Télécommunications et réseaux  
Résumé  
2017/2018

Auteur original : Inconnus

Mise en page : Youri Iacono

Table des matières

[Chapitre 1 : Introduction 8](#_Toc515727283)

[1. Les différentes tailles 8](#_Toc515727284)

[ PAN (Personal Area Network) 8](#_Toc515727285)

[ LAN (Local Area Network) 8](#_Toc515727286)

[ MAN (Metropolitan Area Network) 8](#_Toc515727287)

[ WAN (Wide Area Network) 8](#_Toc515727288)

[2. Les différentes technologies de transmission 9](#_Toc515727289)

[3. Les différentes topologies 9](#_Toc515727290)

[La topologie physique 9](#_Toc515727291)

[La topologie logique 9](#_Toc515727292)

[4. Mode de fonctionnement des réseaux 10](#_Toc515727293)

[5. Internet 10](#_Toc515727294)

[6. Manières d'accéder à Internet 11](#_Toc515727295)

[7. La segmentation et le multiplexage 12](#_Toc515727296)

[8. L'architecture d'un réseau 12](#_Toc515727297)

[La tolérance aux pannes 12](#_Toc515727298)

[L'évolutivité 12](#_Toc515727299)

[La qualité de service 12](#_Toc515727300)

[La sécurité 12](#_Toc515727301)

[9. BYOD 12](#_Toc515727302)

[10. La virtualisation 12](#_Toc515727303)

[11. Le cloud computing 13](#_Toc515727304)

[12. Le CPL (Courant Porteur de Ligne) 13](#_Toc515727305)

[13. Le Big Data 13](#_Toc515727306)

[Chapitre 2 : Communication et protocoles réseaux 13](#_Toc515727307)

[1. Protocole 13](#_Toc515727308)

[2. Codage d'un message 13](#_Toc515727309)

[3. L'encapsulation et la désencapsulassions 14](#_Toc515727310)

[4. Taille des messages 14](#_Toc515727311)

[5. Synchronisation des messages 14](#_Toc515727312)

[6. Option de remise des messages 14](#_Toc515727313)

[7. Protocole propriétaire 14](#_Toc515727314)

[8. Acronymes des protocoles à connaître 14](#_Toc515727315)

[Protocoles de la couche application : 14](#_Toc515727316)

[Protocoles de la couche transport : 15](#_Toc515727317)

[Protocoles de la couche internet : 15](#_Toc515727318)

[Protocoles de la couche réseau : 15](#_Toc515727319)

[9. Acronymes des sociétés de merde 15](#_Toc515727320)

[10. OSI et TCP/IP 16](#_Toc515727321)

[11. Adresse réseau et adresse liaison de données 17](#_Toc515727322)

[Chapitre 3 : Accès réseau 17](#_Toc515727323)

[1. Les ≠ méthodes de codage 17](#_Toc515727324)

[Le codage NRZ (Non Return To Zero) 17](#_Toc515727325)

[Le codage Manchester 17](#_Toc515727326)

[2. Les ≠ types de transmissions 17](#_Toc515727327)

[Asynchrone 17](#_Toc515727328)

[Synchrone 17](#_Toc515727329)

[3. Les ≠ types de supports physiques 17](#_Toc515727330)

[Support de cuivre 17](#_Toc515727331)

[Câbles coaxiaux 18](#_Toc515727332)

[Fibre optique 18](#_Toc515727333)

[Support sans fils 19](#_Toc515727334)

[4. Comment déterminer le type d'un câble 19](#_Toc515727335)

[5. La composition d'une trame 20](#_Toc515727336)

[6. Méthodes d'accès 20](#_Toc515727337)

[Aloha 20](#_Toc515727338)

[CSMA (Carrier Sense Multiple Access) 20](#_Toc515727339)

[CSMA/CD (Collision Detection) 20](#_Toc515727340)

[CSMA/CA (Collision Avoidance) 21](#_Toc515727341)

[Chapitre 4 : Ethernet 21](#_Toc515727342)

[1. Ethernet 21](#_Toc515727343)

[2. La couche liaison de donnée 21](#_Toc515727344)

[3. Adresse MAC 21](#_Toc515727345)

[4. Norme de taille d'une trame 22](#_Toc515727346)

[5. Les types d'adresses MAC 22](#_Toc515727347)

[Monodiffusion 22](#_Toc515727348)

[Diffusion 22](#_Toc515727349)

[Multidiffusion 22](#_Toc515727350)

[6. Protocole ARP 22](#_Toc515727351)

[Le 22](#_Toc515727352)

[13. Le commutateur (SWITCH) 23](#_Toc515727353)

[La table de commutation 23](#_Toc515727354)

[Les ≠ fonctions de bases 23](#_Toc515727355)

[14. Domaine de collisions et de diffusions 23](#_Toc515727356)

[Domaine de collision 23](#_Toc515727357)

[Domaine de diffusion 23](#_Toc515727358)

[15. La fonction auto-MDIX 24](#_Toc515727359)

[16. Méthodes de transmission de trames 24](#_Toc515727360)

[Store and forward 24](#_Toc515727361)

[Cut-through 24](#_Toc515727362)

[17. Mise en mémoire tampon 24](#_Toc515727363)

[Axée sur les ports 24](#_Toc515727364)

[Partagée 24](#_Toc515727365)

[Chapitre 5 : Système d'exploitation de réseau 25](#_Toc515727366)

[1. Périphériques intermédiaires 25](#_Toc515727367)

[2. Cisco IOS (Internetwork Operating System) 25](#_Toc515727368)

[3. Accéder au CLI (Console-Line interface) 25](#_Toc515727369)

[4. Modes d'exploitation Cisco IOS dans l'ordre croissant 25](#_Toc515727370)

[Chapitre 6 : Couche réseau 26](#_Toc515727371)

[1. La couche réseau 26](#_Toc515727372)

[2. Les caractéristiques du protocole IP (Internet Protocol) 26](#_Toc515727373)

[3. Le protocole IPv4 27](#_Toc515727374)

[4. Problèmes de l'IPv4 27](#_Toc515727375)

[5. Apparition de l'IPv6 27](#_Toc515727376)

[6. Le routeur 27](#_Toc515727377)

[Etapes lors du démarrage : 28](#_Toc515727378)

[7. Connexion et interfaces d'un routeur 28](#_Toc515727379)

[8. Le routage 28](#_Toc515727380)

[9. La table de routage 28](#_Toc515727381)

[Fonctionnement 28](#_Toc515727382)

[Chapitre 7 : Couche transport 29](#_Toc515727383)

[1. Introduction 29](#_Toc515727384)

[2. Objectifs de la couche transport 30](#_Toc515727385)

[3. Fiabilité de la couche transport 30](#_Toc515727386)

[4. Les protocoles TCP et UDP 30](#_Toc515727387)

[TCP (Transmission Control Protocol) 30](#_Toc515727388)

[UDP (User Datagram Protocol) 30](#_Toc515727389)

[5. Les numéros de port classé par l'IANA 31](#_Toc515727390)

[6. Etablissement d'une connexion TCP 31](#_Toc515727391)

[7. Fermeture d'une connexion TCP 31](#_Toc515727392)

[8. La taille de fenêtre 31](#_Toc515727393)

[9. Gestion des pertes de segments du TCP 32](#_Toc515727394)

[10. Protocole de la couche application utilisant UDP 32](#_Toc515727395)

[Chapitre 8 : Adressage IP 32](#_Toc515727396)

[1. Adressage IPv4 32](#_Toc515727397)

[2. Les ≠ classes d'adresses 33](#_Toc515727398)

[3. Solution pour pallier aux problèmes de l'IPv4 33](#_Toc515727399)

[Le CIDR (Classless Inter-Domain Routing) 33](#_Toc515727400)

[Utilisation du NAT 33](#_Toc515727401)

[4. Technique calcul IP réseau/diffusion/hôtes 34](#_Toc515727402)

[5. Coexistence IPv4 et IPv6 34](#_Toc515727403)

[Techniques de migration vers l'IPv6 34](#_Toc515727404)

[6. Adressage IPv6 35](#_Toc515727405)

[Règles : 35](#_Toc515727406)

[Adresse anycast 35](#_Toc515727407)

[Adresse de monodiffusion 35](#_Toc515727408)

[Chapitre 9 : Découpage réseau 36](#_Toc515727409)

[1. Comment découper un réseau correctement 36](#_Toc515727410)

[2. Exercice de découpage réseau 36](#_Toc515727411)

[Commercial 37](#_Toc515727412)

[Manufacture 37](#_Toc515727413)

[Marketing 37](#_Toc515727414)

[Info 37](#_Toc515727415)

[R&D (calmez vous les joueurs de call of) 37](#_Toc515727416)

[Dirlo 37](#_Toc515727417)

[Secrétariat 37](#_Toc515727418)

[Compta 37](#_Toc515727419)

[RH 37](#_Toc515727420)

[On rassemble ce qui doit être rassembler (même IP) et on remet dans l'ordre 38](#_Toc515727421)

[Exercice de segmentation sans aide (les consignes sont à droite, le tableau est presque vide de base) 39](#_Toc515727422)

[3. Segmentation IPv6 40](#_Toc515727423)

[1 ère solution 40](#_Toc515727424)

[2 -ème solution 40](#_Toc515727425)

[Chapitre 10 : La couche application 41](#_Toc515727426)

[1. Introduction 41](#_Toc515727427)

[2. Le protocole HTTP 41](#_Toc515727428)

[Caractéristiques du protocole HTTP 41](#_Toc515727429)

[Codes de statut 41](#_Toc515727430)

[Le cache 42](#_Toc515727431)

[Les cookies 42](#_Toc515727432)

[3. Les protocoles Email 42](#_Toc515727433)

[SMTP 42](#_Toc515727434)

[POP3 42](#_Toc515727435)

[IMAP 42](#_Toc515727436)

[4. DNS 42](#_Toc515727437)

[5. DHCP 42](#_Toc515727438)

[6. FTP 43](#_Toc515727439)

/! \ Cette synthèse ne contient aucune info ou très peu sur les débits des câbles / taille des composantes d'une trame, d'un paquet etc… Ce sera peut-être (voir sûrement demandé à l'examen) / ! \

Important les notions à connaître au niveau des TP sont sur Ecampus, dans le cours "Télécom. & réseau TP 1" dans le fichier "Notions fondamentales juin-sept 2017"

# Introduction

Un réseau est un ensemble d'équipements et de logiciels qui permettent l'acheminement d'une information d'un émetteur à un ou plusieurs récepteurs.

L'administrateur doit notamment s’occuper de :

* La gestion des besoins, du budget et des priorités.
* La gestion des ordinateurs et des périphériques
* La gestion des performances des systèmes.
* La gestion des utilisateurs.
* La gestion des fichiers et des disques.
* La gestion des services.
* La gestion des problèmes.
* La gestion des sauvegardes et du stockage des données. La gestion du réseau.
* La gestion de la sécurité.

## Les différentes tailles

### PAN (Personal Area Network)

Réseau simple permettant à des périphériques locaux de partager des fichiers

1 à 10m, exemple : Bluetooth

### LAN (Local Area Network)

Principalement utilisé dans les entreprises, les terminaux s'envoient des trames et n'ont pas besoin d'accès à internet

10m à 1km, exemple : campus

### MAN (Metropolitan Area Network)

Utilise principalement de la fibre optique afin de relier des bâtiments entre eux

1km à 100km, exemple : réseau FedMAN qui relie les bâtiments des administrations fédérales

### WAN (Wide Area Network)

Réseau qui couvre une grande zone géographique.

+ 100km, exemple : Internet

## Les différentes technologies de transmission

* La diffusion (Broadcast 🡪 envoie vers tt le monde)

Un seul support de transmission est partagé par tous les équipements connectés.

* Le point-à-point (Unicast 🡪 envoie vers un seul appareil)

Un seul support de transmission relie une paire d'équipements seulement.

Quand deux équipements non connectés directement entre eux veulent communiquer, ils le font par le biais des autres.

(il existe aussi le multicast pour envoyer à un groupe mais pas tout le monde

## Les différentes topologies

### La topologie physique

Arrangement spatial d'un réseau :

* Réseaux en mode de diffusion
  + Bus
  + Anneau
  + Réseaux en mode point-à-point
* Point-à-point
  + Étoile
  + Maillée

### La topologie logique

Manière dont les stations se partagent le support, on y retrouvera les IP et les ports :

* Ethernet

Repose sur une topologie de type bus linéaire (un seul support de transmission). La communication se fait à l'aide du protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detection) qui gère la manière dont les données sont transmises sur le réseau.

* Token Ring

Accès par jeton : seul le poste ayant le jeton peut transmettre sur le réseau.

Si un poste veut émettre il doit attendre jusqu'à ce qu'il ait le jeton.

* FDDI (Fiber Distributed Data Interface)

Utilise la fibre optique, il est constitué de deux anneaux : l'anneau primaire et l'anneau secondaire qui sert à rattraper les erreurs en cas de problème avec l'anneau primaire.

## Mode de fonctionnement des réseaux

Les périphériques connectés à un réseau s'appellent les périphériques finaux. Ils peuvent envoyer et recevoir un message sur le réseau et peuvent jouer le rôle de client, de serveur ou les deux.

* Les serveurs fournissent des informations
* Les clients demandent des informations et les affichent

Habituellement, on utilise un modèle client-serveur où le serveur est passif et répond aux demandes des clients

Il existe également le modèle P2P (Peer to Peer) qui permet à un ordinateur d'être client et serveur simultanément

Avantages du P2P

* Facile à configurer
* Coût faible
* Moins complexe
* Pratique pour les petits réseaux

Désavantages du P2P

* Pas d'administration centralisée
* Peu sécurisé
* Non évolutif
* Risque ralentissement car client et serveur en même temps

## Les composant d’un réseau

* Les périphériques
  + Hôtes -🡪 forment l’interface entre utilisateurs et le réseau de communication
  + Périphériques intermédiaires 🡪 relient les périphériques finaux
* Support de transmission 🡪 fournit le canal via lequel le message se déplace de la source à la destination grâce à :
  + Câblage en cuivre
    - Fibre optique
  + Transmission sans fil
* Les services et les processus 🡪 programme de communication

Connaitre différents icones pour schéma d’un réseau (p47)

* Carte réseau (nic (Network Internet Card) 🡪 fournit la connexion physique au réseau à partir d’un périphérique hôte
* Port physique 🡪 connection ou prise sur un périphérique réseau par lequel le support est connecté a un hôte
* Interface 🡪 port spécifiques d’un périphérique interréseau qui se connectent à des réseaux individuels

**Grace aux icones on pourra faire des diagrammes de topologie**

Des diagrammes de topologie physique – sur lesquels on va indiquer l'emplacement physique des périphériques intermédiaires, des ports configurés et des câbles. (p49)

Des diagrammes de topologie logique – sur lesquels on retrouvera les périphériques, les ports, et le schéma d'adressage IP. (p50)

## Internet

#### Internet

Ensemble mondial de réseaux interconnectés qui coopèrent pour échanger des informations en utilisant des normes.

#### Intranet

Réseau LAN privé d'une entreprise auquel peuvent accéder uniquement ses membres, ses employés ou des gens autorisés.

Généralement accessible uniquement depuis le site de l'entreprise.

#### Extranet

Utilisé lorsqu'une entreprise fournit un accès sécurisé aux personnes qui travaillent pour d'autres entreprises, mais qui ont besoin de données de l'entreprise en question. 

## Manières d'accéder à Internet

* Par câble

Offre une connexion haut débit.

Un modem sépare le signal Internet des autres signaux et fournit une connexion Ethernet à un ordinateur ou un LAN

* Par xDSL (Digital subscriber Line)

Fonctionne sur un ligne téléphonique divisée en trois canaux :

* Appels téléphoniques
* Download
* Upload

La qualité varie de la distance du central de la compagnie de téléphonie.

* + ADSL (Asymmetric DSL)

Exploite une autre bande fréquence, située au-dessus de celle pour la téléphonie pour échanger des données en parallèle avec une éventuelle conversation téléphonique

* + VDSL (Very-high-bite-rate DSL)

Permet d'atteindre d'obtenir un meilleur débit que les précédents

* + VDSL 2 (Very-high-bit-rate DSL 2)

Encore plus que le premier

* Par fibre

Plus la fibre est proche de l'utilisateur, plus la qualité de service sera meilleure.

Une image contenant texte, capture d’écran, Police, conception

Description générée automatiquement

Car les derniers mètres sont en cuivre, moins il y en a mieux c'est.

* Par satellite

Idéal pour ceux qui n'ont pas accès à la DSL ou au câble. Les débits sont en général élevés comme les frais d'installation.

* Par cellulaire

On peut accéder à Internet partout où il y a un signal cellulaire via notre téléphone.

Les performances sont limitées selon le téléphone et la station de base

* Le WiMax (Worldwide Interoperability For Microwave Access)

Technologie de transmission haut débit par ondes radio conçue pour couvrir des zones importantes (plusieurs km) créé par Intel et Alvarion

Le débit dépend de la distance, de la topographie des lieux et du nombre d'utilisateur sur le réseau

On l'utilise dans les zones rurales comme couverture haut débit avec une superficie importante ou comme hotspot Wi-Fi à une échelle plus étendue

## La segmentation et le multiplexage

La segmentation consiste à découper les données à envoyer en parties moins importantes

Le multiplexage consiste entremêler plusieurs conversations segmentées.

Le seul inconvénient est que ces techniques rendent les communications plus complexes car il va falloir étiqueter toutes les parties afin de les réassembler quand elles seront arrivées à destination.

## L'architecture d'un réseau

Il y a 4 caractéristiques à prendre en compte :

### La tolérance aux pannes

Il faut que le réseaux limite l'impact des pannes => redondance

### L'évolutivité

Lorsqu'un utilisateur vient s'ajouter à un réseau, il faut que les performances restes inchangées pour ceux qui y étaient déjà

=> Utilisation d'un modèle hiérarchisé à plusieurs couches

### La qualité de service

L'utilisateur exige un niveau de qualité et de service ininterrompu.

=> Utilisation de niveaux de priorités

### La sécurité

Avec l'évolution d'Internet comme moyen de transmission de communication, les exigeances en matière de sécu ont évoluées.

=> Mettre en place des mesures de sécurité

## BYOD

Consiste à offrir aux utilisateurs la possibilité d'utiliser leurs propres outils pour accéder aux informations et en envoyer.

## La virtualisation

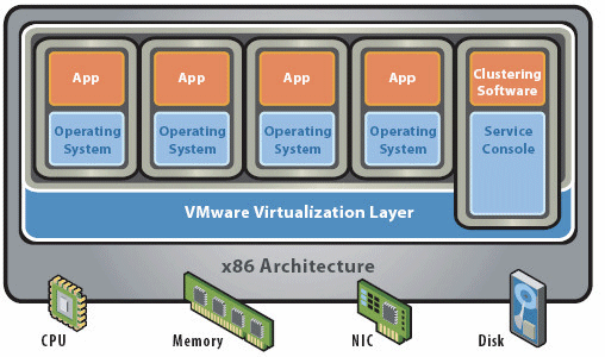
Consiste à faire fonctionner plusieurs systèmes, serveurs ou applications sur le même serveur physique.

Moins coûteux, portabilité, administration simplifiée mais pannes généralisées et coût de mise en œuvre important.

* Hyperviseur type 1

Outil qui s'interpose entre la couche matérielle et logicielle.

Il a accès aux composants de la machine et possède son propre noyau.



* Hyperviseur type 2

Application installée sur un système d'exploitation.

Les performances sont réduites mais propose une parfaite étanchéité entre les systèmes.

Une image contenant texte, capture d’écran, Rectangle, Parallèle

Description générée automatiquement

## Le cloud computing

Permet de stocker ou recevoir des fichiers sur des serveurs via Internet.

* Cloud personnalisé :

Conçus pour répondre aux besoins d'un secteur spécifique

* Cloud public :

Cloud dont les services et app. sont accessibles par tous. Ils peuvent être gratuit ou payant.

* Cloud privé :

Cloud dont les services et app. sont destinés à une entreprise ou à une entité spécifique

* Cloud hybride :

Cloud qui comporte au moins deux cloud.

Avantages

* Accès à tout moment via Internet
* Coûts d'infrastructure réduits,
* Permet de réagir rapidement aux besoins des clients

## Le CPL (Courant Porteur de Ligne)

Permet la construction d'un réseau informatique sur le réseau électrique d'une habitation Une image contenant Appareils électroniques

Description générée automatiquement

## Le Big Data

Solution pour permettre à tout le monde d'accéder en temps réel à des bases de données géantes

Règles des 3V :

* Volume des données considérables à traiter,
* Variété d'informations,
* Vélocité à atteindre = Fréquence de création, collecte et partage

# Système d'exploitation de réseau

DLNA (Digital Living Network Alliance) est une alliance de plus de 250 fabricants d'appareils électroniques, informatiques, etc.

## Périphériques intermédiaires

* Routeur => transfère les paquets de données vers Internet et reçoit des paquets depuis Internet
* Switch   => Connecte des périphériques finaux à l'aide de câbles réseau
* Point d'accès dans fil => émetteur radio capable de connecter des périphérique finaux sans fil
* Pare-feu => Sécurise le trafic sortant et nœud le trafic entrant

## Cisco IOS (Internetwork Operating System)

Terme générique utilisé pour désigner l'ensemble des systèmes d'exploitation réseau utilisés sur les périphériques Cisco.

Lorsqu'un ordinateur est mis sous tensions, il charge le système dans la mémoire vive (RAM). La partie du code du système d'exploitation directement liée au matériel informatique s'appelle le noyau. La partie liée aux applications et à l'utilisateur s'appelle l'interpréteur de commande.

Il est stocké dans la mémoire Flash (mémoire non volatil, ne se reset pas au reboot)

## Accéder au CLI (Console-Line interface)

* Via le port console (CTY)
* Via telnet ou SSH (Secure Shell) (VTY)
* Via le port AUX (ligne téléphonique commutée)

Telnet et SSH permettent un accès distant, SSH est plus sécurisé

**Périphérique cisco contient deux fichiers de configuration :**

* Fichier de configuration (running config) en cours utilisé pat le périphérique en fonctionnement normal
* Le fichier de configuration initial (initial config) chargé dans la mémoire vive que le périphérique démarre (copie sauvegarde de config)

## Modes d'exploitation Cisco IOS dans l'ordre croissant

* Mode d'exécnution utilisateur (visualisation) (symbole : > )
* Mode d'exécution privilégié (visualisation détaillée et accès à la configuration et gestion du périphérique) (symbole : # ) (commande : enable/disable)
* Mode de configuration globale (commandes de configuration globale sur l'équipement) (symbole : (config)# ) (commande :S1# config mode)
* Modes de configuration spécifiques (commandes de configuration d'un service ou d'une interface) (symbole : (config-if)# )

# Communication et protocoles réseaux

## Protocole

Un protocole est une suite de règles qui veillent à ce qu'un message soit correctement transmis et compris.

## Codage d'un message

Un message est d'abord codé en bits qui sont ensuite codé en impulsions électriques ou en ondes lumineuses selon le support

## L'encapsulation et la désencapsulassions

L'encapsulation est un processus permettant d'encapsuler un message dans un format spécifique appelé "trame",

Avant d'être transmis sur le réseau.

Cette trame contiendra l'adresse source, l'adresse de destination ainsi que les données encapsulées (MAC)

La désencapsulassions c'est l'inverse.

## Taille des messages

Lorsqu'un message est trop long, il doit être segmenté en plusieurs trames

## Synchronisation des messages

Méthode d'accès (moment de la prise de parole)

Contrôle de flux (débit de parole)

Délai d'attente de la réponse => réagit en cas de non réponse

## Option de remise des messages

Monodiffusion => un émetteur, un récepteur

Diffusion => un émetteur à tous les récepteurs

Multidiffusion => un émetteur à un groupe de récepteurs

## Protocole propriétaire

Cela signifie qu'une société ou qu'un fournisseur contrôle la définition du protocole et la manière dont il fonctionne

Une suite de protocole se nomme une norme et Il existe 2 types de normes :

* + Norme ouverte, Les normes ouvertes favorisent la concurrence et l'innovation. Elles empêchent également qu'un seul produit d'une entreprise monopolise le marché ou puisse bénéficier d'un avantage inique sur ses concurrents.
  + Les normes propriétaires, Les normes propriétaires sont développées et généralement utilisés par un constructeur qui ne fonctionnent donc qu’avec le matériel de celui-ci

## Acronymes des protocoles à connaître

### Protocoles de la couche application :

* **DNS (Domain Name System) :** A pour rôle de traduire les noms de domaines en adresse IP
* **DHCP (Dynamic Host Configuration Protocol)** : Attribue dynamiquement des adresses IP aux stations clientes au démarrage
* **SMTP (Simple Mail Transfert Protocol)** : Permet aux terminaux d’envoyer un mail à un serveur de messagerie
* **POP (Post Office Protocol)** : Permet aux clients de récupérer ou de télécharger des emails d’un serveur de messagerie
* **IMAP (Internet Message Access Protocol) :** Permet aux clients d’accéder aux emails stockés sur un serveur de messagerie
* **FTP (File Transfert Protocol)** : Permet à un hôte d’accéder à des fichiers sur un autre hôte du réseau et de transférer des fichiers vers un autre hôte du réseau
* **TFTP (Trivial File Transfert Protocol)**: Version simplifiée de FTP, pas d’authentification
* **HTTP (HyperText Transfert Protocol)** : Permet d’échanger du texte ou des fichiers multimédia sur le web

### Protocoles de la couche transport :

* **UDP (User Datagram Protocol)**: Permet à un processus exécuté sur un hôte d’envoyer des paquets à un processus exécuté sur un autre hôte mais sans connexion et sans confirmation de la transmission de datagrammes
* **TCP (Transmission Control Protocol**) : Au contraire d’UDP, permet une connexion fiable entre les processus s’exécutant sur des hôtes distincts

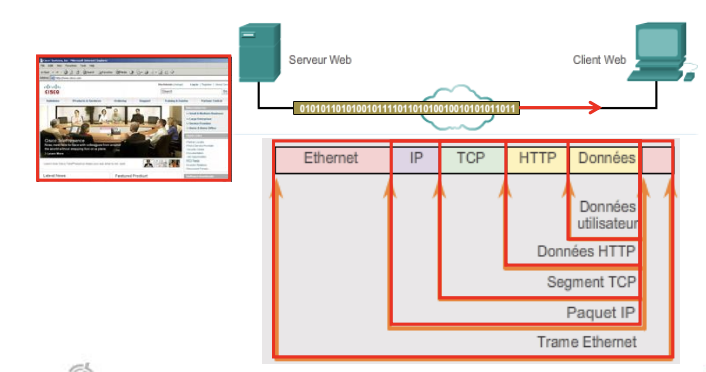
### Protocoles de la couche internet :

* **IP (Internet Protocol)**: Permet de recevoir des segments de message de la couche transport. Il regroupe les messages en paquets et indique leur adresse pour permettre leur acheminement de bout en bout sur un interréseau
* **NAT (Network Address Translation**) : Permet de convertir les adresses IP d’un privé en adresses IP globales et publiques
* **ICMP (Internet Control Message Protocol**) : Permet à l’hôte de destination de signaler à l’hôte source des erreurs liées aux transmissions de paquets
* **OSPF (Open Shortest Path First**) : Protocole de routage à états de liens permettant de faire du routage dynamique
* **EIGRP (Enhanced Interior Gateway Routing Protocol**) : Protocole de routage dynamique propriétaire à Cisco

### Protocoles de la couche réseau :

* **ARP (Address Resolution Protocol**) : Fournit un mappage dynamique entre une adresse logique (IP) et une adresse physique (MAC)
* **PPP (Point to Point Protocol)**: Permet d’encapsuler des paquets pour les transmettre via une connexion en série

Concrètement comment se passe un échange entre 2 périphériques utilisant le modèle TCP/IP



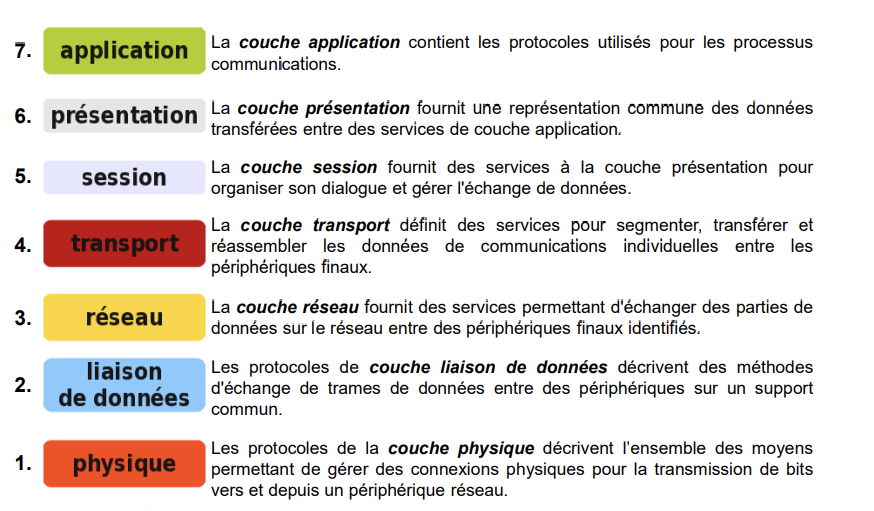
## Acronymes des sociétés de normalisations

* Internet Society (ISOC) qui est chargée de promouvoir le développement, l'évolution et l'utilisation ouverte d'Internet dans le monde entier
* Internet Architecture Board (IAB) qui s’occupe de la gestion et du développement général des normes sur Internet
* **Internet Engineering Task Force (IETF) qui a pour but de développer, de mettre à jour et d’assurer la maintenance d’Internet et des technologies TCP/IP. L'IETF se compose de différents groupes de travail qui constituent les principales entités de développement des spécifications et des recommandations de l'organisme**
* Internet Research Task Force (IRTF) qui se concentre sur la recherche à long terme liée à Internet, aux protocoles TCP/IP, aux applications, aux technologiques et à l’architecture
* **L’Institute of Electronical and Electronics Engineers (IEEE) qui est une association américaine professionnelle s'adressant aux spécialistes du génie électrique et de l'électronique qui souhaitent se consacrer à l'innovation (A créer Ethernet, et le WLAN)**
* **l'organisation internationale de normalisation (ISO). Célèbre pour son modèle OSI**
* L’EIA (Electronic Industries Alliance) connue pour ses normes associées au câblage électrique, aux connecteurs et aux racks de 19 pouces utilisés pour monter l’équipement réseau.
* La TIA (Telecommunications Industry Association) est responsable du développement des normes de communication dans un grand nombre de domaines.
* L’ITU-T (secteur de la normalisation des télécommunications de l’Union Internationale des Télécommunications) définit des normes de compression, de télévision sur IP
* L’ICANN (Internet Corporation for Assigned Names and Numbers) est une association à but non lucratif basée aux états unis qui coordonne l’attribution des adresses IP, la gestion des noms de domaine utilisés par le protocole DNS et les identificateurs de protocole ou numéro de ports utilisés par les protocoles TCP et UDP.
* **L’IANA (Internet Assigned Numbers Authority) est une composante de l’ICANN chargée de superviser et de gérer l’affection des adresses IP, la gestion des noms de domaines et les identificateurs pour le compte de l’ICANN**.

Il existe 2 types de modèles réseau de base

* + Le modèle de protocole, qui suit la structure d'une suite de protocoles donnée. L'ensemble hiérarchique des protocoles associés dans une suite représente généralement toutes les fonctionnalités requises à l'interface entre le réseau humain et le réseau de données. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche des protocoles au sein de la suite TCP/IP.
  + Le modèle de référence assure la cohérence de tous les types de protocoles et services réseau en décrivant les opérations à effectuer à chaque couche, mais n'indique pas leur mise en œuvre. Un modèle de référence, comme le modèle OSI, n'est pas destiné à être une spécification d'implémentation, ni à fournir un niveau de détail suffisant pour définir précisément les services de l'architecture réseau. Le principal objectif d'un modèle de référence est d'assurer une compréhension plus claire des fonctions et des processus impliqués.

## OSI et TCP/IP



Application : contient protocole pour processus communication

Présentation : fournit représentation commune des données transférées entre services de couches application

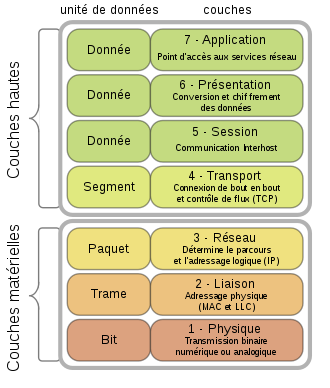
Session : fournit services a la couches présentation pour organiser son dialogue et gérer l’échange de données

Transport : définit des services pour découper, transférer et réassembler les données entre les périphériques finaux

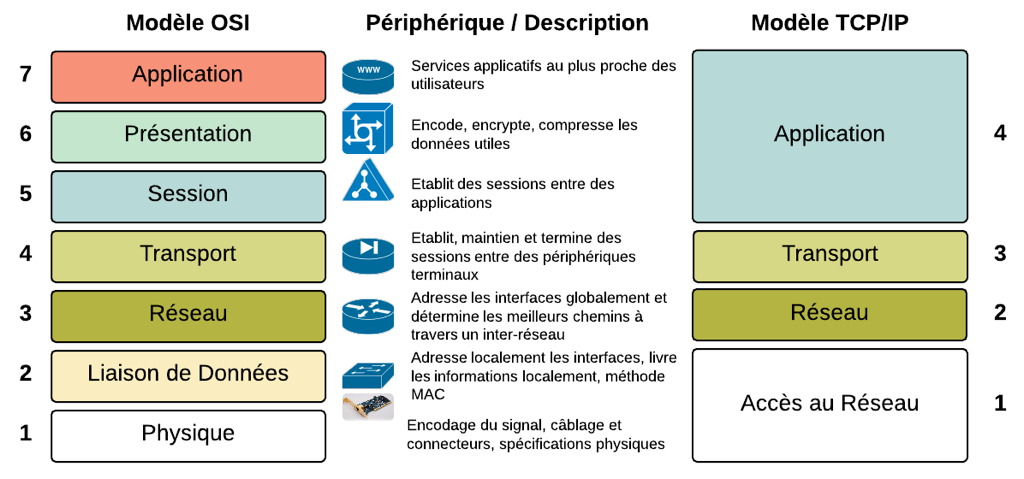
Réseau : fournit des services qui permet d’échanger des bout de données sur le réseau entre 2 périphérique finaux

Liaison de données : décrit les méthodes d'échange de trames de données entre des périphériques sur un support commun.

Physique : décrit l’ensemble des moyens qui permet de gérer des connexion physique pour transmettre des bits vers et depuis un périphérique réseau



|  |  |
| --- | --- |
| OSI : PLRTSPA | TCP/IP : AITA |



Attention modèle TCP/IP couche 2 = Internet pas réseau !

POUT TCP/IP SE CONSTITUE COMME CA :

**Application** : Représente des données pour l’utilisateur, ainsi que du codage et un contrôle du dialogue

**Transport** : prend en charge la communication entre différents périphériques à travers divers réseau

**Internet** : détermine le meilleur chemin à travers le réseau

**Accès réseau :** contrôle les périphériques matériels et les supports qui constituent le réseau

* + Les couches 5, 6 et 7 du modèle OSI servent de références aux développeurs et aux éditeurs de logiciels d’application pour créer des applications fonctionnant sur les réseaux ---------- La couche application TCP/IP inclut plusieurs protocoles qui fournissent des fonctionnalités spécifiques aux applications des utilisateurs finaux
  + La couche 4 du modèle OSI décrit les services et les fonctionnalités de base qui assurent l'ordre et la fiabilité des données acheminées entre les hôtes source et de destination ------------ les protocoles TCP et UDP de la suite TCP/IP fournissent les fonctionnalités nécessaires.
  + La couche 3 du modèle OSI décrit l'éventail de processus qui interviennent dans tous les réseaux de données afin d'adresser et d'acheminer les messages à travers le réseau. -------------- idem TCP/IP

## Adresse réseau et adresse liaison de données

Dans un paquet IP, on retrouve deux adresses logiques : l’IP source et l’IP destination

➢ **L'adresse de liaison de données source** : adresse physique du périphérique qui envoie le paquet. Initialement, c'est la carte réseau qui est la source du paquet IP.

➢ **L'adresse de liaison de données de destination** : adresse physique de l'interface réseau du routeur du tronçon suivant ou de l'interface réseau du périphérique de destination

Dans une trame de liaison de données on retrouve deux adresses physiques : l'adresse MAC source et l'adresse MAC destination

Les adresses MAC sont formées de 48 bits et sont physiquement intégrées à la carte réseau(si héxadecimal -> divisé par 4 donc écrit en 12 bit.

Afin de déterminer l'adresse MAC d'un autre périphérique, on va utiliser le protocole ARP qui permet de déterminer l'adresse MAC d'une station à partir de son adresse IP en effectuant une diffusion.

Dans un tableau ARP, on a donc chaque entrée (ou ligne) qui comporte deux valeurs : une adresse IP et une adresse MAC.

Le tableau ARP peut se remplir de 2 facons :

* + la première étant de manière dynamique
    - En surveillant le trafic et en copiant l’adresse MAC et IP quand elle passe
    - En diffusant une requête ARP (Il demande que celui avec l’adresse ip … lui envoie l’adresse MAC qui lui est lié)
  + Entrées statiques

Un routeur peut aussi être appelé **Passerelle par défaut** (ça peut aussi être l’adresse IP d’un périphérique)

(CHAPITRE 2 PAGE 33)

# Accès réseau

**Comment se connecter a un réseau => grâce aux cartes réseaux (NIC)**

**Il existe 3 formes élémentaires de support réseau :**

* + **Cable de cuivre (signaux de variation d’impulsion électrique)**
  + **Fibre optique (signaux de variations lumineuse)**
  + **Sans fil (signaux de variation de transmission radio**

**Principes fondamentaux de la couche physique :**

## **1.Les composants physique**

C’est les périphérique électroniques, des supports et des connecteurs qui transportent et transmettent les signaux pour représenter les bits

**2. Le codage :**

Le codage de données est une méthode permettant de convertir un flux de bits de données en code prédéfini

## Les ≠ méthodes de codage

### Le codage NRZ (Non Return To Zero)

Le flux de bits est transmis en tant que série de valeurs de tension (tension basse = 0 ; tension haute = 1) (utilisation nule de bande passante et sensible aux interférence électromagnétique

### Le codage Manchester

Représente les valeurs binaires comme des transitions de tension (tensions faible vers éleve = 1 ; tension élevé vers faible =0)

## **3. La signalisation**

La méthode de représentation des bits est appelée méthode de signalisation.

## Les ≠ types de transmissions

### Asynchrone

L'intervalle de temps entre les caractères ou les blocs de donnés peut être défini arbitrairement

--> Les trames doivent contenir des indicateurs de début et de fin.

### Synchrone

Les signaux de données sont envoyés synchronisé. Cela se fait à l'aide d'un signal d'horloge échangé entre les deux périphériques qui doivent communiquer.

La **modulation** est le processus par lequel la caractéristique d'une onde (signal) modifie une autre onde (porteuse).

Modulation de fréquence (FM)

Modulation d’Amplitude (AM)

Modulation par impulsion et codage (PCM) technique dans laquelle un signal analogique (audio), est converti en un signal numérique en échantillonnant l'amplitude du signal et en exprimant les différentes amplitudes sous forme binaire.

----------------------

**La bande passante** est la capacité d'un support à transporter des données et elle est déterminé par :

* + Les propriétés des supports physiques
  + les technologies choisies pour signaliser et détecter les signaux réseau

Pour mesurer la qualité de la bande passante on utilise

* + La latence (le temps pour une donnée de voyager entre un point A et B
  + Le débit (c’est la mesure du transfert de bits sur le support pendant une période donnée) (généralement inférieur a la bande passante car il dépend de la quantité de trafic, le type de trafic et la latence créée par les différent périphérique réseau situé entre la source et la destination
  + Le débit applicatif (mesure les données utilisables transférées sur une période donnée.) (Débit applicatif = Débit **-** la surcharge de trafic pour l'établissement de sessions, les accusés de réception, l'encapsulation et les bits retransmis

## Les ≠ types de supports physiques

### Support de cuivre

Plus souvent utilisé car bon marché, facile à installer donnée transmises sous forme d’impulsions électrique et présente une faible résistance au courant électrique.

Limités par la distance et les interférences du signal.

Risques :

* Interférences électromagnétiques (EMI) ou radioélectriques (RFI)

Déforme et détériore les signaux de données => blindage, mise à la terre

* Diaphonie

Perturbation d'un câble causée par les champs électrique ou magnétiques d'un signal d'un câble adjacent => « solution » torsader les paires de fils

Cable UTP => Cable à paire torsadées non blindées (Unshielded Twisted Pair) => réseaux locaux ethernet

### • Catégorie 5 : La catégorie 5 permet une bande passante de 100 MHz. Ce standard permet l'utilisation du 100BASE-TX et du 1000BASE-T, ainsi que diverses applications de téléphonie ou de réseaux (« Token Ring »).

### • Catégorie 5e : cette catégorie de câble est une adaptation de la catégorie 5. Elle permet une vitesse allant jusqu'à 1000 Mbits/s pour une bande passante max de 100 MHz. Ce type de câblage peut être utilisé sur une distance max de 100m.

### • Catégorie 6 : ce type de câble permet une bande passante max de 250 MHz et un débit maximum de 10Gbit/s. Sa distance maximum d’utilisation est de 55m.

### • Catégorie 7 : cette catégorie de câblage permet l’utilisation d’une bande passante de 600 MHz sur une distance courte (max 15m) et permet un débit allant jusqu’à 100 Gbit/s.

• Catégorie 7a : cette version permet l’utilisation d’une bande passante de 1GHz sur une distance max de 100m avec un débit max pouvant toujours atteindre les 100 Gbit/s.

• Catégorie 8 : cette catégorie permet d’atteindre les 40Gbit/s sur une distance max de 30m avec une bande passante de 2GHz.

### **Câbles coaxiaux**

Composé d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.

Sur ce matériau isolant, il y une torsade de cuivre ou une feuille métallique.

La gaine enveloppe le tout.

Il existe différent connecteur pour ces cables mais le plus utilisé et le BNC

### **Fibre optique**

Il s'agit d'un fil en verre très pur (silice), transparent, flexible et très fin (diamètre d’un cheveux humain).

Les bits y sont codés sous forme d'impulsions lumineuses, le câble sert de guide d'ondes qui transmet de la lumière entre les deux extrémités

Avec un minimum de perte de signal.

Elle peut fonctionner à des longueurs bien supérieures aux supports en cuivre sans régénération de signaux.

Désavantages : coût élevé, matériel différent, manipulation délicate

Domaine d’application : réseaux d'entreprise, FTTH(Fiber To The Home), réseaux longue distance(Millier Km), réseaux sous-marins

Composition : (en commençant du cente) cœur => enveloppe => gaine intermédiaire => renforcement => gaine générale

Type de source lumineuse utilisé dans la fibre optique :

Les lasers (DL) ou les diodes électroluminescentes (DEL) génèrent les impulsions lumineuses utilisées pour représenter les données transmises sous forme de bits sur le support.

Des dispositifs à semi-conducteur électronique appelés photodiodes détectent les impulsions lumineuses et les convertissent en tensions qui peuvent ensuite être reconstituées en trames de données.

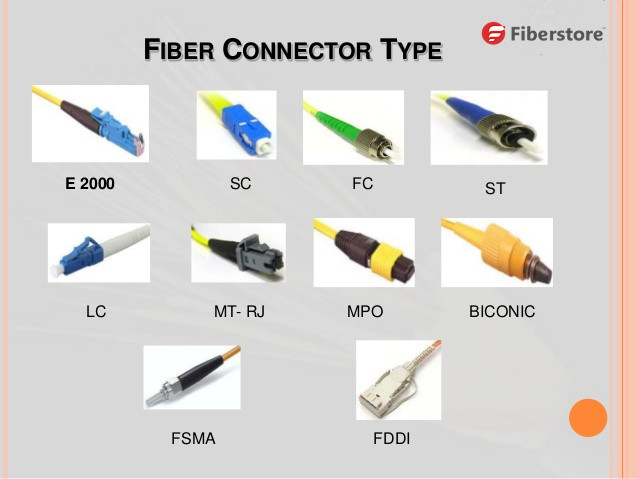
La formule suivante permet de connaitre l’angle critique au dessus duquel le faisceau serra entièrement réfléchi 🡪 θcritique = arcsin(ng /nc )

Il existe deux types de fibre optique:

* **Monomode (SMF) :**

Transporte un seul rayon lumineux souvent émis par un laser (DL) , peut aller jusqu'à 100km, cœur de petit diamètre (8 à 10 microns(10^-6)), moins de dispersion

* **Multimode (MMF)** :  Transporte plusieurs rayons lumineux incohérents, la lumière émise des DEL entre selon différents angles, cœur + large (50 à 62,5 microns), + de dispersion, 2km +-



Faire / ! \ à l'alignement, l'écart à l'extrémité, finition de l'extrémité

**Le connecteur SC (« Suscriber Connector »)** est un connecteur carré fonctionnant par encliquetage (couplage push-pull), ce qui garantit l’insertion dans le bon sens. Il est largement utilisé avec de la fibre optique monomode ou multimode. Son faible coût et sa facilité d'utilisation en font un connecteur très réputé sur le marché.

▪ **Le connecteur LC (« Lucent Connector »)** est un petit connecteur SC. Ainsi, avec les mêmes propriétés, on peut le placer dans des endroits plus difficile d’accès

**Le connecteur ST (« Straight Tip »)** est l'un des premiers types de connecteur utilisés. Ce connecteur offre un verrouillage sécurisé grâce à un mécanisme à baïonnette (de type “Twiston/twist-off”). C’est un connecteur très largement utilisé avec de la fibre optique multimode.

**Au niveau du raccordement de la FO, 3 types d’erreurs sont assez courantes :**

* **Mauvais alignement :** les supports en fibre optique ne sont pas alignés précisément lors de la jonction.
* **Écart à l'extrémité** : les supports ne se touchent pas complètement à l'épissure ou à la connexion.
* **Finition de l'extrémité** : les extrémités des supports ne sont pas bien polies ou de la poussière est présente au niveau du raccordement.
* **LW (Leight Weight )** Ce câble est uniquement utilisé dans les zones d’eau profonde (> 1 500 m) à l’abri des agressions externes. Son diamètre externe est de 17 mm.
* **LWP (Leight Weight Protected**) Ce câble est constitué d’un câble LW enrobé d’une couche d’acier et d’une gaine de polyéthylène à haute densité. Son diamètre externe est de 23 mm.
* **SA (Single Armured )** Câble LW autour duquel des fils d’aciers sont placés afin de constituer ce qui est appelé une couche d’armure : ces fils d’acier ont un diamètre de 3 mm et sont maintenus ensemble par un flux de goudron mélangé à des fibres de polypropylène. Son diamètre externe est de 30 mm.
* **DA (Double Armured )** Câble SA autour duquel une seconde couche de fils d’acier est ajoutée. Son diamètre externe est de 40 mm. Les câbles SA et DA sont déployés en zone d’eaux peu profondes (< 1 500 m) où les agressions externes sont fréquentes.

**DWDM (« Dense Wavelength-Division Multiplexing ») ou multiplexage en longueur d'onde :**

Technique qui permet d'augmenter le débit sur une fibre op canatique en faisant circuler plusieurs signaux de longueurs d'onde différentes sur une seule fibre. (Jusque 80 canaux) (chaque longueur d’onde constitue alors un lien réseau séparé

### Support sans fils

Utilisent les fréquences radio ou micro-ondes

Les contraintes :

* Zone de couverture : dépend tu terrain
* Interférences : peut avoir des interférence a cause d’autre onde
* Sécurité : on peut se connecter sans même avoir besoin de truc physique -> n’importe qui peut se connecter

On retrouve 3 normes courantes :

* IEEE 802.11: WLAN = Wi-Fi, utilise le CSMA/CA
* IEEE 802.15: WPAN = Bluetooth, utilise un processus de jumelage
* IEEE 802.16: WiMax accès à large bande sans-fil à l'aide d'un topologie point-à-multipoints (802.1 = Réseaux locaux)

Dans le futur, le Li-Fi -> utilise le spectre optique (lumière) pour transmettre les données à la place du spectre éléctromagnétique : peut atteindre 45mbit/s, fonctionne jusqu’à Max 10 mètres

En allumant et en éteignant plusieurs de milliers de fois par seconde une lumière à LED, on peut transmettre des informations en créant une fréquence. Si une LED est allumée, elle transmet un bit 1, si elle est éteinte, un bit 0. Il permettrait la communication de véhicule à véhicule, mais également avec l’équipement urbain (feu, barrière, lampadaire, …), dans les hôpitaux pour ne pas avoir de risque d’interference

✓ Le débit peut être important.

✓ Une source lumineuse est simple à mettre en place.

✓ Contrairement aux ondes électro-magnétiques, les ondes lumineuses ne traversent pas le corps humain, et donc ne sont pas susceptibles de poser des problèmes de santé.

✓ C’est directionnel, donc les informations ne peuvent être captées que sur le trajet de l’onde lumineuse, on peut donc penser que cela peut être plus sécurisé que du wifi. (ne traverse pas les murs)

✓ Cela permet d’éviter à terme la saturation des réseaux WiFi en proposant un nouveau canal de distribution de l’information numérique.

**inconvenients**

Puisque l’information ne traverse ni le corps ni les murs, cela rend impossible un réseau LiFi constitué d’un seul émetteur, même dans une maison. Il faudra un émetteur et un récepteur (mais pour le récepteur c’est valable aussi pour le wifi) pour chaque source ayant besoin de recevoir de la donnée. Pour l’instant, cette technologie est très chère

**Le WiMax (Worldwide Interoperability For Microwave Access)**

Technologie de transmission haut débit par ondes radio conçue pour couvrir des zones importantes (plusieurs km) créé par Intel et Alvarion

Le débit dépend de la distance, de la topographie des lieux et du nombre d'utilisateur sur le réseau

On l'utilise dans les zones rurales comme couverture haut débit avec une superficie importante ou comme hotspot Wi-Fi à une échelle plus étendue

**Il existe 2 type d’application au Wimax**

* Version fixe (style wifi) sans (hand-over) cad que lorsque le client se déplace et change de BS, il est déconnecté et doit se reconnecter a un autre
* Version Mobile, assure un hand over horizontal. En fait la carte du client reçoit des signaux des BS l’entourant et va choisir le meilleur signal parmi les signaux reçus

## Comment déterminer le type d'un câble

S/FTP => Shielded Foiled Twisted Pair (cuivre)

Shielded -> Blindage composé de tresses métalliques (cuivre)

Foiled => Blindage grâce à une feuille de métal

Si S devant => Tresses métalliques entourent le tout

Sinon          => Tresses métalliques entourent chaque paire

**Protocoles de la couche liaison de données**

**Contrôle de liaison logique (LLC)** : cette sous-couche supérieure définit les processus logiciels qui fournissent des services aux protocoles de couche réseau. Elle place les informations dans la trame qui indique le protocole de couche réseau utilisé pour la trame

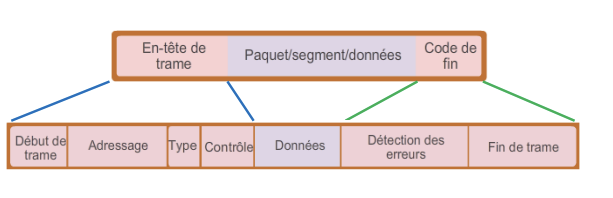
**Contrôle d'accès au support (MAC)** : cette sous-couche inférieure définit les processus d'accès au support exécutés par le matériel. Elle assure l'adressage de couche liaison de données et la délimitation des données en fonction des exigences de signalisation physique du support et du type de protocole de couche liaison de données utilisé

Les protocoles et services fonctionnels de la couche liaison de données sont décrits par :

* Les organismes d'ingénierie qui définissent les normes et protocoles publics et ouverts.
* Les sociétés du secteur des communications qui définissent et utilisent des protocoles propriétaires pour tirer parti de nouvelles avancées technologiques ou d'opportunités commerciales

## La composition d'une trame

* Un en-tête
  + **Indicateur** **de** **début** **de** **trame** (: séquence de bits prédéfinies utilisé par la sous-couche MAC pour identifier le début d’une trame.)
  + **Adresses** (: utilisé par la sous-couche MAC pour identifier les nœuds source et de destination)
  + **Type** (ce champ permet à la sous-couche LLC d'identifier le protocole de couche 3)
  + **Contrôle de flux** (ce champ permet d'identifier les services de contrôle de flux spécifiques.)
* Fin de trame
  + Détection d'erreur
  + Indicateur de fin de trame



## Méthodes d'accès

La méthode de contrôle d'accès au support utilisée dépend des critères suivants :

• **Topologie** : comment la connexion établie entre les nœuds apparaît à la couche liaison de données.

• **Partage** **de** **support** : comment les nœuds partagent les supports. Le partage de supports peut être de type point à point comme dans les réseaux étendus, ou partagé comme dans les réseaux locaux

**Contrôle d’accès au support avec support partagés**

* Le plus simple c’est de ne **définir aucun contrôle**. C’est ce qu’on appelle une **méthode d’accès basé sur le conflit ou accès non déterministe** ! Dans ce cas précis, tous les nœuds sont en concurrence pour utiliser le support, mais savent comment réagir en cas de conflit. (Ethernet, sans fil)
  + - nombreuses collisions,
  + - beaucoup de trames corrompues,
  + - beaucoup de trames ré-envoyées)
* ▪ Le seconde possibilité est d’utiliser des méthodes qui **assurent un niveau de contrôle élevé, ce qui empêche les collisions mais qui provoque également une forte surcharge.** C’est ce qu’on appelle une **méthode d’accès contrôlé ou accès déterministe** ! Dans ce cas, **chaque nœud peut uniquement utiliser le support que lorsque c’est à son tour.** (Token Ring, FDDI) (pas de collision, débit prévisible)

### 

### **Aloha**

Réseau hertzien qui a pour but **de relier ses entités composé** de :

* **1 station centrale (SC) + station secondaire (SS)**
* **2 fréquences radio : une pour la diffusion SC (Station centrale) -> SS( Station secondaire** ) et **l'autre pour l'accès multiple SS -> SC**

Lorsque **SC** **veut** **transmettre** une **info**, elle **l'envoie** et **attend** un **ACK (acknowledge)** , **si** il y a une **collision** il n'y a **pas d'ACK** donc les **stations** **réémettent** **l'information** **après** un délai **d'attente** **aléatoire**

### **CSMA (Carrier Sense Multiple Access)**

**Amélioration de l'Aloha pour les réseaux câblés.**

En **l'absence** **d'informations** à **transmettre**, la **station** **écoute** afin de **recevoir** les **paquets** qui **circulent** sur le media dans les deux sens.

Quand la **station** a besoin **d'émettre**, elle **vérifie** que **rien** ne soit **émise** sur le **media**

**Si c'est le cas, elle commence à émettre**

**Sinon** elle **attend** la **fin** de la **transmission** en cours **avant** **d'émettre**

**/! \ Ne supprime pas complètement les collisions**

### **CSMA/CD (Collision Detection)**

Amélioration du CSMA grâce à la détection de collision.

Une **station** **prête** à **émettre** **transmet** et **continue** à **écouter** le canal.

**S’il y a une collision**, elle **interrompt** sa **transmission** et **envoie** des **signaux** **spéciaux** "**bits de bourrage**" **afin que**

**Toutes** les **stations** présentes sur le réseau soit **prévenus** de la **collision**.

Elle **retentera** une **émission** **ultérieurement** (après un **délai** **aléatoire**)

### **CSMA/CA (Collision Avoidance)**

Le **périphérique** **examine** le **support** pour **établir** si celui-ci **comporte** un **signal**.

**Si** le **support** est **libre**, le **périphérique** **envoie** une **notif** pour **dire** **qu'il va transmettre**

**Ensuite** il **transmet** ses **données**

**ESS** = Extended Service Set : ensemble de plusieurs BSS.

**BSS** = Basic Service Set : il s’agit d’un groupe de stations utilisant la même fréquence.

**AP** = Access Point : station intégrée au WLAN et au système de distribution.

**IBSS** = Independant Basic Service Set : groupe de stations utilisant la même fréquence mais pouvant communiquer directement entre eux.

**Le CSMA/CA utilise une technique appelée DCF (« Distributed Coordination Function »**). Cette **contrôle** **le temps d’attente d’une station avant d’initier une transmission sur un support** (médium) **libre**.

* + **Distributed Interframe Space (DIFS)** : dans un premier temps, les **participants** doivent **surveiller** le **réseau** **pendant** la **durée d’un DIFS** afin de **déterminer** si le **réseau** est bien **libre**. Pour **le CSMA/CA**, cela signifie **qu’aucune** **station** **n’émet** à portée **au** **moment** de la **transmission**. Le **DIFS**, compris **en µs, résulte du SIFS + 2 fois la durée d’un slot (slot time)**.
  + **Short Interframe Space (SIFS)** : c’est le **temps qu’il faut pour traiter un paquet de données**. La **durée** **dépend** de la **norme IEEE 802.11** utilisée eten **µs. Après l’envoi du paquet** de données, le **nœud destinataire envoie** une **notification** **si** la **procédure RTS/CTS** est **aussi** **utilisée**. Cependant cette station **attend également une période de temps fixe avant de transmettre**
  + **Contention Window** : **si** les participants déterminent que le **canal est libre**, ils **attendent** une **période de temps aléatoire** **avant** de commencer à **transmettre**. Cette **durée correspond** à la **fenêtre de contention.** Cette **fenêtre temporelle double à chaque collision** et **correspond** au **BEB (Binary Exponential Backoff), comme dans le CSMA/CD.**

**durée de slot (slot time)** est le **temps** qu’il faut **pour que les données passent à travers** la **longueur** **maximale** du **réseau**.

**Si un participant estime que le réseau est libre il envoie une requête RTS (Request To Send) pour indiquer que les autres ne doivent pas envoyer qq chose pendant un certain temps, la durée maximale du bloquage serra specifié et appelé NAV (Network Allocation Vector)**

**Le destinataire envoie alors une requête CTS (clear to send) pour dire que c’est ok d’envoyer**

**Principe de fonctionnement du CSMA/CA**

* Une **station** qui veut **émettre** va d’abord **écouter** le support pour **voir** si il est **libre**.
* **S’il** s’avère que le **support** de **transmission** est actuellement **occupé**, un **backoff** **aléatoire** est déclenché : la **station** **attend** une période de **temps** **aléatoire** jusqu’à ce qu’un nouveau contrôle commence. Toutes les autres stations, qui ne sont pas occupées à transmettre ou recevoir, font de même. (cela ne se produit que si la station n’est pas déjà consciente que le média est occupé en raison du NAV.)
* Si le **réseau** est **libre**, la **station** initie le **DCF** : tout d’abord, le **canal est vérifié pendant toute la durée du DIFS**. **S’il** **reste libre pendant cette période, un backoff aléatoire démarre** et l’échange **RTS/CTS peut commencer**. Si la trame **RTS est parvenue au destinataire et qu’il n’y a donc pas eu de collision, l’expéditeur reçoit de la trame CTS la permission d’occuper le support d’émission.**

**Trame Ethernet**

Normes IEEE 802.2 et 802.3)

**Utilise les méthodes CSMA/CD** comme méthodes d'accès au support.

**Une image contenant texte, capture d’écran, ligne, Police

Description générée automatiquement**

( - **Préambule** : champ utilisé pour la synchronisation.

- **Adresse de destination** : contient l’adresse MAC du destinataire.

- **Adresse source** : contient l’adresse MAC source de l’émetteur.

- **Type** : valeur indiquant le protocole de couche supérieure qui recevra les données après la fin du processus Ethernet.

- **Données** : généralement un paquet IPv4 qui doit être transporté à travers le support.

**- Séquence de contrôle de trame (FCS)** : valeur utilisée pour vérifier l’absence d’erreurs dans la trame ) 🡪 pas savoir, juste savoir que les schéma se ressemblent fort mais que la taille varie

**Trame PPP (Point to Point Protocol)**

**Utilisé** pour **acheminer** **des trames entre deux nœuds**

**Demeure le protocole de choix pour mettre en œuvre de nombreux réseaux étendus série**

**Pour prendre en compte les différents types de supports, le protocole PPP établit des connexions logiques, nommées sessions, entre deux nœuds**

**Il peut faire de la compréssion de données et permet les liaisons multiples**

**Une image contenant texte, capture d’écran, ligne, nombre

Description générée automatiquement**

**La trame 802.11**

La norme IEEE 802.11 (communément appelée Wi-Fi) utilise une méthode d’accès au support de type CSMA/CA.

Les réseaux 802.11 utilisent également les accusés de réception de liaison de données pour confirmer la bonne réception d'une trame.

Si la station de travail d'envoi ne détecte pas la trame d'accusé de réception, la trame est retransmise.

Avec **l’arrivé de la norme n (802.11n)** 🡪 on a la technologie **MIMO** (**Multiple Input Multiple Output) qui est apparu qui permet a un appareil d’utiliser plusieurs antennes pour communiquer**

**On a aussi eu l’arrivé de 2 autres technologies beamforming et le band steering.**

* + **Beamforming :** beamforming ou focalisation adapte le signal émis par le routeur pour cibler plus précisément un appareil, augmentant les débits sur celui-ci
  + **Band Steering :** technologie qui permet au routeur et au terminal mobile d'échanger des informations et de se connecter sur la bande de fréquence la plus adaptée (2,4 ou 5GHZ)

**On a aussi eu le MU-MIMO (Multiple Users MIMO)**. Ca permet au routeur de communiquer avec plusieurs appareils simultanément en MIMO, plutôt que chacun leur tour.

**/ !\ Toutes les normes ne sont pas compatibles**

# Adressage IP

## Adressage IPv4

**Une IP est le numéro qui identifie chaque ordinateur connecté à Internet, ou plus précisément, l'interface avec le réseau de tout matériel informatique connecte à Internet**.

Elle a un **format de 4 octets (32 bits)** **présentable** en **binaire** ou en **décimal**

Elle contient **deux parties :**

* **ID de réseau (netID)**

**Adresse réseau logique du sous réseau auquel l'ordinateur se rattache**

* **ID d'hôte (HostId)**

**Adresse logique du périphérique logique identifiant chaque ordinateur sur un sous réseau**

## Les ≠ classes d'adresses  (voir p 6 chap 8 pour schéma)

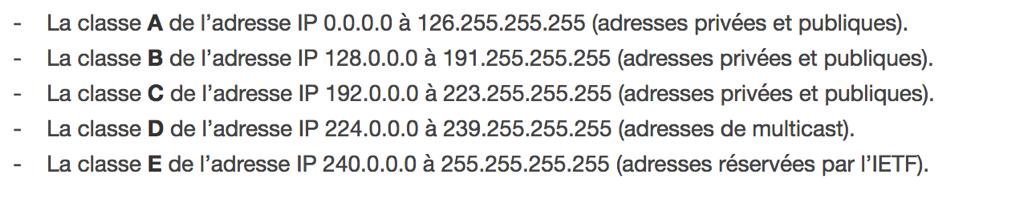
A : 8 bits partie réseau, 24 partie hôte

B : 16 bits réseau, 16 bits hôtes

C : 24 bits réseau, 8 hôtes

D : Réservées pour le multicast(s’adresser à un groupe et pas tout le monde), C’EST TOUJOURS UNE ADRESSE DE DESTINATION

E : Réservées à la recherche ou à des usages futurs



Les adresses réseaux et de diffusions : la première et la dernière addresses ne peuvent pas êtres attribuées à un hôte

L’adresse de bouclage : **c’est une adresse utilisé pour diriger le trafic vers eux même**

Les adresses du bloc 168.254.0.0/16 sont des adresses link-local (c'est du réseau local, elle sont données lorsqu’aucune adresse IP n’est disponible)

Les adresses TEST-NET du bloc 192.0.2.0/24 sont réservées à des fins pédagogiques

Les adresses expérimentales du bloc 240.0.0.0 à 255.255.255.254 sont réservées pour une utilisation future

10.0.0.0 à 10.255.255.255 (10.0.0.0/8)

172.16.255.255 à 172.31.255.255 (172.16.0.0/12)

Conséquence de croissance exponentielle d’internet pour L’IPV4 :

* + Manque d’adresse IP
  + Croissance de la table de routage internet

## Solution pour pallier aux problèmes de l'IPv4

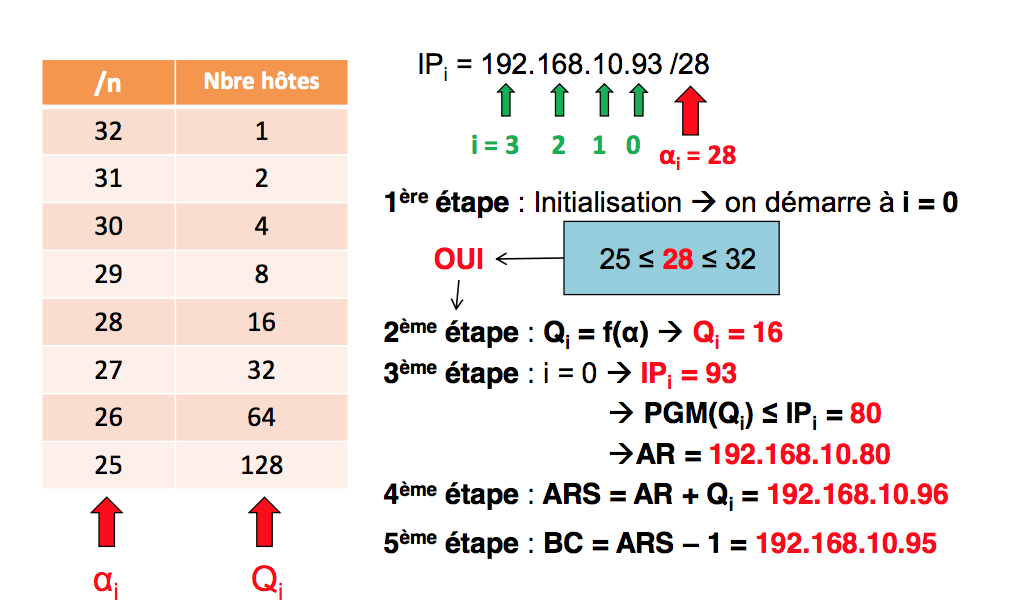
### Le CIDR (Classless Inter-Domain Routing)

 Permet une diffusion plus efficace de l'espace d'adressage IPv4 et retarde la croissance des tables de routages donc la pénurie d'adresses

### Utilisation du NAT (Network Adress Translation) (p 18 🡺 regarder une vidéo ??)

Permet à un ensemble d'hôtes présents sur un réseau local, d'avoir accès à internet en utilisant une adresse IP unique => retarde la pénurie d'adresses

## Technique calcul IP réseau/diffusion/hôtes



(Adresse réseau + nombre d’adresse théorique(ce qu’il y a après le /) -1 DIVISER

## Coexistence IPv4 et IPv6

### Techniques de migration vers l'IPv6

* Double pile

Permet à l'IPv4 et à l'IPv6 de coexister sur le même réseau. Les périphériques exécutent les piles de protocoles IPv4 et v6 simultanément

* Tunneling

Méthode de transport des paquets IPv6 via un réseau IPv4. Les paquets IPv6 sont encapsulés dans les paquets IPv4

* Traduction

Un paquet IPv6 est traduit en paquet IPv4 et inversement

## Adressage IPv6

Une adresse IPv6 est longue de 128 bits (16 octets)

La notation décimale a été abandonnée au profit d'une notation hexadécimale où les 8 groupes de deux octets sont séparés par un signe « : »

### Règles :

* On peut supprimer les 0 de gauche : 01AB devient 1AB et 00CD devient CD mais / ! \ 0000 devient 0 !
* Une (ou plusieurs) suite de groupe de quatre 0 peut être compressée en « :» (une seule fois)

ex : 2001 :DB8 :0 :1111::200 => 2001 :0DB8 :0000 :1111 :0000 :0000 :0000 :0200

La longueur de préfixe (nbr après le /) est utilisée pour indiquer la partie réseau d'une adresse IPv6, elle peut aller de 0 à 128

Si elle vaut 64, il y a 64 bits réseau et 64 bits hôtes

### Adresse anycast

Adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques

Le périphérique le plus proche reçoit le paquet

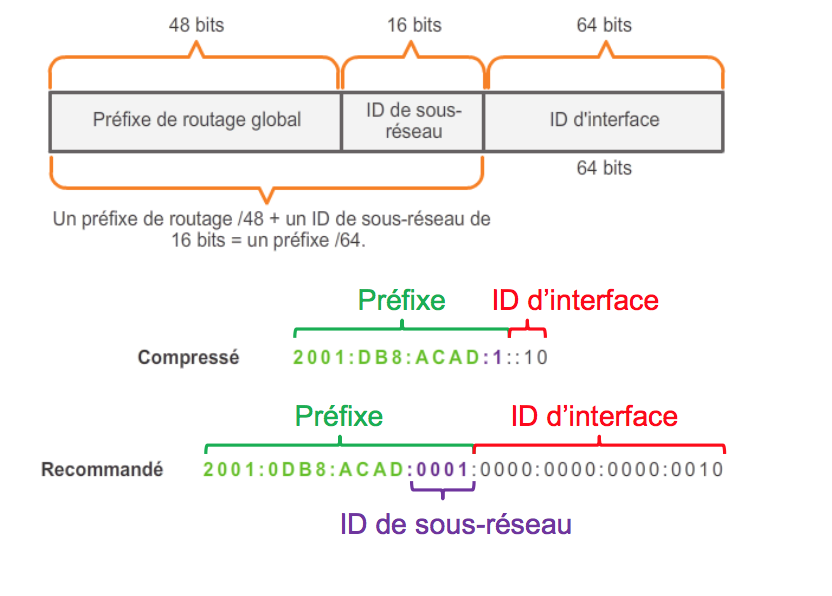
Il n'y a pas d'adresse de diffusion en IPv6 mais on peut faire un multi-diffusions à tous les nœuds dont ça revient au même

### 

### Adresse de monodiffusion

Il existe 6 types mais voici les plus importants :

* Adresse de monodiffusion globale : idem que IPv4, un hôte à un destinataire
  + Elle se compose comme suivant



* Adresse link-local (commencera toujours pas FE80 ::/10) : utilisées pour communiquer avec d'autres périphériques sur la même liaison locale, uniquement utilisable en local

**EXAMEN**

**Exo d’ici**

# Découpage réseau

Certains réseaux sont tellement grands qu'il en devient difficile d'y acheminer les paquets ou encore d'y faire des diffusions

Le fait de sous-diviser un réseau permet d'ajouter un niveau hiérarchique, pour obtenir trois niveaux : un réseau, un sous-réseau et un hôte.

Pour éviter, cela il faut diviser ce réseau en différents sous-réseaux.

On divise un réseau selon les critères suivants :

* Taille
* Nombre d'hôtes par sous réseau
* Méthode d'attribution des adresses d'hôte
* Hôtes nécessitant des adresses IP statiques
* Hôtes pouvant utiliser le protocole DHCP

L'attribution des adresses ne doit pas être laissée au hasard, trois critères sont à prendre en compte :

* Eviter les doubles
* Assurer et contrôler l'accès
* Surveiller la sécurité et les performances

Exemple des règles d'attribution des adresses IP dans chaque plage de sous-réseaux :

• Les imprimantes et les serveurs sont associés à des adresses IP statiques.

• Les utilisateurs obtiennent des adresses IP de la part des serveurs DHCP.

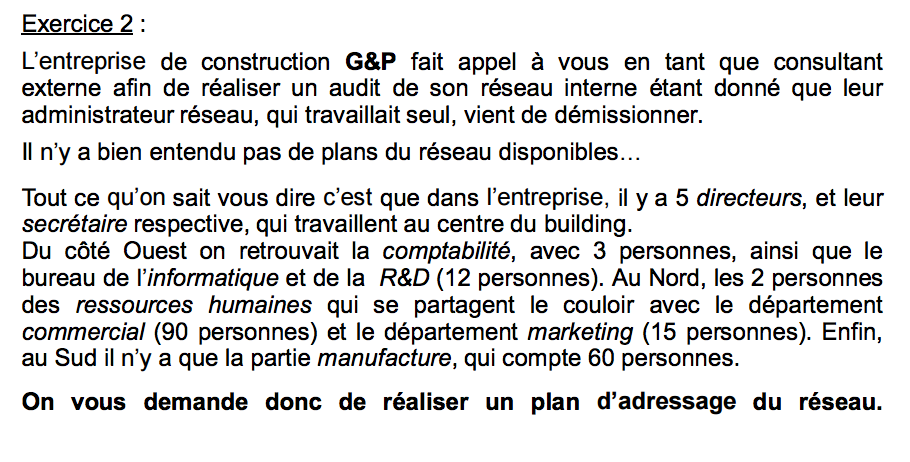
• Les routeurs sont configurés avec les dernières adresses d'hôte disponibles dans la plage fournie par le serveur DHCP.

Pour communiquer entre eux les sous-réseaux doivent passer par un routeur comme passerelle par défaut

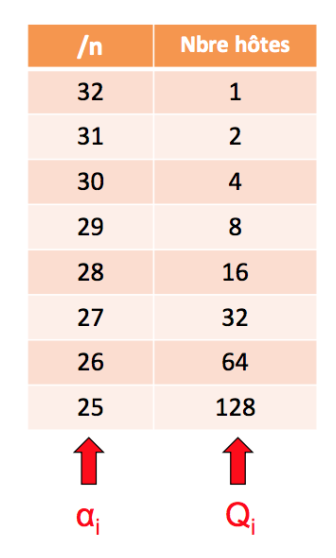
## Comment découper un réseau correctement

* Toujours commencer par décomposer les réseaux en affectant les plages d'adresses les plus grandes en premier
* Quand on place un réseau plus grand que le précédent dans une plage, il faut sauter une certaine plage d'adresses

## Exercice de découpage réseau





En tenant compte de :

### Commercial

195.208.192.33/25 => i = 0, Qi = 128 => PGM 128 ≤ 33 => 0

ASR : 195.208.192.0/25

### Manufacture

195.208.192.133/25 => i = 0, Qi = 128 => PGM 128 ≤ 133 => 128

ASR : 195.208.192.128/25

### Marketing

195.208.192.210/25 => i = 0, Qi = 128 => PGM 128 ≤ 210 => 128

ASR : 195.208.192.128/25

### Info

195.208.193.29/27 => i = 0, Qi = 32 => PGM 32 ≤ 29 => 0

ASR : 192.208.193.0/27

### R&D (calmez vous les joueurs de call of)

195.208.192.77/27 => i = 0, Qi = 32 => PGM 32 ≤ 77 => 64

ASR : 195.208.193.64/27

### Dirlo

195.208.193.11/27 => i = 0, Qi = 32 => PGM 32 ≤ 11 => 0

ASR : 192.208.193.0/27

### Secrétariat

195.208.193.25/27 => i = 0, Qi = 32 => PGM 32 ≤ 25 => 0

ASR : 192.208.193.0/27

### Compta

195.208.193.205/29 => i = 0, Qi = 8 => PGM 8 ≤ 205 => 200

ASR : 192.208.193.200/29

### RH

195.208.193.4/27 => i = 0, Qi = 32 => PGM 32 ≤ 25 => 0

ASR : 192.208.193.0/27

### On rassemble ce qui doit être rassembler (même IP) et on remet dans l'ordre

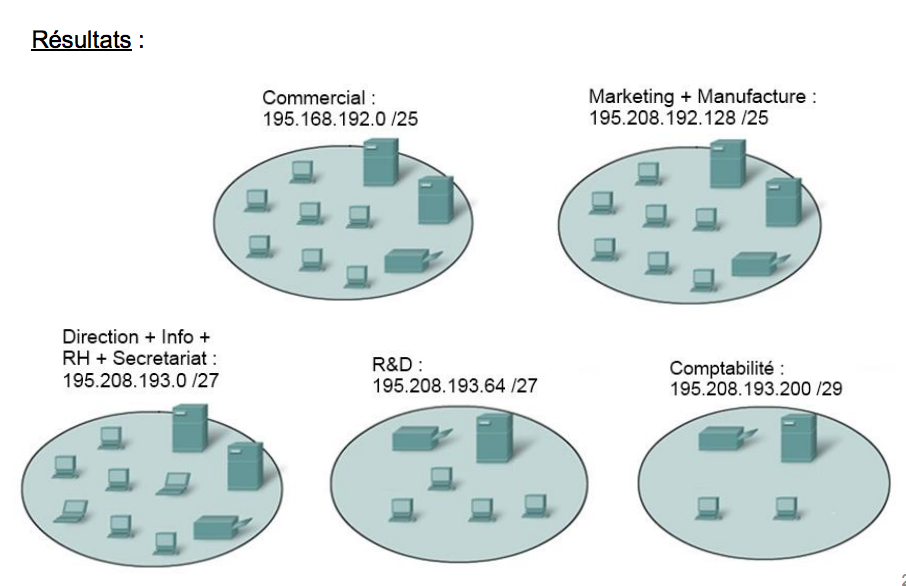
Commercial : 195.208.192.0/25 => 2^ (32-25) = 128 hôtes

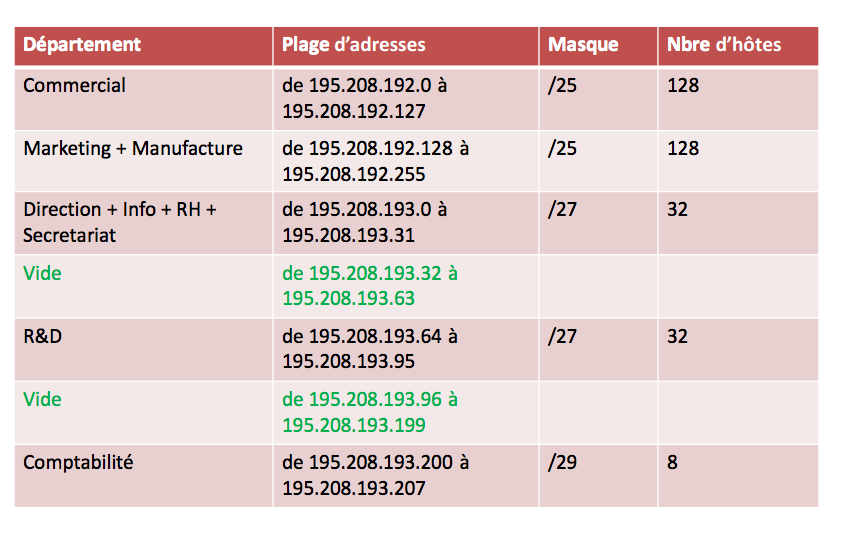
Marketing + Manufacture : 195.208.192.128/25 => 2^ (32-25) = 128 hôtes

Direction + Info + RH + Secrétariat : 192.208.193.0/27 => 2^ (32-27) = 32 hôtes

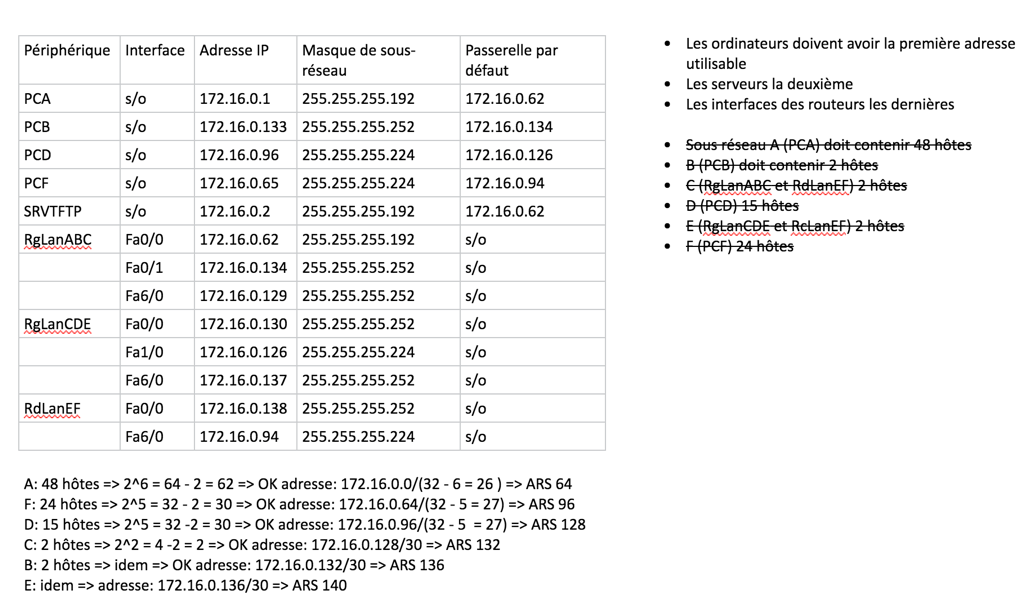
R&D : 195.208.193.64/27 => 2^ (32-27) = 32 hôtes

Comptabilité : 192.208.193.200/29 => 2^ (32-29) = 8 hôtes



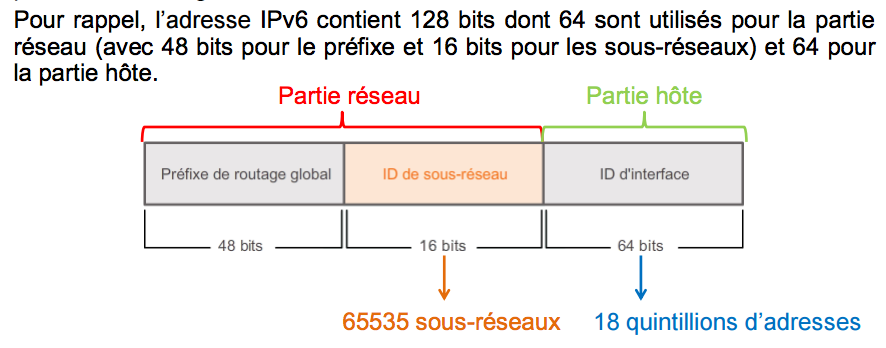


### Exercice de segmentation sans aide (les consignes sont à droite, le tableau est presque vide de base)



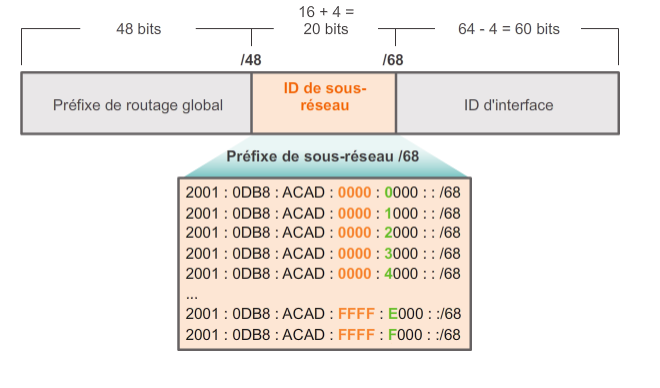
## Segmentation IPv6

### 1 ère solution



### 2 -ème solution

Emprunter un quartet sur l'ID d'interface => plus sécurisé car moins d'hôtes



On ne peut augmenter le masque de sous-réseaux que de 4 (/64 -> /68 -> /72, ….) car on est en hexadécimal (codé en 4 bits)

**Test réseau avec ICMP**

**Ping :**

Pour l’ICMPv4 pour code de destination inacessible

• 0 - Réseau inaccessible

• 1 - Hôte inaccessible

• 2 - Protocole inaccessible

• 3 - Port inaccessible

Pour l’ICMPv6 pour code de destination inacessible

• 0 - Pas de route vers la destination

• 1 - La communication avec la destination est interdite administrativement (pare-feu)

• 2 - Au-delà de la portée de l'adresse source

• 3 - Adresse inaccessible

• 4 - Port inaccessible

**Délai dépassé quand le temps de vie du paquet a été dépassé pour le transfert**

Les messages de délai dépassé sont utilisés par l’outil traceroute.

ICMPv6 offre 4 nouveaux protocoles dans le cadre du protocole NDP (Neighbor Discovery Protocol)

Il y a des messages échangés entre un routeur IPv6 et un périphérique IPv6 :

• Messages de sollicitation de routeur (RS)

• Messages d'annonce de routeur (RA)

Il y a des messages échangés entre des périphériques IPv6 :

• Messages de sollicitation de voisin

• Messages d'annonce de voisin

La commande ping est utilisée pour tester 3 choses :

• Le bon fonctionnement de la boucle locale

Si le ping ne reçois aucune réponse en retour, alors le protocole TCP/IP ne fonctionne pas sur l’hôte, si on reçoit une réponse, tout est ok

• L’accès à la passerelle par défaut Généralement

Un ping réussi vers la passerelle par défaut indique que l'hôte et l'interface du routeur servant de passerelle par défaut sont tous deux opérationnels sur le réseau local. Si erreur ping peut être envoyée à l'adresse IP d'un autre hôte qui est opérationnel sur le réseau local. Si la passerelle ne répond pas, mais qu'un autre hôte répond, cela peut indiquer soit un problème sur l'interface du routeur qui sert de passerelle, soit que l’adresse de passerelle est incorrectement configurée sur l'hôte.

• La connectivité avec un hôte distant

Avec ping, si ça réussit, tout est ok

La commande ping permet de tester la connectivité entre deux hôtes, mais ne fournit pas d'informations sur les détails des périphériques entre les hôtes.

Traceroute (tracert) est un utilitaire qui génère une liste des sauts qui ont été atteints avec succès le long du chemin avec le temps pour les atteindre (si on a une \* il y a eu un problème)

**Une image contenant texte, diagramme, capture d’écran, horloge

Description générée automatiquement**

**SECURITE RESEAU**

**Menaces de sécuritées**

* Vol d’information
* Perte et manipulation de données
* Usurpation d’identité
* Interruption du service

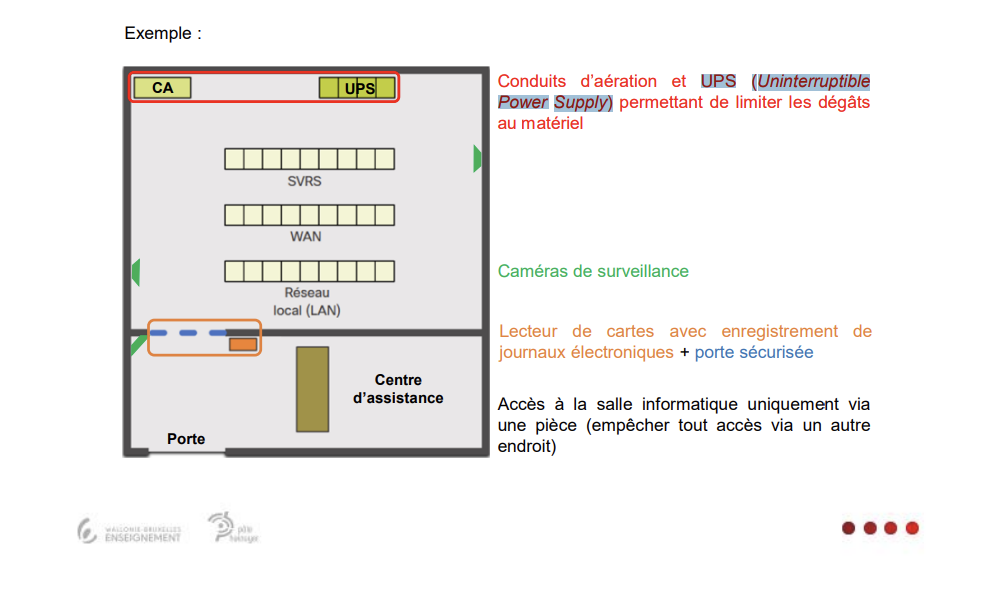
**Types de vulnérabilités**

* **Les vulnérabilités technologiques** : dans ce cas il peut aussi bien s’agir de faiblesses liées à un protocole (comme HTTP par exemple) ou à un système d’exploitation ou encore à des équipements réseaux.
* **Les vulnérabilités de configuratio**n : dans ce cas il peut aussi bien s’agir de comptes utilisateurs non sécurisés ou avec un mot de passe faible, d’utilisation des services Internet mal configurés (JavaScript), d’utilisation de paramètres par défaut non sécurisés dans des périphériques ou d’équipements réseaux mal configurés (protocoles de routage, ACL).
* **Les vulnérabilités de stratégie** : dans ce cas il peut aussi bien s’agir d’absence de stratégies/de politiques de sécurité claires, de la surveillance ou du contrôle insuffisant sur le réseau, l’installation d’applications non approuvées ou l’absence d’un plan de reprise après sinistre

**Menaces physiques**

* **Menaces matérielles** : Cela comprend les dommages physiques aux serveurs, routeurs, commutateurs, installations de câblage et stations de travail.
* **Menaces environnementales** : Cela comprend les extrêmes de température (trop chaud ou trop froid) ou les taux d'humidité (trop humide ou trop sec).
* **Menaces électriques** : Cela comprend des pics de tension, une tension insuffisante, alimentation inappropriée (bruit) et une panne totale de courant.
* **Menaces liées à la maintenance** : Cela comprend la mauvaise manipulation des composants électroniques principaux (décharges électrostatiques), absence de pièces de rechange essentielles, câblage de mauvaise qualité et étiquetage peu efficace

**Exemple de protection**

****

**3 types de malware (logiciel malveillant)**

**Virus** : Un virus informatique est un type de programme malveillant qui se propage, d’un ordinateur à un autre, en insérant une copie de lui-même dans un autre programme (Dos, destruction de données, ..) provient d’un fichier .exe et a besoin d’une action humaine (le lancer) pour qu’il commence

**Vers** : Les vers informatiques sont semblables aux virus en ce sens qu'ils reproduisent des copies fonctionnelles d'eux-mêmes et peuvent provoquer le même type de dommages

**Chevaux de Troie** : un cheval de Troie est une partie de code qui présente une apparence tout à fait légitime (ce qui trompe généralement les utilisateurs) mais qui, une fois activé, peut réaliser un certain nombre d'attaques contre l'hôte. (ouvrir des fenêtres, supprimer des fichiers, usurper des données ou activer et propager d'autres programmes malveillants, comme des virus)

**Attaques sur réseaux**

* **Attaques de reconnaissance** : La découverte et la mappage non autorisés de systèmes, services ou vulnérabilités (nslookup, whois,
* **Attaques par accès** : La manipulation non autorisée des données, des accès aux systèmes ou des privilèges utilisateur.
* **Déni de service** - La désactivation ou corruption de réseaux, de systèmes ou de services (DDOS existe (Distributed Denial of Service) exemple, un acteur de menaces construit un réseau d'hôtes infectés, appelés zombies. Un réseau de zombies est appelé un botnet.)

**Vol de mots de passe**

* **attaque par dictionnaire**, qui se base sur le fait que les utilisateurs ont tendance à employer des mots communs et des mots de passe courts. Le pirate utilise une liste de mots communs, le dictionnaire, et les essaye, bien souvent avec des chiffres avant et/ou après les mots, à l'encontre des comptes d'une entreprise pour chaque nom d'utilisateur.
* **attaque par force brute**, qui, à l’aide d'un programme, va générer des mots de passe potentiels ou même des ensembles de caractères aléatoires. Ces attaques commencent par les mots de passe faibles et couramment utilisés, puis évoluent vers des mots de passe plus complexe (avec des minuscules, majuscules, chiffres,…)
* **attaque via logiciel d’enregistreur de frappe** : le fonctionnement est simple, un logiciel enregistre les touches saisies sur le clavier par l'utilisateur, lui permettant ainsi de connaître non seulement le nom d'utilisateur et le mot de passe d'un compte, mais également le site Web ou l'application exacte sur laquelle l'utilisateur s'est connecté avec les identifiants.
* **attaque par interception de trafic** : ce type d’attaque utilise généralement un logiciel, comme les renifleurs de paquet, pour surveiller le trafic réseau et enregistrer les mots de passe lorsqu'ils sont transmis. En gros, le logiciel surveille et enregistre les informations cruciales. Bien évidemment, si cette information (comme les mots de passe) n'est pas chiffrée, la tâche est simple.
* **attaque d’ingénierie sociale (social ingenering)** . Ce type d’attaque se base sur une vaste gamme de méthodes pour obtenir des informations de la part des utilisateurs (Phishing, Clé usb infecté, l’harponnage (Phishin plus ciblé, …))

Pour atténuer les attaques réseau, vous devez d'abord sécuriser les périphériques, y compris les routeurs, les commutateurs, les serveurs et les hôtes

* **Un pare-feu** : un pare-feu va fournir des services garantissant que le trafic interne peut sortir et revenir mais que le trafic externe ne peut pas établir de connexion avec les hôtes en interne.
* **Un serveur AAA** : un serveur AAA est un serveur d’authentification qui contient une base de données sécurisée de qui est autorisé à accéder (et à gérer) les périphériques réseaux.
* **Un routeur VPN** : un routeur utilisé pour fournir des services VPN (Virtual Private Network) sécurisés avec des sites d’entreprise ainsi qu’un support d’accès à distance pour les utilisateurs distants. C’est par exemple cet appareil qui permet de créer un lien direct entre deux ordinateurs distants, grâce à l’utilisation de tunnels chiffrés sécurisés.
* **Des ESA/WSA** : Un ESA (Email Security Appliance) permet de filtrer les spams et les emails suspects tandis qu’un WSA (Web Security Appliance) permet de filtrer des malwares connus.
* **Un IPS** : un IPS (Intrusion Prevention System) est un outil permettant de surveiller le trafic, entrant et sortant, à la recherche de logiciels malveillants, de signatures d’attaques réseau,... dans le but de les bloquer ou de les arrêter
* **IDS** (Intrusion Detection System) qui est plutôt un outil surveillant un réseau pour déceler toute activité malveillante ou toute violation de politique de sécurité mais contrairement à l’IPS, l’IDS décrit une intrusion suspectée une fois qu’elle a eu lieu, et la signale.

Il faut aussi sauvegarder régulièrement les données

**Types de sauvegarde**

* **Les sauvegardes complètes** : Avec une sauvegarde complète, chaque fois qu’un système est sauvegardé, tous les fichiers et dossiers du système sont copiés.
* **Les sauvegardes incrémentielles** : Avec une sauvegarde incrémentielle, la sauvegarde initiale est complète et ensuite chaque sauvegarde suivante stocke les modifications apportées depuis la dernière sauvegarde.
* **Les sauvegardes différentielles** : Avec une sauvegarde différentielle, la sauvegarde initiale est toujours une sauvegarde complète sauf que par la suite, le système sauvegarde tous les changements depuis la dernière sauvegarde complète

Toujours faires les mise a jour d’antivirus, de l’OS

Le pare-feu autorise la sortie et le retour du trafic provenant du réseau interne. Le pare-feu refuse l’accès du trafic externe à destination du réseau interne.

Un pare-feu permet aux utilisateurs externes de contrôler l'accès à des services spécifiques.

Par exemple, les serveurs accessibles aux utilisateurs externes se trouvent généralement sur un réseau spécial appelé «zone démilitarisée» (DMZ).

La zone DMZ permet à un administrateur réseau d'appliquer des politiques spécifiques pour les hôtes connectés à ce réseau.

**Les techniques des pare feux**

* **Filtrage des URL** : Empêche ou permet l'accès à des sites web basés sur des URL ou des mots clés spécifiques.
* **Filtrage des paquets** : Empêche ou autorise l'accès sur la base d'adresses IP ou MAC.
* **Filtrage des application**s : Interdit ou autorise l'accès à des types d'applications spécifiques en fonction des numéros de ports.
* **Inspection minutieuse des paquets** (SPI pour Stateful Packet Inspection) : Les paquets entrants doivent être des réponses légitimes aux demandes des hôtes internes. Les paquets non sollicités sont bloqués (sauf s'ils sont expressément autorisés). L'inspection SPI peut éventuellement reconnaitre les DoS et y réagir

# Ethernet (chap 4)

## Ethernet

Il s'agit de la technologie réseau local prédominante dans le monde

* Fonctionne au niveau de la couche liaison de donnée et de la couche physique
* Définie par les normes 802.2 et 802.3 de IEEE

Et prend en charge des bandes passantes de données de 10 Mbit/s, 100 Mbit/s, 1 Gbit/s (1 000 Mbit/s) ou 10 Gbit/s (10 000 Mbit/s).

## La couche liaison de donnée

Séparée en deux parties

* Sous-couche LLC Ethernet

Gère la communication entre les couches supérieures et inférieures.

* Sous-couche MAC Ethernet

Elle encapsule les données et contrôle l'accès au support (CSMA/CD)

## Adresse MAC

Valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux. Ils sont regroupés par 2 et séparés par « : » ou « - »

Elles sont uniques au monde.

Les 24 premiers octets sont la partie OUI (Organizationally Unique Identifier) fourni par l’IEEqui est l'identifiant du constructeur (les autres c'est la partie NIC)

Elle est au départ stocké dans la mémoire morte et lorsque l'ordinateur démarre, elle est copiée dans la mémoire vive

## Norme de taille d'une trame

Une trame doit avoir une taille minimale de 64 octets et maximale de 1522 octets, si elle fait plus (ou moins) elle est considérée comme un fragment de collision et est rejetée

## Les types d'adresses MAC

### Monodiffusion

Adresse utilisée lorsqu'une trame est envoyée à partir d'un seul périphérique émetteur à un seul périphérique destinataire

### Diffusion

Ne comporte que des "F", tous les hôtes sur le réseau local recevront le paquet et le traiteront

### Multidiffusion

L'adresse commence par 01-00-5E, permet à un périphérique source d'envoyer un paquet à un groupe de périphériques

## Protocole ARP

Il sert à récupérer l'adresse MAC d'un ordinateur à partir de son adresse IP.

Il met à jour une table ARP soit de manière statique ou de manière dynamique.

Il existe deux façons de le faire en dynamique :

1. Quand un nœud reçoit des trames en provenance d'un support, il enregistre les IP et MAC source dans sa table ARP
2. Le périphérique envoie une requête ARP à tous les périphériques du réseau local, la requête contient l'IP destination et une adresse mac de diffusion. Le périphérique concerné répond à la requête ARP en envoyant une trame de monodiffusion contenant son adresse MAC

Les entrées de la table MAC, obtenues dynamiquement sont HORODATÉES, si cet horodatage expire, le périphérique est supprimé de la table ARP

Le concentrateur (HUB)

Matériel réseau le plus basique. Il utilise la première couche du modèle OSI (physique) et possède un certain nombre de ports (4, 8, 16 ou 32)

Il peut récupérer le signal arrivant sur un port, de le réamplifier et de le diffuser.

Tout ce qui est lié (périphérique finaux) à un HUB est considéré comme UN SEUL domaine de collision.

## Le commutateur (SWITCH) de couche 2

Dispositif permettant de relier des réseaux travaillant avec le même protocole. Il travaille sur les deux premières couches du modèle OSI.

Il analyse les trames arrivantes et filtres (par adresse MAC) les données afin de les aiguiller vers les ports adéquats en fonction de sa table de commutation (MAC).

### **La table de commutation**

Elle fait correspondre les adresses MAC de destination au ports utilisés pour la connexion aux nœuds.

Pour chaque trame entrante, l'adresse MAC de destination dans son en-tête est comparée à la liste d'adresses.

Lorsqu'un port répertorié dans la table est mappé à une adresse MAC, il est utilisé comme port de sortie de la trame.

### Les ≠ fonctions de bases

* L’apprentissage :

Chaque fois qu'une trame entre dans le switch, celui-ci examine son adresse MAC source et l'ajoute dans sa table MAC si elle n'y est pas

* L’horodatage :

Les entrées de la table de commutation acquises à l'aide de l'apprentissage sont horodatées. Une fois le compte à rebours à 0, l'entrée est supprimée

* L'inondation

Quand un commutateur ne sait pas sur quel port envoyer une trame, il fait une diffusion à l'exception du port d'arrivée

L'hôte possédant l'adresse correspondante va traiter la trame et lui répondre afin que le switch met à jour sa table MAC

* Le réacheminement sélectif

Si une trame possède une adresse MAC source connue, le switch va acheminer la trame au port correspondant

* Le filtrage

Abandon de la transmission d'une trame lorsqu'elle est endommagée. Aussi, une trame n'est jamais envoyée à son port d'arrivée

## Domaine de collisions et de diffusions

### Domaine de collision

Région du réseau au sein de laquelle les hôtes partagent l'accès au média (chaque câble sauf pour le hub c'est tout ce qu'il contient en 1 domaine)

### Domaine de diffusion

Zone logique où un ordinateur connecté au réseau peut transmettre à tous les autres ordinateurs du même domaine (chaque partie partant d'un routeur)

## La fonction auto-MDIX

Lorsque vous activez cette fonction, le commutateur détecte le type de câble requis pour les connexions Ethernet cuivre, puis configure les interfaces en conséquence

## Méthodes de transmission de trames

### **Store and forward**

Lorsqu'un switch reçoit une trame, il stocke les données dans des mémoires tampons jusqu'à ce qu'il ait tout reçu, pendant ce temps il recherche dans la trame, des informations sur sa destination et procède à un contrôle d'erreur

### **Cut-through**

Le switch agit sur les données au fur et à mesure qu'il les reçoit, même si la transmission est pas finie. Il met une quantité suffisante en mémoire tampon

Afin de lire l'adresse MAC de destination et déterminer ainsi le port où il faut transmettre les données. Il n'y a pas de contrôle d'erreur donc plus rapide qu'au-dessus

 Il en existe deux variantes :

* Fast-Forward

Offre le niveau de latence le plus faible. Transmet un paquet immédiatement après la lecture de l'adresse de destination

Comme il envoie avant d'avoir tout reçu, les trames peuvent comporter des erreurs.

* Fragment-Free

Le commutateur stocke les 64 premiers octets (car c'est là qu'il y a le plus souvent des erreurs) avant la transmission.

## Mise en mémoire tampon

### **Axée sur les ports**

Les trames sont stockées dans des files d'attentes liées à des ports entrants et sortants. Une trame est transmise au port sortant uniquement si

Toutes les trames qui la précèdent dans la file d'attente ont correctement été transmises. (Une seule trame peut tout retarder si un port de destination est saturé)

### **Partagée**

Le commutateur stocke toutes les trames dans une mémoire tampon commune à tous les ports du commutateur. La capacité est allouée dynamiquement.

Les trames de la mémoire sont liées de manière dynamique au port de destination, ce qui permet de recevoir la trame sur un port et de la transmettre sur un autre sans files d'attente.

**3 types de commutateur**

- Commutateurs fixes

Possèdent des fonctions et des options qui sont limitées à celles fournies à l’origine avec le commutateur (impossible d’ajouter fonctionnalité etc) (le – cher)

- Commutateurs modulaires

Souplesse sur la configuration, on achète un chassis dans lequel on peut mettre ce qu’on veut comme module (le + souple)

- Commutateurs empilables

Commutateurs qui peuvent s’interconnecter entre eux afin de les administrer comme s’il ne s’agissait que d’un seul et même commutateur. (Nombre de connectivité limité) (Meilleur resistance au pannes)

**Technologie PoE (Power over Ethernet):**

Permet à un commutateur de fournir une alimentation à des périphériques par le biais du câblage Ethernet existant, en allouant des paires des cable UTP ou autres a transmettre energie

**EtherChannel**

C’est une technologie d'agrégation de liens utilisé principalement sur les commutateurs de Cisco. Elle permet d'assembler plusieurs liens physiques Ethernet en un lien logique. (faire croire que plein de petit cable sont en faire 1 gigantesque cable)

Un commutateur de couche 3 fonctionne de manière similaire à un commutateur de couche 2 mais, à défaut d'exploiter les informations d'adresses MAC de couche 2 pour décider des opérations de transmission, le commutateur de couche 3 peut également exploiter celles des adresses IP.

**Les principaux types d’interface en couche 3 sont :**

✓ SVI (interface virtuelle du commutateur) : interface logique d'un commutateur associé à un réseau local virtuel (VLAN).

✓ Port routé : port physique sur un commutateur de couche 3 configuré pour servir de port du routeur.

✓ EtherChannel de couche 3 : interface logique d'un périphérique Cisco associé à un ensemble de ports routés.

Les caractéristiques des ports routés sont les suivantes : ▪ Ils ne sont associés à aucun réseau local virtuel spécifique. ▪ Ils peuvent être configurés avec un protocole de routage de couche 3. ▪ Ils constituent des interfaces de couche 3 uniquement et ne prennent pas en charge les protocoles de couche 2.

# Couche réseau

## La couche réseau

Elle fournit des services permettant aux périphériques finaux d'échanger des données sur le réseau.

Elle utilise pour cela, 4 processus de base :

* L'adressage

La couche réseau fournit un adressage qui permettra d'identifier de manière unique les périphériques sur le réseau afin d'acheminer des données via IPv4 ou v6

* L'encapsulation

Durant ce processus, la couche 3 reçoit l'unité de données de protocole de la couche 4 (segment ou datagramme) et ajoute un en-tête de couche 3

Pour créer l'unité de données de protocole de couche 3 appelée paquet

* Le routage

Les paquets vont devoir traverser des périphériques intermédiaires connectant les réseaux (routeurs). Ils vont sélectionner les chemins afin de

Diriger les paquets vers leur destination. Chaque route empruntée par un paquet pour atteindre le périphérique suivant est appelée saut

* La désencapsulassions

Si le paquet est bien adressé à l'hôte de destination, il va le décapsuler et l'unité de donnée de protocole couche 4 est transmise au service de la couche transport

## Les caractéristiques du protocole IP (Internet Protocol)

* Aucune connexion n'est établie avant l'envoi de paquets de données
* Acheminement non fiable : aucune surcharge n'est utilisée pour garantir la transmission des paquets
* Indépendant du support : fonctionne indépendamment du support transportant les données
* Il est qualifié de protocole "non fiable" car il ne sait pas gérer les paquets endommagés ou non remis
* Il n'y a pas de champs requis pour la transmission fiable dans l'en-tête d'un paquet IP mais cela offre moins de surcharge
* On ne sait donc pas si le destinataire est sur le réseau, si le paquet est bien arrivé à destination et si le destinataire peut lire le paquet
* Le destinataire ne sait pas quand le paquet arrive

/! \ La taille maximale d'unité de données de protocole que chaque support peut transporter est déterminé au niveau de la couche de liaison de données et est transmise à la couche réseau. Donc la taille de création des paquets est déterminée.

## Le protocole IPv4

Un paquet IPv4 comporte deux parties

* En-tête IP -> indique les caractéristiques du paquet
* Données utiles -> contient les info. du segment de couche 4 et les données en elles-mêmes

Il possède un "Time To Live (TTL)" (8bits) qui contient une valeur pour limiter la durée de vie d'un paquet. Elle est indiquée en secondes mais généralement appelée "nombre de sauts". Si cette valeur est dépassée, le routeur rejette le paquet et envoie un message de dépassement de délai ICMP à la source

L’en-tête :

* La version -> numéro de la version IP (4 bits)
* Services différencies (DS) (8 bits)
  + Utilisé définir priorité de chaque paquet. Les 6 premiers bits définissent la valeur DCSP (« Differentiated Services Code Point ») qui est utilisée par un mécanisme de qualité de service. Les 2 derniers bits (ECN pour « Explicit Congestion Notification ») identifient la valeur de notification explicite de congestion qui peut être utilisée pour empêcher l'abandon de paquets pendant les périodes d'encombrement du réseau.
* Identification (16 bits) -> Identifie les fragments d’un paquet IP d’origine
* Protocole (8 bits) – indique le type de données utiles transportées par le paquet, ce qui permet à la couche réseau de transmettre les données au protocole de couche supérieure approprié. Les valeurs habituelles sont notamment ICMP (1), TCP (6) et UDP (17).
* Adresse IP source (32 bits) – contient la valeur binaire de l'adresse IP source du paquet.
* Adresse IP de destination (32 bits) – contient la valeur binaire de l'adresse IP de destination du paquet

## Problèmes de l'IPv4

* Manque d'adresses IP => Il y en a 4 milliards mais c'est pas assez
* Croissance de la table de routage Internet => Ces routes IPv4 consomment beaucoup de mémoire et de ressources sur les routeurs Internet
* Manque de connectivité de bout en bout

## Apparition de l'IPv6

Les problèmes de l'IPv4 ont conduit au développement de l'IPv6

* Espace d'adressage plus important (beaucoup beaucoup + d'adresses IP, environs 67 milliards par cm^2 de surface terrestre, oui c’est bcp)
* Traitement des paquets plus efficace => l'en-tête IPv6 a été simplifiée et comporte moins de champs
* Traduction d'adresses réseau non nécessaire => comme y'a beaucoup d'IP, plus besoin de NAT
* Sécurité intégrée => prend en charge les fonctions d'authentification et de confidentialité (pas comme l'IPv4)

## Le routeur

Equipement intermédiaire opérant au niveau de la couche 3 du modèle OSI, il envoie et reçois des paquets IP qui lui sont destinés

Chaque interface du routeur est un membre ou un hôte d'un réseau IP différent

/ ! \ Deux interfaces actives ne peuvent pas appartenir au même réseau

Ils nécessitent :

* Un OS
* Un processeur
* De la mémoire vive => contient l'IOS, fichier de config, table de routage IP, Cache ARP, Mémoire tampon
* De la mémoire morte => instructions de démarrage, le POST (Power On Self Test, pour savoir si tout va bien), une version limitée (de merde) de l'IOS
* Du courage

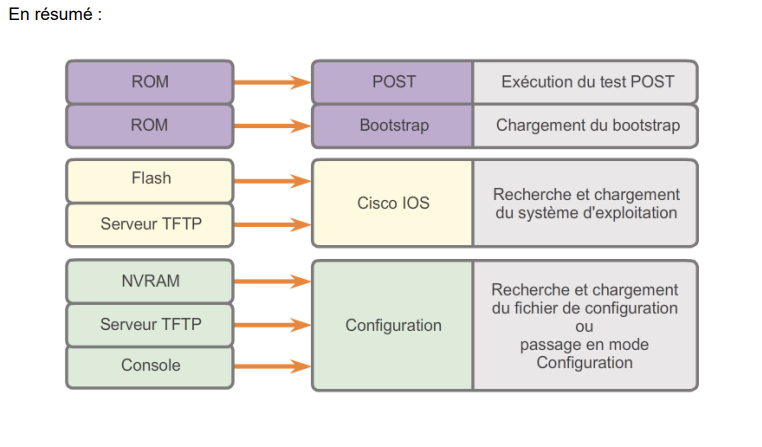
La mémoire vive non volatile est utilisé par IOS comme stockage permanent pour le fichier startup-config

La mémoire Flash est une mémoire non volatile utilisée comme stockage permanent pour l'IOS et d'autres fichiers associés au système, il y est copié de la mémoire

Flash vers la mémoire vive lors du démarrage

### Etapes lors du démarrage :

* Exécution du POST et chargement du Bootstrap (ROM)
* Localisation et chargement de l'IOS (Flash ou TFTP)
* Localisation et chargement du fichier de config initiale (NVRAM, TFTP ou Console)



## Connexion et interfaces d'un routeur

Les connexions sur un routeur Cisco peuvent être regroupées en deux catégories :

* Ports de gestion : ports console et aux utilisés pour configurer, gérer et dépanner le routeur (pas de transfert de paquets)
* Interfaces de routeur : configurée via l'adressage IP pour transporter le trafic.

On peut y accéder avec le port console, telnet ou SSH, le port AUX (comme le switch)

il existe plusieurs moyens d'accéder à la CLI (command-line interface) d'un routeur Cisco :

• via le port AUX

• via le port console

• via des protocoles comme Telnet ou SSH

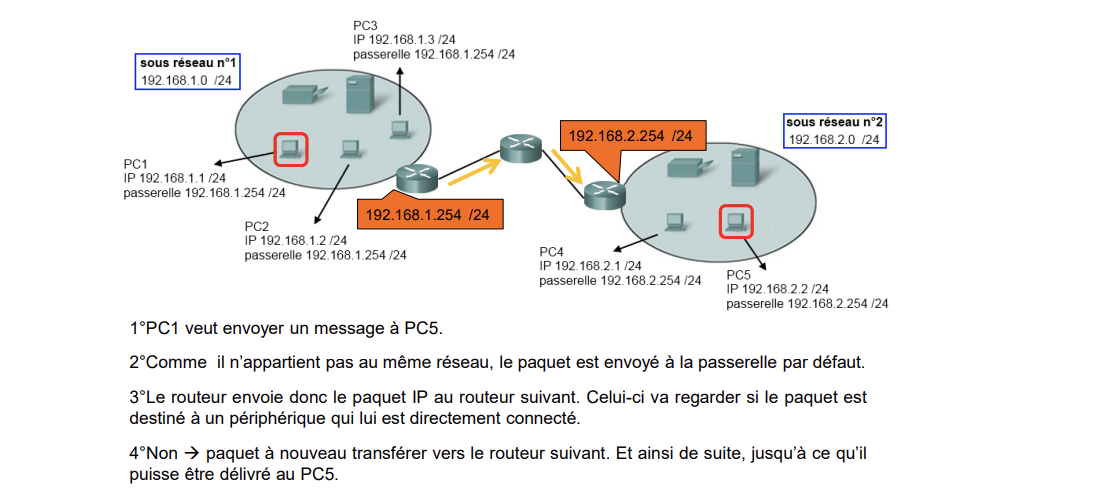
## Le routage

Le rôle principal du routeur c'est d'effectuer la fonction de routage (Hé oui, Jamy) c'est à dire de diriger les paquets entre les hôtes

Un hôte peut envoyer un paquet à :

* Lui (via 127.0.0.1 qui est une interface de bouclage)
* Un hôte local
* Un hôte distant => le routeur sera une "passerelle par défaut"

La passerelle par défaut, dans un réseau domestique, est souvent utilisé pour connecter un réseau local à internet.



## La table de routage

Fichier de donnée stocké dans la mémoire vive qui contient des informations de route sur le réseau connecté ainsi que les entrées de réseaux distants que le périphérique a découvertes. Le routeur utilise ces infos pour trouver le meilleur chemin.

Adresse de tronçons suivant : le prochain endroit ou l’on doit se diriger pour transférer un message (le routeur aka la passerelle par défauts)

Les routes possèdent trois caractéristiques principales :

* Le réseau de destination
* Le tronçon suivant ou la passerelle permettant d'atteindre le réseau de destination
* La métrique associée au réseau de destination

### Fonctionnement

* Le routeur lit l'adresse de destination dans l'en-tête IP et regarde dans sa table de routage s'il connait une route à cette adresse
* Il transfère le paquet au prochain routeur en fonction du tronçon suivant spécifié par cette route.

Un routeur peut être configuré pour posséder une route par défaut. Il s'agit d'un route qui correspond à tous les réseaux de destination.

Dans les réseaux IPv4 l'adresse 0.0.0.0 avec le masque 0.0.0.0 est utilisée à cet effet. La route par défaut est utilisée pour transférer

Les paquets pour lesquels aucune entrée ne figure dans la table de routage pour le réseau de destination.

Quand un routeur reçoit des info. sur des nouvelles routes ou des routes modifiées, il met à jour sa propre table de routage et transmet ces infos aux autres routeurs.

C'est donc du routage dynamique et l'inconvénient est que l'échange d'info. afin d'avoir les routes correctement à jour impose une surcharge de la bande passante.

Le routage statique c’est quand on doit configurer manuellement les tronçons suivant

Les protocoles de routage sont :

* RIP [in peace] (Routing Information Protocol)

Chaque route est associée à une métrique (et nombre de sauts limité à 15)

Chaque routeur envoie à ses voisins ses info. de routage (toutes les 30 sec)

Il va calculer les meilleures routes et déduire sa table de routage selon la métrique calculée

* EIGRP (Enhanced Interior Gateway Routing Protocol)

Calcule les métriques sur base d'une formule composée du délai, de la bande passante, de la fiabilité et de la charge.

Au niveau du réseau, chaque routeur envoie un paquet "Hello" à ses voisins toutes les 5sec afin de dire qu'il est actif et que ses routes sont correctes.

Au niveau de l'échange d'information une mise à jour concernant une table de routage n'est envoyée que lorsque celle-ci est modifiée. Cette màj contiendra que les routes modifiées et sera envoyée qu'aux routeurs concernés

* OSPF (Open Shortest Path First)

Permet d'avoir des routes de plus de 15 sauts

Utilise une métrique plus compliquée (prenant compte des débits)

# Couche transport

## Introduction

La couche transport est chargée de l'établissement d'une session de communication temporaire entre deux applications et de l'acheminement des données entre elles.

La plupart de ses protocoles ont des fonctions essentielles communes :

* Segmentation et reconstitution => diviser un bloc de données en des sous-blocs plus petit et va les reconstituer à la réception
* Multiplexage de conversions => à l'aide du port de l'application ou du service, la couche transport va déterminer à qui les données se rapportent

Dans le cadre du TCP/IP la segmentation et la réorganisation peuvent être fait à l'aide des protocoles TCP et UDP

Objectifs de la couche transport

* Effectuer un suivi des communications individuelles entre les applications résidant sur les hôtes source et de destination
* Segmenter les données et gérer chaque bloc individuel
* Réassembler les segments en flux de données d'application
* Identifier les différentes applications en leur affectant un numéro de port

## Fiabilité de la couche transport

Elle est basée sur 3 opérations de base :

* Effectuer le suivi des données transmises
* Accuser la réception des données
* Retransmettre toute donnée n'ayant pas fait l'objet d'un accusé de réception

## Les protocoles TCP et UDP

### TCP (Transmission Control Protocol) -> Fiable

Protocole de couche transport fiable et complet, qui garantit que toutes les données arrivent à destination.

Il segmente un message en partie numérotées à une destination, si il ne reçoit pas d'accusé de réception, il renvoie tout en supposant que ça a été perdu.

Acheminement fiable : Le protocole TCP garantit que chaque bloc de données envoyé par la source parvienne à la destination, même en cas de corruption ou de perte pendant le transfert sur le réseau. Il demande à la source de retransmettre les données perdues ou endommagées pour assurer l'intégrité de la transmission.

Reconstitution ordonnée des données : Pour pallier aux variations de débit dans les réseaux, le protocole TCP numérote et ordonne les segments de données, assurant ainsi qu'ils sont reçus dans le bon ordre à destination.

Contrôle de flux : Face aux ressources limitées des hôtes du réseau (comme la mémoire ou la bande passante), le protocole TCP régule le flux de données en demandant à l'application émettrice de réduire sa transmission lorsque ces ressources sont surexploitées, assurant ainsi une utilisation efficace des ressources disponibles.

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, document

Description générée automatiquement

En-tête TCP = 20 octets

### UDP (User Datagram Protocol) -> Pas fiable

Protocole de couche transport très simple qui ne permet pas de garantir la fiabilité

Il fournit des fonctions de base permettant d'acheminer des segments entre les applications appropriées avec peu de surcharge.

* **Sans connexion** : Le protocole UDP n'établit pas de connexion entre les hôtes avant que les données puissent être envoyées et reçues.
* **Acheminement non fiable** : Le protocole UDP ne garantit pas que les données sont acheminées de manière fiable. Aucun processus dans le protocole UDP ne permet de faire retransmettre à l'expéditeur les données perdues ou endommagées.
* **Aucune reconstitution ordonnée des données** : Le protocole UDP n'offre aucun mécanisme pour réorganiser les données dans leur ordre initial si elles sont reçues dans un ordre différent de celui dans lequel elles ont été envoyées. Les données sont simplement remises à l'application dans l'ordre où elles arrivent.
* **Aucun contrôle de flux** : Le protocole UDP ne propose aucun service pour contrôler la quantité de données envoyées par la source afin d'éviter de submerger le périphérique de destination. Si les ressources sur l'hôte de destination sont surexploitées, l'hôte de destination abandonne généralement les données envoyées jusqu'à ce que des ressources soient disponibles.

En-tête UDP = 8 octets

Une image contenant texte, capture d’écran, Police, Parallèle

Description générée automatiquement

Donc TCP > UDP

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

## Les numéros de port classé par l'IANA

* Ports réservés (0 à 1023)

Ils sont réservés à des services ou applications

* Ports inscrits (1024 à 49151)

Affecté à des processus ou applications d'utilisateurs

* Ports privés ou dynamiques (49152 à 65535)

Appelés port éphémères, affectés de façon dynamique à des applications clientes lors d'une connexion

Exemple de ports réservés :

* 69 TFTP
* 21 FTP
* 23 Telnet
* 80 HTTP
* 53 DNS

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

## Etablissement d'une connexion TCP

1. Le client demande l'établissement d'une session client-serveur avec le serveur

Envoi d'une demande de synchronisation avec numéro de séquence

1. Le serveur accuse réception de la session et demande l'établissement d'une session serveur-client

Réponse du serveur avec ACK égal au numéro d'ordre reçu +1 et son numéro d'ordre de synchronisation

1. Le client accuse réception de la session serveur-client

Connexion établie, le client répond avec un ACK égal au numéro d'ordre reçu + 1.

• URG : indique que le champ pointeur de donnée urgente est utilisé.

• ACK : indique que le numéro de séquence pour les acquittements est valide.

• PSH : indique au récepteur de délivrer les données à l'application et de ne pas attendre le remplissage des tampons.

• RST : demande la réinitialisation de la connexion.

• SYN : indique la synchronisation des numéros de séquence.

• FIN : indique fin de transmission.

## Fermeture d'une connexion TCP

1. Le client n'a plus rien à envoyer, il envoie un segment pour demander la fin de la connexion (FIN)
2. Le serveur envoie un ACK disant qu'il a bien reçu le segment FIN, afin de fermer la session client-serveur
3. Le serveur envoie un segment FIN au client pour mettre fin à la session serveur-client
4. Le client envoie un ACK pour dire qu'il a bien reçu le segment FIN

Une image contenant texte, capture d’écran, Police, diagramme

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

## La taille de fenêtre

La quantité de données qu'une source peut transmettre avant qu'un accusé de réception soit reçu est la "taille de fenêtre"

Cette taille est définie lors du démarrage de la session

Le protocole TCP peut réduire la taille de la fenêtre afin de mieux contrôler le flux de données (envoie d'ACK plus fréquent, évite les pertes)

## Gestion des pertes de segments du TCP

Quand le protocole TCP source envoie des segments de données, il va placer une copie du segment dans une file d'attente de retransmission

Et va déclencher en même temps un timer. Si il ne reçoit pas d'ACK avant la fin du timer, il va retransmettre à partir du dernier numéro d'accusé de réception

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

## Protocole de la couche application utilisant UDP

UDP c'est quand même pas de la merde, c'est utile pour certains protocoles

* DNS
* DHCP
* TFTP
* RIP
* VoIP

Il n'y a pas de numéro d'ordre dans le protocole UDP, donc il ne sait pas réordonner les datagrammes => Il les réassemble dans l'ordre qu'il les a reçus

# La couche application

## Introduction

Couche la plus proche de l'utilisateur final, elle sert d'interface entre les applications et le réseau sous-jacent

Elle possède trois fonctionnalités principales :

* Met en forme ou présente les données d'un hôte dans un format compatible pour la réception par le périph. Destinataire
* Compresse les données afin qu'elles puissent être décompressée à l'arrivée
* S'occupe du chiffrement/déchiffrement des données en vue de leur transmission

La couche session a pour rôle de créer et gérer les dialogues entre les app source et destination

## Le protocole HTTP

1. Lancement d'une requête HTTP client-serveur
2. Le serveur envoie au client le code HTML de la page web
3. Le client décode à l'aide du navigateur le code HTML

Il s'agit du protocole d'application les plus utilisés.

Il existe trois types de message courant :

* GET => requête cliente pour obtenir des données
* POST et PUT

Servent à uploader des fichiers de données vers le serveur Web

/ ! \ il n'est pas sécurisé => tout est envoyé en texte brut

HTTPS est sécurisé, il chiffre et déchiffre le trafic mais est plus lent à cause de ça

### Caractéristiques du protocole HTTP

Utilise TCP au port 80

Stateless : le serveur ne maintient aucune info sur les requêtes des clients

Non sécurisé => pas de chiffrement

Il y a eu HTTP 1.0 et 1.1, pas de keep-alive dans 1.0 (connexion persistante)

### Codes de statut

1xx : info

2xx : succès

3xx : redirection

4xx : erreurs du client

5xx : erreurs du serveur

### Le cache

Lorsqu'une page ne subit pas de modification, elle est mise en cache

Réduit le temps d'attente

Réduit le trafic des réseaux

Il y a le cache navigateur => permet au navigateur de fournir immédiatement les objets présents dans son cache sans devoir faire de requête

Et le cache mandataire (proxy server) => les clients utilisant un proxy vont disposer de son cache

### Les cookies

Permettent au serveur de mémoriser des données du côté client

## Les protocoles Email

### SMTP

Permet de transférer les e-mails de manière fiable et efficace.

Port :

* 25 sans chiffrement
* D'autres avec chiffrement

### POP3

Port : 110

Permet à ordinateur de récupérer des e-mails à partir d'un serveur de messagerie.

L'email est téléchargé du serveur au client puis supprimé du serveur

### IMAP

143 ou 220 selon la version

Des copies des messages sont téléchargées vers l'application cliente

Les messages originaux sont conservés sur le serveur jusqu'à ce qu'ils

Soient supprimés manuellement.

## DNS

Service de nom de domaine, associe les noms des ressources à l'adresse réseau numérique requise.

=> Associe un domaine à une IP

## DHCP

Port :

* Serveur 67
* Client 68

Permet aux périphériques d'un réseau d'obtenir d'un serveur DHCP des adresses IP et d'autres info

Généralement, on utilise les adresses statiques pour des périphériques réseaux et le serveur DHCP attribue des IP aux autres (périphérique finaux)

## FTP

Permet le transfert de données entre un client et un serveur, port 20 et 21

Existe en version simplifiée appelée TFTP, (pas sécurisé), port 69