LYCEE TECHNIQUE AL KHAWARIZMI
Safi

1ère année BTS SRI

S3 : RESAUX INFORMATIQUES

S31 : NOTIONS DE BASE SUR LES RESEAUX INFORMATIQUES

PLAN DU SOUS SAVOIR S31

Chapitre	Page
A. Terminologie des réseaux.	3
B. Les modèles OSI et TCP/IP.	6
C. Fonctionnalité et protocoles des couches applicatives.	13
D. Couche transport OSI.	15
E. Couche réseau OSI.	19
F. Adressage du réseau : IPv4.	23
G. Couche liaison de données.	35
H. Couche physique OSI.	37
I. Ethernet	43
J. Planification et câblage des réseaux.	51
K. Configuration et test de votre réseau.	62

A . Terminologie des réseaux

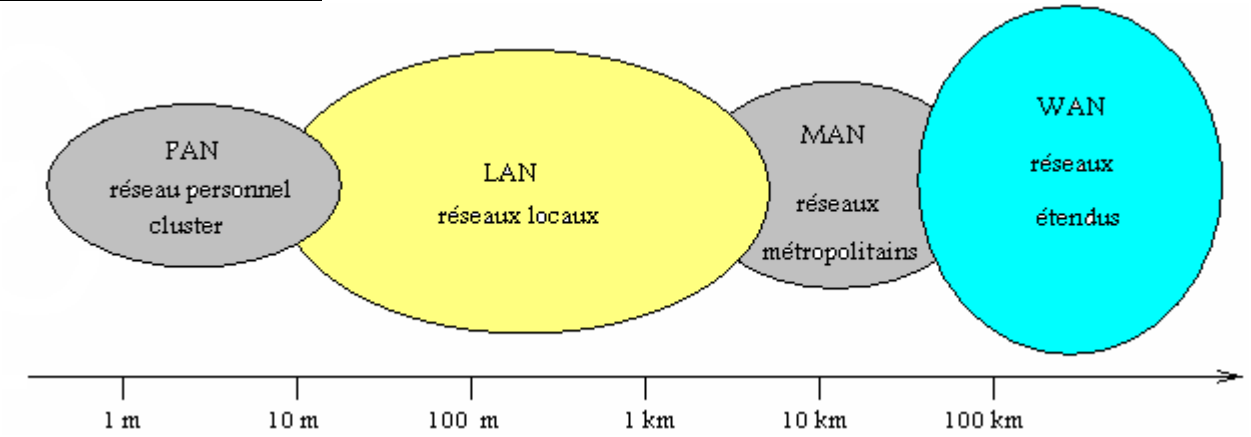
1 . Définition des réseaux informatiques.

Un réseau informatique est un moyen qui permet à des individus ou à des groupes de partager des informations et des services. La technologie des réseaux constitue l'ensemble des outils qui permettent à des ordinateurs de partager des informations et des ressources.

Les services que les réseaux offrent font partie de la vie courante des entreprises et administrations (banques, gestion, commerce, bases de données, recherche, etc...) et des particuliers (messagerie, loisirs, services d'informations par minitel et Internet ...).

On peut classer les réseaux en deux catégories :

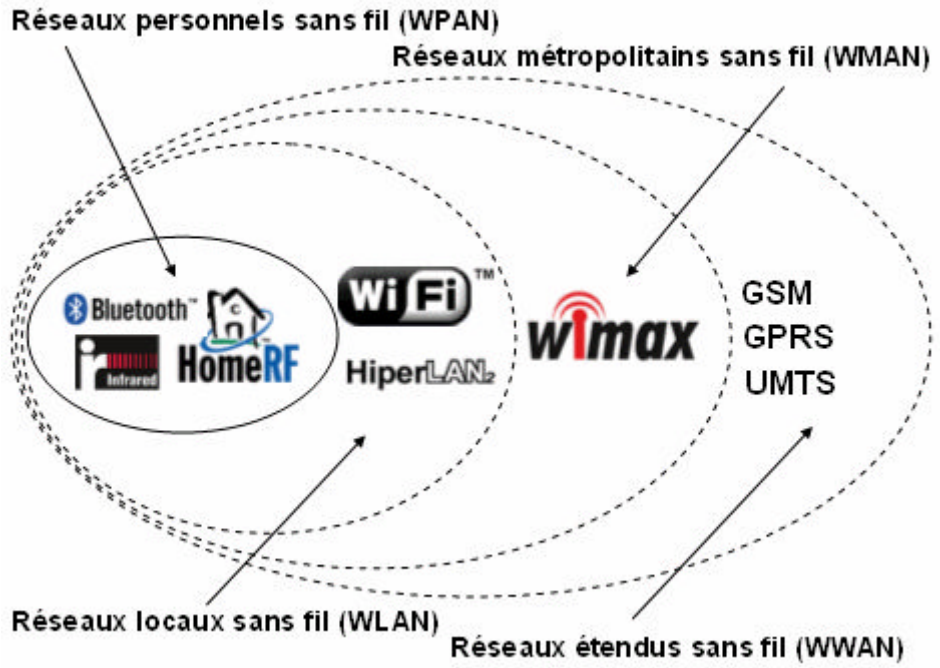
2 . Les réseaux avec fil.



- **Un *réseau personnel* (PAN : Personnal Area Network)** interconnecte (souvent par des liaisons sans fil) des équipements personnels comme un ordinateur portable, un agenda électronique...
- **Un *réseau local* (LAN : Local Area Network)** peut s'étendre de quelques mètres à quelques kilomètres et correspond au réseau d'une entreprise. Il peut se développer sur plusieurs bâtiments et permet de satisfaire tous les besoins internes de cette entreprise.
- **Un *réseau métropolitain* (MAN : Metropolitan Area Network)** interconnecte plusieurs lieux situés dans une même ville, par exemple les différents sites d'une université ou d'une administration, chacun possédant son propre réseau local.
- **Un *réseau étendu* (WAN : Wide Area Network)** permet de communiquer à l'échelle d'un pays ou de la planète entière, les infrastructures physiques pouvant être terrestres ou spatiales à l'aide de satellites de télécommunications.
- **Un *réseau de stockage* (SAN : Storage Area Network)** est un réseau à haute performance dédié qui permet de transférer des données entre des serveurs et des ressources de stockage. Du fait qu'il s'agit d'un réseau dédié distinct, il évite tout conflit de trafic entre les clients et les serveurs et permet de bénéficier d'une connectivité haut débit.
- **Un *réseau privé virtuel* (VPN : Virtual Private Network)** est un réseau privé construit au sein d'une infrastructure de réseau publique telle que le réseau mondial Internet. Au moyen d'un réseau privé virtuel, un télétravailleur peut accéder à distance au réseau du quartier général de sa société.

3. Les réseaux sans fil.

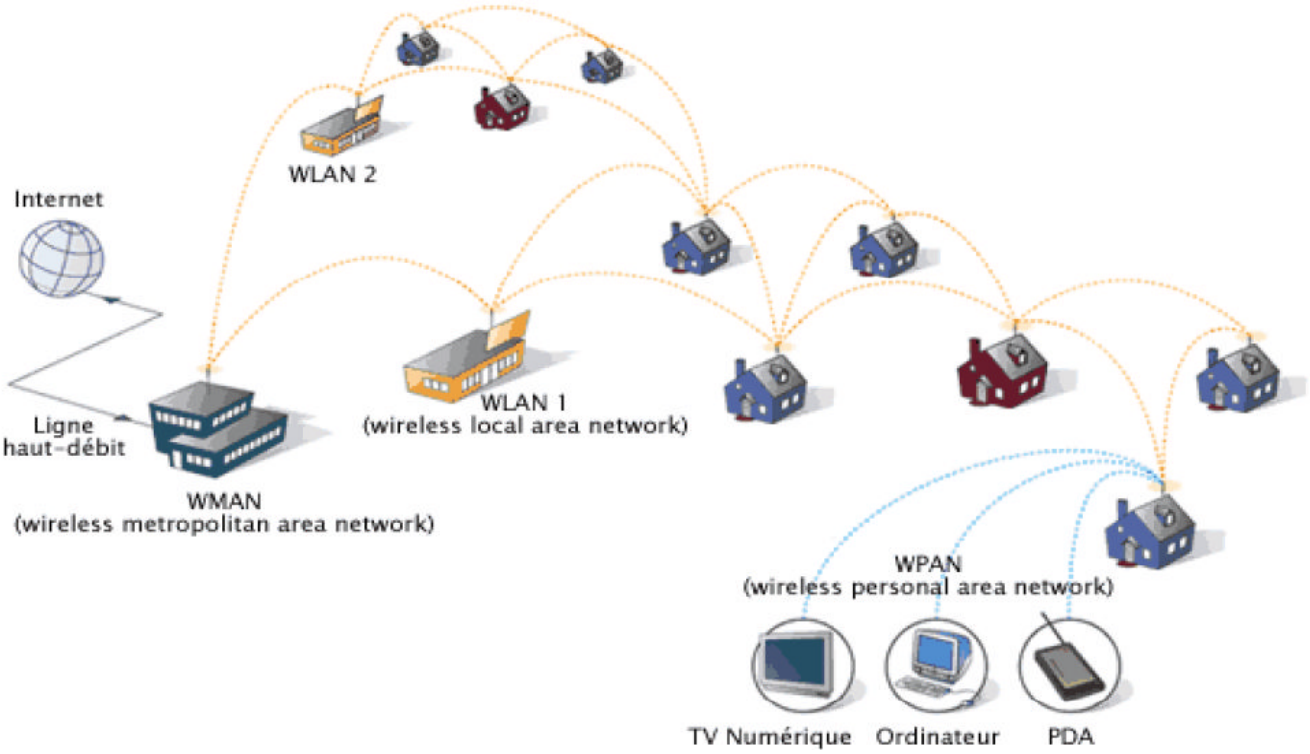
Un réseau sans fil (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".



- **Un réseau personnel sans fil (WPAN : Wireless Personal Area Network)** concerne les réseaux sans fil d'une faible portée : de l'ordre de quelques dizaines mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Il existe plusieurs technologies utilisées pour les WPAN :
  - La principale technologie WPAN est la technologie Bluetooth, lancée par Ericsson en 1994, proposant un débit théorique de 1 Mbps pour une portée maximale d'une trentaine de mètres.
  - HomeRF (pour Home Radio Frequency), propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur
  - Enfin les liaisons infrarouges permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde.
- **Un réseau local sans fil (WLAN : Wireless Local Area Network)** est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :
  - Le Wifi soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.
  - hiperLAN2 (HIgh Performance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 MHz.
- **Un réseaux métropolitains sans fils (WMAN)** est un réseau métropolitain sans fils (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.
- **Un réseau étendu sans fil (WWAN : Wireless Wide Area Network)** est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les

téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes :

- GSM (Global System for Mobile Communication ou en français Groupe Spécial Mobile)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System).
- Wimax (Worldwide Interoperability for Microwave Accessstandard). Basé sur une bande de fréquence de 2 à 11 GHz, offrant un débit maximum de 70 Mbits/s sur 50km de portée, certains le placent en concurrent de l'UMTS, même si ce dernier est davantage destiné aux utilisateurs voyageurs.



B . Les modèles OSI et TCP/IP

I . LE MODELE OSI

1 . Description du modèle OSI (Open Systems Interconnection)

Le processus d'envoi de données peut être décomposé en plusieurs tâches :

- Reconnaissance des données,
- Segmentation des données en paquets plus faciles à traiter,
- Ajout d'informations dans chaque paquet de données afin de :
  - Définir l'emplacement des données
  - Identifier le récepteur
- Ajout d'informations de séquence et de contrôle d'erreurs,
- Dépôt des données sur le réseau et envoi.

Le système d'exploitation réseau effectue chacune des tâches en suivant un ensemble de procédures strictes, appelées protocoles ou règles de conduite

En 1978, l'ISO (International Standard Organisation) publia un ensemble de recommandations sur une architecture réseau permettant la connexion de périphériques hétérogènes. En 1984, l'ISO publia une mise à jour du modèle qui est devenue une norme internationale.

Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau bien 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 plus simples.
- Il uniformise les éléments du réseau afin de permettre le développement et le soutien multiconstructeur.
- Il permet à différents types de matériel et de logiciel réseau de communiquer entre eux.
- Il empêche les changements apportés à une couche d'affecter 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.

2 . Analyse des rôles des 7 couches du modèle OSI

Le modèle OSI est une architecture qui divise les communications réseau en sept couches.
A chaque couche correspond des activités, des équipements ou des protocoles réseau différents.

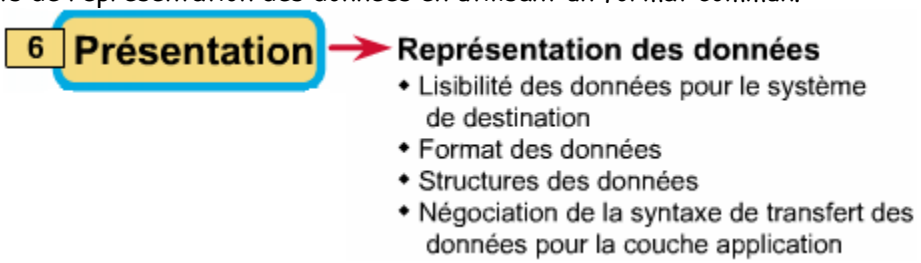
On utilise la phrase suivante comme aide-mémoire : Après Plusieurs Semaines Tout Respire La Pais

Couche 7 : La couche application 7

La couche application est la couche OSI la plus proche de l'utilisateur. Elle fournit des services réseau aux applications de l'utilisateur. Voici quelques exemples de ce type d'application : tableurs, traitements 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 correction d'erreur et de contrôle d'intégrité des données.

Couche 6 : La couche présentation 6

La couche présentation s'assure que les informations envoyées par la couche application d'un système sont lisibles par la couche application d'un autre système. Au besoin, la couche présentation traduit différents formats de représentation des données en utilisant un format commun.

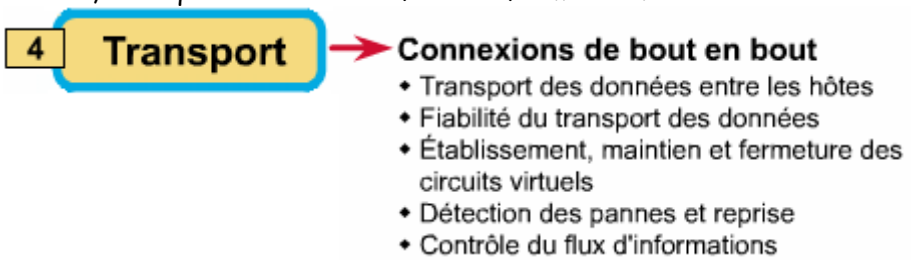


Couche 5 : La couche session 5

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 présentation. Elle synchronise également le dialogue entre les couches de présentation des deux hôtes et gère l'échange des données.

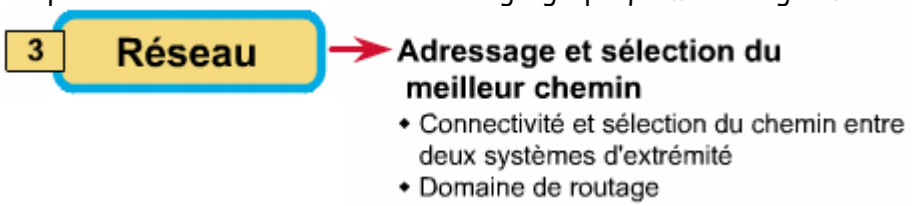
Couche 4 : La couche transport 4

La couche transport segmente les données envoyées par le système de l'hôte émetteur et les rassemble en flux de données sur le système de l'hôte récepteur.
En fournissant un service de communication, la couche transport établit et raccorde les circuits virtuels, en plus d'en assurer la maintenance. La fourniture d'un service fiable lui permet d'assurer la détection et la correction des erreurs, ainsi que le contrôle du flux d'informations.



Couche 3 : La couche réseau 3

La couche réseau est une couche complexe qui assure la connectivité et la sélection du chemin entre deux systèmes hôtes pouvant être situés sur des réseaux géographiquement éloignés.



Couche 2 : La couche liaison de données 2

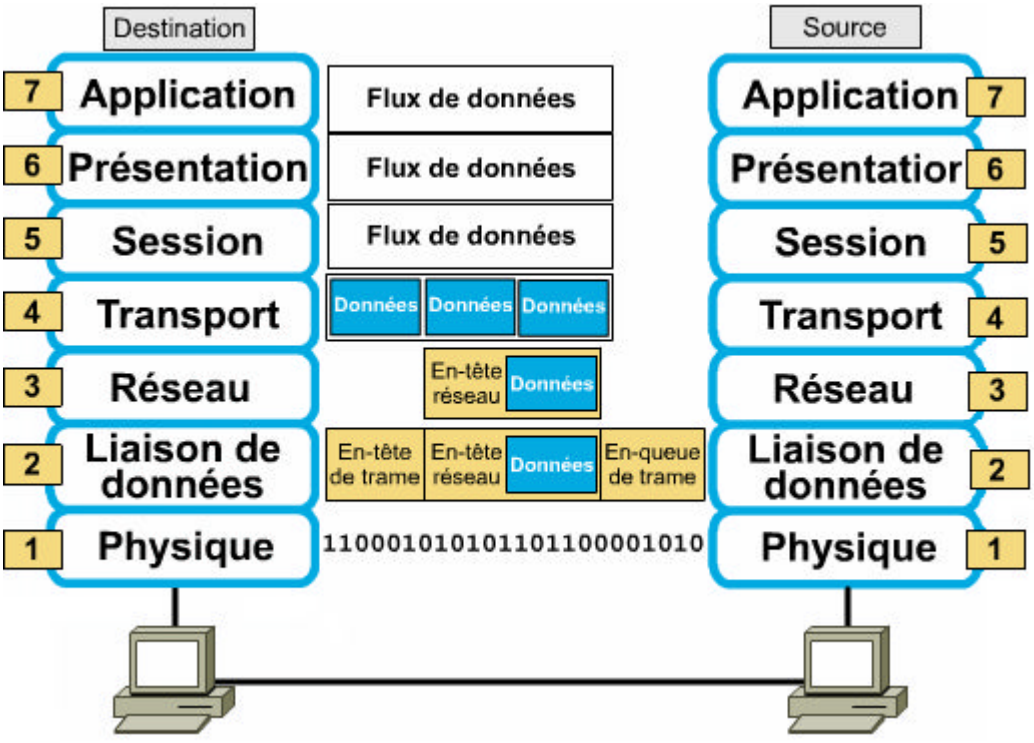
La couche liaison de données assure un transit fiable des données sur une liaison physique. Ainsi, la couche liaison de données s'occupe de l'adressage physique (plutôt que logique), de la topologie du réseau, de l'accès au réseau, de la notification des erreurs, de la livraison ordonnée des trames et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

Couche 1 : La couche physique 1

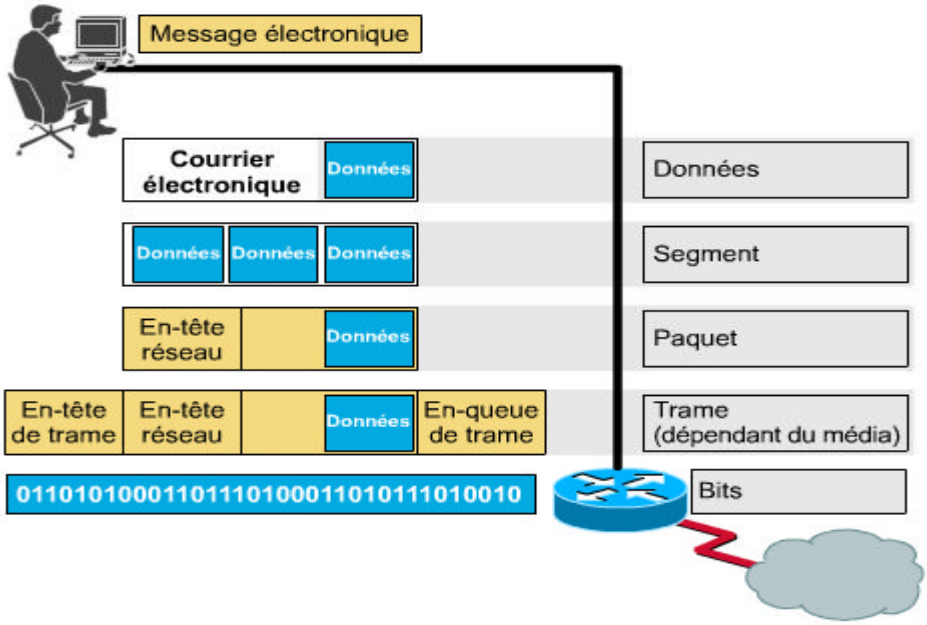
La couche physique définit les spécifications électriques, mécaniques, procédurales et fonctionnelles permettant d'activer, de maintenir et de désactiver la liaison physique entre les systèmes d'extrémité. Les caractéristiques telles que les niveaux de tension, la synchronisation des changements de tension, les débits physiques, les distances maximales de transmission, les connecteurs physiques et d'autres attributs semblables sont définies par la couche physique.

3 . Terminologie liée au modèle OSI

3.1 . Encapsulation des données



3.2 . Exemple d'encapsulation des données



- **Message** c'est un regroupement logique de données au niveau de la couche 7 (application), souvent composé d'un certain nombre de groupes logiques de couches inférieures, par exemple des paquets.
- **Segment** : c'est un terme utilisé pour décrire une unité d'information de la couche de transport.
- **Paquet** : c'est un regroupement logique d'informations comportant un en-tête qui contient les données de contrôle et (habituellement) les données utilisateur. Le terme paquets est le plus souvent utilisé pour désigner les unités de données au niveau de la couche réseau
- **Trame** : c'est un regroupement logique de données envoyé comme unité de couche liaison de données par un média de transmission.
- **Datagramme** : c'est un regroupement logique de données envoyé comme unité de couche réseau par un média de transmission, sans établissement préalable d'un circuit virtuel. Les datagrammes IP sont les principales unités d'information sur Internet.
- **SDU** : **(Service data unit) unité de données de service**. Unité d'information d'un protocole de couche supérieure qui définit une demande de service à un protocole de couche inférieure.
- **PDU** : **(Protocol data unit) unité de données de protocole**. Terme OSI désignant un paquet.

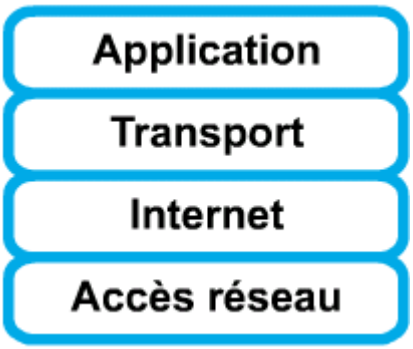
4 . Répartition des éléments d'un réseau en fonction des couches du modèle OSI.

Couche n°	Nom	Unité d'encapsulation ou regroupement logique	Unités ou éléments fonctionnant au niveau de cette couche.
7	Application	Données	Logiciel (passerelles)
6	Présentation	Données	Logiciels
5	Session	Données	Logiciels
4	Transport	Segments	Routeur
3	Réseau	Paquets, datagrammes	Routeur
2	Liaison de données	Trames	Carte réseau (LLC et MAC), pont, commutateur
1	Physique	Bits	Carte réseau (connecteurs physiques - BNC, RJ45, etc.), média (câbles), répéteur, concentrateur, ETCD et ETTD

II . Description des 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. Le ministère de la Défense veut que ses paquets se rendent à 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.

Le modèle TCP/IP comporte quatre couches : la couche application, la couche transport, la couche *Internet* et la couche d'accès au réseau. Comme vous pouvez le constater, 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.



La couche application
La couche application gère les protocoles de haut niveau : représentation codage et 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.

La couche transport
La couche 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'excellents moyens 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 les informations de couche application en unités appelées segments.

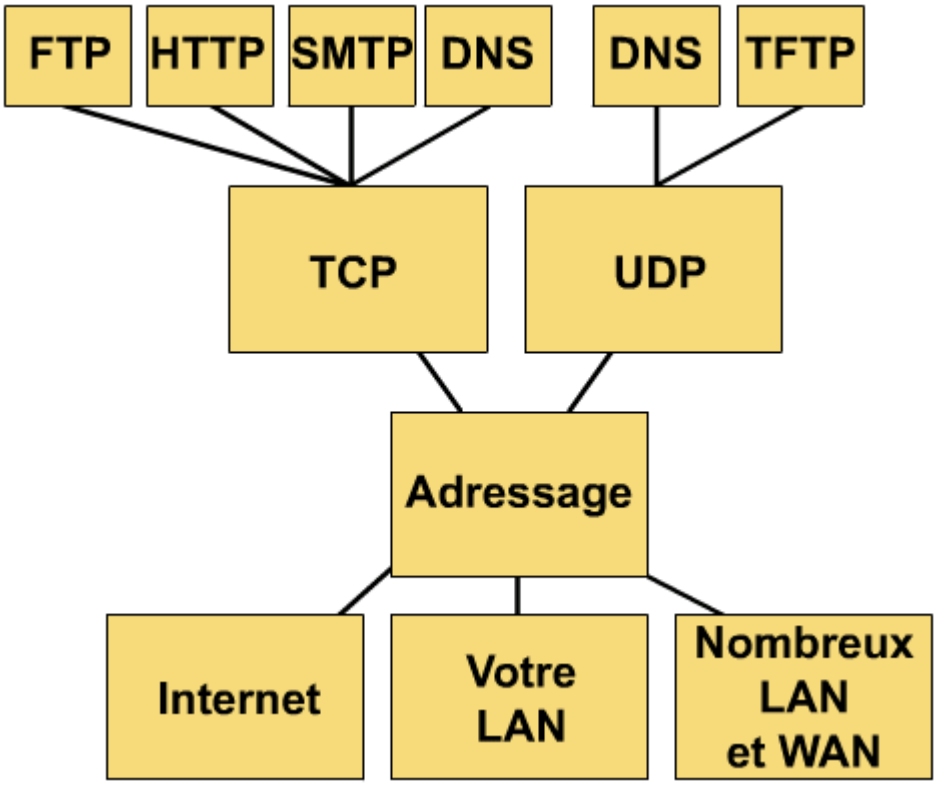
La couche Internet
Le rôle de la *couche Internet* consiste à envoyer des paquets source à partir d'un réseau quelconque de l'interréseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

La couche d'accès au 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 LAN et WAN, ainsi que tous les détails dans les couches physique et liaison de données du modèle OSI.

III . Description des protocoles TCP/IP.

Le diagramme illustré dans la figure suivante est appelé *schéma de protocoles*. Il présente certains protocoles communs spécifiés par le modèle de référence TCP/IP. Au niveau de la couche application, on trouve :

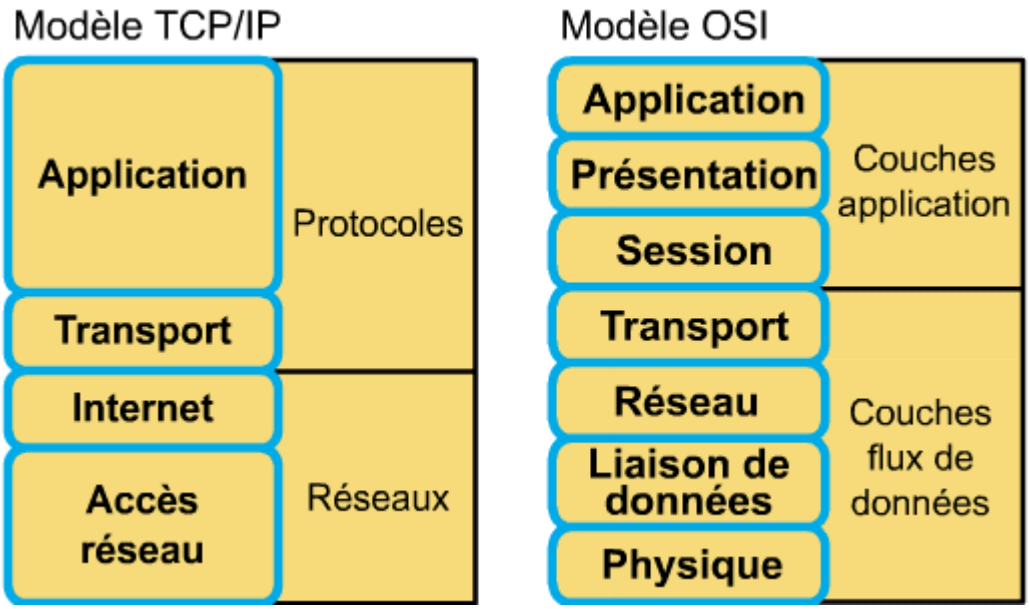
- *FTP* - Protocole de transfert de fichiers ou protocole FTP
- *HTTP* - Protocole HTTP (Hypertext Transfer Protocol)
- *SMTP* - Protocole SMTP (Simple Mail Transfer protocol)
- *DNS* - Système DNS (Domain Name System)
- *TFTP* - Protocole TFTP (Trivial File Transfer Protocol)



Le modèle TCP/IP met l'accent sur une souplesse maximale, au niveau de la couche application, à l'intention des développeurs de logiciels. La couche transport fait appel à deux protocoles : le protocole TCP (protocole de contrôle de transmission) et le *protocole UDP (User Datagram Protocol).*

Dans le modèle TCP/IP, IP (Internet Protocol) est le seul et unique protocole utilisé, et ce, quels que soient le protocole de transport utilisé et l'application qui demande des services réseau. Il s'agit là d'un choix de conception délibéré. *IP* est un protocole universel qui permet à tout ordinateur de communiquer en tout temps et en tout lieu.

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 :

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 l'utilisation de la technologie de commutation de paquets (et non de commutation de circuits).
- Les professionnels des réseaux doivent connaître les deux modèles.

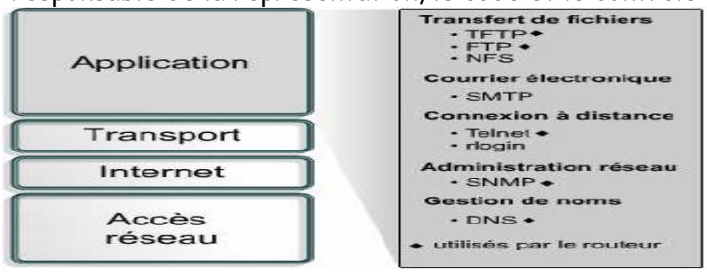
Différences

- TCP/IP intègre la couche présentation et la couche session dans sa couche application.
- TCP/IP regroupe les couches physique et liaison de données OSI au sein d'une seule couche.
- TCP/IP semble plus simple, car il comporte moins de couches.
- Les protocoles TCP/IP constituent la norme sur laquelle s'est développé Internet. Aussi, le modèle TCP/IP a-t-il bâti sa réputation sur ses protocoles. En revanche, les réseaux ne sont généralement pas architecturés autour du protocole OSI, bien que le modèle OSI puisse être utilisé comme guide.

C . Fonctionnalité et protocoles des couches applicatives

1. Introduction à la couche application du modèle TCP/IP :

La couche application est responsable de la représentation, le code et le contrôle du dialogue.



2. DNS :

Il est difficile de retenir l'adresse IP d'un site, car l'adresse numérique n'a aucun rapport apparent avec le contenu du site. ***DNS*** permet de convertir les @IP en des noms de domaine et l'inverse.
Il existe plus de 200 domaines de niveau supérieur sur Internet, notamment :

- **.us** – États-Unis
- **.fr** – France
- **.edu** – sites éducatifs
- **.com** – sites commerciaux …

3. FTP & TFTP :

FTP est un service orienté connexion fiable. L'objectif principal de ce protocole est d'échanger des fichiers dans les deux sens (importation et exportation) entre un ordinateur serveur et des ordinateurs clients en ouvrant une connexion.
TFTP est un service non orienté connexion. Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle IOS Cisco. Ce protocole, conçu pour être léger et facile à mettre en oeuvre, (il ne permet pas d'afficher le contenu des répertoires ni d'assurer l'authentification des utilisateurs).

4. HTTP :

Le protocole ***HTTP*** (*Hypertext Transfer Protocol*) est le support du Web.
Les pages Web sont créées avec un langage de formatage appelé HTML (*HyperText Markup Language*). Le code HTML indique au navigateur comment présenter une page Web pour obtenir un aspect particulier.
Les *liens hypertexte* (ou hyperliens) facilitent la navigation sur le Web. Il peut s'agir d'un objet, d'un mot, d'une phrase ou d'une image sur une page Web.

http://	www.	cisco.com	/edu/
Indique au navigateur le protocole à utiliser.	Indique le nom de l'hôte ou le nom d'un ordinateur précis.	Représente l'entité de domaine du site Web.	Spécifie le répertoire dans lequel la page Web est située sur le serveur. Ainsi, quand aucun nom n'est spécifié, le navigateur charge la page par défaut identifiée par le serveur.

Lorsque vous tapez une adresse, Le navigateur Web examine alors le protocole pour savoir s'il a besoin d'ouvrir un autre programme, puis détermine l'adresse IP du serveur Web à l'aide du système DNS. Ensuite, les couches transport, réseau, liaison de données et physique établissent une session avec le serveur Web.

Le serveur répond à la demande en transmettant au client Web tous les fichiers texte, audio, vidéo et graphique indiqués dans la page HTML. Le navigateur client rassemble tous ces fichiers pour créer une image de la page Web et met fin à la session.

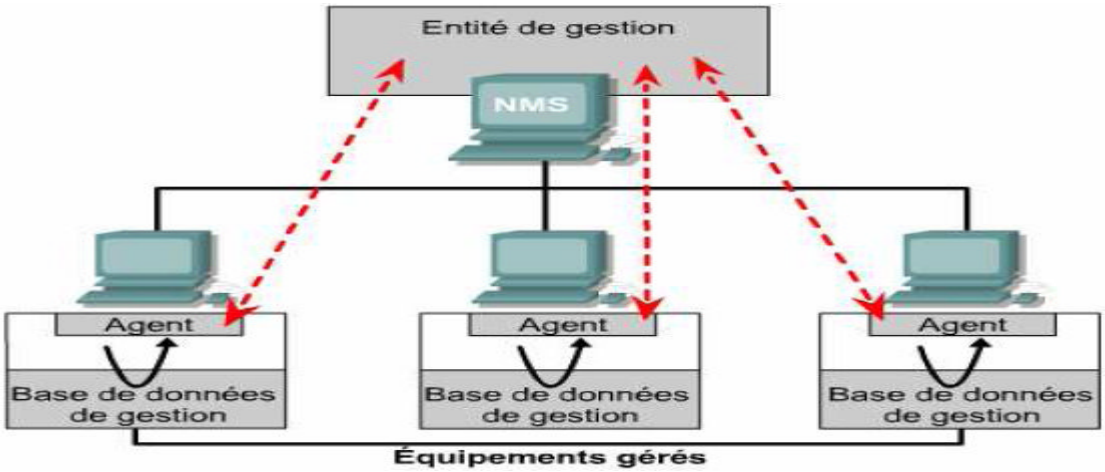
5. SMTP :

Les serveurs de messagerie communiquent entre eux à l'aide du protocole ***SMTP*** (*Simple Mail Transfer Protocol*) pour envoyer et recevoir des messages électroniques. Ce protocole transporte les messages au format ASCII à l'aide de TCP.
Les protocoles de client de messagerie les plus répandus sont POP3 et IMAP4, qui utilisent tous deux TCP pour transporter les données (récupérer les messages), par contre le client utilise toujours le protocole SMTP pour envoyer des messages.
Pour tester l'accès à un serveur de messagerie, établissez une connexion Telnet au port SMTP : C:\>telnet 192.168.10.5 25
Le protocole SMTP ne propose guère d'options de sécurité et ne nécessite aucune authentification.

6. SNMP :

Le protocole ***SNMP*** (Simple Network Management Protocol) est un protocole qui facilite l'échange d'information de gestion entre les équipements du réseau. Il permet aux administrateurs réseau de gérer les performances du réseau, de diagnostiquer et de résoudre les problèmes.
Composants SNMP :

- *Le système d'administration de réseaux (NMS, Network Management System):* le composant NMS fournit la quantité de ressources mémoire et de traitements requises pour la gestion du réseau.
- *Les unités gérées*: ces unités sont des noeuds du réseau contenant un agent SNMP. Ces unités peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des concentrateurs, des ordinateurs hôtes ou des imprimantes.
- *Les agents*: les agents sont des modules logiciels de gestion du réseau résidant sur les unités gérées. Ils contiennent les données locales des informations de gestion et les convertissent en un format compatible avec SNMP.



7. Telnet :

Le logiciel client ***Telnet*** permet de se connecter à un hôte Internet distant sur lequel est exécutée une application serveur Telnet, puis d'exécuter des commandes à partir de la ligne de commande.
Un client Telnet est qualifié d'hôte local. Le serveur Telnet, qui utilise un logiciel spécial appelé «démon», est considéré comme l'hôte distant.
Les opérations de traitement et de stockage sont entièrement exécutées par l'ordinateur distant.

D . Couche transport OSI

1. Introduction à la couche transport :

La couche transport a pour but :

- D'acheminer les données de la source à la destination. « TCP ou UDP »
- De contrôler le flux de ces données. « Fenêtrage »
- De garantir la fiabilité de ces données. « Accusés de réception »

Analogie : Imaginez une personne qui apprend une langue étrangère pour la première fois (il faut répéter les mots, parler lentement …)

Services de transport de base :

- *Segmentation des données* d'application de couche supérieure.
- *Établissement d'une connexion* de bout en bout.
- *Transport des segments* d'un hôte d'extrémité à un autre.
- *Contrôle du flux* assuré par les fenêtres glissantes.
- *Fiabilité* assurée par les numéros de séquence et les accusés de réception.

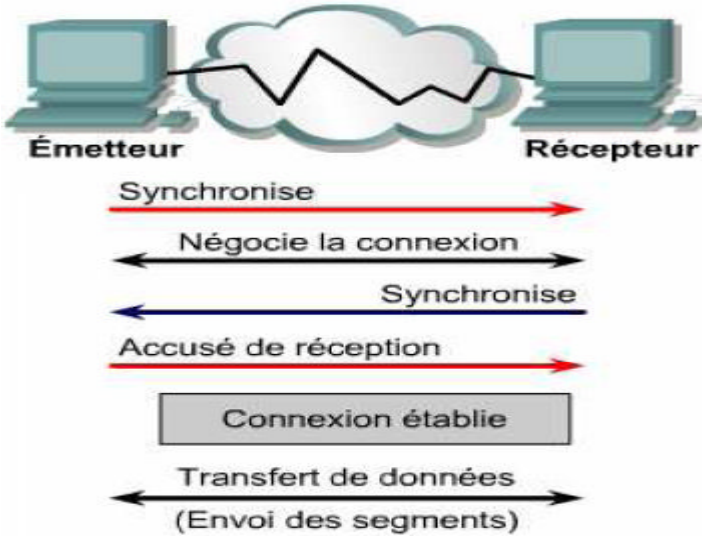
2. Contrôle de flux :

Le ***contrôle de flux*** permet d'éviter le dépassement de capacité des mémoires tampons d'un hôte de destination. Pour ce faire, TCP met en relation les hôtes source et de destination qui conviennent alors d'un taux de transfert des données acceptable. Sinon, le destinataire va rejeter les segments.

3. Établissement, maintenance et fermeture de session

Lorsque l'ordinateur PC1 veut envoyer de l'information à l'ordinateur PC2, il doit tout d'abord établir une session avec ce dernier au niveau de la couche transport.

- Premièrement, PC1 envoie un message de synchronisation à PC2.
- PC2 reçoit le message, et négocie la connexion avec PC1, ensuite il va envoyer à son tour un message de synchronisation des paramètres négociés.
- PC1 envoie finalement un accusé de réception comme quoi la connexion est établit.
- A ce moment là, les deux ordinateurs peuvent échanger les données d'une façon bidirectionnelle.
- Une fois le transfert des données terminé, PC1 envoie un signal indiquant la fin de la transmission. PC2 accuse la réception et la connexion se termine.



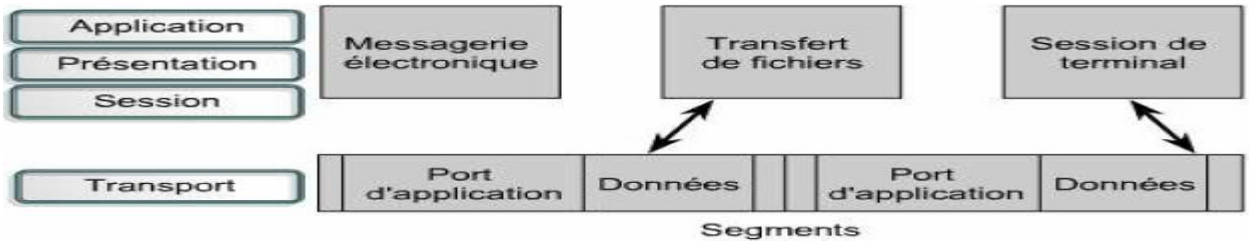
La congestion peut se produire dans deux situations :

- Lorsqu'un ordinateur génère un trafic dont le débit est plus rapide que la vitesse de transfert du réseau.
- Lorsque plusieurs ordinateurs doivent envoyer simultanément des datagrammes à une même destination.

Pour éviter la perte des données, le processus TCP de PC2 envoie un indicateur «***non prêt***» à PC1, afin que ce dernier arrête de transmettre. Lorsque PC2 peut accepter de nouvelles données, il envoie l'indicateur de transport «***prêt***» à PC1 qui reprend alors la transmission des segments.

Le multiplexage :

Les applications envoient des segments de données suivant la méthode du premier arrivé, premier servi. Ce qui est important, c'est que plusieurs applications peuvent partager la même connexion de transport (ça veut dire qu'on peut utiliser deux services d'application ou plus en ouvrant une seule fois la connexion. On parle alors de *multiplexage des conversations de couche supérieure*.



3. Échange en trois étapes

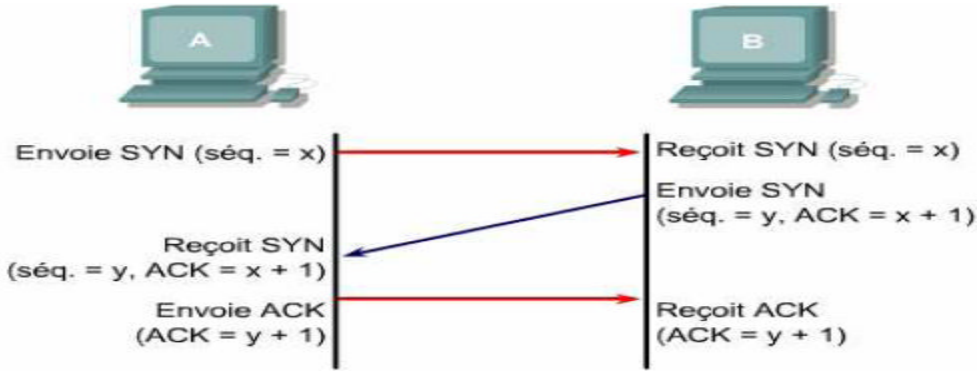
Pour établir une connexion, les deux hôtes doivent synchroniser leurs numéros de séquence initiaux (**ISN** – Initial Sequence Number).

La synchronisation s'effectue via un échange de segments transportant un bit de contrôle SYN et les numéros de séquence initiaux.

La séquence de la synchronisation est la suivante :

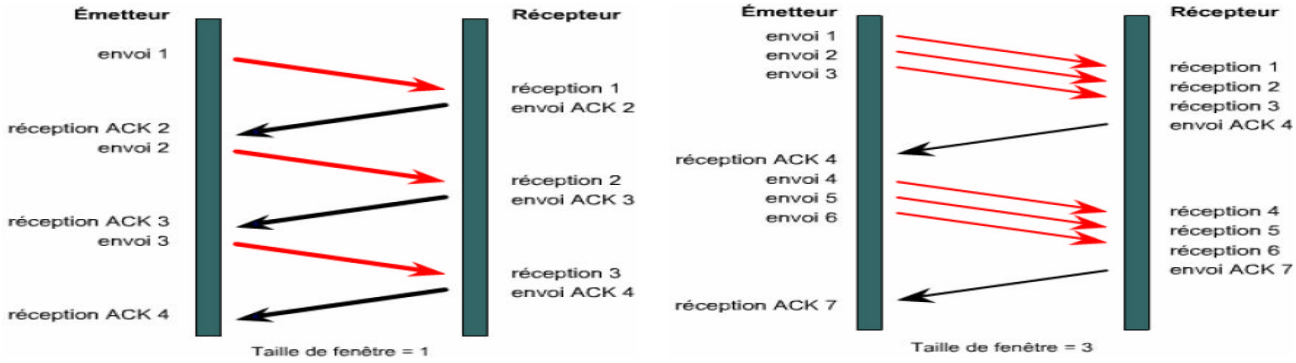
1. L'hôte émetteur (A) initie une connexion *en envoyant un paquet SYN* à l'hôte récepteur (B) indiquant que son numéro de séquence initial ISN = X.
2. B reçoit le paquet, enregistre que la séquence de A = X, répond par un accusé de réception de X + 1 et indique que son numéro de séquence ISN = Y. L'accusé X + 1 signifie que l'hôte B a reçu tous les octets jusqu'à X inclus et qu'il attend l'arrivée de X + 1.
3. L'hôte A reçoit le paquet de B, apprend que la séquence de B est Y et répond par un accusé de Y + 1, qui met fin au processus de connexion:

Cet échange est un ***échange en trois étapes***.



4. Fenêtrage :

Le ***fenêtrage*** est une solution simple qui consiste, pour le destinataire, à accuser une réception à chaque transmission d'un nombre bien précis des segments.



Chaque protocole orienté connexion utilise une *taille de fenêtre* (la taille de la fenêtre indique le nombre des segments que l'hôte de destination est prêt à recevoir).

TCP utilise des accusés de réception prévisionnels. Cela signifie que le numéro de l'accusé indique le paquet suivant attendu.
Le fenêtrage fait référence au fait que la taille de la fenêtre est négociée de manière dynamique pendant la session TCP. Il constitue un mécanisme de contrôle de flux.
Après qu'une certaine quantité de données a été transmise, la machine destination signale une taille de fenêtre à l'hôte source.
Chaque segment est numéroté avant la transmission pour pouvoir réassembler correctement les segments au niveau de la destination. (***Numéros des segments***)

5. Protocole TCP : (Transfert Control Protocol)

TCP est un protocole orienté connexion de la couche transport, qui assure une transmission fiable des données en full duplex.
Les protocoles utilisant TCP sont les suivants: FTP, HTTP, SMTP, Telnet

Structure d'un segment TCP :

Bit 0	Bit 15	Bit 16	Bit 31
Port source (16)		Port de destination (16)	
Numéro de séquence (32)			
Numéro d'accusé de réception (32)			
Longueur d'en-tête (4)	Réservé (6) Bits de Code (6)	Fenêtre (16)	
Somme de contrôle (16)		Urgent (16)	
Options (0 ou 32 le cas échéant)			
Données (variable)			

20 octets

- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Numéro de séquence:** numéro d'ordre de chaque segment.
- **Numéro d'accusé de réception:** octet TCP suivant attendu.
- **HLEN:** nombre de mots de 32 bits contenus dans l'en-tête.
- **Réservé:** champ réglé sur zéro.
- **Bits de code:** fonctions de contrôle (l'ouverture et la fermeture d'une session).
- **Fenêtre:** nombre d'octets que l'émetteur acceptera.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Pointeur d'urgence:** indique la fin des données urgentes.
- **Option:** p.ex. : la taille maximale d'un segment TCP (MSS – Maximum Segment Size)
- **Données:** données de protocole de couche supérieure.

6. Protocole UDP : (User Datagram Protocol)

C'est un protocole simple qui échange des datagrammes sans garantir leur bonne livraison.
UDP n'utilise ni fenêtres ni accusés de réception. La fiabilité est assurée par les protocoles de la couche application. Le protocole UDP est conçu pour les applications qui ne doivent pas assembler de séquences de segments.
Les protocoles utilisant UDP sont les suivants: TFTP, SNMP, DHCP, DNS.

Structure d'un segment UDP :

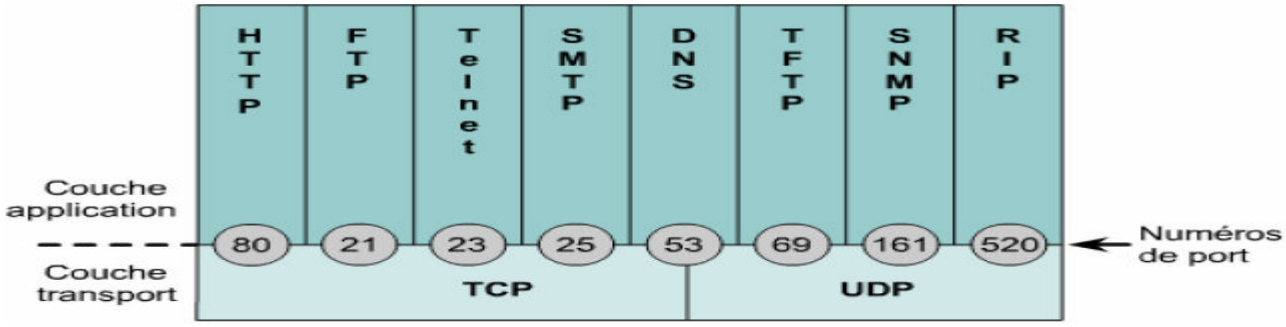
Bit 0	Bit 15 Bit 16 Bit 31
Port source (16)	Port de destination (16)
Longueur (16)	Somme de contrôle (16)
Données (le cas échéant)	

8 octets

- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Longueur:** nombre d'octets de l'en-tête et des données.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Données:** données de protocole de couche supérieure.

7. Numéros de port TCP et UDP :

Les numéros de port servent à distinguer les différentes conversations qui circulent simultanément sur le réseau.
Les développeurs d'applications ont convenu d'utiliser les numéros de port reconnus émis par l'IANA (Internet Assigned Numbers Authority).
Par exemple : **FTP** fait appel aux numéros de port standard 20 et 21. Le port 20 est utilisé pour la partie « données » et le port 21 pour le « contrôle ».



Les plages attribuées aux numéros de port :

- Les numéros inférieurs à 1024 sont considérés comme des numéros de port reconnus.
- Les numéros supérieurs à 1023 sont des numéros attribués de manière dynamique.
- Les numéros de port enregistrés sont destinés à des applications spécifiques d'un fournisseur. La plupart se situent au-delà de 1024.

Les systèmes d'extrémité utilisent les numéros de port pour sélectionner l'application appropriée. L'hôte source attribue dynamiquement les numéros de port source.
Ils sont toujours *supérieurs à 1023*.

E . Couche réseau OSI

1. Introduction à la couche réseau :

Le rôle de la couche réseau, ou couche 3 OSI, consiste à sélectionner le meilleur chemin pour transférer les paquets sur le réseau. Elle fournit des services pour l'échange des éléments de données individuels sur le réseau entre des périphériques finaux identifiés. Pour effectuer ce transport de bout en bout, la couche 3 utilise quatre processus de base :

- l'adressage ;
- l'encapsulation ;
- le routage ;
- le décapsulage.

1.1. Adressage

La couche réseau doit d'abord fournir un mécanisme pour l'adressage de ces périphériques finaux. Si des éléments de données individuels doivent être acheminés vers un périphérique final, ce dernier doit posséder une adresse unique. Dans un réseau IPv4, lorsque cette adresse est ajoutée à un périphérique, celui-ci est alors désigné comme hôte.

1.2. Encapsulation

La couche réseau doit également fournir une encapsulation. Non seulement les périphériques doivent être identifiés par une adresse, mais les éléments individuels (unités de données de protocole de couche réseau) doivent également contenir ces adresses. Durant le processus d'encapsulation, la couche 3 reçoit l'unité de données de protocole de la couche 4 et ajoute un en-tête de couche 3, ou étiquette, pour créer l'unité de données de protocole de couche 3. Dans un contexte de couche réseau, cette unité de données de protocole est appelée paquet. Lors de la création d'un paquet, l'en-tête doit contenir, entre autres, l'adresse de l'hôte auquel il est envoyé. Cette adresse est appelée adresse de destination. L'en-tête de la couche 3 comporte également l'adresse de l'hôte émetteur. Cette adresse est appelée adresse source.

1.3. Routage

La couche réseau doit ensuite fournir des services pour diriger ces paquets vers leur hôte de destination. Les hôtes source et de destination ne sont pas toujours connectés au même réseau. En fait, le paquet peut avoir de nombreux réseaux à traverser. En route, chaque paquet doit être guidé sur le réseau afin d'atteindre sa destination finale. Les périphériques intermédiaires connectant les réseaux sont appelés routeurs. Leur rôle consiste à sélectionner les chemins afin de diriger les paquets vers leur destination. Ce processus est appelé routage.

1.4. Décapsulage

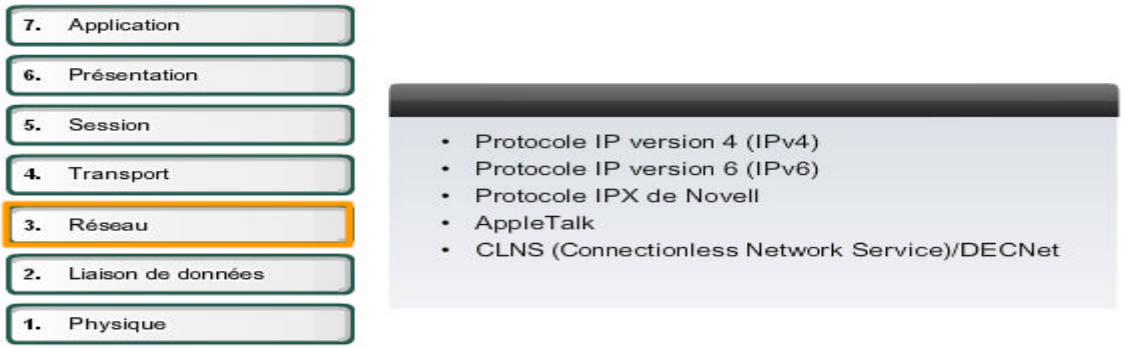
Enfin, le paquet arrive sur l'hôte de destination et est traité par la couche 3. L'hôte examine l'adresse de destination pour vérifier que le paquet était bien adressé à ce périphérique. Si l'adresse est correcte, le paquet est décapsulé par la couche réseau, et l'unité de données de protocole de la couche 4 contenue dans le paquet est transmise au service approprié de la couche transport.

2. Protocoles de couche réseau :

Les protocoles mis en œuvre dans la couche réseau qui transportent des données utilisateur comprennent :

- Protocole IP version 4 (IPv4)
- Protocole IP version 6 (IPv6)
- Protocole IPX de Novell
- AppleTalk
- CLNS (Connectionless Network Service)/DECNet

Le protocole IP (IPv4 et IPv6) constitue le protocole de transport de données de couche 3 le plus répandu et fait l'objet de ce cours. Les autres protocoles ne seront qu'abordés.



Les protocoles de la couche Internet du protocole TCP/IP sont :

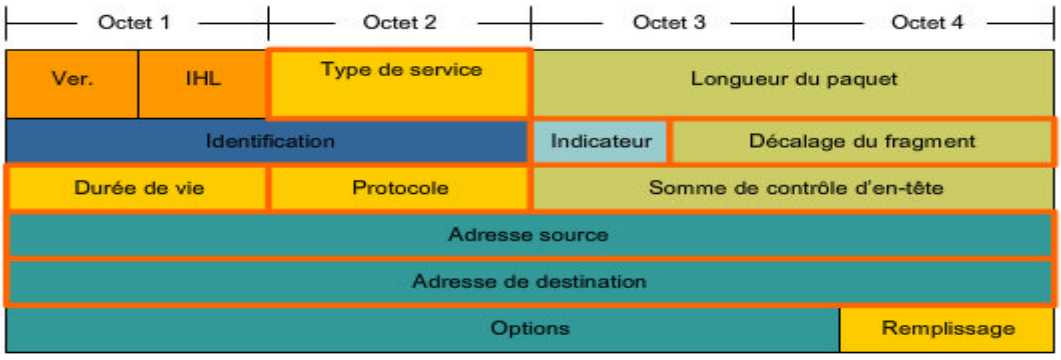
- IP assure l'acheminement au mieux (best-effort delivery) des paquets, non orienté connexion (n'effectue aucune vérification d'erreurs et ne fournit aucun service de correction). Il ne se préoccupe pas du contenu des paquets.
- ICMP (Internet Control Message Protocol) offre des fonctions de messagerie et de contrôle.
- ARP (Address Resolution Protocol) détermine les adresses de la couche liaison de données ou les @MAC pour les @IP connues.
- RARP (Reverse Address Resolution Protocol) détermine l'@ IP pour une @MAC connue.

Le protocole IP effectue les opérations suivantes :

- Il définit un paquet et un système d'adressage.
- Il transfère des données entre la couche Internet et la couche d'accès au réseau.
- Il achemine des paquets à des hôtes distants.

3. En-tête du paquet IPv4 :

Comme l'illustre la figure, un protocole IPv4 définit de nombreux champs différents dans l'en-tête de paquet. Ces champs contiennent des valeurs binaires que les services IPv4 référencent lors de la transmission de paquets sur le réseau.



On examinera les 6 champs clés suivants :

- Adresse source IP
- Adresse de destination IP
- Durée de vie (TTL)
- Type de service (ToS)
- Protocole
- Décalage du fragment

3.1. Adresse de destination IP

Le champ d'adresse de destination IP contient une valeur binaire de 32 bits représentant l'adresse de couche réseau de l'hôte destinataire du paquet.

3.2. Adresse source IP

Le champ d'adresse source IP contient une valeur binaire de 32 bits représentant l'adresse de de couche réseau de l'hôte source du paquet.

3.3. Durée de vie

La durée de vie (TTL, Time to live) est une valeur binaire de 8 bits indiquant la durée de vie restante du paquet. La valeur TTL est décrémentée de 1 au moins chaque fois que le paquet est traité par un routeur (c'est-à-dire à chaque saut). Lorsque la valeur devient nulle, le routeur supprime ou abandonne le paquet et il est retiré du flux de données du réseau. Ce mécanisme évite que les paquets ne pouvant atteindre leur destination ne soient transférés indéfiniment d'un routeur à l'autre dans une boucle de routage. Si les boucles de routage étaient autorisées à continuer, le réseau serait encombré de paquets de données n'atteignant jamais leur destination. Décrémenter la valeur TTL à chaque saut garantit qu'elle finira par devenir nulle et que le paquet avec le champ TTL expiré sera supprimé.

3.4. Protocole

Cette valeur binaire de 8 bits indique le type de données utiles que le paquet transporte. Le champ de protocole permet à la couche réseau de transmettre les données au protocole de couche supérieure approprié.

Exemples de valeurs :

01 ICMP
06 TCP
17 UDP

3.5. Type de service

Le champ de type de service contient une valeur binaire de 8 bits utilisée pour définir la priorité de chaque paquet. Cette valeur permet d'appliquer un mécanisme de qualité de service (QS) aux paquets de priorité élevée, tels que ceux transportant des données vocales de téléphonie. Le routeur traitant les paquets peut être configuré pour déterminer le paquet à transmettre en premier en fonction de la valeur de type de service.

3.6. Décalage du fragment

Comme mentionné précédemment, un routeur peut devoir fragmenter un paquet lors de sa transmission d'un média à un autre de MTU inférieure. Lorsqu'une fragmentation se produit, le paquet IPv4 utilise le champ de décalage du fragment et l'indicateur MF de l'en-tête IP pour reconstruire le paquet à son arrivée sur l'hôte de destination. Le champ de décalage du fragment identifie l'ordre dans lequel placer le fragment de paquet dans la reconstruction.

3.7. Indicateur de fragments supplémentaires

L'indicateur de fragments supplémentaires (MF) est un seul bit du champ Indicateur utilisé avec le décalage du fragment pour la fragmentation et la reconstruction de paquets. L'indicateur de fragments supplémentaires est défini, indiquant qu'il ne s'agit pas du dernier fragment d'un paquet. Quand un hôte récepteur voit un paquet arriver avec l'indicateur MF = 1, il examine le décalage du fragment pour voir où ce fragment doit être placé dans le paquet reconstruit. Quand un hôte récepteur reçoit une trame avec l'indicateur MF = 0 et une valeur non nulle dans le champ de décalage du fragment, il place ce fragment à la fin du paquet reconstruit. Les informations de fragmentation d'un paquet non fragmenté sont toutes nulles (MF = 0, décalage du fragment = 0).

3.8. Indicateur Ne pas fragmenter

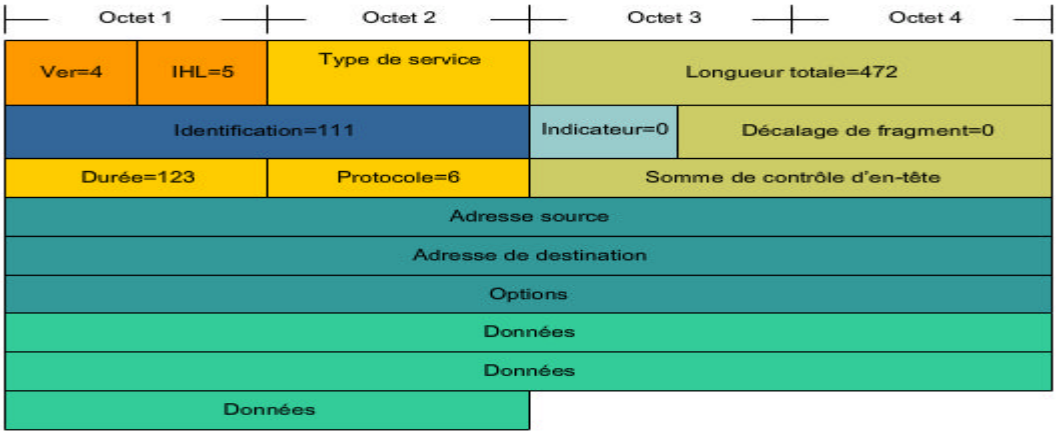
L'indicateur Ne pas fragmenter (DF) est un seul bit du champ Indicateur stipulant que la fragmentation du paquet n'est pas autorisée. Si le bit de l'indicateur Ne pas fragmenter est défini, la fragmentation de ce paquet n'est PAS autorisée. Si un routeur doit fragmenter un paquet pour permettre sa transmission descendante à la couche liaison de données mais que le bit DF est défini à 1, le routeur supprime ce paquet.

3.9. Autres champs de l'en-tête IPv4

- Version : contient le numéro de version IP (4).
- Longueur d'en-tête (IHL) : spécifie la taille de l'en-tête de paquet.
- Longueur du paquet : ce champ donne la taille du paquet entier, en-tête et données compris, en octets.
- Identification : ce champ sert principalement à identifier de manière unique les fragments d'un paquet IP d'origine.
- Somme de contrôle d'en-tête : le champ de somme de contrôle est utilisé pour vérifier l'absence d'erreurs dans l'en-tête de paquet.
- Options : des champs supplémentaires sont prévus dans l'en-tête IPv4 afin de fournir d'autres services, mais ils sont rarement utilisés.

4. Exemple de paquet IP

La figure suivante représente un paquet IP complet avec des valeurs de champ d'en-tête types.



- Ver = 4 : version IP.
- IHL = 5 : taille d'en-tête en mots de 32 bits (4 octets). Cet en-tête est de 5*4 = 20 octets, la taille minimale valide.
- Longueur totale = 472 : la taille de paquet (en-tête et données) est de 472 octets.
- Identification = 111 : identifiant de paquet initial (requis s'il est fragmenté par la suite).
- Indicateur = 0 : stipule que le paquet peut être fragmenté si nécessaire.
- Décalage du fragment = 0 : indique que ce paquet n'est pas fragmenté actuellement (absence de décalage).
- Durée de vie = 123 : indique le temps de traitement de la couche 3 en secondes avant abandon du paquet (décrémenté d'au moins 1 chaque fois qu'un périphérique traite l'en-tête de paquet).
- Protocole = 6 : indique que les données transportées par ce paquet constituent un segment TCP.

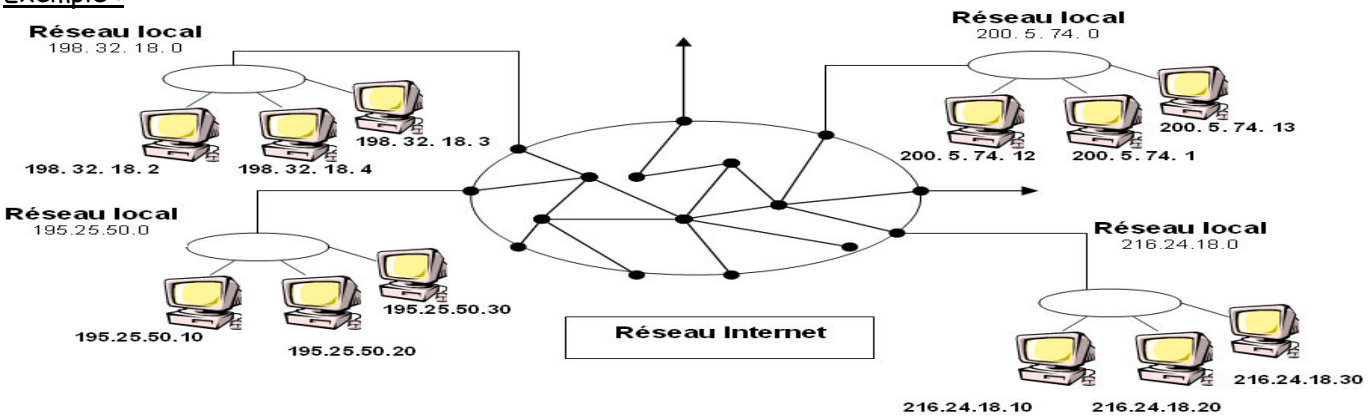
F . Adressage du réseau IPv4

1. Introduction :

Chaque point de connexion, ou interface, d'un équipement dispose d'une adresse IP associée à un réseau. Cette @ permet à d'autres ordinateurs de localiser cet équipement sur un réseau spécifique. Une adresse IP est une séquence de 32 bits composée de 1 et de 0, Afin de faciliter leur lecture, les adresses IP sont généralement exprimées sous la forme de quatre nombres décimaux séparés par des points.

Les longues chaînes de 1 et de 0 répétés sont plus propices aux erreurs, c'est pour cette raison qu'on utilise le format décimal pointé.

Exemple :



2. Adressage IPv4 :

Un routeur utilise l'adresse IP du réseau de destination afin de remettre le paquet au réseau approprié. On parle dans ce cas de système d'adressage hiérarchique, car il contient plusieurs niveaux. Chaque adresse IP regroupe ces deux identificateurs en un seul nombre. La première partie identifie l'adresse réseau du système «partie réseau»,. La seconde, appelée «partie hôte», identifie la machine sur le réseau.

IP address = <network number><host number>

Les adresses IP sont réparties en ***classes*** afin de définir des réseaux de différentes tailles :

- Les adresses de classe ***A*** sont affectées aux réseaux de grande taille.
- Les adresses de classe ***B*** sont utilisées pour les réseaux de taille moyenne
- Les adresses de classe ***C*** pour les réseaux de petite taille.

Classe d'adresses IP	Bits de valeur supérieure	Plage d'adresses du premier octet	Nombre de bits de l'adresse réseau
Classe A	0	0 - 127 *	8
Classe B	10	128 - 191	16
Classe C	110	192 - 223	24
Classe D	1110	224 - 239	28

- Le réseau 127.0.0.0 est réservé pour les tests en bouclage.
- Les adresses de classe D est réservée à la diffusion multicast d'une adresse IP.
- Les adresses de classe E est réservés à des fins expérimentales par le groupe IETF (*Internet Engineering Task Force*)

Adresses IP réservées :

Les adresses hôte réservées se composent des éléments suivants:

- ***Une adresse réseau*** – pour identifier le réseau lui-même.
- ***Une adresse de broadcast*** – pour diffuser des paquets vers tous les équipements.

- Une adresse IP dont tous les ***bits hôte*** sont occupés par des ***0*** binaires est réservée pour l'adresse réseau.
- Une adresse IP dont tous les ***bits hôte*** sont occupés par des ***1*** binaires est réservée pour l'adresse de Broadcast.

Adresses IP publiques et privées :

À l'origine, un organisme portant le nom d'***InterNIC*** (*Internet Network Information Center*) était chargé de la vérification de l'unicité des adresses IP. Celui-ci n'existe plus et a été remplacé par l'***IANA*** (*Internet Assigned Numbers Authority*).

- Chaque adresse IP publique étant unique, deux ordinateurs connectés à un réseau public ne peuvent pas avoir la même adresse IP publique.
- Les adresses IP publiques doivent être obtenues auprès d'un fournisseur d'accès Internet (FAI) ou d'un registre moyennant une participation.

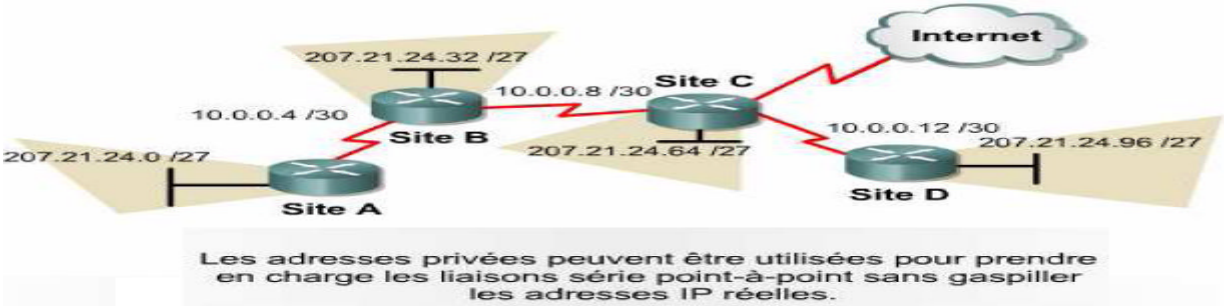
Pour résoudre le problème de pénurie (manque) d'adresses IP publiques plusieurs solutions sont utilisées :

- élaboration du routage CIDR (*Classless interdomain routing*)
- élaboration de la norme IPv6.
- Utilisation des adresses privées.

La spécification RFC 1918 réserve trois blocs d'adresses IP pour une utilisation ***privée*** et interne :

Classe	Plage d'adresses internes RFC 1918
A	10.0.0.0 à 10.255.255.255
B	172.16.0.0 à 172.31.255.255
C	192.168.0.0 à 192.168.255.255

Les adresses IP privées peuvent être mélangées aux adresses publiques.



La connexion d'un réseau à Internet par le biais d'adresses publiques nécessite la conversion des adresses privées en adresses publiques. Ce processus de conversion est appelé «***NAT***» (*Network Address Translation*).

3. Les masques de réseau

Pour que le réseau Internet puisse router (acheminer) les paquets de données, il faut qu'il connaisse l'adresse IP du réseau local de destination. On a vu précédemment qu'une adresse IP est constituée d'une partie Réseau et d'une partie Station.

IP address = <network number><host number>

Il faut donc déterminer cette adresse réseau à partir de l'adresse IP de destination. Pour cela on utilise le masque de sous réseau.

A chaque classe d'adresses est associé un masque de réseau, ou netmask, qui est constitué de 32 bits :

Classe	Masque
A	255. 0. 0. 0
B	255. 255. 0. 0
C	255. 255. 255. 0

❖ Un « ET » logique appliqué entre le masque de réseau et l'adresse IP permet d'obtenir l'adresse d'un réseau correspondant.

- Calcul de l'adresse réseau en décimal

@ IP	193	252	19	3
Masque Réseau	255	255	255	0
@ Réseau	193	252	19	0

- Calcul de l'adresse réseau en binaire

@ IP	1100 0001	1111 1100	0001 0011	0000 0011
Masque Réseau	1111 1111	1111 1111	1111 1111	0000 0000
@ Réseau	1100 0001	1111 1100	0001 0011	0000 0000

❖ Un « ET » logique appliqué entre le complément à 1 du masque de réseau et une adresse IP permet d'obtenir la partie hôte correspondante.

- Calcul de l'adresse hôte en décimal

@ IP	193	252	19	3
Masque Réseau	0	0	0	255
@ Hôte	0	0	0	3

- Calcul de l'adresse hôte en binaire

@ IP	1100 0001	1111 1100	0001 0011	0000 0011
Masque Réseau	0000 0000	0000 0000	0000 0000	1111 1111
@ Hôte	0000 0000	0000 0000	0000 0000	0000 0011

Ainsi, à l'aide du masque de réseau, on peut définir, pour toute adresse IP :

- L'adresse réseau associée,
- La partie hôte associée,
- L'adresse de diffusion associée qui désigne tous les hôtes de ce réseau.

❖ Le tableau suivant fournit ces informations pour trois adresses IP prises parmi les trois classes fondamentales.

Adresse IP	10. 25. 2. 5	172. 17. 5. 8	192. 168. 53. 24
Classe	A	B	C
Masque de réseau	255. 0. 0. 0	255. 255. 0. 0	255. 255. 255. 0
Adresse de réseau	10. 0. 0. 0	172. 17. 0. 0	192. 168. 53. 0
Adresse de diffusion	10. 255. 255. 255	172. 17. 255. 255	192. 168. 53. 255
Complément à 1 du masque	0.255.255.255	0.0.255.255	0.0.0.255
Partie hôte de l'adresse	0.25.2.5	0.0.5.8	0.0.0.24

4. Notion de sous-réseau

Le découpage d'un réseau en sous-réseaux implique l'utilisation du masque de sous réseau afin de fragmenter un réseau de grande taille en segments (ou sous-réseaux) plus petits, plus faciles à gérer et plus efficaces.

Pour créer une adresse de sous-réseau, l'administrateur réseau emprunte des bits au champ d'hôte et les désigne comme champ de sous-réseau.

IP address = <network number><subnet number><host number>

- Le nombre minimal de bits pouvant être empruntés est deux.
- Le nombre maximal de bits pouvant être empruntés est égal à tout nombre laissant au moins deux bits disponibles pour le numéro d'hôte.

4.1. Masque de sous-réseau

Le découpage du numéro d'hôte en numéro de sous-réseau et numéro d'hôte est laissé au libre choix de l'entreprise. L'administrateur du site choisit donc le nombre et la position des bits qu'il veut pour former le numéro de sous-réseau.

Ce choix est précisé par le masque de sous-réseau. Le masque reprend les 32 bits de l'adresse IP et positionne les bits correspondants au numéro de réseau ou de sous-réseau à 1, et les bits correspondants au numéro d'hôte à 0.

4.2. Mise en oeuvre

La mise en œuvre de sous-réseaux passe par les étapes suivantes :

- Déterminer le nombre de sous-réseaux à adresser.
- Déterminer le nombre maximum d'hôtes sur chaque sous-réseau.
- Calculer le nombre de bits nécessaires pour les sous-réseaux et pour les stations (en prévoyant les évolutions)
- Positionner le masque de sous-réseau.
- Lister les différents numéros de sous-réseaux possibles en éliminant les "tout à 0" et les "tout à 1".

Exemple n°1 :

Un réseau d'adresse 160.16.0.0 est divisé en 4 sous-réseaux. Chacun de ces 4 sous-réseaux accueille moins de 254 hôtes.

Nous disposons de 16 bits pour les numéros de sous-réseau et les numéros d'hôtes. Dans ce cas, on peut choisir la solution simple qui consiste à prendre 8 bits pour le numéro de sous-réseau, et 8 bits pour le numéro d'hôte. Ce choix permet d'adresser 256 sous-réseaux et 254 hôtes par sous-réseau.

Le masque de sous-réseau s'obtient en positionnant les bits de réseau et de sous-réseau à 1 et les bits d'hôtes à 0. Ceci donne en binaire :

11111111	11111111	11111111	00000000
réseau		sous réseau	hôte

Soit en représentation décimale : 255.255.255.0

Les adresses de sous-réseaux sont obtenues en listant toutes les possibilités sur les bits de sous-réseaux, et en positionnant les bits d'hôte à 0. Les adresses de sous-réseaux et les adresses d'hôtes seront :

	Numéros de sous-réseaux	Adresses de sous-réseau	Adresses d'hôte
Sous réseau n°0	0	160.16.0.0	160.16.0.1 à 160.16.0.254
Sous réseau n°1	1	160.16.1.0	160.16.1.1 à 160.16.1.254
Sous réseau n°2	2	160.16.2.0	160.16.2.1 à 160.16.2.254
Sous réseau n°3	3	160.16.3.0	160.16.3.1 à 160.16.3.254
Sous réseau n°4	4	160.16.4.0	160.16.4.1 à 160.16.4.254
...	...	...	... à ...
Sous réseau n°254	254	160.16.254.0	160.16.254.1 à 160.16.254.254
Sous réseau n°255	255	160.16.255.0	160.16.255.1 à 160.16.255.254

Exemple n°2

Le même réseau d'adresse 160.16.0.0 est divisé en 8 sous-réseaux. Les sous-réseaux ont au plus 1000 hôtes.

Le masque précédent ne convient plus. Pour adresser 8 sous-réseaux différents, il faut 8 numéros. 3 bits permettent d'adresser 6 (8-2) sous-réseaux et 4 bits permettent d'adresser 14 sous-réseaux. Il faut donc prendre cette dernière solution. Il reste dans ce cas, 12 bits pour le numéro d'hôte ce qui permet 4094 numéros d'hôtes. Le masque sera donc :

11111111	11111111	11110000	00000000
réseau		sous réseau	hôte

Soit en représentation décimale : 255.255.240.0

Pour déterminer les numéros de sous-réseaux, il faut toujours lister les possibilités sur 4 bits, en tenant compte des poids. Ceci nous donne :

0000 (0000) soit 0	0100 (0000) soit 64	1000 (0000) soit 128	1100 (0000) soit 192
0001 (0000) soit 16	0101 (0000) soit 80	1001 (0000) soit 144	1101 (0000) soit 208
0010 (0000) soit 32	0110 (0000) soit 96	1010 (0000) soit 160	1110 (0000) soit 224
0011 (0000) soit 48	0111 (0000) soit 112	1011 (0000) soit 176	1111 (0000) soit 240

Enfin, on obtient les adresses des hôtes sur chacun des sous-réseaux en fixant le numéro de sous-réseau, et en listant les possibilités sur les 12 bits du numéro d'hôte.

	Numéros de sous-réseaux	Adresses de sous-réseau	Adresses d'hôte
Sous réseau n°0	0	160.16.0.0	160.16.0.1 à 160.16.15.254
Sous réseau n°1	16	160.16.16.0	160.16.16.1 à 160.16.31.254
Sous réseau n°2	32	160.16.32.0	160.16.32.1 à 160.16.47.254
Sous réseau n°3	48	160.16.48.0	160.16.48.1 à 160.16.63.254
Sous réseau n°4	64	160.16.64.0	160.16.64.1 à 160.16.79.254
Sous réseau n°5	80	160.16.80.0	160.16.80.1 à 160.16.95.254
Sous réseau n°6	96	160.16.96.0	160.16.96.1 à 160.16.111.254
Sous réseau n°7	112	160.16.112.0	160.16.112.1 à 160.16.127.254
Sous réseau n°8	128	160.16.128.0	160.16.128.1 à 160.16.143.254
Sous réseau n°9	144	160.16.144.0	160.16.144.1 à 160.16.159.254
Sous réseau n°10	160	160.16.160.0	160.16.160.1 à 160.16.175.254
Sous réseau n°11	176	160.16.176.0	160.16.176.1 à 160.16.191.254
Sous réseau n°12	192	160.16.192.0	160.16.192.1 à 160.16.207.254
Sous réseau n°13	208	160.16.208.0	160.16.208.1 à 160.16.223.254
Sous réseau n°14	224	160.16.224.0	160.16.224.1 à 160.16.254.254
Sous réseau n°15	240	160.16.240.0	160.16.240.1 à 160.16.240.254

On peut obtenir l'adresse de sous-réseau d'un hôte à partir de son adresse IP et du masque de sous-réseau. Il suffit de réaliser un ET LOGIQUE entre les deux. Exemple : 160.16.198.1 avec un masque en 255.255.240.0

```
   10100000  00001000 11000110  00000001
ET 11111111  11111111 11110000  00000000
   ----------------------------------------
   10100000  00001000 11000000  00000000
          soit 160.16.192.0
```

5. Comparaison entre IPv4 et IPv6 :

Dans les années 80, la stratégie d'adressage proposée par la version IPv4 s'avérait relativement évolutive. Néanmoins, elle ne réussit pas à satisfaire les exigences liées à l'attribution des adresses.
Les adresses de classe A et B représentent 75% de l'espace d'adresses IPv4. Toutefois, moins de 17 000 organisations peuvent recevoir un numéro de réseau de classe A ou B.
Le nombre d'adresses réseau de classe C est nettement plus important que celui des adresses de classe A et B, bien qu'il ne représente que 12,5 % des quatre milliards d'adresses IP disponibles.

Dès 1992, le groupe IETF (Internet Engineering Task Force) a identifié deux problèmes :
· La diminution inquiétante des adresses réseau IPv4 disponibles.
· La hausse importante et rapide du volume des tables de routage d'Internet.
IPv6 encode les adresses sur ***128 bits*** au lieu de 32 (en utilisant des nombres hexadécimaux), ce qui porte le nombre d'adresses possibles à 340×10^{36}. Cette version devrait ainsi couvrir l'intégralité des besoins en communication pour les années à venir.
Afin de faciliter la lecture des adresses, il est possible d'omettre les zéros de tête dans chaque champ. Le champ «0003» est écrit «3». La représentation abrégée IPv6 de 128 bits consiste en huit nombres de 16 bits, représentés par quatre chiffres hexadécimaux.

6. Obtention d'une adresse Internet :

Un hôte réseau doit se procurer une adresse unique mondialement afin de se connecter à Internet. Le routeur n'utilise pas l'adresse MAC pour transmettre des données au-delà du réseau local.
Les administrateurs réseau font appel à deux méthodes différentes pour affecter les adresses IP. Il s'agit des méthodes **statique** et **dynamique**.

6.1. Adressage statique :

L'attribution statique convient particulièrement aux réseaux de petite taille qui subissent peu de changements. L'administrateur système effectue manuellement les opérations d'affectation et de suivi des adresses IP pour chaque hôte.
Le serveur, les imprimantes et les routeurs doivent être obligatoirement doté d'une adresse statique.

6.2. Attribution d'une adresse IP à l'aide du protocole RARP

Le protocole ***RARP*** associe des adresses MAC connues à des adresses IP.
Le protocole RARP permet à l'équipement de lancer une requête afin de connaître son adresse IP (dans le cas d'une station sans disque dur par exemple).
Les requêtes RARP sont diffusées sur le LAN et c'est le serveur RARP, habituellement un routeur, qui y répond.

Structure d'une requête ARP/RARP :

0 - 15 bits		16 - 31 bits
Type de matériel		Type de protocole
HLen (1 octet)	PLen (1 octet)	Opération
AM expéditeur (octets 1 - 4)		
AM expéditeur (octets 5 - 6)		AP expéditeur (octets 1 - 2)
AP expéditeur (octets 3 - 4)		AM cible (octets 1 - 2)
AM cible (octets 3 - 6)		
AP cible (octets 1 - 4)		
Structure de l'en-tête RARP		

Champ	Description
Type de matériel	Spécifie un type d'interface matérielle pour lequel l'expéditeur attend une réponse.
Type de protocole	Spécifie le type d'adresse de protocole de haut niveau fourni par l'expéditeur.
HLen	Longueur de l'adresse matérielle
PLen	Longueur de l'adresse de protocole
Opération	Les valeurs sont les suivantes : 1 Requête ARP 2 Réponse ARP 3 Requête RARP 4 Réponse RARP 5 Requête RARP dynamique 6 Réponse RARP dynamique 7 Erreur RARP dynamique 8 Requête InARP 9 Réponse InARP
@ Matériel de l'expéditeur	Longueur en Octet HLen
@ de Protocole de l'expéditeur	Longueur en Octet PLen
@ Matériel cible	Longueur en Octet HLen
@ Protocole cible	Longueur en Octet PLen

Exemple :

Requête RARP :

En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	3
FE:ED:F9:23:44:EF	FE:ED:F9:23		
Adresse MAC de destination	44:EF		non défini
FF:FF:FF:FF:FF:FF	non défini		FF:FF
Champ Type	FF:FF:FF:FF		
0X8035 (Ethernet)	non défini		

Réponse RARP :

En-tête de trame	1		0800_{16}
Adresse MAC source	06	04	4
FE:ED:F9:65:33:3A	FE:ED:F9:23		
Adresse MAC de destination	44:EF		192.168
FE:ED:F9:23:44:EF	10.36		FE:ED
Champ Type	F9:65:33:3A		
0X8035 (Ethernet)	192.168.10.98		

6.3. Attribution d'une adresse IP à l'aide du protocole BOOTP

Le protocole ***BOOTP*** *(Bootstrap Protocol)* fonctionne dans un environnement client serveur et ne requiert qu'un seul échange de paquet pour obtenir des informations sur le protocole IP (@IP, @routeur, @serveur …).

Le protocole BOOTP permet à un administrateur réseau de créer un fichier de configuration qui définit les paramètres de chaque équipement. L'administrateur doit ajouter les hôtes et tenir à jour la base de données (pas dynamique 100%).

BOOTP utilise la couche UDP pour transporter les messages.

Lorsqu'un client envoie un message BOOTP, le serveur BOOTP place son adresse IP dans le champ source et une adresse de broadcast dans le champ de destination. Cela permet de récupérer le paquet de réponse BOOTP au niveau de la couche transport en vue de son traitement. Seul un broadcast sera acheminé puisque le client ne connaît pas son adresse IP.

Structure d'une requête BOOTP :

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Non utilisé	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (64 octets)			

Structure des messages BOOTP

Champ	Description
Op	Code des messages (BOOTREQUEST ou BOOTREPLY)
Htype	Type d'adresse matérielle.
HLen	Longueur de l'adresse matérielle
Hops	Utilisé par le serveur pour envoyer les requêtes à un autre réseau
Xid	ID de la transaction
Secs	Secondes écoulées lors du processus.
Ciaddr	Adresse IP du client
Yiaddr	Votre adresse IP (Client)
Siaddr	@ IP du serveur servant dans le bootstrap.
Giaddr	@ IP de l'agent de relais
Chaddr	Adresse matérielle du client
Server Host Name	Le serveur qui doit fournir les informations BOOTP
Boot File Name	Fichier de démarrage suivant le SE utilisé
Vendor Specific Area	Informations facultatives sur le fournisseur.

Exemple :

Requête BOOTP :

En-tête de trame	En-tête du paquet	1	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:23:44:EF	Inconnu	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FF:FF:FF:FF:FF:FF	225.225.225.225	0				
Champ Type		0				
0X8035 (Ethernet)		0				
		FE:ED:F9:23:44:EF				

Réponse BOOTP :

En-tête de trame	En-tête du paquet	2	1	6	0	Vérification
Adresse MAC source	Adresse IP source	221				du CRC
FE:ED:F9:65:33:3A	192.168.10.98	2		Non utilisé		
Adresse MAC de destination	Adresse IP de destination	0				
FE:ED:F9:23:44:EF	225.225.225.225	192.168.10.36				
Champ Type		192.168.10.97				
0X8035 (Ethernet)		192.168.10.97				
		FE:ED:F9:23:44:EF				

6.4. Gestion des adresses IP à l'aide du protocole DHCP

Le protocole ***DHCP*** *(Dynamic Host Configuration Protocol)* a été proposé pour succéder au protocole BOOTP. Contrairement au protocole BOOTP, le protocole DHCP permet à un hôte d'obtenir une adresse IP de *manière dynamique* sans que l'administrateur réseau ait à définir un profil pour chaque équipement. Avec le protocole DHCP, il suffit qu'une plage d'adresses IP soit définie.
Le protocole DHCP dispose d'un avantage majeur sur le protocole BOOTP, car il permet aux utilisateurs d'être mobiles.
Le protocole DHCP offre une relation «***un à plusieurs***» pour les adresses IP.

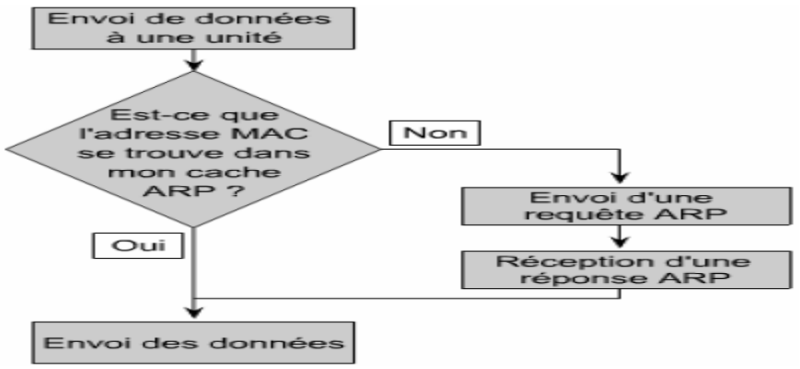
Structure d'une requête DHCP :

0 - 7 bits	8 - 15 bits	16 - 23 bits	24 - 31 bits
Op (1)	Htype (1)	HLen (1)	Hops (1)
Xid (4 octets)			
Secondes (2 octets)		Indicateurs (2 octets)	
Ciaddr (4 octets)			
Yiaddr (4 octets)			
Siaddr (4 octets)			
Giaddr (4 octets)			
Chaddr (16 octets)			
Nom d'hôte du serveur (64 octets)			
Nom du fichier de démarrage (128 octets)			
Zone spécifique du fournisseur (variable)			
Structure des messages DHCP			

Elle est presque semblable à la requête BOOTP

6.5. Protocole ARP (Address Resolution Protocol)

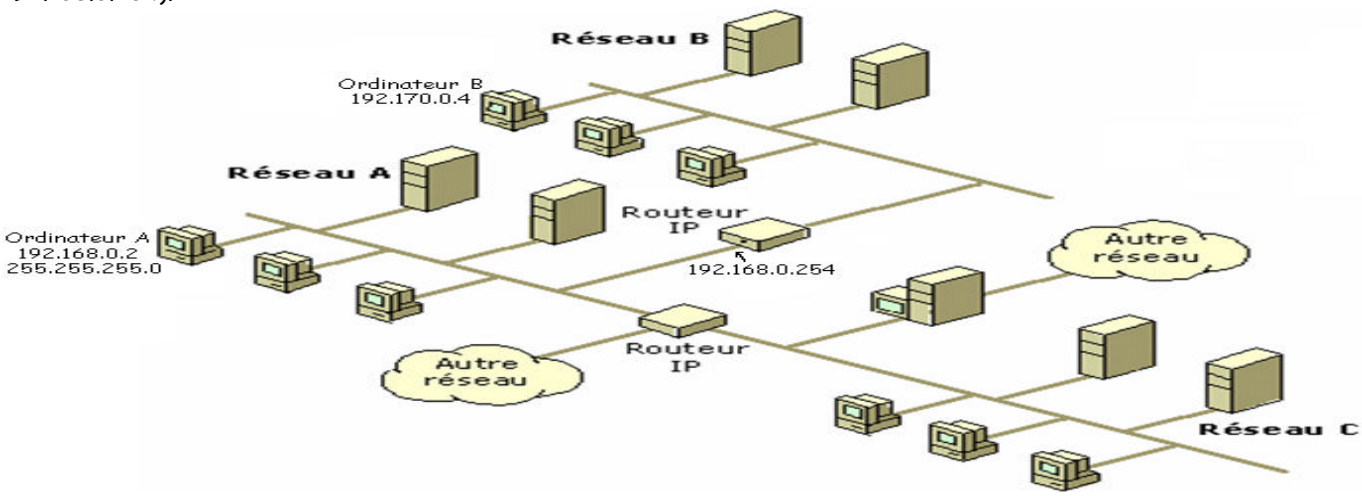
Dans un réseau TCP/IP, un paquet de données doit contenir une adresse MAC de destination et une adresse IP de destination. Si l'une ou l'autre est manquante, les données qui se trouvent au niveau de la couche 3 ne sont pas transmises aux couches supérieures.
Les «***tables ARP***» sont stockées dans la mémoire RAM, où les informations en mémoire cache sont mises à jour automatiquement dans chaque équipement (correspondance @IP &
@MAC pour les stations du même domaine de Broadcast).
Méthodes pour obtenir les adresses MAC :
- la première consiste à surveiller le trafic existant sur le segment du réseau local et enregistrer les adresses source IP et MAC du datagramme dans une table ARP.
- La deuxième consiste à diffuser une requête ARP.
Les routeurs ne transmettent pas les paquets de broadcast. Lorsque la fonction est activée, le routeur exécute une requête via ***Proxy ARP***.
Proxy ARP est une variante du protocole ARP. Dans cette variante, un routeur envoie une réponse ARP, qui contient l'adresse MAC dont l'adresse IP n'appartient pas à la plage d'adresses du sous-réseau local.
Une autre solution pour envoyer des données à l'adresse d'un équipement situé sur un autre segment du réseau, consiste à configurer une passerelle par défaut.



7. Principe du routage des paquets IP

Considérons un ordinateur A du réseau A d'adresse 192.168.0.2 (mettons-lui un masque de sous-réseau de 255.255.255.0). Admettons qu'il veuille envoyer un paquet IP à l'ordinateur B du réseau B d'adresse 192.170.0.4.

En utilisant le masque de sous-réseau, A comprend qu'il ne peut atteindre directement B. Que fait-il donc ? Il envoie sans réfléchir le paquet IP à l'adresse du routeur par défaut (disons que ce dernier a été défini comme 192.168.0.254).



7.1. Qu'est-ce que ce *routeur* ?

Le routeur est une machine pouvant "jouer sur plusieurs sous-réseaux" en même temps. Typiquement, si on utilise un ordinateur, ce dernier possèdera deux cartes réseaux (ou plus), l'une connectée sur l'un des sous-réseaux (dans notre cas, disons qu'elle possède l'adresse 192.168.0.254), l'autre connectée sur l'autre sous-réseau (disons 192.170.0.192). S'il utilise le bon logiciel, un tel ordinateur est capable de faire transiter des paquets IP du réseau 192.168.0.0 vers le réseau 192.170.0.0, et inversément bien sûr. C'est donc grâce à des routeurs que différents sous-réseaux d'un réseau de classe C peuvent communiquer entre eux, par exemple l'ordinateur 192.168.0.2 avec l'ordinateur 192.168.0.120 d'un réseau de classe C subdivisé en 8 sous-réseaux (masque de sous réseau 255.255.255.224).

7.2. Question pertinente : pourquoi subdiviser et ne pas faire de "méga" réseaux ?

Les deux points suivants expliquent en partie pourquoi on procède ainsi.

- Limiter le trafic sur un tronçon donné. Imaginons deux réseaux locaux A et B séparés par un routeur. Lorsque des ordinateurs de A discutent avec des ordinateurs de B, le routeur a pour rôle de transmettre l'information du réseau A vers le réseau B (et inversément). Par contre, si des ordinateurs de A s'échangent entre eux des données, il n'y a pas de raison qu'ils encombrent inutilement le trafic sur le réseau B, et c'est bien pour cette raison que les réseaux A et B sont distincts.
- Autre évidence : si le réseau A tombe en panne, le réseau B n'en est pas affecté. C'est d'ailleurs l'avantage principal de subdiviser : éviter qu'un ennui technique qui pourrait rester localisé ne perturbe la totalité du réseau.
- Autre aspect non négligeable : le *broadcast (diffusion)*. Vous ne le savez peut-être pas, mais dans votre dos, les ordinateurs sont de grands bavards : ils ne cessent de causer entre eux pour signaler leur présence ou se mettre d'accord sur les protocoles qu'ils sont capables de comprendre. Pensez un peu si Internet n'était constitué que d'un seul segment : le broadcast seul des ordinateurs utiliserait l'intégralité de la bande passante avant même qu'un seul octet de données ait pu être transmis ! Pour cette raison, le travail des routeurs est non seulement de faire transiter les paquets IP, mais aussi de **filtrer** le broadcast local qui n'intéresse pas la planète entière.

Vous comprendrez par là que les routeurs jouent un rôle essentiel pour éviter la saturation du trafic.

Disons encore quelques mots sur l'acheminement des paquets IP. Vous comprenez maintenant que lorsqu'un ordinateur doit acheminer un paquet IP, il vérifie tout d'abord s'il peut le transmettre

directement (grâce au masque de sous-réseau); s'il ne peut pas, il l'envoie bêtement, sans réfléchir, au routeur par défaut. A partir de là, les routeurs sont généralement configurés pour savoir où diriger les paquets IP qui leur sont confiés; les routeurs bavardent entre eux (à l'aide de protocoles particuliers de routage, RIP ou OSPF par exemple) pour savoir quelle est la meilleure route (la plus courte généralement) pour qu'un paquet IP atteigne sa destination. De même, si une route est soudainement interrompue, les routeurs sont capables de se reconfigurer et proposer des nouvelles routes de secours.

7.3. Table de routage IP de Windows

Chaque ordinateur exécutant TCP/IP prend des décisions de routage. Celles-ci sont contrôlées par la table de routage IP. Pour afficher la table de routage IP sur un ordinateur exécutant Windows XP, vous pouvez taper route print à l'invite de commandes.
Le tableau suivant illustre un exemple de table de routage IP. Cet exemple s'applique à un ordinateur exécutant Windows XP avec une carte réseau et la configuration suivante :

Adresse IP : 10.0.0.169
Masque de sous-réseau : 255.0.0.0
Passerelle par défaut : 10.0.0.1

Description	Destination du réseau	Masque de réseau	Passerelle	Interface	Métrique
Itinéraire par défaut	0.0.0.0	0.0.0.0	10.0.0.1	10.0.0.169	1
Réseau de bouclage	127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
Réseau local	10.0.0.0	255.0.0.0	10.0.0.169	10.0.0.169	1
Adresse IP locale	10.0.0.169	255.255.255.255	127.0.0.1	127.0.0.1	1
Adresses multidestinataires	224.0.0.0	240.0.0.0	10.0.0.169	10.0.0.169	1
Adresse de diffusion limitée	255.255.255.255	255.255.255.255	10.0.0.169	10.0.0.169	1

Notes

- Les descriptions de la première colonne du tableau précédent ne sont pas actuellement affichées à la sortie de la commande route print.
- La table de routage est automatiquement créée, en fonction de la configuration TCP/IP actuelle de votre ordinateur. Chaque itinéraire occupe une seule ligne dans le tableau affiché. Votre ordinateur recherche dans la table de routage une entrée qui correspondrait le mieux à l'adresse de destination IP.
- Votre ordinateur utilise l'itinéraire par défaut si aucun autre itinéraire d'hôte ou de réseau ne correspond à l'adresse de destination intégrée dans un datagramme IP. L'itinéraire par défaut transmet généralement un datagramme IP (pour lequel il n'existe pas d'itinéraire local correspondant ou explicite) dans une adresse de passerelle par défaut pour un routeur du sous-réseau local. Dans l'exemple précédent, l'itinéraire par défaut transmet le datagramme vers un routeur avec une adresse de passerelle 10.0.0.1.
- Étant donné que le routeur qui correspond à la passerelle par défaut contient des informations relatives au réseau dans l'internet, il transmet le datagramme vers les autres routeurs jusqu'à ce que le datagramme soit éventuellement livré à un routeur IP connecté à l'hôte ou au sous-réseau de destination spécifié dans le réseau le plus grand.

Les sections suivantes décrivent chacune des colonnes affichées dans la table de routage IP : destination du réseau, masque de réseau, passerelle, interface et métrique.

- **Destination du réseau**
  La destination du réseau est utilisée avec le masque de réseau pour correspondre à l'adresse de destination IP. La destination du réseau est comprise entre 0.0.0.0 pour l'itinéraire par défaut et 255.255.255.255 pour la diffusion limitée qui est une adresse de diffusion spéciale vers tous les hôtes du même segment de réseau.

- **Masque de réseau**
  Le masque de réseau est le masque de sous-réseau appliqué à l'adresse de destination IP lors d'une comparaison à la valeur de destination du réseau. Lorsque le masque de réseau est au format binaire, les " 1 " doivent concorder, mais pas les " 0 ". Par exemple, un masque de réseau 0.0.0.0 est utilisé pour l'itinéraire par défaut, ce qui signifie qu'aucun des bits ne doit concorder. Pour les itinéraires d'hôtes on utilise une adresse IP avec un masque réseau 255.255.255.255.
- **Passerelle**
  L'adresse de la passerelle est l'adresse IP que l'hôte local utilise pour transmettre les datagrammes IP vers d'autres réseaux IP. Il s'agit soit de l'adresse IP d'une carte réseau locale, soit de l'adresse IP d'un routeur IP (tel que le routeur de la passerelle par défaut) sur le segment de réseau local.
- **Interface**
  L'interface est l'adresse IP configurée sur l'ordinateur local pour la carte de réseau local utilisée lorsqu'un datagramme IP est transmis sur le réseau.
- **Métrique**
  Une métrique indique le coût de l'utilisation d'un itinéraire qui correspond généralement au nombre de relais vers la destination IP. Un saut correspond à tout ce qui se trouve sur le sous-réseau local. Chaque routeur utilisé au-delà de ce premier saut correspond à un saut supplémentaire. S'il existe plusieurs itinéraires vers la même destination avec différentes métriques, l'itinéraire présentant la métrique la plus faible est sélectionné.
  Pour plus d'informations sur l'ajout d'itinéraires à la table de routage IP, consultez Ajouter un itinéraire IP statique Pour plus d'informations sur la suppression d'itinéraires de la table de routage IP, consultez Supprimer un itinéraire IP statique

7.4. Exemple de hôtes multiples sous Windows XP

Considérons un pc avec deux cartes réseaux ayant les configurations suivantes :

• Carte réseau 1 Adresse IP : 10.0.0.169 Masque de sous-réseau : 255.0.0.0 Passerelle par défaut : 10.0.0.1	• Carte réseau 2 Adresse IP : 192.168.0.200 Masque de sous-réseau : 255.255.0.0 Passerelle par défaut : 192.168.0.1

Destination du réseau	Masque de réseau	Passerelle	Interface	Métrique
0.0.0.0	0.0.0.0	10.0.0.1	10.0.0.169	1
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.200	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
10.0.0.0	255.0.0.0	10.0.0.169	10.0.0.169	1
10.0.0.169	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.0.0	192.168.0.200	192.168.0.200	1
192.168.0.200	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.0.255	255.255.255.255	192.168.0.200	192.168.0.200	1
224.0.0.0	240.0.0.0	10.0.0.169	10.0.0.169	1
224.0.0.0	240.0.0.0	192.168.0.200	192.168.0.200	1
255.255.255.255	255.255.255.255	10.0.0.169	10.0.0.169	1

255.255.255.255	255.255.255.255	192.168.0.200	192.168.0.200	1

Notes :

- Lorsque vous configurez une passerelle par défaut pour chaque carte réseau, vous créez un itinéraire 0.0.0.0 pour chaque carte réseau. Cependant, un seul itinéraire par défaut est en réalité utilisé. Dans l'exemple précédent, l'adresse IP 10.0.0.169 est la première carte réseau des liaisons TCP/IP, c'est la raison pour laquelle l'itinéraire par défaut pour la Carte réseau 1 est utilisé. Dans la mesure où une seule passerelle par défaut est utilisée, il vous suffit de configurer une seule carte réseau avec une passerelle par défaut. Cela réduit les risques de confusion et garantit les résultats attendus.
- Si le routeur IP est un routeur de Windows 2000 et ne possède pas d'interface sur un réseau donné, il a besoin d'un itinéraire pour accéder au réseau. Vous pouvez ajouter des itinéraires statiques ou utiliser des protocoles de routage fournis par le service de routage et d'accès distant. Pour plus d'informations sur le routage IP avec le service de routage et d'accès distant, consultez Routage.

7.5. Commande Route

Gère les tables de routage du réseau. Cette commande est disponible uniquement si le protocole TCP/IP est installé.

route [-f] [-p] [*commande* [*destination*] [masque *masque_sous-réseau*] [*passerelle*] [métrique *coût_métrique*]]

Paramètres :

-f Efface les tables de routage de toutes les entrées de passerelle. Associé à l'une des commandes, ce paramètre purge les tables avant l'exécution de la commande.

-p Associé à la commande add, ce paramètre crée une route persistante au travers des amorçages du système. Par défaut, les routes ne sont pas maintenues lorsque le système est relancé. Associé à la commande print, ce paramètre affiche la liste des routes persistantes enregistrées. Ce paramètre est ignoré pour toutes les autres commandes qui affectent systématiquement les routes persistantes appropriées.

commande

Spécifie une des commandes suivantes :

print	Imprime une route.
add	Ajoute une route.
delete	Supprime une route.
change	Modifie une route existante.

destination

Spécifie l'ordinateur auquel la *commande* est transmise.

masque *masque_sous-réseau*

Spécifie le masque de sous-réseau à associer à cette entrée d'itinéraire. Si le masque n'est pas spécifié, 255.255.255.255 est utilisé.

passerelle

Spécifie la passerelle, tous les noms symboliques spécifiés comme *destination* ou *passerelle* sont référencés à la fois dans le fichier de base de données du réseau appelé Networks et dans le fichier de base de données des noms d'ordinateur nommé Hosts. Avec la commande print ou delete, vous pouvez employer des caractères génériques pour la destination et la passerelle ou omettre l'argument passerelle.

métrique *coût_métrique*

Assigne un coût métrique entier (entre 1 et 9 999) à utiliser pour calculer les routes les plus rapides, fiables et/ou économiques.

G . Couche liaison de données

Méthodes d'accès au support

Sur un canal point à point un émetteur peut transmettre librement. En revanche, lorsque le support est partagé par plusieurs périphériques, il est nécessaire de gérer la façon dont les données sont échangées.

Elles dépendent de l'architecture réseau, c'est-à-dire de la topologie logique. Suivant le cas, le signal sera diffusé sur le support et atteindra les bornes de chaque carte réseau ou transitera de poste en poste en étant répété par chaque station.

Une méthode d'accès décrit les règles qui régissent pour chaque matériel, l'accès, la transmission et la libération du canal partagé. On distingue essentiellement trois types de méthodes : la contention, le polling et le jeton passant.

1. Contention

Avec la contention, chaque station émet quand elle le veut, après écoute du canal (Carrier Sense ou écoute de la porteuse), qui doit être disponible. La trame émise est écoutée, pour vérifier qu'aucun autre signal ne vient perturber l'émission. II n'existe dans ce cas aucun arbitrage du canal. Bien qu'écoutant le support partagé, deux stations peuvent émettre simultanément ce qui conduit à une sur-tension (en coaxial) ou à une réception d'informations sur la paire réceptrice, alors que des données sont émises sur l'autre paire (en paire torsadée).

Dans ce cas, on parle d'une collision. Le plus important, dans cette méthode, est qu'une station émettrice soit capable de déterminer si sa trame est ou non entrée en collision avec une autre.
Ceci est possible à condition de respecter un certain nombre de contraintes (par exemple l'étendue maximale du réseau). C'est ainsi qu'avec Ethernet une trame ne doit pas être inférieure à 64 octets de manière à ce que la station émettrice soit capable de détecter une collision avant d'avoir envoyé le dernier octet de sa trame.
A titre indicatif, un bit de donnée d'une trame en Ethernet 10 Mbps, est représenté par un signal qui s'étend sur 23 mètres. Ce qui implique que la plus petite trame Ethernet (de 64 octets) peut s'étendre sur plus de 10 Km !
Lorsqu'il se produit une collision, la première station qui la détecte prolonge son émission par un signal spécial (trame de brouillage, ou JAM), afin de s'assurer que toutes les stations émettrices apprennent qu'une collision a eu lieu.
Dans ce cas, un temps d'attente différent est défini aléatoirement pour chaque machine qui émettait au moment de la collision. Ainsi toutes les machines n'essaieront pas de reprendre le contrôle du canal au même moment.
Les deux implémentations les plus répandues pour la contention sont CSMA/CD et CSMA/CA.
CSMA correspond à l'écoute de la porteuse (Carrier Sense) sur un support partagé (Multiple Access). Les deux mises en oeuvre se distinguent par le fait que l'une détecte les collisions
(Collision Détection), et l'autre tente de les éviter (Collision Avoidance).
Le second cas constitue une variante par rapport à la méthode décrite ci-dessus. En effet, plutôt que d'essayer de transmettre les données en risquant une collision (après écoute du support), le périphérique va envoyer une trame préliminaire pour avertir les autres stations qu'elle veut prendre possession du canal (pour envoyer sa trame de données).
CSMA/CD correspond à l'implémentation Ethernet, tandis que CSMA/CA est celle adoptée par LocalTalk (réseaux Macintosh).

Avantages et Inconvénients

Le gros avantage de cette gestion du canal est sa simplicité. Cependant, la méthode n'est pas déterministe, car le temps d'accès au canal n'est pas prévisible. De plus aucune gestion de priorité n'est possible pour des matériels qui ont des besoins d'accéder rapidement au support partagé.

2. Polling

Un matériel est désigné comme administrateur de l'accès au canal. Ce matériel, le maître, interroge dans un ordre prédéterminé chacun des autres matériels et leur demande s'ils ont des informations à transmettre. Le plus souvent, le maître est un concentrateur et les matériels secondaires sont les nœuds de l'étoile.

Avantages et Inconvénients

L'avantage est que tous les accès au canal sont centralisés. De plus, le temps d'accès et le volume des données manipulées sur le canal sont prévisibles et fixés.

Cependant, la méthode utilise une partie de la bande passante du réseau pour émettre des messages d'avertissement et des acquittements.

On peut citer comme exemple de polling, la méthode d'accès de priorité à la demande (ou DPAM, Demand Priority Access Method) gérée par la norme 100VG AnyLan.

3. Jeton passant

Dans la méthode du jeton passant, les trames circulent de poste en poste, chacun se comportant comme un répéteur. Initialement, une petite trame (le jeton) est répétée de poste en poste jusqu'à ce qu'une machine qui désire émettre le conserve pendant un temps fixé.

Le jeton est un message d'autorisation qui donne le contrôle du canal à la station qui le possède. La station détentrice du jeton peut émettre sa trame, qui va être répétée par chaque station et faire ainsi le tour de l'anneau. Au passage, le destinataire de la trame qui voit passer le signal en fait une copie (si celle-ci n'est pas erronée et si le récepteur dispose de suffisamment de place dans son tampon de réception). La trame qui a été copiée est marquée par le destinataire pour informer l'émetteur que la trame a ou non été lue. Une fois que la trame a fait le tour de l'anneau, l'émetteur retire sa trame et retransmet le jeton vers la prochaine station.

Avantages et inconvénients

Le jeton passant implémente une solution déterministe qui permet un bon contrôle du canal.

Le débit maximum réel atteint est beaucoup plus élevé qu'en Ethernet qui est sujet aux collisions.

Il existe plusieurs normes à jeton passant. Sur des topologies en anneau (IEEE 802.5, Token Ring ou FDDI) mais aussi sur des topologies en bus (IEEE 802.4).

4. Jeton passant contre contention

La contention est meilleure sur les réseaux à faible charge, car dans ce cas, il n'y a que très peu de collisions.

On a déterminé que 11% de collisions constituait un maximum à ne pas dépasser.

Au contraire, le jeton passant nécessite tout un mécanisme de gestion du canal, ce qui le rend meilleur lorsque la charge réseau est élevée.