SIN 1 : Maquettage d'une solution en réponse à un cahier des charges

Module SIN 1.2 : Concevoir un système local et permettre le dialogue entre l'homme et la machine

Ressources sur : Les Réseaux / Protocole TCP/IP

Sommaire

1. Les réseaux

a) Définition

Un réseau est un ensemble de nœuds (routeurs, commutateurs, …) et de liens filaires (cuivre et optique) et/ou sans fil, sur lesquels circulent des flux (souvent binaires, et structurés selon des protocoles).

Ces réseaux relient des **Objets Techniques Communicants (OTC)** tels que des ordinateurs, des téléphones, des *smartphones*, des télécopieurs, des consoles de jeux, etc. … pour leur permettre de communiquer entre eux.

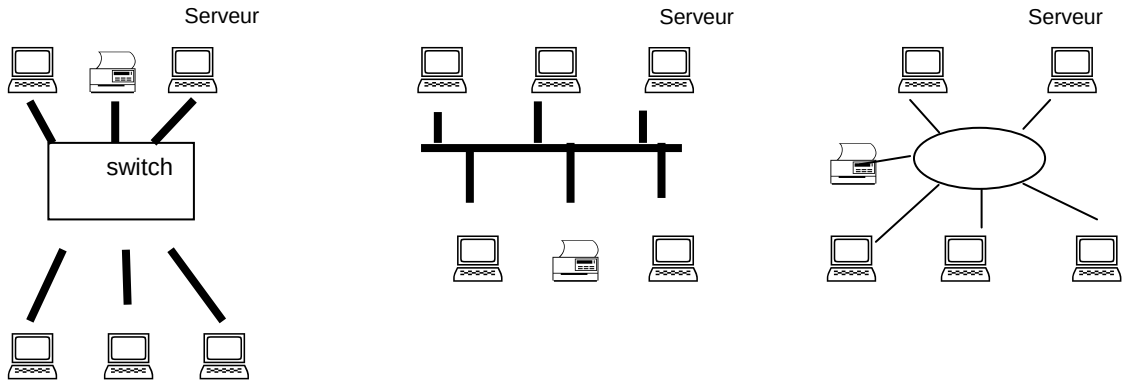
b) Classification des réseaux (voir cours ET234-2)

Les WAN [Wide Area Network] : réseau étendu, national ou international. Regroupe des entités géographiquement très éloignées les unes des autres (plusieurs centaines ou milliers de kilomètres). Ce type de réseau utilise des communications via des fibres optiques (monomodes en général).

Les MAN [Metropolitain Area Network] : réseau regroupant des entités situées dans la même métropole (plusieurs kilomètres). Ce type de réseau utilise des communications via des fibres optiques (multimodes en général).

Les LAN [Local Area Network] : réseau regroupant des entités situées dans le même bâtiment ou dans des bâtiments voisins (plusieurs centaines de mètres). Ce type de réseau utilise des communications via des fibres optiques et des paires torsadées.

c) Les différentes topologies de réseaux



Etoile **BUS** **En anneau**

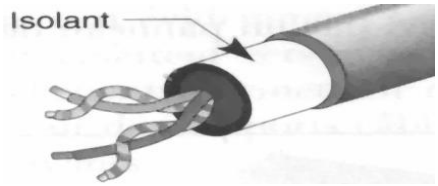
Remarque : Les réseaux sans fils de norme Wifi, normalement en topologie étoile, répondent aux normes EEE802.11 avec des débits de 5Mbits/s (a) 11Mbits (b) à 54Mbits/s (g) à 2,4GHz.

Les réseaux sans fils de norme Bluethooth personnels (PAN), normalement en topologies étoile et maillée (selon mode de fonctionnement), répondent aux normes EEE 802.15.

2. Architecture matérielle des réseaux (voir cours ET234-2)

a) Les liens : la paire torsadée

Elle est composée de paires de fils de cuivre, elle est généralement munie d'un blindage électromagnétique à base de cuivre ou d'aluminium. Elle est peu onéreuse, on la trouve dans les LAN, la vitesse de transmission est faible (100 MHz), la distance entre 2 nœuds ne dépasse pas 100m.



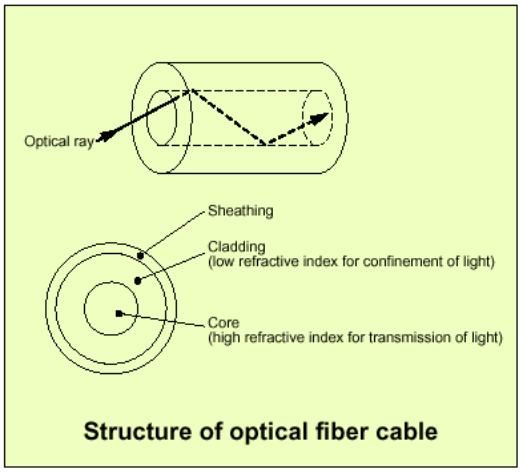
b) Les liens : le câble coaxial

Il est muni d'un blindage électromagnétique à base de cuivre ou d'aluminium. Il est plus onéreux que la paire torsadée, on le trouve dans les LAN. Il est en perte d'utilisation.

c) Les liens : La fibre optique

Une fibre optique est constituée de 3 éléments :

- un fil de silice appelé cœur de très faible diamètre (de l'ordre de la longueur d'onde du signal transmis ;
- une gaine appelée manteau qui entoure le cœur ;
- une enveloppe de protection.



Les rayons lumineux injectés dans le cœur se réfléchissent sur la gaine. Il y a donc propagation de la lumière à travers la fibre. Afin d'assurer une réflexion totale, l'indice de réfraction du cœur est supérieur à l'indice de réfraction de la gaine. L'enveloppe n'a qu'un rôle de protection mécanique de la fibre.

Il existe deux grandes familles de fibres optiques multimodes : les fibres à saut d'indice et les fibres à gradient d'indice.

La fibre optique est peu sensible aux perturbations électromagnétiques. Elle est sécuritaire : il est difficile de brancher une écoute sur la fibre sans être détecté (chute du signal et donc localisation aisée).

d) Les nœuds: le hub ou concentrateur

Par définition c'est un lieu où est rassemblé plusieurs éléments, dans les réseaux il s'agit en fait de répéteur multi port ou multipoint, il permet la régénération et la mise en forme du signal électrique. Le hub tant à disparaître.

e) Les nœuds : Le commutateur

C'est un répéteur multipoint « intelligent ». Il permet la régénération et la mise en forme du signal électrique et se souvient du chemin entre 2 équipements : il est en effet capable de d'ouvrir la communication entre 2 éléments quand elle est nécessaire et de la fermer quand il n'y a plus de besoin.

Le commutateur agit sur les couches physique et liaison du modèle OSI, il filtre et transfère les trames de données en fonction de l'adresse de destination de chacune d'elles. Il peut posséder une extension par fibre optique.

Commutateur
LAN

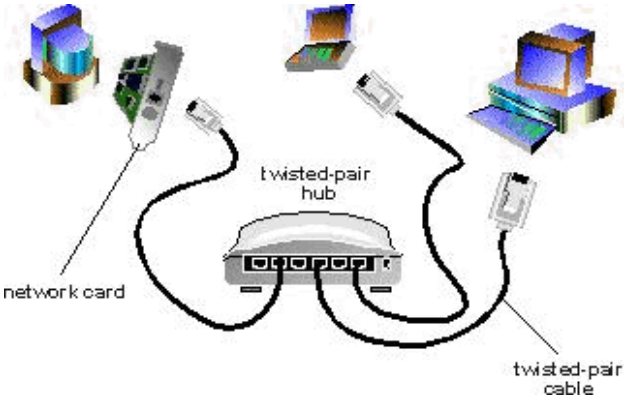


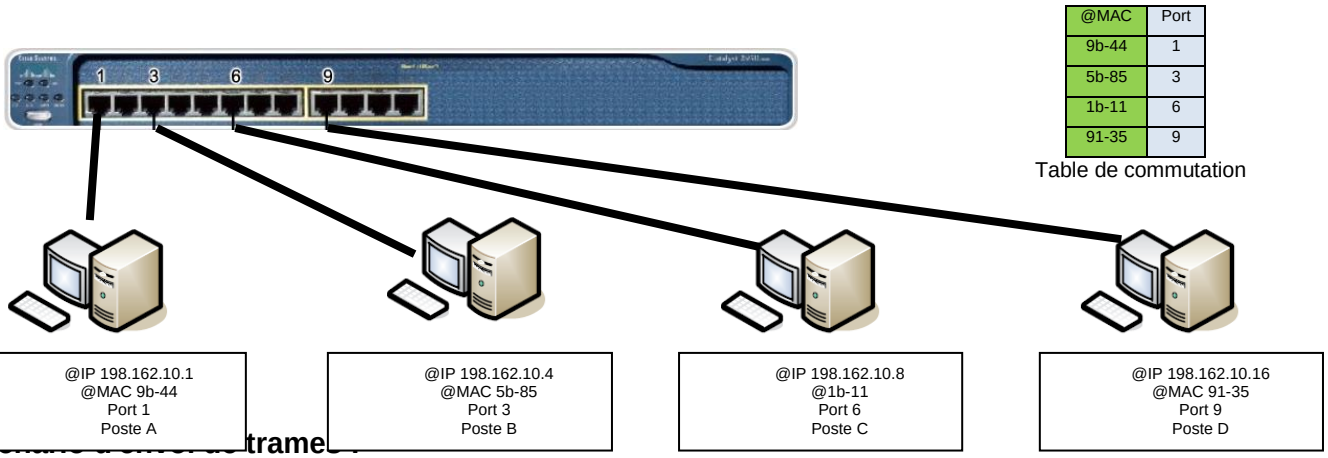
Table de commutation et communication en mode store and forward (stockage et retransmission):

Les commutateurs transfèrent de manière sélective des trames individuelles d'un port récepteur au port sur lequel l'hôte de destination est connecté. Ce processus de réacheminement sélectif peut se comparer à la création d'une connexion point à point momentanée entre les émetteurs (source de la transmission) et les récepteurs (destinataires de la réception). Cette connexion ne dure que le temps d'envoyer une trame unique. Durant ce laps de temps, les deux OTC disposent de l'intégralité de la bande passante.

Physiquement la connexion temporaire n'est pas simultanée entre les deux hôtes. En fait, chaque OTC qui fonctionne en mode bidirectionnel simultané peut transmettre à chaque fois qu'il a une trame, sans tenir compte de la disponibilité de l'OTC de réception. En effet, un commutateur LAN met en mémoire tampon une trame entrante afin de l'envoyer au port correspondant. Ce processus s'appelle **store and forward (stockage et retransmission).** Grâce à ce stockage et à la retransmission, le commutateur reçoit toute la trame, vérifie si elle comporte des erreurs et réachemine la trame vers le port approprié pour l'OTC de destination.

Remarque : un autre mode de fonctionnement, le Cut through, retransmet la trame sur le port de destination sans vérification des erreurs. Ce mode est plus rapide, mais propage des trames en erreur.

Le commutateur gère une table, appelée **table de commutation** ou table MAC qui "mappe" les adresses MAC sources aux ports utilisés par les OTC. Ainsi pour chaque trame entrante, l'adresse MAC de destination figurant dans l'en-tête de trame est comparée à la liste des adresses de la table MAC. Lorsqu'un numéro de port répertorié dans la table est "mappé" à l'adresse MAC, il est utilisé comme port de sortie de la trame.



Sécurité d'une trame :

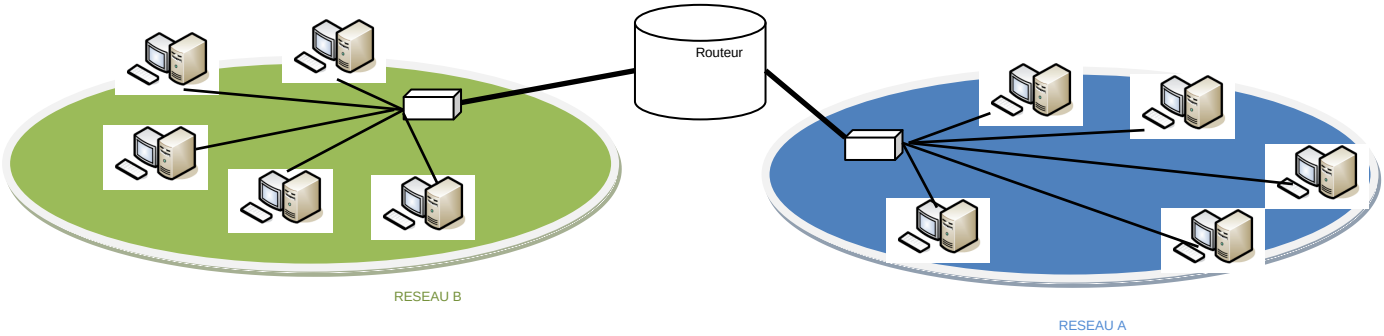
Si l'OTC Poste A envoie une trame au poste D et dans le même temps le Poste B veut envoyer une trame au Poste D, le commutateur va prendre les 2 trames (une entrante sur son port 1, l'autre entrante sur son port 3) va stocker ces trames dans sa mémoire tampon, vérifier si il y à une erreur de checksum, puis en consultant sa table de commutation s'apercevoir que les 2 trames comportent la même adresse MAC de destination correspondant à son port 9, il transmettra donc une première trame (par exemple celle du poste B) en sortie sur son port 9 puis après la seconde trame (celle du poste A).

f) Les nœuds : le routeur

Les routeurs sont des équipements qui agissent sur la couche réseau du modèle OSI. Ils permettent l'acheminement optimal des paquets entre différents réseaux.

À mesure que les réseaux s'étendent, ils présentent des problèmes qui peuvent être au moins partiellement allégés en divisant le réseau en réseaux plus petits, interconnectés. En effet le volume de trafic de données réseau généré croît avec la taille du réseau et les différentes applications génèrent elles aussi du trafic et donc le réseau est ralenti. La division de réseaux en fonction de l'utilisation facilite l'allocation efficace de ressources réseau ainsi que l'accès autorisé à ces ressources.

Un grand nombre d'hôtes connectés au même réseau peut produire des volumes de trafic de données qui peuvent utiliser au maximum, voire épuiser les ressources réseau telles que la bande passante et les capacités de routage. On sépare donc les réseaux avec des routeurs de façon à regrouper les hôtes devant communiquer et pour réduire le trafic entre les réseaux.



g) Remarque : le domaine de diffusion Ethernet.

Il est possible qu'un OTC veuille s'adresser à tous les membres de son réseau ; c'est le mode diffusion : un message envoyé à partir d'un hôte à tous les autres hôtes du réseau utilisera l'adresse MAC FF.FF.FF.FF.FF.FF.

Les diffusions sont contenues dans le réseau : c'est le **domaine de diffusion**.

Sur le schéma précédent, il y a 2 domaines de diffusion Ethernet (réseau A et réseau B), car il y a 2 commutateurs Ethernet.

À noter que le routeur peut aussi joindre tous les OTC, mais au niveau de la couche réseau dans ce cas. Il utilisera une adresse en 255 (voir ci-dessous *broadcast*).

3. Les Protocoles (voir cours ET234-2)

a) Définition

Un protocole permet de standardiser la forme des informations échangées indépendamment du type d'OTC utilisées. Il détermine les stratégies d'acheminement des données et les procédures à effectuer en cas d'erreur.

Les problèmes à résoudre sont nombreux : hétérogénéité des OTC, des logiciels, ….On divise ces problèmes en définissant plusieurs niveaux de communications (voir modèle OSI) et en utilisant un protocole pour chacun d'eux.

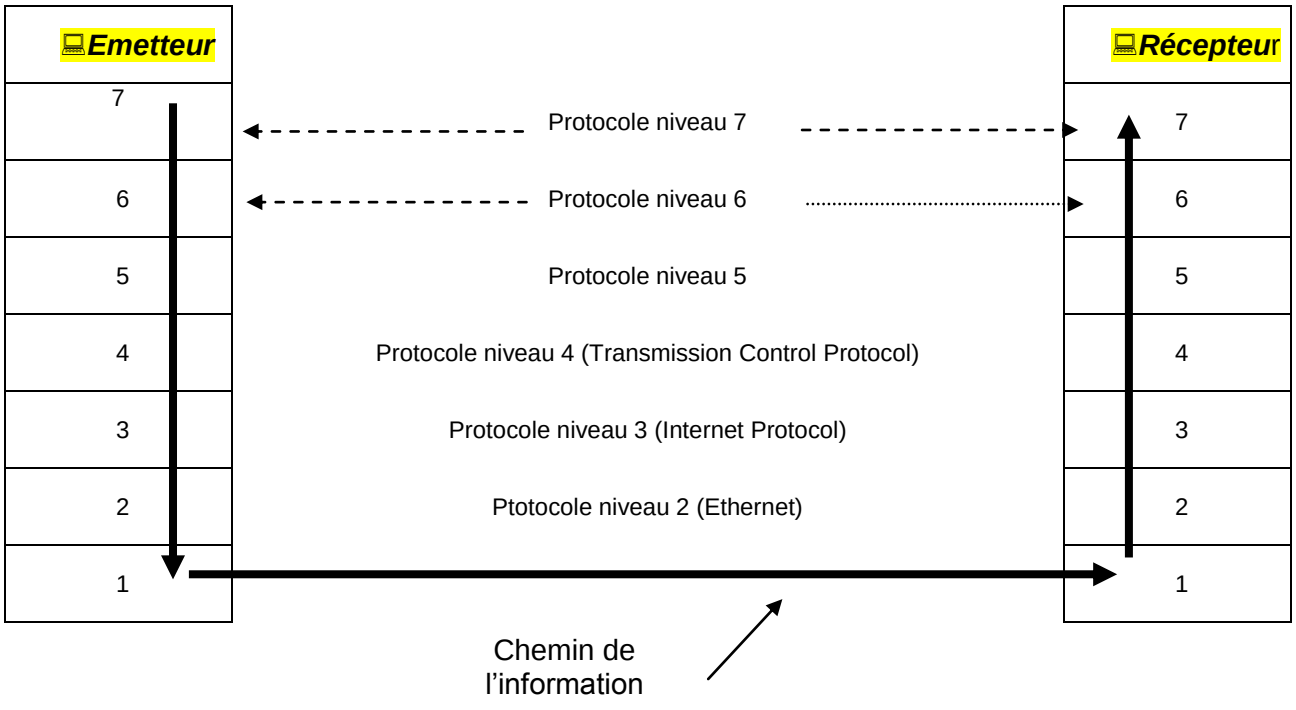
Dans les années 80 le domaine des réseaux est très prolifique (réseau Earn, Bitnet, Csnet, Hepnet, Arpanet, Telepac…) de nombreux standards existaient (X400, TCP/IP, Ethernet, X25, IIEEE802…) depuis 1990 une seule déclinaison est possible : internet avec protocole TCP/IP.

b) Le modèle OSI (Open Systems Interconnection)

Il décompose une transmission en 7 couches différentes :

Niveau :	Nom :	Rôle de la couche :
7	Application	Interface de communications avec les applications communicantes
6	Présentation	Encryptage et compression du code des données
5	Session	Organisation et synchronisation du dialogue
4	Transport	Etablissement et maintien des connexions du transport
3	Réseau	Routage des paquets au travers des nœuds du réseau
2	Liaison	Transmet les données (trames de bits) sans erreur (si erreur, retransmission)
1	Physique	Caractéristiques physiques et électriques des équipements (carte, fils…)

Note : Les couches 1,2,3,4 sont orientées transmission alors que les couches 5,6,7 sont orientées traitement



4. Réseau Ethernet et protocole TCP/IP

7 6 5	**Couches Applications** HTTP: Hyper Text Transfer Protocol: Echange de pages Web au format HTML Telnet: Connexion à un ordinateur distant	Programmes de l'utilisateur
4	**Couche Transport** TCP : Transport Control Protocol	Logiciels dans le système
3	**Couche Réseau** IP: Internet Protocol (routage des paquets d'informations)	Adressage IP
2 1	**Couches physiques et d'interface d'accès au réseau** Topologie bus 10BT ou étoile CSMA/CD : Carrier Sense Multiple Access/Collision Détection (accès au canal de transmission lorsque celui- ci est libre): la machine écoute le bus si rien dessus elle émet.	Adressage matériel Carte réseau Ethernet

Remarque : 10BT signifie un débit de **10** Mbits/s en **B**ande de base sur cuivre Twisted (torsadé) avec **100 m** maxi

a) L'adressage IPv4

Il permet de distinguer un réseau en particulier et un OTC à l'intérieur d'un réseau.

Chaque adresse est codée sur 4 octets, on la représente dans une notation décimale pointée. Par exemple :1100 0001 . 0011 0001 . 1001 0101 . 0110 0100 (C1 31 95 64 en hexa) s'écrira 193.49.149.100.

Remarque: Le protocole IPv4 évolue vers le IPv6 (pour v4, adresse codée sur 32 bits et pour v6, adresse codée sur 128 bits).

b) Classification des réseaux avec IP v4

Il existe 5 classes d'adresse avec le protocole IPv4:

L'adresse est constituée de deux parties : un identificateur de réseau (netid) et un identificateur de la machine (hostid) pour ce réseau.

Classe A : 128 réseaux et 16 777 216 hôtes (7 bits pour les réseaux et 24 pour les hôtes),

Classe B : 16384 réseaux et 65535 hôtes (14 bits pour les réseaux 16 pour les hôtes),

Classe C : 2 097 152 réseaux et 256 hôtes (21 bits pour les réseaux et 8 pour les hôtes).

Les classes D (224.0.0.0 à 239.255.255.255) et E (240.0.0.0 à 247.255.255.255) sont particulières ; la D est réservée au multicast et la E n'est pas utile aux destinataires finaux.

Soit pour les trois premières classes :

Remarque: Il existe 2 adresses réservées par classe (broadcast)

Classe	Identifiants réseau	Identifiants machine	Plage des adresses IP
A	Sur 1 octet : 0+ 7 bits Soit 128 réseaux	Sur 3 octets: 24 bits soit 2^{24} - 2 = 16 777 214 machines	0.0.0.0 – 127.255.255.255
B	Sur 2 octets : 10 + 14 bits Soit 2^{14} = 16384 réseaux	Sur 3 octets: 16 bits soit 2^{16} -2 = 65 533 machines	128.0.0.0 – 191.255.255.255
C	Sur 3 octets : 110+ 21 bits 2 097 152 réseaux	Sur 1 octet: 8 bits soit 2^8 -2 = 254 machines	192.0.0.0 – 223.255.255.255

c) Le masque de réseau

Il permet à une machine d'établir la route à suivre pour atteindre une autre machine. En effet si deux machines situées dans le même réseau veulent dialoguer, alors à l'aide de ce masque, elles sauront qu'il n'est pas nécessaire de passer par une passerelle (routeur).

Exemple : Prenons la classe d'adresses IP 172.16.0.0 ; il s'agit d'une classe B ; prenons comme masque réseau 255.255.0.0.

La machine X d'adresse 172.16.1.10 fait partie du réseau 172.16.0.0

La machine Y a pour adresse 172.16.2.20

Si la machine X veut établir une connexion vers Y alors elle applique le masque sur l'adresse IP de Y :

$$
\begin{array}{rl}
 & \%1010\ 1100\ 0001\ 0000\ 0000\ 0010\ 0001\ 0100 \\
\& & \%1111\ 1111\ 1111\ 1111\ 0000\ 0000\ 0000\ 0000 \\
\hline
 & \%\underbrace{1010\ 1100}\ \underbrace{0001\ 0000}\ \underbrace{0000\ 0000}\ \underbrace{0000\ 0000} \\
 & \underbrace{\$A\quad C}\quad \underbrace{1\quad 0}\quad \underbrace{0\quad 0}\quad \underbrace{0\quad 0} \\
 & 172\quad .\quad 16\quad .\quad 0\quad .\quad 0
\end{array}
$$

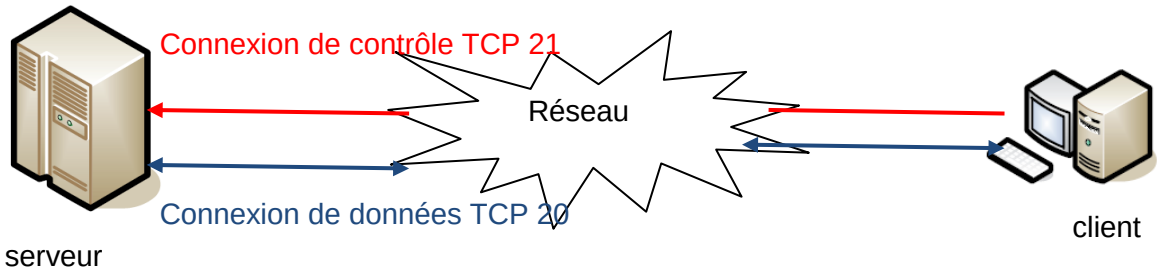
L'adresse obtenue étant égale à l'adresse réseau, alors la machine est « atteignable » sur le même réseau et aucun routeur n'est à utiliser.

d) Le protocole FTP:

Le protocole FTP (Files Transfer Protocol) est un protocole de la couche application (7) du modèle OSI. Il permet le transfert de fichiers entre un client et un serveur, il nécessite 2 connexions entre le client et le serveur.

Le client établit une première connexion (port TCP21) utilisée pour la circulation des commandes du client et les réponses du serveur.

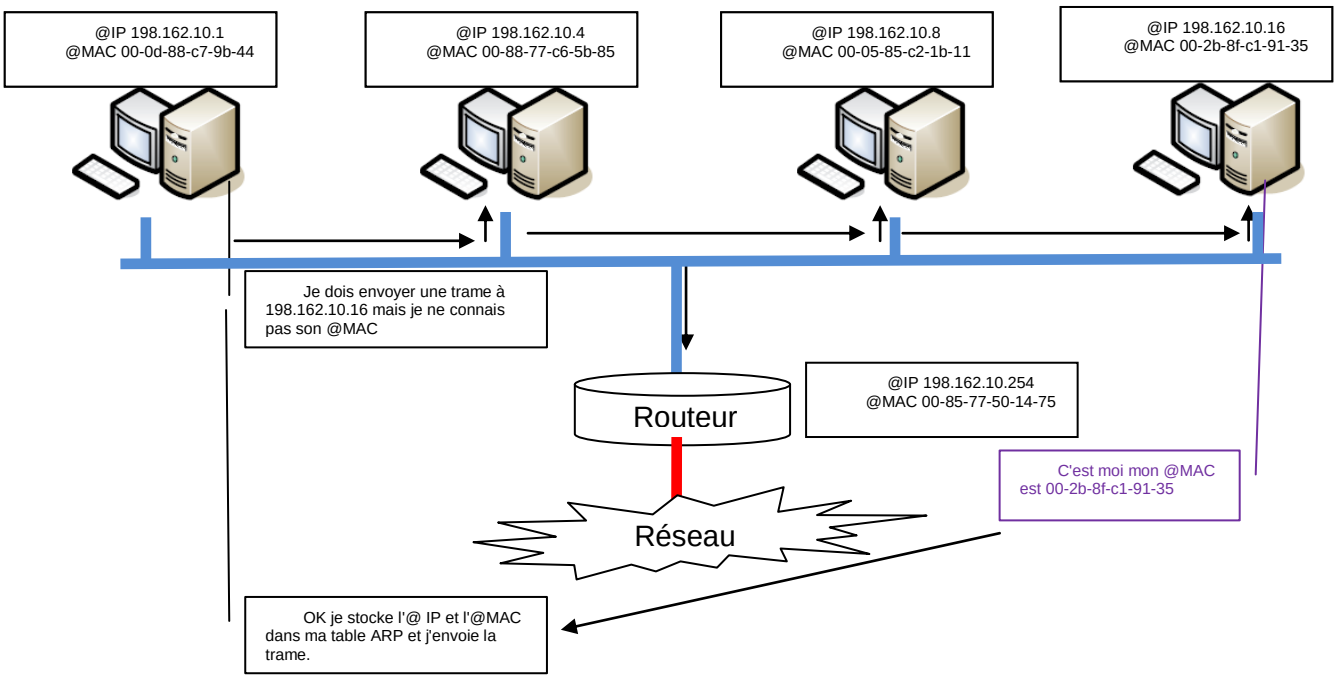
Le client établit uns seconde connexion (port TCP20) utilisée pour le transfert des fichiers de données. Cette connexion est bidirectionnelle le client peut télécharger un fichier à partir du serveur ou vers le serveur.



e) Le protocole ARP:

Le protocole ARP (Address Resolution Protocol) permet de lier l'adresse IP d'un OTC à son adresse MAC. Dans un LAN les informations circulent sous forme de trames encapsulées. A chaque trame doit corresponde son adresse MAC de destination qui est la seule capable d'identifier de manière univoque le destinataire du message.

Chaque OTC garde en RAM une table ARP (tableau ARP ou cache ARP) à 2 entrées : une adresse IP et une adresse MAC, la relation entre ces 2 valeurs s'appelle une mise en correspondance si on rentre par l'adresse IP on ressort avec l'adresse MAC. Le tableau ARP gardé en RAM conserve tout le mappage (adresses IP et MAC) de l'ensemble des périphériques du LAN auquel appartient l'OTC concerné.



Un OTC à 2 méthodes pour mettre à jour sa table ARP:

Soit il observe les trames qui circulent sur le réseau et lorsqu'il reçoit des trames en provenance du support, il enregistre les adresses IP source et MAC dans son tableau ARP. Au fur et à mesure que les trames sont transmises sur le réseau, l'OTC remplit le tableau ARP avec les paires d'adresses des périphériques qui composent son LAN.

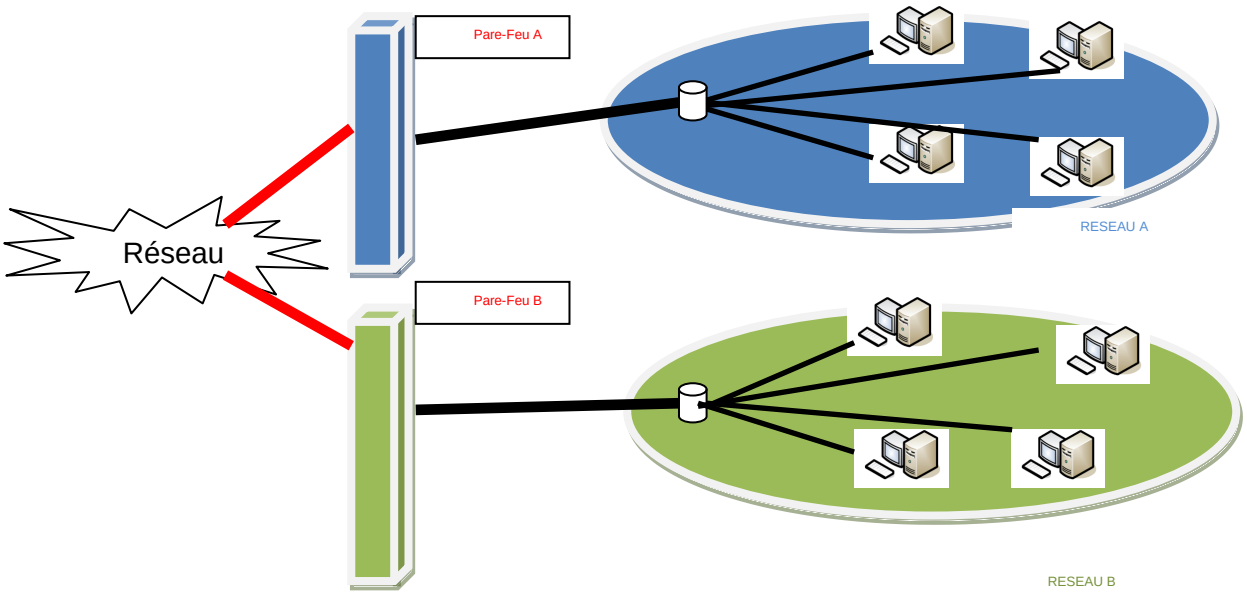
Soit il diffuse une requête ARP : envoi d'un message de diffusion de couche 2 à tous les périphériques du LAN Ethernet. La trame contient un paquet de requête ARP comportant l'adresse IP de l'hôte de destination. Lorsque l'OTC de destination reçoit la trame et identifie sa propre adresse IP, il répond en envoyant un paquet réponse ARP à l'expéditeur, sous la forme d'une trame monodiffusion (à une seule adresse MAC). Cette réponse permet de créer une nouvelle entrée dans le tableau ARP de l'OTC source.

5. Le pare-feu

On aborde ici les problèmes de sécurité des réseaux, à l'origine l'Internet comptait un petit nombre d'utilisateurs de confiance d'agences gouvernementales américaines et des organismes de recherche qu'elles sponsorisaient. Dans cette petite communauté, la sécurité n'était pas un problème important.

La situation a changé à mesure que des individus, des entreprises et des organisations ont mis au point leurs propres réseaux IP connectés à Internet. Un réseau A d'une société A n'a pas besoin de se connecter au réseau B d'une organisation B sans l'autorisation de celle-ci.

La division de réseaux en fonction de la propriété signifie que l'accès à et à partir des ressources extérieures à chaque réseau peut être interdit, autorisé ou surveillé.



La sécurité entre les réseaux est implémentée dans un périphérique intermédiaire (routeur ou dispositif de pare-feu) au niveau du périmètre du réseau. La fonction de pare-feu remplie par ce périphérique permet uniquement aux données connues et de confiance d'accéder au réseau.

6. Le Domaine Name Service

a) Définition

Lorsque l'on s'adresse à une machine sur Internet, il est plus pratique de mémoriser un nom symbolique plutôt que son adresse IP. Toutefois, on peut utiliser l'une ou l'autre des deux formes d'adresse. Ceci est possible grâce au DNS (Domain Name Service né en 1983), qui est chargé de convertir si besoin les adresses IP en noms symboliques ou les noms symboliques en adresses IP.

Lorsque vous recherchez l'adresse IP ou le nom associé à une adresse IP d'une machine du réseau, vous émettez une requête à votre serveur DNS. Chaque serveur DNS gère une plage d'adresses IP.

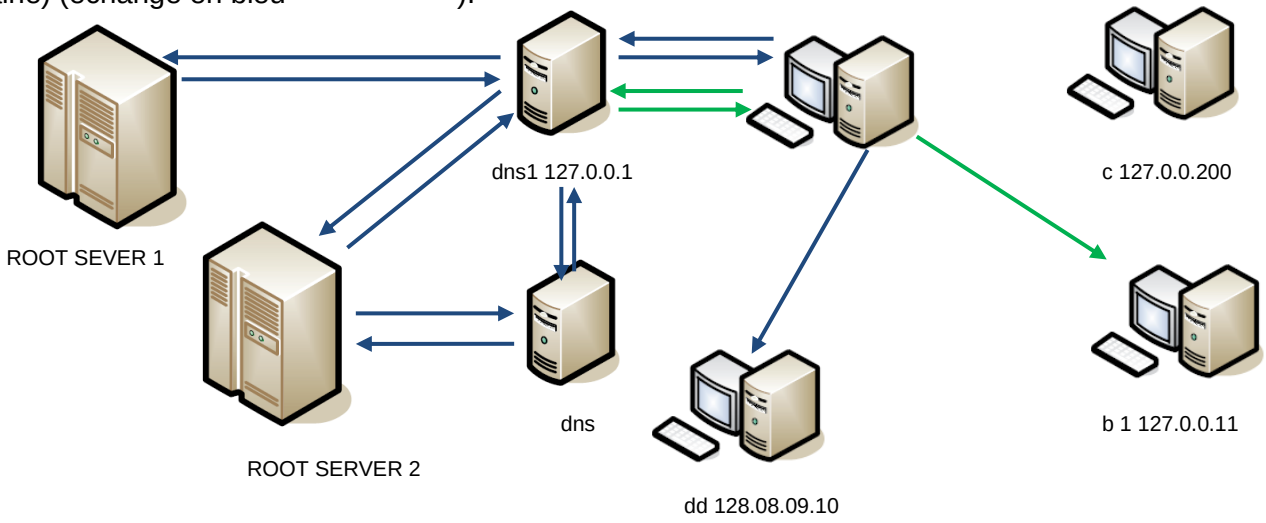
b) Exemple

Prenons par exemple le domaine nommé « internet.fr », et donnons lui la classe C 127.0.0.0 et le masque de réseau 255.255.255.0. Cet organisme dispose donc de 256 adresses IP, dont 2 réservées (0 et 255). C'est lui qui va décider de l'organisation de cette plage d'adresse. Dès lors, une machine est donc installée et désignée comme serveur DNS. C'est sur cette machine que toutes les informations adresses / noms symboliques seront entrées.
Donc, dans notre exemple, nous décidons d'installer trois machines, « a », « b » et « c », plus un serveur DNS que nous appellerons « dns1 ». L'administrateur de ce site a choisi de répartir ainsi ses adresses :
dns1 127.0.0.1 a 127.0.0.10 b 127.0.0.11 c 127.0.0.200

Il va donc rentrer ces informations dans son serveur DNS. Il va aussi confier les adresses à des « ROOT SERVERS ». Les ROOT SERVERS sont quelques machines réparties dans le monde qui maintiennent et s'échange quotidiennement des bases de données référençant chaque couple (plage d'adresses / serveur DNS).

Imaginons maintenant que vous faites une requête à ce serveur. Si la requête concerne votre plage d'adresses (par exemple, la machine « a » demande l'adresse de la machine « b ») alors votre serveur DNS répond de manière autonome (échange en vert ⟶).

Par contre, si jamais votre requête est en dehors de votre domaine, le serveur DNS va demander à un ROOT SERVER à quelle adresse il doit demander cette information. Si le premier ROOT SERVER ne répond pas, il demande alors au suivant, et ce jusqu'à ce qu'un serveur réponde. Le ROOT SERVER va donc retourner une adresse de serveur DNS ayant autorité sur la zone demandée (le nom de domaine) (échange en bleu ⟶).



Lorsque le DNS sait à qui demander l'information, il va alors contacter ce serveur pour lui poser la question. Le serveur DNS alors contacté va alors renvoyer sa réponse.

c) Les domaines

Chacun des domaines de premier niveau a une signification :

.ARPA organismes spécifiques à l'Internet (obsolète),
.COM Entreprises à but commercial,
.EDU Organismes d'enseignements,
.GOUV Organismes gouvernementaux,
.MIL Entités militaires,
.ORG Organisations à but non lucratif

Remarque : la France a elle aussi adoptée une sous hiérarchisation de ses noms de domaines. On dispose maintenant des domaines de premier niveau suivants : .gouv.fr, .asso.fr, .barreau.fr, .cci.fr,.ac.fr, tm.fr…

7. Le NAT

La technique de translation d'adresses (NAT en anglais, RFC 3022) est une pratique courante qui est apparue à l'origine pour palier au manque croissant d'adresses IPv4 libres. Il fut donc décidé de réserver des intervalles d'adresses à des usages privés uniquement (RFC 1918). Ce sont les adresses :

Classe A : 10.0.0.0 - 10.255.255.255 (10/8 prefix)
Classe B : 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
Classe C : 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

En conséquence, ces adresses ne sont pas routables sur Internet et ne doivent pas être utilisées par des machines de ce réseau. Par contre, tous les réseaux privés peuvent utiliser ces adresses sans restrictions.

Le principe repose sur l'utilisation d'une passerelle liée au réseau privé et au réseau public. Une machine du réseau privé utilise la passerelle qui envoie à sa place une requête sur le réseau public. La passerelle réceptionne la réponse et la transfère vers la machine du réseau privée ayant fait la demande.

Le NAT ne permet pas d'accéder à la machine du réseau privé via le réseau public.

a) Le NAT statique

Le Nat statique consiste à utiliser une adresse IP publique pour une machine installé sur un réseau privé (avec une adresse IP privée).

De cette façon, il est possible d'accéder à la machine du réseau privé via le réseau public (internet). Mais cela ne palie pas au manque d'adresse IPv4.

b) Le NAT dynamique

Le Nat dynamique consiste à affecter une adresse IP publique identique à toutes les machines d'un réseau privé.

Afin de pouvoir adresser chaque machine, il faut pratiquer une translation de port (PAT : Port Address Translation) Chaque machine utilise un port TCP différent pour communiquer sur le réseau public.

Ainsi, lors d'une requête d'une machine, la passerelle l'exécute et transmet la réponse en utilisant le port TCP utilisé par la machine ayant fait la demande.

C'est ce que réalisent les Box Internet.

c) Redirection de port (port forwarding)

On affecte un port TCP différent du routeur à chaque machine du réseau privé.

Ainsi, une machine du réseau privé est accessible depuis internet via l'adresse IP du routeur et le numéro du port TCP qui lui est affecté.

L'inconvénient majeur est que le port TCP est ouvert en permanence

d) Déclenchement de port (port triggering)

Pour éviter l'ouverture permanente d'un port, il est possible de conditionner l'ouverture à la présence d'un évènement. C'est le déclenchement de port (ou Port Trigerring).

Il s'agit d'une redirection de port conditionnelle.

8. Bibliographie et sources

Introduction aux réseaux par David Tilloy.
Cours de BTS Iris Lycée Nicolas Appert d'Olivier Commenge (Académie de Nantes)