

Année Universitaire : 2020-2021

Table des matières

Chapitre 0 : Introduction générale	1
I- Applications professionnelles.....	1
II- Applications domestiques	1
III- Utilisateurs nomades.....	2
IV- Aspects sociaux	2
V- Caractéristiques physiques des réseaux.....	2
V-1 Réseaux personnels (PAN)	3
V-2 Réseaux locaux (LAN)	4
V-3 Réseaux métropolitains (MAN).....	4
V-4 Réseaux étendus (WAN)	4
VI- Inter-réseaux	5
Chapitre 1 : Modèle OSI	6
I- Modèle général de communication	6
I-1 Utilisation des couches pour analyser des problèmes dans le flux de matériaux	6
I-2 Protocole	6
II- Modèle de référence OSI	6
II-1 La raison d'être du modèle de référence OSI.....	6
II-2 Les fonctions de chaque couche	7
II-2-1 Couche 1 : La couche physique	7
II-2-2 Couche 2 : La couche liaison de données	8
II-2-3 Couche 3 : La couche réseau.....	8
II-2-4 Couche 4 : La couche de transport	8
II-2-5 Couche 5 : La couche session.....	8
II-2-6 Couche 6 : La couche de présentation.....	9
II-2-7 Couche 7 : La couche application.....	9
II-3 Encapsulation	9
II-3-1 Construction des données.	9
II-3-2 Préparation des données pour le transport de bout en bout.	9
II-3-3 Ajout de l'adresse réseau à l'en-tête.	10
II-3-4 Ajout de l'adresse locale à l'en-tête de liaison de données.....	10
II-3-5 Conversion en bits pour la transmission.....	10
II-4 Désignation des données à chaque couche du modèle OSI	10
Chapitre 2 : Les réseaux locaux	12

I-	Introduction.....	12
II-	Les unités de réseau local de base	12
II-1	Les topologies.....	12
II-1-1	La topologie physique	12
II-1-1-1	La topologie en bus linéaire.....	12
II-1-1-2	La topologie en anneau	13
II-1-1-3	La topologie en étoile	13
II-1-1-4	La topologie en étoile étendue.....	13
II-1-1-5	La topologie hiérarchique.....	13
II-1-1-6	La topologie maillée complète	13
II-1-2	La topologie logique.....	14
III-	Les unités de réseau local dans une topologie.....	15
III-1	Les cartes réseau	15
III-2	Média	15
III-3	Les répéteurs.....	16
III-4	Les concentrateurs	16
III-5	Les ponts	17
III-6	Les commutateurs.....	17
III-7	Les routeurs.....	17
IV-	Unités et couches correspondantes.....	18
	Chapitre 3 : Modèle TCP/IP	19
I-	Introduction.....	19
II-	Les couches du modèle de référence TCP/IP	19
II-1	La couche application.....	19
II-2	La couche de transport.....	20
II-3	La couche Internet.....	20
II-4	La couche d'accès réseau	20
III-	Schéma de protocoles TCP/IP	20
IV-	Comparaison du modèle OSI et du modèle TCP/IP.....	21
	Chapitre 4 : Couche Réseau : Routage et Adressage	23
I-	L'importance de la couche réseau.....	23
I-1	Identificateurs	23
I-2	Segmentation et systèmes autonomes.....	23
I-3	Les communications entre réseaux.....	24

I-4 Unités réseau de la couche réseau	24
II- La sélection de la voie	24
II-1 Sélection de la voie.....	25
II-2 Adressage de couche réseau.....	25
II-3 Couche 3 et mobilité de l'ordinateur	26
II-4 Comparaison de l'adressage linéaire et de l'adressage hiérarchique.....	26
III- Les adresses IP dans l'en-tête IP.....	26
III-1 Datagrammes de couche réseau.....	26
III-3 Champs source et de destination de l'en-tête IP	28
III-4 Adresse IP comme nombre binaire 32 bits	28
III-5 Champs de l'adresse IP	28
IV- Les classes d'adresses IP.....	29
IV-1 Classes d'adresses IP	29
IV-1-1 Classe A	29
IV-1-2 Classe B	29
IV-1-3 Classe C	30
IV-2 Adresses IP exprimées en nombres décimaux.....	30
V- L'espace adresse réservé.....	30
V-1 Buts des ID réseau et des adresses de diffusion.....	30
V-2 ID réseau	31
V-3 Analogie pour les ID réseau	31
VI- Subnetting TCP/IP.....	31
VI-1 L'adressage IP.....	31
VI-2 Les adresses TCP/IP réservées ("privées").....	32
VI-3 Le masque de réseau.	33
VI-4 Pourquoi un subnet sur un LAN ou WAN, MAN ?.....	33
VI-5 La création d'un sous-réseau.	33
VI-6 Les nouveaux masques réseau.	35
VI-7 Les adresses de diffusion (broadcast).....	35
VI-8 Le cas du réseau de classe B.	35
VI-9 Le cas du réseau de classe A.	36
VI-10 Plus de classe : le CIDR.	36
Bibliographie.....	37

Chapitre 0 : Introduction générale

Avant de nous attaquer aux aspects techniques propres aux réseaux, voyons l'intérêt que présentent ces derniers ainsi que leurs applications. Après tout, si personne n'était intéressé par leur emploi, on en construirait peu. Nous débuterons par les utilisations traditionnelles, telles que celles faites par les entreprises et les particuliers, avant de poursuivre avec les réseaux domestiques et les récents développements concernant les utilisateurs nomades, pour terminer par les aspects sociaux.

I- Applications professionnelles

La plupart des entreprises possèdent un nombre considérable d'ordinateurs. Si chacun d'eux à l'origine fonctionnait seul, indépendamment des autres, on a pu décider à un moment donné de les interconnecter pour pouvoir distribuer les informations dans toute l'entreprise. Plus généralement, la question abordée ici est celle du **partage des ressources**. L'objectif est de rendre les programmes, les équipements et surtout les données accessibles à tout utilisateur du réseau (entreprise). Un exemple courant est le partage d'une imprimante par un groupe d'employés.

Un deuxième objectif de la réalisation d'un réseau d'ordinateurs concerne les personnes, et non plus les informations ni même les ordinateurs. En effet, un tel système peut représenter un formidable **moyen de communication** entre employés. Pratiquement n'importe quelle société disposant d'au moins deux ordinateurs possède aujourd'hui un système de messagerie ou de **courrier électronique**.

II- Applications domestiques

À l'origine, on achetait un ordinateur pour le traitement de texte et les jeux. Plus récemment, la principale raison d'acquérir un ordinateur domestique, sans doute, est de pouvoir accéder à **l'Internet**. L'accès à l'Internet fournit aux utilisateurs domestiques la **connectivité** à des ordinateurs distants.

Le modèle **client-serveur** permet d'accéder à nombre de ces informations, mais il en existe un autre, appelé **poste à poste** ou **pair à pair** (*peer-to-peer*) souvent abrégé en P2P. Dans ce modèle, les utilisateurs forment un groupe informel au sein duquel chacun peut communiquer avec tous les autres. L'échange se fait en principe sur un pied d'égalité, et il n'existe pas de division en clients et en serveurs. Toutes ces applications impliquent des interactions à distance entre une personne et une base de données renfermant une quantité d'informations. Des millions d'individus dans le monde emploient quotidiennement le courrier électronique, et son utilisation augmente rapidement. Il sert à transporter aussi bien du texte et des images que des données audio et vidéo.

Des applications peuvent également utiliser l'Internet pour transporter des données vidéo (comme dans le cas de serveur YouTube).

À long terme, l'utilisation des réseaux pour améliorer la communication interhumaine sera peut-être plus importante que toutes les autres. Elle peut même devenir capitale pour les personnes géographiquement isolées, en leur offrant les mêmes services qu'à celles qui vivent au cœur d'une grande ville.

Entre les communications interpersonnelles et l'accès à l'information, on trouve les applications des **réseaux sociaux**. Dans ces derniers, le flux d'information est régi par les relations que les personnes déclarent exister entre elles. L'un des sites les plus connus en la matière est **Facebook**, Il permet à ses membres d'actualiser leur profil personnel et de partager les mises à jour avec ceux qu'ils affirment être leurs amis.

III- Utilisateurs nomades

Les équipements mobiles comme les ordinateurs portables, les assistants personnels ou **PDA** (*Personal Digital Assistant*) et les téléphones intelligents (*smartphones*) représentent l'un des segments à plus forte croissance de l'industrie informatique. En déplacement, les utilisateurs veulent pouvoir lire et envoyer des courriers électroniques et des messages instantanés, ou tout simplement surfer sur le Web à la recherche d'informations, autrement dit faire tout ce qu'ils font chez eux et au bureau. Bien entendu, ils veulent le faire de n'importe où sur terre, en mer ou dans les airs. Puisqu'une connexion filaire est impossible à bord d'un véhicule, d'un bateau ou d'un avion, les réseaux sans fil suscitent un très vif intérêt. Les réseaux cellulaires offerts par les compagnies téléphoniques sont un exemple familier de ce type de réseau qui nous fournit une couverture pour les téléphones mobiles. Les **hotspots** sans fil, basés sur la norme 802.11 sont un autre type de réseau sans fil pour les ordinateurs portables. On les trouve surtout dans les cafés, les hôtels, les aéroports, les écoles, les trains et les avions. Toute personne équipée d'un ordinateur portable et d'un modem sans fil peut se connecter à l'Internet *via* le hotspot comme s'il était connecté à un réseau filaire.

IV- Aspects sociaux

Les réseaux d'ordinateurs permettent aux citoyens ordinaires de diffuser et de voir des contenus de façons inimaginables auparavant. Mais toute médaille a son revers, et cette nouvelle liberté s'accompagne de nombreux problèmes sociaux, éthiques et politiques. Les réseaux sociaux, les forums, les sites de partage de contenus et une foule d'autres applications permettent aux personnes de partager leurs vues avec des individus de même sensibilité. Tant que les sujets abordés restent techniques, peu de problèmes se présentent. La difficulté surgit lorsqu'ils touchent à des domaines plus sensibles, et les opinions exprimées publiquement peuvent alors être choquantes ou, pire encore, insultantes. De plus, elles ne se limitent pas nécessairement au texte : les photographies en couleurs haute résolution et les clips vidéo sont faciles à partager sur les réseaux.

V- Caractéristiques physiques des réseaux

Maintenant que nous avons abordé les aspects techniques liés à leur conception. Deux critères importants permettent de caractériser les réseaux : la technologie de transmission et la taille. D'un point de vue général, on distingue deux types de technologies de transmission largement répandues : **la diffusion** et le **point-à-point**. Les liens point-à-point connectent des paires de machines individuelles. Pour aller de sa source à sa destination sur un réseau formé de tels liens, un court message, appelé paquet dans certains contextes, peut devoir transiter par une ou plusieurs machines intermédiaires. Comme plusieurs routes de longueur différente sont souvent possibles, il est important de pouvoir trouver les meilleures. La transmission point-à-

point entre exactement un émetteur et un destinataire est appelée envoi individuel ou parfois diffusion individuelle (ou unicast). En revanche, dans un réseau à diffusion (broadcast) un seul canal de transmission est partagé par tous les équipements : les paquets sont reçus par toutes les machines. Dans chaque paquet, un champ d'adresse permet d'identifier le destinataire réel. À réception d'un paquet, une machine lit ce champ et procède au traitement du paquet si elle reconnaît son adresse, ou l'ignore dans le cas contraire. Un réseau sans fil est un exemple courant de réseau à diffusion, avec des communications partagées dans une zone de couverture qui dépend du canal sans fil et de la machine émettrice. Les systèmes à diffusion offrent généralement la possibilité d'adresser un paquet à toutes les destinations en utilisant une valeur spéciale dans le champ d'adresse. Dans ce cas, le paquet est non seulement reçu mais aussi traité par toutes les machines. Ce mode de transmission est appelé diffusion générale (ou broadcast). Certains systèmes permettent aussi d'adresser un paquet à un sous-ensemble des machines du réseau. On parle alors de diffusion restreinte (ou multicast).

L'autre critère de différenciation des réseaux est leur taille. La distance est une métrique de classification importante, car elle dicte l'emploi de technologies différentes. La figure 1 présente plusieurs systèmes classés en fonction de leur taille approximative. On trouve en premier le réseau personnel, ou PAN (Personal Area Network), destiné à une seule personne. Viennent ensuite les réseaux opérant sur de plus longues distances, qui se répartissent en trois catégories : les réseaux locaux ou LAN (Local Area Network), les réseaux métropolitains ou MAN (Metropolitan Area Network) et les réseaux étendus ou WAN (Wide Area Network), leur taille augmentant à chaque fois. Enfin, l'interconnexion de plusieurs réseaux s'appelle un inter-réseau. L'Internet, qui fonctionne à l'échelle mondiale, est l'exemple le plus connu, (mais non le seul) d'inter-réseau.

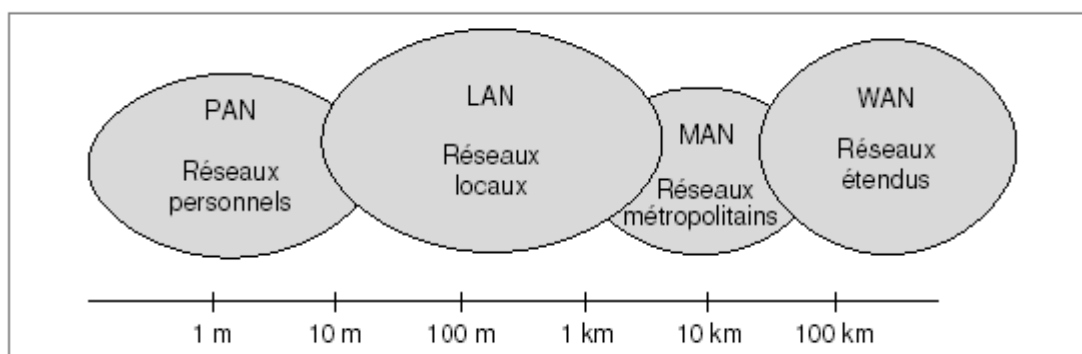


Figure 1 ; catégories de réseaux

V-1 Réseaux personnels (PAN)

Les réseaux personnels, ou PAN, permettent aux équipements de communiquer à l'échelle individuelle. Un exemple courant est celui du réseau sans fil Bluetooth, qui relie un ordinateur à ses périphériques. Le câblage devient inutile, en effet il suffit de poser tout sur son bureau et de les mettre sous tension pour que les connexions fonctionnent. Sous leur forme la plus simple, les réseaux Bluetooth s'appuient sur le paradigme maître-esclave, où le PC est normalement le maître, et la souris, le clavier, etc., sont les esclaves. Le maître indique aux esclaves les adresses à utiliser, le moment où ils peuvent diffuser, pendant combien de temps ils peuvent émettre, les fréquences qu'ils peuvent employer, et ainsi de suite.

V-2 Réseaux locaux (LAN)

Le réseau local, ou LAN est de type réseau privé, qui fonctionne dans une petite aire géographique, comme une maison, un immeuble de bureaux ou une usine. Les LAN sont fréquemment utilisés pour relier des ordinateurs personnels et des équipements électroniques grand public (par exemple des imprimantes) pour leur permettre de partager des ressources et d'échanger des informations. Quand ils sont employés par des organisations, on parle de réseaux d'entreprise. Les LAN sans fil sont très répandus de nos jours, surtout dans les habitations, les immeubles de bureaux anciens, les cafétérias et autres lieux où l'installation de câbles poserait trop de problèmes. Dans ces systèmes, chaque ordinateur dispose d'un modem sans fil, au moyen duquel il communique avec un équipement appelé point d'accès (AP, Access Point), routeur sans fil ou station de base, qui relaie les paquets entre les ordinateurs sans fil, et entre ceux-ci et l'Internet. Il existe pour les LAN sans fil une norme appelée IEEE 802.11, plus connue sous le nom de Wi-Fi, qui est maintenant très répandue. Elle permet des débits d'un à plusieurs centaines Mbit/s. Les LAN filaires font appel à différentes technologies de transmission. La plupart d'entre elles utilisent du fil de cuivre, mais certaines sont à base de fibre optique. Les LAN sont limités en taille, ce qui veut dire que le temps de transmission le plus long est également limité et connu d'avance. Connaître ces restrictions est utile pour la conception des protocoles réseau. Généralement, les LAN filaires offrent des débits de 100 Mbit/s à 1 Gbit/s, et connaissent très peu d'erreurs. Les plus récents peuvent atteindre 10 Gbit/s. Leurs performances sont supérieures en tout point à celles des réseaux sans fil : il est tout simplement plus facile de faire voyager des signaux sur du cuivre ou de la fibre que par voie aérienne. La topologie de nombreux LAN filaires est construite à partir de liens point-à-point. La norme IEEE 802.3, plus connue sous le nom d'Ethernet, est de loin la plus courante pour les LAN filaires. Ethernet commuté représente un exemple de topologie pour ce type de réseau. Chaque ordinateur « parle » le protocole Ethernet et est connecté à un commutateur (d'où son nom) par un lien point-à-point. Un commutateur possède plusieurs ports, chacun d'eux pouvant être connecté à un ordinateur. Sa tâche consiste à relayer les paquets entre les ordinateurs auxquels il est relié, en se basant sur l'adresse MAC présente dans chaque paquet pour déterminer auquel l'envoyer.

V-3 Réseaux métropolitains (MAN)

Un réseau métropolitain, ou MAN couvre une ville. Les MAN interconnectent plusieurs LAN géographiquement proches à des débits importants. Un MAN permet à deux nœuds distants de communiquer comme s'ils faisaient partie d'un même réseau local.

V-4 Réseaux étendus (WAN)

Un réseau étendu, ou WAN s'étend sur une vaste zone géographique (un pays, voire un continent). Chacun des ordinateurs destinés à l'exécution de programmes utilisateur. Nous respectons la tradition et appellerons ces machines des hôtes. Le reste du réseau qui connecte ces hôtes s'appelle un sous-réseau de communication, souvent abrégé en sous-réseau. Celui-ci a pour tâche l'acheminement des messages d'un hôte à un autre. Dans la plupart des WAN, le sous-réseau se compose de deux types de composants : les lignes de transmission et les équipements de commutation. Les lignes de transmission transportent les bits d'une machine à une autre et peuvent être à base de fil de cuivre, de fibre optique ou

même prendre la forme de liaisons radio. Les équipements de commutation, ou plus simplement commutateurs, sont des ordinateurs spécialisés qui servent à interconnecter trois lignes de transmission ou plus. Le plus usité aujourd'hui étant **routeur**.

VI- Inter-réseaux

Il existe beaucoup de réseaux dans le monde, souvent composés de matériels et de logiciels différents. Les personnes connectées à un réseau souhaitent fréquemment communiquer avec d'autres personnes reliées à d'autres réseaux. Pour satisfaire à cette demande, les divers réseaux, souvent incompatibles entre eux, doivent être interconnectés. Un ensemble de réseaux ainsi reliés s'appelle un inter-réseau (internetwork), l'Internet en étant l'exemple le plus connu aujourd'hui. Il utilise des réseaux de FAI pour connecter des réseaux d'entreprise, des réseaux domestiques et bien d'autres réseaux.

Une certaine confusion règne quant à la signification des termes de sous-réseau, réseau et inter-réseau. Le terme de sous-réseau prend tout son sens dans le contexte d'un réseau étendu, où il renvoie à l'ensemble des routeurs et des lignes de transmission qui appartiennent à l'opérateur du réseau les hôtes n'en font pas partie. Un réseau est formé par la combinaison d'un sous-réseau et de ses hôtes.

En ce qu'est un inter-réseau. Nous savons qu'un inter-réseau est formé lorsque des réseaux distincts sont interconnectés. La connexion d'un LAN et d'un WAN ou de deux LAN est la façon habituelle de constituer un inter-réseau. Si les technologies de communication sous-jacentes propres aux diverses parties diffèrent (par exemple à diffusion vs point-à-point, ou sans fil vs filaire), on a probablement affaire à un inter-réseau.

Nous devons parler de la façon dont deux réseaux différents peuvent être connectés. Le nom générique d'un équipement qui établit une connexion entre deux réseaux ou plus, tant en termes de matériels que de logiciels, est une passerelle (gateway en anglais). L'avantage d'un inter-réseau est qu'il permet de connecter des ordinateurs appartenant à des réseaux différents. Nous pouvons maintenant repérer un inter-réseau au fait que c'est un réseau qui contient des routeurs.

Le reste de document est organisé de la façon suivante : Chapitre 1 présente le modèle de référence OSI. Le chapitre 2 présente les aspects des réseaux locaux. Le modèle TCP/IP est présenté dans le chapitre 3 et enfin les aspects de routage, d'adressage et de subnetting de la couche réseau sont traités dans le chapitre 4.

Chapitre 1 : Modèle OSI

I- Modèle général de communication

I-1 Utilisation des couches pour analyser des problèmes dans le flux de matériaux

Le concept de couches vous aidera à comprendre ce qui se produit pendant la communication entre deux ordinateurs. Les questions indiquées dans la figure 2 portent sur le mouvement d'objets physiques comme le trafic routier ou les données électroniques. Ce déplacement d'objets, qu'il soit physique ou logique, s'appelle flux. De nombreuses couches aident à décrire en détail le cheminement du flux.

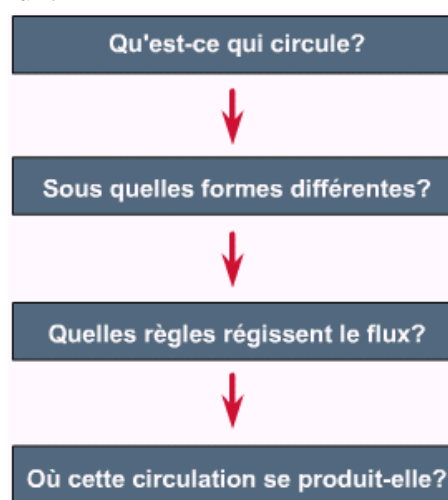


Figure 2 : Notion de flux.

I-2 Protocole

Pour que des paquets de données puissent se rendre d'un ordinateur source à un ordinateur de destination sur un réseau, il est important que toutes les unités du réseau communiquent dans le même langage ou protocole. Un protocole consiste en un ensemble de règles qui rehaussent l'efficacité des communications au sein d'un réseau.

Voici une définition technique d'un protocole de communication de données : ensemble de règles ou convention qui détermine le format et la transmission des données. La couche n d'un ordinateur communique avec la couche n d'un autre ordinateur. Les règles et conventions utilisées lors de cette communication sont collectivement appelées **protocole de couche n**.

II- Modèle de référence OSI

II-1 La raison d'être du modèle de référence OSI

Le modèle de référence OSI est le principal modèle des communications en réseau. Bien qu'il existe d'autres modèles, la majorité des fournisseurs de réseaux relie aujourd'hui leurs produits à ce modèle de référence, particulièrement lorsqu'ils désirent donner aux utilisateurs la formation sur l'utilisation de leurs produits. Ils le considèrent comme le meilleur outil offert pour décrire l'envoi et la réception de données dans un réseau.

Le modèle de référence OSI vous permet de voir les fonctions réseau exécutées à chaque couche. Plus important encore, ce modèle de référence constitue un cadre que vous pouvez utiliser pour comprendre comment l'information circule dans un réseau. En outre, vous pouvez vous servir du modèle de référence OSI pour visualiser comment l'information, ou les données, circule à partir des programmes d'application (ex. : tableurs, documents, etc.), en passant par un média réseau (ex. : fils, etc.), jusqu'à un autre programme d'application se trouvant dans un autre ordinateur en réseau, même si l'expéditeur et le destinataire utilisent des types de réseau différents.

Le modèle de référence OSI comporte **sept** couches numérotées, chacune illustrant une fonction réseau précise. Cette répartition des fonctions réseau est appelée organisation en couches. Le découpage du réseau en sept couches présente les avantages suivants :

- Il permet de diviser les communications sur le réseau en éléments plus petits et simples.
- Il uniformise les éléments du réseau de manière à permettre le développement et le soutien multifournisseur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Il empêche les changements apportés à une couche d'influer sur les autres couches, ce qui assure un développement plus rapide.
- Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement.

Le problème consistant à déplacer de l'information entre des ordinateurs est divisé en sept problèmes plus petits et plus faciles à gérer dans le modèle de référence OSI. Chacun des sept petits problèmes est représenté par une couche particulière du modèle. Voici les sept couches du modèle de référence OSI :

Couche 7 : la couche application

Couche 6 : la couche présentation

Couche 5 : la couche session

Couche 4 : la couche transport

Couche 3 : la couche réseau

Couche 2 : la couche liaison de données

Couche 1 : la couche physique

II-2 Les fonctions de chaque couche

Chaque couche du modèle OSI doit exécuter une série de fonctions pour que les paquets de données puissent circuler d'un ordinateur source à un ordinateur de destination sur un réseau. Vous trouverez ci-dessous une brève description de chaque couche du modèle de référence OSI qui est illustré dans la figure 3.

II-2-1 Couche 1 : La couche physique

La couche physique définit les spécifications électriques, mécaniques, procédurales et fonctionnelles pour activer, maintenir et désactiver la liaison physique entre les systèmes d'extrémité. Les caractéristiques comme les niveaux de tension, la synchronisation des

changements de tension, les débits physiques, les distances maximales de transmission, les connecteurs physiques et autres attributs semblables sont définies par la couche physique.

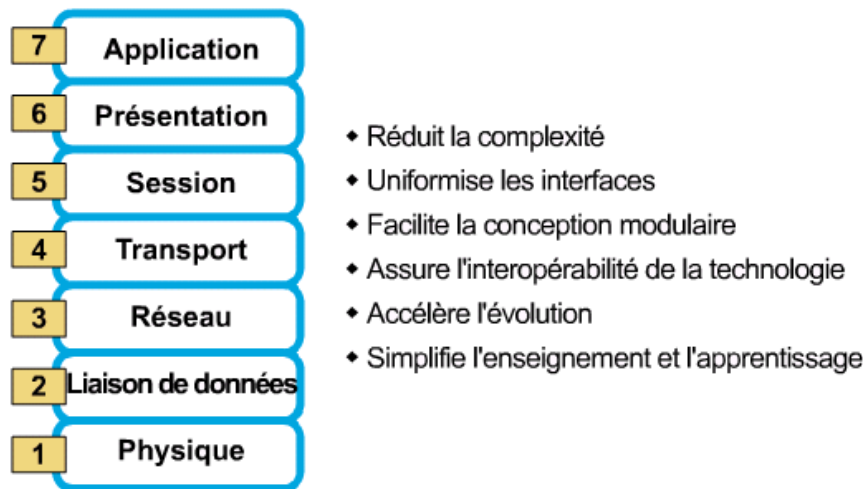


Figure 3 : Les sept couches du modèle OSI.

II-2-2 Couche 2 : La couche liaison de données

La couche liaison de données assure un transit fiable des données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique (adresse MAC) (plutôt que logique), de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et du contrôle de flux.

II-2-3 Couche 3 : La couche réseau

La couche réseau est une couche complexe qui assure la connectivité et la sélection du trajet entre deux systèmes hôte pouvant être situés sur des réseaux géographiquement éloignés. Elle s'occupe de routage et de l'adressage

II-2-4 Couche 4 : La couche de transport

La couche de transport segmente les données envoyées par l'hôte émetteur et les rassemble en flot de données à l'hôte récepteur. La frontière entre la couche session et la couche de transport peut être vue comme la frontière entre les protocoles de couche média et les protocoles de couche hôte. Alors que les couches application, de présentation et de transport se rapportent aux applications, les trois couches qui les suivent se rapportent au transport des données.

La couche de transport tente de fournir un service de transport des données qui protège les couches supérieures des détails d'implantation du transport. Plus particulièrement, les questions comme la façon d'assurer la fiabilité du transport entre deux systèmes hôtes relèvent de la couche de transport. En fournissant un service de communication, la couche de transport établit et raccorde les circuits virtuels, en plus d'en assurer la maintenance. En fournissant un service fiable, elle fait appel à des contrôles de détection des erreurs de transport, de reprise sur incident et de flux d'information.

II-2-5 Couche 5 : La couche session

Comme son nom l'indique, la couche session ouvre, gère et ferme les sessions entre deux systèmes hôtes en communication. Cette couche fournit des services à la couche de

présentation. Elle synchronise également le dialogue entre les couches de présentation des deux hôtes et gère l'échange des données. En plus de la régulation de la session, la couche session assure également le transfert efficace des données et la classe de service, ainsi que la signalisation des écarts de la couche session, de la couche de présentation et de la couche application.

II-2-6 Couche 6 : La couche de présentation

La couche de présentation s'assure que l'information envoyée par la couche application d'un système est lisible par la couche application d'un autre système. Au besoin, la couche de présentation traduit différents formats de représentation des données en utilisant un format commun.

II-2-7 Couche 7 : La couche application

La couche application est la couche OSI la plus près de l'utilisateur ; elle fournit des services réseau aux applications de l'utilisateur. Elle se distingue des autres couches en ce qu'elle ne fournit pas de services aux autres couches OSI, mais seulement aux applications à l'extérieur du modèle OSI. Voici des exemples de ce type d'application : tableurs, traitement de texte et logiciels de terminaux bancaires. La couche application détermine la disponibilité des partenaires de communication voulus, assure la synchronisation et établit une entente sur les procédures de reprise sur incident et de contrôle de l'intégrité des données.

II-3 Encapsulation

Vous savez que toutes les communications dans un réseau partent d'une source, qu'elles sont acheminées à une destination et que l'information envoyée dans le réseau est appelée données ou paquets de données. Si un ordinateur (hôte A) veut envoyer des données à un autre ordinateur (hôte B), les données doivent d'abord être préparées grâce à un processus appelé encapsulation.

Ce processus conditionne les données en leur ajoutant l'information relative au protocole qui est nécessaire, avant que les données soient transmises sur le réseau. Ainsi, en descendant dans les couches du modèle OSI, les données reçoivent des en-têtes, des informations de fin et d'autres informations. (Remarque : Le terme "en-tête" fait référence à l'information d'adresse.) Pour comprendre comment se produit l'encapsulation, examinons la manière dont les données traversent les couches, comme l'illustre la figure 3. Les données qui sont envoyées par l'ordinateur source traversent la couche application et les autres couches. Comme vous pouvez le constater, la présentation et le flux des données échangées subissent des changements au fur et à mesure que les réseaux fournissent leurs services aux utilisateurs. Comme l'illustrent la figure 4, les réseaux doivent effectuer les cinq étapes de conversion ci-dessous afin d'encapsuler les données :

II-3-1 Construction des données.

Lorsqu'un utilisateur envoie un message électronique, les caractères alphanumériques qu'il contient sont convertis en données pouvant circuler dans l'inter réseau.

II-3-2 Préparation des données pour le transport de bout en bout.

Les données sont préparées pour le transport inter-réseau. En utilisant des segments, la fonction de transport s'assure que les systèmes hôtes à chaque extrémité du système de messagerie peuvent communiquer de façon fiable.

II-3-3 Ajout de l'adresse réseau à l'en-tête.

Les données sont organisées en paquet, ou datagramme, contenant un en-tête réseau constitué des adresses logiques source et de destination. Ces adresses aident les unités réseau à acheminer les paquets dans le réseau suivant un chemin déterminé.

II-3-4 Ajout de l'adresse locale à l'en-tête de liaison de données.

Chaque unité réseau doit placer le paquet dans une trame. La trame permet d'établir la connexion avec la **prochaine** unité réseau directement connectée de la liaison. Chaque unité se trouvant sur le chemin déterminé doit effectuer la mise en trame pour pouvoir se connecter à la prochaine unité.

II-3-5 Conversion en bits pour la transmission.

La trame doit être convertie en une série d'un et de zéro (bits) pour la transmission sur le média (habituellement un fil). Une fonction de synchronisation permet aux unités de distinguer ces bits lorsqu'ils circulent sur le média. Tout au long du trajet suivi dans l'inter-réseau physique, le média peut varier. Par exemple, le message électronique peut provenir d'un réseau local, traverser le réseau fédérateur d'un parc de bâtiments, sortir par une liaison réseau longue distance pour atteindre sa destination sur un autre réseau local éloigné. Les informations d'en-tête et de fin sont ajoutées au fur et à mesure que les données descendent dans les couches du modèle OSI.

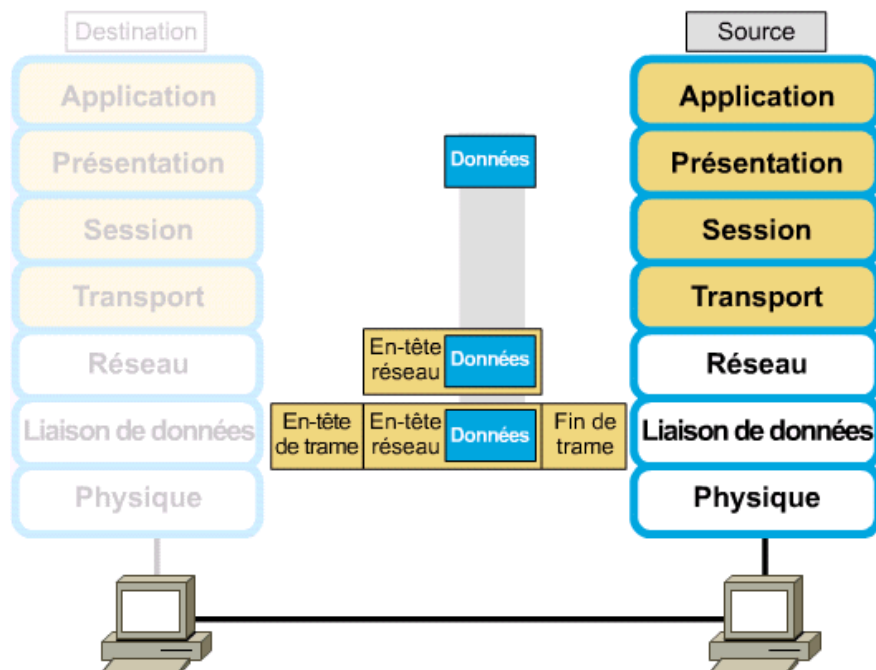


Figure 4 Notion d'encapsulation

II-4 Désignation des données à chaque couche du modèle OSI

Afin de permettre l'acheminement des paquets de données entre l'ordinateur source et l'ordinateur de destination, chaque couche du modèle OSI sur l'ordinateur source doit

communiquer avec sa couche homologue sur l'ordinateur de destination. Cette forme de communication est appelée communication d'égal à égal. Au cours de ce processus, le protocole de chaque couche assure l'échange de l'information, appelée unité de données de protocole (ou PDU), entre les couches homologues. Chaque couche de communication, sur l'ordinateur source, communique avec l'unité de données de protocole propre à une couche, ainsi qu'avec la couche correspondante sur l'ordinateur de destination, comme l'illustre la figure 5.

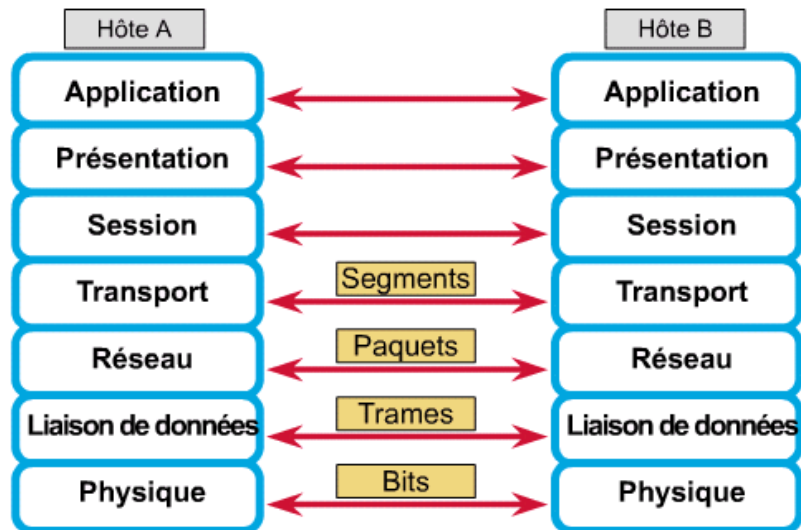


Figure 5 Unité de données de protocole

Dans un réseau, les paquets de données proviennent d'une source et s'acheminent vers une destination. Chaque couche dépend de la fonction de service de la couche OSI sous elle. Pour fournir ce service, la couche inférieure a recours à l'encapsulation pour placer l'unité de données de protocole de la couche supérieure dans son champ de données, puis elle ajoute l'information d'en-tête et de fin dont elle a besoin pour remplir ses fonctions. Ensuite, au fur et à mesure que les données traversent les couches du modèle OSI, d'autres informations d'en-tête et de fin sont ajoutées.

Une fois que les couches 7, 6 et 5 ont ajouté leurs informations, la couche 4 en ajoute d'autres. Ce regroupement des données, soit l'unité de données de protocole de couche 4, est appelé un segment.

La couche réseau, par exemple, fournit un service à la couche de transport, qui présente les données au sous-système de l'inter-réseau. La couche réseau est chargée de déplacer les données dans l'inter-réseau. Pour ce faire, elle encapsule les données et leur joint un en-tête de manière à créer un paquet (soit la PDU de couche 3). L'en-tête contient l'information requise pour effectuer le transfert, notamment les adresses logiques de source et de destination.

La couche liaison de données fournit un service à la couche réseau. Elle encapsule l'information de couche réseau dans une trame (l'unité de données de protocole de couche 2); l'en-tête de trame contient l'information (les adresses physiques, par exemple) nécessaire à l'exécution des fonctions de liaison de données. La couche liaison de données fournit donc un service à la couche réseau en encapsulant l'information de couche réseau dans une trame.

La couche physique fournit un service à la couche liaison de données. Elle code la trame de liaison de données en une série de un et de zéro (bits) en vue de la transmission sur un média (habituellement un fil) à la couche 1.

Chapitre 2 : Les réseaux locaux

I- Introduction

Maintenant que vous avez acquis une compréhension de base du modèle OSI et de ce qui arrive aux paquets de données lorsqu'ils traversent les couches, il est temps de commencer à examiner les unités de réseau élémentaires. Couche par couche, vous étudierez les unités utilisées à chaque couche lorsque les paquets de données circulent de la source à la destination. Ce chapitre porte sur les unités de réseau local. Comme vous le savez, les réseaux locaux sont des réseaux à haute vitesse et à faible pourcentage d'erreur couvrant une région géographique limitée. Les réseaux locaux relient des postes de travail, des périphériques, des terminaux et d'autres unités à l'intérieur d'un immeuble ou d'une région géographique limitée. Dans le présent chapitre, vous étudierez les unités de réseau local de base et l'évolution des unités de réseau. Vous étudierez aussi les unités de réseau qui fonctionnent à chaque couche du modèle OSI, ainsi que la façon dont les paquets sont acheminés par chaque unité lorsqu'ils traversent les couches du modèle OSI. Enfin, vous étudierez les étapes de base de la construction des réseaux locaux.

II- Les unités de réseau local de base

II-1 Les topologies

II-1-1 La topologie physique

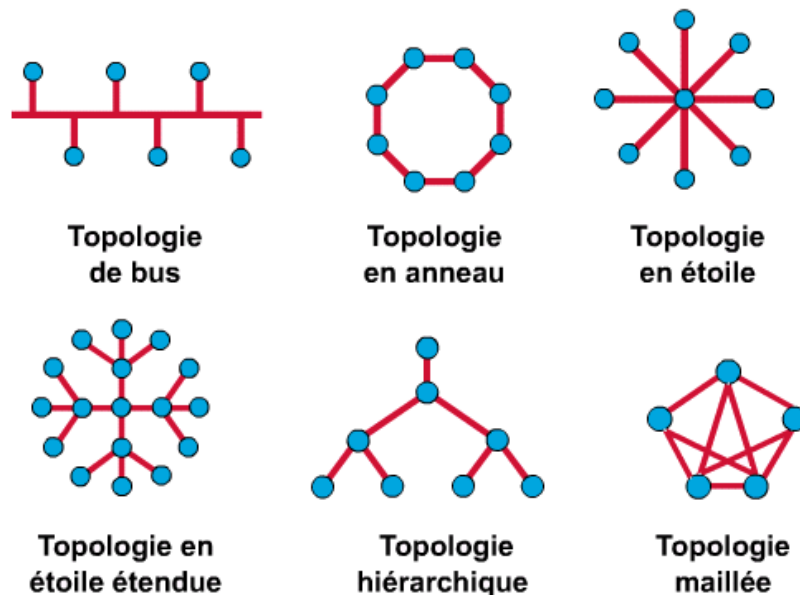


Figure 6 : Différentes topologies physiques.

La topologie physique réfère à la disposition des fils et média qui relient les hôtes. Les topologies physiques couramment utilisées sont la topologie en bus, en anneau, en étoile, en étoile étendue, hiérarchique et maillée. Elles sont illustrées dans la figure 6

II-1-1-1 La topologie en bus linéaire

Dans la topologie en bus, tous les nœuds sont connectés directement à une liaison et il n'y a aucune connexion entre les nœuds.

Chaque unité hôte est connectée à un fil commun. Dans cette topologie, les unités clés sont celles qui permettent à l'unité hôte de joindre le média partagé unique ou de se connecter à lui. L'un des avantages de cette topologie est que toutes les unités hôtes sont connectées entre elles et qu'elles peuvent donc communiquer directement. En revanche, l'un des inconvénients est que les unités hôtes sont déconnectées les unes des autres s'il se produit un bris du câble. Une topologie de bus permet à toutes les unités de réseau de voir tous les signaux de toutes les autres unités, ce qui peut être un avantage si vous voulez que toute l'information se rende à toutes les unités. Cela peut toutefois être un désavantage car les collisions et les problèmes de trafic sont courants.

II-1-1-2 La topologie en anneau

Une topologie en anneau est un anneau fermé constitué de nœuds et de liaisons, chaque nœud étant connecté aux deux nœuds adjacents uniquement. Toutes les unités sont directement connectées les unes aux autres en série. Pour que l'information circule, chaque station doit la passer à la station adjacente.

II-1-1-3 La topologie en étoile

Une topologie en étoile comporte un nœud central, duquel partent toutes les liaisons aux autres nœuds, et ne permet aucune autre liaison. Son principal avantage est que tous les autres nœuds peuvent communiquer entre eux de manière pratique grâce au nœud central. Par contre, son plus grand désavantage est que tout le réseau est déconnecté si le nœud central connaît une défaillance. Selon le type d'unité de réseau utilisé au centre du réseau en étoile, les collisions peuvent s'avérer un problème. Toute l'information en circulation passe par une unité. Cela peut être souhaitable pour des raisons de sécurité ou de restriction d'accès, mais cette méthode souffre de tout problème associé au nœud central de l'étoile.

II-1-1-4 La topologie en étoile étendue

La topologie en étoile étendue est identique à la topologie en étoile, sauf que chaque nœud connecté au nœud central est aussi le centre d'une autre étoile. Une topologie en étoile étendue est constituée d'une topologie en étoile principale dont chacun des nœuds d'extrémité est aussi le centre de sa propre topologie en étoile. L'avantage de cette topologie est qu'elle réduit les longueurs de câble et qu'elle limite le nombre d'unités interconnectées à un nœud central. La topologie en étoile étendue est très hiérarchique et contribue à maintenir l'information à un niveau local. C'est la façon dont le système téléphonique est présentement structuré.

II-1-1-5 La topologie hiérarchique

La topologie hiérarchique ressemble à la topologie en étoile étendue, la principale différence étant qu'elle n'utilise pas un nœud central. Elle utilise plutôt un nœud de circuit duquel partent des branches vers d'autres nœuds. Il existe deux types de topologies arborescentes : l'arbre binaire (chaque nœud se divisant en deux liaisons) et l'arbre de base (un circuit de base comportant des branches de nœud avec des liaisons). Le flux d'information est hiérarchique.

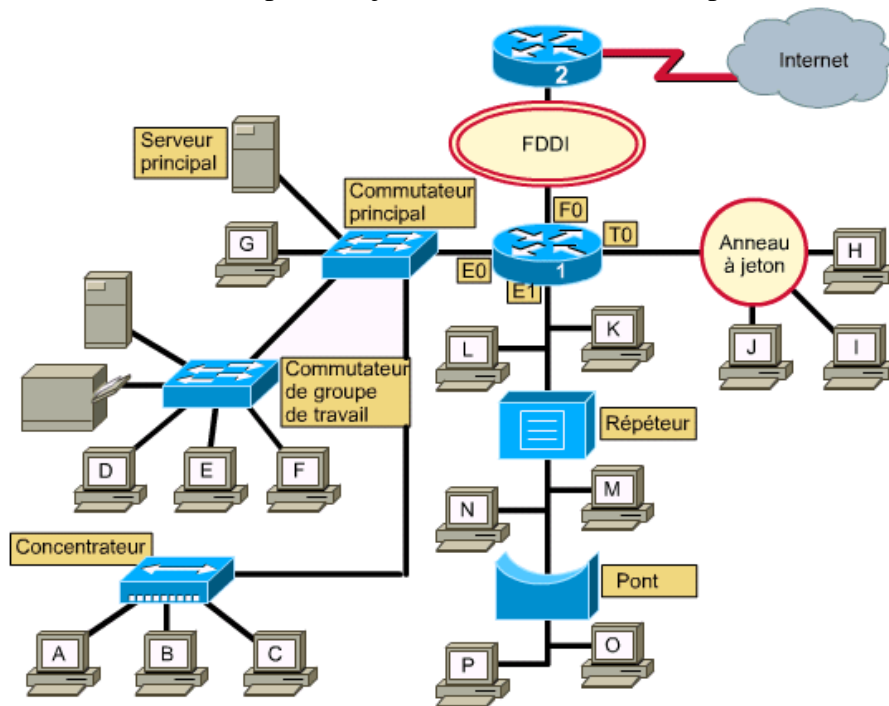
II-1-1-6 La topologie maillée complète

II-1-2 La topologie logique

La topologie logique d'un réseau représente la méthode qu'utilisent les hôtes pour communiquer par le média : elle précise la façon dont les hôtes accèdent au média. Les deux types de topologie logique les plus courants sont la diffusion et le passage de jeton.

La diffusion signifie simplement que chaque hôte envoie ses données à tous les autres hôtes sur le média du réseau. Les stations n'ont pas à respecter un certain ordre pour utiliser le réseau ; il s'agit d'une méthode de type "premier arrivé, premier servi". L'Ethernet fonctionne de cette façon.

Le deuxième type de topologie est le passage de jeton. Selon cette méthode, l'accès au réseau est contrôlé en passant un jeton électronique de manière séquentielle à chaque hôte. Lorsqu'un hôte reçoit le jeton, cela signifie qu'il peut transmettre des données sur le réseau. Si l'hôte n'a pas de données à transmettre, il passe le jeton à l'hôte suivant et le processus est répété.



Le schéma de la figure 7 présente de nombreuses topologies, il représente un réseau local de complexité moyenne, comme celui qu'on retrouve habituellement dans une école ou une petite entreprise. Il fait appel à plusieurs symboles et illustre de nombreux concepts de réseau dont l'apprentissage demande un certain temps.

III- Les unités de réseau local dans une topologie

Les unités directement connectées à un segment de réseau sont appelées hôtes. Ces hôtes peuvent être des ordinateurs, des clients, des serveurs, des imprimantes, des scanners et de nombreux autres dispositifs. Ces unités fournissent les connexions réseau aux utilisateurs grâce auxquelles ils peuvent partager, créer et obtenir de l'information. Les unités hôte peuvent exister sans réseau. Toutefois, les capacités d'un hôte qui n'est pas relié à un réseau sont très limitées.

Les unités hôte n'appartiennent à aucune couche. Elles sont connectées physiquement au média réseau grâce à leur carte réseau et les fonctions des autres couches OSI sont exécutées par des logiciels exploités par l'hôte. Cela signifie que les unités hôte fonctionnent au niveau des sept couches du modèle OSI. Elles se chargent du processus d'encapsulation et de désencapsulation afin de pouvoir envoyer du courrier électronique, imprimer des rapports ou accéder à des bases de données.

III-1 Les cartes réseau

La carte réseau, appartient à la couche 2, la couche liaison de données, du modèle OSI. Pour ce qui est de son aspect physique, une carte réseau est une plaquette de circuits imprimés qui loge dans l'emplacement d'extension d'un bus, sur la carte-mère d'un ordinateur ou sur un périphérique. On l'appelle aussi adaptateur réseau. Sa fonction consiste à adapter l'unité hôte au média de réseau. Les cartes réseau sont considérées comme des dispositifs de couche 2 parce que chaque carte réseau dans le monde porte un nom de code unique appelé adresse MAC (Media Access Control). Cette adresse est utilisée pour contrôler la communication des données de l'hôte dans le réseau. La carte réseau contrôle l'accès de l'hôte au média.

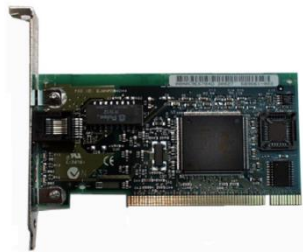


Figure 8 : Carte réseau.

III-2 Média

La fonction de base des médias consiste à acheminer un flux d'informations, sous forme de bits et d'octets, dans un réseau local. Si on exclut les réseaux locaux sans fil (qui utilisent l'atmosphère ou l'espace comme média), de façon générale, les médias de réseau confinent les signaux réseau à des fils, des câbles ou à la fibre optique. Les médias de réseau sont considérés comme des composants de couche 1 des réseaux locaux. Vous pouvez construire des réseaux informatiques en utilisant plusieurs types de médias différents. Chaque média présente des avantages et des désavantages et ce qui constitue un avantage dans le cas d'un média (le coût, dans le cas du câble de catégorie 5) peut être un désavantage dans le cas d'un autre (le coût, dans le cas de la fibre optique). Certains des avantages et des désavantages sont énumérés ci-dessous.

- Longueur de câble

- Coût
- Facilité d'installation
- Nombre total d'ordinateurs connectés au média.

Le câble coaxial, la fibre optique et même l'atmosphère peuvent transporter des signaux de réseau. Toutefois, le principal média se nomme câble à paires torsadées non blindées de catégorie 5.

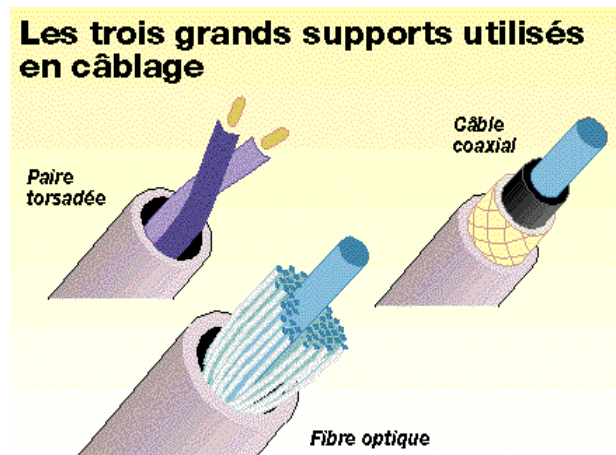


Figure 9 : Différents supports de transmission.

III-3 Les répéteurs

Il existe un grand nombre de médias, qui présentent chacun leurs avantages et leurs inconvénients. Par exemple, pour le câble à paires torsadées non blindées de catégorie 5 la longueur maximale dans un réseau est de 100 mètres. Pour prolonger un réseau au-delà de cette limite, nous devons y ajouter une unité nommée répéteur.



Figure 10 : Schéma de répéteur.

Le but du répéteur est d'amplifier les signaux réseau et de les resynchroniser au niveau du bit pour leur permettre de voyager sur de plus longues distances dans le média. Les répéteurs sont des unités à un seul port "d'entrée" et à un seul port de "sortie". Ce sont des unités de couche 1 du modèle OSI, car ils agissent uniquement au niveau du bit et ne se soucient d'aucune autre information.

III-4 Les concentrateurs

Le but du concentrateur est d'amplifier et de resynchroniser les signaux réseau. Il fait cela au niveau du bit pour un grand nombre d'hôtes (p. ex. 4, 8 ou même 24) en utilisant un processus nommé concentration. Cette définition est très semblable à celle du répéteur, c'est pourquoi le concentrateur est aussi connu sous le nom de répéteur multiport. La différence entre les deux est le nombre de câbles connectés à l'unité. On utilise un concentrateur pour créer une topologie physique en étoile et ainsi accroître la fiabilité d'un réseau, car le concentrateur permet à un câble unique de défaillir sans perturber le fonctionnement d'un réseau entier. Cela diffère de la topologie de bus dans laquelle un câble défectueux perturbe le réseau entier. Les

concentrateurs sont considérés comme des unités de couche 1 parce qu'ils ne font qu'amplifier le signal et le diffuser par tous leurs ports (connexions réseau).



Figure 11 : Schéma de concentrateur (HUB).

Dans un réseau en anneau à jeton, le rôle du concentrateur est assumé par l'unité d'accès au média MAU (Media Access Unit). Physiquement, cette unité ressemble à un concentrateur, mais la technologie en anneau à jeton est très différente. Dans le cas des interfaces FDDI, l'unité d'accès au média est appelée concentrateur. Les unités d'accès au média sont aussi des unités de couche 1.

III-5 Les ponts

Un pont est une unité de couche 2 conçue pour connecter deux segments de réseau local. Le rôle du pont est de filtrer le trafic sur un réseau local pour conserver le trafic local au niveau local, tout en établissant une connectivité avec d'autres parties (segments) du réseau local pour le trafic qui y est destiné. Comme chaque unité de réseautage possède une adresse MAC unique sur la carte réseau, le pont effectue le suivi des adresses MAC se trouvant de chacun de ses côtés et prend des décisions en fonction de cette liste d'adresses.



Figure 12 : Schéma de pont

Il est important de noter que, tout comme un répéteur, un pont connecte deux segments à la fois. Comme nous l'avons vu dans le cas de la combinaison répéteur-concentrateur, une autre unité est utilisée dans le cas des connexions à plusieurs ponts.

III-6 Les commutateurs

Le commutateur est une unité de couche 2 tout comme le pont. En fait, un commutateur se nomme aussi un pont multiport, tout comme un concentrateur est aussi un répéteur multiport. La différence entre le concentrateur et le commutateur est que ce dernier prend des décisions en fonction des adresses MAC et que le concentrateur ne prend aucune décision. En raison des décisions qu'il prend, le commutateur rend le réseau local beaucoup plus efficace. Il effectue cela en "commutant" les données uniquement au port auquel le bon hôte est connecté. Par contraste, un concentrateur achemine les données à tous les ports, de sorte que tous les hôtes doivent examiner et traiter (accepter ou rejeter) toutes les données.



Figure 13 : Schéma de commutateur (SWICH).

III-7 Les routeurs

Le routeur fonctionne à la couche réseau du modèle OSI, aussi nommée couche 3. Travailler à la couche 3 permet au routeur de prendre des décisions en fonction de groupes d'adresses réseau (classes), par opposition aux adresses MAC individuelles utilisées à la couche 2. Les

routeurs peuvent aussi connecter différentes technologies de couche 2, telles qu'Ethernet, l'anneau à jeton et l'interface FDDI. En raison de leur capacité d'acheminer les paquets en fonction de l'information de couche 3, les routeurs sont devenus le fédérateur d'Internet et exécutent le protocole IP.

Le rôle du routeur consiste à examiner les paquets entrants (données de couche 3), à choisir la meilleure voie pour les acheminer sur le réseau et à les commuter ensuite au port de sortie approprié. Sur les grands réseaux, les routeurs sont les dispositifs de régulation du trafic les plus importants. Ils permettent à presque tous les types d'ordinateur de communiquer avec tout ordinateur n'importe où dans le monde !



Figure 14 : Schéma de routeur.

IV- Unités et couches correspondantes

Les ordinateurs hôtes et les serveurs fonctionnent au niveau des couches 2 à 7 et sont responsables de l'encapsulation. Les émetteurs-récepteurs, les répéteurs et les concentrateurs sont tous considérés comme des dispositifs actifs de couche 1, car ils n'agissent que sur les bits et ont besoin d'énergie. Les câbles de raccordement, tableaux de connexions et autres éléments d'interconnexion sont considérés comme des composants passifs de couche 1, car ils fournissent simplement une voie de passage pour le courant (figure 15)

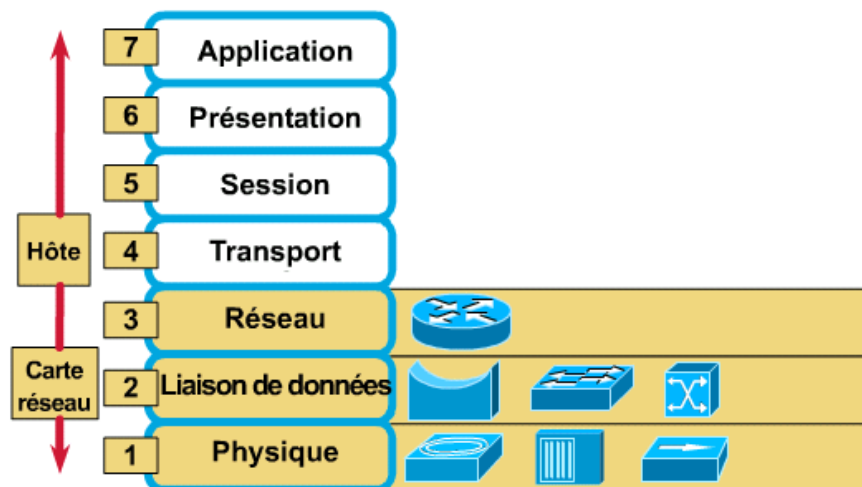


Figure 15 : Les couches et les éléments du réseau correspondant.

À titre de dépositaires des adresses MAC, les cartes réseau sont des dispositifs de couche 2, mais elles sont aussi des dispositifs de couche 1, car elles s'occupent également de signalisation et d'encodage. Les ponts et les commutateurs sont considérés comme des dispositifs de couche 2 parce qu'ils utilisent l'information de couche 2 (adresses MAC) pour décider d'acheminer ou non les trames. Ils fonctionnent aussi à la couche 1 afin de permettre aux bits d'interagir avec le média.

Les routeurs sont considérés comme des unités de couche 3 parce qu'ils utilisent les adresses de couche 3 (adresses réseau) pour optimiser le routage et commuter les paquets sur la bonne route. Les interfaces des routeurs fonctionnent aux couches 1, 2 et 3.

Chapitre 3 : Modèle TCP/IP

I- Introduction

Même si le modèle de référence OSI est universellement reconnu, historiquement et techniquement, la norme ouverte d'Internet est le protocole TCP/IP (pour Transmission Control Protocol/Internet Protocol). Le modèle de référence TCP/IP et la pile de protocoles TCP/IP rendent possible l'échange de données entre deux ordinateurs, partout dans le monde, à une vitesse quasi équivalente à celle de la lumière. Le modèle TCP/IP présente une importance historique tout comme les normes qui ont permis l'essor des industries du téléphone, de l'électricité, du chemin de fer, de la télévision et de la bande vidéo.

II- Les couches du modèle de référence TCP/IP

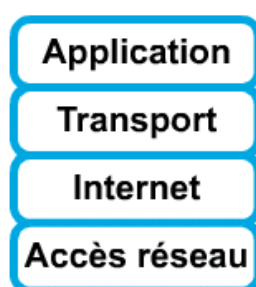


Figure 16 : Les quatre couches du modèle TCP/IP.

Le ministère américain de la Défense a créé le modèle de référence TCP/IP parce qu'il avait besoin d'un réseau pouvant résister à toutes les conditions, même à une guerre nucléaire. Imaginez en effet un monde en guerre, quadrillé de connexions de toutes sortes - fils, micro-ondes, fibres optiques et liaisons satellites. Imaginez ensuite que vous ayez besoin de faire circuler l'information/les données (sous forme de paquets), peu importe la situation d'un nœud ou d'un réseau particulier de l'inter-réseau (qui pourrait avoir été détruit par la guerre). Le ministère de la Défense veut que ses paquets se rendent chaque fois d'un point quelconque à tout autre point, peu importe les conditions. C'est ce problème de conception très épineux qui a mené à la création du modèle TCP/IP, qui, depuis lors, est devenu la norme sur laquelle repose Internet.

Lors de vos lectures sur les couches du modèle TCP/IP, gardez à l'esprit le but initial d'Internet, cela vous aidera à comprendre pourquoi certaines choses sont ainsi. Le modèle TCP/IP comporte quatre couches : la couche application, la couche de transport, la couche Internet et la couche d'accès réseau. Remarquez que certaines couches du modèle TCP/IP portent le même nom que des couches du modèle OSI. Il ne faut pas confondre les couches des deux modèles, car la couche application comporte des fonctions différentes dans chaque modèle.

II-1 La couche application

Les concepteurs de TCP/IP estimaient que les protocoles de niveau supérieur devaient inclure les détails des couches session et présentation. Ils ont donc simplement créé une couche application qui gère les protocoles de haut niveau, les questions de représentation, le code et

le contrôle du dialogue. Le modèle TCP/IP regroupe en une seule couche tous les aspects liés aux applications et suppose que les données sont préparées de manière adéquate pour la couche suivante.

II-2 La couche de transport

La couche de transport est chargée des questions de qualité de service touchant la fiabilité, le contrôle de flux et la correction des erreurs. L'un de ses protocoles, TCP (Transmission Control Protocol - protocole de contrôle de transmission), fournit d'excellentes façons de créer en souplesse des communications réseau fiables, circulant bien et présentant un taux d'erreurs peu élevé. Le protocole TCP est **orienté connexion**. Il établit un dialogue entre l'ordinateur source et l'ordinateur de destination pendant qu'il prépare l'information de couche application en unités appelées segments. Un protocole orienté connexion ne signifie pas qu'il existe un circuit entre les ordinateurs en communication (ce qui correspondrait à la commutation de circuits). Ce type de fonctionnement indique qu'il y a un échange de segments de couche 4 entre les deux ordinateurs hôtes afin de confirmer l'existence logique de la connexion pendant un certain temps. C'est ce qu'on appelle la commutation de paquets.

II-3 La couche Internet

Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'inter-réseau et à les acheminer à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche s'appelle IP (Internet Protocol - protocole Internet). L'identification du meilleur trajet et la commutation de paquets ont lieu à cette couche. Pensez au système postal. Lorsque vous postez une lettre, vous ne savez pas comment elle arrive à destination (il existe plusieurs routes possibles), tout ce qui vous importe c'est qu'elle se rende.

II-4 La couche d'accès réseau

Le nom de cette couche a un sens très large et peut parfois prêter à confusion. On l'appelle également la couche hôte-réseau. Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies de réseau local et de réseau longue distance, ainsi que tous les détails dans les couches physique et liaison de données du modèle OSI.

III- Schéma de protocoles TCP/IP

Le diagramme illustré dans la figure 17 s'appelle un schéma de protocoles. Il présente certains protocoles communs spécifiés par le modèle de référence TCP/IP. À la couche application, vous ne reconnaîtrez peut-être pas certaines tâches réseau, mais vous les utilisez probablement tous les jours en tant qu'internaute. Ces applications sont les suivantes :

- FTP - Protocole de transfert de fichiers ou protocole FTP
- HTTP - Protocole HTTP (Hypertext Transfer Protocol)
- SMTP - Protocole SMTP (Simple Mail Transport protocol)
- DNS - Système DNS (Domain Name Service)
- TFTP - Protocole TFTP (Trivial File Transport Protocol)

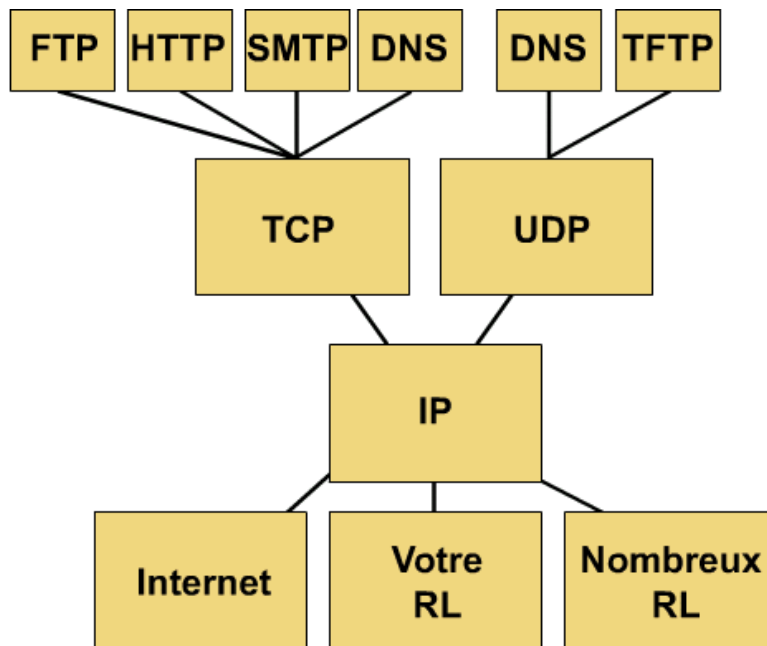


Figure 17 : Exemples de protocole de chaque couche du modèle TCP/IP.

Le modèle TCP/IP met l'accent sur une souplesse maximale, à la couche application, à l'intention des développeurs de logiciels. La couche de transport fait appel à deux protocoles - le protocole TCP (protocole de contrôle de transmission) et le protocole *UDP* (*protocole de datagramme utilisateur*). La couche inférieure, soit la couche réseau, se rapporte à la technologie de réseau local ou de réseau longue distance utilisée.

Dans le modèle TCP/IP, peu importe l'application qui demande des services réseau et le protocole de transport utilisé, il n'y a qu'un seul protocole réseau : IP (Internet Protocol). C'est une décision de conception délibérée. *IP* est le protocole universel qui permet à un ordinateur quelconque de communiquer en tout temps.

IV- Comparaison du modèle OSI et du modèle TCP/IP

En comparant le modèle OSI au modèle TCP/IP, vous remarquerez des similitudes et des différences. Voici des exemples :

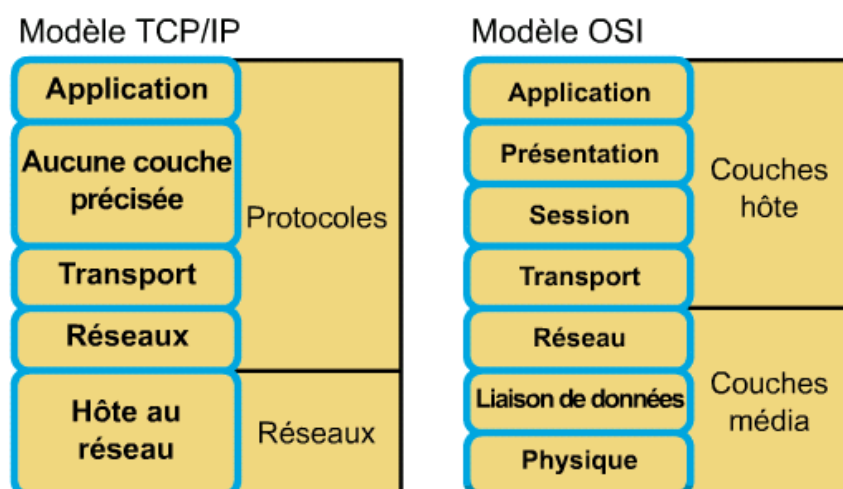


Figure 18 : Comparaison des modèles OSI et TCP/IP.

Similitudes

- Tous deux comportent des couches.
- Tous deux comportent une couche application, bien que chacune fournisse des services très différents.
- Tous deux comportent des couches réseau et transport comparables.
- Tous deux supposent la technologie de commutation de paquets (et non de commutation de circuits).
- Les professionnels du réseau doivent connaître les deux modèles.

Différences

- TCP/IP intègre la couche de présentation et la couche session dans sa couche application.
- TCP/IP regroupe les couches physique et liaison de données OSI en une seule couche accès réseau.
- TCP/IP semble plus simple, car il comporte moins de couches.
- Les protocoles TCP/IP constituent la norme sur laquelle s'articule Internet, aussi le modèle TCP/IP a acquis sa crédibilité en raison de ses protocoles. Par contraste, aucun réseau ne s'articule sur des protocoles particuliers au modèle OSI, même si tous se servent du modèle OSI comme guide.

Chapitre 4 : Couche Réseau : Routage et Adressage

I- L'importance de la couche réseau

I-1 Identificateurs

La couche réseau assure le transport des données parmi un ensemble de réseaux (inter-réseau). Les unités utilisent le système d'adressage de la couche réseau pour déterminer la destination des données pendant leur acheminement.

Les protocoles sans couche réseau ne conviennent qu'aux petits réseaux internes. Ces protocoles n'utilisent généralement qu'un nom (l'adresse MAC) pour identifier les ordinateurs d'un réseau. Le défaut de cette méthode est qu'il devient de plus en plus difficile de gérer les noms à mesure que le réseau grandit, en particulier de s'assurer que tous les noms sont uniques.

Les protocoles qui supportent la couche réseau utilisent une technique d'identification des unités qui garantit l'unicité des désignations. Alors en quoi cet identificateur diffère-t-il d'une adresse MAC qui, elle aussi, est unique? Les adresses MAC utilisent un système d'adressage linéaire qui rend difficile la localisation des unités dans d'autres réseaux. Les adresses de couche réseau utilisent un système d'adressage hiérarchique qui garantit des adresses uniques au-delà des limites du réseau, ainsi qu'une méthode de sélection de la voie d'acheminement des données entre les réseaux.

L'adressage hiérarchique permet aux données de circuler dans des réseaux multiples et de trouver leur destination de manière efficace. Le système téléphonique est un exemple de système d'adressage hiérarchique. Le système téléphonique utilise un indicatif régional pour diriger un appel vers son premier relais (saut). Les trois chiffres suivants représentent le central téléphonique local (deuxième saut). Les quatre derniers chiffres sont le numéro de l'abonné demandé (dernier saut, jusqu'à la destination).

Les unités d'un réseau ont besoin d'un système d'adressage cohérent leur permettant d'acheminer des paquets d'un réseau à un autre dans le cadre de l'inter-réseau (ensemble de réseaux segmentés ou non, utilisant le même système d'adressage). Les unités utilisent le système d'adressage de la couche réseau pour déterminer la destination des données tout au long de leur cheminement dans l'inter-réseau

I-2 Segmentation et systèmes autonomes

La multiplication des réseaux résulte de deux tendances fondamentales : l'augmentation de la taille de chaque réseau et la création constante de nouveaux réseaux.

Lorsqu'un réseau local, un réseau métropolitain ou un réseau longue distance prend de l'expansion, il devient nécessaire - pour des raisons pratiques de gestion du trafic - de le subdiviser en réseaux plus petits appelés segments réseau (ou simplement segments). Notre grand réseau devient donc une mosaïque de réseaux plus petits dont chacun a besoin d'une adresse distincte.

Il existe déjà un grand nombre de réseaux; des réseaux privés sont répandus dans les bureaux, les écoles, les entreprises et les organisations gouvernementales. Tous ces réseaux distincts (ou systèmes autonomes s'ils sont gérés par un seul administrateur réseau) souhaitent

communiquer par l'entremise d'Internet, mais leur interconnexion exige des systèmes d'adressage efficaces et des interfaces appropriées. Si ce n'est pas le cas, il se produira des embouteillages affectant le fonctionnement des réseaux locaux et aussi celui d'Internet.

Pour comprendre la nécessité de la segmentation des réseaux, pensez à un réseau routier et aux véhicules qui y circulent. À mesure que la population des communautés desservies augmente, les routes deviennent de plus en plus encombrées par un nombre croissant de véhicules. Les réseaux fonctionnent de manière très semblable. À mesure que les réseaux s'étendent, le trafic augmente. Comme première solution, on peut augmenter la largeur de bande, ce qui équivaut à élever la limite de vitesse ou à ajouter des voies sur les autoroutes. Une autre solution consiste à utiliser des unités de régulation pour segmenter le réseau et gérer le trafic, de la même façon qu'on utilise les feux de circulation pour régulariser le trafic routier.

I-3 Les communications entre réseaux

Internet est un ensemble de segments de réseaux interconnectés pour faciliter les échanges d'information. Une fois de plus, l'analogie avec le réseau routier est valable avec ses autoroutes à voies multiples servant à relier rapidement les grandes régions géographiques. Les réseaux fonctionnent de façon très semblable grâce à l'apparition de compagnies appelées fournisseurs de services Internet (FSI), qui offrent des services d'interconnexion aux propriétaires de réseaux autonomes.

I-4 Unités réseau de la couche réseau

Comme on l'avait déjà vu au chapitre précédent, les unités d'interconnexion de réseaux (routeurs) qui appartiennent à la couche 3 (couche réseau) du modèle OSI relient des segments de réseau ou des réseaux entiers. Leur rôle consiste à acheminer les paquets de données entre les réseaux en fonction de l'information du protocole réseau de la couche 3.

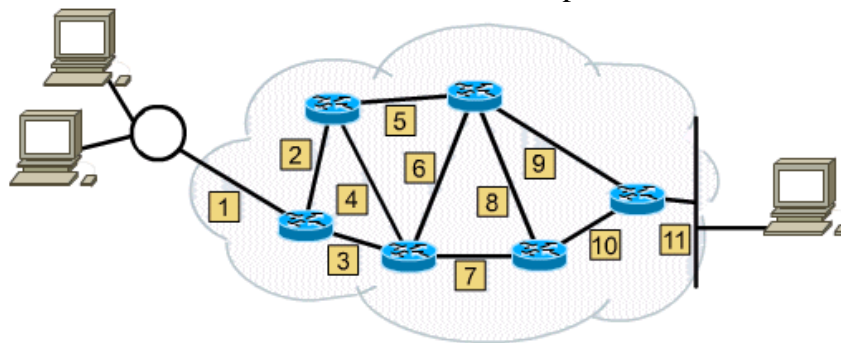


Figure 19 : Routeurs unité de la couche réseau.

Les routeurs prennent des décisions logiques d'optimisation pour choisir la meilleure voie d'acheminement des données d'un réseau à un autre et dirigent ensuite les paquets vers le port de sortie qui correspond au segment de réseau suivant. Le routeur reçoit des paquets de données des unités (postes de travail, etc.) d'un réseau local et, en fonction de l'information de couche 3, les achemine dans l'inter-réseau. Le routage est parfois appelé commutation de couche 3.

II- La sélection de la voie

II-1 Sélection de la voie

La sélection de la voie se fait au niveau de la couche 3 (couche réseau); elle permet au routeur d'évaluer l'état des circuits menant à une certaine destination et d'établir la voie optimale pour un paquet particulier. Les services de routage utilisent l'information de topologie du réseau dans l'évaluation des voies. La sélection de la voie est le processus que le routeur utilise pour choisir le prochain saut du trajet que le paquet empruntera vers sa destination. Ce processus est également appelé le routage du paquet.

La sélection de la voie pour un paquet peut être comparée au cheminement d'un automobiliste qui traverse une ville. Il dispose d'un plan montrant tous les itinéraires qui lui permettent de se rendre à destination. Le trajet d'une intersection à la suivante est un "saut". De même, le routeur utilise un "plan" qui présente toutes les voies possibles vers une destination donnée. Les routeurs prennent aussi des décisions en fonction de la densité du trafic et du débit des liaisons (bande passante), tout comme notre automobiliste peut choisir une voie rapide (une autoroute) ou des rues secondaires moins achalandées.

II-2 Adressage de couche réseau

L'adresse réseau permet au routeur de choisir une voie optimale au sein du réseau. Le routeur utilise les adresses réseau pour identifier le réseau de destination d'un paquet à l'intérieur d'un inter réseau. Dans certains protocoles de couche réseau, l'administrateur du réseau attribue les adresses réseau en fonction d'un plan d'adressage inter-réseau prédéterminé. Dans d'autres protocoles de couche réseau, l'attribution d'adresses est effectuée partiellement ou entièrement de façon dynamique ou automatique. En plus des adresses réseau, les protocoles réseau utilisent une forme quelconque d'adresse de l'hôte ou du nœud. Le schéma illustre trois unités du réseau 1 (deux postes de travail et un routeur), chacun ayant sa propre adresse d'hôte (on voit également que le routeur est relié à deux autres réseaux : les réseaux 2 et 3).

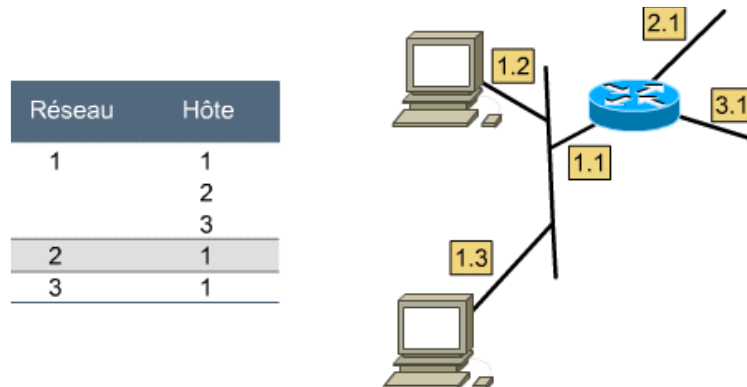


Figure 20 : Adressage des hôtes.

L'adressage est effectué par la couche réseau. Dans l'analogie du numéro de téléphone utilisée pour décrire une adresse réseau, les premières parties (indicatif régional et numéro de central) constituaient l'adresse du central de rattachement du destinataire. Les quatre derniers chiffres, indiquant au commutateur local à quelle ligne de téléphone il doit acheminer l'appel, correspondent à la partie hôte de l'adresse, qui précise l'identité du dispositif de destination.

Sans adressage de couche réseau, le routage devient impossible. Les routeurs ont besoin de l'adresse réseau pour assurer la livraison sans erreur des paquets. Sans une forme quelconque de structure d'adressage hiérarchique, il serait impossible d'acheminer les paquets au sein d'un

inter-réseau. D'une manière analogue, sans structure hiérarchique pour les numéros de téléphone, les adresses postales ou les systèmes de transport, la livraison des biens et des services serait infiniment plus complexe.

II-3 Couche 3 et mobilité de l'ordinateur

L'adresse MAC (physique) est comme le nom d'une personne ; son adresse réseau (logique) est comme son adresse postale. Lorsqu'une personne déménage dans une autre ville, elle conserve son nom, mais son adresse postale indique son nouvel emplacement. Les unités réseau (tant les routeurs que les ordinateurs individuels) sont dotées d'une adresse MAC et d'une adresse de protocole (couche réseau). Si un ordinateur est déplacé physiquement à un réseau différent, il conserve son adresse MAC, mais une nouvelle adresse réseau doit lui être attribuée.

II-4 Comparaison de l'adressage linéaire et de l'adressage hiérarchique

Le rôle de la couche réseau est de trouver la meilleure voie au sein d'un réseau. Pour ce faire, elle utilise deux méthodes d'adressage : l'adressage linéaire et l'adressage hiérarchique. Un système d'adressage linéaire attribue à une unité la prochaine adresse disponible. Aucune importance n'est accordée à la structure du système d'adressage. Les adresses MAC fonctionnent de cette manière. Un fournisseur reçoit un bloc d'adresses ; la première portion de chaque adresse représente le code du fournisseur, le reste de l'adresse MAC est un numéro aléatoire attribué selon un système de numérotation séquentiel.

Dans un système d'adressage hiérarchique, comme celui que le système des postes utilise pour les codes postaux, l'adresse est déterminée par l'emplacement de la maison et non par un numéro attribué au hasard. Le système d'adressage qui utilise le protocole Internet (IP) a une structure spécifique et ces adresses IP ne sont pas attribuées de manière aléatoire.

III- Les adresses IP dans l'en-tête IP

III-1 Datagrammes de couche réseau

Le protocole Internet (IP) est la méthode d'adressage privilégiée des réseaux hiérarchiques. Le protocole IP est le protocole réseau d'Internet. À mesure que les données circulent vers le bas du modèle OSI, les données sont encapsulées à chaque couche. À la couche réseau, les données sont encapsulées dans des paquets (aussi appelés datagrammes). Le protocole IP détermine le format de l'en-tête IP (qui comprend l'information d'adressage et de contrôle), mais ne se préoccupe pas des données proprement dites; il accepte tout ce qui provient des couches supérieures.

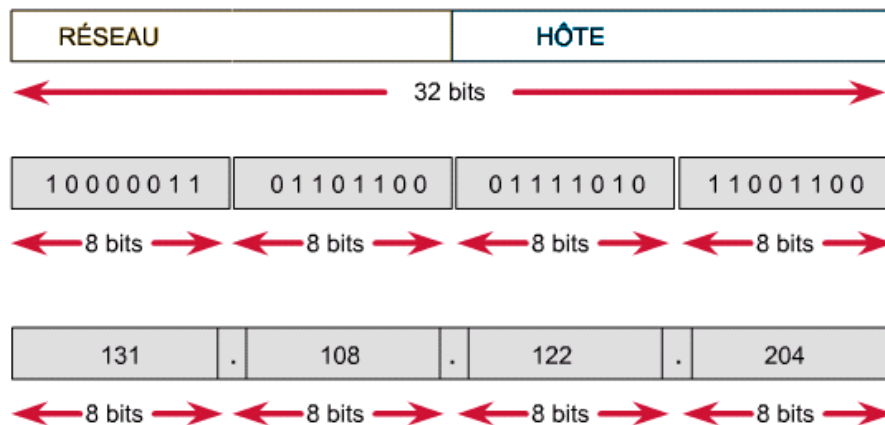


Figure 21 : NetID et hostID.

III-2 Champs de couche réseau

Le paquet ou datagramme de couche 3 devient les données de la couche 2, qui sont ensuite encapsulées en trames (comme nous l'avons déjà mentionné). De même, le paquet IP est composé des données des couches supérieures plus un en-tête IP constitué des éléments suivants :

0		4		8		16		19		24		31	
VERS		HLEN		Type de service		Longueur totale							
Identification						Indicateurs		Décalage fragment					
Durée de vie				Protocole		Total de contrôle d'en-tête							
Adresse IP source													
Adresse IP de destination													
Options IP (s'il y a lieu)										Remplissage			
Données													
...													

Figure 22 Champs d'un paquet IP.

- VERS : indique la version de protocole IP utilisée (4 bits)
- HLEN (IP header length) : indique la longueur de l'en-tête du datagramme en mots de 32 bits (4 bits)
- Type de service : indique l'importance qui lui a été accordé par un protocole de couche supérieure donné (8 bits)
- Longueur totale : précise la longueur du paquet IP en entier, y compris les données et l'en-tête, en octets (16 bits)
- Identification : contient un nombre entier qui identifie le datagramme actuel (16 bits)

- Indicateurs : un champ de 3 bits dont les 2 bits inférieurs contrôlent la fragmentation – un bit précise si le paquet peut être fragmenté et le second indique si le paquet est le dernier fragment d'une série de paquets fragmentés (3 bits)
- Décalage de fragment : ce champ sert à rassembler les fragments du datagramme (16 bits)
- Durée de vie minimum : 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)
- Protocole : précise le protocole de couche supérieure qui recevra les paquets entrants après la fin du traitement IP (8 bits)
- Total de contrôle d'en-tête : assure l'intégrité de l'en-tête IP (16 bits)
- Adresse source : précise le nœud émetteur (32 bits)
- Adresse de destination : précise le nœud récepteur (32 bits)
- Options : permet au protocole IP de supporter différentes options, telle la sécurité (longueur variable)
- Données : contient de l'information de couche supérieure (longueur variable, maximum 64 Ko)
- Remplissage : des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits

III-3 Champs source et de destination de l'en-tête IP

L'adresse IP contient l'information nécessaire pour le routage d'un paquet au sein du réseau. Chaque champ d'adresse source et de destination en IPv4 contient une adresse de 32 bits. Le champ d'adresse source contient l'adresse IP de l'unité qui envoie le paquet. Le champ de destination contient l'adresse IP de l'unité qui reçoit le paquet.

III-4 Adresse IP comme nombre binaire 32 bits

Une adresse IP est représentée par un nombre binaire de 32 bits. Dans un nombre binaire, la valeur du bit à l'extrême droite (bit le moins significatif) est soit 0 ou 1. La valeur décimale correspondant à chaque bit d'un nombre binaire double chaque fois que vous vous déplacez d'une position vers la gauche. Ainsi, la valeur décimale du deuxième bit à partir de la droite est soit 0 ou 2. Le troisième bit est soit 0 ou 4; le quatrième, 0 ou 8, etc.

Les adresses IP sont présentées en format décimal 32 bits. Les 32 bits de l'adresse sont subdivisés en quatre octets (un octet est un groupe de 8 bits). La valeur décimale maximale d'un octet est de 255 (le plus grand nombre binaire de huit bits est 11111111 et ces bits, de droite à gauche, ont des valeurs décimales de 1, 2, 4, 8, 16, 32, 64 et 128 pour un total de 255).

III-5 Champs de l'adresse IP

Le numéro de réseau d'une adresse IP précise le réseau auquel une unité est connectée alors que la portion hôte d'une adresse IP pointe au dispositif spécifique au sein de ce réseau. Puisque les adresses IP sont composées de quatre octets séparés par des points, un, deux ou trois de ces octets peuvent servir à déterminer le numéro de réseau. De même, un, deux ou trois de ces octets peuvent servir à déterminer la partie hôte d'une adresse IP.

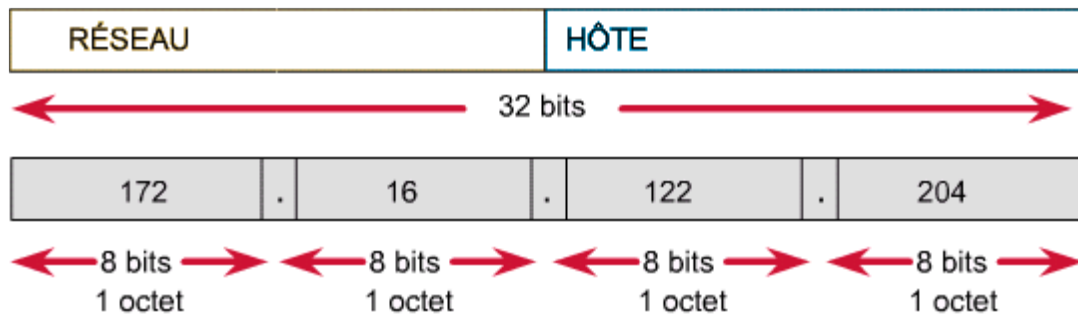


Figure 23 : NetID et hostID.

IV- Les classes d'adresses IP

IV-1 Classes d'adresses IP

Un organisme peut recevoir trois classes d'adresses IP de l'ARIN (ou de son fournisseur de services Internet). Il s'agit des classes A, B et C. L'ARIN réserve maintenant les adresses de classe A aux gouvernements de par le monde (bien que certaines grandes entreprises, telles que Hewlett Packard, en ont déjà reçues) et les adresses de classe B aux entreprises de taille moyenne. Tous les autres demandeurs reçoivent des adresses de classe C.

IV-1-1 Classe A

En format binaire, le premier bit (à l'extrême gauche) d'une adresse de classe A est toujours 0. Un exemple d'adresse IP de classe A serait 124.95.44.15. Le premier octet, 124, représente le numéro de réseau attribué par l'ARIN. Les administrateurs internes du réseau attribuent les valeurs des 24 bits qui restent. Pour déterminer si une unité fait partie d'un réseau de classe A, il suffit de regarder le premier octet de son adresse IP, qui variera entre 0 et 126. (127 commence avec un bit à 0, mais cette valeur est réservée à des fins particulières).

Toutes les adresses IP de classe A n'utilisent que les huit premiers bits pour indiquer la partie réseau de l'adresse. Les trois octets restants peuvent servir pour la portion hôte de l'adresse. Les réseaux qui utilisent un système d'adressage IP de classe A peuvent attribuer jusqu'à $2^{24} - 2$ soit 16 777 214 adresses IP aux unités qui en font partie.



Figure 24 : NetID et hostID de la classe A

IV-1-2 Classe B

Les deux premiers bits d'une adresse de classe B sont toujours 10 (un et zéro). Un exemple d'adresse IP de classe B serait 151.10.13.28. Les deux premiers octets représentent le numéro de réseau attribué par l'ARIN. Les administrateurs internes du réseau attribuent les valeurs des 16 bits qui restent. Pour déterminer si une unité fait partie d'un réseau de classe B, il suffit de regarder le premier octet de son adresse IP. La valeur du premier octet des adresses IP de classe B varie entre 128 et 191.

Toutes les adresses IP de classe B utilisent les 16 premiers bits pour indiquer la partie réseau de l'adresse. Les deux octets restants de l'adresse IP sont réservés à la portion hôte de l'adresse. Les réseaux qui utilisent un système d'adressage IP de classe B peuvent attribuer jusqu'à $2^{16} - 2$ soit 65 534 adresses IP aux unités qui en font partie.



Figure 25 : NetID et hostID de la classe B

IV-1-3 Classe C

Les trois premiers bits d'une adresse de classe C sont toujours 110 (un, un et zéro). Un exemple d'adresse IP de classe C serait 201.110.213.28. Les trois premiers octets représentent le numéro de réseau attribué par l'ARIN. Les administrateurs internes du réseau attribuent les valeurs des 8 bits qui restent. Pour déterminer si une unité fait partie d'un réseau de classe C, il suffit de regarder le premier octet de son adresse IP. La valeur du premier octet des adresses IP de classe C varie entre 192 et 223.

Toutes les adresses IP de classe C utilisent les 24 premiers bits pour indiquer la partie réseau de l'adresse. Seul le dernier octet d'une adresse IP de classe C est réservé à la portion hôte de l'adresse. Les réseaux qui utilisent un système d'adressage IP de classe C peuvent attribuer jusqu'à $2^8 - 2$ soit 254 adresses IP aux unités qui en font partie.



Figure 26 : NetID et hostID de la classe C

IV-2 Adresses IP exprimées en nombres décimaux

Les adresses IP identifient les unités d'un réseau, ainsi que le réseau auquel elles sont connectées. Pour faciliter leur mémorisation, les adresses IP sont généralement exprimées en notation décimale (quatre nombre décimaux séparés par des points, 166.122.23.130, par exemple - rappelez-vous qu'un nombre décimal est un nombre en base 10, le système de numération que nous utilisons quotidiennement).

V- L'espace adresse réservé

V-1 Buts des ID réseau et des adresses de diffusion

Si votre ordinateur voulait communiquer avec toutes les unités d'un réseau, il serait difficile de lister les adresses IP de chacune de ces unités. Vous pourriez préciser deux adresses séparées par un tiret pour représenter toutes les unités au sein de cette plage de nombres, mais cette solution n'est guère plus pratique. Il existe, toutefois, une méthode plus efficace.

Une adresse IP dont tous les bits hôte sont occupés par des zéros binaires est réservée à l'adresse réseau. Ainsi, dans un réseau de classe A, 113.0.0.0 est l'adresse IP du réseau comprenant l'hôte 113.1.2.3. Un routeur utilise l'adresse IP d'un réseau pour acheminer des données sur Internet. Dans un réseau de classe B, l'adresse IP 176.10.0.0 est une adresse de réseau.

Les nombres décimaux qui composent les deux premiers octets d'une adresse de réseau de classe B sont attribués et représentent les numéros de réseau. Les deux derniers octets contiennent des 0, parce que ces 16 bits sont des numéros d'hôte et sont réservés aux unités qui sont connectées au réseau. L'adresse IP de notre exemple (176.10.0.0) est réservée à l'adresse de réseau. Elle ne sera jamais utilisée comme adresse pour une unité connectée au réseau.

Pour envoyer des données à toutes les unités d'un réseau, il vous faudrait utiliser une adresse de diffusion. Une diffusion se produit lorsqu'une source envoie des données à toutes les unités d'un réseau. Pour s'assurer que toutes les unités d'un réseau tiennent compte d'un tel message de diffusion, la source doit utiliser une adresse IP que toutes les unités peuvent reconnaître et recevoir. Les adresses de diffusion IP se terminent par des 1 binaires dans toute la portion hôte de l'adresse (le champ hôte).

Dans le cas du réseau cité en exemple (176.10.0.0), dans lequel les 16 derniers bits constituent le champ hôte (ou portion hôte de l'adresse), le message de diffusion envoyé à toutes les unités du réseau comprendrait l'adresse de destination 176.10.255.255 (puisque 255 est la valeur décimale de l'octet binaire 11111111).

V-2 ID réseau

Il est essentiel de comprendre l'importance de la portion réseau d'une adresse IP - l'ID réseau. Les hôtes d'un réseau ne peuvent communiquer directement qu'avec les unités qui partagent la même ID réseau. Ils peuvent partager le même segment physique, mais s'ils ont des numéros de réseau différents, la communication entre eux est habituellement impossible, à moins qu'une autre unité puisse établir la connexion entre les réseaux.

V-3 Analogie pour les ID réseau

Les codes postaux et les ID réseau fonctionnent de façon très semblable. Les codes postaux permettent au système des postes d'acheminer votre courrier à votre bureau de poste local, et ensuite, à votre quartier. De là, l'adresse postale permet au facteur de déposer votre courrier dans votre boîte aux lettres. Alors que l'ID réseau permet à un routeur de mettre un paquet dans le bon segment de réseau, l'ID hôte aide le routeur à acheminer la trame de couche 2 (en encapsulant le paquet) à l'hôte de destination précis au sein de ce réseau.

VI- Subnetting TCP/IP

VI-1 L'adressage IP

Quand un ordinateur cherche à communiquer avec un autre ordinateur ou avec un périphérique réseau quelconque en utilisant le protocole TCP/IP, la procédure suivante se déroule :

1. Le nom de la machine est transformé en une adresse TCP/IP. Ceci est effectué par le résolveur qui utilise un service de nommage (table hosts, DNS).
2. Les routines des couches TCP/IP associent ce numéro et le masque de réseau pour déterminer si la machine à atteindre fait ou non partie de même réseau.

1. Si oui, l'adresse TCP/IP est résolue en une adresse Ethernet; une trame est alors formée avec cette dernière et est envoyée sur le réseau.

2. Sinon, et s'il existe une table de routage, l'adresse Ethernet du routeur est utilisée pour former une trame qui est envoyée sur le réseau (donc vers le routeur approprié).
3. Sinon, un message d'erreur est renvoyé vers le programme utilisateur (celui qui cherchait à envoyer des données). Ce message indique que l'adresse de la machine destinataire est impossible à joindre.

Pour réaliser le masquage, on utilise l'opération AND binaire. Tout d'abord, les différentes classes d'adresses utilisables peuvent être représentées comme suit ; chaque adresse ayant une largeur totale de 4 octets, soit 32 bits.

Si on somme bit à bit ces deux valeurs (opération 'OU binaire'), on obtient l'adresse du réseau qui est indispensable pour savoir comment expédier le paquet TCP/IP, c'est à dire : 12.0.0.0.

Autre exemple, si on a un réseau de classe B (sans sous-réseau), le masque par défaut est de 255.255.0.0. La machine dont l'adresse TCP/IP est 171.21.36.12 appartient au réseau 171.21.0.0 (AND binaire entre 171.21.36.12 et 255.255.0.0).

L'utilisation de TCP/IP oblige donc de choisir une classe d'adresse. Chaque classe proposée offre un compromis entre le nombre maximum de réseaux et le nombre de machines.

Nom de la classe	Numéros TCP/IP	Nombre max de réseaux pour la classe	Nombre maxi de machines par réseau
Classe A	0.x.x.x 127.x.x.x	127	16 777 216
Classe B	128.x.x.x 191.x.x.x	16383	65534
Classe C	192.x.x.x 223.x.x.x	2 031 616	254

On le voit, plus le nombre de réseaux par classe est important, moins le nombre possible de machines est important.

Note : Dans la classe A, le réseau 127 tient une place à part. Conventionnellement, il désigne l'adresse de la machine (moi-même) dans le contexte TCP/IP. La table « hosts » de toute machine comporte par exemple la mention "127.0.0.1 localhost". Tout autre numéro de ce réseau peut être utilisé pour cet usage.

On peut alors choisir, à partir du nombre de machines que l'on compte mettre en œuvre, le type de classe le plus approprié.

Pour trouver à quelle classe appartient une machine donnée, il suffit de repérer la valeur du premier octet de l'adresse TCP/IP. L'adresse 174.23.2.45 est par exemple une adresse de classe B, car le premier octet, 174, est compris entre 128 et 191. L'adresse 5.6.7.8 est une adresse de classe A.

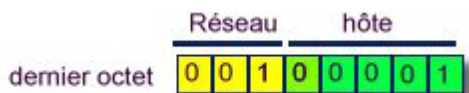
VI-2 Les adresses TCP/IP réservées ("privées").

Il existe aussi, à l'intérieur de chaque classe, un sous-ensemble d'adresses qui sont destinées à un usage privé. Ce qui signifie que tout routeur du marché ne routera pas, par défaut, ces adresses sur Internet. Plusieurs réseaux locaux utilisent donc ces adresses pour leur usage interne. Il n'y a pas de conflit, puisque ce sont des réseaux privés dont les adresses ne sont pas accessibles depuis Internet. Ces adresses sont définies dans la RFC1918 :

1. pour la classe A les adresses 10.x.x.x
2. pour la classe B les adresses 172.16.x.x à 172.31.x.x
3. pour la classe B les adresses 192.168.x.x

204.34.57.0 (bits de sous-réseau = 000)
 204.34.57.32 (bits de sous-réseau = 001)
 204.34.57.64 (bits de sous-réseau = 010)
 204.34.57.96 (bits de sous-réseau = 011)
 204.34.57.128 (bits de sous-réseau = 100)
 204.34.57.160 (bits de sous-réseau = 101)
 204.34.57.192 (bits de sous-réseau = 110)
 204.34.57.224 (bits de sous-réseau = 111)

Remarquez bien que l'on utilise les combinaisons 000 et 111 pour ces sous-réseaux. La RFC950 qui stipulait que la première et la dernière adresse d'un réseau ne devaient pas être utilisées, est maintenant obsolète. En effet, la plupart des routeurs modernes savent très bien gérer des adresses réseau dont tous les bits de sous-réseau sont à 1 ou à 0. Pour plus de précision, reportez-vous à la RFC1878 qui propose un découpage en sous-réseaux indépendant des classes (voir également CIDR ci-dessous). Pour notre exemple, on obtient donc 8 sous-réseaux possibles. Les bits de poids faibles (les bits les plus à droite) vont indiquer, pour chacun de ces sous-réseaux, les adresses à allouer aux machines. Par exemple, dans le réseau 204.34.57.32, la première machine portera l'adresse 1. Le dernier octet aura alors la valeur suivante :



soit 33. L'adresse TCP/IP complète sera donc 204.34.57.33. Ainsi de suite jusqu'à 204.34.57.62. On ne peut utiliser l'adresse 204.34.57.63 pour une machine, car elle correspond à l'adresse de broadcast du sous-réseau 204.34.57.32.

Ensuite, dans le réseau 204.34.57.64, la première machine aura pour adresse 204.34.57.65 et ainsi de suite.

En procédant ainsi, on a découpé un espace où l'on pouvait initialement allouer 254 machines en 8 sous-réseaux dans lesquels on ne peut allouer au total que 8 fois 30 machines. Le tableau ci-dessous montre, en fonction des bits alloués soit au réseau soit aux hôtes, les différentes possibilités envisageables en classe C.

bits réseau/ bits hôte	nb de sous- réseaux	nb d'hôtes	masque
1 / 7	2	126	255.255. 255.128
2 / 6	4	62	255.255. 255.192
3 / 5	8	30	255.255. 255.224
4 / 4	16	14	255.255. 255.240
5 / 3	32	6	255.255. 255.248
6 / 2	64	2	255.255. 255.252

7 / 1	128	0	255.255. 255.254
-------	-----	---	---------------------

La dernière ligne est à écarter, pour des raisons évidentes. Il reste donc 6 possibilités de découpage en classe C. En classe B, ces possibilités sont différentes, mais les contraintes sont les mêmes.

VI-6 Les nouveaux masques réseau.

Avec ces nouveaux sous-réseaux, on doit également modifier le masque de réseau. Dans le cas ci-dessus, le masque initial fourni pour la classe C était de 255.255.255.0. Mais on a utilisé les trois bits de poids fort du dernier octet pour coder les sous-réseaux. Il faut donc rajouter au masque initial le masque de sous-réseau. Ce dernier vaut 32+64+128, soit 224. Le nouveau masque réseau est donc $255.255.255.0 + 224 = 255.255.255.224$.

Ce nouveau masque s'applique à tous les 8 sous-réseaux de l'exemple ci-dessus, puisque les trois bits de poids 32, 64 et 128 sont affectés à la fonction "sous-réseau".

Pour résumer, le masque ne dépend que du nombre de bits affectés au réseau et au sous-réseau : il suffit de positionner ces bits à 1 et de faire une somme binaire (un 'OU binaire') pour obtenir le masque.

Ce masque de réseau est important, car il va déterminer l'adresse de diffusion (broadcast) et, partant, limiter les diffusions aux seules machines faisant partie d'un sous-réseau déterminé.

VI-7 Les adresses de diffusion (broadcast).

Chaque sous-réseau ainsi constitué doit avoir une adresse réseau, un masque de réseau et une adresse de diffusion (broadcast). L'adresse de diffusion est simple à calculer : elle correspond à l'adresse du réseau ou du sous-réseau plus l'adresse de l'hôte dont tous les bits sont à 1.

Chaque sous-réseau possède une adresse de diffusion propre.

Dans le cas du sous-réseau 204.34.57.32, le numéro d'hôte dont tous les bits (les bits à droite de la figure ci-dessus) sont à 1 est 31. Si on ajoute ce nombre à l'adresse du réseau, on obtient $204.34.57.32 + 31 = 204.34.57.63$.

VI-8 Le cas du réseau de classe B.

Dans le cas d'un réseau de classe B, s'il n'y pas de sous-réseau, deux octets sont utilisés pour numéroté les machines. C'est sur l'ensemble de ces deux octets que vont s'effectuer les redécoupages. Il y a bien sûr plus de possibilités de découpage qu'en classe C, mais la démarche reste identique.

bits réseau/ bits hôte	nb de sous- réseaux	nb d'hôtes	masque
1 / 15	2	32766	255.255.1 28.0
2 / 14	4	16382	255.255.1 92.0
3 / 13	8	8190	255.255.2 24.0
4 / 12	16	4094	255.255.2 40.0
5 / 11	32	2046	255.255.2 48.0

6 / 10	64	1022	255.255.252.0
7 / 9	128	510	255.255.254.0
8 / 8	255	254	255.255.255.0

VI-9 Le cas du réseau de classe A.

Dans le cas d'un réseau de classe A, trois octets sont utilisés pour numéroté les machines. C'est sur l'ensemble de trois octets que vont s'effectuer les redécoupages.

VI-10 Plus de classe : le CIDR.

Maintenant que vous avez assimilé cette méthode un petit peu complexe, oubliez là. En voici une à la fois plus simple et plus générale.

Vous savez sans doute que l'on va bientôt arriver à une pénurie d'adresses TCP/IP sur Internet. Pourquoi ? Supposons par exemple que vous ayez 300 machines à installer sur un réseau connecté à l'Internet. Si vous vous faites allouer un réseau de classe B avec 65535 adresses, la plupart ne seront donc pas utilisées.

Partant de ce constat, les organismes chargés d'allouer les adresses ont décidé d'abandonner ce découpage en classes et de proposer le CIDR (Classless Inter Domain Routing) qui est détaillé dans la RFC1519. Ce procédé vise à :

1. alléger les tables de routage sur les routeurs Internet
2. optimiser l'allocation d'adresses en évitant le gaspillage actuel.

Ce procédé consiste à allouer un lot de plusieurs adresses, et un masque de réseau associé qui couvre ces adresses. Par exemple, si on désire 300 adresses, il faut fournir un lot d'adresses correspondant à plusieurs adresses de réseau en classe C :

204.34.50.0 soit 254 hôtes

204.34.51.0 soit 254 hôtes

avec le masque de réseau : 255.255.254.0

Dans ce cas, la notation adoptée est 204.34.50.0/23. Ce qui signifie : adresse de réseau 204.34.50.0 avec un masque de sous réseau de 32 bits dont les 23 bits les plus à gauche sont à 1. Les 9 bits de poids faibles (les plus à droite) sont utilisés pour numéroté les 510 hôtes. Les adresses 204.34.50.0 et 204.34.51.255 étant réservées respectivement pour l'adresse du réseau et l'adresse de diffusion.



En utilisant le CIDR, les fournisseurs d'accès se voient allouer de larges espaces d'adressage qu'ils répartissent ensuite à leurs clients.

Bibliographie

- [1] Andrew S. Tanenbaum « Réseau », Pearson, 4ème édition 2003.
- [2] Guy Pujolle « Les réseaux » Eyrolles. 2008.
- [3] John Davidson « Introduction to a TCP/IP », Springer 1989.