M103 : CONCEVOIR UN RÉSEAU INFORMATIQUE

Table des matières

1 Introduction aux réseaux informatique

1.1 Définition d'un réseau

Un réseau informatique est un ensemble d'équipements informatiques reliés entre eux par des câbles ou avec des technologies sans fil pour échanger des informations.

1.2 Avantages d'un réseau

Voici quelques-uns des avantages des réseaux informatiques :

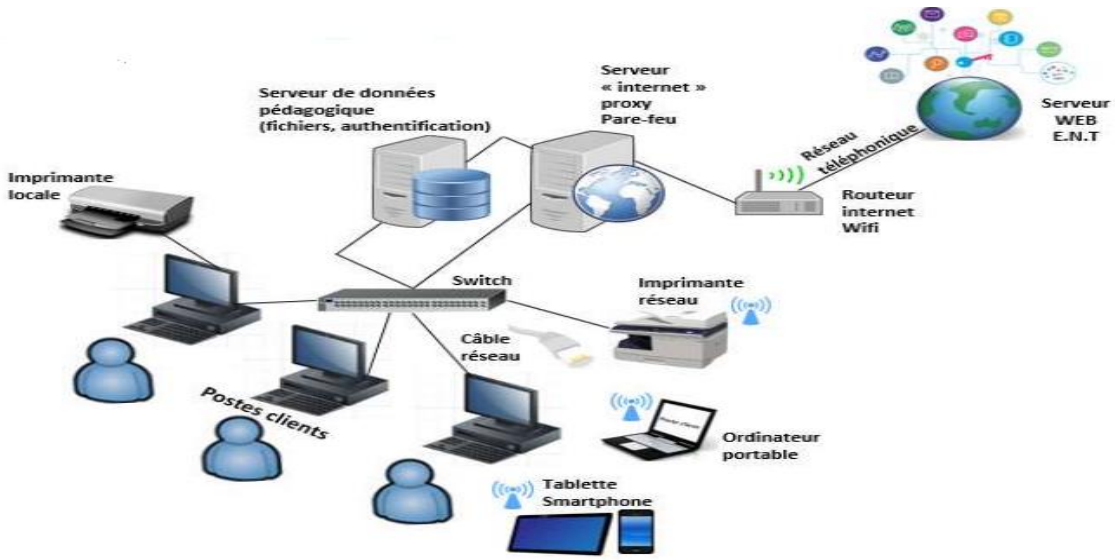
- Partager des données
- Partage de ressources
- Partage d'applications
- La communication entre les membres du réseau

1.3 Composants d'un réseau

Un réseau informatique (comme celui du collège par exemple) est composé principalement :

- De **postes clients** : ce sont des ordinateurs connectés au réseau par l'intermédiaire de cartes réseaux (avec ou sans fils).
- D'un ou plusieurs **commutateurs** (Switch) qui permettent de relier les postes clients, les serveurs, les imprimantes…
- D'un **routeur internet** qui permet de se connecter au réseau internet
- Des **liaisons** par câble (câble Ethernet), fibre optique ou sans fil,

D'un modem (routeur) avec une passerelle pour se connecter au réseau internet (la passerelle permet de « filtrer » l'internet pour sécuriser le réseau local)



1.4 Catégories de réseaux informatiques

On distingue quatre catégories de réseaux informatiques selon leur taille (nombre de machines) et leur étendue :

- Le réseau personnel (**PAN** : Personal Area Network), relie des machines sur quelques mètres
- Le réseau local (**LAN** : Local Area Network), est adapté à la taille d'un site d'entreprise
- Le réseau métropolitain (**MAN** : Metropolitan Area Network), est un réseau étendu à l'échelle d'une ville
- Le réseau étendu **WAN** : (Wide Area Network), couvre une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent

1.5 Topologie des réseaux de type LAN

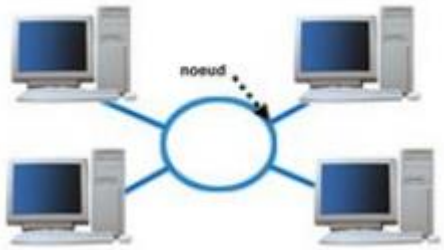
Il existe trois topologies de base pour concevoir un réseau : bus, anneau et étoile

1.5.1 TOPOLOGIE EN BUS

Le bus est un segment central où circulent les informations. Il s'étend sur toute la longueur du réseau et les machines viennent s'y accrocher. Lorsqu'une station émet des données, elles circulent sur toute la longueur du bus et la station destinatrice peut les récupérer. Une seule station peut émettre à la fois. En bout de bus, un « bouchon » permet de supprimer définitivement les informations pour qu'une autre station puisse émettre.

L'avantage du bus réside dans la simplicité de sa mise en œuvre. Par contre, en cas de rupture du bus, le réseau devient inutilisable

1.5.2 TOPOLOGIE EN ANNEAU



Développée par IBM, cette architecture est principalement utilisée par les réseaux Token Ring. Elle utilise la technique d'accès par « jeton ». Les informations circulent de station en station, en suivant l'anneau. Un jeton circule autour de l'anneau. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le jeton à son voisin, et ainsi de suite…

1.5.3 TOPOLOGIE EN ÉTOILE

C'est la topologie la plus courante. Toutes les stations sont reliées à un unique composant central : le concentrateur. Quand une station émet vers le concentrateur, celui-ci envoie les données à celle qui en est le destinataire (switch) ou à toutes les autres machines (hub). Ce type de réseau est facile à mettre en place et à surveiller. La panne d'une station ne met pas en cause l'ensemble du réseau. Par contre, il faut plus de câbles que pour les autres topologies, et si le concentrateur tombe en panne, tout le réseau est hors d'état de fonctionner. De plus, le débit pratique est moins bon que pour les autres topologies.

La méthode d'accès à un réseau définie comment la carte réseau accède au réseau, c'est à dire comment les données sont déposées sur le support de communication et comment elles sont récupérées. La méthode d'accès permet de contrôler le trafic sur un réseau (qui parle, quand et pour combien de temps). La méthode d'accès au réseau est aussi appelée « méthode de transmission ».

1.6 Méthodes d'accès

Les principales méthodes d'accès sont les suivantes :

- Accès aléatoire
  - ✓ CSMA/CD (Collision detection) : pour les réseaux en étoile (Ethernet)
  - ✓ CSMA/CA (Collision avoidance) : pour les réseaux Wifi
- Accès déterministe : une machine a le droit d'émettre si elle possède le jeton.
  - ✓ Token ring : le jeton circule dans l'ordre physique des stations, pour les réseaux en anneau

• **C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **D**etection
– **CSMA** : avant d'émettre, l'émetteur « écoute » le support de transmission (= canal), afin de détecter des émissions en cours
– **CD** : l'émetteur s'aperçoit qu'un autre nœud est en train d'envoyer un message au même moment que lui (= collision)
• Collision = brouillage des trames et réception incorrecte, les trames doivent être émises à nouveau
• Collision Detection : méthode non adaptée aux réseaux sans fil (ex. 802.11), pas d'écoute possible pendant l'émission

2 Transmission de données

2.1 Notions

Nous allons aborder des notions de vocabulaire qu'il faut connaitre :

- ✓ **Une ligne** : c'est le support physique de la communication entre deux ou plusieurs équipements.
- ✓ **Une voie** : c'est la possibilité de transmission sur la ligne, sachant qu'une ligne peut supporter plusieurs voies.
- ✓ **Une liaison :** c'est l'état de la communication entre deux ou plusieurs équipements

On distingue deux types de liaisons :

- **Point à Point** : ce sont deux équipements seulement qui sont reliés entre eux.
- **Multipoin**t : plusieurs équipements sont reliés entre eux. Quand un message est envoyé par un équipement, tous les autres le reçoivent, seul 'équipement concerné doit le prendre en compte.

Une liaison est soit permanente (établie en continue) soit temporaire et dans ce cas elle est dit commutée.

On distingue deux types de commutation :

- **La commutation de circuits** (physique) : le chemin entre l'émetteur et le récepteur qui est assure. La liaison n'appartient qu'aux deux interlocuteurs dès que la communication est établie. L'exemple le plus connu c'est le réseau téléphonique.
- **La commutation de messages** (logique) : c'est une commutation virtuelle dans ce cas, c'est l'acheminement de l'émetteur vers le récepteur qui est assuré.

2.2 Modes de transmissions de données

- **La transmission série :** Les données sont codées et transmises sur un même bus, les une à la suite des autres.
- **La transmission parallèle** : La transmission est simultanée, le parallélisme est réalisé soit par duplication de ligne, soit par le partage de la ligne.
- **La transmission synchrone** : Dans ce mode l'intervalle de temps entre chaque donnée est constant. La synchronisation entre l'émetteur et le récepteur est assurée par une signalisation particulière qui permet de resynchroniser les horloges, l'émetteur et le récepteur sont sur la même fréquence.
- **La transmission asynchrone** : La fréquence peut être irrégulière, la reconnaissance des messages est réalisée par un bit start et un bit stop

2.3 Utilisation d'une voie de transmission.

- **Simplex** : la ligne est utilisée que dans un sens A est émetteur B récepteur.
- **Half Duplex** : Chacun peut être émetteur ou récepteur, mais pas les deux à la fois.
- **Full Duplex** : Chacun peut être émetteur et récepteur en même temps. La ligne est utilisée dans les deux sens simultanément.

3 Les supports de transmission

La transmission d'information s'effectue au travers de médias dont les performances diffèrent fortement, sur le marché on trouve principalement trois types de câbles :

- Les câbles coaxiaux qui sont de moins en moins utilisés.
- Les câbles à pair torsadées qui se généralisent.
- Les câbles en fibre optique qui commencent à émerger.

Il existe trois noms pour désigner le réseau Ethernet :

- **802.3** est le nom qui porte la norme est donc le nom correct à employer.

- **Ethernet** le terme le plus employé.
- **CSMA/CD** est le sigle utilisé pour attribuer le droit de parole sur ce type de réseau.

La norme 802.3 spécifie pour chaque média un nom, et donc à chaque média correspond des caractéristiques spécifiques. Ce nom est de la forme : XX TTT MM

- **XX** représente la vitesse de transmission, en mégabit par seconde.
- **TTT** représente le type de codage des signaux (bande de base).
- **MM** représente l'identification du média, ou la longueur maximum du segment, en centaine de mètre.

NOM	Caractéristiques
10 Base 5	10 Mb/s, en bande de base avec un segment de 500 m au maximum.
10 Base 2	10 Mb/s, en bande de base, avec un segment de 200 m (185 m) au maximum.
10 Base T	10 Mb/s, en bande de base, sur câble en paires torsadées (T = Twister).
10 Base F	10 Mb/s, en bande de base, sur câble fibre optique.
100 Base Tx	100 Mb/s, en bande de base, sur câble en paires torsadées
100 Base T4	100 Mb/s, en bande de base, sur 4 paires torsadées.
100 Base Fx	100 Mb/s, en bande de base, sur câble fibre optique.
1000 Base T	1000 Mb/s, en bande de base, sur 4 paires torsadées.
1000 Base SX	100 Mb/s, en bande de base, sur câble fibre optique monomode
1000 Base LX	100 Mb/s, en bande de base, sur câble fibre optique multimode.
10 Gbase LX4	10 Gb/s sur câble fibre optique

3.1 Le câble coaxial

3.1.1 Le câble coaxial : 10 Base 5 & 10 Base 2

Ce type de câblage n'est plus utilisé, il a été remplacé par la paire torsadé. Sa topologie physique est de type Bus. Sa connexion est réalisée à l'aide d'un connecteur de type BNC ou T-BNC.

T-BNC

Résistance de terminaison

Fiche BNC

Câble coaxial

<u>Règle d'interconnexion d'un réseau Ethernet 10Base5 ou 10Base2 :</u>

- Nombre de station sur l'ensemble de réseau : 1024 stations.
- Nombre maximum de segments en série : 5 segments
- Nombre maximum de répéteurs : 4

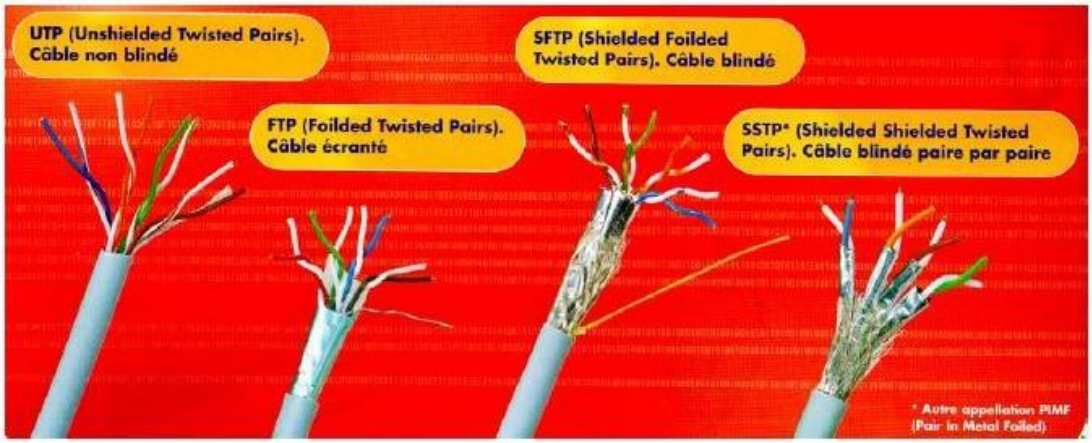
3.1.2 Les paires torsadées

Un câble à paires torsadés est constitué de 4 paires de fils torsadés deux par deux. Un code de couleurs normalisé repère chaque fil. Les torsades permettent de limiter l'effet de diaphonie (influence parasite d'une paire sur l'autre). Un blindage éventuel du câble permet quant à lui de limiter l'influence des parasites extérieurs.

<u>Les blindages</u> :

- **<u>UTP</u>** : Unshielded Twisted Paires. Non blindé utilisé dans les installations non sensibles.

- **FTP** : Foiled Twisted Pairs. Ecranté (avec feuille d'aluminium) le plus utilisé actuellement en lien permanent dans une installation.
- **SFTP** : Shielded Twisted Pairs. Blindé (avec stresse de masse et feuille d'aluminium) utilisé dans les installations proches des courants forts.
- **SST**P : Shielded Shielded Twisted Pairs. Chaque paire est blindée séparément et le tout est blindé à son tour, utilisé pour les installations en environnement très difficile ou avec des fréquences de travail très élevées (CAT 6 et plus).



La langueur maximale du câble est de 100m avec connecteur RJ45

Paire(s) à utiliser

Application	Paires employées
Téléphone analogique	7-8
Téléphone numérique	4-5
Numéris S0	3-6 et 4-5
Ethernet 10/100 Base T	1-2 et 3-6
Gigabit Ethernet	1-2, 3-6, 4-5 et 7-8
Token Ring	3-6 et 4-5
ATM 155	1-2 et 7-8
ATM 622 *(4 x 155)*	1-2, 3-6, 4-5 et 7-8

Norme EIA 568

PIN	568A	568B
1	Blanc-vert	Blanc-orange
2	Vert	Orange
3	Blanc-orange	Blanc-vert
4	Bleu	Bleu
5	Blanc-bleu	Blanc-bleu
6	Orange	Vert
7	Blanc-Marron	Blanc-Marron
8	Marron	Marron

1→ *TxD+* 2→ *TxD-* (Emission) 3→ *RxD+* 6→ *RxD-* (Reception)

En Ethernet 10/100Base T, seuls 4 fils sont utilisés, mais on câble systématiquement les 8 en vue de la norme Gigabit Ethernet.

Dénomination	Caractéristique
Catégorie 1	Transport de la voix
Catégorie 2	Voix et Données 4MB/s
Catégorie 3	Voix et Données 10MB/s
Catégorie 4	Voix et Données 16MB/s
Catégorie 5	Voix et Données 100MB/s
Catégorie 6	Voix et Données 1000MB/s

Câble droit ou croisé :

Câble droit : correspondance entre les pins de connecteurs 1 et 2.

Câble croisé : Inversion des pins (paire à paire) des connecteurs 1 et 2.

Entre deux éléments de même nature (PC à PC, commutateur à commutateur,) en utilise un câble croisé si non un câble droit.

3.1.3 La fibre optique

Les messages sont codés numériquement en impulsions lumineuses et transmis sur de grandes distances le long de ces minces fibres. Sur ce type de support, les signaux transmis sont complétement insensibles aux rayonnements électromagnétiques, ne subissant ainsi aucune altération. Un câble à fibre optiques peut acheminer simultanément plusieurs milliers de messages. La fibre optique permet de très grandes vitesses sur de grandes distances (150 mégabits par seconde (Mbits/s) sur une dizaine de kilomètres. Grâce à de telles vitesses, il devient possible de transmettre en temps réel de sons, et même des images animées. Ce support est encore d'un coût élevé.

Une fibre optique est composée de substances (en silice, quartz fondu ou plastique) d'indices de réfraction différents :

- **Le cœur** dans lequel se les ondes propagent (diamètre 10, 50 ou 62,5 microns).
- **La gaine**, en général, dans les mêmes matériaux que le cœur mais avec des additifs qui confine les ondes optiques dans le cœur.
- **Le revêtement de protection**, généralement en plastique, qui assure la protection mécanique de la fibre.

Une fibre optique est basée sur le principe de la réflexion totale d'une onde lumineuse. Le cœur confine la plus grande partie de l'énergie lumineuse transportée tandis que la gaine, d'indice plus faible, se charge de réfléchir le rayon circulant dans le cœur.

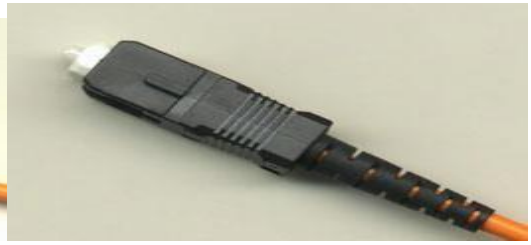
Le phénomène de réflexion totale permet aux rayons d'incidence se propager à l'intérieur du noyau ; à chaque réflexion, il n'y a aucune perte de puissance.

Les fibres sont, ensuite, assemblées en câbles regroupant plusieurs fibres (de 2 à 40 fibres par câble).

La distinction entre fibre **monomode** et **multi mode** concerne les modes de propagation de la lumière dans la fibre, unique pour la fibre monomode (cœur de diamètre très petit, 10 microns environ), multiple pour la fibre multi mode. Dans le cas d'une fibre multi mode, plusieurs longueurs d'onde lumineuse traverse la fibre, pour une fibre monomode au contraire, une seule longueur d'onde est utilisée ce qui supprime les problèmes d'interférences.

Pour relier la fibre optique aux éléments du réseau, on utilise principalement 3 sortes de prises : ST, SC ou LC.

ST



SC

Tableau récapitulatif des normes de câblage.

Type de câble	Connectique	Dénomination uselle	Longueur maximale	Distance entre 2 points
Paire torsadée	RJ45	10 base T	100 m	X
Coaxial épais	AUI	10 base 5	500 m	2.5 m
Coaxial fin	BNC	10 base 2	185 m	0.5 m
Fibre optique*	ST	X	de 2 à 10 KM	de 2 à 10 KM

*en fonction du mode mono ou multi.

3.1.4 Le sans-fil (802.11x)

Il existe différentes technologies et normes sans fil dans lesquelles les communications couvrent des zones de couverture plus petites ou plus grandes.

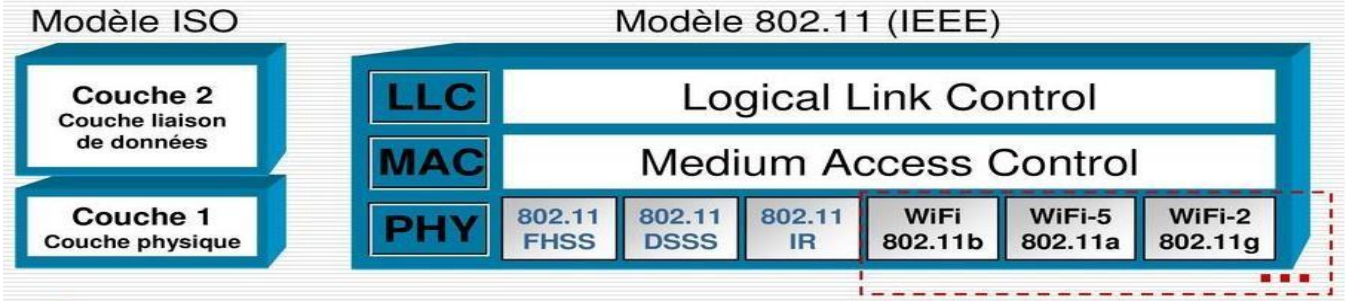
Les technologies sans fil incluent le cellulaire, Bluetooth et Zigbee.

Toutes ces différentes technologies sans fil peuvent être organisées dans les quatre principales topologies sans fil :

- ✓ Réseau étendu sans fil (WWAN)
- ✓ Réseau métropolitain sans fil (WMAN)
- ✓ Réseau personnel sans fil (WPAN)
- ✓ Réseau local sans fil (WLAN)

La norme 802.11 d'originale a été publiée en juin 1997, et elle est souvent appelée 802.11 Prime car c'était la première norme WLAN.

L'IEEE définit spécifiquement les technologies 802.11 au niveau de la couche physique et la sous-couche MAC de la couche liaison de données.



4 Le modèle de référence

4.1 Normalisation

L'établissement de normes permet d'avoir une structure homogène pour faire communiquer différents équipements. La conformité à une norme garantit la satisfaction de règles précises.

Ainsi, des matériels différents, fabriqués par diverses entreprises, peuvent communiquer car la norme offre un cadre compatible entre ces entités hétérogènes.

La normalisation est effectuée par des organismes compétents au sein desquels les différents acteurs du domaine sont représentés. Trois organismes internationaux sont concernés par la normalisation dans le domaine des réseaux :

UIT (Union Internationale des Télécommunications) est l'institution spécialisée dans le domaine des télécommunications.

IEC (International Electrotechnic Commission), fondée en 1906, est chargée de coordonner et d'unifier les normes dans le domaine de l'électricité.

ISO (International Standards Organisation) est une organisation privée chargée de la normalisation dans tous les domaines sauf l'électricité et l'électronique.

Ces organismes regroupent des représentants d'organismes nationaux. En France, les normes sont gérées par l'AFNOR (Association Française de NORmalisation).

4.2 Modèle de référence OSI

Le modèle de référence défini par l'ISO est l'OSI (Open System Interconnection). Il permet à des systèmes hétérogènes de s'interconnecter et d'échanger des informations. Il est par conséquent indépendant de la structure et de la technologie des matériels employés.

La complexité de conception, de réalisation et de maintenance des logiciels et de l'architecture des réseaux, est maîtrisée grâce à une organisation en couches, chaque couche étant bâtie sur la précédente.

4.2.1 Principes de la structuration en couches

Le modèle OSI est composé de sept couches.

Chaque couche peut interagir uniquement avec les deux couches adjacentes.

Une couche N est constituée d'un ensemble d'entités formant un sous-système de niveau N.

Elle ne peut dialoguer qu'avec une couche de même niveau N sur une autre machine. Les communications se font donc entre entités homologues. La communication entre deux entités homologues de niveau N obéit à un ensemble de règles et formats, syntaxiques et sémantiques, prédéfinis pour les entités de niveau N. Ces règles et formats définissent le protocole de niveau N.

Une couche de niveau N fournit des services pour la couche de niveau N + 1. La couche de niveau N + 1 communique à la couche N les caractéristiques du service attendu. Les services fournis par une couche N sont identifiés par des SAP (Service Access Point) ou ports.

4.2.2 Couches du modèle OSI

Les sept couches sont organisées comme indiqué dans le Tableau ci-dessous : Chaque couche a un rôle spécifique :

Modèle OSI

	Type de Donnée	Couche	Fonction
Couches Hautes	Donnée	7. Application	Point d'accès aux services réseaux
		6. Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitable par n'importe quelle autre machine
		5. Session	Communication Interhost, gère les sessions entre les différentes applications
	Segments	4. Transport	Connexions bout à bout, connectabilité et contrôle de flux
Couches Matérielles	Paquet/Datagramme	3. Réseau	Détermine le parcours des données et l'adressage logique
	Trame	2. Liaison	Adressage physique
	Bit	1. Physique	Transmission des signaux sous forme binaire

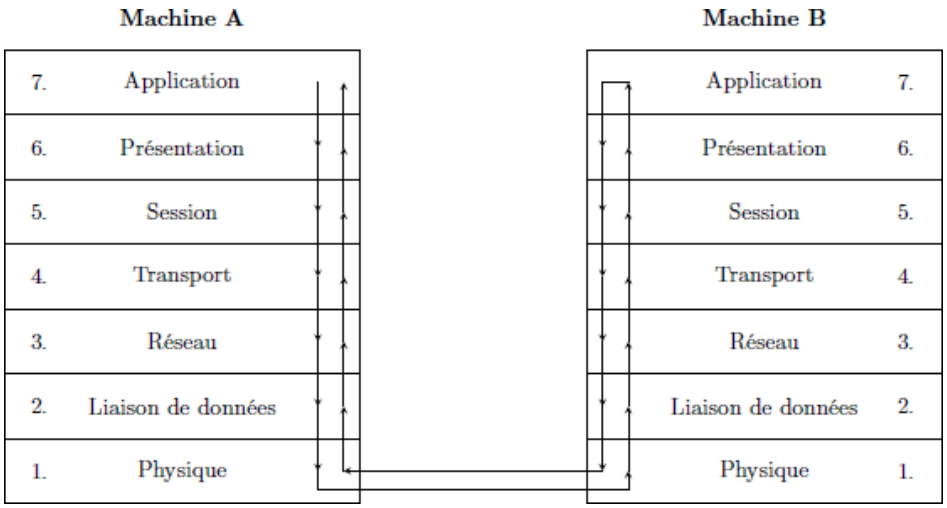
4.2.3 Interactions entre couches

4.2.3.1 Protocoles et Services

Les notions de protocole et de service sont fondamentales.

- **Un protocole** est un ensemble de règles et formats, syntaxiques et sémantiques prédéfinis pour les entités d'un même niveau N de deux machines différentes.
- **Un service** est fourni par une couche de niveau N à la couche de niveau N + 1 d'une même machine.

La Figure ci-dessous décrit la communication entre les 7 niveaux de couches de deux entités communicantes A et B.



4.2.3.2 Encapsulation

L'encapsulation, en informatique et spécifiquement pour les réseaux informatiques, est un procédé consistant à inclure les données d'un protocole dans un autre protocole.

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. À chaque couche, une information est ajoutée au paquet de données, il s'agit d'un entête, ensemble d'informations qui garantit la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'en-tête est lu, puis supprimé. Ainsi à la réception, le message est dans son état originel.

À chaque niveau, le paquet de données change d'aspect, car on lui ajoute un en-tête, ainsi les appellations changent suivant les couches :

- Le paquet de données est appelé **message** au niveau de la couche application
- Le message est ensuite encapsulé sous forme de **segment** dans la couchetransport
- Le segment une fois encapsulé prend le nom de **paquet** dans la couche réseau
- Enfin on parle de **trame** au niveau de la couche liaison
- Et de **signal** au niveau de la couche physique

4.2.3.3 PDU et SDU

Les messages échangés par un protocole de niveau N sont appelés des PDU_N (Protocol Data Unit de niveau N).

Les messages échangés entre la couche N et la couche inférieure N - 1 sont appelés des

SDU_{N-1} (Service Data Unit de niveau N - 1).

De plus, un protocole de niveau N ajoute au SDUN qu'il a reçu des informations de contrôle visant à contrôler la bonne exécution du protocole. Ces informations de contrôle sont appelées PCIN (Protocol Control Information de niveau N).

On a par conséquent :

$PDN_N = SDN_N + PCI_N$

$SDN_N = PDN_{N+1}$

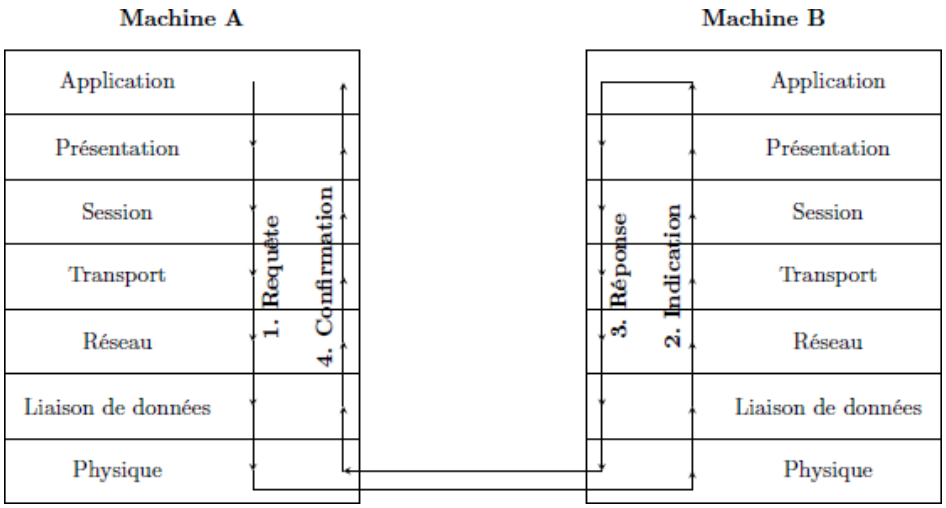
On dit alors que le PDN_N encapsule le SDU_N.

Au lieu d'indexer le PDU ou le SDU par le numéro de la couche, on le fait souvent précéder de la première lettre du nom de la couche (en anglais). Par exemple, NPDU = PDU_3, où le N indique la couche réseau (network).

4.2.3.4 Primitives de service

Il existe 4 primitives de service : requête, indication, réponse et confirmation.

Une requête est initialement envoyée par la couche N à la couche N - 1 d'une même entité. Ensuite, une indication est transmise de la couche N - 1 à la couche N de l'autre entité communicante. La réponse est envoyée par la couche N à la couche N - 1 de cette seconde entité. Enfin, une confirmation est transmise de la couche N - 1 à la couche N de l'entité ayant émis la requête. Ceci est illustré dans la Figure ci-dessous :



4.2.3.5 Types de connexion

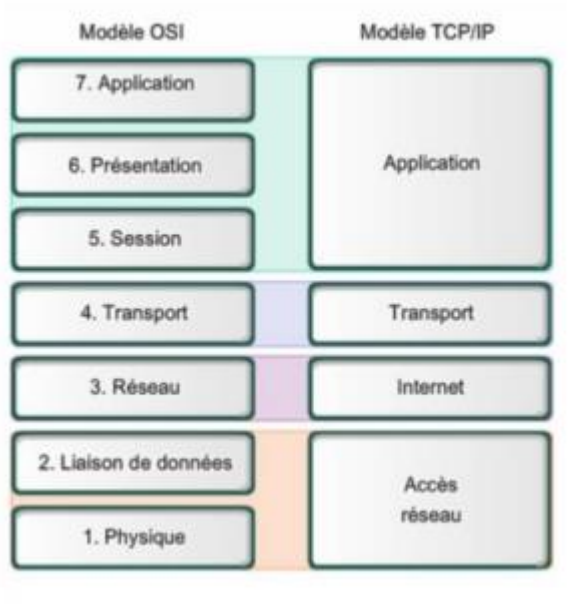
La communication entre entités homologues de même niveau passe par l'établissement d'une connexion. Ce peut être une connexion point à point qui associe exactement deux entités, ou une connexion multipoints qui en associe plus.

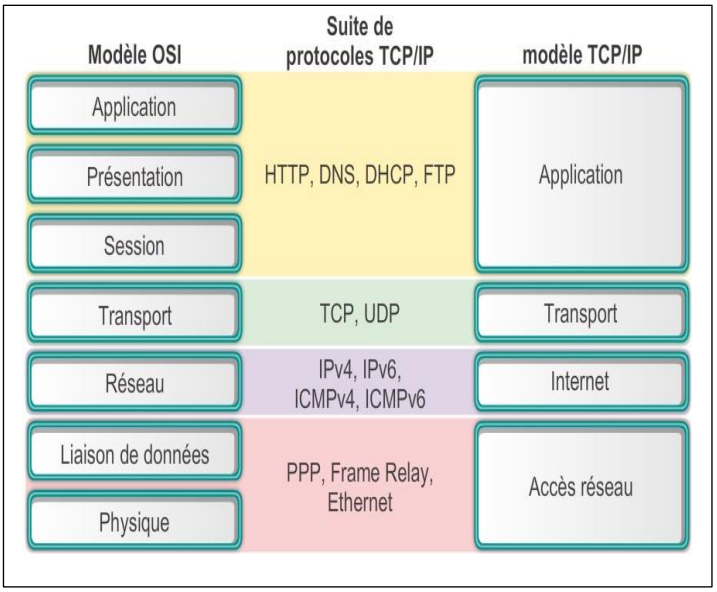
Les modes de communication sont simplex, c'est-à-dire dans un seul sens, ou duplex, dans les deux sens.

Enfin, les protocoles peuvent opérer en mode connecté ou en mode déconnecté. En mode connecté, l'établissement de la connexion comporte trois phases : connexion, transfert, et déconnexion. Le contexte de la communication est préservé. Par contre, en mode déconnecté, seule la phase de transfert a lieu, et la communication s'effectue sans mémoire.

4.3 Modèle TCP/IP

Le modèle TCP/IP n'est pas vraiment éloigné du modèle OSI. Il ne présente cependant que 4 couches.





4.3.1 La couche hôte réseau

Elle est en fait composée de deux couches : Physique et Liaison

La couche physique décrit les caractéristiques physiques de la connexion : câbles, ondes…

La couche liaison spécifie le moyen utilisé pour acheminer les données sur la couche physique : Câble Ethernet, Wi fi.

4.3.2 La couche internet

Son rôle est l'injection de paquets dans n'importe quel réseau. Lorsque deux terminaux communiquent entre eux via ce protocole, aucun chemin pour le transfert des données n'est établi à l'avance : il est dit que le protocole est « non orienté connexion ». Ainsi les paquets envoyés peuvent arriver dans le désordre car ils n'auront pas suivi la même route. C'est le protocole transport qui se chargera de remettre les paquets dans le bon ordre.

4.3.3 La couche transport

Son rôle est similaire à celui de la couche transport du modèle OSI. Les protocoles utilisés à ce niveau sont TCP et UDP.

TCP est fiable, acheminant sans erreur les paquets à destination, utilisant des services d'acquittement, de gestion du temps d'attente…

UDP est non fiable mais plus rapide. Il est utilisé dans les liaisons voix IP, où l'on préfère perdre quelques données qu'attendre. Utilisé aussi pour le streaming ou la vidéo conférence.

Dans l'entête TCP, on retrouve le code du port source et du port destination. Par exemple 80 pour http.

4.3.4 La couche application

Le Modèle TCP/IP est fondé sur le constat que les logiciels réseaux n'utilisent que très peu, ou pas, les couches session et présentation. Cette couche regroupe toute les protocoles de haut niveau (FTP, SMTP, HTTP, DNS…). Cette couche devra choisir un protocole de transport adapté au service demandé

5 Couche Liaison : Ethernet (IEEE 802.3).

La couche liaison : Son rôle est un rôle de « liant » : elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau.

- Fractionne les données en trame
- Transmet ces trames
- Gère les acquittements envoyés à l'émetteur
- Détection et correction dans les informations reçues de la couche physique
- Contrôle de flux pour éviter un trop grand afflux de données.
- Elle s'assure que deux ou plusieurs nœuds n'essaient pas de transmettre des données sur le canal (partagé) de transmission en même temps.

5.1 Réseau local

Support de transmission partagé par plusieurs équipements (en général) : réseau à diffusion.

Un nœud peut vouloir envoyer à une (unicast), plusieurs (multicast) ou tous les nœuds (Broadcast)

Un nœud peut vouloir émettre à tout moment, si support partagé, alors il faut :

- Une manière d'identifier chaque nœud : des adresses (au niveau de la couche Liaison _ @ MAC)
- Des règles pour gérer le « droit de parole » : méthodes d'accès au support

5.2 L'adresse MAC

Chaque machine est identifiée par une clé globalement unique, appelée adresse MAC, pour s'assurer que toutes les machines (plus précisément interfaces Ethernet) sur un réseau Ethernet ont des adresses distinctes. Une adresse MAC est une adresse matérielle, c'est-à-dire une adresse unique stockée sur une mémoire morte (ROM de la carte réseau.

Les adresses MAC comportent 48 bits (6 octets) et sont exprimées sous la forme de 12 chiffres hexadécimaux :

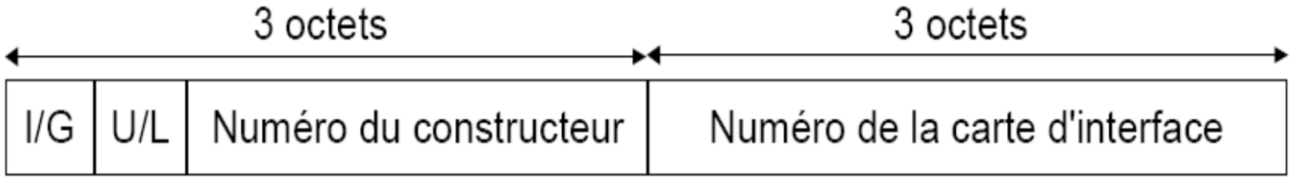
- ✓ 6 chiffres sont administrés par l'IEEE et identifient le fabricant de la carte
- ✓ 6 chiffres forment le numéro de série de la carte

Les LANs de type Ethernet et 802.3 sont des réseaux dits de broadcast, ce qui signifie que tous les hôtes voient toutes les trames. L'adressage MAC est donc un élément important afin de pouvoir déterminer les émetteurs et les destinataires en lisant les trames.

Exemple : 00-00-0c-12-34-56

Ces 48 bits sont répartis de la façon suivante :

- 1 bit I/G : indique si l'adresse est individuelle, auquel cas le bit sera à 0 (pour une machine unique, unicast) ou de groupe (multicast ou broadcast), en passant le bit à 1 ;
- 1 bit U/L : indique si l'adresse est universelle (conforme au format de l'IEEE) ou locale, 1 pour une adresse administrée localement ;
- 22 bits réservés : tous les bits sont à zéro pour une adresse locale, sinon ils contiennent l'adresse du constructeur ;
- 24 bits : adresse unique (pour différencier les différentes cartes réseaux d'un même constructeur).



Adresses de groupe (bit I/G à 1)

Adresse(s) MAC	Type	Description
FF-FF-FF-FF-FF-FF	*Broadcast*	Diffusion généralisée
01-00-5E-00-00-00 à 01-00-5E-7F-FF-FF	*Internet multicast* (RFC 1112)	Diffusion restreinte

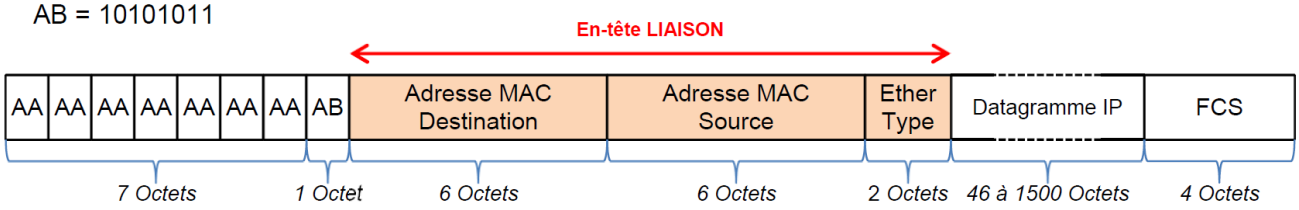
Code fabricant (OUI) sur 3 octets, en hexadécimal	Vendeur / fabricant
00 - 00 - 0C	Cisco
00 – 03 – 93	Apple
02 – 80 - 8C	3Com
08 – 00 – 20	Sun
08 – 00 - 5A	IBM

5.3 Notion de trame Ethernet

L'information numérique qui chemine sur un réseau TCP/IP est une succession de bits appelé **Trame Ethernet**. Cette trame Ethernet contient des informations nécessaires pour joindre l'hôte H2 depuis l'hôte H1.

Format de la trame Ethernet

AA = 10101010
AB = 10101011



Préambule : (7 octets) Annonce le début de la trame et permet aux récepteurs de se synchroniser. Il contient 8 octets dont la valeur est 10101010 (on alterne des 1 et des 0)
SFD : (1 octets) "Starting Frame Delimiter". Il s'agit d'un octet à la valeur 0xAB. Il doit être reçu en entier pour Valider le début de la trame.
En-tête : (14 octets)

- Adresse MAC du destinataire (6 octets) Adresse MAC de l'interface (carte d'accès) Ethernet destinataire de la-. Une seule trame peut avoir plusieurs destinataires. En effet, le format des adresses MAC permet de coder 3 types de destinations :
  - ✓ Unicast : (monodiffusion) un destinataire unique (celui qui possède cette adresse MAC) ;
  - ✓ Multicast : (multidiffusion) un groupe d'interfaces est destinataire.
  - ✓ Broadcast : (diffusion générale) c'est l'adresse **ff : ff : ff : ff : ff : ff** . Elle correspond à toutes les interfaces Ethernet actives sur un réseau Ethernet (tous les équipements se reconnaissent dans cette adresse).
- Adresse MAC de l'émetteur (6 octets) Adresse MAC de la carte Ethernet émettrice de la trame. C'est forcément une adresse unicast.
- EtherType (Type de protocole) (2 octets) Indique quel protocole est concerné par le message.

Exemples de valeurs du champ EtherType

EtherType	Protocole
0x0800	IPv4
0x0806	ARP
0x809B	AppleTalk
0x8035	RARP
0x86DD	IPv6

Données (Datagramme IP) : (46 à 1500 octets)
Données véhiculées par la trame.
Sur la station destinataire de la trame, ces octets seront communiqués à l'entité (protocole) indiquée par le champ **EtherType**.

FCS : (4 octets) Frame Check Sequence.
Ensemble d'octets permettant de vérifier que la réception s'est effectuée sans erreur.

6 La couche réseau

6.1 Présentation de la couche réseau

La couche réseau est chargée de transporter les paquets de la source vers la destination à travers une succession de connexions physiques.
Pour atteindre la destination, il est nécessaire d'effectuer de nombreux sauts de nœud intermédiaire en nœud intermédiaire. Cette fonction est très différente de celle de la couche liaison de données, qui a le rôle de transférer des trames d'un bout à l'autre d'un câble. Cependant, la couche réseau doit être capable de choisir des chemins appropriés à travers le réseau. Les principaux services fournis par cette couche sont :

- Encapsulation/décapsulation
- Adressage
- Routage des paquets

6.2 Principe de routage

Pour transférer un paquet à travers un réseau, il est nécessaire de déterminer quel itinéraire il va suivre (fonction routage), puis à chaque système intermédiaire du réseau d'aiguiller et de retransmettre ce paquet sur une liaison de données convenable (fonction acheminement).

Un système intermédiaire est un nœud de réseau possédant des fonctions de routage et de transmission des paquets en provenance des systèmes terminaux. Un système intermédiaire est souvent appelé un **routeur**. Un système terminal (appelé aussi hôte) est un système qui émet et reçoit des paquets, par exemple un ordinateur de bureau.

Les routes sont consignées dans les **tables de routage**, incluses dans chaque système intermédiaire, mais aussi souvent dans les systèmes terminaux. Dans ces tables sont indiquées, pour chaque destination, le prochain nœud à atteindre (nœud voisin).

Ces tables de routage sont calculées par des **algorithmes de routage** exécutés périodiquement dans les routeurs à partir d'informations sur l'état du réseau observé par le routeur lui-même ou transmises par les autres routeurs en utilisant les protocoles de routage.

Les protocoles de routage sont des protocoles de communication qui permettent aux systèmes terminaux (End Systems (ES)) et intermédiaires (Intermediate Systems (IS) de s'échanger des informations en vue de déterminer les meilleures routes pour les paquets. Ces informations permettent aussi aux ES et IS de découvrir dynamiquement leurs existences réciproques et leur disponibilité (signalisation de présence et de disponibilité). Ces informations sont utilisées par les algorithmes de routage pour calculer les tables de routage.

Les algorithmes de routage permettent de calculer un chemin optimisé, c'est à dire offrant la plus courte "distance", entre deux nœuds d'un réseau. Ils sous-entendent donc une "métrique" pour évaluer les "distances" et un algorithme d'optimisation. Cette "distance" peut être évaluée par le nombre de nœuds traversés, le temps de transit, le coût, la sécurité, etc. Les informations permettant de la calculer sont transmises par les protocoles de routage.

6.3 Type de routage

6.3.1 Routage statique

Routage statique (ou fixe) (prédéterminé, non adaptatif) : les informations sont mises à jour manuellement par l'administrateur (lors de la configuration ou de changements topologiques)

- ✓ Pas de solution de secours en cas de rupture d'un lien,

- ✓ Convient uniquement pour les réseaux de taille modeste.

6.3.2 Routage dynamique

Routage dynamique (adaptatif, évolutif) : utilise des protocoles de routage afin de maintenir la cohérence des informations associées aux routes, son rôle n'est pas de router ; ce rôle revient à l'algorithme mis en place par le protocole retenu.

- ✓ Indispensable dès que la topologie devient complexe

6.4 Adressage

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 qui supportent la couche réseau utilisent un système d'adressage hiérarchique qui garantit l'unicité des adresses au-delà des limites du réseau, ainsi qu'une méthode de sélection du chemin d'acheminement des données entre les réseaux.

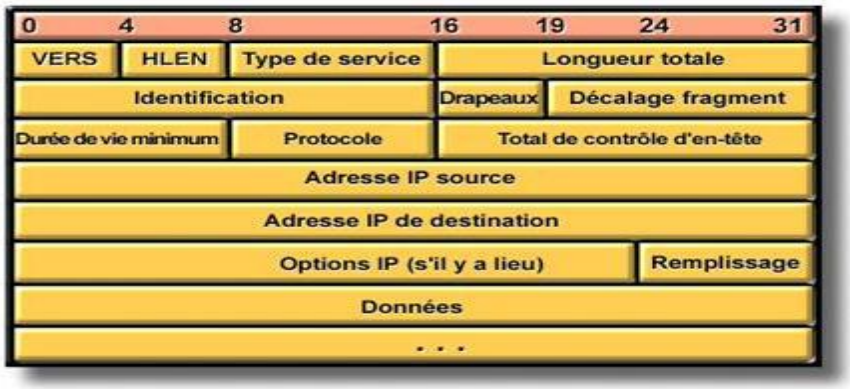
L'adressage hiérarchique permet aux données de circuler dans des réseaux multiples et de trouver leur destination de manière efficace. Le système téléphonique est un exemple de système d'adressage hiérarchique. Le système téléphonique utilise un indicatif régional pour diriger un appel vers son premier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

6.5 Le protocole IP

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, elles sont encapsulées au niveau de chaque couche. Au niveau de 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 les informations d'adressage et de contrôle), mais ne se préoccupe pas des données proprement dites. Il accepte tout ce qui provient des couches supérieures.

L'entête IP est composé de champs :



•**Le champ Version** Sur 4 bits, il indique le numéro de version du protocole IP utilisé (généralement 4).

•**Le champ Header** (longueur d'entête) Sur 4 bits, il indique la longueur de l'entête en nombre de motsde 32 bits (4 octets).

Le champ Type de service Il est sur 8 bits :

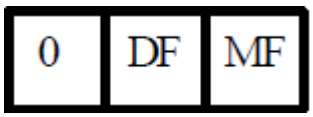
-4 bits "priorité » : D : délai court, T : haut débit R : fiabilité élevée : Coût faible.

- 4 bits "service » : Telnet= 1000, FTP contrôle = 1000FTP data = 0100, SNMP = 0010.

Le champ Longueur total Sur 16 bits, il est exprimé en octets. Il est découpé en segments le datagramme à une longueur supérieure à la taille maximum. L'indication de la longueur totale permet de distinguer le bourrage dans une trame Ethernet.

Le champ Identification Sur 16 bits, il permet d'identifier un datagramme en cas de fragmentation (il est recopié dans chaque segment)

Le champ Flags (drapeaux) Sur 3 bits :



-DF (Don't Fragment), vaut 1 si la trame n'est pas fragmentée.

-MF (More Fragment), vaut 1 si la trame a été fragmentée, et si ce fragment n'est pas le dernier.

Le champ position du fragment Sur 13 bits, Il est utilisé pour la reconstructions de trame IP ayant dû être fragmentées lors de la traversée de certains supports Cette valeur indique la position relative, en multiples de 8 octets, de ce fragment de trame dans la trame initiale. Ce compteur est également utilisé pour la reconstruction des trames fragmentées sur la machine réceptrice, il est décrémenté à chaque seconde tant que l'ensemble des fragments constituant la trame originelle n'est pas arrivé.

Le champ Duré de vie Sur 8 bits, Il indique une durée de vie, en secondes, de la trame. Celle-ci doit être détruite lorsque ce champ devient nul. Toute traversée d'un nœud se traduit, en pratique, par une simple décrémentation de ce champ.

Le champ Protocole Sur 8 bits, il indique les protocoles utilisés au niveau supérieur :

-ICMP = 1,
-TCP = 6,
-UDP = 17.

Le champ Somme de contrôle d'entête Sur 16 bits, c'est un CRC recalculé par chaque routeur avant la retransmission. Il permet de détecter les incohérences de l'entête et les erreurs de transmissions possible. Les données ne sont pas prises en compte.

Le champ Adresse source et destination Chacune sur 4 octets, ils indiquent les adresses IP.

Le champ Option De longueur variable, il peut être nul, avec bourrage pour obtenir un multiple de 32 bits.

6.6 Adresse IP

Sur Internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées **adresses IP**, composées de 4 nombres entiers (4 octets) entre 0 et 255 et notées sous la forme xxx.xxx.xxx.xxx. Par exemple, 194.153.205.26 est une adresse IP donnée sous une forme technique.

6.7 Types d'adresses

Dans la plage d'adresses de chaque réseau, il y a trois types d'adresse :

- **L'adresse réseau** : l'adresse qui fait référence au réseau
- **L'adresse de diffusion** : une adresse spécifique, utilisée pour envoyer les données à tous les hôtes du réseau
- **Des adresses d'hôte** : des adresses attribuées aux périphériques finaux sur le réseau

L'adresse réseau : l'adresse réseau est généralement utilisée pour faire référence à un réseau. Par exemple, le « réseau 10.0.0.0 ». C'est un moyen plus pratique et plus représentatif d'identifier le réseau que d'employer un terme du type « le premier réseau ». Tous les hôtes du réseau 10.0.0.0 ont les mêmes bits réseau.

Dans la plage d'adresses IPv4 d'un réseau, la plus petite adresse est réservée à l'adresse réseau. Dans la partie hôte, cette adresse comporte un 0 pour chaque bit d'hôte.

Adresse de diffusion : l'adresse de diffusion IPv4 est une adresse spécifique, attribuée à chaque réseau. Elle permet de transmettre des données à l'ensemble des hôtes d'un réseau. Pour cela, un hôte peut envoyer un seul paquet adressé à l'adresse de diffusion du réseau.

L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau. Il s'agit de l'adresse dans laquelle les bits de la partie hôte sont tous des « 1 ». Pour le réseau 10.0.0.0 avec 24 bits réseau, l'adresse de diffusion serait 10.0.0.255. Cette adresse est également désignée sous le nom de diffusion dirigée.

Adresses d'hôte : chaque périphérique final nécessite une adresse unique pour remettre un paquet à un hôte. Dans les adresses IP, nous attribuons les valeurs situées entre l'adresse réseau et l'adresse de diffusion aux périphériques de ce réseau.

6.8 Les classes de réseaux

Les adresses IP sont réparties en classes, selon le nombre d'octets qui représentent le réseau. Le but de la division des adresses IP en trois classes A, B et C est de faciliter la recherche d'un ordinateur sur le réseau. En effet avec cette notation il est possible de rechercher dans un premier temps le réseau que l'on désire atteindre puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau.

Classe A :

Dans une adresse IP de classe A, le premier octet représente le réseau. Le bit de poids fort (le premier bit, celui de gauche) est à zéro, ce qui signifie qu'il y a 27 (00000000 à 01111111) possibilités de réseaux, soit 128 possibilités. Toutefois, le réseau 0 (bits valant 00000000) n'existe pas et le nombre 127 est réservé pour désigner votre machine.
Les réseaux disponibles en classe A sont donc les réseaux allant de **1.0.0.0** à **126.0.0.0** (les derniers octets sont des zéros ce qui indique qu'il s'agit bien de réseaux et non d'ordinateurs !)
Les trois octets de droite représentent les ordinateurs du réseau, le réseau peut donc contenir un nombre d'ordinateur égal à : 2^{24}-2 = 16777214 ordinateurs.

Une adresse IP de classe A, en binaire, ressemble à ceci :

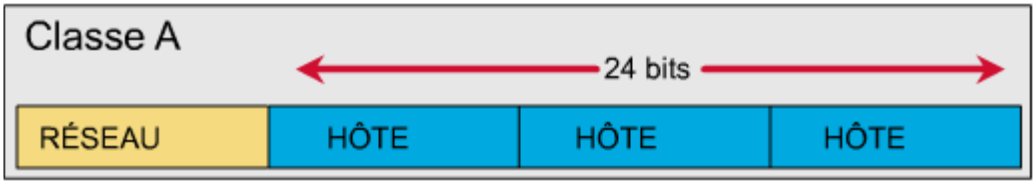


Figure 1 : Représentation de classe A

Classe B

Dans une adresse IP de classe B, les deux premiers octets représentent le réseau.

Les deux premiers bits sont 1 et 0, ce qui signifie qu'il y a 214 (10 000000 00000000 à 10 11111111111111) possibilités de réseaux, soit 16384 réseaux possibles. Les réseaux disponibles en classe B sont donc les réseaux allant de **128.0.0.0** à **191.255.0.0**

Les deux octets de droite représentent les ordinateurs du réseau. Le réseau peut donc contenir un nombre d'ordinateurs égal à : 2^{16}-2 = 65534 ordinateurs.

Une adresse IP de classe B, en binaire, ressemble à ceci :

Figure 2 : Représentation de classe B

Classe C

Dans une adresse IP de classe C, les trois premiers octets représentent le réseau. Les trois premiers bits sont 1,1 et 0, ce qui signifie qu'il y a 221 possibilités de réseaux, c'est-à-dire 2097152. Les réseaux disponibles en classe C sont donc les réseaux allant de **192.0.0.0** à **223.255.255.0** L'octet de droite représente les ordinateurs du réseau, le réseau peut donc contenir : 2^{8}-2 = 254 ordinateurs.

Une adresse IP de classe C, en binaire, ressemble à ceci :

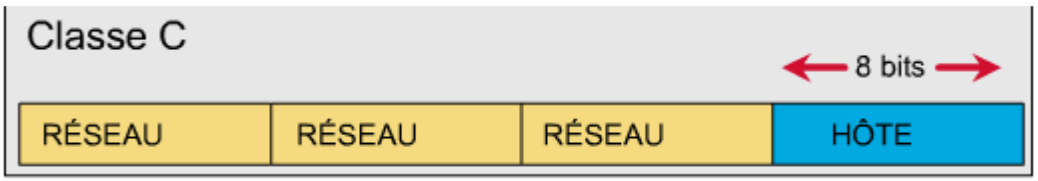


Figure 3 : Représentation de classe C

6.9 Le masque de sous réseaux

Un masque est une adresse codée sur 4 octets, soit 32 bits, Il permet de faire la séparation entre la partie réseau et la partie machine de l'adresse IP : - La partie réseau est représentée par des bits à 1, et la partie machine par des bits à 0, le masque ne représente rien sans l'adresse IP à laquelle il est associé.

Classe	*Adresse IP*	*masque*
A	N.H.H.H	255.0.0.0
B	N.N.H.H	255.255.0.0
C	N.N.N.H	255.255.255.0

6.10 Les cous réseaux

6.10.1 Définition

Les administrateurs réseau doivent parfois diviser les réseaux, notamment les réseaux de grande taille, en réseaux plus petits. Appelés sous-réseaux, ces entités assurent une souplesse accrue au niveau de l'adressage.

Le réseau postal marocain se décompose en un premier sous réseau : les régions, chaque région se décompose elle-même en un sous réseau : les villes etc…

Cette décomposition permet de structurer le réseau. Il en est de même pour les réseaux informatiques, au même titre que l'adresse postale, l'adresse IP contient le ou les sous réseaux auxquels elle appartient.

6.10.2 Principe général

S'il est évident, sur une adresse postale, de savoir à quel réseau ou sous réseau appartient cette adresse, ça l'est beaucoup moins avec une adresse IP du type 195.52.150.12 ! Une adresse IP est toujours associée à un masque de sous réseau, c'est grâce à celui-ci que l'on pourra extraire de l'adresse IP, le numéro de la machine et le sous réseau auquel elle appartient.

Par défaut, lorsqu'il n'y a pas de sous réseaux, les masques sont :

- En classe A : 255.0.0.0
- En classe B : 255.255.0.0
- En classe C : 255.255.255.0

Pour déterminer l'identifiant réseau d'une adresse IP, on effectue l'opération logique suivante :

Adresse réseau = Adresse IP **ET** Masque

Exemple :

L'adresse IP 195.52.150.12, adresse de classe C, a donc pour masque 255.255.255.0, son identifiant réseau sera donc :

192.52.150.12 s'écrit en binaire : 11000011.00110100.10010110.00001100

255.255.255.0 s'écrit en binaire : 11111111.11111111.11111111.00000000

On effectue un **ET** logique on obtient : 11000011.00110100.10010110.00000000

L'identifiant réseau (adresse réseau) de l'adresse IP **195.52.150.12** est donc **195.168.150.0**

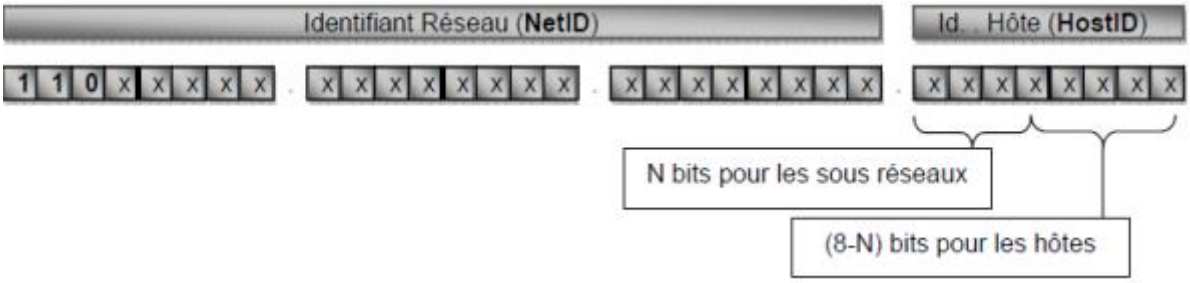
L'adresse d'un réseau est toujours indiquée en mettant à 0 l'adresse des hôtes, par exemple :

- En classe B : 150.80.**0.0**
- En classe C : 200.90.23.**0**

6.10.3 Création des sous réseaux

a. Principe

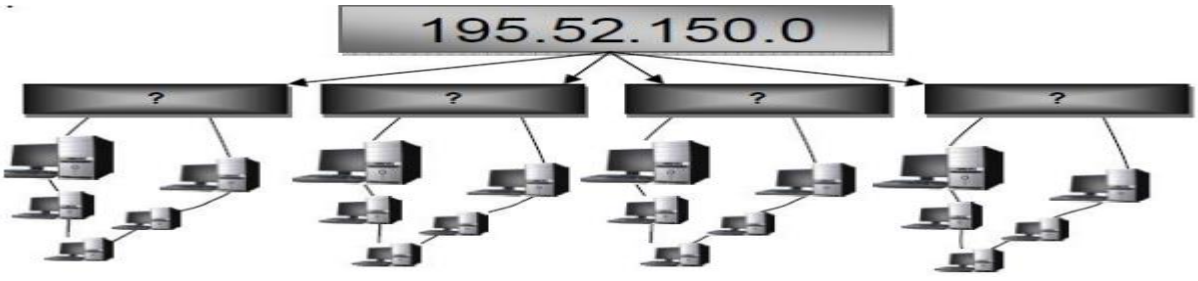
On utilise une partie des bits réservés à l'identification des hôtes afin de créer des sous réseaux, par exemple, pour une adresse de classe C, les 3 premiers octets identifient le réseau, il reste donc le dernier octet, c'est-à-dire 8 bits pour la création de sous réseaux et l'identification des hôtes dans ces sous réseaux.



Reste à déterminer combien de bits (N) seront nécessaires pour la création des sous réseaux.
A noter que la norme RFC 1878 interdit les sous réseaux tout à 1 (réservé au broadcast), c'est-à-dire que si N=3, le sous réseau <111> est interdit.

b. Exemple

On dispose d'une adresse réseau de classe C : 195.52.150.0 et on désire la découper en 5 sous réseaux :



Si l'on choisit 1 bit (N=1) pour les sous réseaux :

- On dispose de 2 possibilités : « **0** » et « **1** »

- Le « « 1 » seul est interdit (selon la RFC 1878), il reste donc un seul sous réseau possible, ce qui est donc sans intérêt !

Si l'on choisit 2 bit (N=2) pour les sous réseaux :

- On dispose de 2^2=4 possibilités : « **00** », « **01** », « **10** » et « **11** »
- La combinaison «11 » est interdite (selon la RFC 1878), on peut créer 3 sous réseaux, insuffisant dans notre cas.

Si l'on choisit 3 bit (N=3) pour les sous réseaux :

- On dispose de 2^3=8 possibilités : « **000** » à « **111** »
- La combinaison «111 » est interdite (selon la RFC 1878), on peut créer 8-1=7 sous réseaux, ce qui nous convient.

Nous devrons donc réserver les 3 bites de poids fort du champ identifiant hôte (machine) de l'adresse 195.152.150.0 pour nos sous réseaux. Les adresses de sous-réseaux utilisables seront donc :

Sous réseau 0 (« 000 ») : 11000011.00110100.10010110.**000**00000 soit 195.52.150.**0**
Sous réseau 1 (« 001 ») : 11000011.00110100.10010110.**001**00000 soit 195.52.150.**32**
Sous réseau 2 (« 010 ») : 11000011.00110100.10010110.**010**00000 soit 195.52.150.**64**
Sous réseau 3 (« 011 ») : 11000011.00110100.10010110.**011**00000 soit 195.52.150.**96**
Sous réseau 4 (« 100 ») : 11000011.00110100.10010110.**100**00000 soit 195.52.150.**128**
Sous réseau 5 (« 101 ») : 11000011.00110100.10010110.**101**00000 soit 195.52.150.**160**
Sous réseau 6 (« 110 ») : 11000011.00110100.10010110.**110**00000 soit 195.52.150.**192**

Dans notre cas nous, nous n'avons besoin que de 5 sous réseaux, nous utiliserons donc les sous-réseaux de 0 à 4.

Quelles sont les adresses des hôtes pour chaque sous réseau ?

Prenons le sous réseau **0** : 195.52.150.**0** et intéressons-nous au 4ème octet (**000**00000) :

- Les adresses **000**00000 (adresse sous réseau) et **000**11111 (adresse de diffusion = broadcast) ne peuvent être attribuées à un hôte.
- Le 1èr hôte aura pour adresse **000**00001, et aura donc l'adresse IP 195.52.150.**1**
- Le 2ème hôte aura pour adresse **000**00010, et aura donc l'adresse IP 195.52.150.**2**
- Le 3ème hôte aura pour adresse **000**00011, et aura donc l'adresse IP 195.52.150.**3**
- Etc……
- Le dernier hôte aura pour adresse **000**11110, et aura donc l'adresse IP 195.52.150.**30**

Prenons le sous réseau **1** : 195.52.150.**32** et intéressons-nous au 4ème octet (**001**00000) :

- Les adresses **00**010000 (adresse sous réseau) et **001**11111 (adresse de diffusion = broadcast) ne peuvent être attribuées à un hôte.
- Le 1èr hôte aura pour adresse **001**00001, et aura donc l'adresse IP 195.52.150.**33**
- Le 2ème hôte aura pour adresse **001**00010, et aura donc l'adresse IP 195.52.150.**34**
- Le 3ème hôte aura pour adresse **001**00011, et aura donc l'adresse IP 195.52.150.**35**
- Etc……
- Le dernier hôte aura pour adresse **001**11110, et aura donc l'adresse IP 195.52.150.**62**

Prenons le sous réseau **2** : 195.52.150.**64** et intéressons-nous au 4ème octet (**010**00000) :

- Les adresses **010**00000 (adresse sous réseau) et **010**11111 (adresse de diffusion = broadcast) ne peuvent être attribuées à un hôte.
- Le 1èr hôte aura pour adresse **010**00001, et aura donc l'adresse IP 195.52.150.**65**
- Le 2ème hôte aura pour adresse **010**00010, et aura donc l'adresse IP 195.52.150.**66**
- Le 3ème hôte aura pour adresse **010**00011, et aura donc l'adresse IP 195.52.150.**67**
- Etc……
- Le dernier hôte aura pour adresse **010**11110, et aura donc l'adresse IP 195.52.150.**94**

Prenons le sous réseau **3** : 195.52.150.96 et intéressons-nous au 4ème octet (**011**00000) :

- Les adresses **011**00000 (adresse sous réseau) et **011**11111 (adresse de diffusion = broadcast) ne peuvent être attribuées à un hôte.
- Le 1èr hôte aura pour adresse **011**00001, et aura donc l'adresse IP 195.52.150.**97**
- Le 2ème hôte aura pour adresse **011**00010, et aura donc l'adresse IP 195.52.150.**98**
- Le 3ème hôte aura pour adresse **011**00011, et aura donc l'adresse IP 195.52.150.**99**
- Etc……
- Le dernier hôte aura pour adresse **011**11110, et aura donc l'adresse IP 195.52.150.**126**

Prenons le sous réseau **4** : 195.52.150.0 et intéressons-nous au 4ème octet (**100**00000) :

- Les adresses **100**00000 (adresse sous réseau) et **100**11111 (adresse de diffusion = broadcast) ne peuvent être attribuées à un hôte.
- Le 1èr hôte aura pour adresse **100**00001, et aura donc l'adresse IP 195.52.150.**129**
- Le 2ème hôte aura pour adresse **100**00010, et aura donc l'adresse IP 195.52.150.**130**
- Le 3ème hôte aura pour adresse **100**00011, et aura donc l'adresse IP 195.52.150.**131**
- Etc……
- Le dernier hôte aura pour adresse **100**11110, et aura donc l'adresse IP 195.52.150.**158**

Dans notre exemple, combien d'hôtes peut-il y avoir dans chaque sous réseaux ?

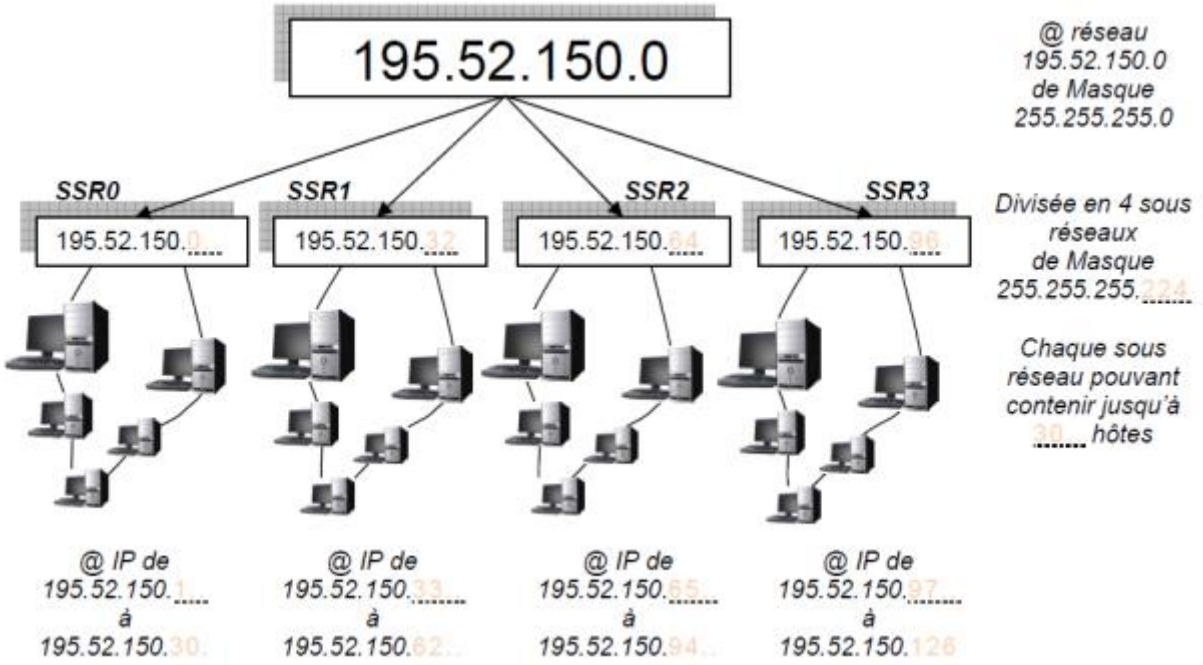
On a réservé 3 bites pour les sous réseaux dans le 4ème octet, il reste donc 8-3=5 bits pour les hôtes, soit 2^5 combinaisons auxquelles il faut soustraire celles tous à « «0 » (adresse sous réseau) et celles tous à « 1 » (adresse de broadcast), ce qui nous donne au final 2^5-2=32-2=30 adresses hôtes possibles.

Quels sera le masque de sous réseau dans notre cas ?

Nous avons vu que pour une adresse de classe C, le masque par défaut (sans sous réseaux) est :255.255.255.0, or sur le 4ème octet, nous allons devoir « masquer » les 3 bits correspondants à nos sous-réseaux.

Pour cela, nous allons placer à « 1 » les bots correspondant dans le masque par défaut, c'est-à-dire les 2 bits de poids fort du 4ème octet :

Masque de classe C sans sous-réseaux :	11111111.11111111.11111111.00000000
Masque de classe C avec nos sous-réseaux :	11111111.11111111.11111111.**111**00000
Ce qui donne en décimale pointée :	255 . 255 . 255 .**224**



Utilisation du masque de sous-réseau :

A quel sous réseau appartient l'adresse IP 195.52.150.196 ?

Pour obtenir le sous réseau auquel appartient cette adresse, il faut effectuer un ET logique entre l'adresse IP et le masque :

195.52.150.196 en binaire s'écrit :	11000011.00110100.10010110.11000100
255.255.255.224 en binaire s'écrit :	11111111.11111111.11111111.11100000
On effectue un ET logique :	11000011.00110100.10010110.11000000
C'est-à-dire en décimale pointée :	195 . 52 . 150 . 192

Cette adresse sous réseau correspondrait au sous réseau N^{0}6.

6.10.4 Notation CIDR (Classless InterDomain Routing)

On a vu que pour connaitre l'adresse d'un réseau, il fallait également connaitre le masque. Une forme plus courte est connue sous le nom de « notation CIDR ». Elle donne le numéro du réseau suivi par un slash ("/") et le nombre de bits à 1 dans la notation binaire du masque de sous-réseau.

Le masque 255.255.0.0, équivalent en binaire à 11111111.11111111.00000000.00000000, sera donc représenté par /16 (16 bits à la valeur 1).

Exemple :

186.15.0.0 /16 L'attribution d'adresses en utilisant le système CIDR a aujourd'hui remplacé les classes, devenues obsolètes

6.11 VLSM (VARIABLE LENGHT SUBNET MASKING)

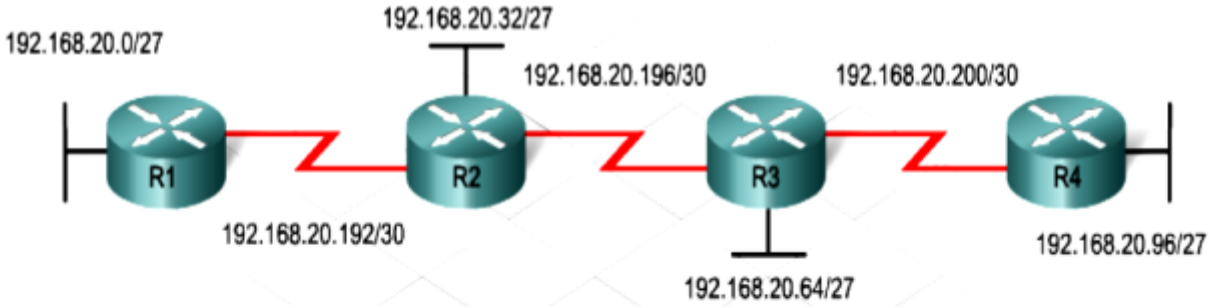
La création de base de sous-réseaux est suffisante pour les petits réseaux mais n'offre pas la souplesse requise pour les grands réseaux d'entreprise.

Les masques de sous-réseau de longueur variable (VLSM) permettent une utilisation efficace de l'espace d'adressage.
Le principe du VLSM consiste à créer des sous-réseaux d'un sous-réseau. Cette technique a initialement été développée pour optimiser l'efficacité de l'adressage.

6.11.1 Avantages

- Utilisation efficace de l'espace d'adressage ;
- Utilisation de plusieurs longueurs de masque de sous-réseau ;
- Division d'un bloc d'adresses en blocs plus petits ;
- Prise en charge des résumés du routage ;
- Plus grande souplesse de conception de réseau ;
- Prise en charge des réseaux d'entreprise hiérarchiques

6.11.2 Exemple



R = 192.168.20.0/24	
N° de S/R	@ de S/R
1	192.168.20.0/27
2	192.168.20.32/27
3	192.168.20.64/27
4	192.168.20.96/27
5	192.168.20.128/27
6	192.168.20.160/27
7	**192.168.20.192/27**
8	192.168.20.224/27

S/R du S/R = 192.168.20.192	
N° de S/S/R	@ de S/S/R
1	**192.168.20.192/30**
2	**192.168.20.196/30**
3	**192.168.20.200/30**
4	**192.168.20.204/30**
5	**192.168.20.208/30**
6	**192.168.20.212/30**
7	**192.168.20.216/30**
8	**192.168.20.220/30**

Pour le subnetting on a utilisé 3 bits, ce qui donne 8 sous réseaux. Le sous-réseau 192.168.20.192 a subi un autre subnetting.

Normalement l'adresse 192.168.20.192/27 sera utilisée sur un seul segment de 25 -2 = 32-2 = 30 hosts. Cette même adresse a été utilisée dans 8 autres segments de 2 hôtes chacun. Le nombre d'hôtes est petit, mais cela permet de placer ces adresses dans des segments qui ne comptent que deux interfaces par exemple.

Le VLSM permet l'utilisation de masques différents pour chaque sous-réseau. Une fois qu'une adresse réseau est divisée en sous-réseaux, toute autre division de ces sous-réseaux entraîne la création de sous-sous-réseaux.

7 La couche transport

7.1 Rôle de la couche transport

Le rôle de la couche transport est d'établir une session de communication temporaire entre deux applications pour acheminer les données entre elles. TCP/IP utilise deux protocoles pour cela :

- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)

Fonctions principales des protocoles de la couche transport :

- Suivre les communications individuelles entre les applications résidant sur les hôtes source et de destination
- Segmenter les données pour faciliter la gestion et réassembler les données segmentées en flux de données d'application vers la destination
- Identifier l'application appropriée pour chaque flux de communication

7.2 Fiabilité de la couche transport

Toutes les applications n'ont pas besoin du même degré de fiabilité. TCP/IP fournit deux protocoles de la couche transport, TCP et UDP.

Transmission Control Protocol (TCP) :

- Assure un acheminement fiable – Toutes les données arrivent à destination
- Utilise les accusés de réception et d'autres mécanismes pour garantir la transmission
- Orienté connexion : création d'une session entre la source et la destination
- Acheminement fiable : retransmission des données perdues ou endommagées
- Reconstitution ordonnée des données : numérotation et séquencement des segments
- Contrôle de flux : régulation de la quantité de données transmises
- Protocole avec état : garde une trace de la session

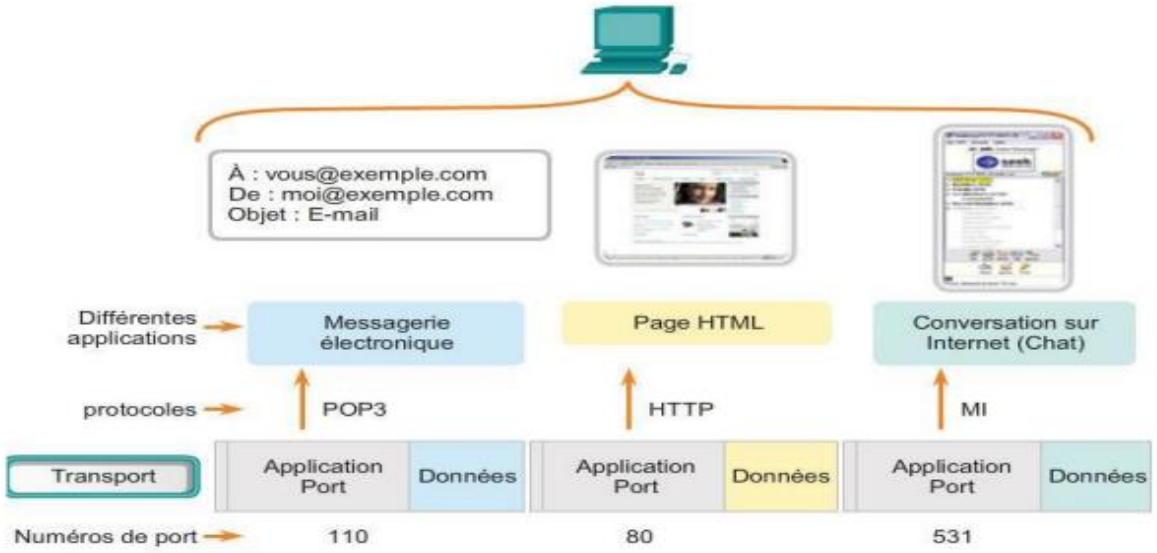
User Datagram Protocol (UDP) :

- Fournit juste les fonctions de base pour la transmission, sans aucune garantie
- Sans négociation préalable
- Sans garantie de remise
- Sans reconstitution ordonnée des données
- Sans contrôle de flux
- Protocole sans état

7.3 Séparation des communications multiples

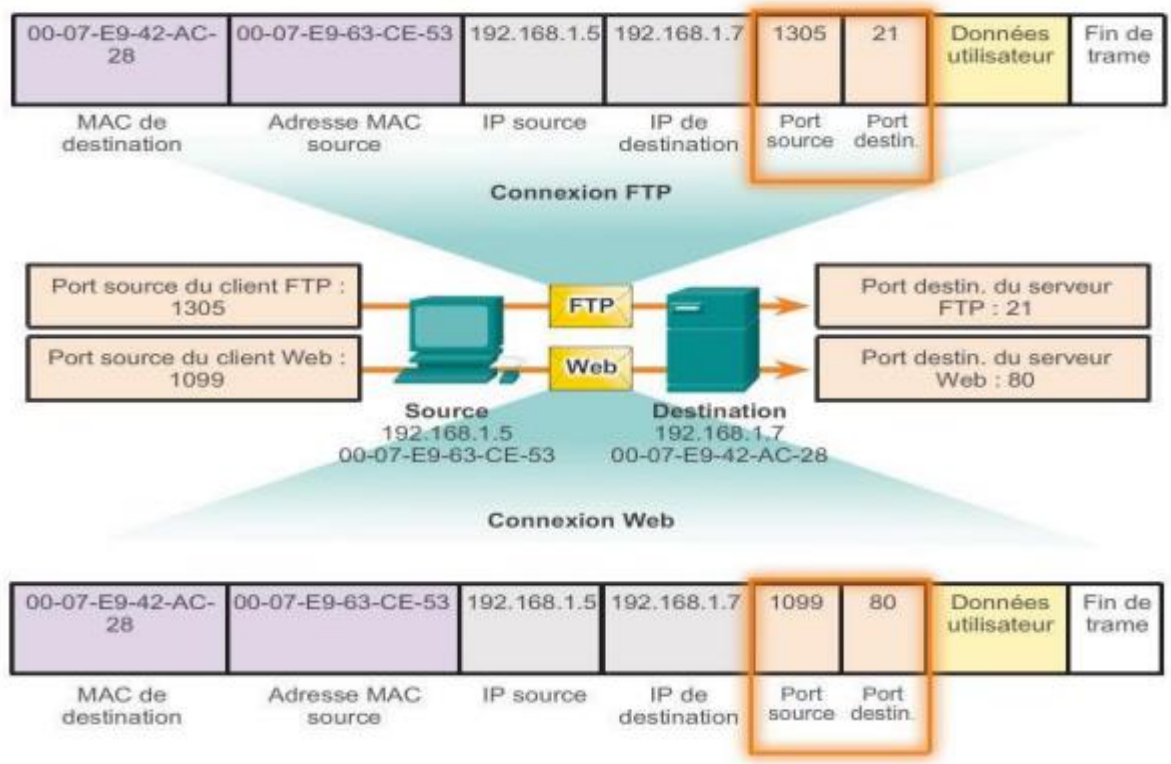
Les numéros de port sont utilisés par les protocoles TCP et UDP pour différencier les applications.

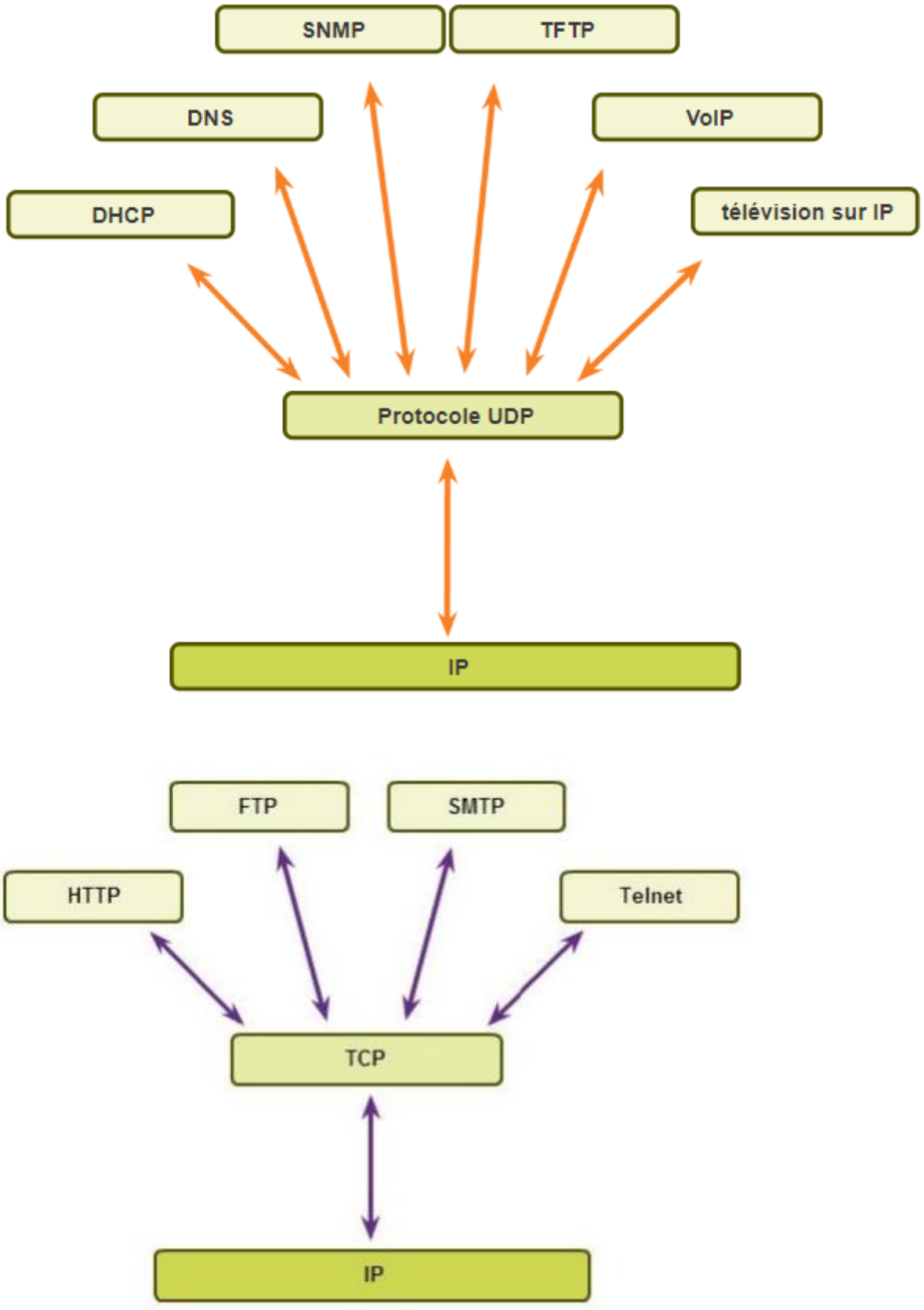
Adressage de port



Les données des différentes applications sont dirigées vers l'application adéquate car chaque application dispose d'un numéro de port unique.

7.4 Adressage de ports TCP et UDP




SNMP
TFTP
DNS
VoIP
DHCP
télévision sur IP
Protocole UDP
IP
FTP
SMTP
HTTP
Telnet
TCP
IP

8 Les couches hautes

Les couches hautes du modèle OSI offrent des services orientés vers les utilisateurs, alors que les couches dites basses sont concernées par des communications fiables de bout en bout.

8.1 La couche session

La couche session fournit aux entités de la couche présentation les moyens d'organiser et synchroniser les dialogues et les échanges de données.

La principale fonction de la couche session est de fournir aux utilisateurs (entité de la couche de présentation ou processus de la couche application) les moyens d'établir des connexions appelées sessions et d'y transférer des données en bon ordre.

8.2 La couche présentation

Chaque ordinateur ayant un mode de représentation propre, il est nécessaire de prévoir des mécanismes de conversion afin de s'assurer que des machines différentes puissent se comprendre. C'est à ce niveau que peuvent être implantées des techniques de compression et de chiffrement de données.

- La compression des données consiste à réduire la taille de la représentation des données que cela soit pour minimiser l'espace disque qu'il occupe ou le temps de transfert.
- Le chiffrement désigne l'ensemble des techniques permettant de rendre des messages inintelligibles

8.3 La couche application

La couche application gère les programmes de l'utilisateur

La couche fournit à ces utilisateurs quelques applications et services généraux

Protocole orienté transfert de fichier :

FTP (File Transfer Protocol) est utilisé dès qu'il s'agit de transférer des données entre deux machines A et B.

NFS (Network File System) permet à un ordinateur d'accéder via un réseau à des fichiers distants.

Protocoles de type « session distance » :

Telnet (Telecommunication Network) permet à une machine client de se connecter sur un serveur.

SSH (Secure Shell) protocole de communication sécurisé.

Protocoles orientés messageries :

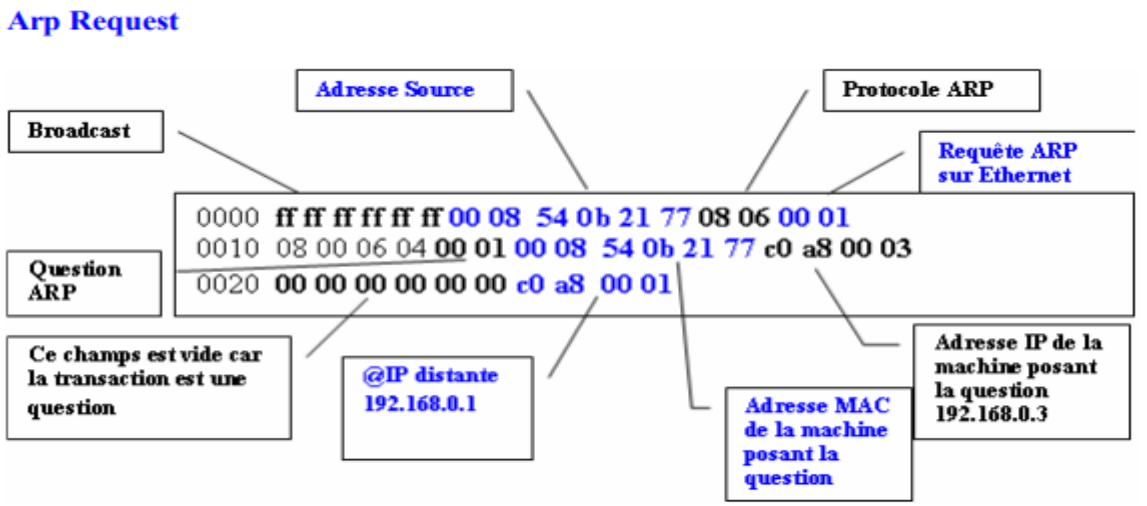
SMTP (Simple Mail Transfert Protocol) permet le transfert des courriers électroniques.

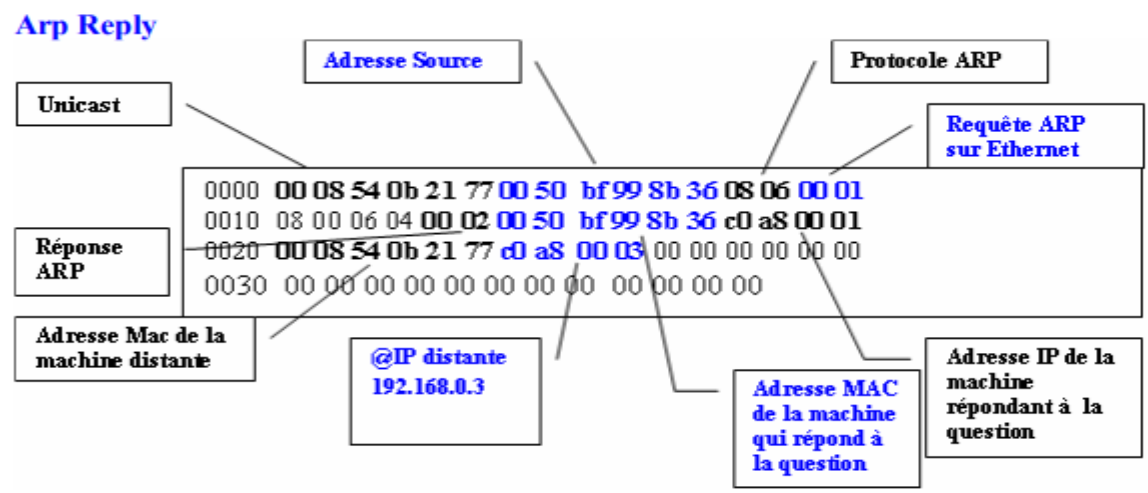
POP (Post Office Protocol) IMAP (Internet Message Access Protocol)

9 Le protocole ARP et RARP

9.1 Le protocole ARP : Address Resolution Protocol

Le protocole ARP permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse (en anglais ARP signifie Address Resolution Protocol). Le protocole ARP émet une requête sur le réseau. L'ensemble des machines du réseau vont comparer cette adresse logique à la leur. Si l'une d'entre-elles s'identifie à cette adresse, la machine va répondre à la requête ARP qui va stocker le couple d'adresses dans la table de correspondance et la communication va alors pouvoir avoir lieu... Pour visualiser cette table, il existe la commande « arp » sous windows.





9.2 Le protocole RARP: Reverse Address Resolution Protocol

Le protocole RARP effectue le travail inverse du protocole ARP.

- RARP utilise les mêmes procédures de communication qu'ARP avec des requêtes transmises par diffusion et des réponses transmises en mono destinataire
- Un ordinateur qui envoie une requête RARP essaie de découvrir une information sur lui même
- Comme l'hôte ne connaît pas encore son adresse IP, le champ IP de l'émetteur contient la valeur 0.0.0.0.