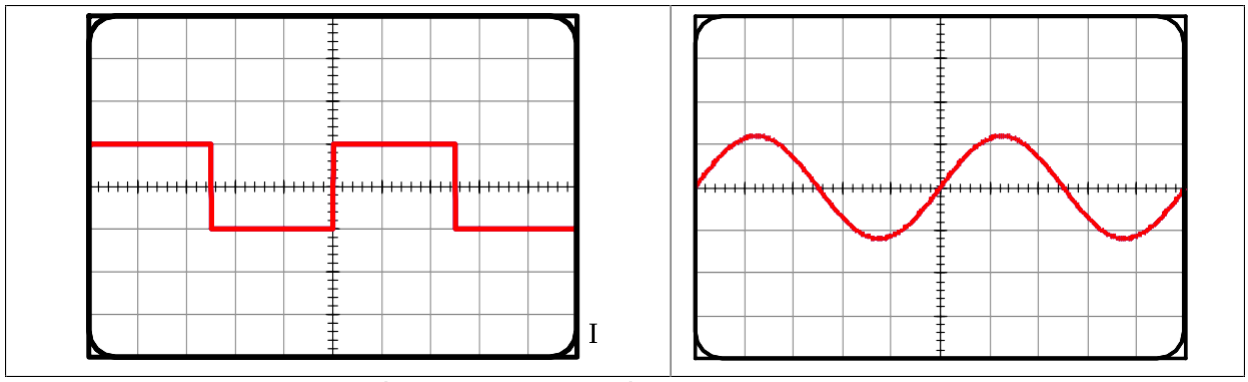
3. Couche 1 : Médias et équipements réseau

Ce chapitre a pour but de vous présenter les différentes connexions physiques entre ordinateurs.

3.1. Les notions de base sur les signaux et le bruit dans les systèmes de communication

3.1.1. Comparaison des signaux analogique et numériques

Lors de l'envoi de données sur un réseau, celles-ci transitent par des liaisons physiques, il convient donc d'observer comment sont-elles représentés dans ces liaisons.



Représentation d'un signal numérique et d'un signal analogique

Signal : tension électrique souhaitée, modèle d'impulsions lumineuses ou encore onde électromagnétique modulée. Il permet d'acheminer les données dans le média.

Le signal numérique dispose d'un graphique de tension que l'on va définir comme « sautillant », il se rapproche d'une onde carrée ou la tension passe quasi instantanément d'un état de basse tension à un état de haute tension.

Le signal analogique présente les caractéristiques suivantes :

- Il oscille
- Son graphique de tension varie constamment en fonction du temps et peut être représenté par une sinusoïde
- Il est utilisé pour les télécommunications depuis le début
    - Exemple : téléphone et radio

Les deux caractéristiques importantes d'une onde sont son amplitude (A), c'est-à-dire sa hauteur et sa longueur, ainsi que sa période. La fréquence de l'onde peut être calculée avec cette formule : f = 1/T.

3.1.2. La représentation d'un bit dans un média physique

Un bloc d'information est un élément binaire, connu sous le nom de bit ou impulsion. Un bit, dans un milieu électrique, est un signal correspondant à un 0 binaire ou à un 1 binaire. Cela peut être aussi simple que 0 (zéro) volts pour un 0 en binaire, et +5 volts pour un 1 binaire, ou un codage plus complexe.

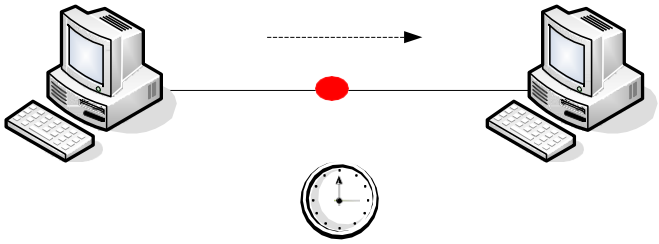
La mise à la terre de référence est un concept important concernant tous les médias de gestion réseau qui emploient des tensions pour diffuser des messages. C'est une masse électrique permettant d'établir une tension zéro dans un graphique de signalisation

3.1.3. Les facteurs pouvant affecter un bit

Il existe différents facteurs pouvant affecter le signal et de ce fait les bits transportés sur le média :

La propagation de signaux réseau :

Le terme de propagation fait référence au temps que met un bit, c'est-à-dire une impulsion, à se déplacer dans le média. Il est impératif que la propagation soit homogène dans le réseau.

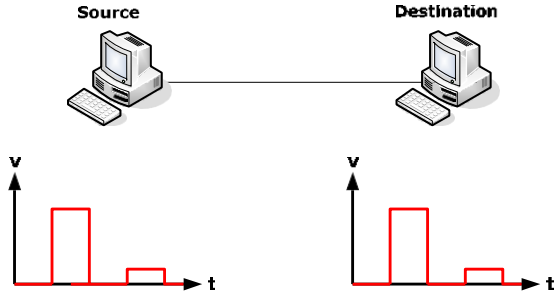


L'atténuation du signal réseau :

Perte de la force du signal. Ce problème est limitable par un bon choix des médias réseau utilisés

La réflexion réseau :

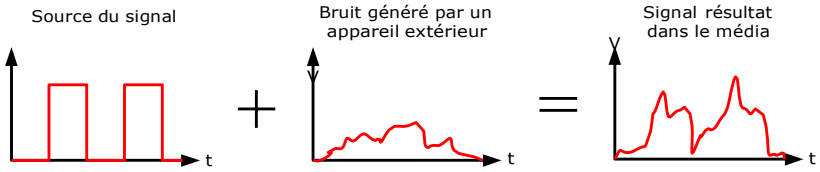
Retour d'énergie causée par le passage des impulsions dans le média. Si ce retour est trop fort, il peut perturber le signal des impulsions suivantes. Le système binaire, et donc à 2 états, peut être perturbé par ces énergies supplémentaires se déplaçant dans le média.



Le bruit :
Ajout indésirable à un signal. Des sources d'énergie situées à proximité du média fournissent un supplément d'énergie venant perturber le signal.

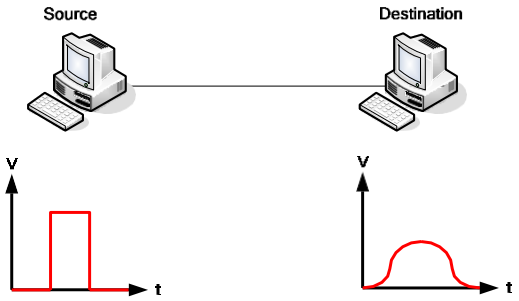
Diaphonie : bruit ajouté au signal d'origine d'un conducteur par l'action du champ magnétique provenant d'un autre conducteur

Paradiaphonie : diaphonie causée par un conducteur interne au câble

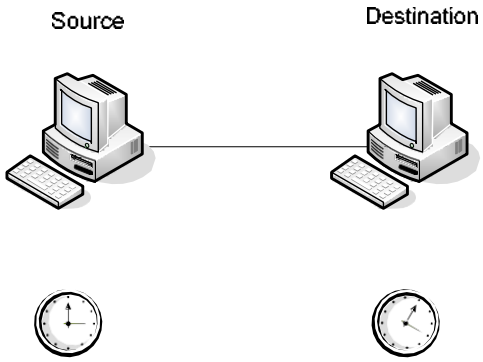


Le bruit peut être causé par des sources d'alimentations externes, des variations thermiques, des interférences électromagnétiques ou encore des interférences de radio fréquences.

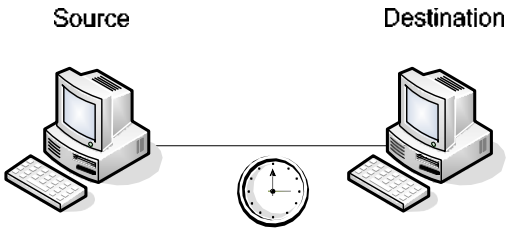
La dispersion :
Étalement des impulsions dans le temps. Si la dispersion est trop forte, le signal d'un bit peut recouper le signal du précédent ou du suivant. La durée d'une impulsion est fixe, la dispersion correspond à une modification de cette durée au fur et à mesure que le signal se propage dans le média.



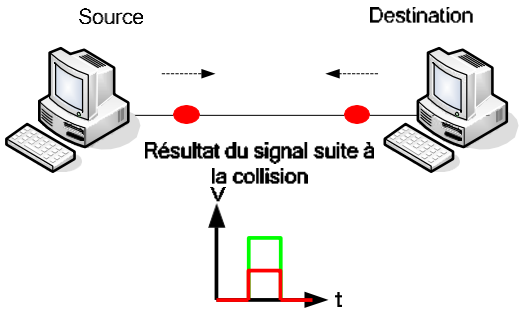
La gigue :
Les systèmes numériques sont synchronisés, tout est réglé par des impulsions d'horloge. Si les horloges de la source et du destinataire ne sont pas synchronisées, on obtient alors « une gigue de synchronisation ».



La latence :
Retard de transmission. Principalement du au déplacement du signal dans le média et à la présence de composants électroniques entre la source et la destination.



Les collisions :
Se produit lorsque 2 ordinateurs utilisant le même segment de réseau émettent en même temps. Les impulsions se mélangent, détruisant alors les données.



Dès qu'un bit accède au média, il est sujet à tous ces paramètres pouvant perturber la transmission. Dans la mesure où le but n'est pas de transmettre un bit, mais des quantités gigantesques (parfois 1 milliard de bits à la seconde) ; ces paramètres ne sont pas à négliger, car le moindre défaut peut avoir des conséquences importantes sur la qualité de la transmission.

Il faut aussi savoir qu'une liaison entre 2 équipements A et B peut être :

- Simple (unidirectionnelle) : A est toujours l'émetteur et B le récepteur. C'est ce que l'on trouve par exemple entre un banc de mesure et un ordinateur recueillant les données mesurées.
- Half-duplex (bidirectionnelle à l'alternat) : Le rôle de A et B peut changer, la communication change de sens à tour de rôle (principe talkies-walkies).
- Full-duplex (bidirectionnelle simultanée) : A et B peuvent émettre et recevoir en même temps (comme dans le cas du téléphone).

3.2. Médias de cuivres

3.2.1. Le câble à paires torsadées non blindées

Le câble UTP est composé de 4 paires de fils torsadées 2 à 2, chacune de ses paires étant isolées des autres. Ce câble compte uniquement sur l'effet d'annulation produit par les paires torsadées pour limiter la dégradation du signal causée par une perturbation électromagnétique et une interférence radioélectrique.

Annulation : Afin de réduire au maximum la diaphonie entre les paires d'un câble à paires torsadées non blindées, le nombre de torsades des paires de fils doit respecter exactement le nombre de torsades permises par mètre de câble.

Lorsque le câble à paires torsadées non blindées est utilisé comme média de réseau, il comporte quatre paires de fils de cuivre. La paire torsadée non blindée utilisée comme média de réseau a une impédance de 100 ohms. Ceci la différencie des autres types de câblage à paires torsadées comme ceux utilisés pour le câblage téléphonique.

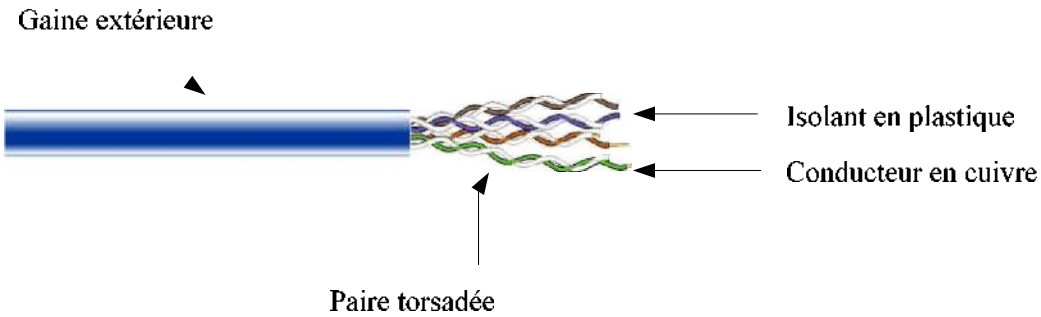
Comme le câble à paires torsadées non blindées à un diamètre extérieur de 0,43 mm et un coût relativement faible, sa petite taille peut s'avérer avantageuse lors d'une installation.

Avantages :

- Simple à installer
- Peu coûteux
- Petit diamètre (pour installation dans des conduits existants)

Inconvénient :

- Sensible aux interférences



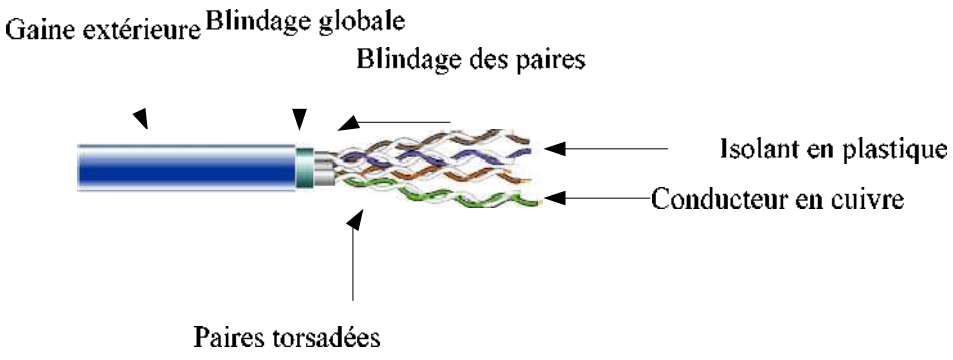
Câble UTP

3.2.2. Le câble à paires torsadées blindées

Le câble à paires torsadées et blindées, ou STP, ajoute aux spécifications de l'UTP une méthode de blindage, d'annulation et de torsion de câbles. Comme le précise les spécifications pour les installations de réseau Ethernet, des câbles à paires torsadées blindées de 100 ohms correctement installés offrent une résistance à l'interférence électromagnétique, ainsi qu'à l'interférence de radiofréquences, sans toutefois augmenter sensiblement la taille ou le poids du câble.

Le câble à paires torsadées blindées présente tous les avantages et désavantages du câble à paires torsadées non blindées en assurant cependant une plus grande protection contre toute interférence externe au prix certes d'un diamètre plus élevé.

Le blindage de ce type de câble doit être mis à la terre lors de son installation, si cela n'est pas effectué correctement, de nombreux problèmes peuvent survenir, car le blindage agit comme une antenne en absorbant les signaux électriques des autres fils du câble et des parasites électriques externes au câble.



Câble STP

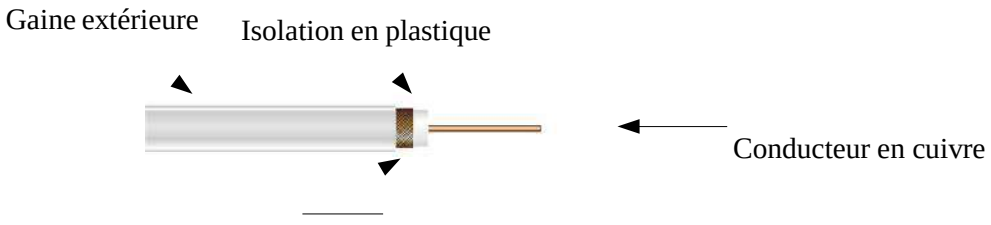
3.2.3. Le câble coaxial

Un câble coaxial est constitué d'un fil de cuivre entouré d'un isolant flexible, lui-même entouré d'une torsade de cuivre ou d'un ruban métallique qui agit comme le second fil du circuit et comme protecteur du conducteur intérieur. Cette deuxième couche ou protection peut aider à réduire les interférences externes. Une gaine de câble enveloppe ce blindage.

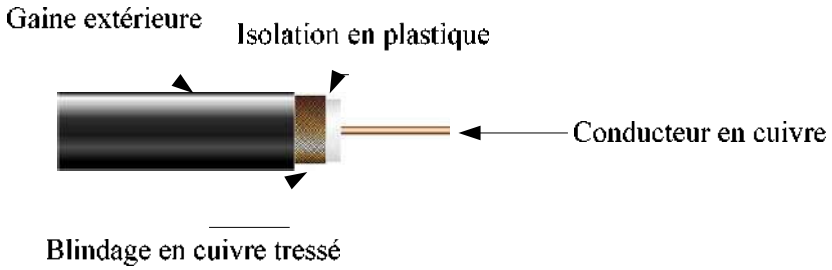
Le câble coaxial offre de nombreux avantages du fait de sa capacité à s'étendre sur une plus grande distance et de son coût parmi les plus faibles. C'est une technologie utilisée depuis de nombreuses années pour tous les types de communications de données.

Le câble coaxial existe en plusieurs variantes :

- **Thicknet** : Epais et raide à cause de son blindage, il est recommandé pour l'installation de câble fédérateur. Sa gaine est jaune.
- **Thinnet** : D'un diamètre plus réduit, il est plus pratique dans des installations comprenant des courbes. De plus, il est plus économique, mais dispose d'un blindage moins conséquent.
- **Cheapernet** : Version économique et de faible diamètre du câble coaxial.



Câble Thinnet



Câble Thicknet

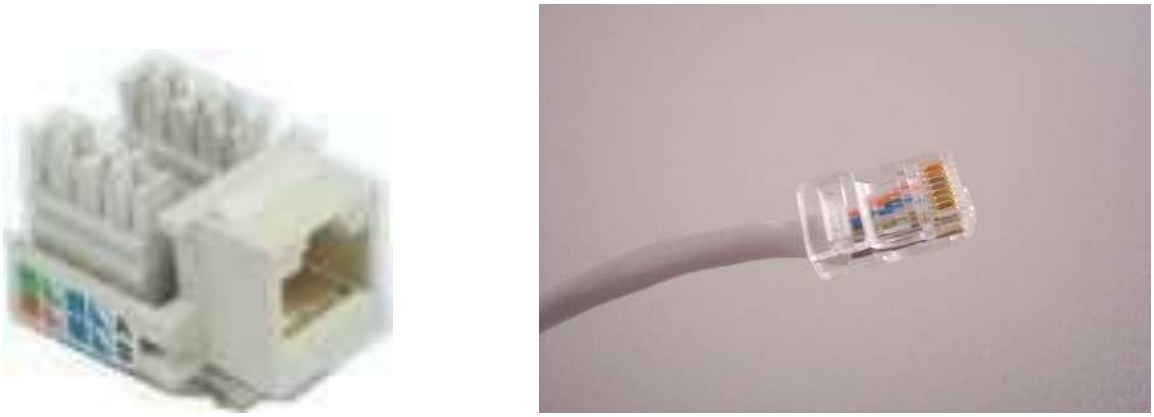
Il importe d'apporter une attention particulière à la mise à la terre. On doit assurer une solide connexion électrique aux deux extrémités du câble. Manquer à ce principe entraîne des parasites électriques qui causent une interférence au niveau de la transmission du signal du média réseau.

3.2.4. Les connecteurs RJ-45

Le raccordement 10BaseT standard (le connecteur de point d'extrémité sans prise) est le RJ-45. Il réduit les parasites, la réflexion et les problèmes de stabilité mécanique et ressemble à une prise téléphonique, sauf qu'il compte huit conducteurs au lieu de quatre.

Il s'agit d'un composant réseau passif, car il sert uniquement au passage du courant entre les quatre paires torsadées de câbles torsadés de catégorie 5 et les broches du connecteur RJ-45.

Les connecteurs RJ-45 s'insèrent dans les réceptacles ou les prises RJ-45. Les prises mâles RJ-45 ont huit connecteurs qui s'enclenchent avec la prise RJ-45.De l'autre côté de la prise RJ-45, il y a un bloc où les fils sont séparés et fixés dans des fentes avec l'aide d'un outil semblable à une fourche. Cecioffre un passage de courant en cuivre aux bits.



Prise RJ-45 et connecteur RJ-45

Voici un tableau récapitulant les différents types de câbles ainsi que leur débit :

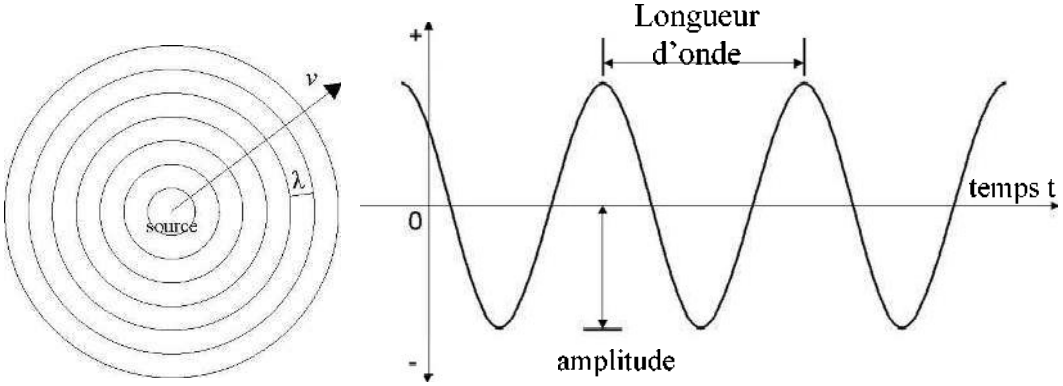
Technologie	Type de câble	Débit théorique	Longueur Max	Connecteur	Coût
10 Base 2 (Thinnet)	Coaxial	10 Mbits/s	200 m	BNC	Peu cher
10 Base 5 (Thicknet)	Coaxial	100 Mbits/s	500 m	BNC	Peu cher
10 Base T	UTP cat 5	10 Mbits/s	100 m	RJ45	Bon marché
100 Base TX	UTP cat 5	100 Mbits/s	100 m	RJ45	Bon marché
10 Base FL	Fibre optique	10 Mbits/s	2000 m	SC	Elevé
100 Base FX	Fibre optique	100 Mbits/s	400 m	SC	Elevé

3.3. Médias optiques

3.3.1. Phénomènes physiques :

Spectre électromagnétique

Les ondes radio, l'infrarouge, les rayons lumineux visibles, ainsi que les rayons gamma et X sont tous des types d'énergie électromagnétique. Cette énergie est créée lorsqu'une source change répétitivement en intensité. Les émissions amplifiées et diminuées créent des ondes, des vibrations qui se déplacent comme des vagues créées par un caillou jeté dans l'eau.



Propagation d'ondes électromagnétiques

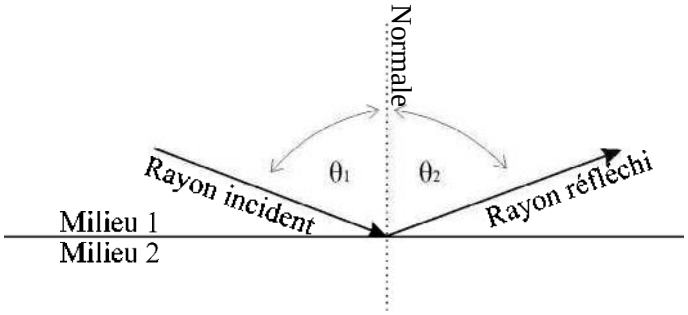
La distance entre les ondes est appelée la longueur d'onde et est désignée par λ. Elle dépend de la fréquence d'altérations de charge. Plus la fréquence d'émission est grande, plus petite est la distance entre les summums (maximums) d'ondes.

Les ondes électromagnétiques partagent des propriétés similaires. Entre autres, elles se propagent toutes à la vitesse de la lumière *c* (299 792 458 m /s) quand elles traversent le vide. Quant à un autre environnement, tel que l'air, l'eau ou le verre, leur vitesse *v* est atténuée.

Lorsqu'on regroupe les ondes électromagnétiques commençant par celles qui ont la plus petite longueur jusqu'aux ondes qui ont la plus grande longueur, on obtient le **spectre électromagnétique**. Les ondes de longueur entre 400 nm et 700 nm constituent la lumière visible. La lumière d'une longueur d'onde supérieure est appelée la lumière infrarouge. Les longueurs couramment utiliséespour le transport d'informations dans la fibre optique sont précisément les longueurs de l'infrarouge : 850 nm, 1310 nm et 1550 nm.

Réflexion

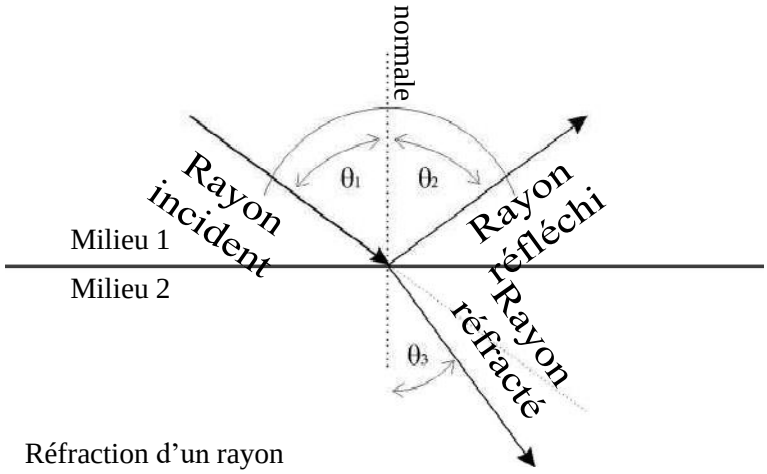
Un rayon passant dans un milieu 1, qui rencontre sur son chemin un autre milieu 2 est appelé **rayon incident**. Une fois arrivé sur la surface de l'autre milieu, le rayon incident se réfléchit. Selon la **loi de réflexion**, l'angle incident θ_1 est égal à l'angle réfléchi θ_2.



Réflexion d'un rayon où $\theta 1 = \theta 2$

Réfraction

Supposons qu'un rayon incident traverse un milieu transparent, par exemple l'air, et arrive sur la surface d'un autre milieu, également transparent, soit l'eau. Au lieu de se réfléchir complètement, il est possible que le rayon incident traverse la surface qui sépare les deux milieux (le dioptre), ainsi en pénétrant dans l'eau. Lorsque le rayon traverse la surface, son angle s'approche vers la normale. On peut observer ce cas sur le schéma ci-dessous où l'angle θ_1 est supérieur à θ_3. Ce phénomène est appelé la **réfraction** et l'on dit pour le rayon traversé qu'il est **réfracté**.



Réfraction d'un rayon

Pour qu'un rayon soit réfléchi sans être réfracté, il faut que son angle d'incidence soit plus grand que **l'angle critique** des deux milieux.

Il est important de connaître le facteur qui détermine l'importance de déviation subi par le rayon réfracté. Ce coefficient, nommé **l'indice de réfraction**, est le rapport entre la vitesse de la lumière dans le vide et dans le milieu : ***n = c / v.***

Il faut également retenir que l'indice de réfraction dépend de la longueur d'onde λ. Cela veut dire que deux rayons ayant deux différentes longueurs d'ondes ne se comportent pas de la même façon dans un milieu M, à savoir que l'une se déplace plus vite que l'autre. C'est d'ailleurs pour cette raison que l'on a choisi la lumière infrarouge et non pas une autre pour le transport d'informations dans la fibre optique.

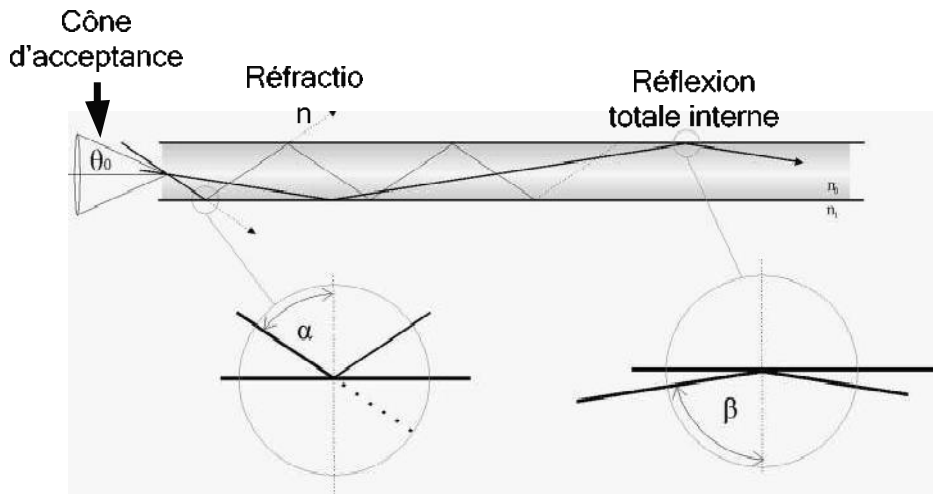
La réflexion interne totale

Dans une fibre optique, les données sont transmises de façon similaire à une transmission réalisée dans un fil électrique : s'il y a de la lumière, l'information traduite en bit 1, sinon en bit 0. L'objectif est évidemment que le rayon, le porteur de l'information, arrive bien de la source jusqu'à destination et

sans être affaibli. Pour ce faire, le rayon doit être guidé dans la fibre sans réfraction, il doit se propager en faisant la **réflexion interne totale**.

Les deux conditions principales pour réaliser la réflexion interne totale sont :

- l'indice de réfraction $\mathbf{n_0}$ du cœur de la fibre doit être **supérieur** à l'indice de réfraction de la gaine $\mathbf{n_1}$,
- le rayon entrant doit se situer dans le **cône d'acceptance**.



Réflexion interne totale

Sur l'image au dessus l'on voit que le premier rayon entrant est en dehors du cône, avec un angle supérieur à θ_0. Remarquez sur la première partie agrandie que le rayon est effectivement réfracté et rappelez-vous que dans ce cas, l'angle d'incidence α est bien inférieur à l'angle critique.

Le deuxième rayon, quant à lui, passe bien par le cône, son angle d'incidence β est supérieur à l'angle critique, et il se propage par la réflexion totale interne tout au long de la fibre. C'est un **rayon guidé**.

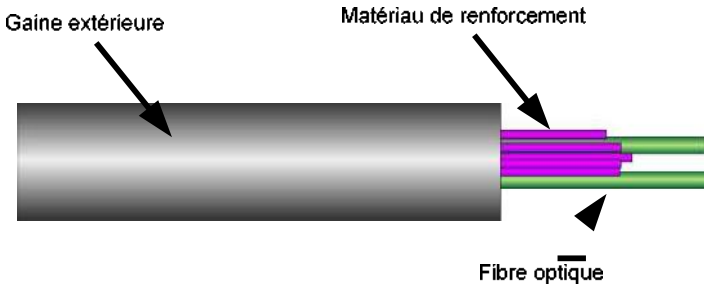
3.3.2. Composants optiques

Fibre optique

Une fibre optique transmet des données dans un sens seulement. Aussi pour que deux entités communiquent en full duplex, un câble optique doit contenir deux fibres optiques : l'une pour transmission et l'autre pour réception. Un câble peut contenir de 2 jusqu'à 48 fibres. Les fibres réunies ensemble dans un câble ne créent pas de bruit, car elles ne portent pas d'impulsions électriques qui pourraient induire des interférences électromagnétiques. Donc elles n'ont pas besoin d'une protection par blindage, comme les fils en cuivre.

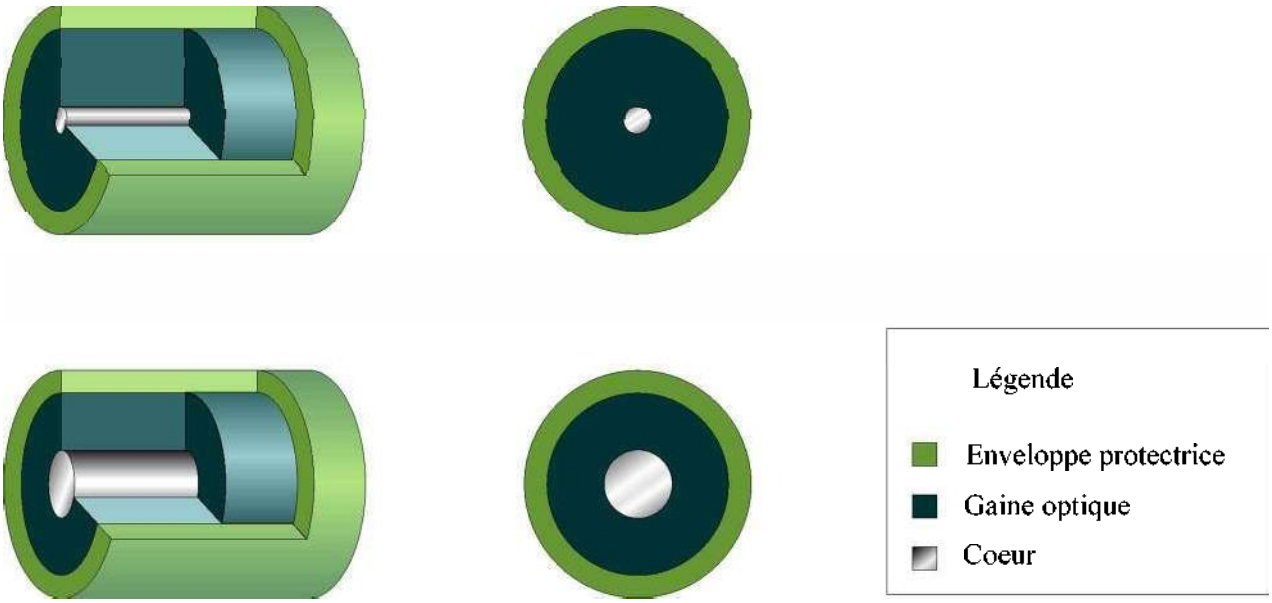
Full duplex avec deux fibres optiques

Un câble à fibres optiques est soutenu avec des fils de renforcement en plastique, tel que le Kevlar. Ceci rend un câble plus résistant, assurant ainsi que les fibres optiques ne s'abîment pas lorsqu'elles sont pliées.



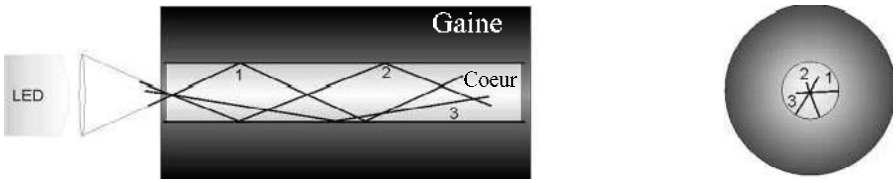
Câble optique

La lumière est guidée dans le centre de la fibre, appelé **cœur**. Le cœur est constitué en majorité de silicium dioxyde (silice), enrichi avec d'autres éléments. Il est entouré par la gaine optique. La gaine est également faite de silice, mais son indice de réfraction est bien inférieur à celui du cœur. Cela permet justement à la lumière de se réfléchir. La gaine optique est protégée par une enveloppe, fabriquée fréquemment en plastique.



Deux fibres optiques : monomode et multimode

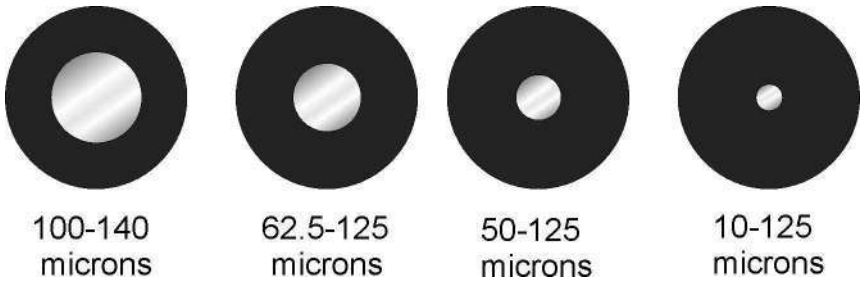
Le chemin fait par un rayon est aussi appelé un **mode**. Lorsqu'une fibre optique transmet un seul rayon, elle est appelée fibre **monomode**. La fibre qui transmet plusieurs rayons, elle est appelée fibre **multimode**. Pour transmettre plusieurs rayons, avec des chemins différents, le cœur de la fibre multimode doit être plus grand que celui de la fibre monomode.



Propagation des rayons dans une fibre multimode

Les sources qui diffusent la lumière dans la fibre ne sont pas les même pour les fibres monomode et multimode. En effet, une fibre multimode utilise la LED (Light Emitting Diode), en français « DEL », Diode Electroluminescente, alors qu'une fibre monomode utilise le laser, qui est en général plus cher. Un laser émet des rayons de longueur plus longue que celle des rayons émis par une LED. De ce fait, la longueur maximale de la fibre multimode est 2000 m. Tandis que la longueur maximale de la fibre monomode est 3000 m. Les fibres monomode sont plus coûteuses et leur utilisation est fréquemment destinée aux liaisons WAN, entre différents bâtiments. Les fibres multimode sont moins chères et plus utilisées dans l'entreprise.

Les diamètres des fibres ont des tailles différentes. Sur le schéma ci-dessous, on peut voir les types multimode et monomode alignés, montrant les diamètres différents en tailles relatives.



La plupart des équipements pour les réseaux locaux transmettent des données en forme électrique. Afin d'intégrer la fibre optique dans un tel réseau, les signaux électriques doivent être transformé en impulsions lumineuses. Pour se faire, il existe des transmetteurs qui transforment, codent et envoient les signaux de lumière. Comme déjà énoncé, il y a deux types de source de lumière :

- **DEL** : diode électroluminescente produit de la lumière infrarouge de longueur de 850 nm, ou 1310 nm.
- **LASER** : (en anglais : Light Amplification by Stimulated Emission Radiation) Amplification de lumière par l'émission de radiation stimulée produit des rayons étroits de lumière infrarouge d'une grande intensité et de longueur d'onde de 1310 nm ou 1550 nm.

A l'autre bout de la fibre se trouve le récepteur. Il transforme les impulsions lumineuses en impulsions électriques qui sont ensuite transférées aux autres équipements réseaux.

Les extrémités de fibre sont attachées aux connecteurs qui se branchent dans les prises des transmetteurs et récepteurs. Les connecteurs de type **SC** (Subscriber Connecter) sont le plus souvent utilisés pour les fibres multimode et les connecteurs de type **ST** (Straight Tip) les plus fréquemment utilisés pour les fibres monomode. Le schéma ci-dessous montre les connecteurs ST et SC, respectivement.

Les deux connecteurs de fibre optique : ST et SC (simplex)

Une paire de connecteurs joints dans un emboîtement s'appelle un connecteur duplex. Un connecteur simplex est un connecteur simple, reliant une fibre seulement.

Les câbles optiques qui dépassent leur longueur maximale sont prolongés par des répéteurs, des équipements d'amplification de signaux de lumière.

Signaux et bruit dans les fibres optiques

Malgré le fait que la fibre optique est le meilleur média de transmission, les signaux qui y transitent peuvent être atténués par différents facteurs. Le plus important facteur est la diminution du signal causée par la dispersion. Elle arrive lorsque la fibre est trop pliée ou serrée. L'angle incident d'un rayon peut alors devenir inférieur à l'angle critique faisant ainsi qu'une partie du rayon soit réfractée. L'absorption est une autre forme d'atténuation. Elle arrive lorsqu'un rayon rencontre des impuretés surson chemin.

Pour contrer les problèmes d'atténuations, on teste les liaisons en fibre optique avec des outils qui mesurent la perte d'énergie et les temps de voyage des signaux.

3.4. Médias sans fil

3.4.1. Fonctionnement d'un réseau sans fil

Les réseaux sans fils ou WLAN (pour Wireless WAN), réussissent à conjuguer tous les avantages d'un réseau filaire traditionnel comme Ethernet mais sans la limitation des câbles.
La mobilité est maintenant l'attrait principal pour les entreprises, la possibilité d'étendre son réseau LAN existant selon les besoins de l'organisation.

Un WLAN à également besoin, tout comme un LAN, d'un média. Au lieu de câbles à paires torsadées, les WLANs utilisent des fréquences radio à 2,4 GHz et 5 GHz.

On parle de "réseaux sans fils" mais la plupart du temps, ces réseaux sont intégrés aux LANs traditionnels, juste considérés comme une extension à l'existant. Aujourd'hui, grâce à des normalisations de l'IEEE et du "Wi-Fi Alliance", les équipements sans fils sont standardisés et compatibles, ce qui explique l'engouement croissant pour ce type de réseau de moins en moins coûteux.

Il faut savoir que la première version d'un réseau sans fil offrait un débit de l'ordre de 1 à 2 Mbps. Grâce à la mobilité rendue possible, cette technologie fut rapidement mise en place.

En effet, tout d'abord pour faciliter certains métiers comme la gestion des stocks dans les entrepôts, rapidement les réseaux sans fils se sont étendus à d'autres secteurs comme dans les hôpitaux, les écoles et universités. Standardiser cette technologie devenait nécessaire, un groupe de travail a donc été mis en place en 1991 par plusieurs constructeurs, le WECA (Wireless Ethernet Compatibility Alliance), plus tard, ce nom changera pour le Wi-Fi (Wireless Fidelity).

En Juin 1997, L'IEEE publie les standards 802.11 pour les réseaux locaux sans fils.

Les réseaux sans fils peuvent fonctionner à deux bandes de fréquences, selon la technologie utilisée.
Soit aux alentours de 2400 Mhz (2,4 Ghz) pour le 802.11b et 802.11g soit aux alentours de 5000 Mhz pour le 802.11a.

La bande la plus utilisée pour le moment est l'ISM (Industrial Scientific and Medical) cela correspond à la bande des 2,4 GHz avec une largeur de bande de 83,5 MHz. Soit des fréquences allant de 2,4 GHz à 2,4835 GHz.

Tableau récapitulatif des fréquences et débits :

	802.11b	**802.11a**	**802.11g**
Bande de fréquence	2,4 Ghz	5 Ghz	2,4 Ghz
Débit maximum	11 Mbps	54 Mbps	54 Mbps

Les lois de la radio :

- Débit plus grand = Couverture plus faible
- Puissance d'émission élevée = Couverture plus grande mais durée de vie des batteries plus faible
- Fréquences radio élevées = Meilleur débit, couverture plus faible

Pour qu'un réseau sans fil fonctionne, il faut au moins 2 périphériques au minimum, comme un point d'accès (AP) et une carte sans fil pour le client. Voici les différents composants que l'on peut trouver dans un WLAN :

- **Les adaptateurs du client :**
  - PCMCIA : Utilisé sur les ordinateurs portables en externe, antenne intégrée
  - LM : Identique au PCMCIA, même bus, mais sans antenne
  - PCI : Utilisé pour les ordinateurs fixes
  - Mini PCI : Utilisé sur les ordinateurs portables en interne, nécessite une antenne supplémentaire
- **Les points d'accès (AP)** : Les modèles Cisco Aironet 1100 et 1200 sont les plus utilisés pour un accès aux utilisateurs
- **Les ponts, ou Wireless bridges (BR) :** Périphérique principalement utilisé pour relier deux réseaux filaires
- **Les antennes :**
  - Directionnelles
  - Omnidirectionnelles
- **Les périphériques sans fil natifs :**
  - PDA
  - Ordinateur portable
  - Téléphones IP
  - Imprimantes

3.4.2. Authentification et sécurité

Avec la venue du 802.11 et des réseaux sans fil, le problème de la sécurité s'est bien évidemment posé. Bien évidemment la propagation des ondes fut le premier souci, la solution matérielle des antennes directionnelles ainsi que la pose de filtres sur les vitres de manières à ne pas laisser passer lesondes fut une des solutions, mais trop onéreuse pour beaucoup d'entreprises. Plusieurs solutions logicielles ont donc vu le jour.

La première repose sur l'utilisation d'un SSID (Service Set Identifier) qui permet de se connecter au réseau si l'on connaît le SSID. Cette solution est tout de même peu sécurisée du fait qu'un logiciel permettant de capturer des trames peut facilement récupérer ce SSID.

Une autre sécurisation peut agir sur l'adresse MAC de la carte directement. Cette méthode est tout de même un peu plus sécurisé puisque se basant sur les adresses MAC enregistrées comme ayant accès au réseau. Néanmoins cette méthode reste statique est chaque nouvel utilisateur doit être validé dans la base d'adresses MAC. Pour les grandes entreprises cela représenterait une charge importante de travail. Cette solution est à réserver pour de petits réseaux (PME ou LAN).

Une troisième solution consiste en une clé de chiffrement qui crypte les transferts. Cette clé est nécessaire pour se connecter à l'AP et pour maintenir la connexion. On parle de clé WEP (Wired Equivalent Privacy). Le cryptage se fait sur 64 ou 128 bits .La norme WPA (Wi-Fi Protected Access) met en place un système de clé dynamique.

Il est bien évident que le jumelage de ces différentes solutions peut augmenter la sécurité de votre réseau, mais cela reste encore inférieur à un réseau filaire .Il faut donc attendre la spécification 802.11iou l'application de la norme WPA 2 pour en théorie enfin avoir un niveau sécurité acceptable pour un réseau de grande envergure.

3.4.3. Modes d'implémentations

Considérons deux stations équipées chacune d'une carte Wi-Fi.
Nous avons deux possibilités de connecter ces stations entre elles :

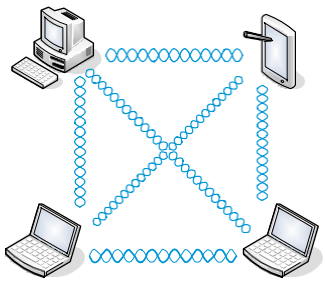
- Soit en les connectant directement l'une à l'autre (comme on pourrait le faire avec un câble croisé et deux cartes réseau Ethernet)
- Soit en passant d'abord par une borne (comme on pourrait le faire avec un concentrateur et une paire de câbles Ethernet droits).

Dans le cas du Wi-Fi, ce n'est pas le média qu'il faut modifier afin de choisir la méthode deconnexion, mais la configuration de la carte.
En effet, une carte Wi-Fi ne se configure pas de la même façon suivant que l'on veuille établir une connexion en mode Ad-Hoc (connexion directe d'une station à l'autre) ou en mode Infrastructure (en utilisant une borne).

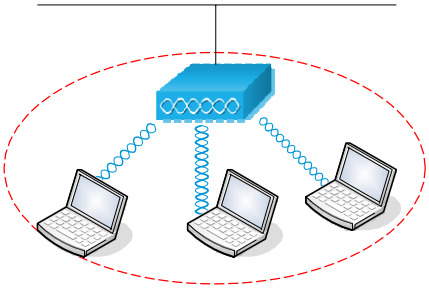
Le mode Ad-Hoc apporte l'avantage de la mobilité. En effet, on peut mettre en réseau deux stations mobiles tant que chacune d'elles se situe dans la zone de couverture de l'autre, on peut donc facilement se déplacer tout en conservant la connectivité par exemple dans une salle de réunion.

Le mode infrastructure, quant à lui, permet de connecter un réseau Wi-Fi à un réseau filaire (internet, ou d'entreprise par exemple). Cependant la mobilité d'une telle configuration est limitée à la zone de couverture de la/ les borne(s) reliée(s) au réseau filaire.

Nota : contrairement à l'Ethernet, il est possible de connecter plusieurs stations entre elles en mode Ad-Hoc, cependant, il arrive fréquemment que l'on perde la porteuse, ce qui rend le service instable. Pour des raisons de performances et de qualité de connexion, il est déconseillé de connecter plus de 4 stations en mode Ad-Hoc :



- Infrastructure : connexion en passant par une borne (équivalent au concentrateur Ethernet).



3.5. Equipements de couche 1

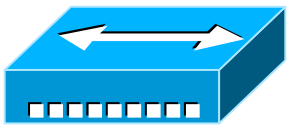
3.5.1. Répéteur

Le répéteur est un composant actif. Son rôle est de régénérer et de resynchroniser le signal afin de pouvoir étendre la portée des câbles.

Symbole d'un répéteur

3.5.2. Concentrateur

Le concentrateur, ou répéteur multi ports, reprend le fonctionnement du répéteur en ajoutant une fonctionnalité de connectivité. En effet, il dispose de plusieurs ports ce qui permet d'interconnecter plusieurs équipements réseau. Chaque signal arrivant sur un port est régénéré, resynchronisé et ré émis au travers de tous les autres ports.



Symbole d'un Concentrateur 10 Base T

Symbole d'un concentrateur 100 base T

Tous ces équipements, passifs ou actifs, créent ou manipulent des bits. Ils ne reconnaissent aucune information dans les bits, ni les adresses, ni les données. Leur fonction se limite donc à déplacer les bits.

3.5.3. Emetteur/récepteur

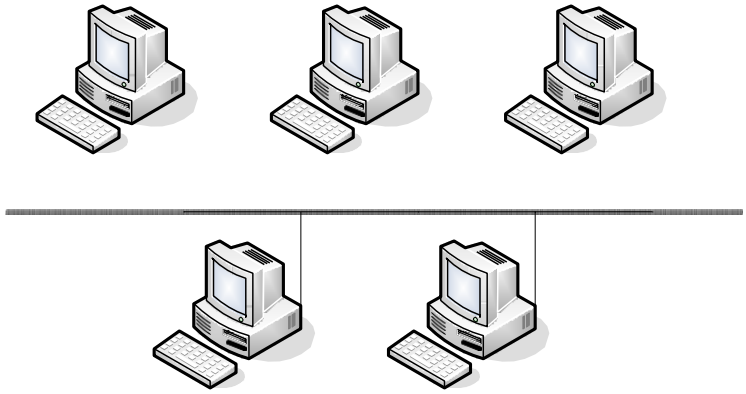
Un émetteur-récepteur (transceiver) convertit un signal en un autre. Il est souvent intégré aux cartes réseau.

3.6. Les topologies de base utilisées dans les réseaux

Topologie : décrit la manière dont les équipements réseau sont connectés entre eux. Nous distinguerons les topologies physiques, décrivant la manière dont les équipements sont reliés par des médias, des topologies logiques, décrivant la manière dont les équipements communiquent.

3.6.1. La topologie en bus

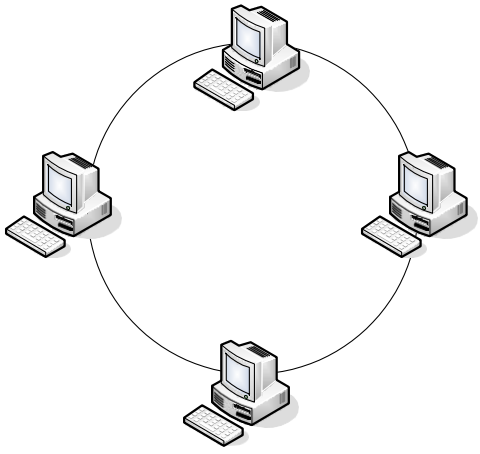
- **Perspective physique** : Tous les hôtes sont connectés directement à une liaison
- **Perspective logique** : Tous les hôtes voient tous les signaux provenant de tous les autres équipements



Topologie en bus

3.6.2. La topologie en anneau

- **Perspective physique** : Les éléments sont chaînés dans un anneau fermé
- **Perspective logique** : Chaque hôte communique avec ses voisins pour véhiculer l'information

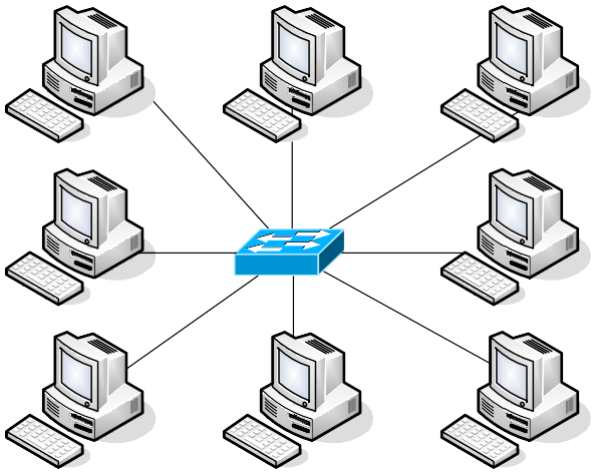


Topologie en anneau

Une variante de cette topologie est le double anneau ou chaque hôte est connecté à 2 anneaux. Ces deux anneaux ne communiquent pas entre eux. Le deuxième anneau est utilisé comme lien redondant en cas de panne sur le premier.

3.6.3. La topologie en étoile

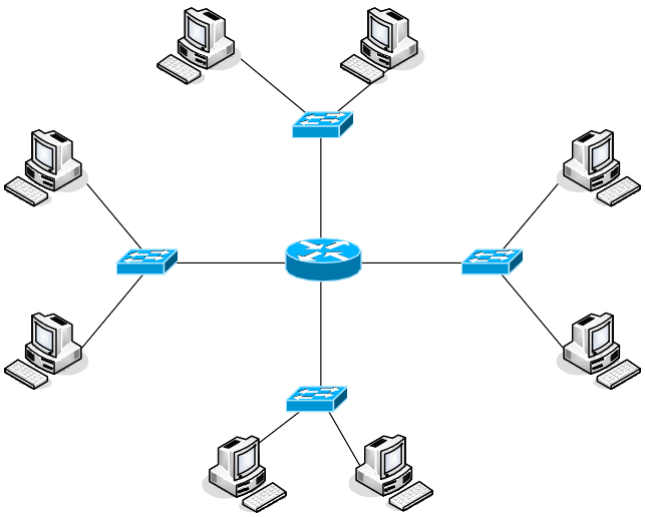
- **Perspective physique** : Cette topologie comporte un nœud central d'où partent toutes les liaisons avec les autres nœuds.
- **Perspective logique** : Toutes les informations passent par un seul équipement, par exemple un concentrateur



Topologie en étoile

3.6.4. La topologie en étoile étendue

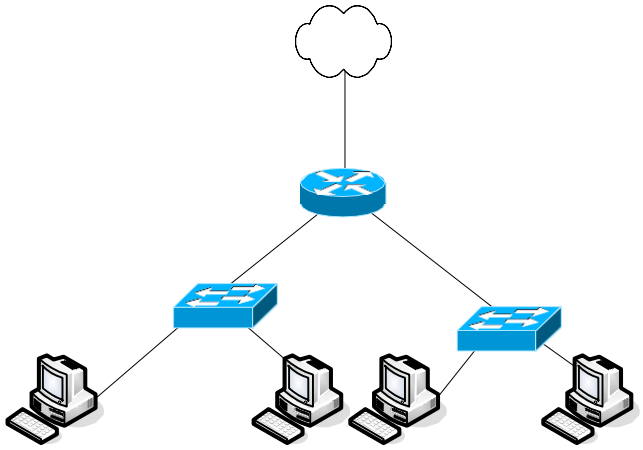
Cette topologie est identique à la topologie en étoile si ce n'est que chaque nœud connecté au nœud central est également le centre d'une autre étoile.



Topologie en étoile étendue

3.6.5. La topologie hiérarchique

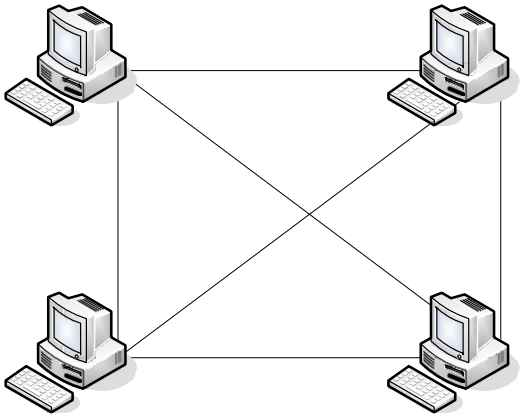
- **Perspective physique** : Cette topologie ressemble à une topologie en étoile sauf qu'ellen'utilise pas de nœud central. Elle utilise un nœud de jonction à partir duquel elle se branche vers d'autres nœuds.
- **Perspective logique** : Le flux d'informations est hiérarchique



Topologie hiérarchique

3.6.6. La topologie complète (maillée)

- **Perspective physique** : Chaque nœud est connecté avec tous les autres
- **Perspective logique** : Dépend des équipements utilisés



Topologie complète

4. Couche 2 : Technologies Ethernet

4.1. Introduction aux technologies LAN

Un LAN (Local Area Network) est un réseau local, il a donc une taille géographiquement limitée (quelques milliers de mètres maximum).

Un LAN permet un accès multiple aux médias à large bande tout en assurant une connectivité continue aux services locaux (ressources et accès Internet partagés, messagerie, etc.). Son but est de relier physiquement des terminaux réseaux proches (stations de travail, serveurs, imprimantes, etc.) par une liaison physique.

Ils sont caractérisés par un haut débit et un faible pourcentage d'erreurs dues à l'atténuation. Ils relient les différents périphériques, terminaux et stations de travail entre eux.

4.2. Introduction à Ethernet

Ethernet est la technologie de base des réseaux LAN la plus utilisée actuellement. Le principe repose sur le fait que toutes les machines sont reliées à une même ligne de communication. L'institut IEEE l'a normalisé et adapté dans son modèle IEEE 802.3. Ces deux technologies sont très similaires (elles diffèrent sur un champ de trame seulement).

4.2.1. Ethernet et le modèle OSI

La technologie Ethernet opère au niveau de la couche physique et de la couche liaison de données (la couche MAC seulement).

Lorsque plusieurs terminaux communiquent par le biais d'un média partagé, les données passent le plus souvent par un répéteur (accessoirement multi ports). Toutes les stations connectées à ce même média « voient » donc ce trafic. Elles communiquent entre elles également par ce même média. Des collisions se créent alors, car elles utilisent ce média en concurrence. On peut donc assimiler un domaine de collision à un environnement partagé.

4.2.2. Spécifications et normes

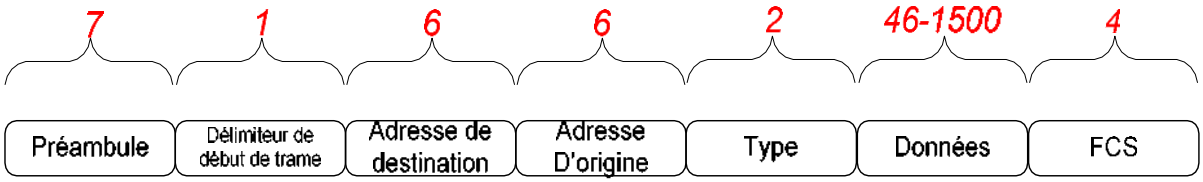
Chaque désignation de technologie utilise une normalisation qui permet d'identifier ses caractéristiques. Celles-ci sont de la forme : vitesse en Mbps – type de signal – type de câble. (ex : 100Base TX)

- Deux types de signalisation existent : Baseband (transmission numérique) ou Broadband (utilisation de porteuse : transmission par ondes par exemple).
- Le type de câble utilisé : cuivre à paires torsadées non blindé (Unshielded Twisted Pairs), ou de type fibre optique (Fiber).
- On exprime aussi sa capacité à supporter le Full Duplex par un X. (à l'exception du 10 Base T qui supporte tout de même le mode Full Duplex).

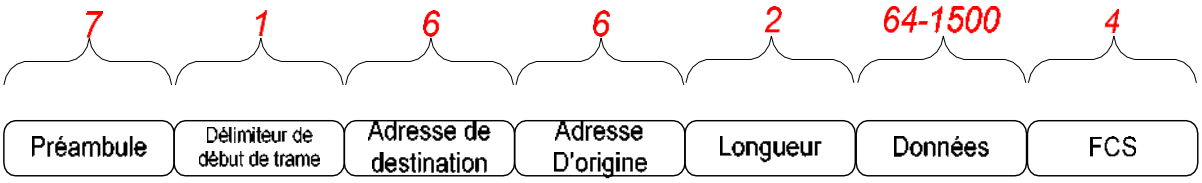
L'IEEE a définit des normes pour les différentes technologies Ethernet :

Norme	Appellation	Débit	Média utilisé
802.3	Ethernet	10 Mbps	Coaxial / UTP / fibre optique
802.3u	Fast Ethernet	100 Mbps	UTP / Fibre optique
802.3z	Gigabit Ethernet	1000 Mbps	Fibre optique
802.3ab	Gigabit Ethernet	1000 Mbps	Câble UTP
802.3ae	10 Gigabit Ethernet	10 000 Mbps	Fibre Optique

4.2.3. Trames Ethernet et IEEE 802.3



Trame Ethernet



Trame IEEE 802.3

- **Préambule** : composé de 1 et de 0 en alternance, annonce si la trame est de type Ethernet ou 802.3.
- **Début de trame** : IEEE 802.3 : l'octet séparateur se termine par 2 bits à 1 consécutifs, servant à synchroniser les portions de réception des trames de toutes les stations.
- **Champ d'adresse de destination** : peut être de type unicast, multicast ou broadcast.
- **Champ d'adresse d'origine** : toujours de type unicast.
- **Type (Ethernet)** : précise le type de protocole de couche supérieure qui reçoit les données.
- **Longueur (802.3)** : indique le nombre d'octets de données qui suit le champ.
  - C'est sur cette partie que diffèrent les trames 802.3 et Ethernet : la valeur du champ permet de déterminer le type de trame : 802.3 ou Ethernet.
  - La trame est de type 802.3 si la valeur hexadécimale du champ est strictementinférieure à 0X600 ; La trame est de type Ethernet si la valeur hexadécimale du champest égale à 0X600.
- **Données** :
  - **Ethernet** : une fois le traitement de couche 1 et 2 terminé, les données sont transmises au protocole de la couche supérieure indiqué dans le champ type. On peut avoir recours à des octets de remplissage s'il n'y a pas assez de données pour remplir les 64 octets minimaux de la trame.
  - **IEEE 802.3** : une fois le traitement de couche 1 et 2 terminé, les données sont transmises au protocole de la couche supérieure indiqué dans le champ donnée de la trame. On peut ici aussi avoir recours au remplissage.
- **FCS** : Séquence de contrôle de trame. Cette séquence contient un code de redondance cyclique permettant à l'unité réceptrice de vérifier l'intégrité des données transmises.

4.3. Fonctionnement d'Ethernet

4.3.1. MAC

Le principe utilisé pour partager l'accès à des ressources communes est appelé MAC pour Media Access Control (à ne pas confondre avec l'adresse MAC).

Dans un environnement où plusieurs hôtes se partagent un média unique de communication, un problème de priorité doit être résolu. Le problème est le même que dans une situation courante : lors d'une discussion à l'intérieur d'un groupe de personnes, une seule personne parle à la fois si elle veut être comprise par son ou ses interlocuteurs.

Dans un environnement Ethernet, c'est au niveau de la sous-couche MAC que l'on va utiliser un processus de détection des collisions : plusieurs hôtes émettent en même temps sur le même média.
Ethernet et 802.3 utilisent un principe d'accès au média non déterministe : CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Les hôtes se partagent donc le média. Si l'un d'eux désire émettre, il vérifie au préalable que personne n'est en train de le faire, puis commence à émettre (CSMA).

Si cependant 2 hôtes émettent en même temps, il se produit alors une collision. La première station qui détecte une collision envoie alors un signal de bourrage, se traduisant par un arrêt d'émission de tous les hôtes. Les paquets concernés sont alors détruits.

Chaque hôte calcule alors une valeur aléatoire définissant la durée avant de recommencer à émettre, puis le mécanisme de CSMA se remet en fonction.

4.3.2. Erreurs possibles

Pendant une transmission de données, de nombreux facteurs peuvent entraîner une corruption de celle-ci.
Le but est de détecter ces erreurs correctement pour déterminer quelles trames doivent être retransmises afin de récupérer des données intègres.

Collisions

Dans un environnement partagé, la première corruption rencontrée est de type collision. Lorsque deux hôtes ou plus émettent un signal au même instant sur le média, il se produit un survoltage qui ne signifie plus rien en terme de données. Ces collisions ne se produisent que dans un environnement Half-Duplex. (car dans un environnement Full-Duplex, chaque paire torsadée n'est utilisée qu'entre deux hôtes dans un seul sens de transmission.). L'algorithme CSMA/CD permet de détecter ces collisions et de les éviter.

Il existe trois types de collision :

- Collision locale
- Collision distante
- Collision de retard

La collision locale est de type survoltage, comme vu dans l'exemple précédent.

Une collision distante résulte d'une trame ayant une longueur inférieure au minimum ou d'un FCS incorrect. Elle est souvent rencontrée à une certaine distance d'environnement répété (hub ou répéteur) mais n'a pas de problème de survoltage. Il peut s'agir de fragments de collision non détruits par un équipement de type répéteur par exemple.

Une collision de retard n'est pas détectée par la couche liaison de données. En effet, elle est caractérisée par une erreur dans les données à partir du 64ème octet. Contrairement aux deux autres types de collision, une collision de retard ne déclenche pas une réémission directe de la trame (car elle n'a pas été détectée par la couche de liaison). La station réceptrice analyse d'abord cette trame avec une couche supérieure (qui détecte l'erreur dans la trame) puis demande un renvoi de cette trame.

Trames longues

Ce type d'erreur est un simple dépassement de la taille maximale d'une trame.
La taille du champ « Données » (variable) d'une trame ne doit pas excéder 1500 octets. Une trame a donc une taille maximale de 1526 octets. Une trame de taille supérieure est donc considérée comme fausse.

Trames courtes

Comme pour les trames longues, l'erreur se situe au niveau du champ « données » qui doit avoir une taille minimale de 46 octets (ou 64 pour IEEE 802.3). Les trames courtes se caractérisent donc par une taille inférieure à 72 octets (ou 90 octets pour IEEE 802.3) mais avec un FCS valide : sinon elle serait considérée comme un fragment de trame, détruit lui aussi.

Autres types d'erreur

D'autres erreurs peuvent survenir du fait de la mauvaise qualité du média (ou d'interférences extérieures) :

- FCS incorrect : le résultat du FCS est faux quant aux données transmises
- le champ longueur ne concorde pas avec la taille du champ « données »
- longueur de champ incorrecte : le préambule ne fait pas 7 octets, …

Une fois qu'une erreur de ce type est détectée, la couche supérieure (de la station réceptrice) va demander un renvoi de cette trame à la station émettrice, jusqu'à obtenir une trame valide.

5. Couche 2 : Commutation Ethernet

5.1. Domaine de collision

On appelle domaine de collision la partie d'un réseau comprenant un environnement partagé. C'est dans ce domaine que les hôtes vont accéder en concurrence à une ressource. De ce fait, des collisions vont se créer sur cette partie du réseau. Le domaine de collision s'étend sur la plus grande partie du réseau contenant des équipements de couche 1 interconnectés.

5.2. Segmentation

Les domaines de collision posent des problèmes, proportionnellement à leur taille. En effet, plus un domaine de collision est grand (mesuré en nombre d'hôtes), plus la bande passante par hôte est faible, et plus le nombre d'erreurs est grand.

Pour diminuer ces effets néfastes, il suffit de segmenter un domaine en plusieurs, de tailles inférieures. On aura alors moins de collisions par segment, donc une plus grande fiabilité et une meilleure bande passante.

Le principe de la segmentation est de n'envoyer des données que sur la portion de réseau concernée. On va ainsi réduire le trafic inutile, ainsi que le nombre d'utilisateurs concurrents du même média.
Pour la segmentation, des équipements de couche 2 sont nécessaires. C'est à ce niveau que l'on peut prendre des décisions d'adressage (sur quel média transmettre une trame).

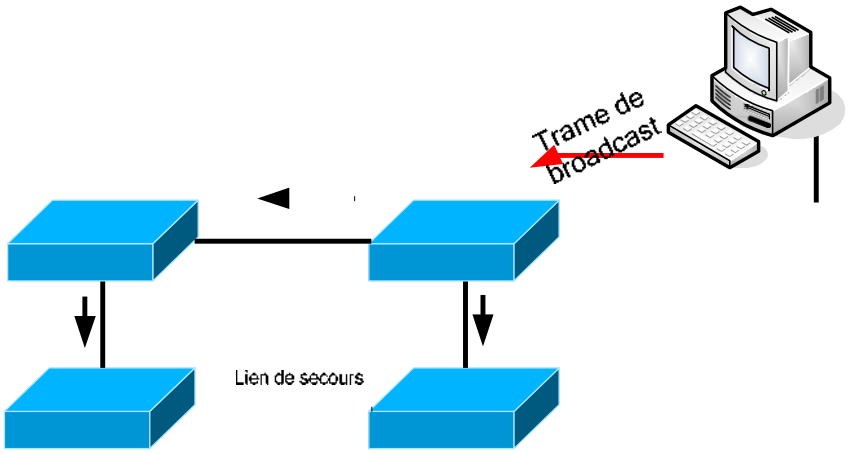
5.2.1. Segmentation par ponts

Les ponts permettent de segmenter un réseau en n'envoyant les données que sur la partie du réseau concernée. Après avoir appris sur quelle portion se trouvent les hôtes (par leur adresse mac), un pont filtrera le trafic suivant l'adresse de destination. Il laissera donc transiter les données vers la partie du réseau qui contient l'adresse de destination, et bloquera les paquets qui ne sont pas destinés à cette même partie.

5.2.2. Segmentation par commutateurs

Les commutateurs sont l'équivalent de répéteurs multi ports intelligents. Chaque hôte où groupe d'hôtes connecté à un port du commutateur veut envoyer des données. Au lieu de retransmettre ces données sur chaque port, le commutateur ne va renvoyer que sur le port où se trouve la partie duréseau contenant le(s) destinataire(s).
Pour se faire, le commutateur va apprendre les adresses MAC de chaque hôte connecté à ses ports. Il saura ainsi quels hôtes se trouvent sur chacun de ses ports. Il stocke ces données dans une table d'adresses MAC.
Les commutateurs fonctionnent beaucoup plus vite que les ponts et créent des domaines sans collisions entre 2 ports en interne (par l'utilisation de circuits virtuels).

5.2.3. Spanning Tree



Dans un réseau utilisant de nombreux commutateurs, des chemins redondants sont souvent utilisés afin d'établir une connectivité fiable et tolérante aux pannes. Un problème se pose alors, car du fait de ces chemins redondants, des boucles de commutation peuvent apparaître. Des tempêtes de broadcast peuvent alors se produire, entraînant une congestion du réseau.

Le protocole Spanning Tree a été développé dans le but de contrer ce problème de boucles de commutation.
Chaque commutateur utilisant le protocole Spanning Tree, envoie des datagrammes BPDU (Bridge Protocol Data Units) à ses compères pour indiquer sa présence. Chaque commutateur calcule alors les routes optimales suivant la topologie et élimine les chemins redondants inutiles grâce à l'algorithme STA (Spanning Tree Algorithm).

Lors de l'utilisation de Spanning Tree, un port de commutateur peut prendre 5 états différents :

- Blocage : aucune trame acheminée, unités BPDU entendues
- Ecoute : aucune trame acheminée, écoute des trames
- Apprentissage : aucune trame acheminée, apprentissage des adresses
- Acheminement : trames acheminées, apprentissage d'adresses
- Désactivation : Aucune trame acheminée, aucune unité BPDU entendue

Le protocole Spanning Tree permet donc de créer un réseau sans liaisons redondantes sans leséliminer. Ces chemins sont alors utilisables en cas de nécessité : si une liaison n'est plus disponible, l'algorithme Spanning Tree recalcule un arbre de chemins permettant de remplacer la liaison manquante.

6. Couche 3 : Protocole IP

6.1. Protocoles routables

Protocole : Ensemble formel de règles et de conventions qui régit l'échange d'informations entre des unités.

Un protocole routable définit la notion d'adressage hiérarchique : un hôte est défini par une adresse unique sur un segment de réseau unique.

Un protocole de routage (à ne pas confondre avec protocole routable), grâce à la structure du protocole routé, a toutes les informations nécessaires pour envoyer un paquet sur le segment spécifié à l'hôte spécifié.

6.1.1. Protocoles orientés connexion et non orientés connexion

Un protocole non orienté connexion ne définit pas de chemin unique pour acheminer les paquets d'un hôte source vers un hôte de destination. Les paquets peuvent alors emprunter des chemins différents suivant la topologie réseau existante entre ces deux hôtes. Cela implique une durée de trajet différente pour chaque paquet et donc un ordre d'arrivée différent de celui d'émission. L'hôte de destination ne peut pas réordonner les paquets.
Le protocole IP est un protocole non orienté connexion.

Un protocole orienté connexion définit un chemin unique entre l'hôte source et l'hôte de destination. Les paquets empruntent alors le même chemin et arrivent donc dans le même ordre. Pour ce faire, l'hôte source établit en premier lieu une connexion avec l'hôte de destination. Une fois cette connexion établie, chaque paquet est envoyé par ce seul chemin. On appelle ce processus « commutation de circuits ».
Le protocole TCP est un protocole orienté connexion.

6.1.2. Protocoles routés

Protocole routé : c'est un protocole de communication de couche 3. Il définit le format des paquets, et notamment la manière de désigner le destinataire du paquet. Un protocole routé peut être **routable** ou **non routable**.

- **Routable** : les messages envoyés à l'aide de ce protocole peuvent sortir de leur réseau (via un routeur). En effet, le format du paquet comprend une distinction entre la partie hôte et la partie réseau.
- **Non routable** : les messages envoyés à l'aide de ce protocole ne peuvent pas sortir de leur réseau. En effet, le format du paquet ne comprend pas de mécanisme permettant à un élément réseau de faire suivre ces paquets au travers de différents réseaux.

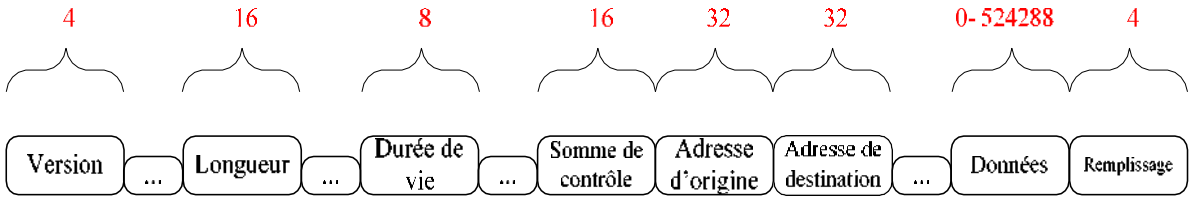
La liste des protocoles routés suivante présente les protocoles les plus connus :

Nom du protocole routé	Protocole routable ?
IP	Oui
IPX	Oui
Appletalk	Oui
CLNP	Oui
NetBEUI	Non
SNA	Non

6.2. Protocole IP

6.2.1. Paquet IP

Les informations provenant de la couche 4 sont encapsulées dans le PDU de couche 3 : le paquet, dont voici les principaux éléments :



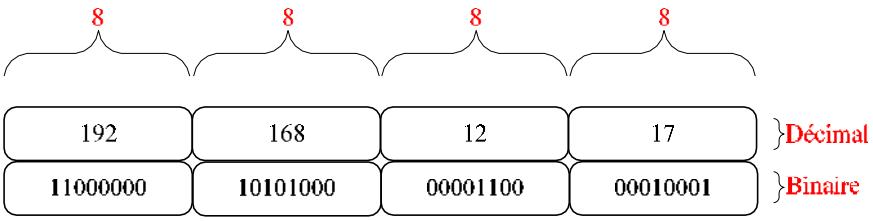
Exemple de paquet IP

Champs	Description
Version	Indique la version de protocole IP utilisée (4 bits).
Longueur totale	Précise la longueur du paquet IP en entier, y compris les données et l'en-tête, en octets (16 bits).
Durée de vie	Un compteur qui décroît graduellement, par incréments, jusqu'à zéro. À ce moment, le datagramme est supprimé, ce qui empêche les paquets d'être continuellement en boucle (8 bits).
Somme de contrôle	Assure l'intégrité de l'en-tête IP (16 bits).
Adresse d'origine	Indique le nœud émetteur (32 bits).
Adresse de destination	Indique le nœud récepteur (32 bits).
Données	Cet élément contient des informations de couche supérieure (longueur variable, maximum 64 Ko).
Remplissage	Des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP soit toujours un multiple de 32 bits.

6.2.2. Adressage IP

Comme nous l'avons vu, une adresse IP est une adresse 32 bits notée sous forme de 4 nombres décimaux séparés par des points. On distingue en fait deux parties dans l'adresse IP :

- Une partie désignant le réseau (on l'appelle netID)
- Une partie désignant les hôtes (on l'appelle host-ID)



Exemple d'adresse IP

Les hôtes situés sur un réseau ne peuvent communiquer qu'avec des hôtes situés sur le même réseau, même si des stations se trouvent sur le même segment. C'est ce même numéro qui permet au routeur d'acheminer le paquet au destinataire.

6.2.3. Classes d'adresses IP

L'organisme chargé d'attribuer les adresses IP publiques est l'InterNIC (Internet Network Information Center).

On appelle « Bits de poids fort », les premiers bits de l'octet le plus à gauche.
Les adresses IP sont réparties en plusieurs classes, en fonction des bits qui les composent :

Classe	Bits de poids fort	Plage	Masque par défaut
A	0	1 à 126	255.0.0.0
B	10	128 à 191	255.255.0.0
C	110	192 à 223	255.255.255.0
D	1110	224 à 239	Aucun
E	1111	240 à 255	Aucun

Dans la classe A, il existe 2 adresses réservées, la plage 0.0.0.0 qui est inutilisable car non reconnue sur les réseaux, ainsi que la plage 127.0.0.0 qui est réservée pour la boucle locale.

Dans toute adresse IP, il existe 2 parties, la partie réseau et la partie hôte. Ces parties sont délimitées grâce au masque de sous réseau associé.
Les bits à 1 représentant la partie réseau et les bits à 0 la partie hôte.
Par exemple la partie réseau d'une classe C sera les 3 premiers octets et la partie hôte le dernier octet.

Il existe 2 adresses IP particulières et réservées dans un réseau, la toute première adresse IP appelée adresse réseau qui caractérise le réseau lui-même et la toute dernière de la plage est l'adresse de broadcast qui est définie par une adresse IP pouvant atteindre toutes les machines du réseau.
Pour une adresse réseau, tous les bits de la partie hôte seront à 0.
Pour une adresse broadcast, tous les bits de la partie hôte seront à 1.

Il arrive fréquemment dans une entreprise qu'un seul ordinateur soit relié à Internet, c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à Internet (on parle généralement de passerelle).

Dans ce cas, seul l'ordinateur relié à Internet a besoin de réserver une adresse IP auprès de l'InterNIC. On caractérise cette adresse d'adresse publique. Toutefois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble de façon interne. Ce sont des adresses privées.

Ainsi, l'InterNIC a réservé trois plages d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet sans risquer de créer de conflits d'adresses IP sur le réseau public. Il s'agit des plages d'adresse suivantes :

- 10.0.0.1 à 10.255.255.254
- 172.16.0.1 à 172.31.255.254
- 192.168.0.1 à 192.168.255.254

6.2.4. IPv4 et IPv6 (IPng / IP next generation)

Le protocole IPv4, le standard actuel, était censé avoir une taille suffisante pour fournir des adresses IP (2^{32}, soit 4 294 967 296 adresses possibles). Néanmoins cette limite est en passe d'être atteinte. Pour palier à cela, en 1992, l'organisme IETF (*Internet Engineering Task Force*) a alors décidé de « moderniser » le système d'adressage IP afin d'éviter cette pénurie.

Différentes solutions ont été mises en place, dans un premier temps afin de réduire cette consommation d'IP.
IPv6 emploie 128 bits à la place des 32 bits actuellement utilisés par IPv4. IPv6 emploie des nombres hexadécimaux pour représenter une adresse, alors qu'IPv4 utilise des nombres décimaux. IPv6 fournit $3{,}4*10^{38}$ adresse IP ($2^{128)}$. Cette version d'IP devrait donc fournir assez d'adresses pour les futurs besoins des nouveaux pays développés.

Exemple d'une adresse IP v4 :

Valeur : 34.208.123.12
Nombre d'octets utilisés : 4

Exemple d'une adresse IP v6 :

Valeur : 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A
Valeur simplifiée: 21DA:D3::2F3B:2AA:FF:FE28:9C5A
Nombre d'octets utilisés : 16

On peut noter que ces nouvelles adresses seront bien plus difficiles à retenir que les adresses IP actuelles : aussi l'organisme en charge de cette version à aussi créer une méthode permettant de simplifier ces IPs : on retire les 0 de chaque début de bloc et, si cela supprime un bloc, on le remplace par « :: ».

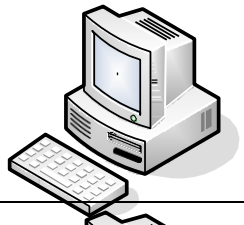
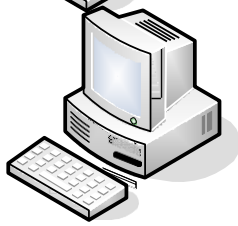
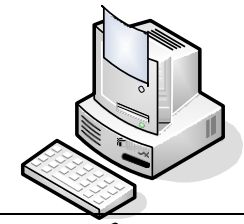
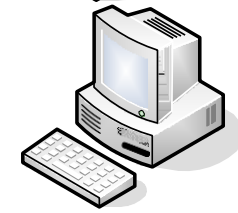
6.3. Gestion des adresses IP

6.3.1. Méthodes d'obtention

On distingue 2 méthodes d'attribution d'adresses IP pour les hôtes :

- **Statique** : chaque équipement est configuré manuellement avec une adresse unique
- **Dynamique** : On utilise des protocoles qui attribuent des IP aux hôtes
    - **RARP** : Protocole associant les adresses MAC aux adresses IP. Il permet à des stations sans disque dur local connaissant leur adresse MAC de se voir attribuer une IP.

- **BOOTP** : Ce protocole permet à un équipement de récupérer son adresse IP au démarrage. L'émetteur envoi un message de broadcast (255.255.255.255) reçu par le serveur qui répond lui aussi par un broadcast contenant l'adresse MAC de l'émetteur ainsi qu'une IP.
- **DHCP** : Remplaçant de BOOTP, il permet l'obtention dynamique d'IP. Lorsqu'un ordinateur entre en ligne, il communique avec le serveur qui choisit une adresse et un masque de sous réseau et l'attribue à l'hôte. Il permet de plus d'obtenir des serveurs DNS, la passerelle par défaut ainsi qu'optionnellement les adresses des serveursWINS.

	Envoi d'un message de broadcast par un client (paquet UDP utilisant le port de BOOTP) afin de contacter un serveur DHCP, s'il en existe un sur le réseau.
	Réponse d'un serveur DHCP si celui-ci a des adresses IP libres.
	Requête du client pour une adresse IP auprès du serveur et négociation du bail
	Renvoi par le serveur de l'adresse IP et du bail accordé.

6.3.2. Résolution d'adresses

- Le protocole ARP

Le protocole ARP permet d'identifier l'adresse physique d'un hôte (adresse MAC unique) à partir de son adresse IP. ARP signifie Address Resolution Protocol.

Chaque machine connectée au réseau possède une adresse physique de 48 bits. Ce numéro unique est en fait encodé dans chaque carte réseau dès la fabrication de celle-ci en usine (adresse MAC).Toutefois, la communication sur un réseau ne se fait pas directement à partir de ce numéro car cette adresse n'est pas hiérarchique. On ne peut donc pas déterminer l'appartenance d'un hôte à un réseau à partir de cette adresse. Pour cela on utilise une adresse dite logique : l'adresse IP.

Ainsi, pour faire correspondre les adresses physiques aux adresses logiques, le protocole ARP interroge les machines du réseau pour connaître leur adresse physique, puis crée une table de correspondance entre les adresses logiques et les adresses physiques dans une mémoire cache.

Lorsqu'une machine doit communiquer avec une autre, elle consulte la table de correspondance. Si jamais l'adresse demandée ne se trouve pas dans la table, le protocole ARP émet une requête sur le réseau. L'ensemble des machines du réseau va comparer cette adresse logique à la leur.

Si l'une d'entre-elles s'identifie à cette adresse, la machine va répondre à l'émetteur qui va stocker le couple d'adresses dans la table de correspondance et la communication sera possible.

- Le protocole RARP

Le protocole RARP (Reverse Address Resolution Protocol) permet de connaître l'adresse IP d'un hôte, à partir de son adresse physique.
Lorsqu'une machine ne connaît que l'adresse physique d'un dispositif, elle peut émettre une requête RARP afin d'avoir son adresse IP.

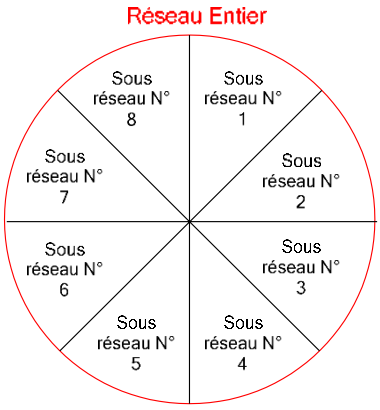
6.3.3. Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole qui permet de gérer les informations relatives aux erreurs générées au sein d'un réseau IP. Etant donné le peu de contrôles que le protocole IP réalise, il permet, non pas de corriger ces erreurs, mais de faire part de ces erreurs. Ainsi, le protocole ICMP est utilisé par tous les routeurs, qui l'utilisent pour reporter une erreur (appeléDelivery Problem).
Un exemple typique d'utilisation du protocole ICMP est la commande ping. Lors de l'exécution de cette commande, des informations précises peuvent être obtenues : le temps mis par un paquet pour atteindre une adresse, ou bien un éventuel problème de routage pour atteindre un hôte.

7. Couche 3 : Subnetting

7.1. Intérêt du Subnetting

Afin d'augmenter les capacités de gestion de trafic dans un réseau, il est possible de subdiviser ce dernier en plusieurs sous réseaux afin de permettre une segmentation des domaines de broadcast.



Pour cela, on emprunte à la partie hôte des bits que l'on désigne comme champ de sous réseaux. Le nombre minimal de bits à emprunter est de 2 et le nombre maximal est égal à tout nombre laissant 2 bits à la partie hôte.

Il faut savoir qu'il y a une perte d'adresses quand on utilise le mécanisme de création de sous réseaux :

- Tout d'abord au niveau des sous réseaux eux-mêmes, le premier sous réseau et le dernier doivent être enlevés. En effet, La première adresse sera l'adresse de réseau : ce sera l'adresse réseau pour la globalité du réseau. La dernière plage ayant l'adresse de broadcast pour leréseau tout entier. Il faut donc enlever les deux plages entières pour éviter toute confusion. On aura donc N-2 sous réseaux utilisables.
- Pour les hôtes également, il y a une perte d'adresses, sans faire de sous réseaux, on avait une seule adresse réseau et une seule adresse broadcast, avec les sous réseaux, on va avoir une adresse de sous réseau à chaque sous réseau et une adresse de broadcast de sous réseau à chaque sous réseau. Il faut donc également penser à la règle des N-2 pour les hôtes.

7.2. Méthodes de calcul

7.2.1. Méthode classique

On entend par méthode classique le fait de procéder sans formule spécifique, par la méthode calculatoire.

Cette méthode se détaille en 6 étapes :

- Empruntez le nombre de bits suffisants
- Calculez le nouveau masque de sous réseau
- Identifiez les différentes plages d'adresses IP
- Identifiez les plages d'adresses non utilisables
- Identifiez les adresses de réseau et de broadcast
- Déterminez les plages d'adresses utilisables pour les hôtes.

- **Empruntez le nombre de bits suffisant**

Il faut tout d'abord déterminer le nombre de bits que l'on va emprunter à la partie réseau.
On détermine tout d'abord le nombre d'hôtes ou de sous réseaux maximums que l'on désire, car suivant ce nombre, on n'utilisera pas les même plages d'adresses (254 hôtes maximum pour une plage de classe C, 65534 pour une plage de classe B et 16 777 216 pour une plage de classe A)
On écrit en binaire le chiffre souhaité de sous-réseaux ou d'hôtes ce qui nous donne le nombre de bits à emprunter ou à laisser. Il faut penser à la règle des N-2, on cherche des plages utilisables. Il faut donc penser à additionner 2 aux hôtes ou aux sous réseaux utilisables que l'on cherche à avoir.
Pour les sous réseaux nous allons emprunter des bits à la partie hôte (allonger le masque) et pour les hôtes nous allons laisser les bits à 0 pour le nombre d'hôtes souhaités

- **Calculez le nouveau masque de sous réseau**

Maintenant que l'on sait combien de bits l'on va emprunter, on calcule le nouveau masque de sous réseau auquel on emprunte les bits à la partie hôte. Pour cela on prend le masque de la plage que l'on veut utiliser, on le convertit en binaire, puis on emprunte le nombre de bits nécessaires à 1 pour la création des sous réseaux.
Ou bien on laisse le nombre suffisant de bits à 0 pour les hôtes.

- **Identifiez les différentes plages d'adresses**

A l'aide du masque de sous réseau on calcule les différentes plages d'adresses possibles. Pour cela il suffit d'écrire chaque possibilité binaire sur les bits que l'on a empruntés pour la création des sous réseaux.

- **Identifiez les plages d'adresses non utilisables**

On retire maintenant la première et la dernière plage d'adresse des différents choix que l'on a. La première adresse sera l'adresse de réseau : ce sera l'adresse réseau pour la globalité du réseau. La dernière plage ayant l'adresse de broadcast pour le réseau tout entier.

- **Identifiez les plages de réseau et de broadcast**

Des plages d'adresses qui restent, on retire aussi les premières et dernières adresses. La première servira d'adresse réseau pour la plage d'adresse. La dernière servira d'adresse de broadcast pour la plage spécifiée.

- **Déterminez les plages d'adresses Hôtes.**

Maintenant qu'il ne nous reste plus que les plages d'adresses utilisables, on a donc les plages d'adresses IP utilisables par les hôtes pour communiquer sur le sous réseau.

7.2.2. Méthode du nombre magique

Cette méthode permet d'aller plus vite dans le calcul, elle est basée sur la formule que voici :

256 = Masque de sous réseau + Taille du sous réseau

Cette formule va vous permettre de calculer rapidement :

- Un masque de sous réseau
- Un nombre d'hôtes par sous réseau

Cette formule est propre à l'octet modifié avec le masque de sous réseau.
Elle permet de trouver le nombre d'hôtes par sous réseaux très vite, dès que l'on a le masque.
Il suffit de soustraire au nombre magique la valeur de l'octet du masque modifié, le résultat ainsi donné est la taille du sous réseau par rapport à cet octet.

Exemple :
On vient de faire du Subnetting sur une classe C, on a donc un masque résultant en 255.255.255.224.
On applique le nombre magique, 256-224=32, il va donc y avoir 32 hôtes par sous réseau (30 utilisables).
On peut également extrapoler, et ce résultat indique donc que les plages de sous réseau seront espacées de 32.

En annexe, on peut également utiliser une formule logique afin de simplifier la création de sous réseaux :

256 = Taille du sous réseau * Nombre de sous Réseaux

Exemple :
On désire savoir le nombre d'hôtes sur 5 sous réseaux avec une classe C on aura donc un masque de type 255.255.255.X
La puissance de 2 la plus proche et supérieur à 5 est donc 8.

On prend la formule :
256 = Taille du sous réseau * Nombre de sous Réseau

Et on l'applique :
256 = Taille du sous réseau * 8
Taille du sous réseau = 256/8 = 32
En enlevant les 2 adresses (celle du sous réseau et celle de broadcast) on a un total de 30 adresses utilisables par sous réseau.

Cela donnera donc un masque de 255.255.255.224 (256-32 = 224)
Et donnera une donc une configuration de type :

Adresse de début du sous réseau : 192.168.0.32
Adresse de fin du sous réseau : 192.68.0.63

Adresse de début du sous réseau : 192.168.0.64
Adresse de fin du sous réseau : 192.68.0.95

Adresse de début du sous réseau : 192.168.0.96
Adresse de fin du sous réseau : 192.68.0.127

Et ainsi de suite

En utilisant ces 2 formules, il est donc beaucoup plus rapide de calculer un masque de sous réseau ou un nombre d'hôte. Néanmoins il vaut mieux bien comprendre la méthode de base avant d'utiliser celle-ci, afin de ne pas faire d'erreur lorsque vous les utilisez, toujours garder à l'esprit que ces formules sont valides uniquement pour l'octet modifié par la création de sous réseaux.

8. Couche 3 : Introduction au routage

8.1. Principes fondamentaux

Avant de commencer ce chapitre, il convient de définir commutation de trames et commutation de paquets (routage). Car, si au premier abord il pourrait sembler que ces 2 termes désignent la même chose, ce n'est pas du tout le cas. La première distinction vient du fait que la commutation de trames s'effectue au niveau de la couche 2 du modèle OSI, alors que le routage s'effectue au niveau de la couche 3 du modèle OSI. Cela indique donc que les routeurs et les commutateurs ne prennent pas leur décision avec les mêmes informations.

Pour joindre les hôtes non locaux, une machine va faire une requête ARP pour avoir l'adresse MAC de la station de destination, si la destination n'est pas locale la requête ARP va échouer, la station enverra alors la trame à sa passerelle par défaut, c'est-à-dire au routeur.

Le routeur examine l'adresse de destination de la couche 3 du paquet, effectue un ET logique binaire avec le masque de sous réseau pour identifier le réseau de destination et prendre la bonne décision de commutation.

De la même manière qu'un commutateur garde une table des adresses MAC connues, un routeur garde une table des adresses réseaux dans sa table de routage. Il va ainsi être capable de commuter les paquets vers un réseau spécifique.

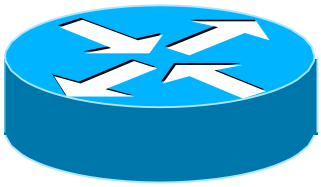
8.2. Domaine de broadcast

Un domaine de broadcast est un domaine logique ou n'importe quels hôtes connectés à un réseau peuvent envoyer des données à une autre machine sans passer par des services de routage.
Plus spécifiquement c'est un segment réseau composé d'hôtes et de dispositifs pouvant être atteint en envoyant un paquet à l'adresse de broadcast. Ces domaines de broadcast sont toujours séparés par des dispositifs de couche 3.

8.3. Les équipements de couche 3 : les routeurs

Routeur :
Équipement de couche 3 permettant d'interconnecter deux réseaux ou plus en se basant sur les adresses de couche 3. Le routeur permet également une segmentation des domaines de broadcast et des domaines de collisions.

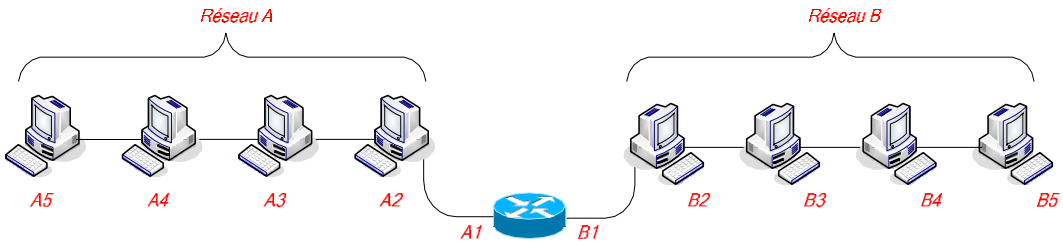
Routeur Cisco de type 2600



Symbole logique du routeur

Le routeur dispose d'une interface (une carte réseau) le reliant au réseau local. Celle-ci dispose d'une adresse IP.

Par exemple, sur le schéma ci-dessous, les adresses des hôtes sont A5, A4, A3 et A2, faisant partie du réseau A. On attribue A1 à l'interface du routeur, lui permettant ainsi de se connecter au réseau A.
Un autre réseau, B, est lui aussi connecté au routeur. Ce dernier dispose donc d'une interface ayant pour IP B1 afin de pouvoir communiquer avec le réseau.



Supposons maintenant que l'on souhaite envoyer des données de A vers B :

- Le routeur reçoit la trame de couche 2, supprime l'en tête de liaison de données
- Il examine l'adresse de couche 3 afin de déterminer le destinataire
- Il effectue un ET logique entre l'adresse IP et le masque de sous réseau afin de déterminer le réseau de destination
- Il consulte sa table de routage pour déterminer l'interface par laquelle les données doivent être envoyées.

C'est pour cela que chaque interface du routeur doit être sur un réseau différent. Sinon le routeur ne pourra pas déterminer par quelle interface envoyer les informations. C'est le principe de commutation de paquets ou routage.

8.4. Détermination du chemin

Les méthodes de sélection du chemin permettent aux équipements de couche 3, les routeurs, de déterminer la route à suivre pour acheminer les informations au travers de différents réseaux.

Les services de routage utilisent les informations de topologie du réseau pour évaluer les chemins. Ce processus est aussi appelé routage des paquets et prend en compte divers paramètres ou "métriques" comme :

- Densité du trafic
- Nombre de routeurs à franchir pour joindre la destination
- Vitesse des liaisons
- Etc.

8.5. Systèmes autonomes, IGP et EGP

Un système autonome est un réseau ou un ensemble de réseaux sous un contrôle administratif commun. Un système autonome est composé de routeurs ayant les mêmes règles et fonctions.

Deux familles des protocoles de routage sont les protocoles IGP (Interior Gateway Protocol) et les protocoles EGP (Exterior Gateway Protocol).

Les IGP routent les données dans un système autonome, comme nous venons de le voir :

- RIP and RIPv2
- IGRP
- EIGRP
- OSPF
- IS-IS

EGP route les données entre les réseaux autonomes. Un exemple d'EGP est BGP.

8.6. Routage statique et dynamique

Il existe différents protocoles de routage permettant de trouver le meilleur chemin. Chaque protocole utilise différents systèmes, différents algorithmes pour fournir au routeur les informations nécessaires à la mise en place de la table de routage.

Voici un tableau récapitulatif de ces différents protocoles avec leurs descriptions :

Nom du protocole	Type (IGP ou EGP)	Algorithme	Métriques	Mise à jour	Remarque
RIP	IGP	Vecteur de distance	15 sauts maximums	30 sec	15 sauts maximums
RIP v2	IGP	Vecteur de distance	15 sauts maximums	30 sec	Inclus des préfixes de routage et les masques de sous réseau dans les informations de routage
IGRP	IGP	Vecteur de distance	Délais, charge, bande passante, fiabilité	90 secondes	Choisi le meilleur chemin selon différent critères. Propriétaires Cisco.
EIGRP	IGP	Hybride	Délais, charge,	Instantanée	Propriétaire Cisco.

			bande passante, fiabilité	à chaque changement topologique	Meilleur convergence et moins de bande passante utilisée.
OSPF	IGP	Etat de lien	Le coût de la route	Instantanée à chaque changement topologique	Utilisé pour les réseaux à grandes échelles
IS-IS	IGP	Etat de lien	Poids du lien	Instantanée à chaque changement topologique	Supporte de multiples protocoles routés tel qu'IP.
BGP	EGP	Vecteur de chemin	Politique réseau, Attribut de chemin		Protocole utilisé par la plupart des ISP et les grandes compagnies.

8.7. Protocole RIPv2

8.7.1 Rappels sur RIPv1

RIPv1 est un protocole de routage intérieur classful, à vecteur de distance qui base ses décisions d'acheminement sur une métrique qui emploie essentiellement le nombre de saut. Le nombre maximum de saut est de 15.

- Il transmet des mises à jour de routage complètes toutes les 30 secondes. D'autre part, il lui faut entre 3 et 5 minutes pour converger. Le tableau suivant récapitule les principales caractéristiques de RIPv.1:
- RIPv1 est un protocole de routage intérieur (IGP), car il ne fonctionne qu'à l'intérieur d'un système autonome.
- C'est est un protocole de routage à vecteur de distance
- Il utilise une métrique basée sur le nombre de saut.
- Toutes les 30 secondes, il diffuse sa mise à jour de routage par broadcast.
- RIPv1 a une convergence lente.
- Il utilise une métrique de mesure infini (maximum hop count), le split horizon ainsi que des compteurs de retenue (hold down timers) mais aussi le route poisoning pour limiter les effets des boucles de routage.
- RIPv1 est un protocole de routage classful et par conséquent ne supporte pas VLSM et CIDR.

8.7.2 Spécifications de RIPv2

RIPv2 est une version améliorée de son prédécesseur et partage donc certaines caractéristiques :

- Tous deux sont des IGP (Interior Gateway Protocol).
- RIPv1 et RIPv2 sont des protocoles de routage à vecteur de distance.
- Ils utilisent une métrique basée sur le nombre de saut.
- Ils emploient un nombre maximum de sauts, des compteurs de retenue dont la valeur est fixé à 180s par défaut, ainsi que le split horizon et le route poisoning pour limiter les effets de boucles de routage.
- Leur configuration est aisée.

RIPv2 apporte également des fonctionnalités supplémentaires tels que :

- Le support du routage classless.

- La diffusion du masque réseau dans les mises à jour de routage.
- Le support de VLSM.
- La diffusion des mises à jour de routage par multicast avec l'adresse de classe D 224.0.0.9.
- L'authentification de la source de la mise à jour de routage par un texte en clair **(actif par défaut)**, ou un texte crypté suivant l'algorithme MD5 (Message-Digest 5).
- L'utilisation d'indicateurs de route externe **(route tag)** afin de pouvoir différencier les routes apprises d'autre protocole de routage et redistribuées dans RIP.

8.7.3 Configuration

a. Commandes générales

- router rip
  - Mode de configuration globale
  - Active le protocole RIP sur le routeur.

- version 2
  - Mode de configuration du protocole de routage
  - Permet d'utiliser RIPv2 à la place de RIPv1

- network {adresse réseau}
  - Mode de configuration du protocole de routage
  - Permet d'indiquer les réseaux utilisant RIP directement connectés au routeur.

- ip default-network {adresse réseau}
  - Mode de configuration globale
  - Permet de spécifier une route par défaut (passerelle).

- default-information originate
  - Mode de configuration du protocole de routage
  - Permet de propager la route par défaut dans les mises à jour de routage.

- no auto-summary
  - Mode de configuration du protocole de routage
  - Désactive l'auto-agrégation.

- Debug ip rip
  - Mode privilégié
  - Affiche les routes apprises par RIP.

b. Authentification

- key-chain {nom}
  - Mode de configuration globale
  - Permet d'identifier un groupe de clef d'authentification (groupe = clef + mot de passe).

- key {id}
  - Mode de configuration de clé
  - Permet de créer une clef dans un groupe de clef. L'identifiant de clef peut prendre une valeur de 0 à 2147483647. Les identifiants de clef peuvent ne pas être consécutifs.

- key-string {mot de passe}
  - Mode de configuration de clé
  - Permet de définir un mot de passe pour une clef.

- ip rip authentication key-chain {nom}
  - Mode de configuration d'interface
  - Active l'authentification RIP sur une interface, en utilisant le groupe de clef spécifié.

- ip rip authentication mode {text | d5}
  - Mode de configuration d'interface
  - Permet de spécifier le type d'authentification en clair ou crypté.

9. CIDR & VLSM

9.1. Introduction au routage Classless

Au début des années 90, Internet subissait une croissance exponentielle annonçant un épuisement des adresses IPv4, notamment celles de classe B, on a cru voire la fin de l'Internet.

Cette pénurie d'adresse est principalement due au découpage fixe de l'espace d'adressage total IPv4 en classes (classe A, classe B, classe C) qui fige le nombre de réseaux possibles et le nombre d'hôtes maximum par réseau ce qui a valu des gaspillages d'adresses considérable sur le réseau public.

En effet, lorsque l'on utilise un **adressage classful,** les masques de sous-réseaux ne sont pas envoyés sur le réseau. Les équipements réseaux utilisent donc des masques de sous-réseaux par défaut qui sont les suivants :

- Classe A : 255.0.0.0 ou /8
- Classe B : 255.255.0.0 ou /16
- Classe C : 255.255.255.0 ou /24

Il est dans ce cas impossible de créer des sous-réseaux et de former des groupes d'utilisateur de différentes tailles au sein d'un réseau d'entreprise.

Ce problème est résolu avec l'utilisation d'un **adressage classless** (sans classe) qui permet d'envoyer le masque de sous-réseau utilisé aux autres équipements et de ce fait, de créer des sous-réseaux de taille variable.

Le CIDR (Classless Inter Domain Routing) et le VLSM (Variable Length Subnet Mask) sont des exemples de procédures utilisant un adressage classless. Bien que complémentaires, celles-ci sont différentes ce qui nécessite une parfaite compatibilité des équipements entre eux.

Il existe cependant des règles à suivre concernant la création et l'utilisation de sous-réseaux. Ces règles sont régies par les RFC 950 (règle du 2^n-2) et RFC 1878 (règles du 2^n-1 et du 2^n) :

- **Règle du 2^n - 2** → impossible d'utiliser le premier sous-réseau ainsi que le dernier sous-réseau
- **Règle du 2^n - 1** → impossible d'utiliser le premier sous-réseau
- **Règle du 2^n** → utilisation de tous les sous-réseaux

L'utilisation d'une de ces règles par rapport à une autre dépend uniquement des capacités techniques des équipements. De nos jours la majorité des réseaux utilisent la règle du 2^n puisqu'elle permet de limiter au maximum le gaspillage d'adresses IP.

9.2. CIDR

L'expansion d'Internet a entraîné l'augmentation de la taille des tables de routage sur de nombreux routeurs, notamment les routeurs des fournisseurs d'accès à Internet.

Pour alléger de manière considérable ces tables de routage, une solution permettant d'agréger plusieurs routes en une seule a dû être mise en place : c'est le principe du **CIDR** (Classless Inter- Domain Routing).

Pour ce faire, une comparaison binaire de l'ensemble des adresses à agréger est nécessaire. Il faut en effet arriver à déterminer les bits de la partie réseau qui sont en commun dans toutes ces adresses et mettre à zéro tous les bits restant.

De cette manière une délimitation entre la partie réseau commune et le reste de l'adresse sera effectuée. Celle-ci permettra de déterminer l'adresse agrégée ainsi que le nouveau masque de sous- réseau à utiliser.

L'exemple suivant illustre l'utilisation d'une agrégation de quatre adresses réseaux en une seule adresse. Il faut en effet agréger les 4 réseaux ci-dessous :

- 10.3.4.0 255.255.255.0 (ou /24)
- 10.3.5.0 255.255.255.0 (ou /24)
- 10.3.6.0 255.255.255.0 (ou /24)
- 10.3.7.0 255.255.255.0 (ou /24)

Processus d'agrégation (ou summarization) de routes en une seule :

Adresses réseaux :
10.3.4.0 - 00001010 . 00000011 . 00000100 . 00000000
10.3.5.0 - 00001010 . 00000011 . 00000101 . 00000000
10.3.6.0 - 00001010 . 00000011 . 00000110 . 00000000
10.3.7.0 - 00001010 . 00000011 . 00000111 . 00000000

Nouveau masque : 255.255.252.0 - 11111111 . 11111111 . 11111100 . 00000000

Nouvelle route agrégée : 10.3.4.0 255.255.252.0 (ou /22)

Cependant l'emploi de CIDR n'est possible que si :

- Le protocole de routage utilisé transporte les préfixes étendus dans ses mises à jour.
- Les routeurs implémentent un algorithme de la correspondance la plus longue.
- Un plan d'adressage hiérarchique est appliqué pour l'assignation des adresses afin que l'agrégation puisse être effectuée.
- Les hôtes et les routeurs supportent le routage classless.

9.3. VLSM

L'utilisation du masque de sous-réseau à taille variable (**V**ariable **L**ength **S**ubnet **M**ask) permet à un réseau classless d'utiliser différents masques de sous-réseaux au sein d'une organisation et d'obtenir par conséquent des sous-réseaux plus appropriés aux besoins.

Cependant, certaines conditions sont requises pour utiliser le VLSM :

- Il est nécessaire d'employer un protocole de routage supportant le VLSM. **RIPv.2**, **OSPF**, **IS-IS**, **EIGRP, BGP** ainsi que le **routage statique** supportent VLSM. Les protocoles de routage classless, contrairement aux protocoles de routage classful (RIPv.1, IGRP), transmettent dans leurs mises à jour de routage, le masque de sous-réseau pour chaque route.

- Les routeurs doivent implémenter un algorithme de la correspondance la plus longue. En effet, les routes qui ont le préfixe le plus élevé sont les plus précises. Les routeurs dans leurs décisions d'acheminement doivent être capables de déterminer la route la plus adaptée aux paquets traités.

- Un plan d'adressage hiérarchique doit être appliqué pour l'assignation des adresses afin que l'agrégation puisse être effectuée.

VLSM repose sur l'agrégation. C'est-à-dire que plusieurs adresses de sous-réseaux sont résumées en une seule adresse. L'agrégation est simple, l'on retient simplement la partie commune à toutes les adresses des sous-réseaux.

Pour conceptualiser un réseau conforme VLSM, il faut:

- Recenser le nombre total d'utilisateurs sur le réseau (prévoir une marge pour favoriser l'évolutivité du réseau).
- Choisir la classe d'adresse la plus adaptée à ce nombre.
- Partir du plus haut de l'organisation (couche principale) et descendre au plus près des utilisateurs (couche accès).
- Décompter les entités au niveau de chaque couche. Par exemple, les grandes agglomérations, avec pour chaque agglomération, les villes, le nombre de bâtiments dans chaque ville, le nombre d'étages par bâtiment et le nombre d'utilisateur par étage.
- Pour chacune de ces entités, réserver le nombre de bits nécessaire en prévoyant l'évolutivité du réseau.
- Calculer le masque de sous-réseau à chaque niveau de l'organisation.

9.4. Procédure de réalisation

Les procédures de réalisation de plan d'adressage avec du VLSM symétrique puis asymétrique sont expliquées. Néanmoins, il faut savoir que le VLSM symétrique n'est qu'une étude de cas scolaire et que le VLSM asymétrique est ce qui est réellement utilisé dans la réalité.

9.4.1. VLSM Symétrique

Le VLSM symétrique est un plan d'adressage qui fait un découpage récursif du la topologie du réseau de l'entreprise sachant que les différents découpages sont similaires.
Exemple : si l'entreprise a deux bâtiments par ville, on devra avoir deux bâtiments dans chaque ville.

Dans cette procédure, on parle de sous réseau uniquement pour les parties les plus proches des utilisateurs. Tous les autres niveaux de la hiérarchie seront considérés comme une adresse agrégée.

Procédure :

- Etape 1 : Identifier le besoin

Recenser les différents niveaux hiérarchiques de l'entreprise et dessiner la topologie.

- Etape 2 : Au niveau utilisateur

Connaître la taille du sous-réseau.

- Etape 3 : Recensement

Déterminer le nombre de bits nécessaires pour recenser chaque instance du niveau hiérarchique.

- Etape 4 : Classe d'adresse utilisée

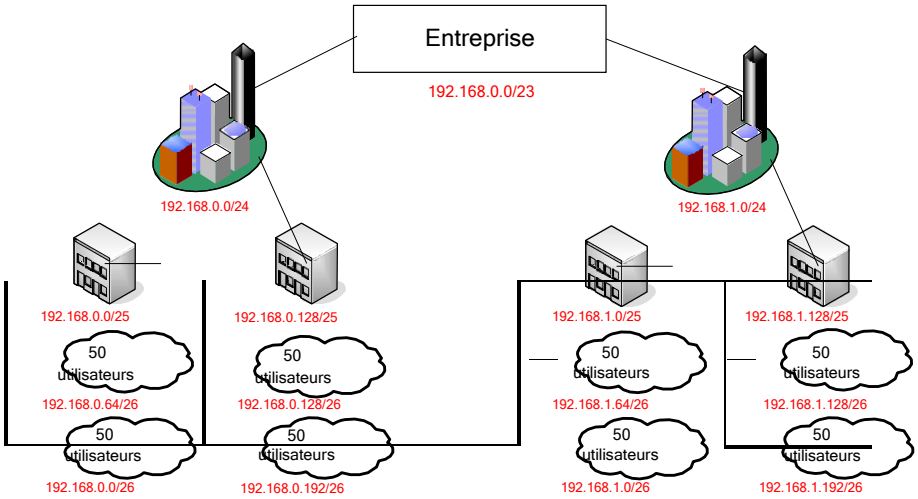
Déterminer la classe d'adresse ou l'agrégat d'adresses (le choix dépendant du contexte), en additionnant tous les bits nécessaires pour identifier chaque niveau hiérarchique de l'entreprise.

- Etape 5 : Découpage et attribution des sous-réseaux

On procède ensuite au découpage de la classe d'adresse de l'entreprise et de l'attribution à chaque instance du niveau hiérarchique.

Cette procédure est valable quelque soit la méthode d'adressage utilisée (RFC 950 ou 1878) à une différence prêt, si on applique la règle du 2^n-1 ou 2^n-2, il faudra l'appliquer une seule fois sur toute la topologie au niveau hiérarchique limitant la perte (induit par le nombre de bits de ce niveau hiérarchique).

Exemple :



Etape 1 : Une entreprise dans deux villes. Deux bâtiments par ville. Deux étages par bâtiment. 50 utilisateurs par étage.

Etape 2 : 50 utilisateurs / sous-réseau +1 adresse pour le broadcast +1 adresse pour le réseau +1 adresse pour la passerelle = 53 adresses IP.

Etape 3 : 2^x >=53 x=6 Il faut donc 6 bits par sous-réseau soit un /26 (255.255.255.192)

Etape 4 : Dans ce contexte, on peut découper une classe B (beaucoup de gaspillage) ou agréger plusieurs classe C. On choisira une classe C

Etape 5 : Chaque instance du niveau hiérarchique se voit attribuer un préfixe et un masque. (en rouge sur le dessin)

9.4.2. VLSM Asymétrique

Le VLSM Asymétrique, ou plus simplement, VLSM, correspond à une topologie d'entreprise ou les différents niveaux hiérarchiques et les instances ne sont pas similaires (nombre, taille etc.)

Procédure :

- Etape 1 : Identifier le besoin

Dessiner la topologie, identifier les besoins a chaque niveau hiérarchique.

- Etape 2 : Recensement

Connaître le nombre d'utilisateurs pour chaque sous-réseau (puisqu'ils peuvent être différents à chaque niveau maintenant), ce qui revient à connaître la taille de chaque sous-réseau (ne pas oublier qu'on ne peut pas utiliser la première ni la dernière adresse et qu'il faut une adresse IPpour la passerelle).

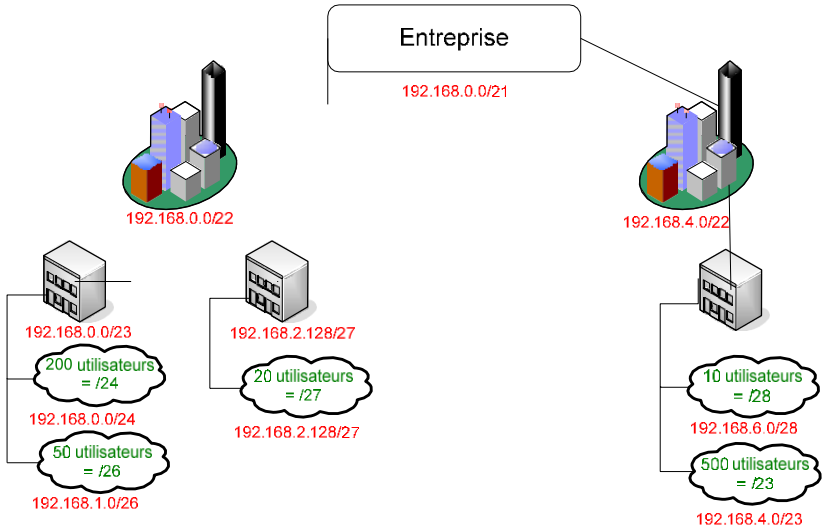
Si le nombre d'utilisateur n'est pas connu a chaque niveau de la hiérarchie, on peut suivre un processus descendant ('top down') : repartir équitablement le nombre d'utilisateur pour un niveau hiérarchique supérieur vers le niveau directement inférieur.

- Etape 3 : Classe d'adresse utilisée

Déterminer la classe d'adresse ou l'agrégat d'adresses (le choix dépendant du contexte), en additionnant tous les bits nécessaires pour identifier chaque niveau hiérarchique de l'entreprise.

- Etape 4 : Détermination des aggrégats

En suivant un processus remontant récursif maintenant, on va agréger les différents instances d'un niveau pour obtenir l'identifiant réseau du niveau hiérarchique directement supérieur jusqu'a obtenir l'adresse agrégée de toute l'entreprise.



Etape 1 : Une entreprise dans deux villes. Deux bâtiments dans la première ville, un seul bâtiment dans la deuxième ville. Tous les bâtiments ont deux étages sauf un qui en a qu'un seul. Le nombre d'utilisateur varie d'un étage a l'autre.

Etape 2 : Recensement (en vert). Ne pas oublier l'adresse pour le broadcast, l'adresse pour le réseau et l'adresse pour la passerelle.

Etape 3 : Dans ce contexte, on peut découper une classe B (beaucoup de gaspillage) ou agréger plusieurs classe C. On choisira une classe C

Etape 4 : En remontant, on adresse chaque étage, chaque bâtiment etc. (en rouge)

Le VLSM permet en effet d'éviter le gaspillage d'adresse au sein d'une organisation en utilisant des masques de taille variable, tandis que le CIDR permet de diminuer significativement le nombre d'entrées des tables de routage en utilisant des agrégations de routes.

9.4.3. Configuration

Lorsque la règle du 2^n-1 est appliquée, il est convenu de ne pas utiliser le premier sous-réseau pour éviter toute confusion. En effet, l'adresse réseau du premier sous-réseau correspond à l'adresse réseau de toute la plage d'adresse.

Pour limiter le gaspillage d'adresse, en utilisant la règle du 2^n, il suffit d'utiliser la commande **ip subnet-zero** qui permet l'utilisation du premier sous-réseau calculé. Cette fonctionnalité est active par défaut depuis la version 12.0 de l'IOS.

- ip subnet-zero
  - Mode de configuration globale
  - Permet d'utiliser le premier sous-réseau (2^n)

Par ailleurs, la commande **ip classless** active la prise en charge des informations ne respectant pas le découpage d'adresses en classes. C'est-à-dire qu'elle permet d'activer le support des masques de sous-réseau et d'une route par défaut. Cette commande est active par défaut.

- ip classless
  - Mode de configuration globale
  - Permet d'activer le support des masques de sous-réseau et d'une route par défaut

Lors de l'emploi du VLSM, il faut avant tout s'assurer du bon calcul des masques de sous-réseaux. Une fois cette étape effectuée nous pouvons configurer les interfaces.

- interface {type} {numéro}
  - Mode de configuration globale
  - Permet de passer dans le mode de configuration d'interface

- ip address {IP} {masque}
  - Mode de configuration d'interface
  - Permet d'attribuer une adresse IP à cette interface

10. Les VLANs

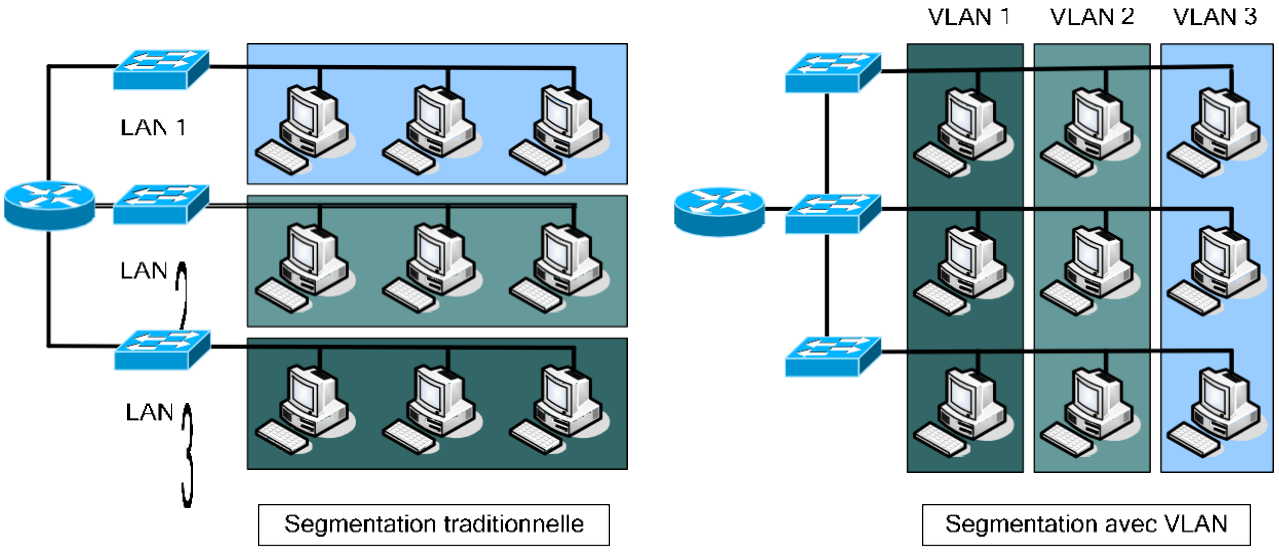
10.1. Concepts des VLANs

10.1.1. Définitions et principes

Un LAN virtuel est un ensemble logique d'unités regroupées en domaine de broadcast quelque soit l'emplacement de leur segment physique. Ils peuvent être regroupés en fonction du service auxquels ils appartiennent, des applications utilisées, des protocoles, etc.

Les principales différences entre la commutation traditionnelle et les LAN virtuels sont:

- Les LAN virtuels fonctionnent au niveau des couches 2 et 3 du modèle OSI.
- La communication inter LAN virtuels est assurée par le routage de couche 3.
- Les LAN virtuels fournissent une méthode de contrôle des broadcasts.
- Les LAN virtuels permettent d'effectuer une segmentation selon certains critères:
  - Des collègues travaillant dans le même service.
  - Une équipe partageant le même applicatif.
- Les LAN virtuels peuvent assurer la sécurité des réseaux en définissant quels nœuds réseaux peuvent communiquer entre eux, en restreignant le nombre d'utilisateurs dans un Vlan.
- Les LAN virtuels empêchent d'autres utilisateurs d'accéder au réseau s'ils n'ont pas été autorisés



Il est donc possible de segmenter le réseau en plusieurs domaines de broadcast afin d'en améliorer les performances.

On distingue 2 méthodes de création pour les LAN virtuels :

10.1.2. LAN statique

Pour la mise en place de ces LANS virtuels, nous allons avoir besoin d'utiliser des commutateurs gérant l'utilisation des VLANs. Il faut savoir que par défaut tous les ports du commutateur sont présents dans un VLAN d'administration qui est le VLAN1 par défaut. On ne peut ni le supprimer ni le renommer.

Les VLANs statiques sont dits "accès sur les ports". L'appartenance à un VLAN est en effet fonction du port sur lequel est connecté un utilisateur. La configuration des commutateurs se fait donc en attribuant un port à un VLAN.

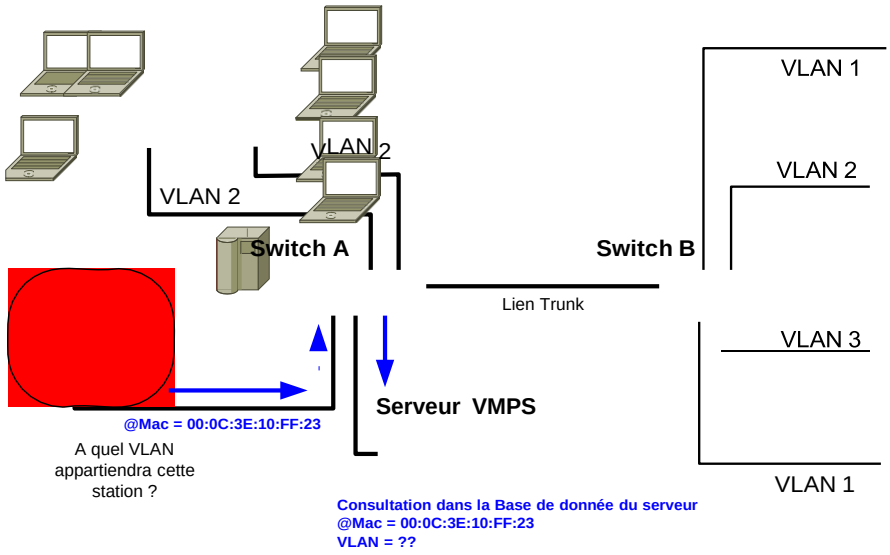
10.1.3. LAN dynamique

Dans cette configuration, l'appartenance à un VLAN est déterminée par une information de couche supérieure : 2 ou plus (corrélation de couche>=2 <-> VLAN). Typiquement, on peut baser l'appartenance à un VLAN en fonction de l'adresse MAC de l'utilisateur.

Cette configuration nécessite un logiciel d'administration réseau (ex : CiscoWorks 2000) basé sur un serveur. Lors de la connexion d'un hôte au commutateur, ce dernier enverra une requête au serveur lui indiquant, par exemple, l'adresse MAC du nouvel hôte connecté.

Le serveur, grâce à une base de donnée liant MAC et VLAN (remplie par l'administrateur), renverra alors au commutateur le VLAN d'appartenance de l'hôte concerné.

Cela nécessite donc que la base de donnée du serveur soit régulièrement mise à jour et que le parc informatique dispose d'une bande passante pour faire véhiculer le trafic.



10.1.4. Commandes générales

- vlan database
  - Mode privilégié
  - Permet d'accéder au mode de configuration de VLAN.

- vlan vlan_id [name { nom du vlan }]
  - Mode de configuration des VLAN (vlan database)
  - Permet de créer et nommer les VLANs.

- switchport mode {access | dynamic {auto | desirable} | trunk}
  - Mode de configuration d'interface
  - Permet de configurer une interface pour le trunking ou pour un VLAN.

- switchport access vlan vlan-id
  - Mode de configuration d'interface
  - Permet de configurer un VLAN statique sur une interface.

- Configurer un VLAN statique
  - Entrez dans le mode de configuration de VLAN à l'aide de la commande **vlan database**.
  - Créez le VLAN avec la commande **vlan** {vlan number}.
  - Entrez dans le mode de l'interface que vous souhaitez associer au VLAN.
  - Spécifiez le mode du port pour un VLAN : **switchport mode access**.
  - Spécifiez le VLAN avec la commande **switchport access vlan** vlan-id.

- Sauvegarder la configuration VLAN
  - Les configurations de VLAN sont automatiquement sauvegardées dans la flash dans le fichier **vlan.dat**.

10.1.5. Commandes de débogages

- show interfaces [interface-id | vlan vlan-id] [switchport | trunk]
  - Affiche les statuts du trunking.

- show vlan [brief | id vlan-id | name vlan-name | summary]
  - Liste les informations sur le VLAN.

- show vlan [vlan]
  - Affiche des informations sur le VLAN.

- show spanning-tree vlan vlan-id
  - Affiche les informations spanning-tree pour le VLAN spécifié.

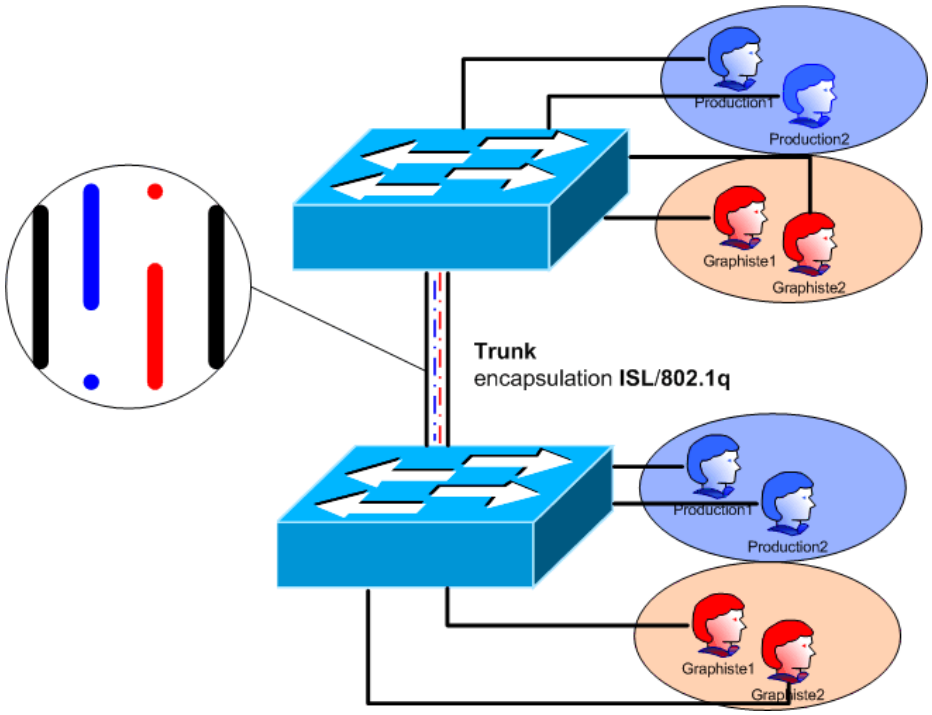
10.2. Trunking

10.2.1. Principes du trunking

Le trunking permet, dans des réseaux comportant plusieurs commutateurs, de transmettre à un autre commutateur via un seul port et un seul média, le trafic de plusieurs VLAN dont les membres sont dispatchés sur plusieurs commutateurs. Le problème étant que différents trafics isolés (de différents VLAN) doivent emprunter un seul câble.

On a donc plusieurs trafics logiques sur une liaison physique : on appelle cette notion un trunk.

Afin d'identifier l'appartenance des trames à leurs VLAN respectifs, on utilise un système d'étiquetage (ou encapsulation) sur ce lien.



Il en existe deux protocoles :

- **ISL** (Inter Switch Link) qui est un protocole propriétaire Cisco.
- **802.1q** qui est un standard de l'IEEE.

10.2.2. Le protocole ISL

Cisco avait développé bien avant l'IEEE son protocole ISL. ISL étant un protocole propriétaire Cisco, il ne peut être appliqué qu'à des commutateurs Cisco.

Avec l'emploi d'ISL, la trame originelle est encapsulée entre un en-tête de 26 octets et un en-queue de 4 octets.

Trame ISL

En-tête ISL 26 octets	Trame Ethernet encapsulée	FCS 4 octets

Composition de l'en-tête ISL

DA 40 bits	Type 4 bits	Util. 4 bits	SA 48 bits	LEN 16 bits	AAAA03 24 bits	HSA 24 bits	VLAN 16 bits	BPDU 1 bit	INDEX 16 bits	RES 16 bits

- DA : Adresse multicast de destination qui prend la valeur 0x01-00-0C-00-00 ou 0x03-00-0C-00-00.
- Type : Indique le type de trame (Ethernet, Token Ring, etc.).
- Util : Indique la priorité de traitement de la trame.
- SA : Adresse MAC source.
- LEN : Longueur de la trame encapsulé moins les 18 bits des champs DA, Type, Util., SA, LEN et FCS.
- AAAA03 : Champ SNAP d'une valeur fixe 0xAAAA03.
- HSA : Contient la portion constructrice de l'adresse MAC source.
- VLAN : Identifiant de VLAN.
- BPDU : Utilisé par l'algorithme Spanning Tree pour déterminer les informations topologiques.
- INDEX : Employé à des fins diagnostiques uniquement.
- RES : Utilisé quand une trame Token Ring ou FDDI est encapsulé dans une trame ISL.

10.2.3. Protocole 802.1q

Contrairement à ISL le protocole développé par L'IEEE 802.1q n'encapsule pas la trame Ethernet originale, mais insère un en-tête additionnel de 4 octets qui contient un champ d'identification du VLAN.

Le champ de contrôle de trame (FCS) doit être recalculé à cause de l'ajout de l'en-tête additionnel.

Trame Ethernet avec 802.1q.

Dest	Src	Etype	Tag	Long/Type Ether	Données	FCS

En-tête Tag.

Priorité		ID VLAN

- Comparaison entre ISL et IEEE 802.1q

ISL	IEEE 802.1q
Encapsule la trame d'origine	Ajoute un en-tête additionnel à la trame d'origine
Comporte un champ d'identification de VLAN de 12 bits	
Utilisation de PVST (Per VLAN Spanning Tree) pour obtenir un arbre STP par VLAN	

10.2.4. Commandes associées

- switchport mode trunk
  - Mode de configuration d'interface
  - Active le mode « Trunking » sur l'interface

- switchport trunk [allowed | encapsulation | native | pruning]
  - Mode de configuration d'interface
  - Autorise la transport du trafic de certain VLAN sur le lien « trunk »
  - Spécifie le type d'encapsulation (ISL, 802.1q)
  - Permet d'activer le « Pruning » des VLAN (Pruning : le commutateur ne transmet pas la trame sur le trunk si le commutateur à l'autre bout n'est pas configuré pour le VLAN ciblé)

- show port capabilities [numéro/sous-numéro]
  - Mode privilégié
  - Affiche les fonctionnalités supportées par l'interface.

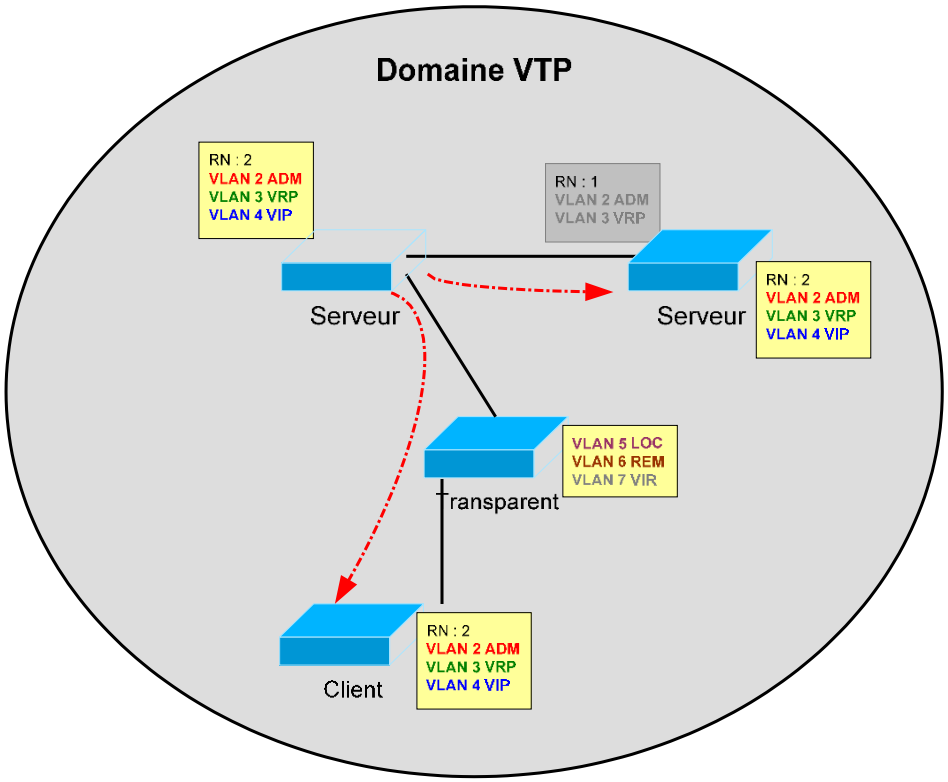
- show interface trunk
  - Mode privilégié
  - Permet de vérifier la configuration du « trunking ».

10.3. VTP

10.3.1. Principes du VTP

VTP (VLAN Trunking Protocol), protocole propriétaire Cisco permet, aux commutateurs qui l'implémentent, d'échanger des informations de configuration des VLAN.

Il permet donc de redistribuer une configuration à d'autres commutateurs, évitant par la même occasion à l'administrateur de faire des erreurs, en se trompant par exemple de nom de VLAN. VTP diffuse ses mises à jour au sein du domaine VTP toutes les 5 min ou lorsqu'une modification a lieu.



Les mises à jour VTP comportent:

- Un numéro de révision (**Revision Number**) qui est incrémenté à chaque nouvelle diffusion. Cela permet aux commutateurs de savoir s'ils sont à jour.
- Les noms et numéro de VLAN.

Dans un domaine VTP, on distingue une hiérarchie comprenant trois modes de fonctionnement :

- VTP **serveur**
- VTP **client**
- VTP **transparent**

10.3.2. Les modes VTP

Les commutateurs qui font office de serveur VTP peuvent créer, modifier, supprimer les VLAN et d'autres paramètres de configuration. Ce sont eux qui transmettront cette configuration aux commutateurs en mode client (ou serveur) dans leur domaine VTP.

Les commutateurs fonctionnant en mode client ne peuvent que recevoir et transmettre les mises à jour de configuration.

Le mode transparent, lui, permet aux commutateurs de ne pas tenir compte des mises à jour VTP. Ils sont autonomes dans le domaine VTP et ne peuvent configurer que leurs VLAN (connectés localement). Cependant, ils transmettent aux autres commutateurs les mises à jour qu'ils reçoivent.

Les commutateurs en mode serveur et client mettent à jour leur base de données VLAN, si et seulement si, ils reçoivent une mise à jour VTP concernant leur domaine et contenant un numéro de révision supérieur à celui déjà présent dans leur base.

Fonction	Mode Serveur	Mode Client	Mode Transparent
Envoi de messages VTP	OUI	NON	NON
Réception des messages VTP ; Synchronisation VLAN	OUI	OUI	NON
Transmission des messages VTP reçus	OUI	OUI	OUI
Sauvegarde de configuration VLAN (en NVRAM ou Flash)	OUI	NON	OUI
Edition des VLANs (création, modification, suppression)	OUI	NON	OUI

Lorsqu'un hôte d'un VLAN envoie un broadcast, celui-ci est transmit à tous les commutateurs du domaine VTP. Il peut arriver que dans ce domaine, des commutateurs n'ait pas le VLAN concerné sur un de leur port.

Ce broadcast leur est alors destiné sans aucune utilité. Le **VTP pruning** empêche la propagation de ces trafics de broadcast aux commutateurs qui ne sont pas concernés.

10.3.3. Commandes associées

- vlan database
  - Mode privilégié
  - Permet d'accéder au mode de configuration de VLAN.

- vlan vlan_id [name { nom du vlan }]
  - Mode de configuration de VLAN
  - Permet de créer et nommer les VLANs.

- vtp domain nom de domaine { password mot de passe | pruning | v2-mode | {server |client | transparent}}
  - Mode de configuration de VLAN
  - Spécifie les paramètres VTP.

- show vtp status
  - Mode privilégié
  - Affiche la configuration VTP et le statut

11. Les ACLs

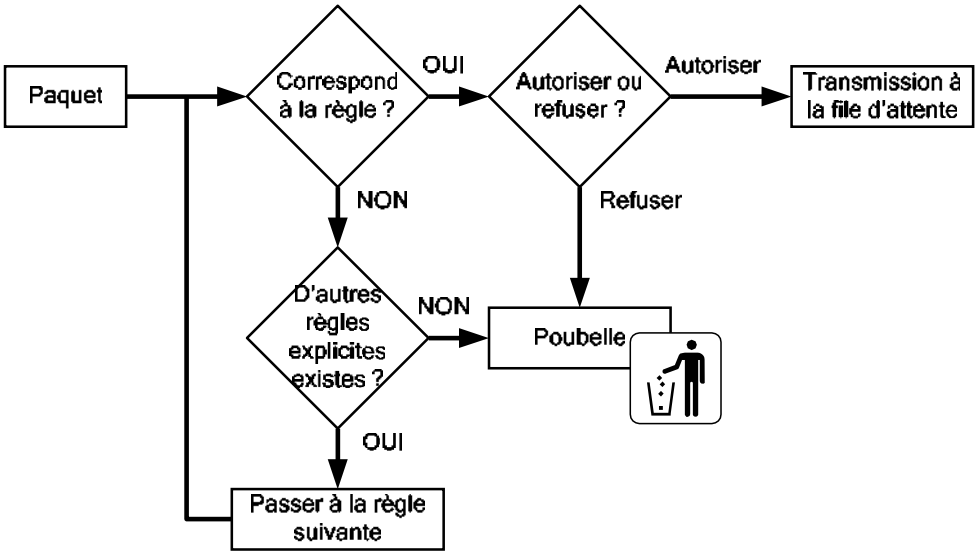
11.1. Théorie

11.1.1. Principe fondamental

Une ACL (Access Control List) est une liste séquentielle de critères utilisée pour du filtrage des paquets. Les ACLs sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie.

Cette liste est parcourue de la première à la dernière instruction jusqu'à trouver une correspondance. Si le paquet répond aux critères d'une instruction, le reste des instructions est ignoré et le paquet est autorisé ou refusé. Si aucune correspondance n'est trouvée dans les critères explicités par l'administrateur, le paquet est implicitement supprimé.

Il ne peut y avoir qu'une seule ACL par protocole, par interface et par direction (entrée/sortie).



Parcours des instructions d'une ACL

Les ACLs permettent ainsi d'autoriser ou d'interdire des trafics en fonctions de critères tels que les adresses sources et destinations, les protocoles utilisés et les numéros de ports.

Une ACL est identifiable par son numéro ou son nom, attribué suivant le protocole et le type :

- ACL standard (numérotée)
- ACL étendue (numérotée)
- ACL nommée (peut être de type standard ou étendue)

Plage de numéros	Type d'ACL associé
1 à 99 et 1300 à 1999	Standard pour IP
100 à 199 et 2000 à 2699	Etendue pour IP
600 à 699	AppleTalk
800 à 899	Standard pour IPX
900 à 999	Etendue pour IPX
1000 à 1099	IPX/SAP

L'avantage principal des ACLs est donc de fournir une base de sécurité réseau en filtrant les trafics traversant un routeur.

Le principal inconvénient est malheureusement un traitement supplémentaire à effectuer pour chaque paquet entrant et/ou sortant du routeur, rallongeant ainsi à la latence réseau et à la surcharge CPU.

La configuration des ACLs se fait en deux parties distinctes, à savoir :
- Création de l'ACL
- Application de l'ACL sur une interface réseau

Quelques précautions sont à prendre en compte lors de la configuration ou de l'utilisation des ACLs :
- Les instructions sont toujours parcourues de la première à la dernière, jusqu'à correspondance des critères.
- Si aucune instruction ne correspond au paquet, la dernière instruction implicite indique alors de supprimer ce paquet.
- Une ACL appliquée sur une interface mais dont les instructions ne sont pas configurées n'a pour seule instruction que la dernière qui bloque tout. Tout trafic serait alors interdit.
- Lors de la création des instructions, il faut toujours procéder du plus précis (exceptions) jusqu'au plus générique.
- Une ACL IP qui interdit un paquet enverra automatiquement un message ICMP Host Unreachable.
- Une ACL pour un trafic sortant n'affecte pas le trafic originaire du routeur local.

11.1.2. Masque générique

Les instructions utilisées dans les ACLs utilisent les masques génériques (Wildcard Mask) conjointement à des préfixes réseaux pour identifier des plages d'adresses.

Un masque générique est une valeur 32 bits noté sous la forme décimale pointée (comme les IP et les masques de sous-réseaux), sachant que :
- **"0" binaire** : Doit correspondre
- **"1" binaire** : Peut varier

On observe donc qu'un masque générique est l'inverse binaire d'un masque de sous-réseaux, ou, du point de vue décimal pointé, est le complément à 255 du masque de sous-réseau correspondant :

Masque de sous-réseau	**1111 1111.1111 1111.1110 000.0000 0000**
Masque générique	**0000 0000.0000 0000.0001 111.1111 1111**

```
   255 . 255 . 224 .  0   (Masque de sous-réseau(
+    0 .   0 .  31 . 255   (Masque générique(
=  255 . 255 . 255 . 255
```

Par conséquent, un masque générique ne peut prendre que ces valeurs (pour chaque octet) :

0	1	3	7	15	31	63	127	255

Au niveau syntaxique, deux masques génériques précis (les deux extrêmes, à savoir tout ou rien) peuvent s'écrire normalement, sous la forme préfixe/masque générique, ou sous une forme plus conviviale. Ces deux exceptions d'écriture sont les suivantes :
- **{IP} {0.0.0.0}** = **host {IP}**
- **{IP} {255.255.255.255}** = **any**

11.2. ACL standard

Une ACL standard permet d'autoriser ou d'interdire des adresses spécifiques ou bien un ensemble d'adresses ou de protocoles, sachant que, dans les instructions d'une ACL standard, on ne peut indiquer que des adresses sources.

Ce sont les ACLs les plus simples et, par conséquent, les moins gourmandes en ressources CPU. Elles sont par exemple utilisées pour autoriser ou interdire toute une plage d'adresses réseaux ou encore pour le filtrage des informations contenues dans des mises à jour de routage.

Pour configurer une instruction pour une ACL standard pour IP, il faut utiliser la commande suivante :

- **access-list {numéro} {permit | deny} {préfixe} [masque générique] [log]**

- **access-list {numéro} {remark} {commentaire}**
  - Mode de configuration globale
  - Si le masque générique n'est pas précisé, le masque générique par défaut 0.0.0.0 est utilisé.
  - **log** permet de garder en mémoire le nombre de paquets correspondant à l'instruction en cours.
  - Le mot clé **remark** suivi d'un commentaire permet d'indiquer l'utilité de l'instruction.

L'ordre de parcours des instructions dépend de l'ordre dans lequel on a configuré les instructions. Une nouvelle instruction est donc obligatoirement ajoutée à la fin de la liste, et il est impossible de supprimer une instruction particulière.

Pour toute modification, il est donc conseillé d'utiliser un éditeur de texte, de copier la liste des instructions de l'ACL devant être modifiée, de supprimer cette ACL sur le routeur, d'éditer les instructions pour faire lesmodifications voulues puis de les insérer dans le routeur.

11.3. ACL étendue

Une ACL étendue permet de faire un filtrage plus précis qu'une ACL standard. En effet, une ACL étendue permet de filtrer en fonction de :

- Protocole utilisé (couche 3 et 4)
- Adresse source
- Adresse de destination
- Numéro de port

La commande permettant de configurer une ACL étendue pour IP est :

- **access-list {numéro} {permit | deny} {protocole} {préfixe source} {masque source} [{opérateur} {opérande}] {préfixe destination} {masque destination} [{opérateur} {opérande}] [icmp-type] [log][established]**

- **access-list {numéro} {remark} {commentaire}**
  - Mode de configuration globale
  - **protocole** peut être soit le nom (IP, TCP, UDP, ICMP, IGRP, etc.) soit le numéro du protocole (de 0 à 255).
  - Le couple **opérateur**/**opérande** est pour les numéros de ports TCP ou UDP uniquement, et peut être spécifié pour la source et/ou pour la destination :

Opérateur	Signification
eq	Egal à
neq	Différent de
lt	Inférieur à
gt	Supérieur à
range	Entre (nécessite 2 numéros de port)

  - Le paramètre **icmp-type** ne peut être utilisé que pour le protocole ICMP, et correspond au nom ou au numéro du type de message ICMP devant être vérifié.
  - Le paramètre **established** ne peut être utilisé que pour le protocole TCP et permet de faire correspondre uniquement les sessions TCP déjà établies (drapeaux ACK, FIN, PSH, RST, SYN ou URG).

Pour l'ordre de parcours ou la modification, les règles sont les mêmes qu'avec une ACL standard.

11.4. ACL nommée

Depuis la version 11.2 d'IOS, il est possible d'utiliser les ACLs nommées. Les ACLs nommées permettent l'identification par des chaînes alphanumériques plutôt que par la représentation numérique actuelle.

Une ACL nommée peut être de type standard ou étendue.

Deux nouveaux modes de configuration sont donc étudiés :

Mode de configuration	Invite de commande associée
ACL nommée standard	(config-std-nacl)#
ACL nommée étendue	(config-ext-nacl)#

Les ACLs nommées permettent :
- D'identifier intuitivement les listes de contrôle d'accès à l'aide d'un code alphanumérique.
- De supprimer une instruction particulière sans avoir à tout supprimer et réécrire.

Les commandes suivantes permettent de configurer une ACL nommée :
- **ip access-list {standard | extended} {nom}**
  - Mode de configuration globale
  - Permet de créer une ACL nommée standard ou étendue
  - Permet de passer dans le mode de configuration de l'ACL nommée

    - **{permit | deny} {préfixe} [masque] [log]**
  - Mode de configuration d'ACL nommé standard
  - Les paramètres sont identiques que pour une ACL standard numérotée.

- **{permit | deny} {protocole} {préfixe source} {masque source} [{opérateur} {opérande}] {préfixedestination} {masque destination}[{opérateur} {opérande}] [icmp-type] [log] [established]**
  - Mode de configuration d'ACL nommée étendue
  - Les paramètres sont identiques que pour une ACL étendue numérotée

- **remark {commentaire}**
  - Mode de configuration d'ACL nommée (standard ou étendue)
  - Fournit un commentaire pour indiquer l'utilité de l'ACL

11.5. Mise en place et vérification des ACLs

La création des ACLs étant faite, il faut maintenant les appliquer en utilisant les commandes suivantes :

- **ip access-group {numéro | nom} {in | out}**
  - Mode de configuration d'interface
  - Applique une ACL (standard, étendue ou nommée) sur l'interface pour filtrer le trafic entrant ousortant

- **access-class {numéro | nom} {in | out}**
  - Mode de configuration de ligne
  - Applique une ACL sur la ligne pour filtrer les accès à cette dernière

- **no access-list {numéro}**
  - Mode de configuration globale
  - Supprime complètement une ACL numérotée

Les commandes suivantes servent à vérifier le placement des ACLs, ainsi que leurs instructions :

- **show access-lists [numéro | nom]** : Affiche la liste des ACLs créées sur le routeur, leurs instructions ainsique le nombre de correspondance pour chaque instruction

- **show ip interface [{type} {numéro}]** : Permet entre autres de voir quelles sont les ACLs appliquées sur lesinterfaces et pour quelle direction

Placement d'une ACL en fonction de son type

Parce que les ACLs standards ne permettent que de filtrer en fonction d'adresses sources, il faut les placer au plus près de la destination, et inversement pour les ACLs étendues qui doivent toujours être placées au plus près de la source.

De plus, les ACLs standards, interdisant intégralement un trafic pour une source donnée, bloquent implicitement le trafic dans le sens opposé (explicitement bloqué de la source vers la destination et implicitement bloqué de la destination à la source).

12. Couche 4 : Couche transport

12.1. Introduction

Nous avons vu dans les chapitres précédents comment TCP/IP envoie les informations de l'émetteur au destinataire. La couche transport ajoute à ce mécanisme la notion de « qualité de service », à savoir la garantie d'un acheminement fiable des informations au travers du réseau.

12.2. TCP et UDP

La pile de protocoles TCP/IP comprend 2 protocoles de couche 4 : TCP et UDP

TCP est un protocole orienté connexion, c'est-à-dire qu'il associe au transport des informations la notion de qualité en offrant les services suivants :

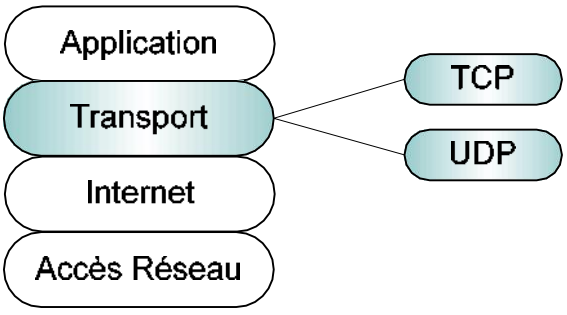
- Fiabilité
- Division des messages sortants en segments
- Ré assemblage des messages au niveau du destinataire
- Ré envoi de toute donnée non reçue

Segments : PDU de couche 4

UDP est lui un protocole non orienté connexion, c'est-à-dire qu'il n'offre pas de fonction de contrôle du bon acheminement :

- Aucune vérification logicielle de la livraison des messages
- Pas de réassemblage des messages entrants
- Pas d'accusé de réception
- Aucun contrôle de flux

Cependant, UDP offre l'avantage de nécessiter moins de bande passante que TCP. Il peut donc être intéressant d'utiliser ce protocole pour l'envoi de messages ne nécessitant pas de contrôle de qualité.



12.2.1. Numéros de ports

Afin que plusieurs communications puissent circuler en même temps, TCP et UDP utilisent des numéros de ports. Des conventions ont été établies pour des applications :

Protocole	nº de port	Description
FTP data	20	File Transfer (données par défaut)
FTP	21	File Transfer (contrôle)
SSH	22	Secure SHell
Telnet	23	Telnet
SMTP	25	Simple Mail Transfer
DNS	53	Domain Name System
HTTP	80	World Wide Web HTTP
POP3	110	Post Office Protocol - Version 3
NNTP	119	Network News Transfer Protocol
IMAP2	143	Interactive Mail Access Protocol v2
NEWS	144	News
HTTPS	443	Protocole HTTP sécurisé (SSL)

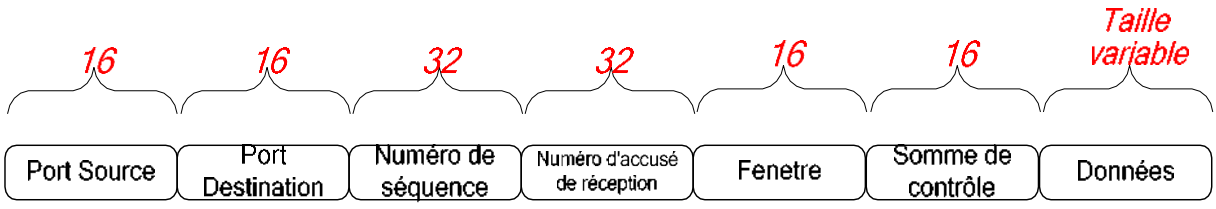
Numéros de ports

Les ports sont attribués de la manière suivante :

Plage de ports	Utilisation
0 à 1023	réservés aux applications publiques
1023 à 65535	attribué aux entreprises pour les applications commerciales et utilisé par le système d'exploitation pour l'attribution dynamique des ports source.

12.2.2. Structures d'un segment TCP

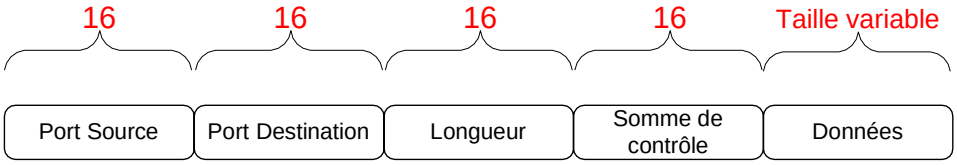
Le protocole TCP encapsule les informations provenant de la couche supérieure dans des segments dont voici les principales informations :



Champs	Descriptions
Port source	Numéro du port appelant
Port de destination	Numéro du port appelé
Numéro de séquence	Numéro utilisé pour assurer le séquençage correct des données entrantes
N° d'accusé de réception	Prochain octet TCP attendu
Somme de contrôle	Somme de contrôle calculée des champs d'en-tête et de données
Données	Données du protocole de couche supérieure

12.2.3. Structure d'un datagramme UDP

UDP étant un protocole non orienté connexion, il dispose d'un en-tête de taille réduite par rapport aux en-têtes des segments TCP :



Structure d'un datagramme UDP

Le protocole UDP est conçu pour les applications ne devant pas assembler de séquences de segments. Il laisse aux protocoles de la couche application le soin d'assurer la fiabilité.

12.3. Méthode de connexion TCP

Un service orienté connexion comportent 3 points importants :

- Un chemin unique entre les unités d'origine et de destination est déterminé
- Les données sont transmises de manière séquentielle et arrivent à destination dans l'ordre
- La connexion est fermée lorsqu'elle n'est plus nécessaire

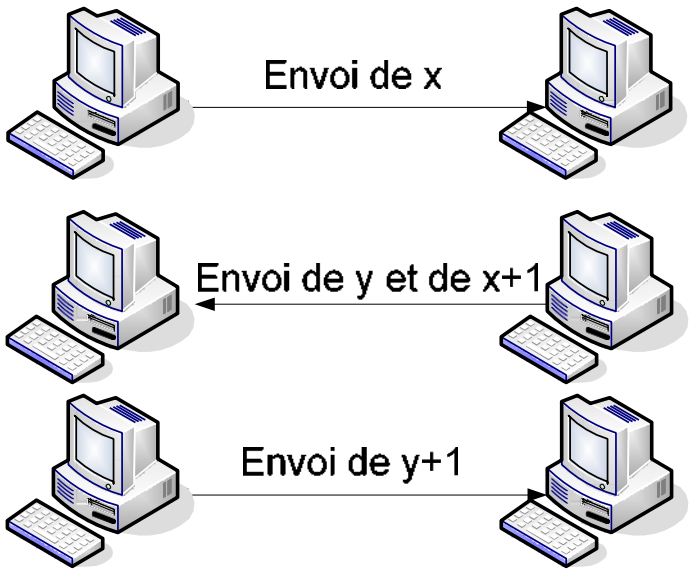
12.3.1. Connexion ouverte/échange en 3 étapes

Les hôtes TCP établissent une connexion en 3 étapes, appelée aussi « connexion ouverte » :

L'émetteur envoie un paquet avec un numéro de séquence initial (x) avec un bit dans l'en-tête pour indiquer une demande de connexion.

Le destinataire le reçoit, consigne le numéro de séquence initial, répond par un accusé de réception «x+1 » et inclut son propre n° de séquence (y).

L'émetteur reçoit x+1 et renvoie y+1 pour dire au destinataire que la réception s'est bien passée.



Il existe également des méthodes garantissant la fiabilité des protocoles

12.3.2. Positive Acknowledgement Retransmission

La technique Positive Acknowledgement Retransmission ou PAR, consiste à envoyer un paquet, démarrer un compteur puis attendre un accusé de réception avant d'envoyer le suivant.

Si le compteur arrive à expiration avant l'arrivé de l'accusé, les informations sont alors retransmises plus lentement et un nouveau compteur est déclenché.

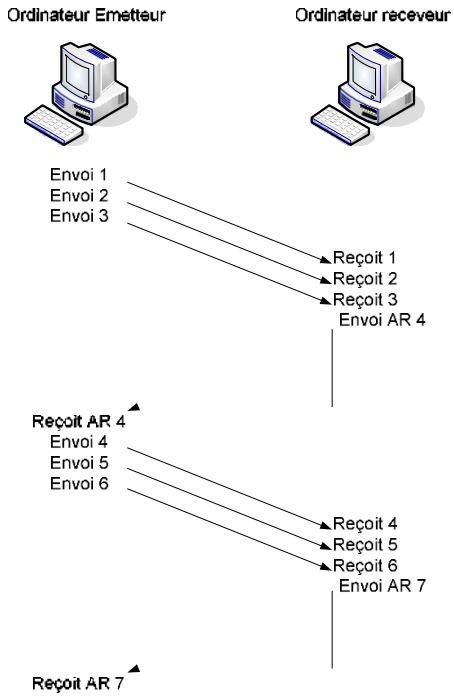
Cependant, cette technique est consommatrice de bande passante, c'est alors qu'intervient le mécanisme de fenêtrage.

12.3.3. Fenêtrage

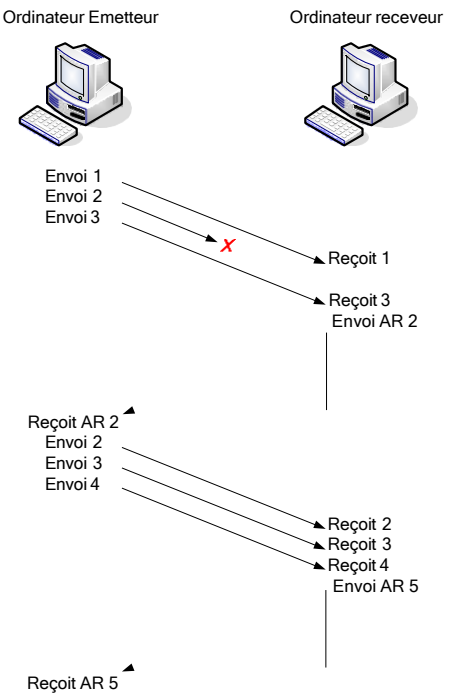
Le Fenêtrage est un mécanisme dans lequel le récepteur envoi un accusé de réception après avoir reçu un certain nombre de données. Si le destinataire n'envoi pas d'accusé, cela signifie pour l'émetteur que les informations ne sont pas parvenues correctement et dans ce cas sont retransmises.

La taille de la fenêtre détermine la quantité de données que l'on peut transmettre avant de recevoir un accusé de réception.

TCP utilise un système d'accusé de réception prévisionnel, ce qui signifie que le numéro d'accusé renvoyé indique la prochaine séquence attendue



Transmission sans perte de paquets



Transmission avec perte de paquets : ici le paquet 2 est renvoyé (le 3 aussi même s'il a été reçu).

13. Couche 5 : Couche session

Comme nous l'avons vu précédemment, une session est un ensemble de transactions entre deux unités réseau ou plus.

Une analogie pour comprendre la couche session est une communication entre plusieurs individus. Si l'on souhaite que la conversation se déroule correctement, il est impératif de mettre en place diverses règles, afin que les interlocuteurs ne s'interrompent pas, par exemple.

Cette notion de contrôle du dialogue est le point essentiel de la couche session.

Le rôle de la couche session est d'ouvrir, gérer et fermer les sessions entre les applications. Cela signifie qu'elle prend en compte :

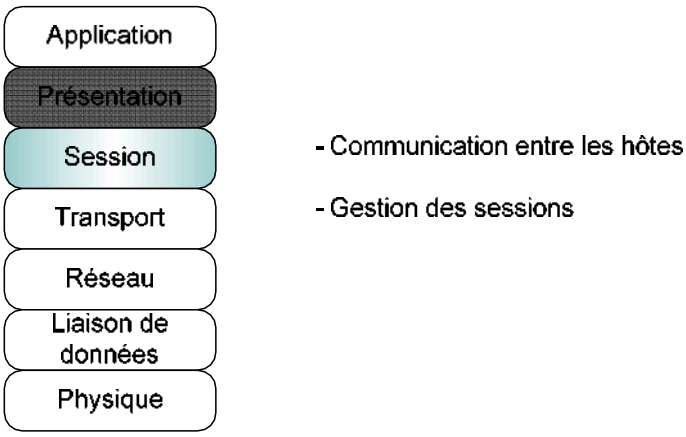
- le lancement des sessions
- la resynchronisation du dialogue
- l'arrêt des sessions

Elle coordonne donc les applications qui communiquent au travers des différents hôtes.

Une communication entre ordinateurs suppose de nombreuses conversations courtes (commutation de paquets comme nous l'avons vu précédemment) avec en plus de cela d'autres communications pour s'assurer de l'efficacité de la communication.

Ces conversations nécessitent que les hôtes jouent à tour de rôles celui de client (demandeur de services) et de serveur (fournisseur de services).

Le contrôle du dialogue consiste en l'identification des rôles de chacun à un moment donné.



13.1. Contrôle du dialogue

La couche session décide si la conversation sera de type bidirectionnel simultané ou alterné. Cette décision relève du contrôle du dialogue.

- Si la communication bidirectionnelle simultanée est permise :
    - La gestion de la communication est assurée par d'autres couches des ordinateurs en communication.
- Si ces collisions au sein de la couche session sont intolérables, le contrôle de dialogue dispose d'une autre option : la communication bidirectionnelle alternée
    - Ce type de communication est rendu possible par l'utilisation d'un jeton de données au niveau de la couche session qui permet à chaque hôte de transmettre à tour de rôle.

13.2. Synchronisation du dialogue

Cette étape est des plus importantes, elle permet aux hôtes communicants au travers d'un réseau de marquer une pause pour par exemple sauvegarder la communication en cours et resynchroniser le dialogue.

Pour cela ils utilisent un « point de contrôle », envoyé par l'un des interlocuteurs à l'autre pour enregistrer la conversation, vérifier l'heure de la dernière portion de dialogue effectuée, comme si vous aviez un double appel avec votre cellulaire. Ce processus est appelé la synchronisation du dialogue.

Comme dans le langage humain, il est important dans une discussion de montrer à son interlocuteur le début d'une conversation (« allo » dans le cas d'une conversation téléphonique) ainsi que de signifier que l'on se prépare à mettre fin à la conversation (« au revoir »). C'est pour cela que les deux contrôles principaux sont :

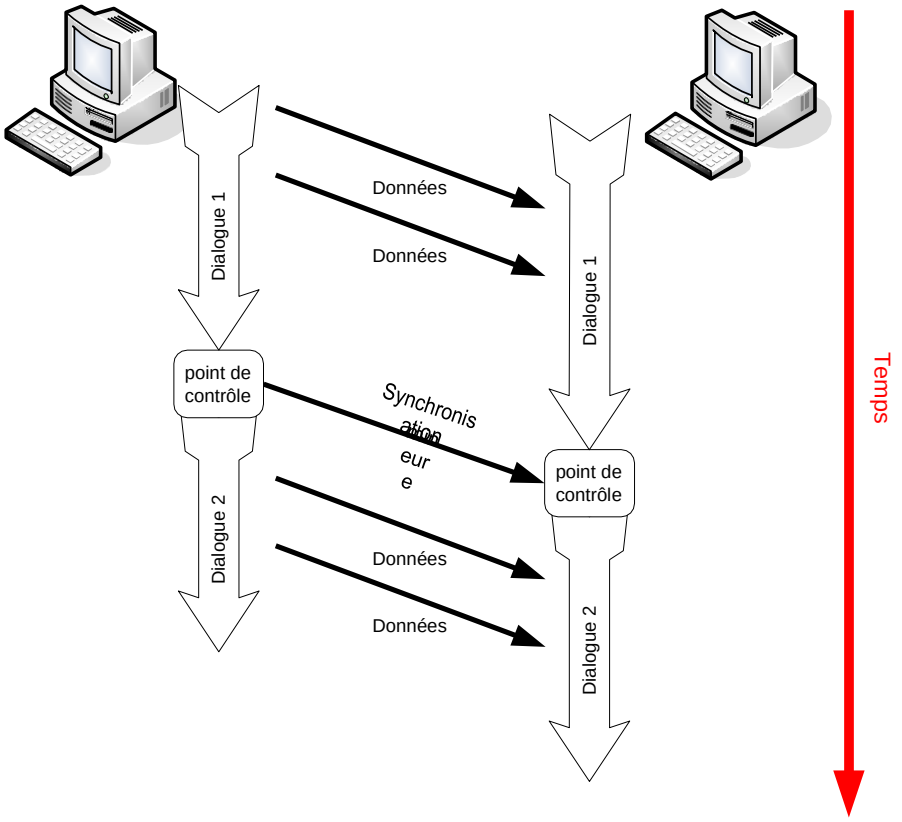
- Lancement ordonné de la communication
- Fin de la communication

13.3. Division du dialogue

La division du dialogue englobe le lancement, la gestion ordonnée et la fin de la communication.

Notre schéma représente une petite synchronisation. Au niveau du point de contrôle, la couche session de l'hôte A envoie un message de synchronisation à l'hôte B, et les deux hôtes exécutent la séquence qui suit :

- Sauvegarder les fichiers donnés.
- Sauvegarder les paramètres réseau.
- Sauvegarder les paramètres de synchronisation.
- Noter le point d'extrémité de la conversation.



Les points de contrôle fonctionnent comme un logiciel de traitement de texte lorsqu'il fait une pause d'une seconde pour effectuer une sauvegarde automatique d'un document. Ces points de contrôle servent toutefois à séparer les parties d'une session, préalablement appelées dialogues.

Nous venons de voir comment les hôtes s’organisent autour de la communication, nous allons maintenant voir comment les données sont générées pour que les hôtes se comprennent.

14. Couche 6 : Couche présentation

Afin que deux hôtes communiquant puissent se comprendre, il est nécessaire qu'il parle le même langage : c'est à cette tâche qu'est dévolue la couche présentation.

14.1. Fonctions et normes

L'un des rôles de la couche présentation est de présenter les données dans un format que le dispositif récepteur est capable de comprendre. La couche présentation peut être comparée à un traducteur lors d'une conférence internationale : elle s'occupe de « traduire » les données de manière à ce que l'hôte récepteur soit en mesure de comprendre.

La couche présentation, ou couche 6, assure trois fonctions principales, à savoir :

- Le formatage des données (présentation)
- Le cryptage des données
- La compression des données

Après avoir reçu les données de la couche application, la couche présentation exécute certaines ou toutes ces fonctions avant d'acheminer les données à la couche session.

Au niveau de la station de réception, la couche présentation reçoit les données de la couche session et exécute les fonctions nécessaires avant de les faire suivre à la couche application.

Les normes de la couche 6 définissent également la présentation des graphiques. Les trois principaux formats graphiques sont :

- BMP (BitMaP) est un format ancien encore largement répandu, il est maintenant supplanté par le JPEG, qui fourni des fichiers avec un meilleur taux compression/taille
- JPEG (Joint Photographic Experts Group) - Format graphique le plus utilisé pour la compression des images fixes complexes et des photographies.
- PNG (Portable Network Graphics) est un format graphique en émergence sur Internet qui compresse les textures.

D'autres normes de la couche 6 concernent la présentation des sons et des séquences animées. Les normes suivantes appartiennent à cette catégorie:

- MPEG (Motion Picture Experts Group) - Format de compression et de codage de vidéo animée pour CD ou tout autre support de stockage numérique.
- MP3 (MPEG Layer 3) - Format de compression de musique le plus utilisé pour le moment. Il utilise l'étude de l'oreille humaine ainsi des algorithmes de compression.
- Divx (MPEG 4) format de compression créé à partir du format MPEG 4 développé par Microsoft et permettant une compression bien meilleure que le MPEG 1 ou 2 (exemple : faire tenir un film sur un CD au lieu d'un DVD).

Représentation des données :

- Lisibilité des données par le destinataire
- Formatage des données
- Contrôle de la syntaxe

Les normes de la couche présentation établissent donc des standards de formats de fichier afin que les hôtes soient en mesure de comprendre les informations.

14.2. Le cryptage des données

Le cryptage est défini par l'utilisation d'algorithmes permettant d'encoder le message de manière à ce que seul l'hôte à qui on l'adresse puisse le comprendre.

Le cryptage permet de protéger la confidentialité des informations pendant leur transmission.

Une clé de cryptage peut être utilisée pour crypter les données à la source en encodant les données avec elle, ce qui obligera l'hôte récepteur à posséder cette clé pour les décrypter. Un algorithme est donc utilisé pour rendre ces données incompréhensibles a quiconque ne disposant pas de la clé.

14.3. La compression des données

La couche présentation assure également la compression des fichiers.

La compression applique des algorithmes (formules mathématiques complexes) pour réduire la taille des fichiers. L'algorithme cherche certaines séquences de bits répétitives dans les fichiers et les remplace par un« jeton »".

Le jeton est une séquence de bits raccourcie qui est substituée à la séquence complète.
Exemple : Remplacer« "LaboratoireCisco »" par« Lab »"

On peut aussi utiliser un dictionnaire pour remplacer certains mots trop long : ils sont constitué des mots ou des séquences revenant le plus souvent ainsi que des séquences de remplacement, de manièreà réduire considérablement les fichiers.

15. Couche 7 : Couche application

15.1. Introduction:

Le rôle de cette couche est d'interagir avec les applications logicielles. Elle fournit donc des services au module de communication des applications en assurant :

- L'identification et la vérification de la disponibilité des partenaires de communication
- La synchronisation des applications qui doivent coopérer
- L'entente mutuelle sur les procédures de correction d'erreur
- Le contrôle de l'intégrité des données

Dans le modèle OSI, la couche application est la plus proche du système terminal (ou la plus proche des utilisateurs).

Celle-ci détermine si les ressources nécessaires à la communication entre systèmes sont disponibles. Sans la couche application, il n'y aurait aucun support des communications réseau. Elle ne fournit pas de services aux autres couches du modèle OSI, mais elle collabore avec les processus applicatifs situés en dehors du modèle OSI.

Ces processus applicatifs peuvent être des tableurs, des traitements de texte, des logiciels de terminaux bancaires.

De plus, la couche application crée une interface directe avec le reste du modèle OSI par le biais d'applications réseau (navigateur Web, messagerie électronique, protocole FTP, Telnet, etc.) ou une interface indirecte, par le biais d'applications autonomes (comme les traitements de texte, les logiciels de présentation ou les tableurs), avec des logiciels de redirection réseau.

Voici en détails les principaux protocoles utilisés par la couche transport :

15.2. DNS

15.2.1. Présentation du protocole DNS

Chaque station possède une adresse IP propre. Cependant il est nettement plus simple de travailleravec des noms de stations ou des adresses plus explicites comme par exemple http://www.labo- cisco.com, qu'avec des adresses IP.

Pour répondre à cela, le protocole DNS permet d'associer des noms en langage courant aux adresses numériques.

Résolution de noms de domaines : Corrélation entre les adresses IP et le nom de domaine associé.

15.2.2. Les noms d'hôtes et le « domain name system »

Aux origines de TCP/IP, étant donné que les réseaux étaient très peu étendus, c'est-à-dire que le nombre d'ordinateurs connectés à un même réseau était faible, les administrateurs réseau créaient des fichiers appelés tables de conversion statique (fichiers généralement appelé hosts ou hosts.txt), associant sur une ligne, grâce à des caractères ASCII, l'adresse IP de la machine et le nom littéral associé, appelé nom d'hôte.

Ce système à l'inconvénient majeur de nécessiter la mise à jour des tables de tous les ordinateurs en cas d'ajout ou modification d'un nom de machine. Ainsi, avec l'explosion de la taille des réseaux, et de leur interconnexion, il a fallu mettre en place un système plus centralisé de gestion des noms. Ce système est nommé Domain Name System, traduisez Système de nom de domaine.

Ce système consiste en une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente.

On appelle nom de domaine, le nom à deux composantes, dont la première est un nom correspondant au nom de l'organisation ou de l'entreprise, le second à la classification de domaine. (.fr, .com, ...). Chaque machine d'un domaine est appelée hôte. Le nom d'hôte qui lui est attribué doit être uniquedans le domaine considéré (le serveur Web d'un domaine porte généralement le nom WWW).

L'ensemble constitué du nom d'hôte, d'un point, puis du nom de domaine est appelé adresse FQDN (Fully Qualified Domain, soit Domaine Totalement Qualifié). Cette adresse permet de repérer de façon unique une machine. Ainsi, www.cisco.com représente une adresse FQDN.

Les machines appelées serveurs de nom de domaine permettent d'établir la correspondance entre le nom de domaine et l'adresse IP sur les machines d'un réseau. Chaque domaine possède ainsi, un serveur de noms de domaines, relié à un serveur de nom de domaine de plus haut niveau. Ainsi, le système de nom est une architecture distribuée, c'est-à-dire qu'il n'existe pas d'organisme ayant à charge l'ensemble des noms de domaines. Par contre, il existe un organisme (l'InterNIC pour les noms de domaine en..com,.net,.org et .edu par exemple). Le système de noms de domaine est transparent pour l'utilisateur, néanmoins il ne faut pas oublier les points suivants.

Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server.

L'adresse IP d'un second Domain Name Server (secondary Domain Name Server) peut également être introduite : il peut relayer le premier en cas de panne.

15.2.3. Codes des domaines internet

La classification du domaine, parfois appelées TLD (Top Level Domain, soit domaines de plus haut niveau), correspond généralement a une répartition géographique.

Toutefois, il existe des noms, créés pour les Etats-Unis à la base, permettant de classifier le domaine selon le secteur d'activité, par exemple :

- .com correspond aux entreprises à vocation commerciales (désormais ce code de domaine ne rime plus à grand chose et est devenu international)
- .edu correspond aux organismes éducatifs
- .gov correspond aux organismes gouvernementaux
- .net correspond aux organismes ayant trait aux réseaux
- .org correspond aux entreprises à but non lucratif
- .biz correspond aux entreprises en générale
- .info réservé aux sites d'informations

15.3. FTP et TFTP

15.3.1. FTP

FTP est un protocole fiable et orienté connexion qui emploie TCP pour transférer des fichiers entre les systèmes qui supportent ce protocole. Le but principal du ftp est de transférer des fichiers à partir d'un ordinateur à un autre en copiant et/ou en déplaçant des fichiers des serveurs aux clients, et des clients vers les serveurs. Le protocole FTP est assigné au port 21 par défaut.

Quand des fichiers sont copiés d'un serveur, FTP établit d'abord une connexion de contrôle entre le client et le serveur. Alors une deuxième connexion est établie, qui est un lien entre les ordinateurs par lequel les données sont transférées. Le transfert de données peut se faire en mode Ascii ou en mode binaire. Ces modes déterminent le codage utilisé pour le fichier de données, qui dans le modèle OSIest une tâche de couche présentation, comme nous l'avons vu précédemment.

Après que le transfert de fichiers ait fini, la connexion de transfert de données se coupe automatiquement. La connexion de contrôle est fermé quand l'utilisateur se déconnecte et clôt la session.

15.3.2. TFTP

TFTP est un service non orienté connexion qui emploie UDP. TFTP (Trivial FTP) est employé sur un routeur pour transférer des dossiers de configuration et des images d'IOS de Cisco et aussi pour transférer des fichiers entre les systèmes qui supportent TFTP. TFTP est conçues pour être léger et simple à utiliser. Néanmoins TFTP peut lire ou écrire des fichiers sur un serveur à distance mais il ne peut pas lister les répertoires et ne supporte pas une authentification utilisateur. Il est utile dans certains LANs parce qu'il fonctionne plus rapidement que le ftp.

15.4. HTTP

Le protocole de transfert hypertexte (HTTP) fonctionne avec le World Wide Web, qui est la partie la plus utilisée et la plus importante d'Internet. Une des raisons principales de cette croissance extraordinaire est la facilité avec laquelle il permet l'accès à l'information.

Un navigateur web est une application client/serveur, qui implique l'existence d'un client et d'un serveur, composant spécifique installé sur les 2 machines afin de fonctionner.

Un navigateur web présente des données dans un format multimédia, c'est-à-dire un contenu réagissant aux actions de l'utilisateur. Le contenu peut être du texte, des graphiques, du son, ou de la vidéo.

Les pages web sont écrite en utilisant l'HTML *(HyperText Markup Language)* : un navigateur web reçoit la page au format HTML et l'interprète de manière à afficher la page d'une manière beaucoup plus agréable qu'un document texte.

Pour déterminer l'adresse IP d'un serveur HTTP distant, le navigateur utilise le protocole DNS pour retrouver l'adresse IP à partir de l'URL. Les données qui sont transférées au serveur HTTP contiennent la localisation de la page Web sur le serveur.

Le serveur répond à la requête par l'envoi au navigateur du code html ainsi que des différents objets multimédia qui agrémente la page (son, vidéo, image) et qui sont indiqués dans les instructions de la page HTML. Le navigateur rassemble tous les fichiers pour créer un visuel de la page Web, et termine la session avec le serveur. Si une autre page est demandée, le processus entier recommence.

15.5. SMTP

Les serveurs d'email communiquent entre eux en employant le *Simple Mail Transfer Protocol (SMTP)* pour envoyer et recevoir du courrier. Le protocole SMTP achemine des messages email dans le format Ascii en utilisant TCP. On l'utilise souvent en tant que protocole d'envoi de mail, rarement en tant que protocole de récupération d'email, car il est peu sécurisé et surtout n'offre aucune authentification.

15.6. SNMP

Le *Simple Network Management Protocol* (SNMP) est un protocole de la couche application qui facilite l'échange d'information de gestion entre les dispositifs d'un réseau. Le SNMP permet à des administrateurs réseau de contrôler l'état du réseau, détecter et résoudre des problèmes de réseau, et de prévoir le développement du réseau, si jamais celui-ci arrive à saturation. Le SNMP emploie le protocole UDP en tant que protocole de couche transport.

Un réseau contrôlé par SNMP comprend les trois composants clés suivants:

- **Système de gestion de réseau (NMS / Network Management System)** : NMS exécute les applications qui supervisent et contrôle les dispositifs gérés. Un ou plusieurs NMS doivent exister sur n'importe quel réseau géré.
- **Dispositifs managés** : Les dispositifs managés sont des nœuds du réseau qui contiennent un agent SNMP et qui résident sur un réseau managé. Les dispositifs managés rassemblent et stockent des informations de gestion et rendent cette information disponible à NMS à l'aide des dispositifs SNMP. Les dispositifs managés, parfois appelés éléments de réseau, peuvent être des routeurs, des serveurs d'accès, des commutateurs, et des ponts, des concentrateurs, des ordinateurs hôtes, ou des imprimeurs.
- **Agents** : Les agents sont des modules de logiciel réseau - gestion qui résident dans des dispositifs managés. Un agent a la connaissance locale d'information de gestion et traduit cette information en un format compatible avec SNMP.

15.7. Telnet

15.7.1. Présentation du protocole Telnet

Le protocole Telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client à un interpréteur de commande (côté serveur).

Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet. Il fournit ainsi un système orienté communication, bidirectionnel alterné (half-duplex), codé sur 8 bits facile à mettre en œuvre.

Le protocole Telnet repose sur trois concepts fondamentaux :

- Le paradigme du terminal réseau virtuel (NVT)
- Le principe d'options négociées
- Les règles de négociation

Ce protocole est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite TCP/IP (FTP, SMTP, POP3, etc.).

Les spécifications de Telnet ne mentionnent pas d'authentification, car Telnet est totalement séparé des applications qui l'utilisent (le protocole FTP définit une séquence d'authentification au-dessus de Telnet).
En outre, le protocole Telnet est un protocole de transfert de données non sûr, c'est-à-dire que les données qu'il véhicule circulent en clair sur le réseau (de manière non chiffrée). Lorsque le protocole Telnet est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23.

Hormis les options et les règles de négociation associées, les spécifications du protocole Telnet sont basiques. La transmission de données à travers Telnet consiste uniquement à transmettre les octets dans le flux TCP (le protocole Telnet précise tout de même que les données doivent par défaut, c'est-à-dire si aucune option ne précise le contraire, être groupées dans un tampon avant d'être envoyées. Plus exactement cela signifie que par défaut les données sont envoyées ligne par ligne). Lorsque l'octet 255 est transmis, l'octet suivant doit être interprété comme une commande. L'octet 255 est ainsi nommé IAC (Interpret As Command, traduisez Interpréter comme une commande).

15.7.2. La notion de terminal virtuel

Aux débuts d'Internet, le réseau (ARPANET) était composé de machines dont les configurations étaient très peu homogènes (claviers, jeux de caractères, résolutions, longueur des lignes d'affichage). D'autre part, les sessions des terminaux possédaient également leur propre façon de contrôler les flux de données en entré/sortie.

Ainsi, au lieu de créer des adaptateurs pour chaque type de terminal afin qu'il puisse y avoir une interopérabilité de ces systèmes, il a été décidé de mettre au point une interface standard, appelée NVT (Network Virtual Terminal, traduisez Terminal réseau virtuel), fournissant une base de communication standard, composée de :

- Caractères ASCII 7 bits auxquels s'ajoutent le code ASCII étendu
- Trois caractères de contrôle
- Cinq caractères de contrôle optionnels
- Un jeu de signaux de contrôle basique

Le protocole Telnet consiste ainsi à créer une abstraction du terminal, permettant à n'importe quel hôte (client ou serveur) de communiquer avec un autre hôte sans connaître ses caractéristiques.