Niveau 3 : Réseau et adressage

Avec l'ouverture des réseaux locaux sur l'extérieur, l'adressage des réseaux locaux est passé d'une simple reconnaissance de machine à la structuration en ensembles logiques

Les réseaux sont l'interconnexion de multiples équipements, organisés selon des lieux, des services, des entreprises. Pour les mettre en communication, il faut que chacun possède un identifiant distinct, et, si possible, que cet identifiant soit structuré de sorte à distinguer l'ensemble (le réseau) et l'unité (l'hôte).

Après des années de domination du protocole IPX/SPX pour la gestion des réseaux, TCP/IP s'est imposé jusqu'au poste utilisateur.

Nous présenterons ici principalement les éléments relatifs à IP, tout en les mettant en rapport avec les autres moyens d'adresser un équipement.

Adressage dans les réseaux locaux

Au sein des réseaux locaux, le moyen de communication incontournable entre les postes est l'adresse MAC. Celle-ci permet de distinguer chaque machine de manière non ambiguë, de sorte qu'il n'est pas nécessaire d'intervenir pour qu'un poste devienne un membre actif d'un réseau. Elle est codifiée sur 6 octets comme dans les exemples ci-dessous.

0020AF41B75F	02608C7A5400	00A024594BD	02608C9ACB59

L'inconvénient majeur de cette solution est l'absence d'organisation liée à cet adressage. En effet, géré au niveau international, l'adressage MAC permet de donner des informations sur le fabricant de la carte, sur la série ou le numéro de composant, mais il ne peut être utilisé pour réaliser une affectation personnalisée des adresses aux équipements présents sur le réseau.

De plus, il est impossible de mettre en relation l'ensemble des matériels informatiques déployés dans le monde sur la seule base d'une information aussi peu significative. Aucun matériel ne pourrait efficacement retenir la localisation de plusieurs milliards d'équipements interconnectés.

Enfin, l'absence d'organisation logique dans cet adressage n'autorise pas la communication d'ensemble à ensemble (un réseau vers un autre), ce qui complique grandement les possibilités d'organiser les communications.

Adressage de niveau 3

C'est pourquoi les concepteurs de réseau se sont penchés sur la possibilité de structurer les différents ensembles d'une manière plus intelligible.

On parlera d'adressage logique, situé au niveau 3 du modèle OSI. On devra réaliser l'acheminement d'information selon cette organisation logique par le biais de la technique de routage, puis terminer l'échange d'équipement physique à équipement physique par le biais de l'adressage de niveau 2.

I Principes

L'adressage logique permet de distinguer les sous-ensembles que sont les réseaux. Toutefois, il n'est pas intelligible aux utilisateurs

La constitution d'un adressage routable repose sur la possibilité de reconnaissance des ensembles, et de traitement des informations par des matériels. Toutefois, pour rendre l'information intelligible aux utilisateurs, des niveaux supérieurs ont été ajoutés.

1.1 Adressage logique et logique d'adressage

La mise en place d'un adressage logique nécessite que celui-ci soit :

- Intelligible, aussi bien au niveau de la machine que pour un administrateur, ce qui n'est pas le cas de l'adresse MAC,
- Paramétrable, c'est à dire non figé sur un matériel
- Évolutif, permettant de changer l'adresse d'une machine, d'augmenter le nombre de matériels dans un réseau, etc
- Numérique, de sorte à pouvoir opérer des traitements simples, ou à les faire réaliser par des circuits électroniques (carte réseau, SE, routeurs).

Pour qu'une logique se dégage d'un tel adressage, il faut que l'on puisse distinguer l'ensemble (ou réseau) de l'équipement (ou hôte) et les ensembles entre eux. Les adressages logiques comportent donc une partie réseau et peuvent utiliser différentes possibilités pour la partie machine :

- IP inclue dans sa numérotation la partie machine et sépare les deux composantes par un masque
- IPX utilise l'adressage MAC pour distinguer les postes.

1.2 Adresses routables et routage

À partir du moment où un adressage peut être interprété selon une logique d'ensembles, on peut se préoccuper de l'acheminement d'une information d'un ensemble à un autre. On parle de Routage. Le principe repose sur une connaissance a priori des différentes routes possibles par les matériels d'acheminement : les routeurs.

L'ensemble de ces informations est stocké dans une table de routage.

IP, la référence

Devenu **LE** protocole d'interconnexion des réseaux informatiques, IP (Internet Protocol) est issu des travaux de l'armée américaine pour produire un système de communication susceptible de pouvoir acheminer un message sur n'importe quel type d'infrastructure, en autorisant le choix d'un trajet dynamique en fonction des disponibilités des différentes interconnexions.

Avant d'avoir subi une normalisation par l'IETF (Internet Engineering Task Force), TCP/IP était devenu un standard de fait, grâce à la simplicité de sa mise en œuvre et au déploiement intensif des réseaux sous serveur Unix (à l'époque où SNA d'IBM, IPX/SPX de Novell occupaient le marché).

L'ensemble des spécifications de TCP/IP et des protocoles qui lui sont associés (on parle de Pile TCP/IP, comprenant notamment ARP, DHCP, DNS, TELNET, HTTP, FTP….) sont définis dans des RFC (Request For Comment), qui sont les principes de mise en œuvre de ces différents outils.

IP offre deux fonctionnalités étroitement liées : l'adressage réseaux/hôtes et la fonction de routage (acheminement et communication entre routeurs). Une fiche traite spécifiquement du routage IP.

1.3 Les niveaux d'adressage et les protocoles de traduction

A différents niveaux, la reconnaissance des équipements nécessite un système d'adressage : MAC, IP, FQDN, Netbios sont autant de moyens de reconnaître une machine. Chacun répond à des besoins spécifiques.

- MAC : reconnaît la carte réseau en tant que matériel
- IP distingue logiquement un poste
- NETBIOS : nom d'une machine dans un réseau Windows
- FQDN (Fully Qualified Domain Name) : donne un nom lisible à une machine sur un réseau IP grâce à un serveur DNS

II IPv4 (Internet Protocol Version 4)

Apparu dans les années 70, l'adressage IPv4 est toujours la solution actuelle d'identification des postes sur les réseaux locaux. IPv6 est l'adressage des interconnexions réseau en attendant son extension sur le LAN.

2.1 Caractéristiques

Défini dans la RFC 791 et mis à jour dans la RFC 1349, IP est un protocole :

- point à point : il est donc étudié par chaque matériel de niveau 3 traversé, et pas seulement par les éléments terminaux de la communication. Le contenu peut être modifié par les intermédiaires (NAT, Proxy, Qualité de Service, VPN etc).
- sans contrôle d'erreur sur les données : une erreur est donc propagée. On considère que ces fonctions de contrôle doivent être réalisées au niveau 2 (pour les intermédiaires) ou 4/5 pour l'équipement terminal. Toutefois, un contrôle d'erreur est fait sur les entêtes, nécessaire pour véhiculer l'information vers un destinataire correct.
- sans contrôle de flux (non sécurisé) : aucune fonction ne permet d'adapter les échanges ou de gérer la congestion, ni de vérifier l'arrivée ou la perte de paquets. Cela est renvoyé au niveau des protocoles inférieurs ou supérieurs.

2.2 Datagramme IP

Il s'agit du paquet manipulé à ce niveau.

- Taille : jusqu'à 4096 octets
- En-tête : contient, entre autres
    - le numéro du paquet
    - le numéro du fragment, en cas de redécoupage (voir 2.3)
    - TTL (time to live) : nombre d'intermédiaires traversables avant que le paquet ne soit considéré comme perdu (dans une boucle par exemple). Permet de faire de la prioritarisation
    - Adresse IP de l'émetteur et du récepteur
    - Protocole de niveau supérieur
- CRC (Circular Redundant Check) zone de contrôle d'erreur sur l'entête (pas sur les données)
- Données : informations transmises par les couches supérieures

2.3 Fragmentation

Lorsque les informations lui parviennent de la couche 4, IP peut les séparer en éléments plus petits pour respecter les contraintes du réseau vers lequel il les envoie.

Cette fragmentation d'un segment TCP, par exemple, nécessite une numérotation de chacun des fragments pour que la couche IP de la machine réceptrice puisse recomposer les datagrammes initiaux.

III Adressage IP

L'organisation de l'adressage IP a débuté par un découpage en classe qui a été progressivement abandonné pour faire face à une demande croissante en adresses pour tous les équipements (entreprises, particuliers, mobiles, etc)

Pour que le travail IP puisse fonctionner, le recours à un adressage logique a été défini. Nous allons étudier ici l'adressage IPv4.

La partie IPv6 est décrite ailleurs.

3.1 Adressage IP et classes

Les adresses définies par le protocole IP comportent 4 valeurs numériques sur un octet.

10	70	27	244

Ces adresses sont constituées de deux parties :

- l'identification du réseau, sur 1, 2 ou 3 octets
- l'identité de la machine dans ce réseau, sur 3, 2 ou 1 octets.

Elles ont été découpées en trois classes principales, permettant de proposer un nombre de réseaux conséquents, et des tailles de réseaux plus ou moins étendues selon les besoins.

Les classes A, B et C ont été construites selon un découpage binaire : la première moitié des adresses (128 valeurs, bit de poids fort à 0) est de classe A, la seconde est pour le reste. On procède à

nouveau à un découpage de la partie restante, une première moitié devient la classe B (64 valeurs, 2 premiers bits à 10). La classe C occupe les 32 valeurs suivantes (3 premiers bits à 110). Voir illustration ci-dessous.

Les classes D et E correspondent respectivement à une adresse commençant par 1110—- et 11110— et ne sont pas utilisées pour la gestion des machines mais pour le multicast ou la gestion des groupes (IGMP)

Deux machines présentes sur une infrastructure IP publique ne peuvent avoir la même adresse IP.

Adressage Unicast, Multicast et Broadcast

Quel que soit le niveau auquel on se situe (IP, MAC, mail, etc), l'expédition d'une information peut se faire vers un destinataire unique (unicast : machine, mail), vers un ensemble d'abonnés (multicast : liste de diffusion, visioconférence) ou vers l'ensemble des équipements présents dans un espace donné (broadcast : DHCP, ARP).

Association IP et MAC : ARP

Pour un utilisateur ou un matériel, l'adressage le plus couramment utilisé est le plus significatif : l'adresse IP (du routeur, du serveur DNS, d'un composant réseau, d'un serveur, etc).

Toutefois, nous avons vu qu'il faut s'adresser au matériel par son niveau 2 (MAC) pour qu'il sache qu'il est destinataire d'une trame.

Le protocole ARP (Address Resolution Protocol), fait une demande à la cantonade (broadcast) pour connaître l'adresse MAC correspondant à un composant connu par son adresse IP (par exemple son routeur ou son serveur DNS).

Tout matériel est destinataire d'un broadcast MAC, donc chaque poste, reçoit la trame.

La réponse (ARP-Reply) est retournée par le seul composant étant aussi destinataire IP.

Cette étape est préalable à tout échange entre un matériel et son prochain.

3.2 RFC 1597 et 1918 : l’adressage privé

La RFC (Request For Command) 1597, préconisation établie par l’IETF en 1994, présente une solution permettant de pallier le manque de disponibilité d’adresses IP de classe A et B et la multiplication des sites équipés (entreprises, particuliers).

En effet, nombre d’organisations disposent d’un parc de machines sur un même réseau plus important que les seules 254 offertes par les adresses de classe C.

Elle a été mise à jour par la RFC 1918 en 1996.

On a observé que les entreprises ont besoin d’une large plage d’adresses pour la communication interne, et que les faits suivants sont aussi vrais :

- peu de machines auront un besoin simultané d’accéder à l’extérieur, l’essentiel du trafic

s’effectuant en interne,
- quand bien même tout le monde peut avoir un besoin d’accéder aux fonctions de courrier électronique, un seul poste pour l’ensemble de l’organisation nécessite une adresse IP unique sur Internet,
- la plupart des compagnies utilisent un Firewall (pare-feu) entre l’internet et le réseau interne, seule porte ouverte directement sur l’extérieur.

Cela a amené les penseurs d’internet à la conclusion suivante : une entreprise n’aura besoin que d’une plage restreinte d’adresses uniques sur le Web (adresses pouvant communiquer sur le réseau des réseaux) relevant de la classe C, et en interne d’une plage plus importante (classe B ou A).

La fonction de translation d’adresses (étudiée dans la fiche sur le routage), généralement fournie avec le logiciel d’un routeur, suffira à faire la communication entre le réseau interne et l’extérieur.

La RFC 1597 réserve donc une plage d’adresses pour une utilisation privée (uniquement en interne), ces adresses ne pouvant être valides sur l’Internet. Le routeur saura donc s’il doit ou non établir une translation lorsqu’il reçoit un message à orienter.

Les plages d’adresses privées sont indiquées dans le tableau ci-dessous.

Nombre de bits d’adresse	**Nb réseaux Classe**	**Plage d’adresses IP De …A**
24	1 / Classe A	10.0.0.0 … 10.255.255.255
20	16 /Classe B	172.16.0.0 … 172.31.255.255
16	256 / Classe C	192.168.0.0 … 192.168.255.255

Toutes les autres adresses sont publiques, mais certaines valeurs ont des usages réservés.

3.3 Adressages spéciaux

Un certain nombre d’adresses est réservé à des usages spécifiques (voir RFC 3330 pour toutes les valeurs réservées).

- L’**adresse de réseau**, pour une classe donnée, met à 0 tous les bits de l’hôte (les bits réservés à l’adresse de la machine)
- L’**adresse de diffusion**, qui permet, dans un réseau donné, d’adresser un message unique à toutes les machines, met à 1 tous les bits de l’hôte
- L’**adresse de bouclage** ou **Loopback** (RFC 1700) qui permet à une machine de remonter l’information vers les couches hautes du modèle OSI : 127.0.0.1. Le numéro de réseau 127.0.0.0 est entièrement réservé à cet usage.
- L’**adressage multicast** (RFC 3171) permettant d’expédier un message à plusieurs destinataires en un seul envoi ; utilise notamment le réseau n° 224.0.0.0
- L'**adressage de lien local** (RFC 3927) ou **APIPA** : Lorsque l'adressage est distribué par un serveur DHCP, la défaillance du serveur empêche les postes de pouvoir communiquer sur le réseau local. Pour limiter l'impact négatif de la panne du serveur, un poste peut s'auto-configurer sur un adressage réservé à une communication interne au format 169.254.0.0/16. Le poste s'attribue une adresse, demande si quelqu'un l'a déjà et, si ce n'est pas le cas, la conserve.

3.4 Masque de réseau

Les classes IP déterminent donc la portion attribuée au réseau et aux hôtes. Pour assurer une séparation plus souple que celle définie par la classe, on utilise une information supplémentaire nommée Masque de réseau. Le masque indique les positions binaires d'une adresse qui font partie du numéro de réseau

Ce masque permet aussi à une machine de savoir si une adresse réseau manipulée est dans le même réseau qu'elle (pour le routage notamment).

Utilisation du masque

On compare deux adresses IP (a1 et a2) à travers un masque (m). Chaque bit du masque à 1 demande de vérifier la correspondance binaire entre les bits correspondants des adresses a1 et a2. en cas de concordance, les deux adresses sont sur le même réseau.

Pour parvenir à comparer les adresses, une machine procède par l'application d'un ET logique entre chacune des deux adresses et le masque. Le résultat obtenu doit être identique.

C'est seulement en l'absence d'indication qu'on applique le masque standard de chacune des classes comme suit :

Classe	Masque standard	Explication
A	255.0.0.0	1 seul octet significatif pour déterminer le réseau
B	255.255.0.0	2 octets significatifs
C	255.255.255.0	3 octets significatifs

Mais la configuration d'une machine doit nécessairement indiquer la valeur du masque. Les outils de configuration proposent le masque de classe par défaut.

3.5 Masque de sous-réseau

Lorsque l'on se trouve dans un réseau donné, déterminé par son adresse IP et son masque, on peut tout de même vouloir organiser des sous-ensembles distincts.

Pour cela, il faut prolonger le masque de réseau en monopolisant quelques bits assignés aux machines pour séparer les sous-ensembles : on constitue un masque de sous-réseau.

On déterminera le nombre de bits nécessaires pour la partie sous-réseau en encadrant le nombre de sous-réseaux par les puissances de 2 les plus proches et en retenant la puissance la plus haute.

IV Adressage « classeless » CIDR

Avec la multiplication des intervenants (opérateurs télécom, opérateurs mobiles, grandes entreprises, etc) sur les accès au réseau des réseaux, la notation historique de l'adressage IP et son découpage en classes est devenu trop restrictif.

Avant la mise en place définitive de la version 6 du protocole qui porte la taille des adresses à 128 bits (16 octets), des assouplissements ont été apportés à l'adressage, qui permettent de distribuer des valeurs moins ou plus grandes que les adresses organisées en classes, et assure une simplification des tables de routage.

4.1 CIDR (Classeless Inter Domain Routing)

En le déconnectant de la notion de classe (classeless), les concepteurs d'internet ont donné à l'adressage IP une plus grande souplesse et une capacité à organiser les ensembles au plus près des besoins. Au même titre que les sous-réseaux dans un réseau, il s'agit de jouer sur le masque en le gérant bit à bit et non plus par paquet de 1, 2 ou 3 octets.

Aujourd'hui, l'ensemble de l'adressage au cœur des réseaux est classeless.

Notation CIDR

La première étape de simplification a été de remplacer le masque de réseau/sous-réseau par un nombre de bits. Ainsi, le masque standard de classe B (255.255.0.0) se notera /16 (sur 16 bits). Le masque calculé dans l'exemple du 3.5 sera noté /27.

Aujourd'hui, les FAI français (par exemple) ont comme plages d'adresses IP :

- Free : 62.147.0.0/16, 78.192.0.0/10, 81.56.0.0/15, etc
- Neuf/SFR : 195.3.0.0/18, 212.30.96.0/19, 62.106.128.0/17, etc

4.2 Sur réseau

Lors de l'attribution des adresses de réseau, on s'arrange pour distribuer des ensembles consécutifs à un même opérateur. Cela permet de joindre par un cheminement unique cet ensemble de valeurs contiguës regroupées derrière une point de passage unique (la porte d'entrée de l'opérateur).

Dès lors, on pourra diminuer le nombre de lignes dans une table de routage en rassemblant plusieurs lignes consécutives accessibles par un même trajet (on passe par la même passerelle) en les adressant par le biais d'un masque de sur-réseau adapté.

Ce masque de sur-réseau vise à regrouper les lignes présentant une combinaison binaire identique sur une portion de bits de la partie réseau. On pourra regrouper un ensemble d'adresses de réseau contiguës (on ne s'occupe pas de la partie machine) ayant une partie commune sur les bits de poids fort et représentant toutes les combinaisons de 0 et de 1 sur la partie de poids faible des numéros de réseau.

Pour le routeur central du schéma ci-contre, toutes les lignes derrière le routeur terminal correspondent à un trajet unique. Elles peuvent être regroupées dans la table de routage du routeur central si elles ont des parties binaires communes.

Un sur-réseau regroupe toujours un nombre de réseaux multiple d’une puissance de 2.

4.3 VLSM (Variable Length Subnet Mask)

Si, dans l'adressage historique basé sur les classes, les sous-réseaux sont basés sur un masque commun, l'approche CIDR va permettre de faire des sous-ensembles plus souples, en procédant à l'image du découpage en classes. On pourra alors créer des sous-réseaux permettant d'organiser des ensembles de machines de taille variable grâce à un masque de sous-réseau de taille variable (VLSM).