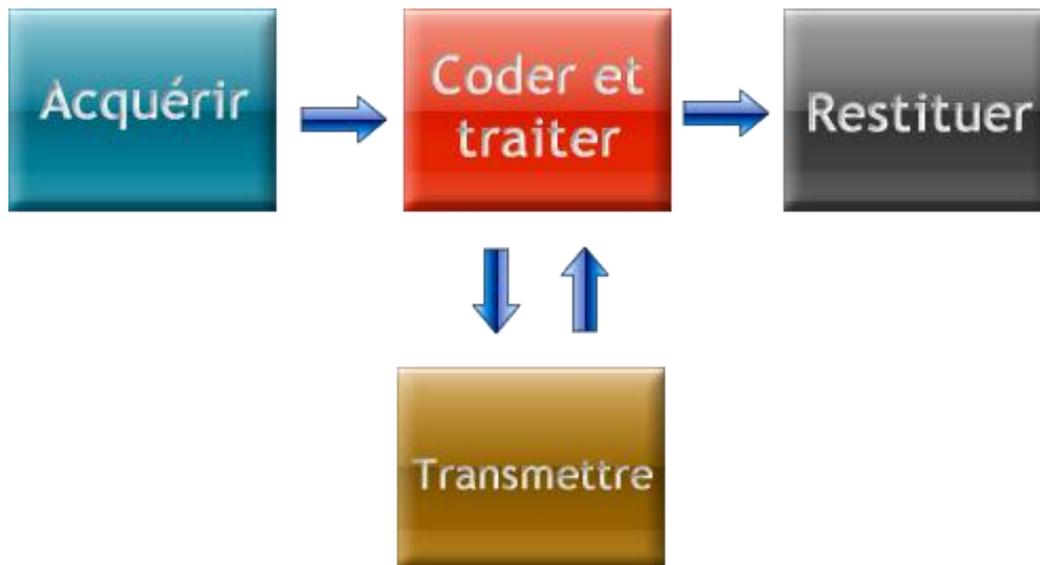


Cours SIN

Réseau informatique

1. ANALYSE DETAILLEE

On peut découper cette chaîne en plusieurs blocs fonctionnels.



1.1. Transmettre

C'est la fonction qui va permettre de transmettre le signal entre la fonction acquérir et une interface (valise de diag etc).

Il faut qu'il soit adapté en fonction du signal

Le signal et son support	
Le signal	Le support
Les impulsions électriques	Le cuivre pour les câbles coaxiaux et en paires torsadées
Les impulsions lumineuses	Le verre des câbles en fibre optique
Les vibrations mécaniques	L'eau pour les dauphins... Le cuir de la peau de bête pour les tambours... L'aluminium ou la fonte pour les casseroles de la ménagère...
Les ondes	L'air ou l'espace pour les ondes radio et les ondes des satellites

En général, la distance affaiblit le signal ; et, en particulier pour l'informatique, le contrôle des erreurs ou la régénération du signal ralentissent l'acheminement des données.

Deux types de supports existent:

- les supports limités (filaire) : torsadé, coaxial, fibre optique ;
- les supports non limités (non filaire) : l'air, les ondes électromagnétiques, infrarouges ou ondes radios.

Caractéristiques communes à tout support à prendre en compte :

- la bande passante
- le bruit et la distorsion
- la capacité
- le prix
- la résistance physico-chimique au milieu ambiant
- l'adaptation aux conditions de pose

2. Réseau informatique

2.1. Historique

C'est en 1965 que Lawrence G. Roberts va, avec Thomas Merill, connecter le premier 'ordinateur TX-2 au Massachussets avec l'ordinateur Q-32 en Californie par une liaison téléphonique. Cette expérience va prouver la faisabilité et l'utilité d'un réseau d'ordinateurs.

En décembre 1970, Le Network Working Group sous la direction de S. Crocker détermine le protocole de communication entre ordinateurs pour le réseau ARPANET appelé Network Control Protocol ou NCP. C'est à partir de cette date que des utilisateurs de ce réseau purent développer les premières applications.

A cette époque, le réseau ARPANET est constitué de 23 ordinateurs sur 15 sites différents reliés par des liaisons à 50 kbits/s.

En 1976, Le DoD (Department of Defense) commence ses expérimentations sur le protocole TCP/IP et décide rapidement de migrer le réseau ARPANET vers ce protocole.

Août 1980, Vinton Cerf, scientifique au DARPA propose un plan d'interconnexion (inter-network connection) entre les réseaux CSNET et ARPANET utilisant le protocole TCP/IP ce qui va lancer le réseau internet tel que nous le connaissons actuellement.

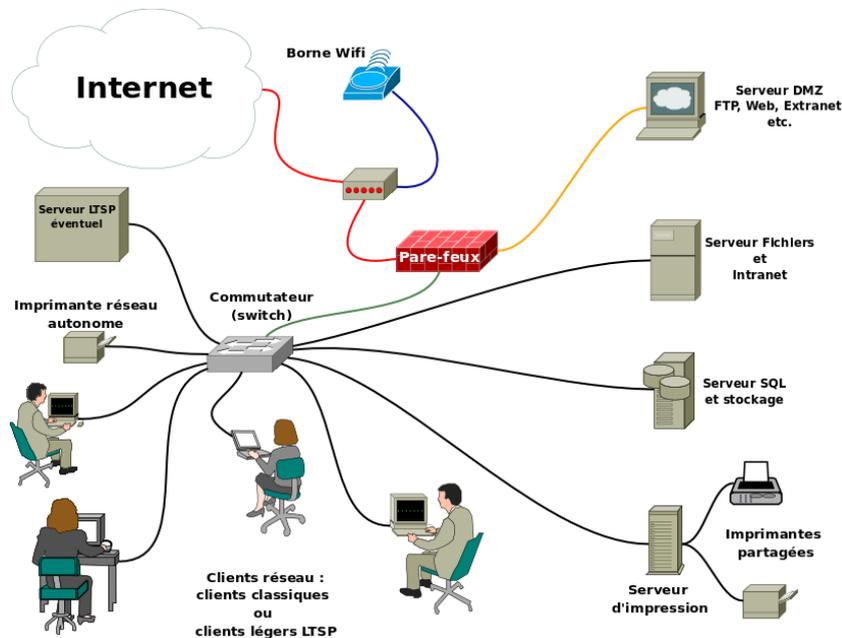
2.2. Présentation

Par définition un réseau est un ensemble de nœuds (ou pôles) reliés entre eux par des liens (ou canaux) afin d'échanger des informations, de partager des ressources, de transporter de la matière ou de l'énergie. En terme informatique c'est un ensemble d'équipements reliés entre eux pour échanger des informations.

Un réseau informatique peut servir à plusieurs choses

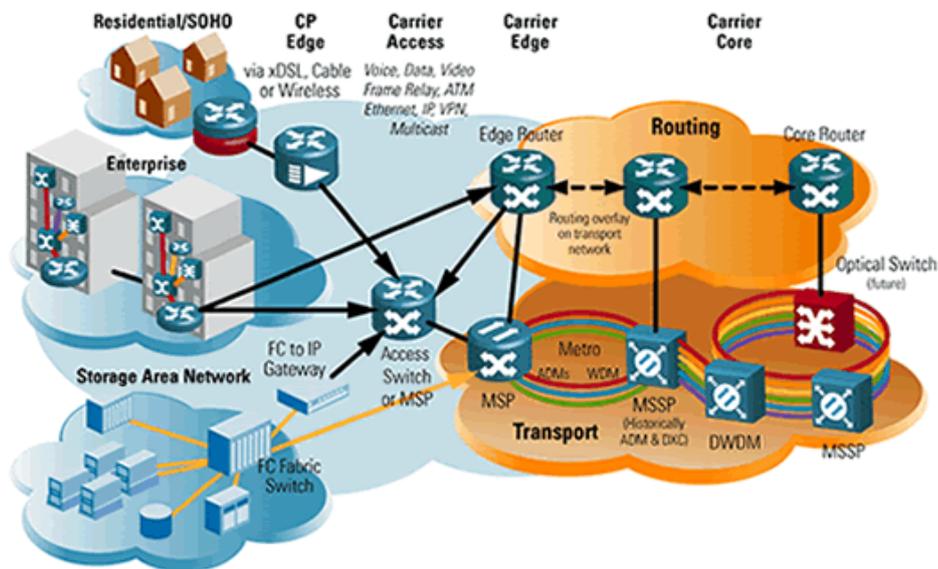
- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct, etc.)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau)
- Le jeu vidéo multi-joueurs

Exemple réseau d'entreprise



2.3. Principe de fonctionnement

Dans la pratique, les ordinateurs ne sont pas directement reliés entre eux. Ils sont d'abord interconnectés au sein d'un institut ou d'un bâtiment formant ainsi une multitude de petits sous-réseaux. Puis par sous réseau une machine est chargée de s'interconnecter avec d'autres machines. Enfin progressivement la planète entière est interconnectée avec à chaque étape du maillage une machine désignée pour se connecter au niveau supérieur.



Chaque nœud du réseau est constitué par un ordinateur identifié par une adresse IP (Internet Protocole) qui est son identificateur.

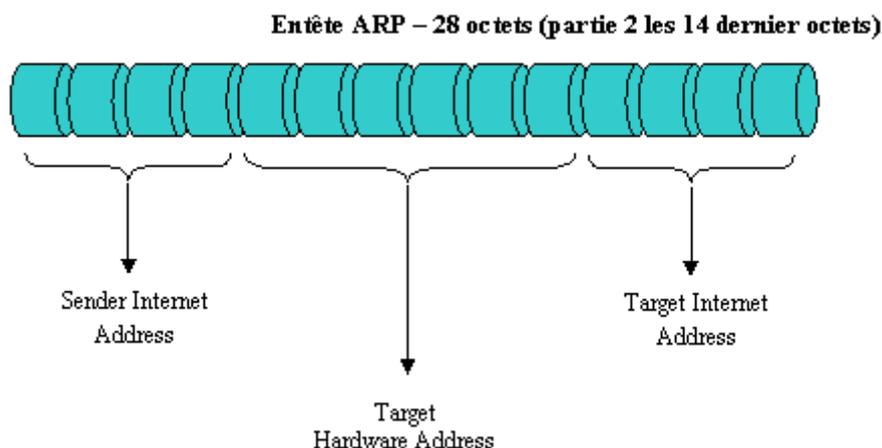
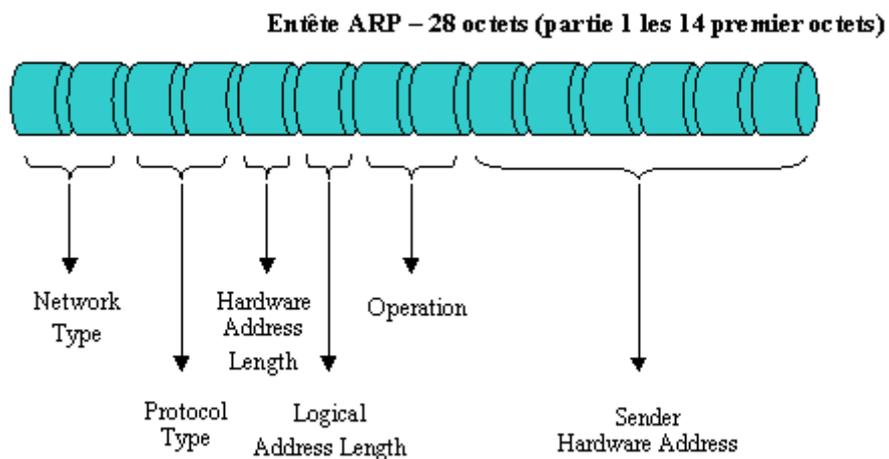
Pour permettre la communication entre eux, on utilise une méthode standard qui s'appelle un protocole. Qui est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur le réseau.

Depuis les années 80, c'est la norme TCP/IP (Transmission Control Protocol / Internet Protocol) qui définit la norme de communication.

Il existe plusieurs types de protocole :

- **HTTP L'HyperText Transfer Protocol**, c'est est un protocole de la couche application. Il peut fonctionner sur n'importe quelle connexion fiable, dans les faits on utilise le protocole TCP comme couche de transport. Un serveur HTTP utilise alors par défaut le port 80 (443 pour HTTPS). Les plus connus sont les navigateurs WEB
- **DNS** permet de retrouver une adresse IP en fonction d'un nom d'ordinateur (un peu comme un annuaire).
- **FTP** sert à transporter des fichiers d'un ordinateur à l'autre.
- **IRC** permet de créer des «salons» de discussion en direct.
- **ICQ** permet de savoir si quelqu'un est en ligne et de dialoguer avec lui.
- **NTP** permet de mettre les ordinateurs à l'heure par internet à 500 millisecondes près.
- **P2P** permettent de partager des fichiers à grande échelle.
- **NNTP** permet d'accéder à des forums de discussion sur des milliers de sujets différents.
- **SSH** permet d'avoir un accès sécurisé à des ordinateurs distants.
- **SMTP** permet d'envoyer des emails, et le protocole POP3 de les recevoir.
- **ARP** : Le protocole **ARP** a un rôle phare parmi les protocoles de la couche Internet de la suite TCP/IP, car il permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP, c'est pour cela qu'il s'appelle Protocole de résolution d'adresse (en anglais ARP signifie Address Resolution Protocol).

Structure :



Définition des différents champs

- Hardware type

Ce champ est placé en premier afin d'indiquer quel est le format de l'entête Arp.

- 01 - Ethernet (10Mb) [JBP]
- 02 - Experimental Ethernet (3Mb) [JBP]
- 03 - Amateur Radio AX.25 [PXX]
- 04 - Proteon ProNET Token Ring [Doria]
- 05 - Chaos [GXP]
- 06 - IEEE 802 Networks [JBP]
- 07 - ARCNET [JBP]
- 08 - Hyperchannel [JBP]
- 09 - Lanstar [TU]
- 10 - Autonet Short Address [MXB1]
- 11 - LocalTalk [JKR1]
- 12 - LocalNet (IBM PCNet or SYTEK LocalNET) [JXM]
- 13 - Ultra link [RXD2]
- 14 - SMDS [GXC1]
- 15 - Frame Relay [AGM]
- 16 - Asynchronous Transmission Mode (ATM) [JXB2]
- 17 - HDLC [JBP]
- 18 - Fibre Channel [Yakov Rekhter]
- 19 - Asynchronous Transmission Mode (ATM) [RFC2225]
- 20 - Serial Line [JBP]
- 21 - Asynchronous Transmission Mode (ATM) [MXB1]
- 22 - MIL-STD-188-220 [Jensen]
- 23 - Metricom [Stone]
- 24 - IEEE 1394.1995 [Hattig]
- 25 - MAPOS [Maruyama]
- 26 - Twinaxial [Pitts]
- 27 - EUI-64 [Fujisawa]
- 28 - HIPARP [JMP]
- 29 - IP and ARP over ISO 7816-3 [Guthery]
- 30 - ARPSec [Etienne]
- 31 - IPsec tunnel [RFC3456]
- 32 - InfiniBand (TM) [Kashyap]
- 33 - TIA-102 Project 25 Common Air Interface (CAI) [Anderson]

- Hardware Address Length

Ce champ correspond à la longueur de l'adresse physique. La longueur doit être prise en octets. Voici des exemples de valeurs courantes.

- 01 - Token Ring
- 06 - Ethernet

- Protocol Address Length

Ce champ correspond à la longueur de l'adresse réseau. La longueur doit être prise en octets. Voici des exemples de valeurs courantes.

- 04 - IP v4

- 16 - IP v6

- Operation

Ce champ permet de connaître la fonction du message et donc son objectif. Voici les différentes valeurs possibles.

- 01 - Request [[RFC 826](#)]

- 02 - Reply [[RFC 826](#)]

- Sender Hardware Address

Ce champ indique l'adresse physique de l'émetteur. Dans le cadre spécifique d'Ethernet, cela représente l'adresse Mac source.

- Sender Internet Address

Ce champ indique l'adresse réseau de l'émetteur. Dans le cadre spécifique de TCP/IP, cela représente l'adresse Ip de source.

- Target Hardware Address

Ce champ indique l'adresse physique du destinataire. Dans le cadre spécifique d'Ethernet, cela représente l'adresse Mac destination. Si c'est une demande Arp, alors, ne connaissant justement pas cette adresse, le champs sera mis à 0.

- Target Internet Address

Ce champ indique l'adresse réseau du destinataire. Dans le cadre spécifique de TCP/IP, cela représente l'adresse Ip de destination.

Ressource : <http://www.frameip.com/entete-arp/>

2.4. Architecture et caractéristiques d'un réseau interne

L'architecture d'un réseau est définie par l'ensemble des couches et la description des protocoles et des services de chacune d'elles.

- Une couche offre un ensemble de services à la couche immédiatement au-dessus
- Chaque passage à la couche inférieure ajoute son en-tête
- Chaque passage à la couche supérieure enlève les informations propres à la couche du dessous

Exemple modèle OSI

On a 7 couches

physique	Elle est chargée de la transmission effective des signaux entre les interlocuteurs. Son service est limité à l'émission et la réception d'un bit ou d'un train de bit continu (notamment pour les supports synchrones).
Liaison de données	Elle gère les communications entre 2 machines adjacentes, directement reliées entre elles par un

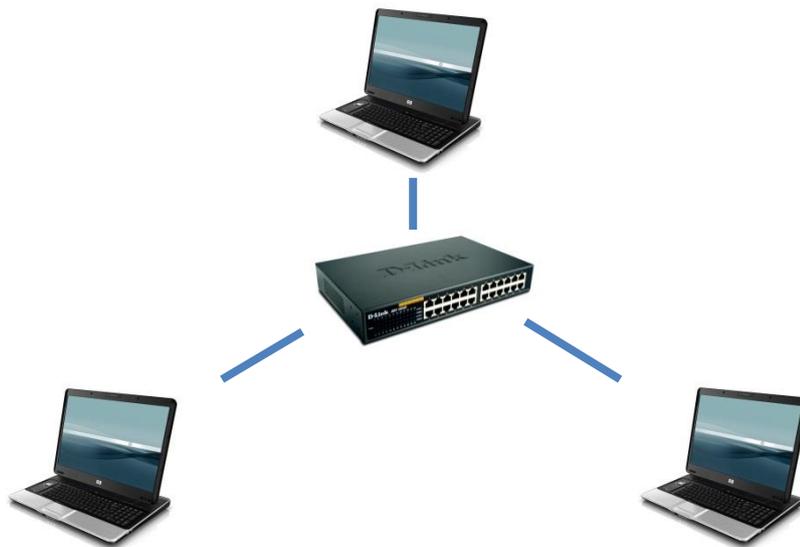
	support physique.
réseau	Elle gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets
transport	Elle gère les communications de bout en bout entre processus (programmes en cours d'exécution).
session	Elle gère la synchronisation des échanges et les « transactions », permet l'ouverture et la fermeture de session.
présentation	Elle est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises.
application	Elle est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme.

D'un point de vue typologique, l'architecture est respectivement qualifiée de LAN (Local Area Network), MAN (Metropolitan Area Network) et WAN (Wide Area Network) lorsque le réseau s'étend sur un périmètre local (< 1 km), métropolitain (< 100 km) et longue distance.

Il existe plusieurs types de topologie de réseau :

- en étoile

Toutes les stations sont connectées à un concentrateur, on parle de topologie en étoile. Les nœuds du réseau sont tous reliés à un nœud central. Dans cette topologie tous les PC sont interconnectés grâce à un SWITCH



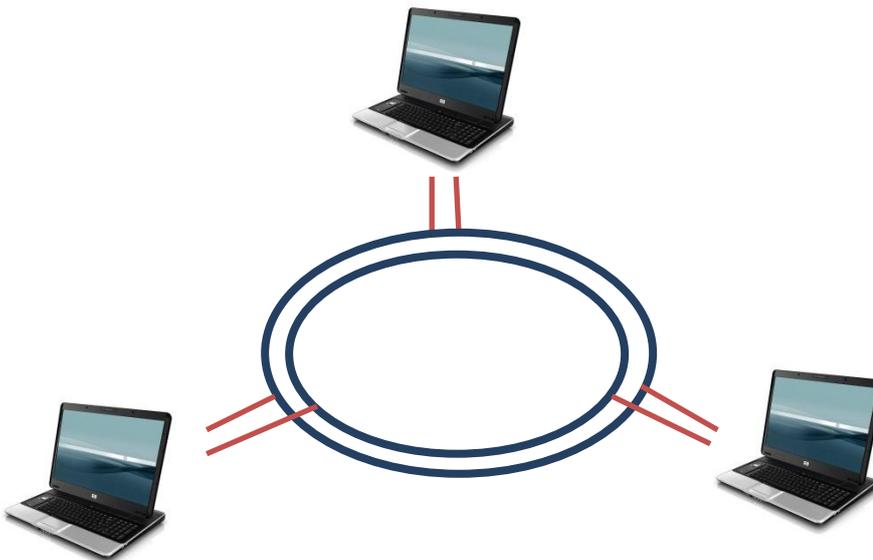
- en bus

Les machines sont reliées par un câble coaxial (le bus) et chaque ordinateur est connecté en série sur le bus, on dit encore qu'il forme un nœud.



- en anneau

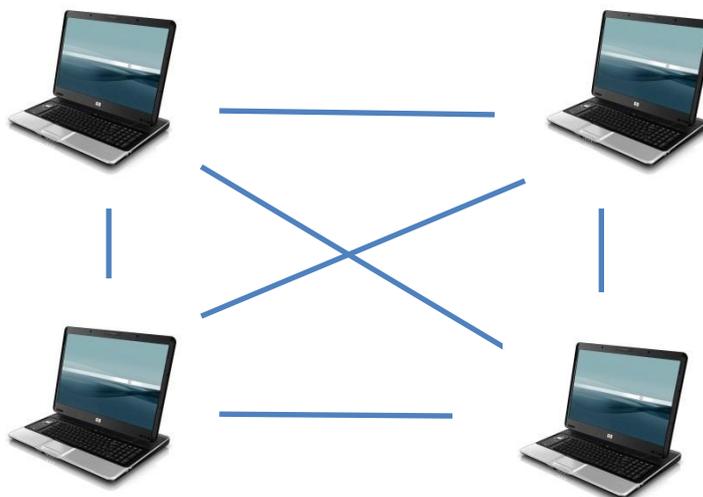
Les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. Cela ressemble à un bus mais qui serait refermé sur lui-même : le dernier nœud est relié au premier.



- maillé

Les réseaux maillés utilisent plusieurs chemins de transferts entre les différents nœuds. C'est une structure réseau hybride reprenant un câblage en étoile regroupant différents nœuds de réseaux.

INTERNET est une topologie maillée (sur le réseau étendu (WAN), elle garantit la stabilité en cas de panne d'un nœud.



Lorsqu'on configure un réseau, on parle souvent de masque de sous réseau. Celui-ci sert à des ordinateurs d'un même réseau à communiquer entre eux. En fonction du masque, des restrictions d'accès sont appliquées, et les ordinateurs ne pourront pas communiquer, donc ne se verront pas dans les favoris réseau.

Ce masque de sous réseau va permettre aux ordinateurs ayant une adresse IP ayant 3 premiers octets identiques de communiquer ensemble. Ex : l'ordinateur ayant l'IP 192.168.0.1 pourra communiquer avec l'autre ayant une IP telle que 192.168.0.2, mais pas 192.169.0.2

L'adresse IP (avec IP pour Internet Protocol) est un numéro d'identification qui est attribué à chaque appareil connecté à un réseau informatique utilisant l'Internet Protocol. Il existe des adresses IP de version 4 et de version 6. La version 4 est actuellement la plus utilisée.

2.4.1.Composition d'une adresse IP

Une adresse IP est une adresse 32 bits, généralement notée sous forme de 4 nombres entiers séparés par des points. On distingue en fait deux parties dans l'adresse IP :

- Une partie des nombres à gauche désigne le réseau et sont appelés ID de réseau (en anglais *netID*),
- Les nombres de droite désignent les ordinateurs de ce réseau et sont appelés ID d'hôte (en anglais *host-ID*).

Notion de classe d'adresse IP :

Elle a été utilisée sur Internet pour distribuer des plages d'adresses IPv4 à des utilisateurs finaux. Avec cette méthode, le masque de réseau pouvait être déduit de l'adresse IP et les protocoles de routage comme Border Gateway Protocol (jusqu'à la version 3), RIPv1 et IGRP sont dits classful car ils font usage d'un masque réseau implicite lié à l'adresse.

La notion de classe est obsolète depuis le milieu des années 1990. Les assignations d'adresses du protocole IPv4 (et de son successeur IPv6) ne tiennent plus compte de la classe d'adresse et les protocoles de routage modernes indiquent explicitement le masque réseau de chaque préfixe routé.

En 1981, la RFC 790 (Assigned numbers²) prévoit qu'une adresse IP est divisée en deux parties : une partie servant à identifier le réseau (net id) et une partie servant à identifier un poste sur ce réseau (host id).

Il existe cinq classes d'adresses IP. Chaque classe est identifiée par une lettre allant de A à E.

Ces différentes classes ont chacune leurs spécificités en termes de répartition du nombre d'octet servant à identifier le réseau ou les ordinateurs connectés à ce réseau :

- Une adresse IP de classe A dispose d'une partie net id comportant uniquement un seul octet.
- Une adresse IP de classe B dispose d'une partie net id comportant deux octets.
- Une adresse IP de classe C dispose d'une partie net id comportant trois octets.
- Les adresses IP de classes D et E correspondent à des adresses IP particulières.

Résumé

Classe	Bits de départ	Début	Fin	Notation CIDR	Masque de sous-réseau par défaut
Classe A	0	0.0.0.0	127.255.255.255 ²	/8	255.0.0.0
Classe B	10	128.0.0.0	191.255.255.255	/16	255.255.0.0
Classe C	110	192.0.0.0	223.255.255.255	/24	255.255.255.0
Classe D (multicast)	1110	224.0.0.0	239.255.255.255	/8	non défini
Classe E (réservée)	1111	240.0.0.0	255.255.255.255		non défini

2.5. Etude structurelle

Dans l'ensemble un réseau est constitué des éléments suivant :

- Ceux à connecter
 - Les ordinateurs
 - Les serveurs
- Ceux interconnectant
 - Routeur
 - Répéteur
 - Commutateur

2.5.1. Serveurs

C'est un dispositif informatique matériel ou logiciel qui offre des services, à différents clients. Il fonctionne en permanence, répondant automatiquement à des requêtes provenant d'autres dispositifs informatiques (les clients), selon le principe dit client-serveur.

Actuellement les systèmes d'exploitation populaires sur les serveurs sont la série Windows NT de Microsoft (Windows NT, Windows 2000, Windows 2003 et Windows 2008), Novell NetWare, la famille Unix, parmi lesquels il y a Linux, Mac OS X de Apple et les systèmes BSD.



2.5.2. Le routeur

Un routeur est un élément intermédiaire dans un réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre au mieux, selon un ensemble de règles. Dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 (OSI)

Il autorise l'utilisation de plusieurs classes d'adresses IP au sein d'un même réseau. Il permet ainsi la création de sous-réseaux.

Il est utilisé dans les plus grandes installations, où il est nécessaire (notamment pour des raisons de sécurité et de simplicité) de constituer plusieurs sous-réseaux

Le routage est aujourd'hui très souvent associé au protocole de communication IPv4, alors que la migration vers IPv6 fait également intervenir le routage d'IPv6. D'autres protocoles moins populaires existent, et sont également routables.



2.5.3. Répéteur ou hub

C'est le matériel réseau le plus basique. Il est utilisé pour un réseau local avec un nombre très limité de machines. Il n'est ni plus ni moins qu'une 'multiprise RJ45' qui amplifie le signal réseau (base 10/100).

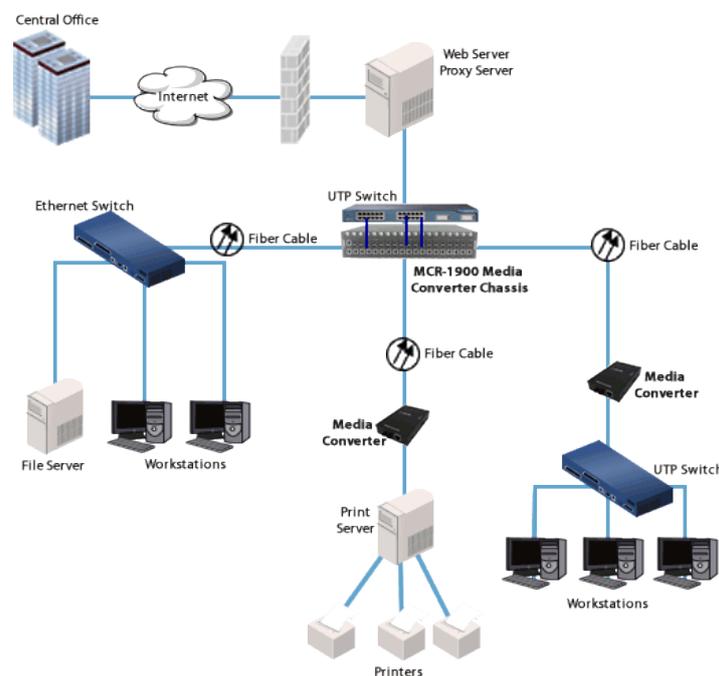


2.5.4. Commutateur ou switch

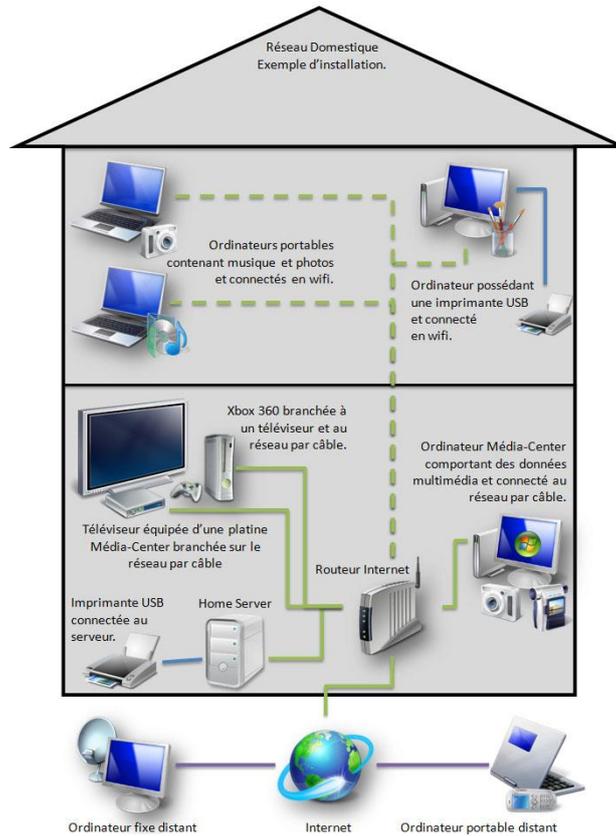
Il travaille lui sur les deux premières couches du modèle OSI, c'est-à-dire qu'il distribue les données à chaque machine destinataire, alors que le hub envoie toutes les données à toutes machines qui répondent. Conçu pour travailler sur des réseaux, avec un nombre de machines légèrement plus élevé que le hub, il élimine les collisions de paquets éventuelles



Exemple réseau entreprise



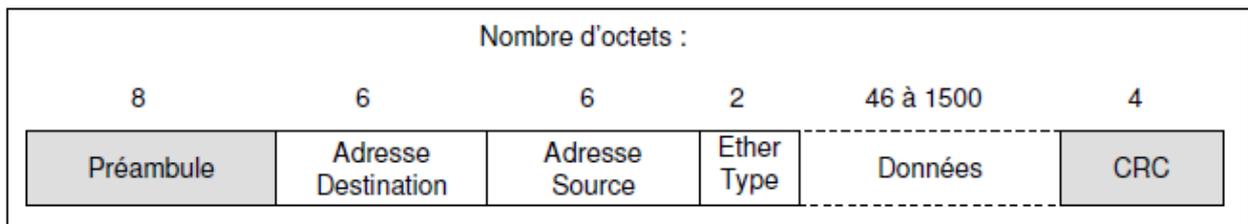
Exemple réseau domestique



3. L'Ethernet

Il est basé sur le principe de membres pairs sur le réseau (dans le cas de l'échange de fichiers sur des réseaux « pair à pair », les ordinateurs des internautes qui participent à l'échange sont tour à tour demandeur et donneur, client et serveur, la communication s'effectue sur un pied d'égalité).

Il envoie des messages dans ce qui était essentiellement un système radio, captif à l'intérieur d'un fil ou d'un canal commun, parfois appelé l'éther. Chaque pair est identifié par une clé globalement unique, appelée adresse MAC, pour s'assurer que tous les postes sur un réseau Ethernet aient des adresses distinctes.



Préambule : (8 octets)

Annonce le début de la trame et permet la synchronisation. Il contient 8 octets dont la valeur est 10101010 (on alterne des 1 et des 0), sauf pour le dernier octet dont les 2 derniers bits sont à 1.

Adresse Destination : (6 octets)

Adresse physique de la carte Ethernet destinataire de la trame. On représente une adresse Ethernet comme ses 6 octets en hexadécimal séparés par des ':'.

Exemple : **08:00:07:5c:10:0a**

Adresse Source : (6 octets)

Adresse physique de la carte Ethernet émettrice de la trame.

EtherType : ou type de trame (2 octets)

Indique quel protocole est concerné par le message. La carte réalise un démultiplexage en fournissant les données au protocole concerné.

Exemple de type de protocole

- 0x0800 : [IPv4](#)
- 0x86DD : [IPv6](#)
- 0x0806 : [ARP](#)
- 0x8035 : [RARP](#)
- 0x809B : AppleTalk
- 0x88CD : [SERCOS III](#)
- 0x0600 : XNS
- 0x8100 : [IEEE 802.1Q](#)

Données : (46 à 1500 octets)

Les données véhiculées par la trame. Sur la station destinataire de la trame, ces octets seront communiqués à l'entité (protocole) indiquée par le champ EtherType. Notons que la taille minimale des données est 46 octets. Des octets à 0, dits de "bourrage", sont utilisés pour compléter des données dont la taille est inférieure à 46 octets.

CRC : (Cyclic Redundancy Code)

Champ de contrôle de la redondance cyclique. Permet de s'assurer que la trame a été correctement transmise et que les données peuvent donc être délivrées au protocole destinataire.

4. Problème de sécurité

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde.

4.1. Les standards de sécurité

Il existe plusieurs protocoles

- WEP
- WPA
- WPA2

4.1.1. WEP

Le **Wired Equivalent Privacy** (abrégé **WEP**) est un protocole pour sécuriser les réseaux sans fil de type Wi-Fi. Les réseaux sans fil diffusant les messages échangés par ondes radioélectriques, sont particulièrement sensibles aux écoutes clandestines. Le WEP tient son nom du fait qu'il devait fournir aux réseaux sans fil une confidentialité comparable à celle d'un réseau local filaire classique.

Cependant, plusieurs faiblesses graves ont été identifiées par les cryptologues. Le WEP est parfois surnommé avec le sobriquet de Weak Encryption Protocol. Le WEP a donc été supplanté par le WPA en 2003, puis par le WPA2 en 2004 (WPA2 est la version de la norme IEEE 802.11i certifiée par la Wi-Fi Alliance).

Le WEP 64 bits utilise une clé de chiffrement de 40 bits à laquelle est concaténé un vecteur d'initialisation (initialization vector ou IV en anglais) de 24 bits. La clé et le vecteur d'initialisation forment ainsi une clé RC4 de 64 bits permettant de chiffrer les données échangées.

Un vecteur d'initialisation (en anglais initialization vector ou IV) est un bloc de bits combiné avec le premier bloc de données lors d'une opération de chiffrement. Il est utilisé dans le cadre des modes d'opération d'un algorithme de chiffrement symétrique par blocs ou pour un chiffrement par flux comme RC4.

4.1.2.WPA

Il respecte la majorité de la norme IEEE 802.11i et a été prévu comme une solution intermédiaire pour remplacer le WEP en attendant que la norme 802.11i soit terminée. WPA a été conçu pour fonctionner, après mise à jour de leur micro-logiciel, avec toutes les cartes Wi-Fi, mais pas nécessairement avec la première génération des points d'accès Wi-Fi.

Il est conçu pour les réseaux personnels ou de petites entreprises, car il n'y a pas besoin d'utiliser un serveur d'authentification. Chaque équipement du réseau sans fil s'authentifie auprès du point d'accès en utilisant la même clé sur 256 bits.

Les données sont chiffrées en utilisant l'algorithme de chiffrement par flot RC4, avec une clé de 128 bits et un vecteur d'initialisation (initialization vector ou IV en anglais) de 48 bits.

4.1.3.WPA2

Successeur du WPA, il comprend tous les éléments obligatoires de la norme 802.11i. C'est la version de la norme IEEE 802.11i certifiée par la Wi-Fi Alliance. En particulier, la norme WPA2 impose de prendre en charge le mécanisme CCMP, lequel s'appuie sur AES. Le protocole CCMP est considéré comme complètement sécurisé ; en mai 2004, le NIST (National Institute of Standards and Technology) l'a approuvé. Il est pris en charge depuis 2005 sur Windows XP et par tous les Macintosh comportant une carte AirPort Extreme.

Le standard WPA définit deux modes distincts :

- WPA-PSK Mode : repose sur l'utilisation d'un secret partagé pour l'authentification ;
- WPA Enterprise Mode : repose sur l'utilisation d'un serveur RADIUS pour l'authentification.

Exemple paramétrage sécurité wifi :

NETGEAR
Connect with Innovation™

Configuration | Monitoring | Maintenance | Support

System | IP | Wireless | **Security** | Wireless Bridge | WPS

Profile Settings
Advanced

Edit Security Profile

Profile Definition

Wireless Network Name (SSID)

Broadcast Wireless Network Name (SSID) Yes No

Authentication Settings

Network Authentication

Data Encryption

WPA Type PSK Passphrase

WPA Passphrase (Network Key)

WPA PSK

Wireless Client Security Separation

5. Commandes réseau

5.1. Ping suivi de l'adresse Ip avec un espace entre les deux

Vérifie la connectivité IP d'un ordinateur utilisant le protocole TCP/IP en envoyant des messages (requête écho) dans le but d'avoir des réponses d'une machine. Ping utilise le protocole ICMP (Internet Control Message Protocol). Les réponses à la requête écho, s'affichent, avec les temps des parcours circulaires.

```
C:\Users\ >ping 192.168.1.10
Envoi d'une requête 'Ping' 192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

5.2. Nslookup

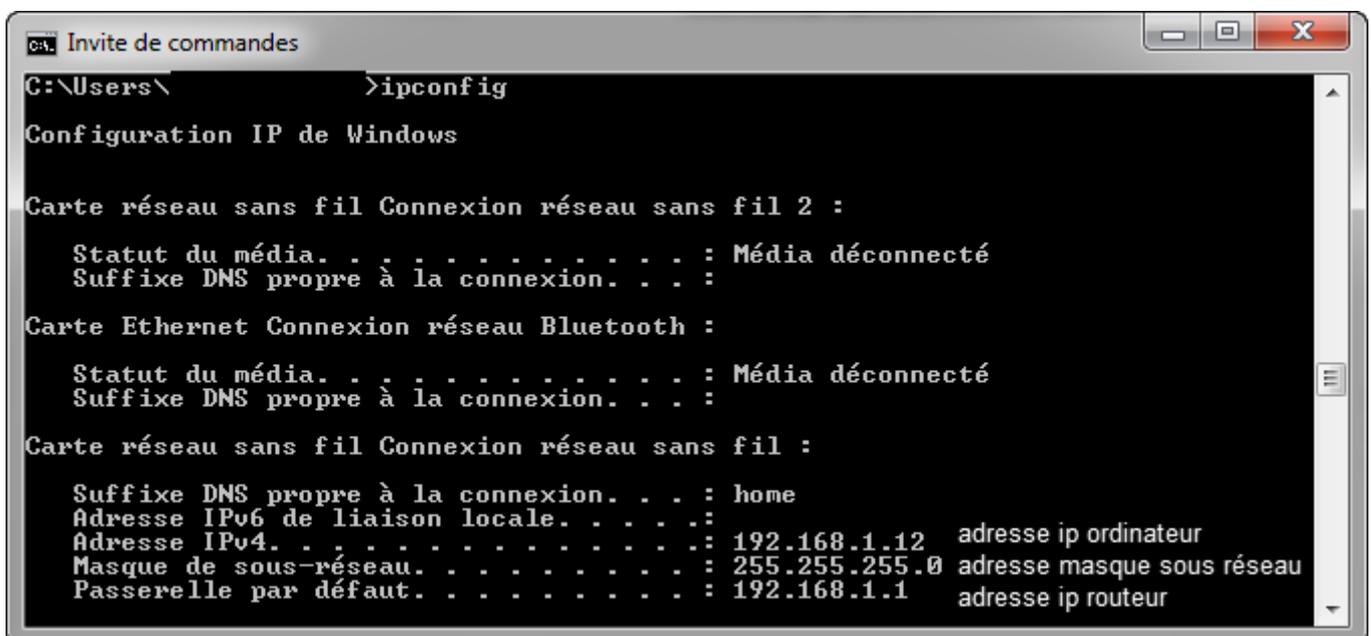
Affiche des informations que vous pouvez utiliser pour diagnostiquer l'infrastructure DNS (Domain Name System). Affiche les correspondances entre les noms de domaine et les adresses IP.

5.3. Tracert (= traceroute sous Unix)

Détermine l'itinéraire vers une destination par la transmission de messages ICMP (messages Requête d'écho). L'itinéraire affiché correspond à la série d'interfaces de routeurs sur l'itinéraire situé entre un hôte source et une destination. Utilisée sans paramètre, la commande tracert permet d'afficher l'aide.

5.4. Ipconfig (=ifconfig sous unix)

Affiche toutes les valeurs de la configuration du réseau TCP/IP et actualise les paramètres DHCP (Dynamic Host Configuration Protocol) et DNS (Domain Name System). Utilisé sans paramètres, Ipconfig affiche l'adresse IP, le masque de sous-réseau et la passerelle par défaut de toutes les cartes.



```
CA Invite de commandes
C:\Users\ >ipconfig

Configuration IP de Windows

Carte réseau sans fil Connexion réseau sans fil 2 :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Ethernet Connexion réseau Bluetooth :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

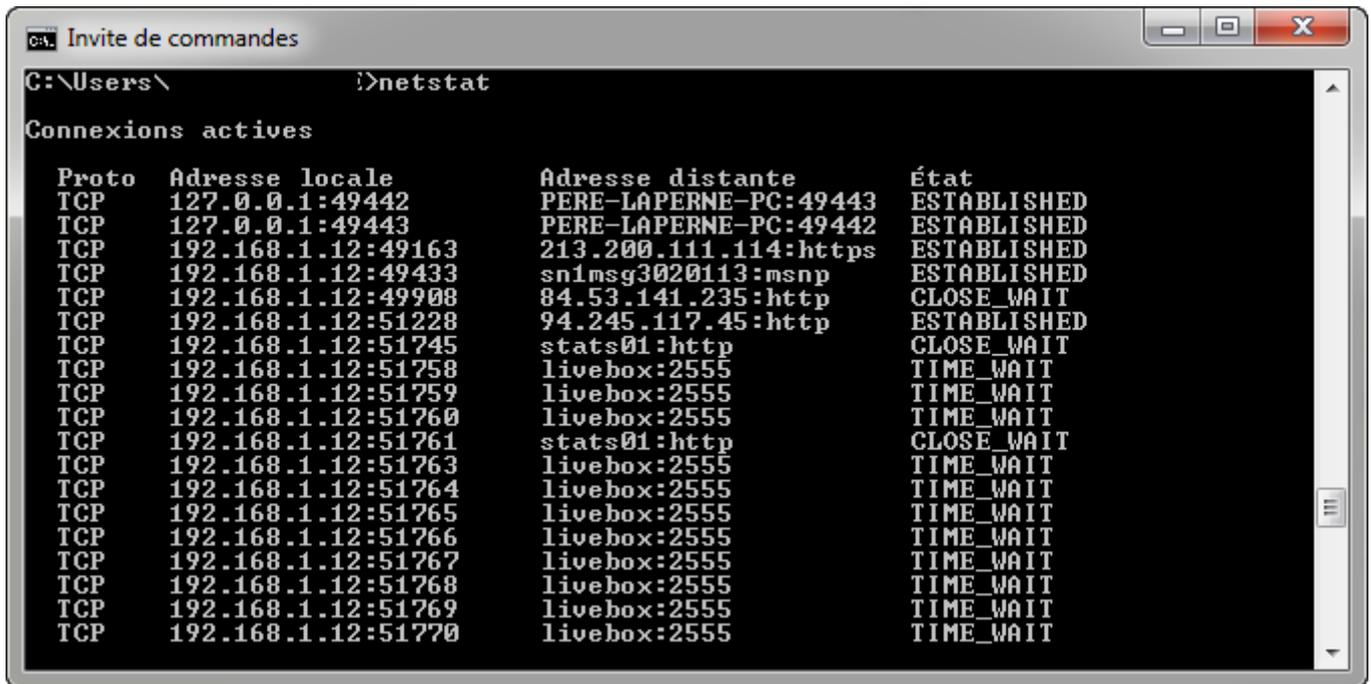
Carte réseau sans fil Connexion réseau sans fil :
    Suffixe DNS propre à la connexion. . . : home
    Adresse IPv6 de liaison locale. . . . :
    Adresse IPv4. . . . . : 192.168.1.12  adresse ip ordinateur
    Masque de sous-réseau. . . . . : 255.255.255.0  adresse masque sous réseau
    Passerelle par défaut. . . . . : 192.168.1.1  adresse ip routeur
```

5.5. Ipconfig/all

Affiche un résumé des propriétés IP des cartes réseaux

5.6. Netstat

Affiche les connexions TCP actives et les ports sur lesquels l'ordinateur écoute, il affiche aussi la table de routage IP et les statistiques Ethernet, IPv4 et IPv6 (pour les protocoles IP, ICMP, TCP et UDP). Utilisée sans paramètre, la commande Netstat affiche les connexions TCP actives.



```
C:\Users\>netstat

Connexions actives

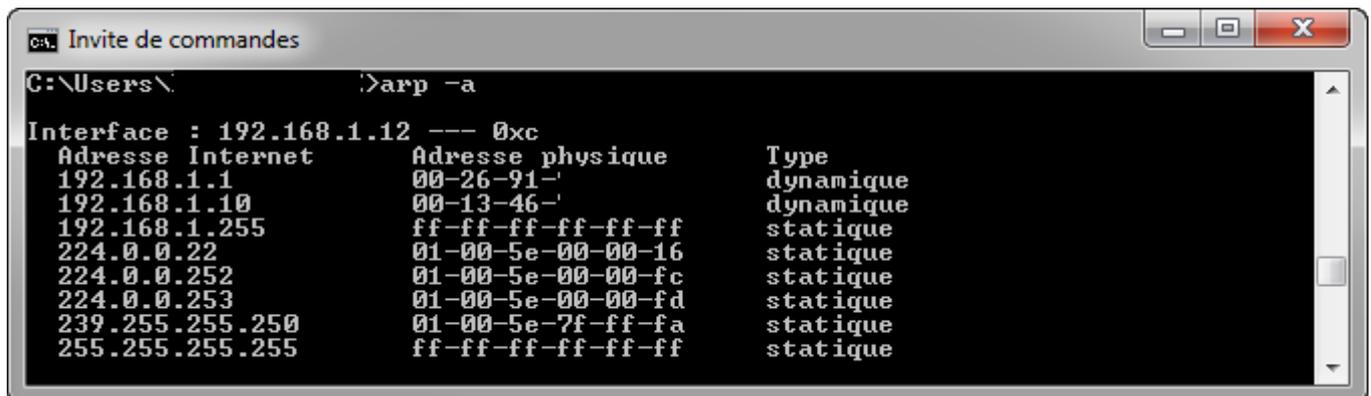
Proto  Adresse locale          Adresse distante        État
TCP    127.0.0.1:49442         PERE-LAPERNE-PC:49443  ESTABLISHED
TCP    127.0.0.1:49443         PERE-LAPERNE-PC:49442  ESTABLISHED
TCP    192.168.1.12:49163      213.200.111.114:https   ESTABLISHED
TCP    192.168.1.12:49433      sn1msg3020113:msnp     ESTABLISHED
TCP    192.168.1.12:49908      84.53.141.235:http     CLOSE_WAIT
TCP    192.168.1.12:51228      94.245.117.45:http     ESTABLISHED
TCP    192.168.1.12:51745      stats01:http           CLOSE_WAIT
TCP    192.168.1.12:51758      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51759      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51760      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51761      stats01:http           CLOSE_WAIT
TCP    192.168.1.12:51763      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51764      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51765      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51766      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51767      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51768      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51769      livebox:2555           TIME_WAIT
TCP    192.168.1.12:51770      livebox:2555           TIME_WAIT
```

5.7. Route

Affiche et modifie les entrées dans la table de routage IP locale. Utilisée sans paramètres, la commande route permet d'afficher l'aide.

5.8. Arp -a

Affiche la correspondance IP / adresse mac des ordinateurs et périphériques connectés. Les correspondances dynamiques utilisent le DHCP pour configurer l'adresse IP.



```
C:\Users\>arp -a

Interface : 192.168.1.12 --- 0xc
Adresse Internet    Adresse physique      Type
192.168.1.1         00-26-91-'           dynamique
192.168.1.10        00-13-46-'           dynamique
192.168.1.255       ff-ff-ff-ff-ff-ff    statique
224.0.0.22          01-00-5e-00-00-16    statique
224.0.0.252         01-00-5e-00-00-fc    statique
224.0.0.253         01-00-5e-00-00-fd    statique
239.255.255.250     01-00-5e-7f-ff-fa    statique
255.255.255.255     ff-ff-ff-ff-ff-ff    statique
```