Introduction aux réseaux

On peut définir un réseau comme un ensemble de noeuds reliés par un ensemble de chemins. Un réseau peut être représenté par un graphe. La topologie du réseau, c'est à dire la localisation des noeuds et l'agencement des liens entre les noeuds peut être très variée.

Un réseau informatique est un réseau dont les noeuds sont constitués par des unités de traitement de l'information (routeurs, stations terminales). Celles-ci échangent de l'information par l'intermédiaire de canaux de transmission (câbles/fibres, faisceaux hertziens).

Pour pouvoir communiquer, deux unités de traitement doivent respecter les mêmes règles. On parle de protocoles de communication. Comme un réseau informatique est par nature très hétérogène (du point de vue matériel, système et logiciel) on a défini des niveaux de préoccupation : du niveau le plus bas (physique), où on s'occupe de transmettre des bits jusqu'au niveau le plus haut (application) où on trouve des fonctions directement appelables par les programmes.

Plusieurs organismes de normalisation de droit s'occupent des réseaux informatiques : ISO (International Standardization Organization), l'UIT-T (Union Internationale des Télécommunications), l'Institute of Electrical and Electronics Engineers (IEEE), l'Internet Engineering Task Force (IETF), ou encore l'Electrical Industries Association (EIA) parmi les plus importants.

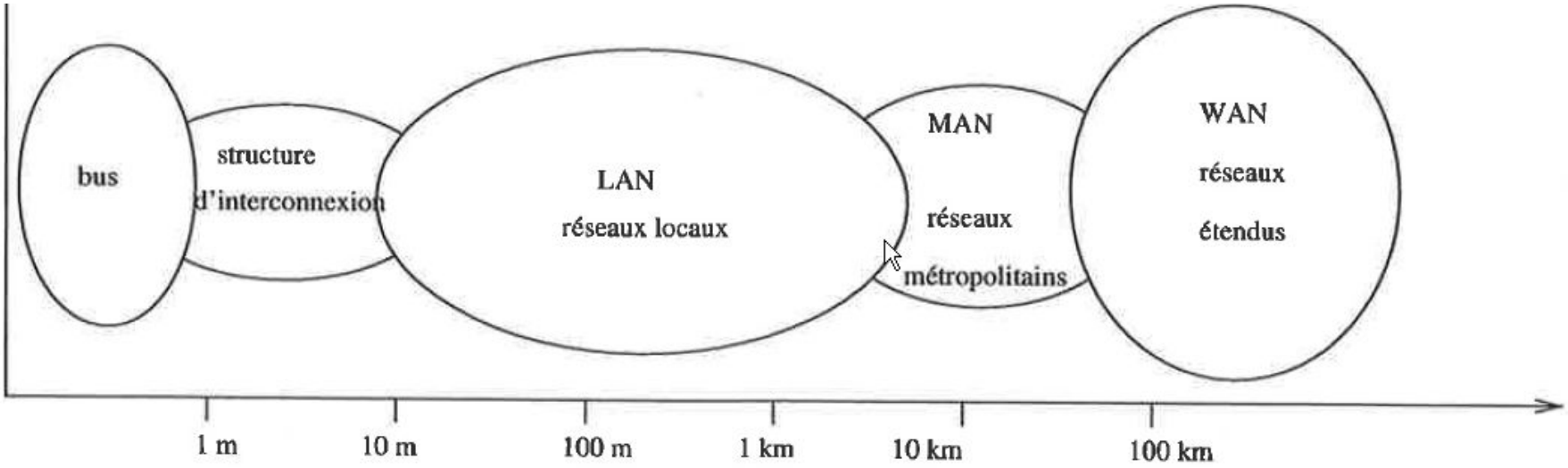
Classification des réseaux selon leur taille/couverture géographique

PAN (Personal Area Nework) : réseau personnel, quelques mètres

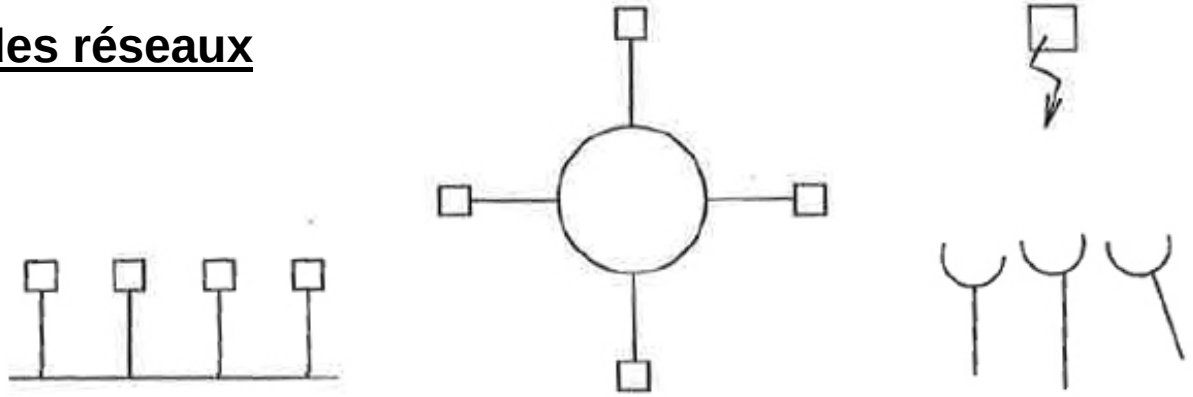
LAN (Local Area Network) : réseau local, celui d'une entreprise par exemple, étendue géographique peu importante.

MAN (Metropolitain Area Network) : réseau métropolitain ou de campus, interconnecte par exemple les différents site d'une université ou d'une administration (agrégats de réseaux locaux), étendue de quelques km.

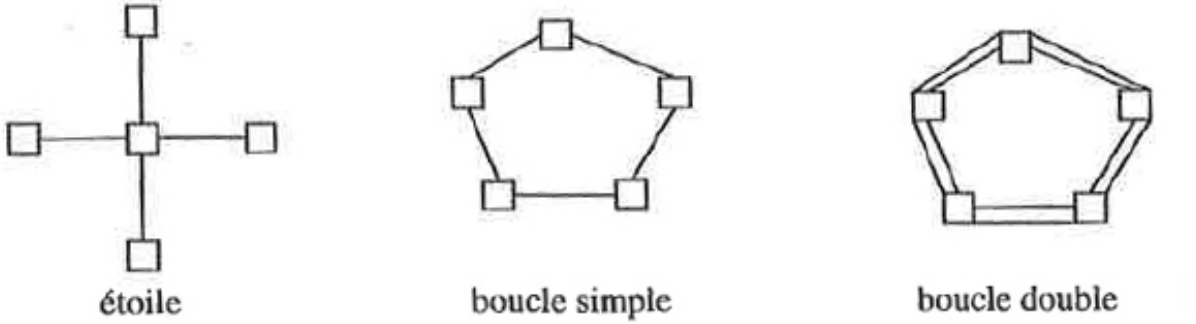
WAN (Wide Area Network) : couverture géographique importante, réseau grande distance (nationale, ou internationale)



Topologie des réseaux



réseaux en mode de diffusion



réseaux en mode point à point

Mode de diffusion

Mode point à point : le support physique de communication (câble) relie un équipement à un autre seulement. Quand 2 noeuds non directement connectés entre eux veulent communiquer, ils le font par l'intermédiaire des autres noeuds du réseau. Exemples : réseaux locaux en boucle, en étoile, maillés.

Mode multi-diffusion : le même support relie plusieurs équipements entre eux. Lorsque l'un d'eux envoie un message, les autres le reçoivent. C'est l'adresse spécifique placée dans le message qui permettra alors à chacun de savoir si le message lui était adressé ou non. Exemples : réseaux locaux en bus, en anneau, réseaux satellitaires, radio.

Sens de communication

Simplex : communication unidirectionnelle. Une station émet, l'autre reçoit. Exemples : la diffusion radio, TV.

Half-duplex : communication bidirectionnelle. Les stations peuvent émettre et recevoir, mais chacune à leur tour. Exemple : le talkie-walkie.

Full-duplex : les stations peuvent émettre/recevoir en même temps. Exemple : la communication téléphonique.

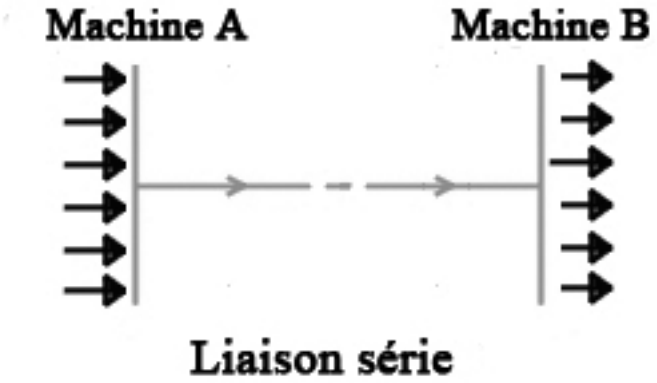
Remarque : pour la transmission simplex et half-duplex, un seul conducteur suffit ; pour la transmission full-duplex, il en faut 2 : un pour l'émission, l'autre pour la réception.

Transmission série/parallèle

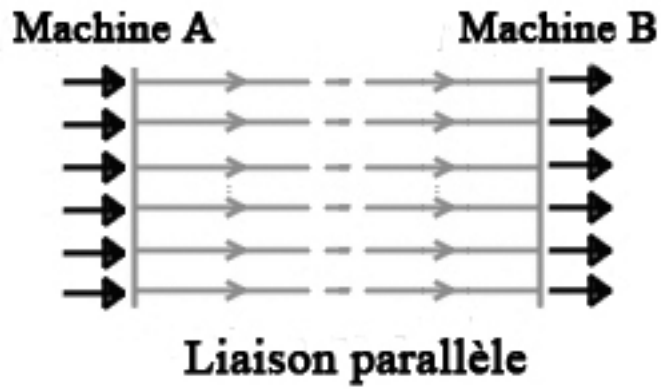
Transmission parallèle : transmission de plusieurs bits simultanément. Le parallélisme est réalisé soit par duplication des fils (c'est le cas du bus). Remarque : la duplication des fils pose des problèmes de synchronisation et ne peut être utilisé que sur de très courtes distances.

Transmission série : les informations sont transmises sur la même ligne, les unes après les autres et se succèdent dans le temps. Exemple : sur un réseau local, en utilisant un câble à paire torsadé.

Remarque : la sérialisation d'un signal parallèle est faite grâce à un registre de décalage.



Liaison série



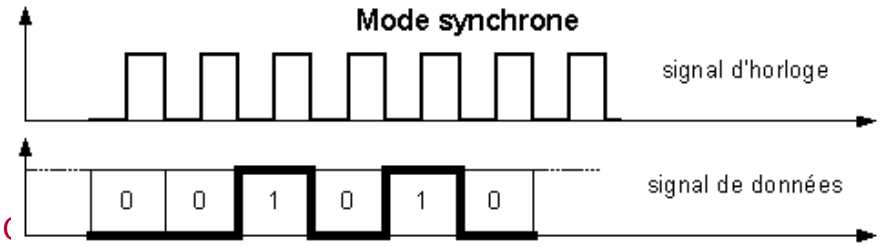
Liaison parallèle

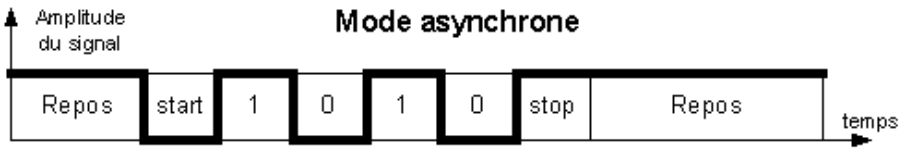
Transmission synchrone/asynchrone

Le récepteur doit savoir à quelle fréquence l'émetteur envoie les bits sur la ligne de transmission. Sans cela, il est impossible d'interpréter correctement les signaux reçus (un bit peut être par exemple lu au lieu de 2 si la fréquence de réception est 2 fois moins élevée que la fréquence d'émission. Il y a ainsi nécessité de synchroniser les horloges de l'émetteur et du récepteur.

Transmission synchrone : le signal d'horloge généré par l'émetteur est parfois transmis au récepteur par un conducteur qui accompagne la ligne des données. Les horloges sont ainsi synchronisées pendant toute la durée de la communication. Bien adapté à une transmission régulière de bits

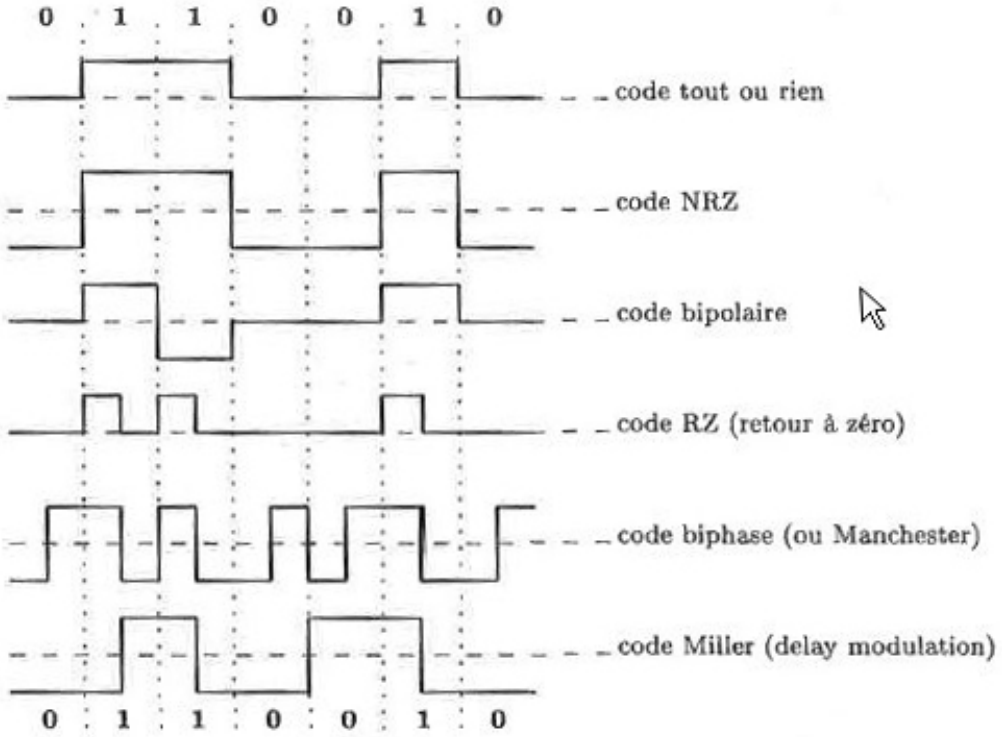
Transmission asynchrone : il n'y a pas de ligne dédiée pour le signal d'horloge. Il y a donc re-synchronisation des horloges de l'émetteur et du récepteur à chaque transmission. Il faut alors reconnaître le début et la fin de la transmission, ce qui est fait en ajoutant un bit de début (start-bit) et un bit de fin (stop-bit). Bien adapté à une transmission irrégulière, par exemple des caractères tapés au clavier.





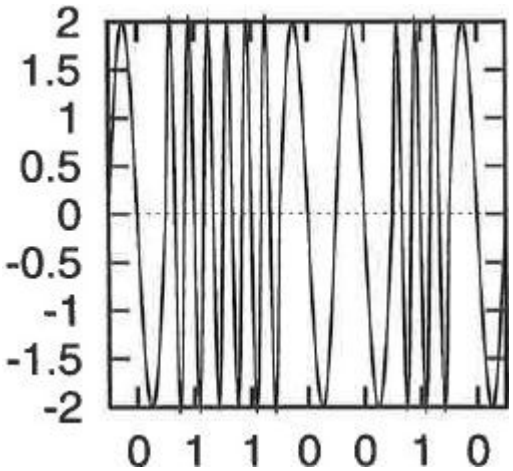
Transmission en bande de base / en large bande

Transmission en bande de base : transmission de signaux carrés (impulsions discrète avec interruption entre chaque impulsion) correspondant directement à la suite de bits que l'on veut émettre. Par exemple avec un courant électrique avec 2 niveaux de tensions, +V =1 et -V=0. Transmission sur une unique fréquence. Exemples : codage NRZ, manchester ... Dégradation du signal avec la distance et nécessité d'utiliser des répéteurs. Solution généralement choisie sur de courtes distances mais peut aussi être mise en œuvre sur de grandes distances.

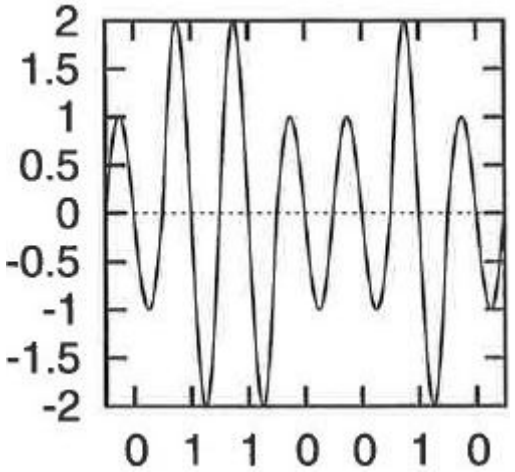


Remarque : malgré son atténuation sur de longues distances, un signal numérique est moins sensible au bruit qu'un signal analogique. En effet, un signal numérique bien régénéré est identique au signal original, tandis qu'un signal analogique est régénéré avec les défauts introduits par le support et le bruit.

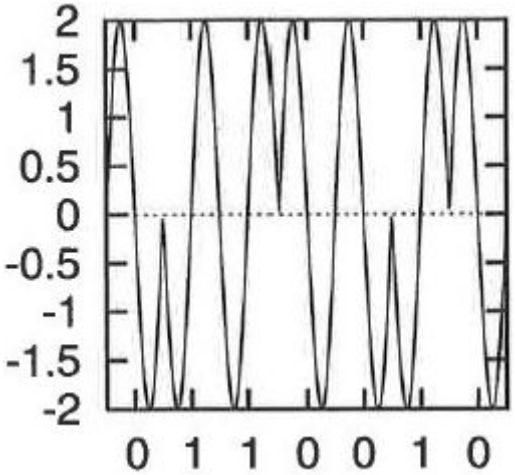
Transmission en large bande : transmission de signaux analogiques sous la forme d'ondes électromagnétiques ou optiques. Signaux continus (sans interruption). Possibilité de modulation de fréquence, d'amplitude, de phase ; modulation notamment utilisée pour le multiplexage. La modulation de fréquence est la plus robuste au bruit (la modulation d'amplitude la moins). Transmission analogique généralement mise en oeuvre sur de grandes distances. Nécessité d'amplificateurs pour régénérer le signal.



Modulation de fréquence



Modulation d'amplitude



Modulation de phase

La conversion entre un signal analogique et numérique est permise grâce à un modem (modulateur/démodulateur) : la modulation est la transformation du signal numérique en analogique, la démodulation le contraire.

Débit, bande passante, rapidité de modulation

Débit (binaire) D : il correspond au nombre de bits émis/transmis par seconde : il s'exprime en bits/s (bps). On peut distinguer le *débit théorique* d'une ligne du *débit utile (ou efficace)* qui tient compte des caractéristiques de la communication (information utile Vs en-têtes, accusés de réceptions ...).

Bande passante W : elle correspond à la bande de fréquences que peut prendre un signal modulé pour être correctement transmis (fréquence max - fréquence min). C'est une grandeur physique/électronique qui s'exprime en Hz. La bande passante ne peut être définie que pour un signal analogique. L'utiliser pour désigner un débit binaire est un abus de langage.

Rapidité de modulation R : nombre de signaux émis par seconde : il s'exprime en bauds. Sur une ligne non bruitée : $\mathbf{R_{max} = 2 \times W}$ (Théorême de Nyquist).

Valence V : nombre d'états du signal. Si n est le nombre de bits émis par signal : $\mathbf{n=\log_2 V}$. Donc $\mathbf{V = 2^n}$. Un signal avec 2 niveaux de tension permet de coder 1 bit …

Débit théorique max sur une ligne non bruitée : $\mathbf{D_{max} = R \times n}$ (Nyquist)

Débit binaire max sur une ligne bruitée : $\mathbf{D = W \log_2(1 + PS/PB)}$ (Shannon)

PS/ PB : puissance du signal /puissance du bruit. En général, on préfère exprimer ce rapport en décibels : $\mathbf{S/B = 10 \log_{10}(PS/PB)}$. Donc $\mathbf{PS/PB = 10^{S/(10 \times B)}}$

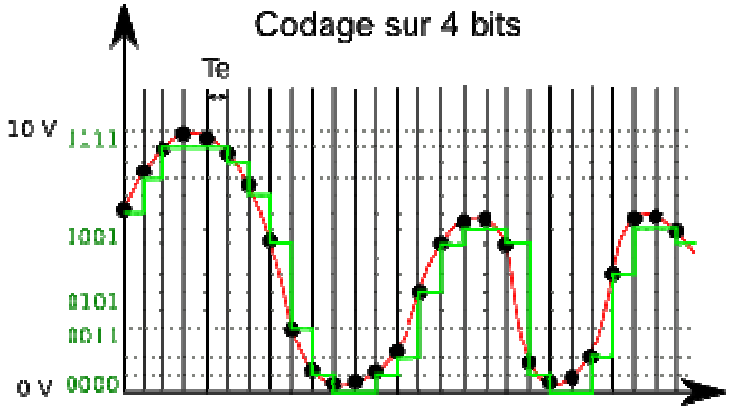
Numérisation d'un signal analogique

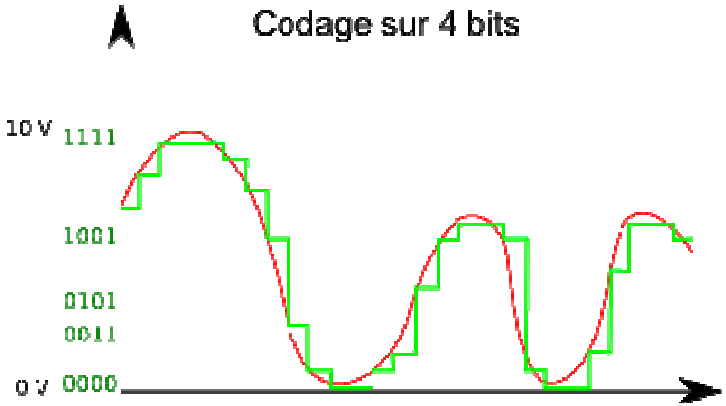
Plusieurs étapes :

1. Echantillonnage : on prélève le signal analogique à intervalles réguliers (intervalle de temps =1/fréquence d'échantillonnage)

2. Quantification : on définit un certain nombre de niveaux de quantification, puis chaque valeur précédente est ramené au niveau le plus proche (la quantification est donc une approximation du signal réel).

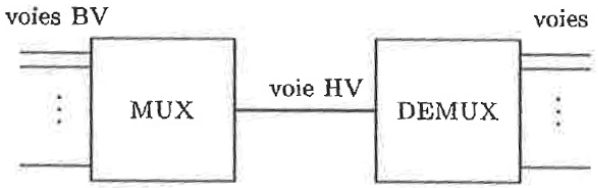
3. Codage : le nombre de bits nécessaire pour coder un échantillon est lié au nombre de niveaux de quantification N. **$n=\log_2 N$**.





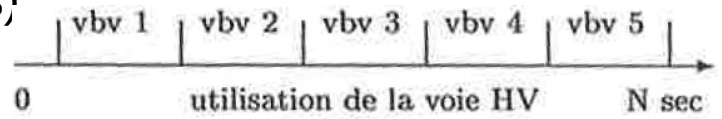
Multiplexage

Transport simultané sur une même ligne (haut débit) de données provenant de plusieurs liaisons (bas débit).

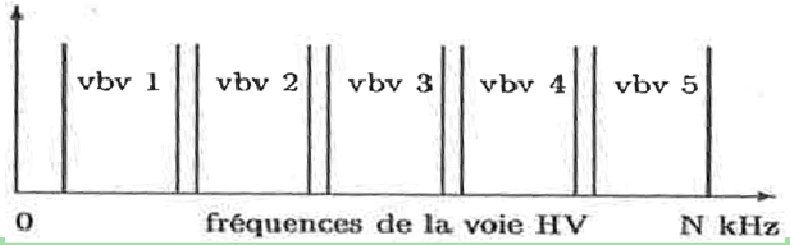


Multiplexage à l'émission, démultiplexage à la réception.

Multiplexage temporel : Allouer successivement et cycliquement à chaque liaison (équipement) un quota de temps pendant lequel il dispose de toute la bande passante. Plus adapté à la transmission numérique. Exemple : la transmission numérique de la voix (codage MIC). On peut parler aussi de multiplexage statistique lors que les quotas de temps sont allouées en fonction des besoins de chaque liaison (multiplexeurs intelligents)



Multiplexage fréquentiel : modulation d'une onde porteuse en définissant une plage de fréquences) pour chaque liaison. Bien adapté pour les signaux de type analogique. Exemple : RTC (Réseau Téléphonique Commuté).



Exemple : le codage MIC (Modulation d'impulsion codée)

Défini par l'UIT-T pour la représentation numérique des signaux de voix dans les systèmes de téléphonie.

Fréquence d'échantillonnage à 8Khz (ce qui correspond à un prélèvement d'échantillon tous les 1/8000s, soit 1 mesure chaque 125 x 10^{-6} s), nombre de niveaux de quantification choisi : 256, donc codage (théorique) sur 1 octet (MIC Européen). Débit : 64000 bps (8 bits à transmettre chaque 125 x 10^{-6} s).

Transmission numérique en utilisant un codage pseudo-ternaire appelé mode à haute densité HDB3 qui a pour but d'éviter les zéros successifs. Ou pour les transmissions de débits plus élevés, un code appelé CMI (Code Manchester Inversion) du type 1B2B.

Multiplexage temporel : on affecte cycliquement un intervalle de temps (IT) à chacune des communications à transmettre. La séquence correspondant à un balayage de tous les canaux multiplexés s'appelle une trame. Une trame est fixée à 32 IT. Comme 2 IT sont utilisés pour la gestion, le multiplexage peut donc concerner 30 voies. Comme on l'a vu, chacune ayant un débit de 64 Kbps, il faut donc que la voie principale aie un débit de 32 x 64 = 2048 Kbps. La trame complète doit durer 125 x 10^{-6} s (ce qui correspond à la période d'échantillonnage), chaque voie dispose donc d'un IT de 125 x 10^{-6} / 32 = 3,90 x10^{-6} s.

Commutation de circuits, de message, de paquets

Commutation : Action réalisée au niveau des noeuds du réseau. Mise en relation d'une entrée avec une sortie.

Commutation de circuits : un circuit est établi entre l'émetteur et le destinataire. Sur l'ensemble des segments réseaux qui le constitue, il y a une bande (temporelle, fréquentielle) qui est réservée pour cette communication. Service orienté connexion. Exemple : le réseau téléphonique. Avantage : délai de traversée constant. Inconvénient : gaspillage possible de la bande passante.

Commutation de messages : Pas de réservation de ressources. Les messages qui arrivent dans un noeud de commutation sont traités selon leur ordre d'arrivée (file d'attente FIFO). Store and Forward (mode différé), le message est transmis après traitements des erreurs. Avantage : meilleure utilisation des ressources. Inconvénient : durée de traversée variable (fonction du trafic).

Commutation de paquets : découpage de messages en paquets (taille variable mais avec un maximum). *Mode circuit-virtuel* : tous les paquets d'une même liaison doivent emprunter le même circuit (exemple TCP). *Mode datagramme* : les paquets peuvent emprunter des noeuds différents (exemple UDP). En mode circuit virtuel, la technique du Store and Forward peut comprendre la possibilité de reconstituer la totalité d'un message avant de re-transmettre. Avantage : gestion encore plus fine du réseau. Inconvénient : nécessité de réassemblage à l'arrivée.

Mode connecté/non connecté

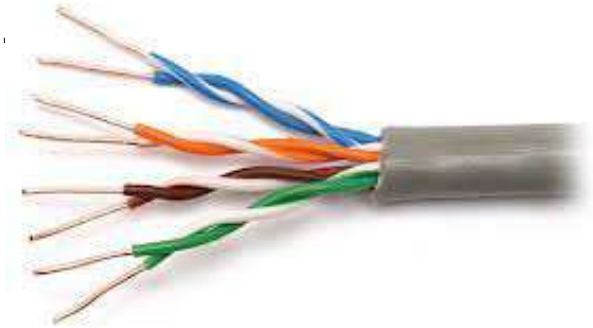
Mode connecté : l'émetteur demande l'établissement d'une connexion. Si le récepteur accepte, la connexion est alors établie. Généralement, il y a établissement d'un circuit (réel ou virtuel) entre les deux de sorte que tous les envois (de messages/paquets) suivent le même chemin. Ils sont donc censés arriver dans l'ordre. Chaque envoi donne généralement lieu à un accusé de réception. Ce mode est généralement associé à la notion de qualité de service QoS (Quality of Service) : assurance de la disponibilité des noeuds intermédiaires, négociation de paramètres à respecter lors de l'échange ... A la fin, la connexion est libérée. C'est le fonctionnement du réseau téléphonique classique.

Mode déconnecté : il n'y a pas d'établissement de connexion. L'émetteur envoie ses données (on parle de datagrammes) sans savoir si le récepteur est prêt à recevoir. En fonction de la dynamique du réseau (état d'engorgement des nœuds …), les envois successifs peuvent typiquement emprunter des chemins différents (et donc arriver dans le désordre). L'avantage de ce mode est sa rapidité (pas d'établissement de connexion, pas de négociation préalable, en général, pas d'accusés de réception). Ce service est celui du courrier postal classique.

Supports de transmission

Paires torsadées et câbles coaxiaux (ondes électriques), câbles optiques (ondes lumineuses), liaisons sans fil (ondes radio)

Paire torsadée : Blindée (STP) ou non (UTP). Sur éthernet, on parle de 10/100/1000 Base T. Vitesse de transmission resp de 10/100/1000 Mbps. Transmission en bande de base. Transporte un signal sur une distance d'environ 100 mètres sans affaiblissement. 4 segments max (400 m). Nb de postes par segment : plus de 100. Connecteurs RJ45. Topologie en étoile. Avantages : faible coût. Inconvénients : distance limitée, peu résistant physiquement, faible immunité au bruit.

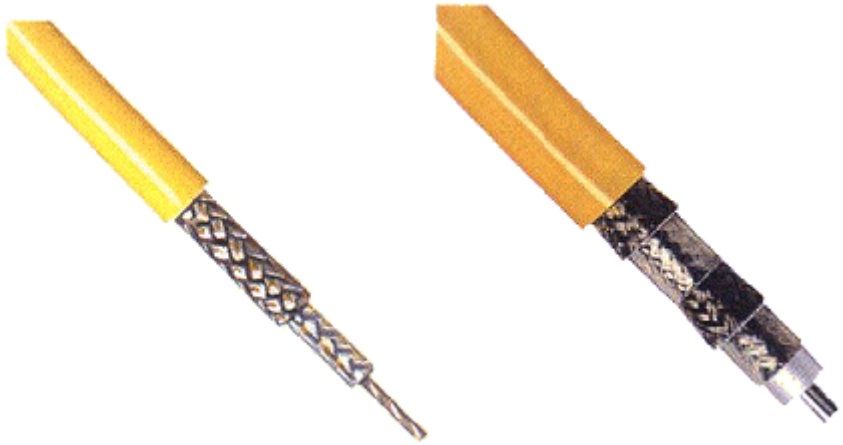


Remarque : Sur éthernet, la paire torsadée a supplanté le câble coaxial

Remarque : Explication 10BaseT, 10Base5, 10Base2 : le premier nombre 10 signifie 10Mbps (on parlera de 100BaseT pour le fast éthernet, de 1000BaseT pour le Gigabit Ethernet ...), base signifie réseau à bande de base (plutôt qu'à large bande), le chiffre final donne la longueur maximale d'un segment de câble (5 => 500 mètres, 2 => 200 mètres, T signifie torsadé)

Câble coaxial fin / Thinnet (bande de base) : Sur éthernet, on parle de 10Base2. Vitesse de transmission : 10Mbps. Transmission en bande de base. Transporte un signal sur une distance d'environ 185 mètres sans affaiblissement. 30 postes/segments. 5 segments max (925 m). Avantages : facile à installer, bonne immunité au bruit, faible coût de maintenance, assez flexible. Inconvénients : plus coûteux que la paire torsadée. Prise BNC. Topologie en bus

Câble coaxial épais / Thicknet (large bande) : Sur éthernet, on parle de 10Base5. Vitesse de transmission : 10Mbps. Transmission en bande de base. Transporte un signal sur une distance d'environ 500 mètres sans affaiblissement. 100 postes/segments. 5 segments max (2500 m). Avantages : grande immunité au bruit, supporte la transmission de l'image, de la voix, bonne résistance physique. Inconvénients : difficile à installer et à maintenir, coûts élevés. Prise vampire. Topologie en bus.



Remarque : Un transceiver est utilisé comme intermédiaire entre un câble coaxial et une station : généralement interne à la carte réseau : rôle d'écoute, de réception-émission, de détection des collisions, de contrôle de durée de transmission, d'interruption d'une trame anormalement longue. Un transceiver externe permet quant à lui de relier entre eux un câble coaxial fin et épais.

Fibre optique : Monomode ou multimode. Vitesse de transmission : 1 Tbps. Distance : plusieurs centaines/milliers de kms. Avantages : supporte la transmission de l'image, de la voix, bonne résistance physique, grande immunité au bruit, peu d'affaiblissement du signal, très large bande passante, très sécurisé. Inconvénients : très difficile à installer, coûts élevés.

Ondes radios : Débit : quelques dizaines de Kbps (GSM/GPRS), quelques dizaines de Mbps (Wi-fi/LAN), quelques centaines de Mbps (WiMAX), voire beaucoup plus (satellites). Distance : quelques dizaines/centaines de mètres (Wi-fi), quelques kilomètres (GSM), quelques dizaines de kilomètres (WiMAX), plusieurs milliers de kilomètres (satellite). Avantages : facilité de déploiement (pas de support). Inconvénients : possibilité d'écoute par un tiers (sécurisation nécessaire), qualité du signal dépendant de l'environnement (pluie, brouillard ...).

Equipements réseaux

Concentrateur (hub) : Un concentrateur est un équipement permettant de relier plusieurs segments réseaux (câbles). Un concentrateur reçoit un paquet sur un port et le retransmet sur tous les ports. Equipement de niveau physique (1).

Répéteur : Permettent de regénérer les signaux s'ils doivent circuler sur une distance longue, c'est à dire lorsque la longueur totale d'un câble est plus importante que la longueur maximale autorisée pour ce type de câble 10/100BaseT => 100 mètres, 10Base2 => 185 mètres, 10Base5 => 500 mètres). Un répéteur travaille au niveau physique (1). On peut avoir l'impression que les répéteurs ne s'utilisent que sur des réseaux éthernet câblés avec du coaxial. En fait, c'est simplement qu'avec les réseaux 10/100BaseT, le répéteur n'est pas un engin séparé : c'est le concentrateur/commutateur qui joue ce rôle.

Commutateur (switch) : A la différence d'un concentrateur, un commutateur qui reçoit un paquet sur un port le retransmet juste sur la bonne sortie. Utilisation d'une table contenant les adresses MAC et les sorties correspondantes. Donc par rapport au concentrateur, diminution du trafic réseau et augmentation de la sécurité puisque les ordinateurs n'ont accès qu'aux paquets qui leurs sont destinés. Equipement de niveau liaison (2).

Remarque : un hub travaille en half-duplex, la majorité des switch travaillent en full duplex

Pont (bridge) : Equipement de niveau 2. C'est un switch avec simplement 2 ports (ancêtre du switch). Il permet de connecter 2 réseaux pour qu'ils n'en forment plus qu'un. Ils sont notamment utilisés dans le but de partitionner un grand réseau en deux plus petits pour des questions de performances (désencombrer ce réseau) et/ou de sécurité. Contrairement à un hub, un pont va inspecter chaque message qui lui parvient et le diffuser de l'autre côté seulement si cela s'avère nécessaire (c'est à dire si le destinataire est de l'autre côté).

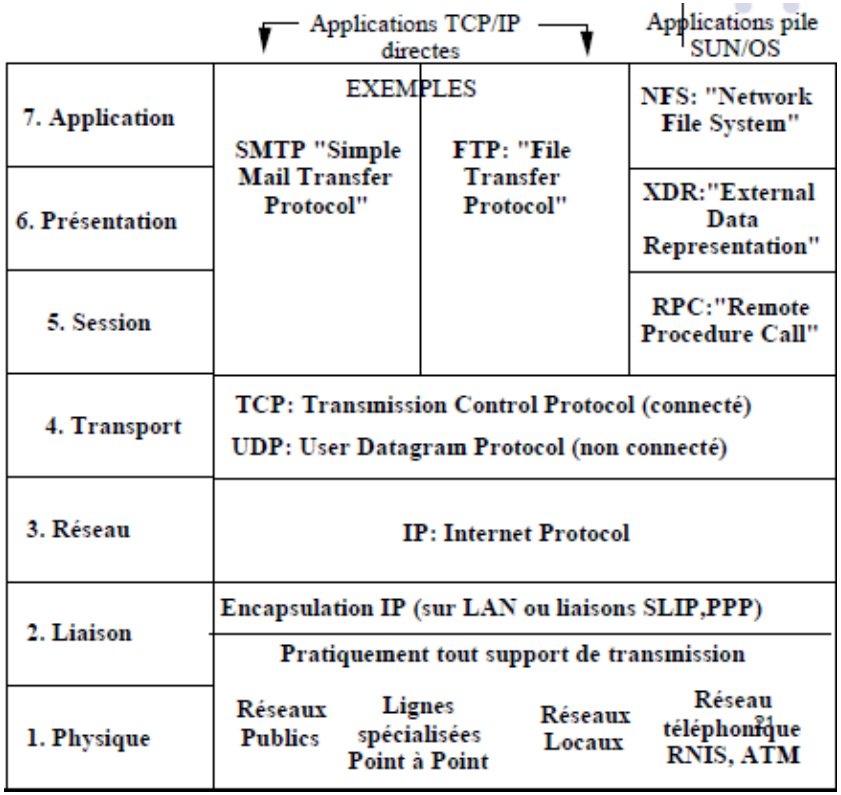
Remarque : un pont peut être utilisé pour connecter 2 réseaux locaux de technologie différente et à ce titre, faire de la conversion de format, ce que ne fait pas les switch

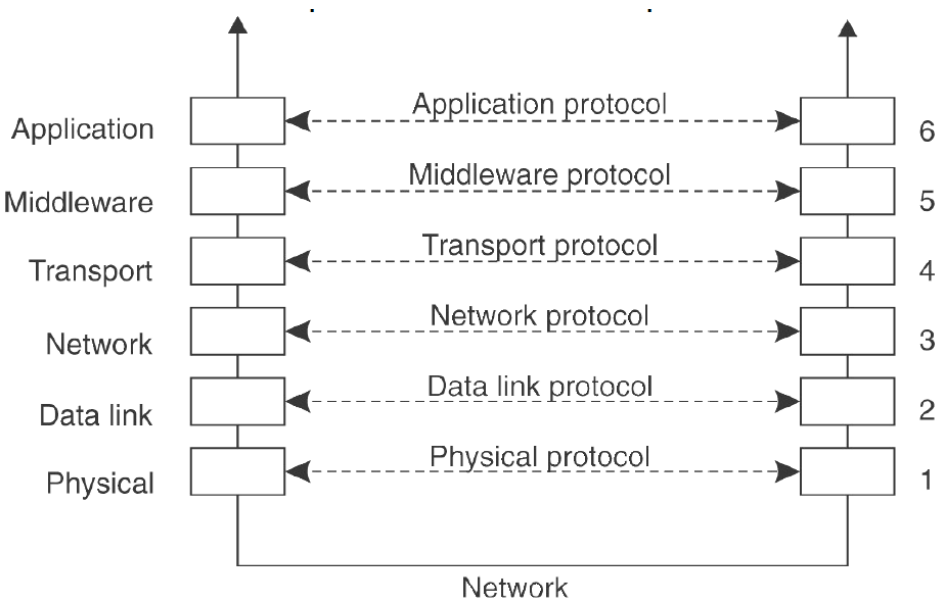
Routeur : Même principe que les ponts/commutateurs mais à un plus haut niveau : équipement de niveau Réseau/IP (3). Un routeur va examiner l'adresse IP contenu dans le paquet pour l'envoyer dans la bonne direction. Les routeurs échangent avec d'autres routeurs et permettent donc de relier des réseaux entre eux, réseaux qui sont potentiellement très éloignés les uns des autres (lignes téléphoniques classiques, fibre optique ...).

Passerelle : Routeur particulier (reliant un/des réseau(x) local(ux) à l'extérieur) et généralement aux fonctionnalités étendues. Une passerelle peut ainsi faire office de firewall (filtrage des adresses IP, des numéros de port ...), mettre en place le NAT (translation d'adresses publiques/privées), jouer le rôle de proxy (masquage des informations des machines du réseau local : @IP, système d'exploitation, navigateur, mise en cache des pages les plus demandées, journalisation des requêtes ...).

Le modèle OSI (Open Systems Interconnection)

Modèle de communication entre ordinateurs proposé par l'ISO, censé garantir l'interopérabilité entre ordinateurs et l'évolutivité des communications. Son organisation en couches décrit des niveaux de préoccupation. Une couche propose un ensemble de services. Elle utilise les services de la couche en dessous et fournit ses services à la couche au dessus.





La couche physique

Elle fournit les moyens physiques (mécaniques, électriques, fonctionnels, procéduraux) nécessaires à la transmission de bits entre deux entités de liaison de données .

Les bits sont transmis de façon brute mais la transmission est toujours cadencée par une horloge (vitesse de la ligne en bauds, débit en bps).

La transmission est en série (bits émis les uns à la suite des autres). La transmission en parallèle (bits émis sur des fils différents) pose des problèmes de synchronisation et n'est valable que sur de courtes distances (bus par exemple) .

La transmission est soit synchrone (cadencement de l'émetteur et de récepteur sur un top d'horloge qui se répète pendant tout l'échange), soit asynchrone (pas de négociation préalable mais bit de start et de stop pour chaque caractère envoyé) .

La transmission est en bande de base (signaux carrés) ou modulée (signaux sinusoïdaux, modulation de fréquence, d'amplitude et/ou de phase).

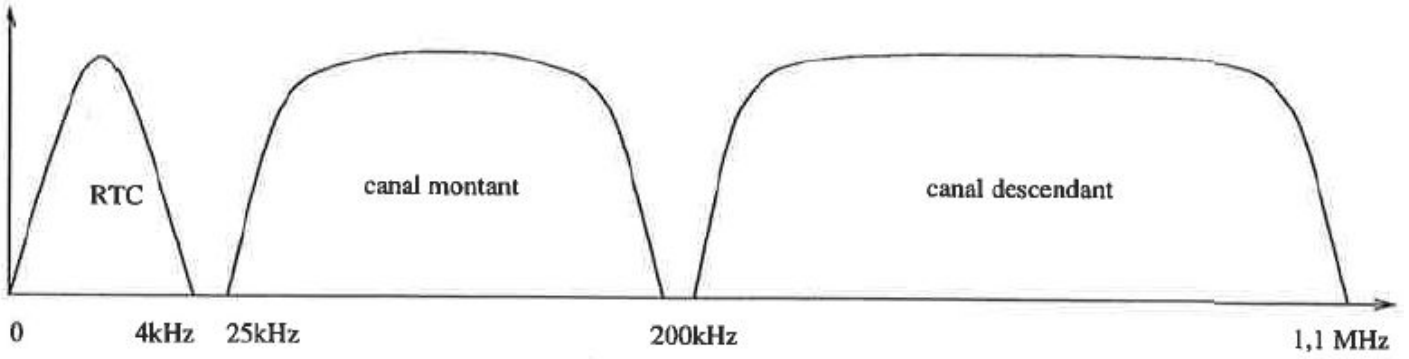
Les supports de transmission : câbles à paire torsadée, câbles coaxiaux, ondes Wi-Fi (dans les réseaux locaux), RTC (lignes téléphoniques classique), ADSL, RNIS, fibre optique, liaisons satellite (pour les liaisons grandes distances).

ADSL (Asynchronous Digital Subscriber Line)

L'ADSL est né de l'observation qu'une ligne téléphonique possède une bande passante d'environ 1 Mhz dans laquelle seule une bande de 3-4 Khz (300 – 3100 Hz) est utilisée pour les communications téléphoniques.

ADSL réserve alors 2 autres bandes : une pour le flux de données usager vers réseau (upstream data = voie montante) allant de 25 à 200 KHz et une autre pour le flux de données réseau vers usager (dowstream data = voie descendante) allant de 200 KHz à 1,1 MHz (beaucoup plus grande donc).

Utilisation d'un filtre ADSL (placé entre la prise téléphonique et la fiche de connexion du téléphone) pour séparer les flux téléphonique et de données et réaliser un filtrage passe-bas et passe-haut afin d'éviter les chevauchements.



La couche liaison

Elle fournit les moyens fonctionnels et procéduraux pour superviser les échanges entre machines adjacentes sur le réseau. C'est elle qui est chargée d'adresser (physiquement) les machines (adressage MAC par exemple), de superviser le dialogue, de détecter (et si possible corriger) les erreurs de transmission …

Plusieurs types de liaisons : liaison avec ou sans connexion, avec ou sans accusés de réception, half ou full duplex.

Deux sortes de mise en trames : trames de caractères (unité de transmission : caractère, utilisation de caractère de contrôle), trames de bits (unité de transmission : bit, utilisation de fanion de bits).

Traitement des erreurs (codes détecteurs ou correcteurs) : bits/tableaux de parité, codes de redondance cyclique (CRC), code de Hamming.

Gestion des AR / Contrôle de flux : send and wait (half-duplex : un AR pour chaque envoi ; si pas d'AR reçu au-delà d'un certain délai, on re-transmet), fenêtre glissante (on envoie plusieurs trames avant de recevoir un AR ; possibilité de full duplex).

Protocoles d'accès au réseau : Ethernet, HDLC, Wi-Fi, Token Ring, FDDI,

Ethernet

Protocole de réseau local à commutation de paquets, utilisant un codage en bande de base (code de Manchester) et standardisé sous le nom IEEE 802.3.

A supplanté les autres standards (Token Ring, FDDI, ARCNet ...)

Les réseaux 802.3 sont aujourd'hui généralement créés grâce à des câbles à paires torsadées (avec des connecteurs RJ-45).

Implémente la couche physique et une partie de la couche liaison (adressage des machines, correction d'erreurs). Classé au niveau liaison (2). Au dessus, c'est la sous-couche couche LLC (Logical Link Control) 802.2 qui fait la charnière entre la éthernet et les couches supérieures.

Offre classiquement un débit standard de 10 Mbps (en pratique, les données ne sont pas transmises aussi rapidement car elles doivent être transmises par paquets de 1500 octets maximum = MTU) mais les nouvelles versions d'éthernet offrent des débits plus élevés : fast éthernet (100 Mbps), gigabit éthernet (1 Gbps) et même 10 Gigabit Ethernet (10 Gbps).

Remarque : la plupart des composants réseaux commercialisés aujourd'hui supportent au moins les 3 premiers débits (on les appelle souvent composants 10/100/1000 Mbps).

Evolution de la norme 802.3 : initialement, communication en half-duplex avec détection des collisions.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

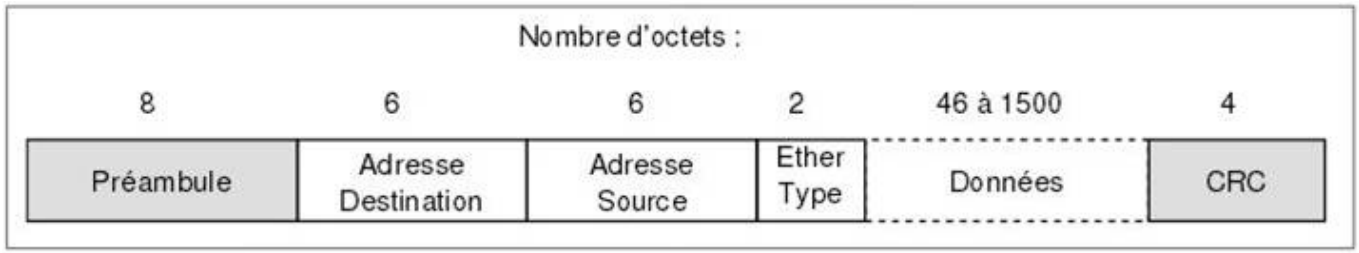
- *Carrier Sense Multiple Access (CSMA)* : Accès multiple avec écoute de la porteuse.
Cette méthode permet à une station d'écouter le support physique de liaison (câble ou fibre) pour déterminer si une autre station transmet une trame de données (niveau déterminé de tension électrique ou de lumière). Si tel n'est pas le cas (donc s'il n'y a pas eu de signal), elle suppose qu'elle peut émettre.

- *Collision Detection (CD)* : Détection des collisions
L'accès multiple implique que plusieurs stations peuvent émettre au même moment ce qui provoque une collision (donc une perte de données). Comme les stations écoutent aussi les collisions elles savent qu'elles doivent réémettre après avoir attendu pendant un délai aléatoire.

Depuis, la norme 802.3 propose une communication en full-duplex, et qui évite l'utilisation du CSMA/CD. Doublement du débit.

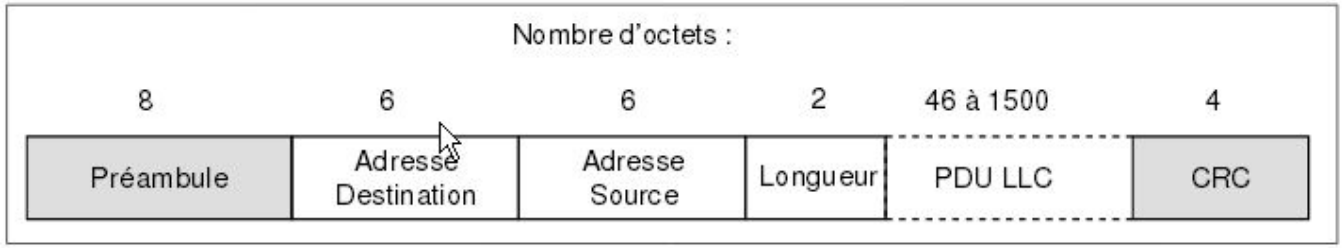
Mise en trame éthernet

Deux formats de trames (légèrement différents) sont utilisés dans un réseau éthernet : V2 et IEEE 802.3. Les trames V2 sont généralement émises par des équipements terminaux tandis que les trames 802.3 sont généralement utilisées par les switchs.



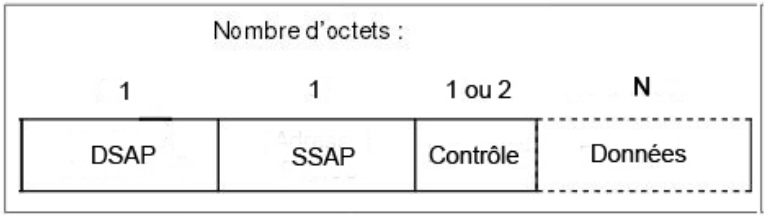
Format de la trame Ethernet V2

Préambule (8 octets) : Annonce le début de la trame et permet à l'horloge du récepteur de se synchroniser sur celle de l'émetteur (transmission asynchrone). Il contient 8 octets dont la valeur est 10101010 (on alterne des 1 et des 0), sauf pour le dernier octet dont le dernier bit est à 1.
Adresses MAC (6 octets) : Identifiant physique stocké sur la carte réseau, unique au monde. Une adresse MAC est généralement représentée sous forme hexadécimale de la façon suivante : 5E:FF:56:A2:AF:15. Dans un réseau Ethernet, l'adresse MAC de diffusion générale est FF:FF:FF:FF:FF:FF
Type de trame (2 octets) : 0x0806 pour ARP, 0x0800 pour IPv4 …
Données (46-1500 octets) : paquet IP, ARP … Si longueur < 46 octets, bits de bourrage
Somme de contrôle (4 octets) : vérification & correction des erreurs de transmission sur les champs précédents



Format de la trame Ethernet 802.3

Mêmes champs que précédemment sauf :
Longueur (qui remplace le champ Type) et qui indique la longueur de la trame
PDU (trame) LLC (à la place du champ Données) qui correspond une trame LLC (elle-même englobant les données)



Format de la trame LLC

DSAP & SSAP : Destination & Source Service Access Point : Permet de préciser de quel type de service de niveau supérieur il s'agit. Par exemple, pour IP : 0xF0
Contrôle : Permet de distinguer 3 types de trames : d'information, de supervision, non numérotée (même principe que pour HDLC, voir après). Permettent une communication non connectée & sans AR (type 1), connectée avec AR (type 2) et non connectée avec AR (type 3)

Remarque : Les équipements reconnaissent le type de trame grâce au champ EtherType/Longueur : si sa valeur est inférieure à 1500, c'est qu'il s'agit d'une trame IEEE 802.3, sinon c'est une trame Ethernet V2.

HDLC (High-Level Data Link Protocol)

Protocole à fanion de bits, à fenêtre d'anticipation, de type multipoints (dissymétrique : une station primaire commande, les stations secondaires répondent) ou point à point (symétrique - les stations primaire et secondaire envoient commandes et réponses - ou dissymétrique - la station primaire commande, l'autre répond). Une variante de HDLC a été développé par les routeurs Cisco.

Fanion de début	Adresse	Commande	Données	Frame Check Sequence	fanion de fin
8 bits (01111110)	8 bits	8 bits	...	16/32 bits	8 bits (01111110)

Fanions de début et de fin (01111110) : délimiteurs de trame

Adresse : pas utilisée en liaison point à point. En liaison multipoints c'est celle d'une station secondaire (esclave) dans le cas d'une commande, et celle de la station primaire dans le cas d'une réponse.

Données : champs rempli pour les trames d'information. De longueur variable. La longueur n'a pas à être un multiple de 8 (donc pas besoin de bits de bourrage).

FCS : le Frame Check Sequence. Il est habituellement codé sur 16 bits mais après négociation peut être codé sur 32. C'est un CRC calculé sur les champs adresse + commande + données.

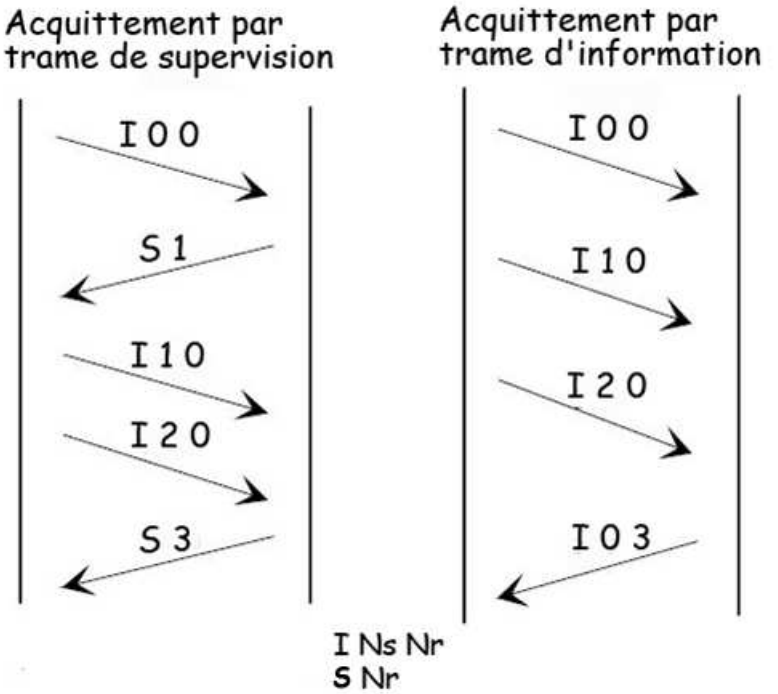
Commande : permet de distinguer 3 types de trame :

- Trames d'information (données) : transportent les données de la couche réseau. Format : **0 Ns P/F Nr**

- Trames de supervision : transportent des commandes ou des réponses liées au contrôle de d'erreur et au contrôle de flux. Format : **1 0** _ _ **P/F Nr**
RR = Receive Ready : **1 0 0 0 P/F Nr** : le récepteur est prêt à recevoir
RNR = Receive Not Ready **: 1 0 1 0 P/F Nr** : le récepteur ou la couche réseau est débordé
REJ = Reject : **1 0 0 1 P/F Nr** : demande de retransmission des trames de numéro supérieur ou égal à Nr
SREJ = Selective Reject **: 1 0 1 1 P/F Nr** : demande de retransmission de la trame numéro Nr

- Trames non numérotées : transportent des commandes et des réponses concernant la gestion de la liaison (établissement, rupture …). Format : **1 1** _ _ **P/F** _ _ _
- *Commandes* (station primaire -> secondaire)
SABM = Set Asynchronous Balanced Mode : **1 1 1 1 P 1 0 0** : demande de connexion
SABME = Identique à SABM, mais mode étendu (numéroté en modulo 128).
DISC = Disconnect : **1 1 1 1 P 0 1 0** : libération de connexion
- *Réponses* (station secondaire -> primaire)
UA = Unnumbered Acknowledgement : **1 1 0 0 F 1 1 0** : acquittement de trame non-numérotée
FRMR = FRaMe Reject : **1 1 1 1 F 0 1 1** : rejet de trame
DM = Disconnect Mode : **1 1 1 1 F 0 0 0** : connexion libérée (le terminal est déconnecté).

Ns : numéro de séquence de la trame d'information courante
Nr : numéro de séquence de la trame d'information attendue (accusé de réception jusqu'à la trame Nr-1)
P/F = Poll/Final (Commandes/Réponses) : vaut P dans une trame de commande (station primaire -> secondaire) et F dans une trame de réponse (station secondaire -> primaire). P=1 : demande de réponse immédiate ; F=1 : réponse à la demande de réponse immédiate (P=1).



Timers :

- Timer T_1 : délai d'attente d'un acquittement à l'émission d'une trame.

- N : nombre de réémissions de la même trame au-delà duquel on considère la liaison comme hors service (N=10).

- Timer T_2 : délai maximal d'attente avant d'acquitter une trame reçue ; si aucune trame I disponible, il faut envoyer une trame S.

Transparence

Comme le fanion sert de délimiteur de trame, il ne doit pas être retrouvé dans les données transportées. Pour éviter cela, deux méthodes :

- *Bourrage de bits* = Bit stuffing (méthode la plus répandue) : A l'écriture de la trame, on ajoute un 0 après une suite de cinq 1 consécutifs.

- *Bourrage d'octets* : A l'écriture, si parmi les bits de données, on rencontre la valeur du fanion 7E (01111110), on remplace celui-ci par 7D puis 5E. Du coup, il faut aussi s'assurer que la valeur 7D 5E ne se trouve pas dans les données, si c'est le cas, la valeur 7D est alors remplacé par les valeurs 7D et 5D.

Questions de cours

1) Parmi les différentes topologies de réseaux (bus, anneau, boucle, étoile, maillé, satellite), lesquelles prévoient (au niveau physique) une communication en point à point ? En multipoint ?

2) Dans un transmission entre deux machines, pourquoi y a t-il nécessité de synchroniser les horloges ? Quel genre de problème pourrait-on avoir sans cela ?

3) Dans une transmission en bande de base, est-ce que chaque signal code forcément pour un bit ? Donnez un exemple. Combien peut-on transmettre de bits avec un signal à 2 niveaux de tension ? Et 3 ? Et 4 ?

4) Dans une modulation à 2 niveaux de fréquence, 2 niveaux d'amplitude et 2 niveaux de phase, combien de bit peut-on transmettre par signal ?

5) Une voie de transmission véhicule 16 signaux distincts. Quelle est la quantité d'information binaire maximale pouvant être transportée

6) Un canal de télévision a une largeur de bande de 6 MHz. Quel débit binaire peut être obtenu sur cette liaison si un signal quadrivalent est utilisé. On suppose le canal sans bruit.

7) Soit un support de transmission caractérisé par ses fréquences extrêmes de 60 et 108 KHz et par un rapport S/B de 37 dB. Quel est le débit binaire théorique maximal de cette ligne ?

8) Entre un signal analogique et sa correspondance numérique, lequel est de meilleure qualité, en supposant dans les deux cas une transmission "parfaite" (non bruitée) ?

9) On veut numériser un signal analogique en vue d'une transmission numérique. On choisit 64 niveaux de quantification et on prend une fréquence d'échantillonnage de 1000 Hz. Combien de bits sont nécessaire pour coder chaque prélèvement ? Quel est le débit de cette transmission numérique ?

10) Multiplexage fréquentiel. Soit une voie de bande de fréquence allant de 100 à 3100 Hz (transmission analogique). Quelle principe (simple) peut-on prévoir afin de multiplexer N communications sur cette voie.

11) Dans la norme éthernet, quelles informations sont contenues dans l'appellation 10Base2 (ou 10Base5 ou 10/100BaseT ...) par exemple ?

12) Commutation de circuits, de messages, de paquets.
a) En mode commutation de circuits, les messages peuvent-ils arriver dans le désordre ? Et en mode commutation de paquets ?
b) En mode commutation de circuits, une liaison peut-elle être multiplexée ? Et en mode commutation de paquets ?
c) De la commutation de messages et de paquets, laquelle a le meilleur ratio données utiles / totalité des données transmises ?
d) De la commutation de circuits, de messages ou de paquets, laquelle permet aux messages d'arriver le plus vite possible ? Laquelle optimise l'utilisation du réseau ?

13) Pourquoi dit-on qu'un commutateur (switch) consomme t-il moins de bande passante qu'un concentrateur (hub) ?

14) Peut-on faire du filtrage d'adresse IP au niveau d'un concentrateur ? d'un commutateur ? d'un routeur ?

15) Quelle est la taille minimale d'une trame éthernet ? Et la taille maximale ?

16) Pourquoi dit-on qu'éthernet n'implémente pas entièrement la couche liaison. Quel(s) service(s) prévus par cette couche, éthernet ne rend t-elle pas ?

La couche réseau (le protocole IP)

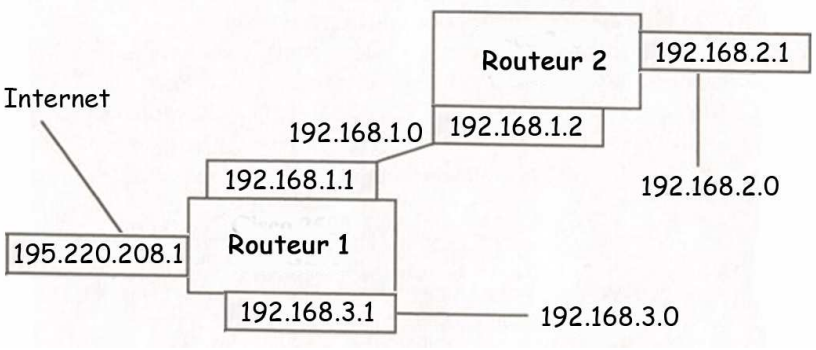
Routage IP

Le but du protocole IP est d'acheminer des messages/paquets sur Internet. Les paquets transitent par un ensemble de routeurs.

Un routeur dispose de plusieurs interfaces (cartes réseaux), chacune étant connecté à un réseau local particulier ou à un autre routeur.

le routeur qui reçoit un paquet IP le transfère soit vers un ordinateur (si celui-ci appartient à un réseau auquel le routeur est directement connecté) soit vers un autre routeur.

Chaque routeur dispose d'une table de routage. Celle-ci lui permet de savoir où transmettre le paquet.



Organisation réseau

Réseau destination	Masque de sous-réseau	Passerelle	Interface	Métrique
192.168.1.0	255.255.255.0	Direct	192.168.1.1	0
192.168.2.0	255.255.255.0	192.168.1.2	192.168.1.1	1
192.168.3.0	255.255.255.0	Direct	192.168.3.1	0
Défaut	255.255.255.0	A renseigner (routeur externe)	195.220.208.1	/

Table de routage de Routeur 1

Donc routage, 3 possibilités :

1) Le paquet est destiné à un ordinateur appartenant à un (sous-)réseau auquel le routeur est directement connecté : transfert direct vers cet ordinateur.

Exemple : Paquet d'@ IP source 192.168.3.2 et d'@ IP destination 192.168.3.3

2) Le paquet est destiné à un ordinateur appartenant à un (sous-)réseau auquel le routeur n'est pas directement connecté mais faisant l'objet d'une entrée dans la table de routage : transfert vers un routeur interne.

Exemple : Paquet d'@ IP source 192.168.3.2 et d'@ IP destination 192.168.2.2

3) Le paquet est destiné à un réseau inconnu : transfert vers le routeur par défaut.

Exemple : Paquet d'@ IP source 192.168.3.2 et d'@ IP destination 134.59.59.10

Remarque : Dans tous les cas, le paquet est encapsulé dans une trame de bas niveau avant transmission.

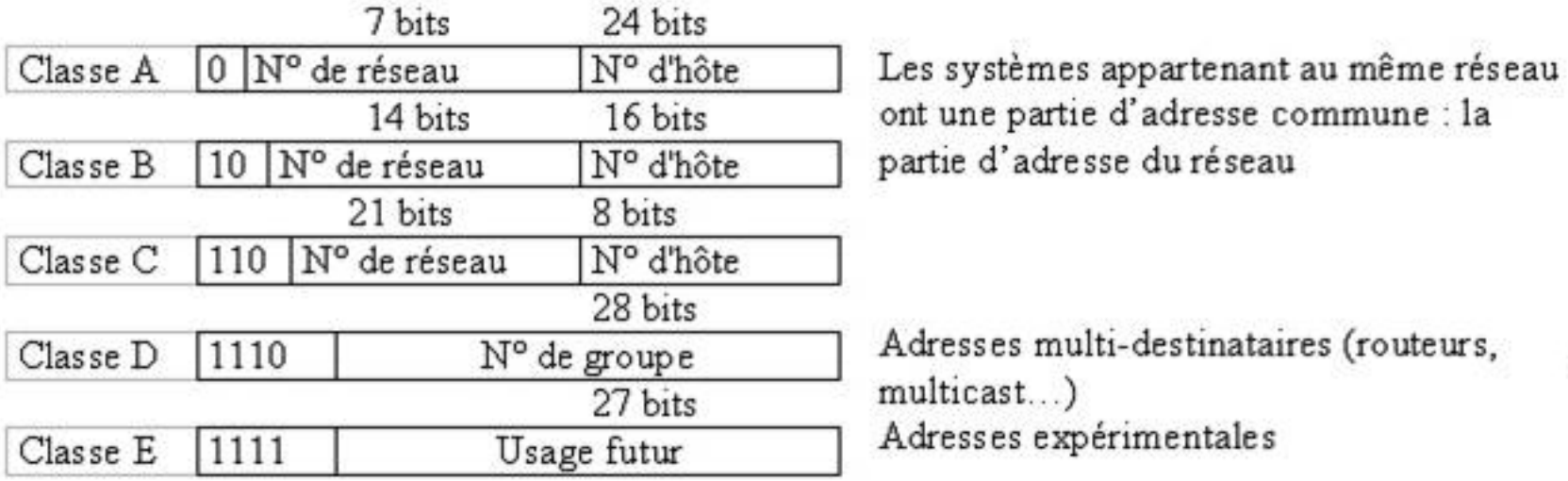
Construction et mise à jour des tables de routage. En fonction de la place du routeur dans le réseau internet, la table de routage sera construite de différentes façons :
- *Système autonome* : réseau ou système de réseaux relevant d'une même responsabilité administrative. Ex : réseau de l'université de Toulon, de Nice ...
- *Routeurs voisins internes* : routeurs appartenant au même système autonome et directement connectés.
- *Routeurs voisins externes* : routeurs directement connectés mais n'appartenant pas au même système autonome.

Si un routeur n'a que des voisins internes, alors la table de routage peut-être construite de 2 façons :
- De façon statique (manuellement) par l'administrateur système : pour les systèmes autonomes de petite taille et/ou évoluant peu.
- Dynamiquement grâce à l'utilisation d'un *IGP (Interior Gateway Protocol)* : au delà d'une certaine taille, les mises à jours manuelles sont fastidieuses et sources d'erreurs. Un IGP permet aux routeurs voisins internes de s'échanger régulièrement des informations de routage. Exemples : RIP, OSPF.

Si un routeur a aussi des voisins externes, sa table est complétée à partir d'informations échangées via un B*GP (Border Gateway Protocol)*. Exemples : XORP, BIRD.

Classes d'adresses IP

Les adresses IP (version 4) sont réparties en 5 classes. Dans les classes A, B et C, les parties de l'adresse destinées à identifier un réseau et un hôte sur le réseau sont différentes. La classe D est réservée au multicast et la classe E est expérimentale (non utilisée).



Classe A : nombre restreint de très gros réseaux (2^7 réseaux de 2^{24} -2 machines).

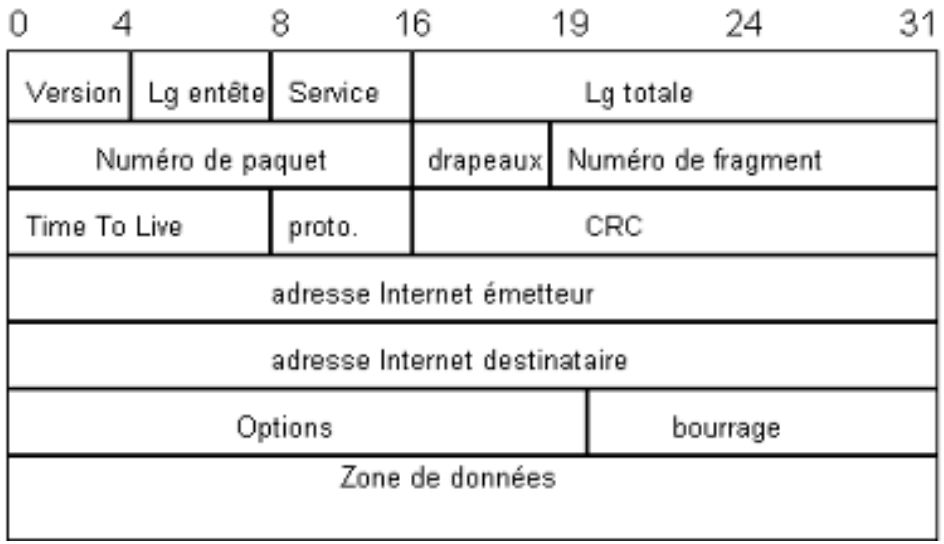
Classe C : nombre potentiellement très grand de petits réseaux (2^{21} réseaux de 2^8 -2 machines).

Masques de sous-réseau

Le système précédent manque de souplesse. On peut pallier à ce problème en utilisant des masques de sous réseau. Masque de sous-réseau : on met à 1 tous les bits de la partie 'identifiant de réseau' (par exemple pour un réseau de classe B, les 2 premiers octets) et aussi les N premiers bits de la partie 'identifiant d'hôte'

Exemple : Adresse de classe B avec 4 sous-réseaux (identifiés sur 2 bits, soit 00, 01,10 et 11) : 11111111.11111111.11000000.00000000 => Soit en notation décimale : 255.255.192.0

Paquet IP



Version : numéro de version, habituellement 4
Lg en-tête : longueur de l'en-tête, en multiple de 4 octets (pour IPv4, vaut 5 si champs *Options* vide)
Type de service : qualité de service souhaitée pour l'acheminement (priorité …).
Longueur totale : en-tête + données
Numéro de paquet (identification) : permet de reconstituer les différents fragments.
Drapeaux : indicateurs pour la fragmentation
Numéro de fragment (décalage) : 0 pour le premier fragment, 1 pour le second …
Durée de vie (TTL) : décrémenté de 1 à chaque fois que le paquet traverse un routeur ; à 0, le paquet est détruit.
Protocole : ICMP, TCP, UDP …
Options : de taille variable (éventuellement plusieurs options).
Bourrage : octets à 0 pour s'assurer que la taille de l'en-tête soit un multiple de 4 octets.

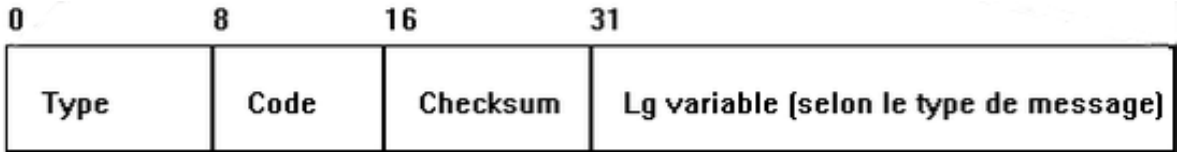
ICMP (Internet Control Message Protocol)

ICMP est un protocole de la couche réseau (3) qui contrôle les erreurs de transmission (pas leur correction). Il est encapsulé dans un paquet IP (dont la fonction est le transport de données, pas le contrôle d'erreurs). C'est donc grâce à ce protocole qu'une machine émettrice peut savoir si il y a eu un incident sur le réseau.

Pour comprendre le fonctionnement, il faut se rappeler que sur internet, la topologie est maillée. Les messages peuvent suivre différentes directions (donc différents routeurs) pour atteindre leurs cibles. De plus, le message est le plus souvent découpé à l'émission pour être reconstruit à la réception.

Ce protocole assure donc plusieurs fonctions :
- Eprouver la connectivité du réseau
- Optimiser le réseau, à une certaine échelle
- Gérer les erreurs de transmission (réseau / machine / port / … inaccessible …)

Paquet ICMP



Quelques exemples de type/code ICMP

Type 0, **Code 0** : Réponse d'ECHO (echo-reply) ; réponse au message de type 8.

Type 3, **Codes 0 à 15** : Le réseau ou destinataire inaccessible, accès interdit, service indisponible.

Code 0 : le réseau n'est pas accessible.
Code 1 : la machine n'est pas accessible.
Code 2 : le protocole n'est pas accessible.
Code 3 : le port n'est pas accessible.

Type 4, **Code 0** : le routeur ou le destinataire est saturé (vitesse de transfert trop importante / buffer de réception plein) et demande à l'émetteur de ralentir le rythme des envois.

Type 5, Codes 0 à 3 : Le routeur constate que la route empruntée par un ordinateur ou un réseau auquel est connecté ce routeur n'est pas optimale et envoie l'adresse du routeur à rajouter dans la table de routage de l'ordinateur ou des ordinateurs du réseau.

Type 8, **Code 0** : demande d'ECHO (echo-request) ; demande de renvoi d'informations, avec la commande PING par exemple.

Type 11, **code 0** & **1** : durée de vie d'un datagramme ou temps de réassemblage de ses fragments dépassé.

Type 12, **Code 0** : en-tête erroné.

Type 13, **Code 0** et **Type 14**, **Code 0** : demande d'heure système et réponse.

Type 15, **Code 0** et **Type 16**, **Code 0** : demande de son adresse IP et réponse.

Type 17, **Code 0** et **Type 18**, **Code 0** : demande de son masque de sous-réseau et réponse.

NAT (Network Address Translation)

NAT est une solution pour faire face à la pénurie d'adresses IP ; elle présente aussi un intérêt en matière de sécurité

Il existe 3 plages d'adresses privées qui ne doivent jamais circuler sur internet
- 10.0.0.0 à 10.255.255.255 (classe A)
- 172.16.0.0 à 172.31.255.255 (classe B)
- 192.168.0.0 à 192.168.255.255 (classe C)

NAT fonctionne en établissant une correspondance entre des adresses IP publiques et les adresses IP privées. Le routeur vers l'extérieur maintient 2 tables :

- Une table de traduction statique. Correspondance permanente, donc adresse publique fixe. Nécessaire pour les services internet devant être accessibles depuis l'extérieur (exemple : serveur Web).

- Une table de traduction dynamique. Pour les machines qui ne sont pas destinées à recevoir des connexions depuis l'extérieur. Lorsqu'elle voudra se connecter à l'extérieur, une adresse IP sera choisie dans un pool d'adresses disponibles (le pool est parcouru dans l'ordre croissant jusqu'à ce qu'il trouve une adresse libre de toute association). Un délai (time-out) est associé à cette entrée, l'association sera détruite si au delà de ce timeout si la machine n'a plus fait d'accès vers l'extérieur.

PAT (Port Address Translation)

Problème avec NAT : si trop de machines veulent se connecter en même temps vers l'extérieur, il risque de manquer d'adresses IP disponibles (dans ce cas, le routeur envoie aux machines en question un message ICMP indiquant que les machines externes ne sont pas joignables).

Avec PAT, ce n'est pas seulement l'adresse privée qui est traduite mais aussi le port source de la connexion. La table de traduction ne contient plus des paires @IPprivée - @IPpublique mais des quadruplets @IPprivée, PSprivé - @IPpublique, PSpublic.

Lorsque PAT est activé, la table de traduction dynamique contient maintenant une entrée par connexion. Une machine qui ouvre plusieurs connexions fera l'objet de plusieurs entrées dans la table NAT.

PAT n'affecte en rien la table des traductions statiques. Cette table contient toujours une entrée par machine.

ARP et RARP ((Reverse) Address Resolution Protocol)

Dans le cadre d'un réseau éthernet, chaque machine est connectée au réseau via une interface appelée carte éthernet. Cette carte contient une adresse physique (MAC), adresse qui est inscrite sur cette carte.

Dans le cadre d'une communication via TCP/IP, une adresse logique appelée @IP est allouée à chaque interface. L'adresse IP est gérée au niveau du système d'exploitation.

Le protocole ARP permet d'obtenir une adresse MAC à partir d'une adresse IP. Avec RARP, c'est l'inverse.

Remarque : le protocole RARP est rarement utilisé : il l'est essentiellement pour les stations de travail n'ayant pas de disque dur et souhaitant connaître leur adresse IP.

But de ARP : Permettre par exemple à une machine A située sur un réseau local éthernet d'initier une communication, Telnet par exemple, avec une machine B à partir de la connaissance de sa seule adresse IP. Rappelons que sur un réseau éthernet, les paquets IP doivent être encapsulés dans une trame éthernet et que pour cela, il faut connaître l'adresse MAC du destinataire.

Exemple avec A et B situées sur le même réseau local :

- A partir de son adresse IP et de son masque de sous-réseau, A peut connaitre l'adresse du réseau local. A partir de l'adresse IP de B, elle constate que B appartient au même réseau local.
- Pour connaitre l'adresse physique de B, A envoie alors une requête ARP en broadcast éthernet (FF.FF.FF.FF.FF.FF), c'est à dire à destination de toutes les machines situées sur le réseau éthernet (supportant le réseau logique en question) : "Qui a la machine d'adresse IP 134.59.59.5 ?" (la requête ARP est encapsulée dans une trame éthernet : elle constitue les données de cette trame).
- Toutes les machines du réseau vont donc recevoir la requête mais seule B va y répondre. Réponse ARP (après avoir récupéré l'adresse MAC de A) : "C'est moi, mon adresse MAC est 00:10:5A:AF:AB:E9".
- A peut maintenant envoyer son premier paquet de commande Telnet à destination de B.
- A l'issue de cette communication, A aura mémorisé l'adresse MAC de B dans une table ARP (cache ARP).

Si A et B ne sont pas situées sur le même réseau local

- A constate que B n'est pas sur son réseau local
- A envoie alors une requête ARP afin de récupérer l'adresse physique de la passerelle du réseau.
- A envoie ensuite son premier paquet de connexion Telnet dont l'adresse de destination éthernet (MAC) est celle de sa passerelle et dont l'adresse de destination IP est celle de B
- Ainsi de suite ...

La couche transport

A ce niveau, on décide de l'établissement ou non d'une connexion entre l'émetteur et le destinataire

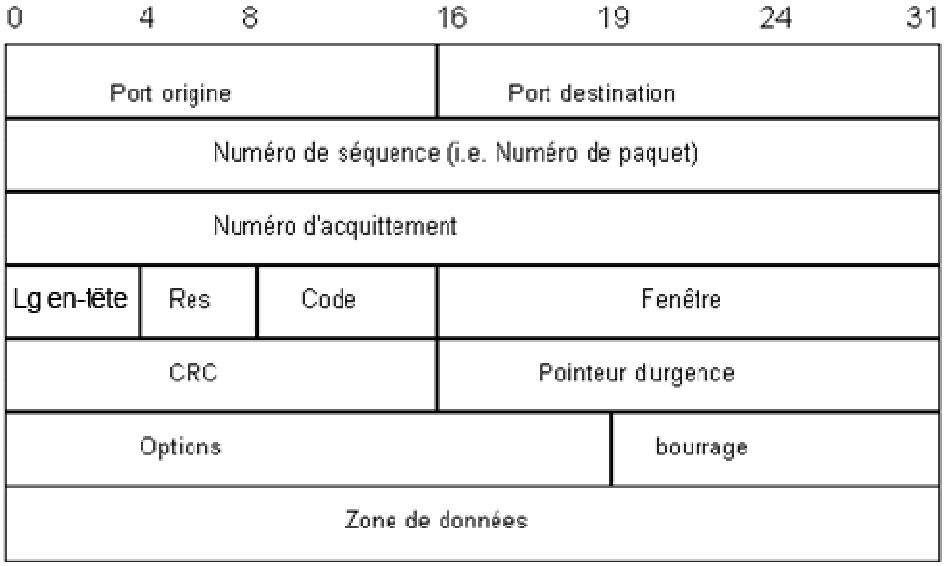
Protocole UDP/Mode datagramme (non connecté) : pas de connexion ; envoi sans savoir si le destinataire est prêt ; chaque paquet emprunte un chemin indépendant (la détermination du chemin optimal se fait pour chaque paquet) ; pas de garantie d'ordre (une remise en ordre des paquets doit être faite à l'arrivée) ; aucune garantie sur la bonne livraison des paquets (pas d'acquittement) ; pas contrôle de flux ; avantage : sa rapidité et le fait qu'il permet de faire de la multidiffusion.

Protocoles couches hautes basés sur UDP : DNS, DHCP, SNMP, NTP, RTP (protocole de transport de flux audio/vidéo en temps réel : voix, visioconf,streaming)

Protocole TCP/Mode circuit virtuel (connecté) : principe du handshake pour établir (flags SYN, SYN/ACK, ACK) et terminer (flags FIN, ACK, FIN, ACK) la connexion ; tous les paquets empruntent le même chemin réseau (un paquet de routage sans données est émis vers le destinataire (il détermine un circuit virtuel qu'emprunteront tous les paquets de la connexion) ; contrôle des pertes par numéros de séquence et d'acquittement ; contrôle de flux (taille de fenêtre) ; liaison en point à point uniquement.

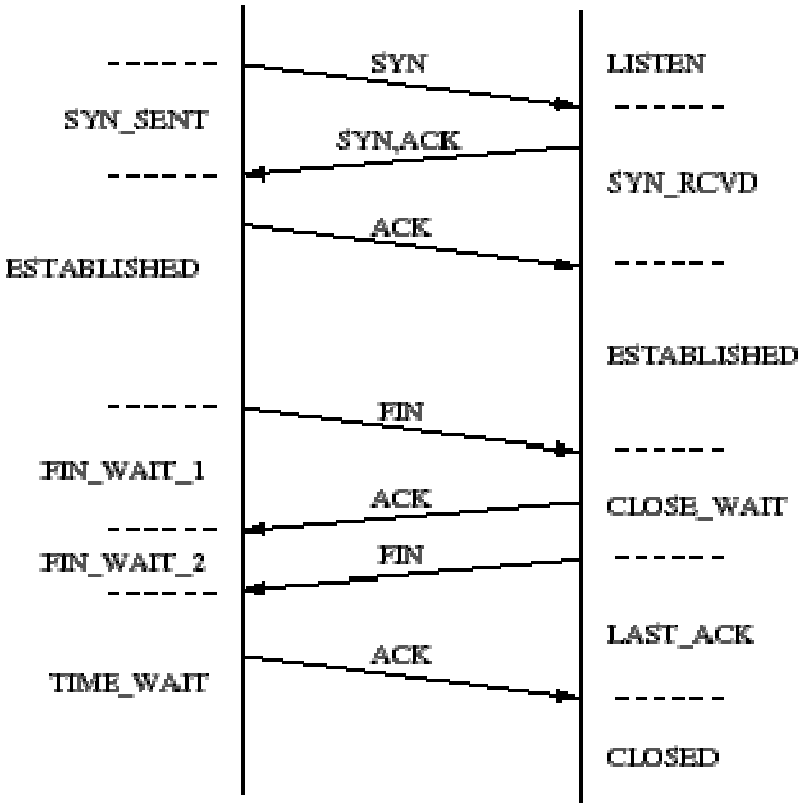
Protocoles couches hautes basés sur TCP : la plupart, dont HTTP, FTP, Telnet, SMTP, POP, IMAP.

Paquet TCP



Port origine (source) et destination : identification des processus communicants.
Numéro de séquence et d'acquittement : pour le contrôle des pertes.
Lg-en-tête : longueur de l'en-tête, en multiple de 4 octets.
Reservé : non utilisé de nos jours.
Code : contient entre autres les bits *SYN* (synchronisation : établissement d'une connexion), *ACK* (accusé de réception), *FIN* (déconnexion), *URG* (segment contenant des données urgentes) …
Fenêtre : taille de la fenêtre glissante en octets (contrôle de flux).
CRC : pour le contrôle des erreurs.
Pointeur d'urgence : si le segments contient des données urgentes et d'autres qui ne le sont pas, les premières doivent être placées au début de la zone de données et ce pointeur identifie alors leur position de fin.
Options : peut par exemple désigner une taille maximale de segment TCP (cela peut être utile pour des machines ayant de petits buffers).
Bourrage : nécessaire (car le champ *Options* est de taille variable) ; permet que l'en-tête soit un multiple de 4 octets.
Zone de données : contient le paquet IP.

TCP : connexion et déconnexion



TCP : transfert de données

Temporisation : Après l'envoi d'un segment, on attend un certain délai la réception du ACK correspondant. Si on ne l'a pas reçu, on re-transmet. Remarque : le calcul du délai utilise un algorithme adaptatif tenant compte des caractéristiques du réseau (délai moyen).

Numéros de séquence et d'acquittement : Ce sont des numéros d'octets (et plus des numéros de segments) ; Par exemple, si l'émetteur a envoyé 1000 octets avec le numéro de séquence 34570, le prochain numéro de séquence prendra la valeur 35570.

La couche session

La couche session fournit les moyens d'organiser les dialogues et l'échange de données. Par exemple, qui parle (dialogue simplex, half/full-duplex ?), comment se passe la gestion des accusés de réception.

La notion de session est également et surtout liée à celle de connexion :
- Dans certains cas, connexion et session se correspondent exactement : on peut alors parler indistinctement de connexion ou de session de communication.
- Dans d'autres cas, une connexion peut contenir plusieurs sessions : Exemple : un système de transfert de fichiers vers un serveur peut nécessiter l'établissement d'une connexion (handshake, identification, négociation de paramètres utilisateur …) ; mais en plus, au sein de cette connexion, on peut vouloir regrouper certains transferts au sein de sessions transactionnelles ; cela signifie qu'au sein d'une même session, soit tous les fichiers sont bien reçus et la transaction confirmée, soit il y a eu un problème (secteur disque défectueux par exemple) et la transaction est annulée.
- Il est aussi possible que plusieurs connexions soient nécessaires pour une même session. Par exemple, si une connexion tombe en panne ; sauvegarde et restauration du contexte de session.

La couche session est aussi associée à la notion de synchronisation : en cas d'erreur, pouvoir par exemple revenir à un état antérieur stable et connu de tous les communicants (point de reprise)

La couche présentation

Un réseau est un environnement hétérogène où les données peuvent être codées de différentes manières. Exemple : le codage des entiers Big endian/Little endian dépend du processeur, le codage des caractères dépend du système d'exploitation, la représentation de tableaux ... pourra dépendre du langage.

Nécessité d'une description de haut niveau des données échangées, donc indépendante de la représentation au niveau machine ou système : ASN 1 (Abstract Syntax Notation)

ASN englobe les notions de syntaxe abstraite et de syntaxe de transfert
- Syntaxe réelle : Représentation des données applicatives sur un hôte donné : dépend de "critères réels" : langage, système d'exploitation, processeur. Ce sont les données telles qu'elles sont codées sur une machine donnée (niveau physique/machine).
- Syntaxe abstraite : Représentation qui décrit le contenu sémantique mais qui est indépendante de tout critère réel. Données que l'on cherche à échanger (niveau conceptuel).
- Syntaxe de transfert : Représentation la plus approprié lors d'un échange entre deux parties applicatives. Souvent négociée au début d'une connexion (à une syntaxe abstraite, peut correspondre plusieurs syntaxes de transfert). Données telles qu'elles circulent sur le réseau (niveau physique/réseau).

Syntaxe abstraite ASN :

- Composants de type simple (primitif) : **BOOLEAN**, **INTEGER**, **REAL**, **UTCTIME**, **GENERALIZEDTIME**, **BIT STRING**, **OCTET STRING**, etc.

- Sous-types : par exemple, **INTEGER (3|4|6|10)**, **INTEGER (4 .. 100)**, **INTEGER (4 < .. < 100)**, etc.

- Types construits : **CHOICE**, **SEQUENCE**, **SEQUENCE OF**, **SET**, **SET OF**

- Si le composants est optionnel *:* **OPTIONAL**

- avec une valeur par défaut *:* **DEFAULT**

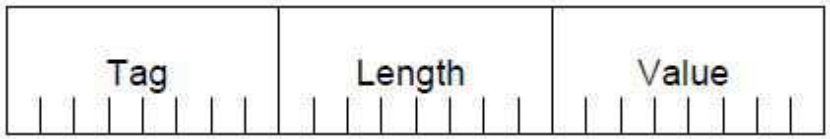
- Etiquetage : chaque type a une étiquette par défaut (par exemple INTEGER a l'étiquette 2), étiquette que l'on peut parfois être obligé de redéfinir pour lever les ambiguïtés. Etiquetage implicite *(*mot-clé **IMPLICIT***)* si la nouvelle étiquette attribuée remplace l'étiquette courante ou explicite (**EXPLICIT**) si elle s'y ajoute (EXPLICIT par défaut).

Exemple : **Quantity ::= CHOICE {**
units [0] INTEGER,
millimeters [1] INTEGER,
milligrams [2] INTEGER }

- Possibilité de définir des *Macros*, des *Modules* (sortes de meta-structures)

Syntaxe de transfert

Exemple BER (Basic Encoding Rules) :*Triplet de 3 champs T L V* ou chaque champs est un multiple de 8 bits.



- *T =Tag* : valeur d'étiquette du type (bits 1-5) + indication type primitif/construit (bit 6 : resp 0/1) + classe Universal/Application/Context-specific/Private (bit 7-8 : resp 00/10/01/11).
- *L=Length* (longueur de la valeur en octets). Si elle tient sur un octet, bit le plus à gauche à 0 et les 7 bits suivants indiquent cette longueur, sinon bit de gauche 1 et les 7 bits suivants indiquent le nombre d'octets pour coder cette longueur et si cette dernière n'est pas définie, champ L à 10000000 et on utilise un délimiteur de fin (2 octets à 0) après le champ Value.
- V= Value (valeur). Si la taille de codage n'est pas un multiple de 8 (exemple : BIT STRING '111100001'), on utilise des bits de bourrage.

Exemple : encodage de l'entier -3 (nombre négatif codé avec méthode du complément à 2)

T = 2	L = 1	V = -3
00000010	00000001	11111101

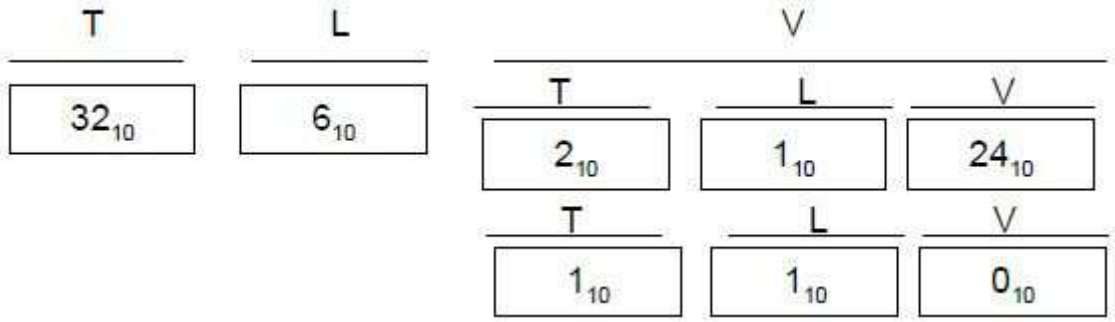
Exemple : encodage du bit string '111100001'

T	L	V		
3_{10}	3_{10}	7_{10}	11110000	1xxxxxxx

Un octet est rajouté qui indique le nombre de bits de bourrage

Dans le cas des types construits (choix, séquences, ensembles), on utilise une forme récursive de TLV (où le champ V contient lui même plusieurs triplets TLV).

Exemple : v SEQUENCE { age INTEGER, single BOOLEAN } ::= { age 24, single TRUE }



Autres syntaxes de transfert : *CER, DER, PER, XER*

Conception/développement d'une application : on commence par décrire les données utilisées sous leur forme abstraite. Un compilateur ASN est ensuite utilisé pour générer automatiquement les syntaxes réelles correspondantes + les fonctions permettant de passer de la syntaxe réelle à la syntaxe de transfert et réciproquement (fonctions de codage et de décodage).

Utilisation d'ASN : messagerie X400, système d'annuaire X500, SNMP & CMIP (protocoles d'administration de réseaux), HTTP ...

La couche application

Elle comporte des protocoles de communication de haut niveau. Cela correspond à des services réseaux directement utilisables par les applications.

Il ne faut pas confondre protocole et application :
- Une application Web (écrite en PHP …) utilise les services du protocole HTTP pour permettre la communication entre un client et un serveur Web.
- Une même application peut supporter plusieurs protocoles (ex : POP, IMAP et SMTP pour les applications de messagerie).

Quelques exemples de protocoles de la couche application

HTTP (Hypertext Transport Protocol) : protocole du Web ; communément utilisé pour faire communiquer un navigateur et un serveur Web.

FTP : (File Transfert Protocol) : protocole de manipulation de fichiers distants : création, modification, suppression … Alternatives : NFS (réseaux locaux UNIX/Linux), SMB (réseaux locaux, interopérabilité Windows/Unix) …

DHCP (Dynamic Host Configuration Protocol) : protocole prévu pour distribuer automatiquement des adresses IP aux hôtes qui en font la demande.

Telnet (TELetypewriter Network Protocol) : système permettant à un terminal virtuel d'ouvrir une session et d'exécuter des commandes à distance.

SMTP (Simple Mail Transfert Protocol) : service d'envoi de courrier électronique ; pour la réception : POP, IMAP …

POP3 (Post Office Protocol Version 3) : protocole qui permet au client de relever à distance le courrier stocké dans sa boite aux lettres

IMAP4 (Interactive Mail Access Protocol Version 4) : protocole de réception également. Il devrait prendre la place de POP3 ; il propose des fonctionnalités plus fines que POP3 qui ne permet de traiter les messages qu'une fois rapatriés localement ; il est déjà implémenté par Free

DNS (Domain Name Server) : Correspondance entre adresses IP et nom(s) de domaine dans des bases de données réparties dans le monde.

SNMP (Simple Network Management Protocol) : protocole d'administration de réseau (interrogation, configuration des équipements).

SSH (Secure Shell) : protocole sécurisé permettant d'ouvrir une connexion sécurisée sur un shell distant : il impose un échange de clés de chiffrement au début de la connexion, tous les segments TCP envoyés sont ensuite chiffrés.

NNTP (Network News Transfert Protocol) : il est utilisé pour les forums de discussion Usenet.

NTP (Network Time Protocol) : protocole horaire en réseau qui permet de synchroniser des horloges sur celle d'un serveur de temps.

HTTP

Une requête/réponses HTTP contient 2 parties : une partie en-tête (headers) et un corps (texte plat / page HTML / message XML / …).

Les principaux "en-têtes" (headers) HTTP (requête et/ou réponse) :

Content-Length : longueur du contenu
Content-Type : type du contenu
Connection : possibilité d'établir une connexion pour un ensemble de requêtes
If-Modified-Since/Last-Modified : pour les get conditionnels
Host : domaine de l'URL
Location : localisation d'une ressource créée, déplacée
Date : estampille pour les requêtes et réponses
Accept : types-MIME (formats) acceptés par le client (text/plain, text/html …)
Accept-Encoding : codages acceptés (compress, xgzip, x-zip …)
Accept-Language : liste de langages (fr, en, de …)
Accept-Charset : jeu de caractères préférés du client
Expires : date d'expiration de la représentation de la ressource dans le cache
Cache-control : date d'expiration dynamique (maintenant + …)
User-Agent : information sur l'agent utilisateur (navigateur)
Status : codes d'état de HTTP (dans une réponse)
- **1**xx : méta-données *100 : Continue (le client peut envoyer la suite de la requête)*
- **2**xx : tout va bien *200 : OK* *204 : No Content (pas de corps de réponse)*
- **3**xx : redirection *301 : Redirection* *302 : Moved Temporaly*
- **4**xx : erreur client *401 : Unauthorized* *404 : Not found* *406 : Not aceptable*
- **5**xx : erreur serveur *503 : Service anavailable*

Les méthodes de HTTP :

GET : demander une ressource au serveur,
HEAD : obtenir des informations sur une ressource du serveur,
POST : envoyer à une ressource du serveur des données pour traitement ou une ressource subalterne pour création.
PUT : ajouter ou remplacer une ressource sur le serveur.
DELETE : supprimer une ressource du serveur
OPTIONS : obtenir des informations de communication …
TRACE : demander au serveur de renvoyer dans le corps de sa réponse les en-têtes qu'il a reçu dans sa requête
CONNECT : demander à un serveur proxy de se connecter au serveur désiré (tunneling). Utile pour les connexions chiffrées de type HTTPS (HTTP +SSL/TLS)

Exemples :

PUT /mon_repertoire/mon_fichier.txt HTTP/1.1
Host: mon_serveur.com
Content-Type: text/plain
Content-Length: 44
…
Bonjour, voici le contenu d'un fichier texte

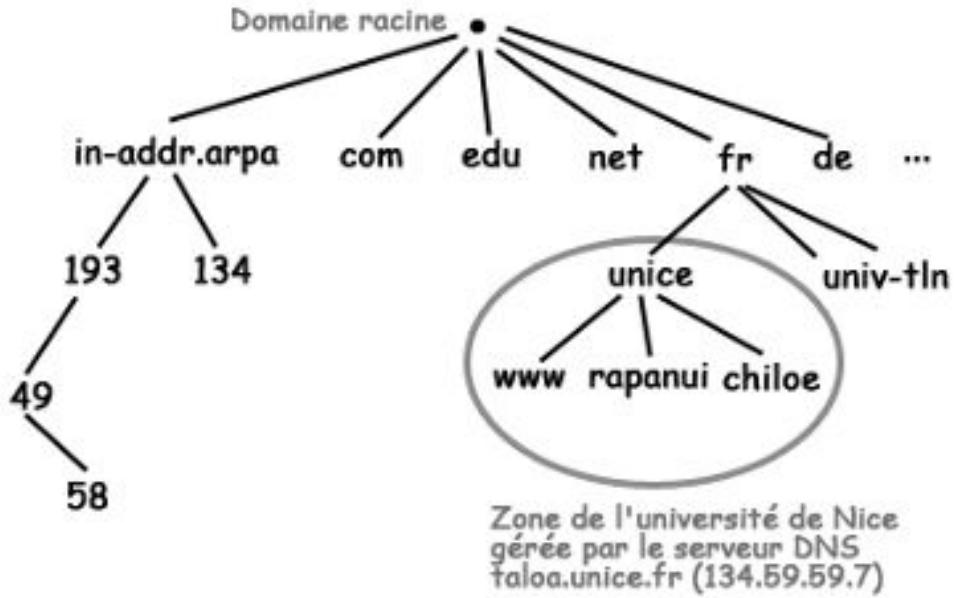
GET /mon_repertoire/mon_fichier.xml HTTP/1.1
Host: mon_serveur.com
Content-Type: application/xml

DNS (Domain Name System)

DNS permet de faire correspondre des adresses IP à des noms de domaines. A une adresse IP peut correspondre plusieurs noms de domaine, un nom principal et plusieurs alias.

Trouver l'adresse IP d'une machine à partir d'un nom consiste à effectuer une résolution de nom. Le contraire est une résolution inverse.

Architecture DNS : Base de données distribuée (chaque DNS contient une partie de la BD) et hiérarchique. Zone : partie de l'arborescence qui est gérée par un serveur.



Mécanisme de résolution :

1. DNS_A fait autorité sur la zone concernée par la requête. DNS_A consulte ses fichiers et fournit sa réponse.
2. DNS_A ne fait pas autorité sur la zone, mais la possède la réponse dans son cache. DNS_A fournit la réponse.
3. La requête concerne une machine appartenant à une zone ou DNS_A a délégué la gestion à un autre serveur. 2 cas :
- DNS_A retourne l'@IP de DNS_B au client qui soumet donc à nouveau sa requête (mode itératif).
- DNS_A devient client DNS et soumet lui-même la requête à DNS_B (mode récursif).
4. La requête concerne une machine appartenant à un domaine inconnu de DNS_A. DNS_A soumet la requête à un serveur faisant autorité sur la zone racine.

Mécanisme de résolution inverse

- Une requête du type : "Quelle est le nom de la machine d'@IP 193.49.58.8 ?" est interprété comme : "Quel est le nom de la machine de nom inverse 8.58.49.193.in-addr.arpa ?".
- Par exemple, pour le réseau (de classe C) 193.49.58.0, on créera une zone inverse dans le domaine in-addr.arpa. La zone de recherche inverse dans le domaine deviendra : 58.49.193.in-addr.arpa. Cette zone devra répondre pour toutes les adresses déclarées dans la tranche 193.49.58.0 à 193.49.58.254. On inscrira dans cette zone tous les noeuds du réseau pour lesquels on désire que la résolution inverse fonctionne.
- Une zone DNS de résolution inverse est nécessaire si vous souhaitez créer un serveur de messageries, si vous ne le faîtes pas vos emails arriveront en tant que SPAM (s'ils arrivent).

DHCP (Dynamic Host Configuration Protocol)

Permet l'attribution dynamique d'adresses IP.

Un serveur DHCP est un ordinateur serveur (la plupart des systèmes d'exploitation disposent de fonctionnalités DHCP) ou un routeur (lesquels sont souvent équipés de serveurs DHCP intégrés).

Ce serveur centralise les requêtes (généralement générées au démarrage des machines clientes) et peut fournir, en plus de l'adresse IP, d'autres informations comme l'adresse de la passerelle ou l'adresse du serveur.

La configuration du serveur DHCP comprend la définition de :
- La plage d'adresses IP gérées par le serveur) : nom, description, adresses de début et de fin, masque de sous-réseau, plages d'adresses exclues (adresses IP statiques, dont celle du serveur courant), adresses recommandées (adresse statique mais obtenue par une requête/réponse DHCP à chaque fois : évite d'avoir à gérer des plages d'exclusion, permet que les paramètres autres que l'adresse IP soient fournis par le serveur DHCP).
- La durée de bail : durée pendant laquelle l'hôte client est autorisé à utiliser l'adresse IP (par exemple 8 jours). Le client tentera de renouveler ce bail lorsque la moitié du temps sera écoulée (4 jours).
- L'adresse de la passerelle par défaut pour le réseau local.
- Le nom de domaine et l'adresse IP des serveurs DNS.

Attribution d'une adresse DHCP

Le client émet une requête **DHCPDISCOVER** en broadcast IP 255.255.255.255 (adresse généralement bloquée par les routeurs et qui concerne alors uniquement le réseau local).

Le(s) serveur(s) DHCP envoie(nt) une réponse **DHCOFFER** (en broadcast également, seul moyen d'atteindre le client) en proposant une adresse IP avec une durée de bail et en fournissant aussi d'autres informations comme le masque, l'adresse de la passerelle et du DNS, sa/leur propre adresse IP.

Si plusieurs serveurs DHCP, le client sélectionne la première adresse IP reçue et envoie une demande d'utilisation de cette adresse au serveur DHCP concerné (**DHCPREQUEST**). Envoi en broadcast pour permettre à l'ensemble des autres serveurs DHCP de retirer leur proposition.

Le serveur accuse réception et accorde l'adresse en bail (**DHCPACK**), les autres serveurs retirent leur proposition.

Renouvellement de bail

Le client va généralement tenter de renouveler son bail avant l'expiration de ce dernier si possible avec la même adresse IP. Requête **DHCPREQUEST** (cette fois-ci en unicast) et réponse **DHCPACK**.

Autres commandes DHCP

DHCPNAK : envoyée lorsque le serveur ne peut pas donner au client l'adresse IP demandée ou lorsque sa durée de bail est épuisée. Le client démarre alors immédiatement le processus pour obtenir un nouveau bail.

DHCPDECLINE : le client informe le serveur que les paramètres qu'il lui a envoyé sont invalides (typiquement l'adresse IP envoyée est en cours d'utilisation par un autre ordinateur.

DHCPRELEASE : le client informe le serveur qu'il renonce à son adresse IP et libère e bail en cours.

DHCPINFORM : le client dispose déjà de son adresse IP mais demande les paramètres de configuration locaux. Cette commande peut être utilisée par certains serveurs DHCP pour détecter les autres serveurs DHCP non autorisés.

Questions de cours

1) Classer ces paquets suivants du plus englobant au moins englobant : paquet IP, TCP, Ethernet, HTTP. Pour chacun, indiquer un ou deux champs d'en-têtes importants.

2) Citez 2-3 avantages de TCP et 2-3 avantages de UDP.

3) Avec TCP, on veut mettre place une communication entre N parties. Combien de connexions cela nécessitera t-il ?

4) Quel couple de valeurs permet d'identifier n'importe quel processus adressable sur le réseau internet ?

5) En mode connecté avec TCP par exemple, par quel mécanisme un émetteur peut-il suspecter la perte d'un message ? Et un récepteur ?

6) Au niveau bas du modèle OSI, quelle couche s'occupe d'organiser le dialogue entre deux entités communicantes ? Et à un niveau plus haut ?

7) Dans une communication réseau, quel est le problème posé par l'hétérogénéité des entités communicantes ? Quel couche du modèle OSI prend en charge ce problème ?

8) Qu'est ce que la négociation de contenu HTTP ? Citez 2-3 exemples de champs d'en-tête permettant de faire cela ?

9) Une machine A située sur un réseau local éthernet veut communiquer avec une machine B située sur un réseau distant. De quelles adresse IP & MAC a-t-elle besoin dans cette communication ?

10) a) A partir d'une adresse IP seule, peut-on connaître l'adresse de son sous-réseau (réseau local) ? Si oui, comment ?

11) A partir d'une adresse IP et d'un masque de sous-réseau, peut-on connaître l'adresse du réseau local ? Si oui, comment ?

12) A partir d'une adresse IP, peut-on savoir sur quelle classe (A, B ou C) cette adresse a t-elle été définie ? Si oui, comment ?

13) A partir d'un masque de sous-réseau, peut-on savoir sur quelle classe (A, B ou C) ce sous-réseau a t-il été défini ? Si oui, comment ?

14) A partir d'un masque de sous-réseau, peut-on connaître le nombre de machine maximal sur le réseau local ? Si oui, comment ?

15) Les masques de sous-réseau suivants sont-ils corrects ? Pourquoi oui/non ?

1. 255.255.0.0
2. 0.0.0.0
3. 255.224.255.0
4. 255.224.0.0
5. 255.255.255.255
6. 255.255.176.0
7. 224.0.0.0
8. 255.255.255.224

Remarque : 224 <=> 11100000
176 <=> 10110000

16) A partir d'une adresse de sous-réseau, peut on obtenir le masque de sous-réseau associé ?
Exemple avec l'adresse de sous-réseau 192.168.4.0 (11000000.10101000.000000100.00000000)

17) Nous disposons d'une adresse IP et d'un masque de sous-réseau.
a) A partir de ces informations (binaires), quel calcul logique permet d'obtenir l'adresse du réseau local ?
b) Même question pour obtenir l'adresse de diffusion (broadcast) sur ce réseau local.