SIMULATEUR RESEAU

OBJECTIF : ETUDE des concepts de base d'un réseau local de type Ethernet , le rôle du concentrateur, du commutateur, de la méthode d'accès CSMA/CD et du système d'adressage MAC. Il permet aussi de simuler l'interconnexion de réseaux locaux à travers des routeurs IP.

Il permet donc d'illustrer les **concepts** associés à la couche 2 et à la couche 3 du modèle OSI.

Les concepts n'approfondissent pas les différentes versions (10baset 100baset 1000baseT 10gbaseT etc...), ni les normes de câblage associées.
Tous les protocoles associés à la couche 3 ne sont pas non plus simulés par la version 1.0 (DHCP, DNS par exemple)
Le simulateur n'implémente pas le Wi-fi (802.11).

PREREQUIS
La progression proposée ici concerne la couche liaison et réseau. Elle présuppose que le modèle OSI ait été exposé auparavant mais pas forcément approfondi. Ici nous ne rentrons pas volontairement dans le détail 802 sous couche MAC et LLC qui doit être vu avec le modèle OSI.

TABLE DES MATIERES

Architecture technique d'un réseau : La couche liaison

1. Qu'est ce que la couche liaison ?

Toute communication nécessite un émetteur, un récepteur et un média de communication. Dans un réseau les émetteurs et les récepteurs sont les cartes réseaux. Le média de communication est formé par les câbles et les matériels d'interconnexion (concentrateurs et commutateurs).

Mais pour pouvoir dialoguer entre deux machines, il faut parler le même langage et respecter des règles communes de conversation : **des protocoles**.

Il n'y a pas qu'un seul protocole pour effectuer toute tâche complexe d'un réseau mais à chaque niveau de préoccupation dans un réseau correspond une famille de protocoles.

Il y a des protocoles qui proposent des services aux utilisateurs d'un réseau et des protocoles transparents aux utilisateurs qui prennent en charge les différents périphériques réseaux et rendent possible la communication.

Comme dans une communication téléphonique pour que les deux interlocuteurs puissent dialoguer dans le **langage** de leur choix du **sujet** de leur choix, il faut au préalable qu'un circuit de communication ait été établi. Ce circuit traverse différents commutateurs téléphoniques qui ont été mis en relation les uns aux autres. Chaque relation entre commutateur constitue une **liaison point-à-point** et la somme de ces liaisons constitue un **circuit**.

Dans un réseau, pour que deux machines puissent communiquer il faut aussi établir une ou plusieurs liaisons pour établir un circuit. C'est ce niveau de préoccupation, qu'on appelle **la couche liaison** (*dans le modèle OSI*), auquel on s'intéresse ici.

On veut répondre ici à cette question : comment l'ensemble cartes réseaux, câbles, concentrateurs, commutateurs est-il utilisé par les protocoles réseaux associés à la couche liaison pour établir des circuits de communication ?

Le simulateur réseau s'appuie sur une famille technologique de protocoles de la couche liaison : **Ethernet** et sur ses implémentations actuelles **(paires torsadées et commutation).**

2. Le concentrateur

Pour communiquer des postes doivent être reliés (fil ou sans fil)

En standard on relie les cartes à un boîtier d'interconnexion qui répète les signaux reçus sur un port sur tous ses autres ports.

Le concentrateur agit donc au niveau de la couche 1 du modèle OSI (couche physique).

Les cartes réseaux sont reliées aux concentrateurs par l'intermédiaire de câbles en paire torsadées ou en fibre optique. Il y a systématiquement deux voies de communication, une voie pour l'émission, l'autre pour la réception.

Si on veut interconnecter deux cartes réseaux sans concentrateur, il faut croiser ces voies. Si on veut interconnecter deux concentrateurs, il faut soit utiliser un câble croisé, soit inverser le câble au niveau du port d'interconnexion d'un des concentrateurs (*port uplink*).

Un port de concentrateur ou de commutateur est appelé un port MDI (Medium Dependant Interface). Un port MDI a le comportement suivant : ce qu'il reçoit sur sa paire d'émission il l'émet sur les paires de réception des autres ports. Il existe sur les concentrateur et les commutateurs des ports MDI-X, ce sont les ports de cascade. Le comportement d'un port MDI-X est le suivant : il croise (d'où le X), ce qu'il reçoit en émission est renvoyé en émission.
Ceci nous donne les règles de câblage suivantes :

- *Entre deux ports MDI il faut un câble croisé.*
- *Entre deux ports MDI-X, il faut toujours un câble croisé.*
- *Par contre entre un port MDI et un port MDI-X il faut un câble droit*.
- *Il existe des ports auto*-sense ou *auto-négociation* (ils s'autoconfigurent).

Un concentrateur répète ce qu'il reçoit sur un câble d'émission, reçoit le message sur tous les câbles de réception, il **diffuse**. Mais seule la carte destinataire du message le lit, ceci implique que la carte destinataire doit savoir que le message lui est adressé.

3. La trame et l'adresse du destinataire dans la trame

Chaque poste sur un réseau a donc une adresse (appelé adresse MAC *Médium Access Control*). **Cette adresse est associée à la carte réseau.**

L**e message qui circule sur le réseau contient l'adresse de l'émetteur et l'adresse du destinataire** comme une lettre postale *(le simulateur affiche la trame qui circule).*

Mais comme le concentrateur ne connaît pas l'emplacement d'un poste, pour être sûr que le message lui arrive il l'envoie à tous les postes (principe de la diffusion).

Les messages transmis entre les postes sont découpés pour pouvoir être transportés plus facilement et pour mieux répartir entre les postes le support de communication (si on ne faisait pas ça un poste téléchargeant un film de 3 heures monopoliserait le réseau).

L'unité de transfert entre poste est une **trame**, sa taille maximum d'une trame Ethernet est de **1514 octets**. Une trame est composée de l'information à transmettre (découpée) de l'adresse MAC du destinataire et de l'adresse MAC de l'émetteur (ainsi on peut lui répondre).

Ici on doit approfondir sur l'adresse MAC (Medium Access Control) et son véritable format sur 48 bits (trois octets qui identifient le constructeur et trois octets pour la carte) car le simulateur utilise des adresses « pédagogiques » (mac1, mac2, etc). On exposera aussi les adresses de diffusion (broadcast) et on évoquera l'existence d'adresses de groupe (multicast).
On doit aussi exposer le format de la trame échangée 802.3 ou DIX (Digital Intel XEROX dite aussi Ethernet II, c'est d'ailleurs cette dernière que le simulateur visualise).

4. La méthode d'accès au support : CSMA/CD

Le partage d'un même support de communication par tous les postes implique une méthode d'accès à celui-ci. En effet, comme dans une communication classique si tout le monde parle en même temps on ne se comprend pas, il faut donc régler les temps de parole. Différentes techniques sont possibles.

La technologie Ethernet se caractérise par la **méthode d'accès CSMA/CD**. Si plusieurs cartes émettent en même temps cela provoque une collision.

En effet le concentrateur réémet immédiatement la trame reçue sur un port, sur les autres ports sans vérifier s'il n'y a pas déjà une trame qui circule sur celui-ci.
Les deux trames vont se brouiller et devenir illisible, il faut donc les réémettre. La collision est renforcée par le concentrateur et par les cartes qui la détectent *(jamming*).

Les cartes réseaux à l'origine de la collision doivent pouvoir la détecter pour réémettre leur trame. Cette réémission sera faite après un temps aléatoire qui doit être différent entre les cartes (mais qui ne l'est pas toujours).

5. La détection de collision et le « round trip delay »

La carte détecte la collision sur la paire de réception, c'est pourquoi une carte réseau ne peut émettre et recevoir en même temps car sa voie de réception est monopolisée par la détection de collision, elle travaille à l'**alternat** (**half-duplex**). *Attention on verra plus loin que ce n'est plus vrai dans une architecture entièrement commutée.*

Pour pouvoir détecter la collision, la carte doit rester à l'écoute (on parle d'écoute de la porteurse) jusqu'à ce que la trame ait parcouru l'ensemble du réseau et qu'une collision qui a pu se produire à l'extrémité du réseau se soit propagée en retour jusqu'à elle.
Cela correspond en fait au délai d'aller / retour d'une trame (**le round trip delay**).

Celui-ci est déterminé par la norme ETHERNET en fonction d'une taille de trame minimale, d'un délai de répétition par les répéteurs et d'une longueur maximum de câble. Quand les normes ne sont pas respectées, une carte peut ne pas détecter une collision et des trames peuvent ainsi être perdues.

Il convient ici d'approfondir (différencier 10baseT et 100baset avec répéteur classe1 et classe2) et utiliser si cela n'a pas encore été fait l'exonet précédent.

En 10 mbps, la période d'émission d'un bit (bit time) est de 0,1 microsecondes et en 100 de 0,01 ms.

Le standard Ethernet définit un "round trip delay" maximum au sein de chaque domaine Ethernet de 576 périodes bit, ce qui correspond à 57,6 microsecondes pour 10mbps et 5,76 pour 100mbps.
576 correspond à une taille de trame minimum de 64 octets (512 bits) plus 64 bits (7 octets de préambule et un octet de délimiteur de trame). Si le temps du signal (émission sur câble plus retardement au sein des répéteurs) dépasse cette valeur, l'équipement émetteur ne peut reconnaître la collision.

Lorsqu'une carte émet une trame en 10 mbps elle écoute pendant 57,6 µs et pendant 5,76 µs en 100mbps, il faut que la collision soit détectée dans ce temps.
Entre deux trames on attend 96 bits time soit 9,6 µs.

A 200 000 km par seconde qui est la vitesse approximative de propagation on fait 200 m par microseconde soit 0,5 µs pour 100m.
*Soit 200 * 57,6 soit 11520 mètres en 10 et 200 * 5,76 soit 1152m en 100.*
Donc théoriquement si les câbles le supportent deux stations peuvent être séparées par ces distances.

*Mais l'affaiblissement sur les câbles à transmission électrique implique des distances maximums de 500m pour le coaxial épais, 185 m pour le coaxial fin et 100 m pour la paire torsadée. Les répéteurs sont donc nécessaires mais ils engendrent des délais de transmi*ssion supplémentaires.

En 10baseT la règle est la suivante :
On ne peut pas avoir plus de 4 concentrateurs séparant deux stations en 10 mbps et 500m de câble entre les stations.

En 100base T on distingue :
Les répéteurs de classe 1 qui ont un temps de retardement de 0,7 microsecondes.
Les répéteurs de classe 2 qui ont un temps de retardement de 0,46 microsecondes.
En 100mbps entre deux stations on peut avoir au plus un seul répéteur de classe 1 et 200 m de câble en paire torsadée.

En 100mbps entre deux stations on peut avoir au plus deux répéteurs de classe 2 ces répéteurs étant séparés de 5 m au maximum et chaque station étant séparée au plus de 100m du concentrateur.

Remarques:

- *Ne pas confondre cascade de concentrateurs (racks) et pile de concentrateurs (une pile (stack) de concentrateurs est vue comme un seul concentrateur, donc la règle ne s'applique pas).*

- *Avec le gigabit ethernet le délai d'écoute (round trip delay) passe à 512 octets time soit 512 * 8 = 4096 bits time. Il s'agit du délai, la taille minimum de la trame, elle ne change pas*

6. Le commutateur

Contrairement à un concentrateur, un commutateur ne diffuse pas les trames. Il met en relation les seuls postes concernés par l'échange.

Pour cela il s'appuie sur **l'adresse de l'émetteur de la trame**.

A chaque fois qu'un message lui parvient, le commutateur associe le port par lequel arrive la trame à l'adresse de l'émetteur de la trame. Ainsi après un certain nombres de trames, le commutateur connaît « l'emplacement » (c'est à dire le port de rattachement) des postes sur le réseau et peut les mettre en relation deux à deux.

Cet emplacement est géré dans des tableaux d'association « adresse MAC / port » présents dans chaque commutateur.

Avant de réémettre les trames le commutateur vérifie que le support de communication est libre. Un commutateur évite donc les collisions au contraire d'un concentrateur.

Il y a deux modes de fonctionnement du commutateur :

- *Store and forward* : il stocke les trames entièrement avant de les ré emettre. Il ne ré emet donc pas les trames erronées (CRC "Control Redundancy Check" faux) ou en collision. Par contre ces commutateurs sont plus lents et nécessitent des mémoires tampons importantes

- *On the fly* (appelé aussi *cut through* chez CISCO) : à la volée, les commutateurs réémettent immédiatement après lecture de l'adresse MAC destinataire, c'est plus rapide mais on propage les trames erronées - notamment les trames en collision et celles dont le CRC est faux.

Le commutateur permet de répartir la bande passante d'un réseau. La bande passante c'est le débit d'un réseau. En ne diffusant pas à tous les postes mais aux seuls postes concernés par l'échange, le commutateur optimise l'utilisation de la bande passante. Ainsi un commutateur 100 mb/s de 12 ports garantira 100 mb/s par port alors qu'un concentrateur 100 mb/s de 12 ports divisera cette bande passante entre tous ses ports.

7. Ethernet commuté

L'actualité des architectures réseau est **l'Ethernet entièrement commuté** et donc la disparition progressive des concentrateurs**. Si on n'a que des commutateurs, il n'y a plus de collision possible.** Car chaque port forme un mini-segment composé du commutateur et d'une carte ou aucune collision ne peut se produire.

Dans ce cas pendant l'émission d'une trame, la paire de réception n'est plus monopolisée par la détection de collision et on peut recevoir en même temps, c'est à dire travailler en mode **bidirectionnel** (***full duplex*****).**

Dans une architecture entièrement commutée on met généralement en œuvre des interconnexions redondantes entre commutateurs pour une plus grande tolérance aux pannes. Les liaisons redondantes doivent être invalidées quand elles ne sont pas utiles et validées en cas de rupture d'une liaison. Cette gestion de la redondance est prise en charge par le **protocole 802.1d (arbre de recouvrement, en anglais *spanning tree*).**

8. Les réseaux locaux virtuels (VLAN).

Les notions de port mirroring et VLAN peuvent être approfondies par l'intermédiaire des exonets (à remplir en fonction du numéro)

Avec les concentrateurs et les commutateurs de première génération, la séparation des flux gérés par la couche 2 ne peut se faire qu'en regroupant géographiquement les groupes de travail. En effet, si le commutateur segmente les domaines de collision, il maintient un seul domaine de diffusion. La séparation des domaines de diffusion exigeait, avant l'apparition des Vlans (réseaux virtuels), une séparation géographique et une interconnexion par routeur.

Un VLAN permet de créer des domaines de diffusion (domaines de *broadcast*) gérés par les commutateurs indépendants de l'emplacement où se situent les nœuds.

Les avantages des VLANs :

- réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN. Ainsi les *broadcasts* d'un serveur peuvent être limités aux clients de ce serveur.
- création de groupes de travail indépendants de l'infrastructure physique ; possibilité de déplacer la station sans changer de réseau virtuel.
- augmentation de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).

Il existe trois méthodes pour créer des VLAN :

- **VLAN de niveau 1** : on affecte chaque port des commutateurs à un VLAN. L'appartenance d'une carte réseau à un VLAN est alors déterminée par sa connexion à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN.

- **VLAN de niveau 2** : on affecte manuellement chaque adresse MAC à un VLAN. L'appartenance d'une carte réseau à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLAN en fonction de l'adresse MAC de l'hôte qui émet sur ce port. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (bien adapté à l'utilisation de machines portables).

- **VLAN de niveau 3** : on affecte un protocole de niveau 3 ou de niveau supérieur à un VLAN. L'appartenance d'une carte réseau à un VLAN est alors déterminée par le protocole de niveau 3 ou supérieur qu'elle utilise. En fait, il s'agit à partir de l'association protocole/VLAN d'affecter dynamiquement les ports des commutateurs à chacun des VLAN. Dans ce type de VLAN, les commutateurs apprennent automatiquement la configuration des VLAN en accédant aux informations de couche 3. Ceci est un fonctionnement moins rapide que niveau 2.

Une carte réseau ne peut-être associée qu'à un seul VLAN. Une carte réseau associée à un VLAN par une de ces trois méthodes ne peut communiquer qu'avec une carte réseau associée à un même VLAN. Une trame de diffusion (broadcast) émise par une carte réseau associée à un VLAN sera transmise à toutes les cartes réseaux composant ce VLAN et uniquement à celles-ci.

Protocole 802.1q : Un commutateur peut gérer plusieurs VLAN et un VLAN peut être géré par plusieurs commutateurs. L'appartenance à un VLAN, d'une trame circulant entre les commutateurs est déterminée par un « marquage » de la trame (*tag*) qui rajoute à celle-ci l'identifiant du VLAN.

Le protocole 802.1q marque les trames en modifiant l'en-tête MAC de la trame. Il ajoute notamment dans cet entête un identifiant de VLAN qui permet rapidement au commutateur d'associer la trame à un VLAN sans consulter ses tables.

Trame 802.1q

- Adresse destination : 2 octets
- Adresse Source : 2 octets
- VPID (Vlan Protocol Identifier) : 2 octets. Fixé à 0x8100. Attention à ne pas confondre avec l'identifiant d'un VLAN. Ici il s'agit d'identifier une trame de type 802.1q
- UP (User priority) : 3 bits. Permet de définir 8 niveaux de priorités. Utilisé par le protocole 802.1p.
- CFI (Canonical Format Identifier) : 1bit. indique que le format est standard (utilisé par le routage par la source)
- **VID** (Vlan Identifier) : 12 bits. Indique pour quel Vlan circule la trame.
- Longueur/type : 2 octets. En 802.3 donne la longueur de la trame. En Ethernet II ou DIX(Digital Intel Xerox) indique le type de données transporté.
- Données : 46 à 1500 octets
- FCS : 4 octets. Frame Check Sequence.

Cette modification du format de la trame est généralement faite par les commutateurs sur les liaisons inter-commutateurs (*trunk link*) en utilisant des ports spéciaux, les ports 802.1q (ports *trunk link*).

En effet, la modification de l'entête implique que les éléments recevant la trame marquée (taggée) disposent du protocole 802.1q. Ce n'est généralement pas le cas des cartes réseaux.
Les ports trunk link associés à ce type de lien ajoutent ou enlèvent le PDU (Protocole Data Unit) 802.1q selon qu'ils transmettent ou non la trame à un commutateur.

Remarque : 802.1q est basé sur un protocole propriétaire CISCO ISL (*Inter Switch Linking*) et permet également de gérer la qualité de service (QoS) par la même technique de marquage de la trame.

Le simulateur n'implémente pas le **protocole 802.1.p** qui utilise 3 bits dans la marque 802.1q pour gérer 8 niveaux de priorité.

Le simulateur n'implémente pas l'agrégation de liens. L'agrégation de liens permet de multiplexer sur un port d'interconnexion entre commutateurs les flux en provenance de plusieurs ports (par exemple un port d'interconnexion avec 1 débit d'un gigabit/s pour multiplexer les flux de ports 100mbps).

Architecture technique d'un réseau : La couche réseau

1. Introduction à la couche réseau (notion d'adresse IP).

Pour établir une liaison entre deux postes par l'intermédiaire d'un réseau mondialisé comme Internet, on ne peut se contenter du système d'adressage qu'on vient de voir.

En effet dans un réseau local, le nombre d'adresses est limité et leur modification peut être maîtrisée (changement de carte), les commutateurs peuvent donc les gérer mais ils sont incapables de gérer la totalité des adresses d'un réseau comme Internet (en 2003, 660 millions d'internautes, nombre en croissance permanente et dont l'adressage n'est pas stable). Dès lors que l'on veut relier des postes partout dans le monde il faut changer de système d'adressage

Pour réduire le nombre d'adresses à gérer il faut identifier des regroupements de postes (tous les postes d'une entreprise, d'un lycée .etc.). On peut dire que des postes reliés par des concentrateurs et des commutateurs forment une unité logique qu'on peut appelé **réseau**. Mais comment l'identifier ?

Le problème vient du fait que l'adresse MAC est associée à une carte réseau, c'est un adressage plat (non hiérarchique). Pour contourner cette difficulté, on va associer à une adresse de carte réseau (appelée adresse MAC) une adresse logique unique qui permettra d'identifier l'appartenance du poste à un regroupement appelé **réseau** (ce qu'on appelle actuellement une adresse IP).

L'adresse de réseau va être utilisée pour faire communiquer des réseaux entre eux par des matériels d'interconnexion spécifiques : les **routeurs.** Un routeur est un matériel qui permet de relier des réseaux entre eux par l'intermédiaire de leur adresse de réseau sans utiliser les adresses des cartes réseaux (hôtes) qui le composent.

Un routeur est connecté à plusieurs réseaux. L'interconnexion des routeurs entre eux permet d'interconnecter des réseaux. Pour aller d'un réseau à un autre on peut traverser un ou plusieurs routeurs.

Le niveau de préoccupation a changé, on ne s'occupe pas d'établir une liaison entre deux postes mais entre deux réseaux. On est ici dans la **couche réseau.** A noter que les routeurs ne laissent pas passer les messages en diffusion (*broadcast*), à défaut, le réseau mondial serait immédiatement saturé !

L'adressage IP permet de mettre en relation des réseaux, dans chaque réseau cependant, les commutateurs et les concentrateurs utilisent l'adressage MAC pour faire parvenir les trames aux bons postes.

Dans un réseau local les deux systèmes d'adressage sont utilisés mais cette association est transparente pour l'utilisateur. L'utilisateur ne perçoit que l'adresse réseau de son poste (l'adresse IP) voire même que le nom de son poste (adresse symbolique), ce sont les matériels d'interconnexion qui transforment l'adresse IP en adresse MAC pour répondre à leurs objectifs.

Ainsi trois types d'adressages coexistent : physique (adresses MAC), logique (adresse IP) et symbolique (nom d'hôte). Le simulateur gère ces trois niveaux d'adressage. Le protocole ARP permet de passer d'une adresse logique à une adresse physique (RARP permet l'inverse), le protocole DNS permet de passer d'une adresse symbolique à une adresse logique (et l'inverse).

2. Le paquet (datagramme)

L'unité de transmission entre carte réseau est la **trame**.
La trame est transmise d'une carte réseau à une autre en utilisant les adresses MAC destinataire et source.
Une trame ne peut être transmise à un poste se trouvant sur un autre réseau IP, car on ne peut pas connaître son adresse MAC, et quand bien même on la connaîtrait on ne pourrait pas diffuser ou commuter vers ce réseau qui peut être distant (les routeurs ne transmettent pas les diffusions).
L'unité de transmission entre réseau est le **paquet**. Un paquet contient l'adresse IP du destinataire et l'adresse IP de l'émetteur, puis les données à transmettre.
Un paquet est rangé dans une trame pour être diffusé ou commuté sur un réseau local.
L'adresse de destination du paquet permet de déterminer la route que devra emprunter ce paquet à travers les réseaux intermédiaires pour atteindre le destinataire.
L'adresse MAC destinataire de la trame permet d'établir une liaison physique entre deux postes s'échangeant des trames directement.

3. L'adresse IP

Dans la version 4 d'IP, une adresse est composée de 4 octets exprimés sous forme décimale, exemple : 10.169.27.50

Une partie de l'adresse identifie le réseau (*net-id*) et l'autre l'hôte (*host-id*). Un hôte du réseau est une carte réseau, c'st-à-dire un port conecté au réseau et actif. Un oste équipé d'une seule carte est hôte du réseau. S'il est équipé de plusieurs cartes réseau, ce poste héberge plusieurs hôtes.
Pour différencier la partie identifiant le réseau et la partie identifiant le poste, on utilise un **masque de sous-réseau**.

Le masque 255.255.255.0 associé à l'adresse 210.169.27.50 définit le poste 50 sur le réseau 210.169.27.0

Un réseau IP est en ensemble de hôtes partageant la même adresse réseau.
Pour comprendre comment on détermine l'adresse d'un réseau IP à partir de l'adresse d'un poste, il faut convertir l'adresse de l'hôte et le masque en binaire, puis appliquer l'opération ET logique (comme nous le verrons ultérieurement).

CLASSE A, B et C.

A l'origine les concepteurs d'INTERNET ont décomposé le système d'adressage pour répondre aux besoins des grandes, moyennes et petites organisations.
Classe A : le premier octet désigne le réseau et le premier bit de l'adresse est égal à zéro. Adresse : ***0****rrrrrrrr.hhhhhhhh.hhhhhhhh.hhhhhhhh Masque* ***255****.0.0.0*
Classe B : les deux premiers octets désignent le réseau et les deux premiers bits de l'adresse sont égaux à ***10****rrrrrrr.rrrrrrrr.hhhhhhhh.hhhhhhhh Masque* ***255.255****.0.0*
Classe C : les trois premiers octets désignent le réseau et les trois premiers bits de l'adresse sont égaux à 110. Masque ***255.255.255****.0*

4. Les adresses IP réservées ou interdites

Certaines adresses ne peuvent être attribuées à des postes car elles sont réservées au besoin du protocole IP.

L'adresse du réseau

Chaque réseau IP est désigné par une adresse obtenue en mettant tous les bits de la partie hôte à zéro. Cette adresse ne peut donc être attribuée à un poste.
Exemple :

200.100.40.12 masque 255.255.255.0
Le réseau désigné par le masque appliqué à cette adresse est :
200.100.40.0

Un réseau IP est identifié par son adresse.
L'adresse du réseau d'un poste est obtenue en appliquant le masque de sous-réseau sur son adresse IP à l'aide de l'opérateur logique ET (0 ET 0 = 0 ; 0 ET 1 = 0 ; 1 ET 0 = 0 ; 1 ET 1 = 1). Autrement dit, sont conservés intacts les bits de l'adresse IP qui correspondent à des bits à 1 dans le masque ; alors que sont mis à 0 les bits de l'adresse IP qui correspondent à des bits à 0 dans le masque

Seuls les hôtes appartenant à un même réseau IP peuvent communiquer directement entre eux.

L'adresse de diffusion IP (IP broadcast)

Cette adresse est utilisée pour diffuser un paquet (datagramme) à tous les postes d'un réseau IP désigné (*directed broadcast*). Elle est obtenue en positionnant à 1 tous les bits de la partie hôte (host-id).
Exemple :

200.100.40.12 masque 255.255.255.0
Le réseau désigné par le masque appliqué à cette adresse est :
200.100.40.0
L'adresse de broadcast IP sur ce réseau est 200.100.40.255

Remarque; cette adresse peut passer un routeur.

L'adresse de bouclage (loopback)

Cette adresse est utilisée pour désigner le réseau dans lequel on est (le réseau local) ou le poste sur lequel on est (la machine locale).
Il s'agit des adresses :

127.0.0.0 et 127.0.0.1

(en principe de 127.0.0.0 à 127.255.255.255)
L'adresse 127.0.0.1 est intéressante pour tester le fonctionnement de la pile IP d'un poste sans descendre jusqu'à la carte réseau et pour la communication inter-processus sur le poste qui utilise ce mécanisme. C'est une adresse toujours utilisée en interne sur le poste.

L'adresse tout à zéro

Lorsque la partie net-id ne comporte que des zéros, elle fait référence au réseau sur lequel on se trouve.
Cette adresse est intéressante dans le cas où un ordinateur veut communiquer sur le réseau qui le dessert mais qu'il n'en connaît pas encore l'adresse.
Par extension, une adresse IP « tout à zéro » dans les tables de routage désignera une route par défaut. (voir plus loin)

L'adresse tout à un

Cette adresse permet de diffuser sans préciser le réseau (*utilisée notamment par DHCP)*
Il s'agit de l'adresse 255.255.255.255.
Cette adresse n'est jamais routée.

5. Adresses IP privées et adresses publiques

Pour permettre la communication inter-réseau il faut que les adresses IP des réseaux et des postes soient uniques. Sur Internet cette règle peut être contraignante. On peut cependant utiliser en interne des adresses privées qui seront rejetées par les routeurs d'Internet.

Les adresses privées

Ces adresses sont réservées à la communication au sein d'un réseau local elle ne sont pas utilisables dans des communications sur INTERNET.
Il y a une plage d'adresses réservées dans chaque classe (A, B et C)

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255

- 192.168.0.0 à 192.168.255.255

Attribution des adresses IP publiques

Pour communiquer sur Internet les adresses publiques doivent être uniques. Il faut donc un organisme qui dirige leur attribution.
Au niveau international il s'agit de l'IANA (*Internet Assigned Number Authority*)
Il y a bien sûr des délégations au niveau de chaque pays.

6. Fixer statiquement ou dynamiquement l'adresse IP d'un poste

Une adresse IP est soit fixée par l'administrateur réseau sur le poste soit obtenue dynamiquement grâce au protocole DHCP.

Qu'est-ce que DHCP (Dynamic Host Configuration Protocol) ?
Le protocole DHCP (RFC 1533 1534) est une extension de BOOTP (RFC 1532), il gère l'attribution des informations de configuration IP en affectant automatiquement les adresses IP à des ordinateurs configurés pour l'utiliser.

Que doit fournir au minimum un serveur DHCP pour qu'un client fonctionne ?
Un poste TCP/IP doit pour fonctionner sur son réseau disposer au minimum d'une adresse IP et d'un masque de sous-réseau.
Que pourrait-il fournir en plus ?
Un serveur DHCP peut fournir toutes les informations IP complémentaires, l'adresse de la passerelle, l'adresse des serveurs DNS, l'adresse des serveurs WINS... etc

Les avantages de DHCP dans l'administration d'un réseau sont les suivants :

- La distribution d'adresses est centralisée sur un serveur ce qui permet de contrôler les différentes affectations.
- Le changement de plan d'adressage se trouve facilité par le dynamisme d'attribution. Les postes itinérants sont plus faciles à gérer.
- Enfin dans un contexte de pénurie d'adresses IP, un fournisseur d'accès par exemple attribue une adresse à la demande le temps d'une connexion et la réaffecte dès que celle-ci se libère.

Fonctionnement de DHCP
L'obtention d'un bail IP est un processus en 4 phases utilisant des paquets de diffusion (*broadcast*) :

- Demande de bail IP (DHCPDISCOVER) avec adresse IP source 0.0.0.0 et adresse IP destination 255.255.255.255 et l'adresse mac de l'émetteur
- Proposition de bail IP (DHCOFFER) les serveurs DHCP disposant d'adresses valides envoient une proposition au client avec une durée de bail et l'adresse IP du serveur DHCP
- Sélection de bail IP (DHCPREQUEST) : le client sélectionne les informations de la première proposition reçue et diffuse une demande de location de l'adresse
- Accusé de réception (DHCPACK) : le serveur répond au message, les autres serveurs retirent leur proposition.

Renouvellement de bail IP :
Lorsqu'un client redémarre, il tente d'obtenir un bail pour la même adresse avec le serveur DHCP d'origine, en émettant un paquet DHCPREQUEST. Si la tentative se solde par un échec, le client continue à utiliser la même adresse IP s'il lui reste du temps sur son bail.
Les clients DHCP tentent de renouveler leur bail lorsqu'ils ont atteint 50% de sa durée par un DHCPREQUEST. Si le serveur DHCP est disponible il envoie un DHCPACK avec la nouvelle durée et éventuellement les mises à jour des paramètres de configuration.
Si à 50% le bail n'a pu être renouvelé, le client tente de contacter l'ensemble des serveurs DHCP lorsqu'il atteint 87,5% de son bail, avec un DHCPREQUEST, les serveurs répondent soit par DHCPACK soit par DHCPNACK dans ce cas devra obtenir un bail pour une adresse IP différente.
Lorsque le bail expire ou qu'un message DHCPNACK est reçu, le client doit cesser d'utiliser l'adresse IP et retourner au processus de souscription. Lorsque le bail expire et que le client n'obtient pas d'autre adresse la communication TCP/IP s'interrompt.

Qui peut-être client DHCP ?
Tous les postes peuvent être clients DHCP sauf bien sûr le serveur DHCP. Ceci dit, cela est théorique. Certains postes "sensibles" doivent avoir des adresses statiques, les routeurs par exemple, ou les différents serveurs sur une réseau (DNS, WINS, SAMBA, PDC, BDC, ORACLE...). Pour concilier dynamisme et stabilité, on peut faire affecter par DHCP, à ces postes des adresses réservées et à bail illimité.

Tolérance de panne en utilisant plusieurs serveurs DHCP
La tolérance de panne signifie presque toujours redondance. En cas de panne du serveur DHCP (impossible pour un fournisseur d'accès), il vaut mieux disposer d'un deuxième serveur DHCP. Pour que cela fonctionne, il faut que les étendues d'adresses délivrées par les serveurs DHCP ne se chevauchent pas.
On peut avoir plusieurs serveurs DHCP sur un même réseau, ou répartis sur des réseaux différents.
On peut par exemple imaginer plusieurs sous-réseaux disposant chacun d'un serveur DHCP pour les postes du sous-réseau. Chaque serveur DHCP gère une partie d'adresses pour un des sous-réseaux adjacents.

Plusieurs serveurs DHCP sur des sous-réseaux différents
Il est préconisé que chaque serveur DHCP dispose d'une étendue pour chaque sous-réseau distant, contenant approximativement 25% des adresses disponibles pour un sous-réseau.
Mais comment un poste appartenant à un sous-réseau peut-il demander une adresse IP à un serveur situé sur un autre sous-réseau ?
Théoriquement c'est impossible, puisque DHCP fonctionne à partir de broadcast et que ceux-ci ne traversent pas les routeurs. Ce qu'il faut c'est un processus sur le réseau qui intercepte les broadcast DHCP et les "dirige" vers le serveur DHCP à travers un routeur.

Routeur et agent relais DHCP (RFC 1542)
Un agent relais DHCP relaie les messages DHCP échangés entre un client et un serveur DHCP situés sur des sous-réseaux différents.
Il est généralement installé sur un routeur. Pour pouvoir diriger les messages vers le serveur DHCP, il doit connaître l'adresse IP de celui-ci.

7. Passer d'une adresse MAC à une adresse IP (le protocole ARP)

Les cartes réseaux et les commutateurs (de niveau 2) utilisent l'adressage MAC. Une trame transmise par une carte réseau possède un entête contenant (entre autre chose) l'adresse MAC du destinataire et l'adresse MAC de l'émetteur. Ce niveau d'adressage est obligatoire, c'est celui qui permet la communication physique. C'est pourquoi on parle souvent d'adresse physique quand on parle de l'adresse MAC.

Les processus utilisent l'adresse IP qui est un paramètre dépendant de la machine et non du poste. On dit parfois que l'adresse IP est une adresse logique. Les adresses IP destinataire et source sont les champs essentiels de l'entête du paquet qui sera confié à la couche liaison pour être transmise physiquement.

Un paquet est encapsulé dans une trame pour pouvoir être adressée à une carte réseau. Cela sous-entend que l'on puisse déterminer à partir de l'adresse IP destinataire du paquet, l'adresse MAC destinataire de la trame.

C'est le protocole ARP (*Address Resolution Protocol*) intégré au protocole IP qui se charge de ce travail.

Avant de construire les trames dans lesquelles seront encapsulés les paquets à transmettre, il faut déterminer les entêtes de ces trames.
L'adresse MAC source ne pose pas de problème puisqu'elle correspond à l'adresse MAC de la carte réseau de l'émetteur. Mais l'adresse MAC destinataire, comment la connaître ?

Qui connaît sur le réseau l'association adresse IP / adresse MAC recherchée ? Le poste destinataire des trames. Il faut donc le lui demander.

Oui mais comment demander à un poste dont on ne connaît pas l'adresse MAC (on tourne en rond) ? En utilisant l'adresse de broadcast.

Le protocole ARP consiste à envoyer une trame de broadcast contenant un "request arp" : "Quelle est l'adresse MAC correspondant à l'adresse IP suivante ?"

Le poste qui reconnaît son adresse IP répond en fournissant son adresse MAC. Cette association adresse IP/adresse MAC est mise en cache et sera utilisée ultérieurement dans l'échange.

Au passage les postes qui ont reçu la demande ARP diffusée mettent en cache l'association adresse IP/adresse MAC du demandeur.

***Remarque** : le protocole ARP est souvent utilisé au démarrage d'un poste pour tester l'unicité de son adresse IP sur le réseau. En effet celui-ci envoie ce qu'on appelle un ARP gratuit qui demande la résolution de sa propre adresse, si quelqu'un répond cela veut dire que cette adresse est déjà utilisée sur le réseau. Le poste ne peut donc utiliser cette adresse*.