TOM DENEYER

TELECOMMUNICATIONS ET RESEAUX

2023-2024

Email : tomdeneyer@gmail.com
Discord : Littl3T

HAUTE ECOLE EN HAINAUT

Sciences et technologies

Tables des matières

Commandes Cisco-Laboratoire

Modes du terminal

1. > : Mode utilisateur : accès par défaut, aucun droit intéressant pour la configuration
2. # : Mode privilégié, permet certaines actions utiles sur le périphérique, visualisation, enregistrer les configurations…
3. (config)# : Mode de configuration globale, permet la configuration des éléments propre à l'appareil lui-même.
4. (config-if)# : Mode de configuration spécifique, permet la configuration de ports, et autres éléments spécifiques.

Configurations de bases

1. Changer le nom de l'appareil : *Mode de configuration globale*
   ➔**enable**
   ➔**configure terminal**
   ➔ **hostname** *nom_du_périphérique*
2. Mot de passe du port console : *Mode de configuration spécifique de la ligne console…*
   ➔**enable**
   ➔**configure terminal**
   ➔**line console 0**
   ➔**password** *mot_de_passe*
   ➔**login** ~~(login permet d'activer le mdp)~~
3. Mot de passe pour passer en mode privilégié : *Mode de configuration globale*
   ➔**enable**
   ➔**configure terminal**
   ➔**enable secret** *mot_de_passe* OU **enable password** *mot_de_passe*
   Ensuite, ajouter le chiffrement du mot de passe via…
4. Sécuriser les lignes Vty : *Mode de configuration spécifique aux lignes vty*
   ➔**enable**
   ➔**configure terminal**
   ➔**line vty 0 15**
   ➔**password** *mot_de_passe*
   ➔**login**
5. Chiffrer les mots de passe : *Mode configuration globale*
   ➔**enable**
   ➔**configure terminal**
   ➔**service-password-encryption**
6. Message de bannière : *Mode configuration globale*
   ➔**enable**
   ➔**configure terminal**
   ➔**banner motd «***message* **»**
7. Enregistrer les configuration : *Mode privilégié*
   ➔**enable**
   ➔**copy running-config startup-config**

Configuration Ipv4

1. Adresser une ip à une interface/port… : *Mode de configuration spécifique au port*
   ➔**enable**
   ➔**configure terminal**
   ➔**interface** *nom_interface*
   ➔**ip address** *adresse_ipv4 masque_de_sous_réseau*
   ➔**no shutdown**
2. Ajouter une description sur l'interface : *Mode de configuration spécifique au port*
   ➔**enable**
   ➔**configure terminal**
   ➔**interface** *nom_interface*
   ➔**description** *description*
3. Ajouter une default-gateway : *Mode de configuration globale*
   ➔**enable**
   ➔**configure terminal**
   ➔**ip default-gateway** *adresse_ipv4*

Configuration Ipv6

1. Adresser une ipv6 à une interface/port… : *Mode de configuration spécifique au port*
   ➔**enable**
   ➔**configure terminal**
   ➔**interface** *nom_interface*
   ➔**ipv6 address** *adresse_*ipv6**/**masque*_de_sous_réseau*
   ➔**no shutdown**
2. Adresser une adresse link local, adresse accécible uniquement au sein du réseau. L'adresse link local du routeur est utilisé comme passerelle par défaut (souvent fe80 ::) : *Mode de configuration sépcifique au port*
   ➔**enable**
   ➔**configure terminal**
   ➔**interface** *nom_interface*
   ➔**ipv6 address** *adresse_*ipv6 ***link-local***
   ➔**no shutdown**
3. Activer le routage Ipv6 : *Mode de configuration globale*
   ➔**enable**
   ➔**configure terminal**
   ➔**ipv6 unicast-routing**

Cours théoriques

Chapitre 1 *(introduction)*

Unités

- Capacité = Volume maximum Volume = Quantité de donnée
  Capacité ≠ Volume
- bit = binary digit
  Octet(byte) = 8bits (256valeurs décimales possibles)
  Bit/s ou bps = nombre de bit/seconde transférés
- Base décimale et binaire…

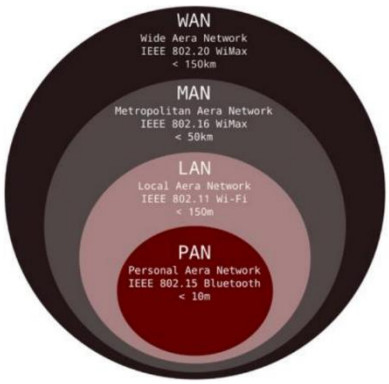
2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
256	128	64	32	16	8	4	2	1

Rôle d'administrateur

1. Gestion de budget, priorités, besoins, ordinateurs et périphérique, des utilisateurs, performances systèmes, fichiers et disques, gestion des problèmes, du réseau, des sauvegardes de données, de la sécurité et de l'infrastructure en générale.
2. Gérer les menaces, qui sont de différents types…
   - Virus, vers, chevaux de Troie
   - Logiciel espions et publicitaire
   - Attaque zero-day
   - DDOS
   - Interception des données, usurpation d'identité, …
3. Protection de l'infrastructure ➔ Salles fermées, accès restreints, pare-feu, chiffrement des données, politique de sécurité pour les employés, etc…
4. Être à jour sur les technologies sur le marché…

Communication aujourd'hui

- Utilisation
  Jouer – E-commerce – Parler – Apprendre – Echange de fichier…
- Fonctionnement des lignes
  - ➢ Téléphone fixe/mobile (télécommunication)
  - ➢ Télédistribution (Câblo-opérateur)
  - ➢ Internet (Réseau Informatique)
- Etendues des réseaux
  - ➢ PAN (personal area network)
  - ➢ LAN (local area network)
  - ➢ MAN (metropolitan area network)
  - ➢ WAN (wide area network)

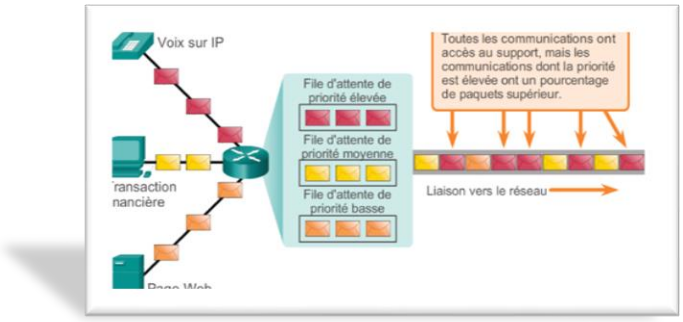


- Modes de transmissions
  - Diffusion : le périphérique envoie à tous les appareils (broadcast)
  - Point à point : le périphérique envoie à un seul destinataire (unicast)
    Topologie Etoile, maillée, point à point
- Topologies
  - Physique : forme du réseaux avec ses périphériques
    - Diffusion : bus, anneau
    - Point à point : étoile, maillée
  - Logique : Se concentre sur le partage du réseau, les Ip…
    - Ethernet : accès au média via CSMA/CD
    - Token Ring : accès via le token, MAU(Media Acces Unit)
    - FDDI(Fiber distributed data interface): utilise câbles optiques et token.
- Mode de fonctionnement
  - Serveur/client : Le serveur écoute et attend que le client intervienne.
  - P2P (Peer to peer) : Chaque client est lui-même un serveur.
- Composants d'un réseau
  - Périphériques finaux : hôtes, utilisateur.
  - Périphériques intermédiaires : relient les finaux, offrent une connectivité.
  - Support de transmission : cuivre, optique, wireless
  - Services et processus : programmes de communications
- Vocabulaire
  - NIC (carte réseau) : permet à un ordinateur de se connecter au réseau
  - Port physique : Connecteur d'un périphérique
  - Interface : port spécifique d'un périphérique réseau
  - Internet : Ensemble mondial de réseaux
  - Intranet :Réseau LAN, accessible depuis une localisation uniquement.
  - Extranet : Réseau privé, accessible depuis l'extérieur
  - FAI : Fournisseur d'accès internet
- Accès internet
  - Câble
  - xDSL : DSL haut débit
  - DSL *(Digital Subscriber Line)* : fonctionne sur ligne téléphonique comportant trois canaux :
    - Canal appel téléphonique
    - Canal download
    - Canal upload
  - ADSL *(Asymmetric Digital Subscriber Line)* : DSL avec une asymétrie de débit sur les canaux
  - VDSL *(Very-high-bit-rate DSL)* : Plus haut débit de donnée.
  - VDSL2 : Encore plus rapide que le VDSL
  - Par fibre, FTTx (x étant l'endroit ciblé par la fibre) :
    - FTTN = Fiber To The Neighborhood
    - FTTC= " " curb (trottoir)
    - FTTB= " " building
    - FTTH= " " Home
  - Satellite
  - Cellulaire (ex: telephone portable)

- Par ligne commutée (ancêtre de l'ADSL)
- WiMax *(Worldwide Interoperability for Microwave Access)*: Transmission via onde radio (maximum 70mbit/s à 50km)

Concepts avancés

- Réseaux dédiés: une infrastructure par type de technologie (info, tv, téléphone)
- Réseau convergents : infrastructure globale avec tous les services concentrés
- Communication simultanées…
  - Segmentation : couper les données en petits blocs
  - Multiplexage : entremêler différentes conversations (leurs segments à suite) ensemble.
- Règle des 5 neufs : 99,999% de fiabilité (5,26minutes indisponible par ans)
- Qualité de service QoS
- Niveaux de priorités…
- BYOD : bring your own device
- CPL: Réseau pas les prises de courant électrique



Virtualisation

- Centraliser différents services/serveurs en un seul plus gros.

Avantage	Inconvénient
- Un seul serveur à acheter - Portabilité du serveur - Administration simplifiée - Réduction d'éléctricité - Accélération de la mise en place	- Coût plus élevé - Panne généralisées - Vulnérabilité généralisée

- Hyperviseurs

Type 1	Type 2
Dans la base sur la machine, pilote des OS qui sont installés, comme Microsoft HyperV, XEN…	Architercure herbergée, application insallée sur un OS existant, comme VirtualBox, VmWare Workstation…

Cloud Computing

- Utilisation des ressources d'une machine distante, via le réseau.
- Ex : Windows Azure, AWS, iCloud, OneDrive…

Chapitre 2 *(communication)*

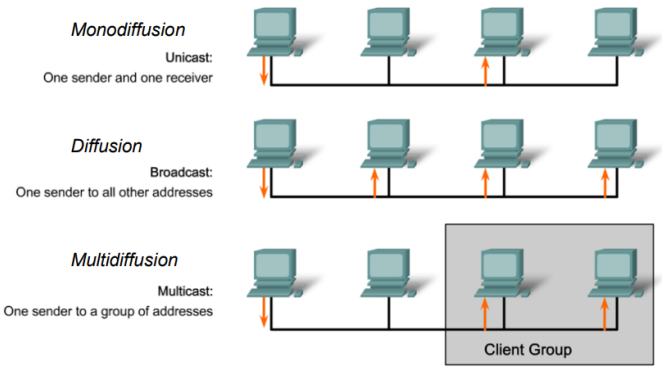
Un routeur domestique fait : Routeur/Switch/Par-feu/point d'accès sans fil

Cisco ISO (Internet networking operating system)

- Un routeur Cisco fait: sécurité réseau, adressage IP, configuration interfaces, QoS, Routage, prise en charge des technologies.
- Accès interface CLI (interface commande) via…
  - Port console
  - Telnet ou SSH (secure shell), accès aux sessions vty à distance
  - Port AUX
- Fichiers de configuration : startup config au démarrage depuis la NVRAM, se charge dans la RAM ensuite.
- Configuration actuelle : running config, pour être sauvegardée, écrase la startup-config.
- Possible de sauver à distance via FTP (sur serveur).
- Hiérarchie de l'IOS…
  - Mode exécution
  - Mode privilégie (enable)
  - Mode configuration globale (configure terminal)
  - Mode configuration spécifique (…)
- Affectation de noms sur IOS
  - Commence par un lettre, pas d'espace, termine par lettre/chiffre, 64 charactères maximum.

Fonctionnement protocoles

- Les protocoles réseaux régissent la communication sur le réseau.
- Encapsulation = mettre le message dans une « enveloppe », avec le destinataire, l'origine, etc… et dedans se trouve les données du message.
- Transmission d'une donnée :
  - Codage, transformation de la donnée dans un format acceptable et transmissible
  - Formatage des données dans une trame
- Synchronisation des échange
  - Méthode d'accès : comment réagir si collisions..
  - Contrôle de flux : Quantité d'information envoyé et vitesse…
  - Délai d'attente de la réponse : supposition d'une erreur d'acheminement…



Modèle de protocole TPC/IP

Model de protocole basé sur une norme ouverte, gratuite et utilisable par tous les constructeurs et développeurs.

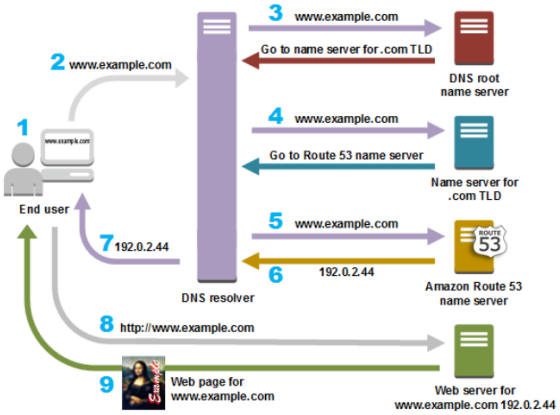
Couche application

Informations depuis l'application utilisée pour sortir les données transportées, *ex : depuis un site internet http. Couche la plus proche de l'utilisateur et des applications.*

➔SMTP (Simple mail transfert protocol) : Transfert les mails, orienté connexion.

➔DNS (Domain Name System ou Domain Name Service) qui a pour rôle de traduire les noms de domaines. Par exemple www.cisco.com en adresse IP
Etapes simplifiées pour résoudre l'adresse :

1) Check si adresse est connue dans le navigateur en cache. Si non…
2) Demande à l'OS de check son cache, si non…
3) Requête envoyée au DNS du FAI, le DNS resolver va regarder s'il connait l'adresse dans son cache, si oui il lui envoie, si non…
4) Le resolver contacte le serveur racine (Root server), il y en a 13 au monde qui contiennent toutes les adresses, et ainsi de suite.



➔DHCP (Dynamic Host Configuration Protocol) qui attribue dynamiquement des adresses IP aux stations clientes au démarrage.

➔POP (Post Office Protocol) et IMAP (Internet Message Access Protocol) qui permettent aux clients de récupérer des e-mails depuis un serveur de messagerie.
POPv3 ne sauvegarde pas les emails et donc pas adapté pour une petite entreprise qui a besoin de garder ceux-ci en mémoire.
IMAP lui garde en mémoire sur un serveur les emails.

➔FTP (File Transfert Protocol), SFTP (Secure FTP) et TFTP (Trivial FTP) qui permettent à un utilisateur d'accéder à des fichiers sur un autre hôte du réseau.

➔HTTP (HyperText Transfert Protocol) et HTTPS (HTTP Secure) qui permettent d'échanger du texte, des graphiques, des sons, des vidéos et autres fichiers multimédias sur le Web.

Requête GET = obtenir les données
Requête POST et PUT = télécharger des fichiers

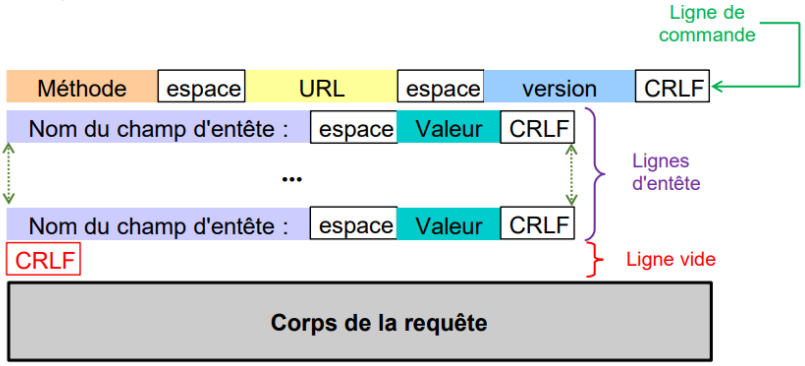
Quels sont les caractéristiques du protocole HTTP ?

HTTP utilise le service de transport TCP
- Le client initie une connexion TCP vers le serveur, port 80
- Le serveur accepte les connexions TCP du client
- Les messages http sont échangés entre le navigateur (client http) et le serveur web (serveur http)
- La connexion TCP est fermée

HTTP est dit "stateless"
- Le serveur ne maintient aucune information sur les requêtes des clients.

HTTP est un protocole non sécurisé
- Les messages POST téléchargent des informations vers le serveur dans un format de texte clair pouvant être intercepté et lu. De même, les réponses du serveur (généralement, des pages HTML) ne sont .pas chiffrées.
- Si l'on veut que les informations soient sécurisées, il faut alors utiliser le protocole

http 1.1 reste disponibles après une requête fermée pendant un certain temps (keep-alive)
les requêtes ressemblent à ceci :



Codes http :
1xx = informations
2xx = Succès
3xx = redirection
4xx = erreurs du client (exemple 404...)à
5xx = erreurs du serveur

Serveur proxy

Intermédiaire entre les périphériques d'un Lan et internet, sert à faire une distinction entre les réseaux externes à un réseau et à s'y connecter, permettant à tous les périphériques de disposer de son cache.

Cookies (miam)

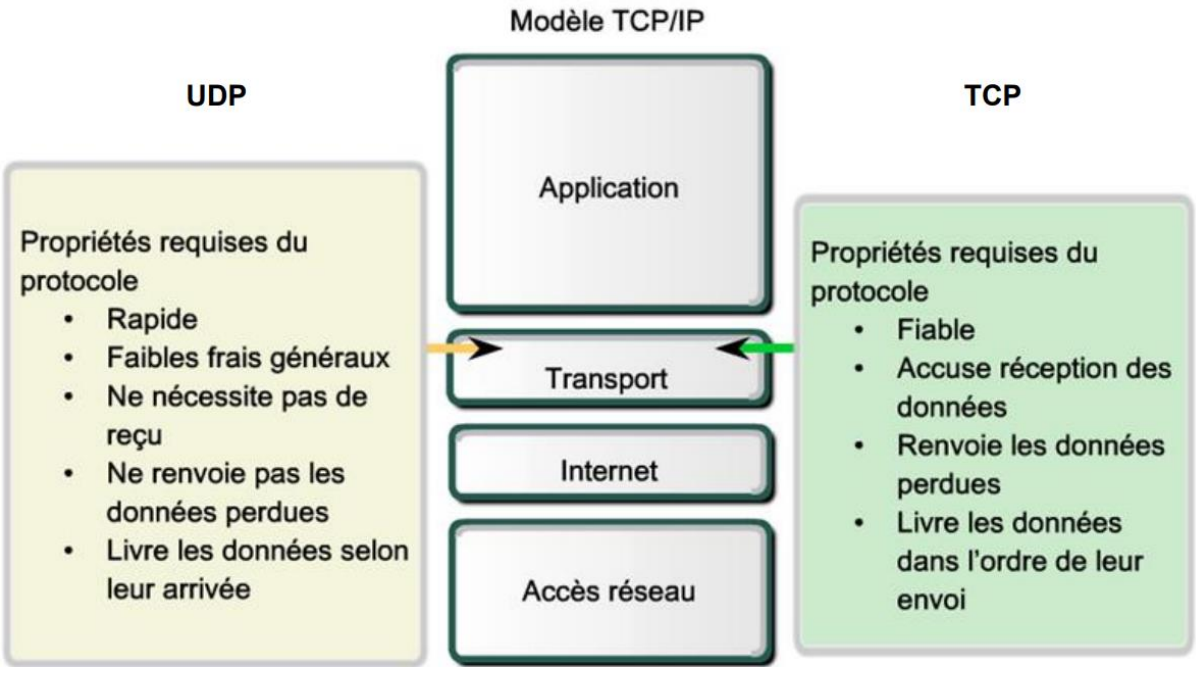
Mémorisation du cache coté client. Max 4ko, stocké dans le navigateur et fournit par un serveur.

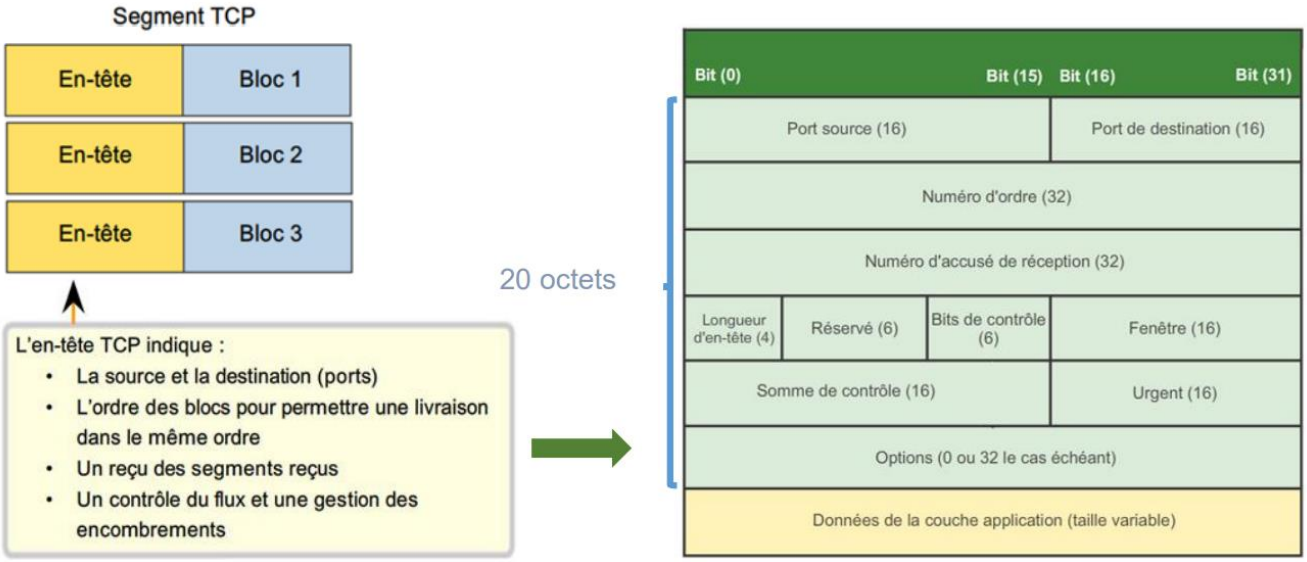
Couche transport

Fournit une méthode de transport des informations,
Segmentation et réorganisation via deux protocoles de transport…
Les segments sont attribué à certains « numéro de port » qui sont liés à des applications des périphériques.

➔TCP (Transmission Control Protocol) Très fiable garantissant à toutes les données d'arriver, utilise un accusé de réception. Transmet les données qui n'ont pas fait l'objet d'un accusé de réception.

➔UDP (User Diagram Protocol) Plus simple que le TCP mais moins fiable, permet l'envoie à un hôte sans connexion au préalable, mais sans confirmation de réussite de la transmission.



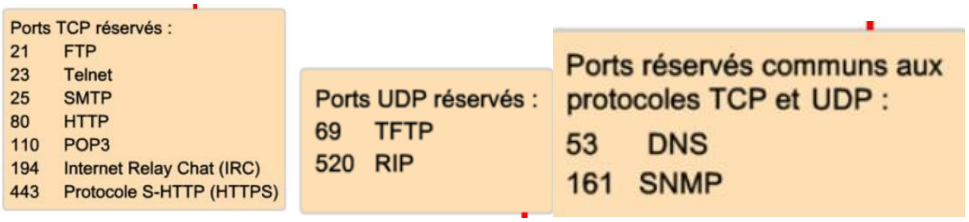


Numéro de port

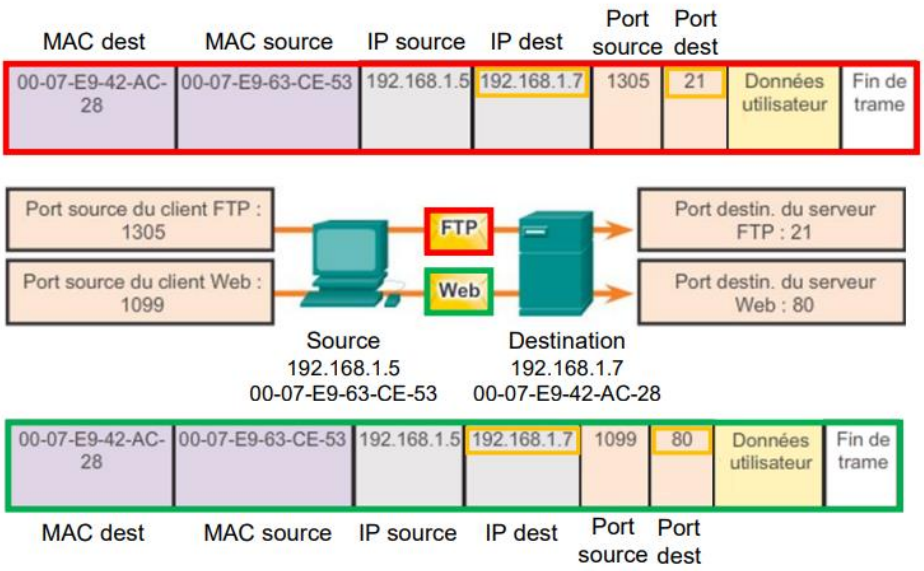
Sert à distinguer les différentes applications dans les en têtes des segments du transport. Avec un port source associé à une application et un port de destination.

Listes des ports réservés :

1) 0-1023 : services et applications les plus utilisés (http, pop3, ...)
2) 1024-49151 : ports inscrits affectés à des processus d'utilisateurs courants
3) 49152-65535 : port privés/dynamiques, éphémères et affectés de façon dynamique.



Trame transport



Etapes de connexion TCP

1) Client demande une session de communication avec le serveur
   Demande de synchronisation (SYN) et numéro de séquence SEQ= 100

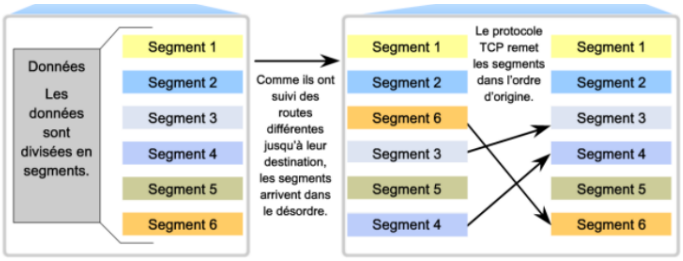
2) Le serveur revoie un accusé de réception de la session et demande une session serveur-client
   Accusé de réception ➔ ACK=101 et SEQ=300, et indicateur SYN
3) Le client revoie un accusé de réception au serveur
   Connexion établie, ACK=301. Quand les deux sessions sont établies, CTL = ACK

Bits de contrôle TCP

- **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.

Fiabilité

Si les segments arrivent dans le mauvais ordre, le protocole arrive à remettre ceux-ci dans le bon ordre, grâce à des numéro de segment. (Contrairement au protocole udp qui ne peut pas)



Couche Internet

Adressage des périphériques via protocoles IP (4 ou 6)

Encapsulation des données et routage de ceux-ci pour arriver à destination et procéder à la désencapsulation.

Protocoles de la couche internet :

➔IP (Internet Protocol) qui permet de recevoir des segments de message de la couche transport. Il regroupe les messages en paquets et il indique l'adresse des paquets pour permettre leur acheminement de bout en bout sur un inter réseau.

➔NAT (Network Address Translation) qui permet de convertir les adresses IP d'un réseau privé en adresses IP globales et publiques. (CAR MANQUE D'ADRESSE IPv4)

➔CMP (Internet Control Message Protocol) qui permet à un hôte de destination de signaler à l'hôte source des erreurs liées aux transmissions de paquets.

➔RIP (Routing Information Protocol) qui est un protocole de routage dynamique à vecteur de distance.

Couche Accès Réseau

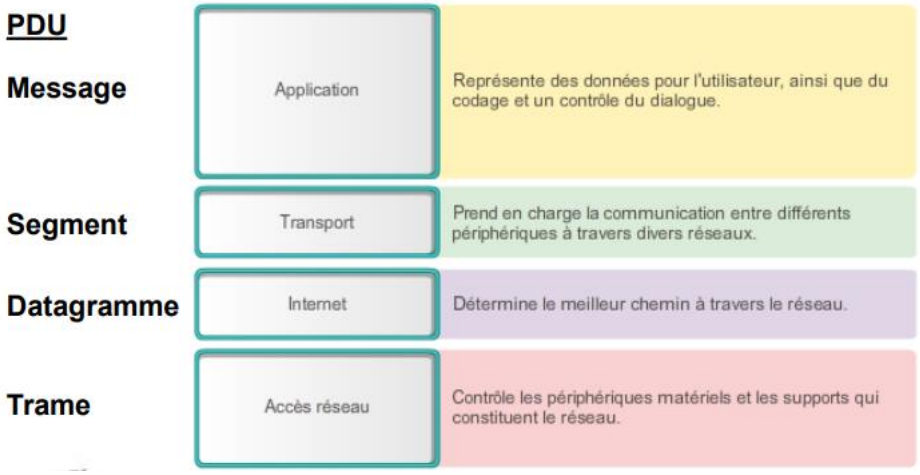
➔ARP (Address Resolution Protocol) Créer un lien entre l'adresse Ip et l'adresse MAC dans une table ARP

Table remplie soit dynamiquement avec l'analyse des messages passant, soit de manière statique

➔Ethernet qui définit les règles de câblage et de signalisation de la couche d'accès reseau.

➔WLAN (Wireless LAN) qui définit les règles de signalisation sans fil sur les fréquences radio 2,4 GHz et 5 GHz.

PDU (Protocol data unit) du modèle TCP/IP



Modèle OSI (open systems interconnection)

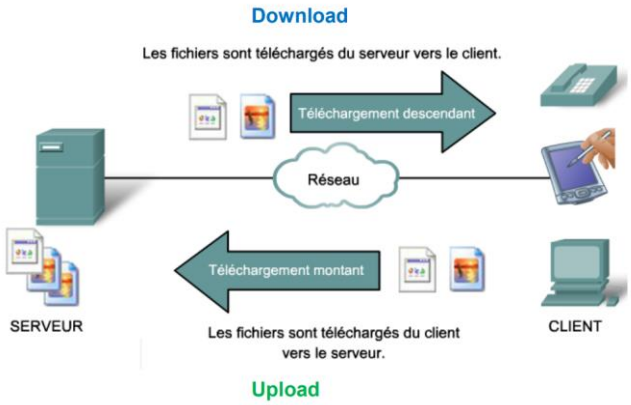
7.	**application**	La ***couche application*** contient les protocoles utilisés pour les processus communications.
6.	**présentation**	La ***couche présentation*** fournit une représentation commune des données transférées entre des services de couche application.
5.	**session**	La ***couche session*** fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.
4.	**transport**	La ***couche transport*** définit des services pour segmenter, transférer et réassembler les données de communications individuelles entre les périphériques finaux.
3.	**réseau**	La ***couche réseau*** fournit des services permettant d'échanger des parties de données sur le réseau entre des périphériques finaux identifiés.
2.	**liaison de données**	Les protocoles de ***couche liaison de données*** décrivent des méthodes d'échange de trames de données entre des périphériques sur un support commun.
1.	**physique**	Les protocoles de la ***couche physique*** décrivent l'ensemble des moyens permettant de gérer des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

Couches Application (7)

Couche la plus proche de l'utilisateur. Sert d'interface entre les applications et le réseaux sous-jacent. Les protocoles de cette couche sont utilisés pour échanger les données entres les programmes. (DNS, http, ftp, ...)

Modèle P2P

Peer-to-peer. Les réseaux P2P et applications P2P sont similaires mais fonctionnent différemment. La caractéristique principale est la décentralisation des ressources. Cependant, les applications P2P permettent à un périphérique de faire client et serveur dans une même communication (le plus connu étant le partage de fichier comme BitTorrent, eMule...)



Présentation (6)

Met en forme les données dans un format compatible pour la réception de celles-ci.

S'occupe aussi de la compression et chiffrement des données. (compression ex : MPEF, GIF, JPEG, ETC)

Session (5)

Rôle est de créer et gérer les dialogues entres les applications sources et destinations. Maintient le dialogue et redémarre les sessions interrompues ou inactives.

Couche Transport (4)

Assure la fiabilité des données acheminées entre hôte et destination. Incluant un accusé de réception. Fonctionne via les protocole TCP ou UDP de la suite TCP/IP

Couche Réseau (3)

Protocole IP utilisé pour l'acheminement des messages à travers le réseau.

Les protocoles IP sont appelles « Best-effort » car aucune surcharge n'est utilisé pour garantir la transmission des paquets. Ces protocoles sont indépendants du support mais « peu fiables », ce pourquoi on utilise TCP pour résoudre la fiabilité.

Passerelle par défaut

Lorsqu'un hôte doit envoyer un message à un réseau distant, il doit obligatoirement passer par une interface d'un routeur, également appelé « passerelle par défaut »

La passerelle par défaut est l'adresse IP d'une interface d'un routeur se trouvant sur le même réseau que l'hôte expéditeur.

Encapsulation

La couche 3 reçoit les données de la couche 4, et ajoute un en tête, pour créer un paquet.

Routage

La couche réseau fournit les services pour diriger les paquets vers les destinations. Chaque routeur traversé pour arriver à destination est appelé un *saut*.

Désencapsulation

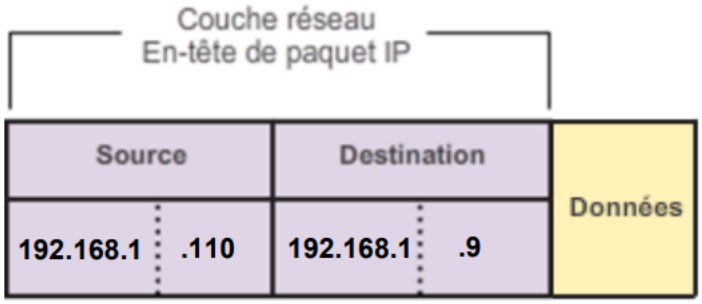
Vérification que le paquet est bien adressé, si oui désencapsulation par la couche réseau (3) ensuite transmission vers la couche transport

Nomenclature

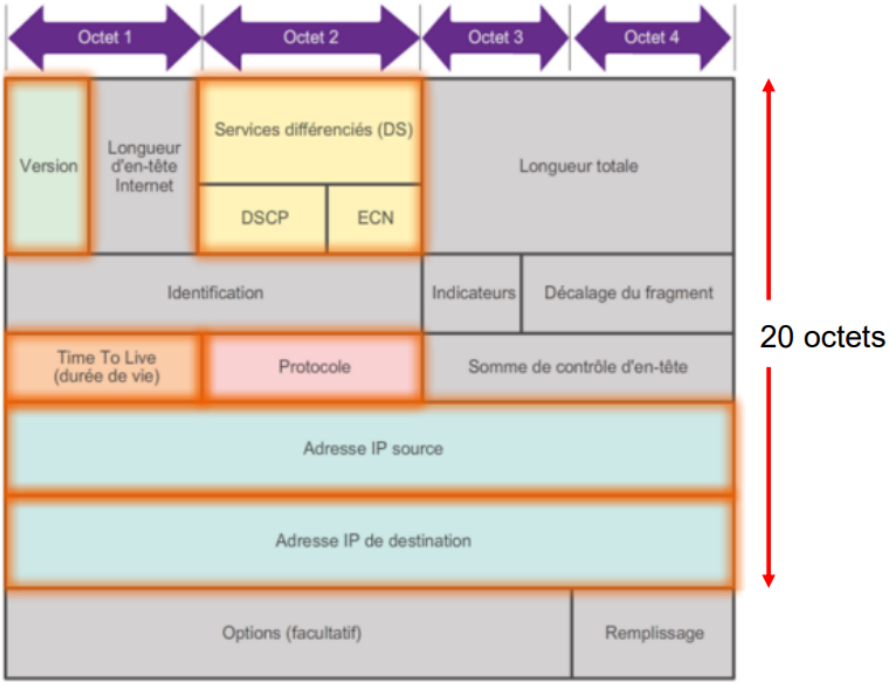
- Adresse IP source
- Adresse IP de destination

En-tête du paquet IP

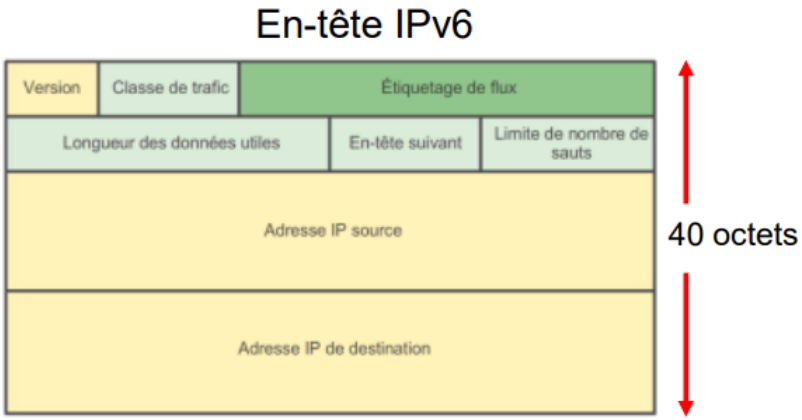
- Préfixe réseau
- Préfixe hôte



De manière plus complète :



Et en ipv6:



Couches liaison de données (2)

Couche liaison de données divisé en deux parties :

LLC (sous-couche supérieure)

Gère la communication entre les couches supérieurs/inférieurs, extrait les données et ajoute informations de contrôle.

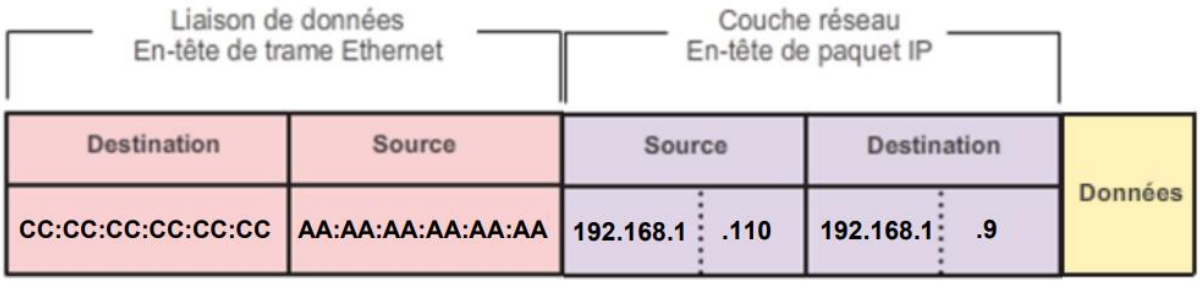
MAC (sous-couche inferieure)

Encapsulation des données + contrôle d'accès au support.
➔ en tête de trame + données + code de fin de **trame**

Adresse MAC :

- 48bits, 12chiffres hexadécimaux
- Exemple d'adresse MAC Ethernet : AA :B1 :34 :2F :18 :0^{E} (soit « : » soit «-»)
- Toutes les adresses MAC sont uniques (norme IEEE)

Entête de trame

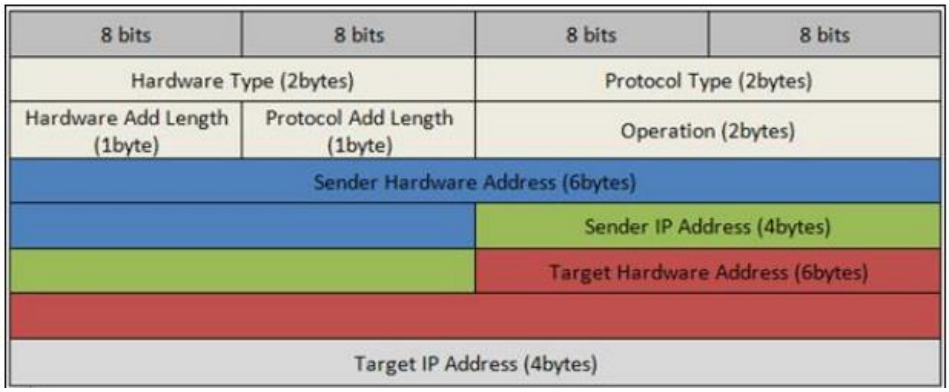


Protocole ARP

Faire le lien entre adresse IPv4 et adresse MAC
Charge table ARP (liste adresses) dans la RAM

Il complète la table ARP dynamiquement en analysant les flux avec le temps (ou de façon statique)

- Un périphérique à deux moyens pour la mise à jour de sa table ARP…
  - Surveiller le trafic sur le segment du réseau local. Enregistre des IP et MAC sources sous forme de mappage.
  - Envoie d'une requête ARP, diffusion de couche 2 à tous les périphériques du réseau local. L'adresse de destination est donc FF-FF-FF…, les nœuds dont l'adresse IP correspond à la requête ARP répondent avec une trame de monodiffusion. Et le périphérique fait le lien avec l'envoyeur et son adresse MAC/IP
- Message ARP :



Couche physique(1)

NIC

Les NIC sont les cartes réseau, qui connectent un périphérique au réseau. Carte Ethernet en filaire, Carte WLAN en sans-fil local.

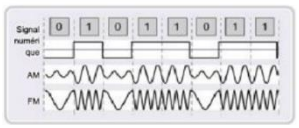
Supports réseau

- Fibre optique
- Sans fil
- Câble de cuivre

Pour un support à câble de cuivre, les signaux sont des variations d'impulsions électriques.

Pour la fibre optique, les signaux sont des variations lumineuses.

Pour les supports sans fil, les signaux sont des variations de transmissions radio.



Composants physique (--1)

Support électroniques, support et connecteurs qui transportent et transmettent les signaux (bits)

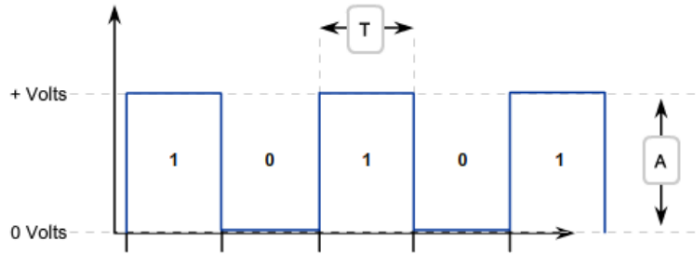
Le codage (--2)

Convertir un flux de bits de données en code prédéfini…

CODAGE NRZ

Non Return to Zero

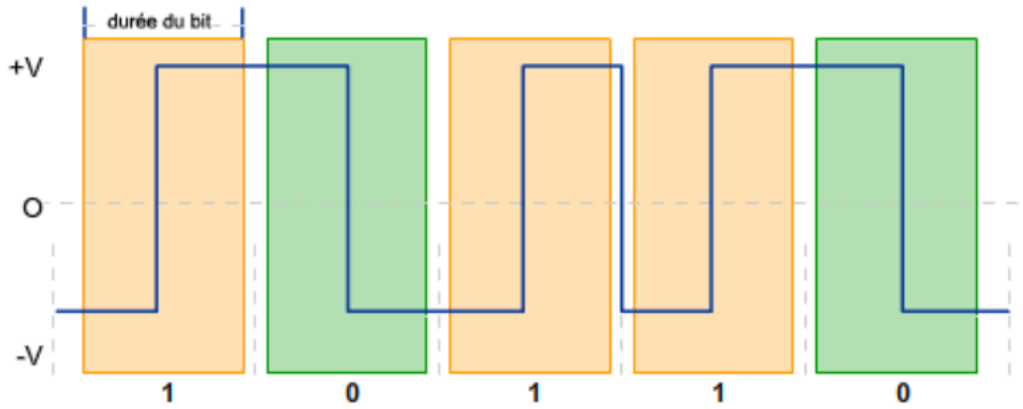
Bits sous une valeur de tension



T = durée du bit
A = Amplitude (hauteur des impulsions)

CODAGE MANCHESTER

Transitions de tension, au milieu de chaque durée de bit

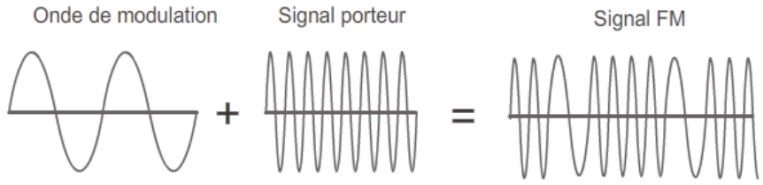


La signalisation (--3)

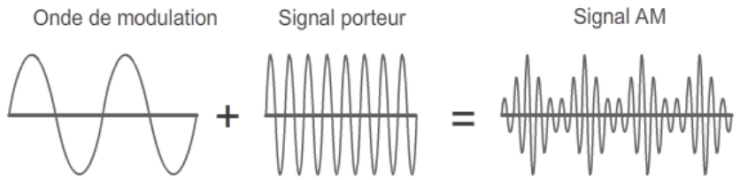
- Asynchrone : L'intervalle de temps entre les caractères ou les blocs de données peut être défini arbitrairement, ce qui signifie qu'il n'est pas normalisé. → les trames doivent comporter des indicateurs de début et de fin.
- Synchrone : les signaux de données sont envoyés synchronisés (c-à-d qu'ils se produisent à des intervalles réguliers appelés temps bits). Cette synchronisation se fait à l'aide d'un signal d'horloge échangé entre les deux périphériques qui doivent communiquer.

MODULATIONS DE LA SIGNALISATION

▪ **Modulation de fréquence (FM)** : méthode de communication dans laquelle la fréquence porteuse varie selon le signal.



▪ **Modulation d'amplitude (AM)** : technique de transmission dans laquelle l'amplitude de la porteuse varie selon le signal.



Bande passante

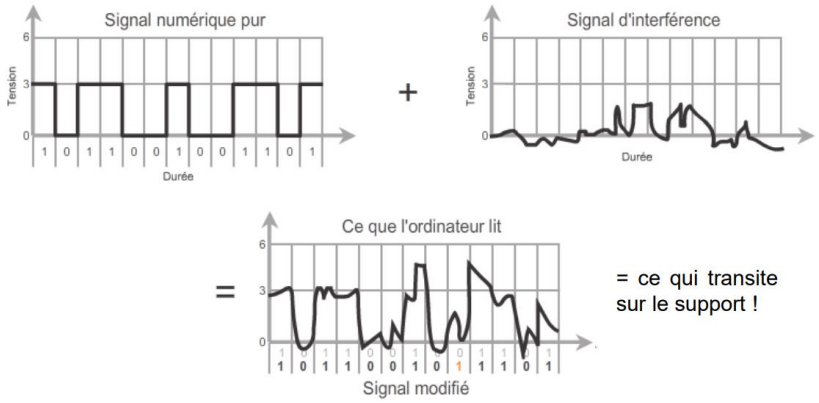
Quantité de donnée qui débite sur une période donnée, en kilobit par seconde (kbit/s) ou Mbit/s

Latence : Temps nécessaire d'un point A à un point B

Débit : Mesure de transfert de bit sur une période donnée

Débit applicatif : débit de données utilisables

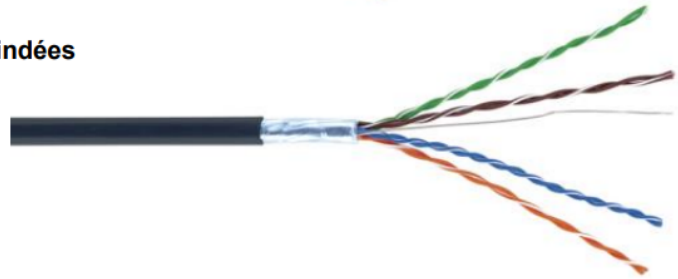
Perturbations électromagnétiques



Supports en cuivre

- **les câbles à paires torsadées non blindées**

- **les câbles à paires torsadées blindées**



- **les câbles coaxiaux**

(pour câble coaxiaux, connecteur BNC le plus répandu)

Torsade= protection interférences

Gaine= protection physique

Plastique sur les fils= protection électrique

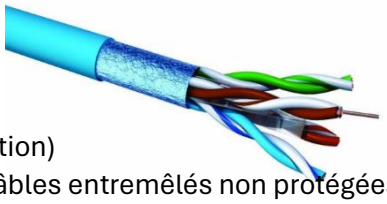
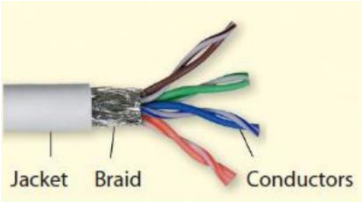


Figure 1 : Category 6A F/UTP cable

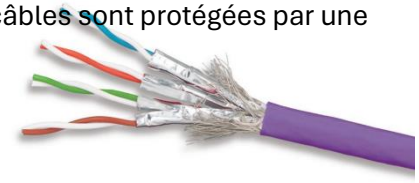
1) F/UTP (FTP) :
   F= foil shield (feuille en aluminium de protection)
   UTP = Unscreened twisted pairs (paires de câbles entremêlés non protégées)

2) S/UTP :
   S= Braid screen (une gaine tressée de protection)
   UTP…

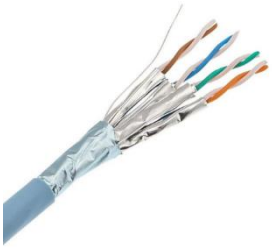


3) SF/UTP :
   SF= S + F (un tressage + une feuille de protection)
   UTP…

4) S/FTP :
   S= Braid Screen (Gaine tressée)
   FTP = Foil Screened twisted pairs (les paires de câbles sont protégées par une feuille de protection en aluminium)

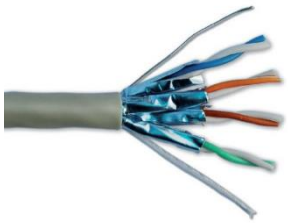


5) F/FTP :



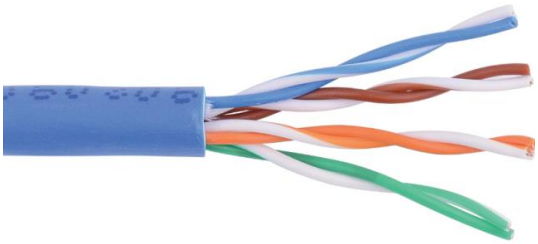
6) U/FTP :

U= pas de feuille ni tressage de protection globale



7) U/UTP :

Aucune protection du tout. (j'espère que le réseau prend la pilule au moins...)

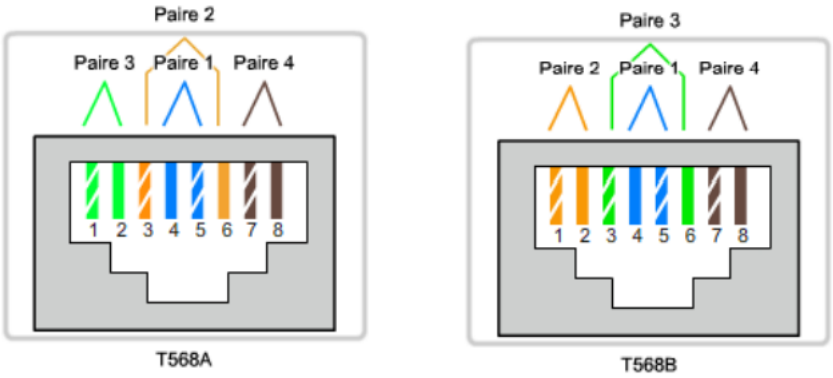


Ces normes (établies conjointement par la TIA et l'EIA) concernant le câblage utilisé permettent de différencier ainsi plusieurs catégories de câbles :

- **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 6a** : ce type de câble permet toujours un débit maximum de 10Gbit/s mais va permettre une bande passante plus haute (500MHz) et une distance maximum plus grande (100m).
- **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.

CONNECTEURS RJ-45

Type de câble	Standard	Application
Ethernet droit	Les deux extrémités T568A ou T568B	Connexion d'un hôte réseau à un périphérique réseau tel qu'un commutateur ou un concentrateur.
Ethernet croisé	Une extrémité T568A, l'autre T568B	Connexion de deux hôtes réseau. Connexion de deux périphériques intermédiaires réseau (un commutateur à un commutateur, ou un routeur à un routeur).
Renversement	Exclusif à Cisco	Connexion d'un port série de station de travail à un port console de routeur, à l'aide d'un adaptateur.



Nous avons vu que le câble droit permettait de relier :

- Un hôte réseau (PC, imprimante,...) à un hub ou un switch
- Un switch à un routeur

Nous avons vu que le câble croisé permettait de relier :

- Un ordinateur à un ordinateur
- Un switch à un switch
- Un routeur à un routeur

Fibre optique

Deux Types...

- Monomode (SMF) un seul rayon lumineux par un laser (cœur en verre 8-10microns (longues distances)
- Multimode(MMF) principe des émetteurs à LED, plusieurs signaux (cœur en verre 50-62microns (courtes distances)

Connecteurs :

Au niveau de la connectique, il existe beaucoup de connecteurs différents :

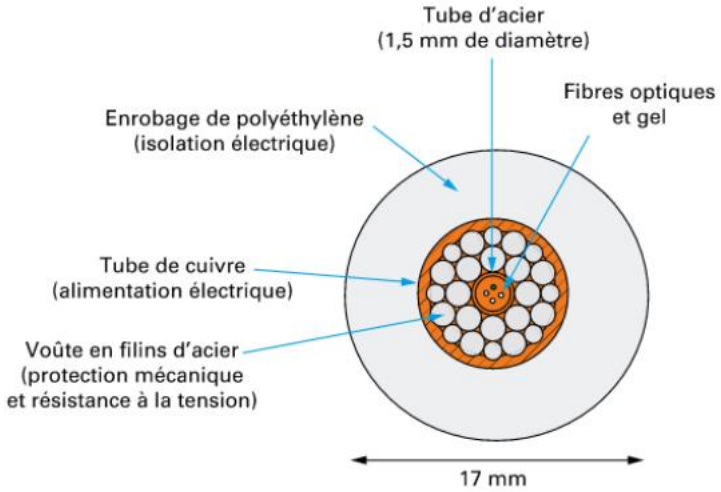
Un connecteur à fibre optique termine l'extrémité d'un câble à fibre optique.
Un connecteur optique est constitué d'un raccord et de deux fiches.

Les fiches optiques contiennent des férules (de 1,25 ou 2,5 mm) assurant le raccordement et le positionnement des deux extrémités de fibre avec précision. Ces fiches optiques sont raccordées via un raccord qui assure l'alignement.

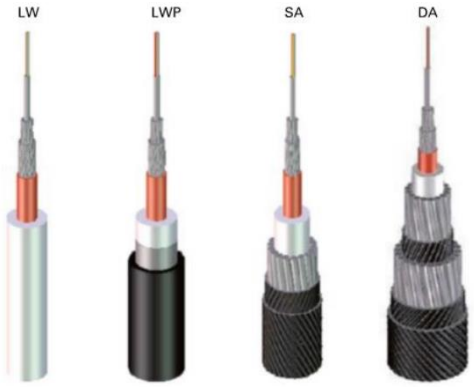
Le montage d'un connecteur sur une extrémité de fibre optique engendre une perte du signal optique, appelée la perte d'insertion (IL).

Une petite partie du signal transmis est également réfléchit par le connecteur directement vers la source lumineuse d'émission, ce qui engendre aussi des pertes (ORL).

CABLES SOUS-MARINS



vue en coupe d'un câble LW



DWDM (DENSE WAVELENGTH DIVISION MULTIPLEXING)

DWDM permet des communications bidirectionnelles sur un même brin. Il est capable de multiplexer jusqu'à 80 canaux de 10 Gbps sur une seule fibre.

PDU (Protocol data Unit) du modèle OSI

données	application
	présentation
	session
segment	transport
paquet	réseau
trame	liaison de données
bit	physique

Normes IEEE dans couches liaisons de donnée et physique

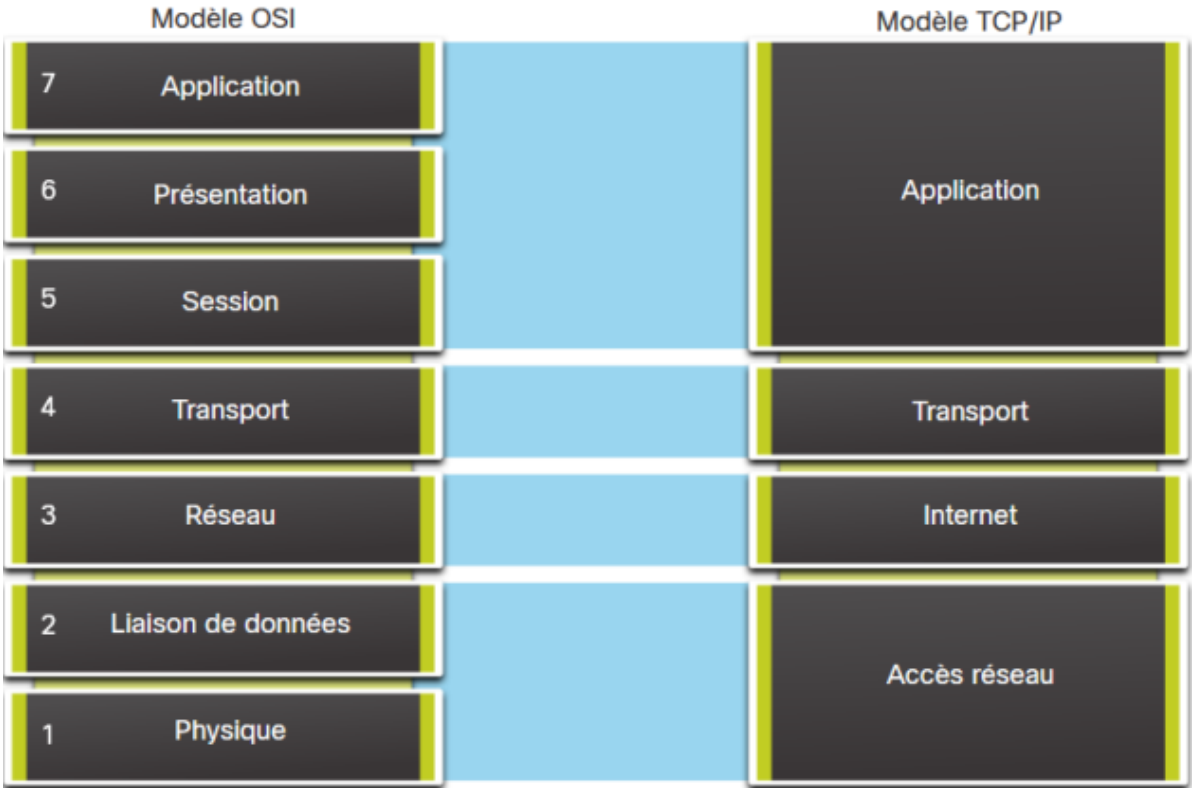
- IEEE 802.11 : Norme WLAN (Wifi)
- IEEE 802.15: Norme Bluetooth
- IEEE 802.16: Norme WiMAX (Worldwide Interoperability for Microwave Access)

Li-Fi

Transmission via le spectre optique (lumière)

Grace à une lumière Led, transfert de Bits 1/0 allumé/éteint

Comparaison OSI – TCP/IP



Organisme de normalisation

Internet society (ISOC)

chargée de promouvoir le développement, l'évolution et l'utilisation ouverte d'Internet dans le monde entier.

Internet Architecture Board (IAB)

S'occupe de la gestion et du développement généraux des normes Internet. Il assure la surveillance des protocoles et des procédures d'architecture utilisés par Internet. Les membres de l'IAB agissent en qualité de personnes privées et ne représentent aucune entreprise, aucune institution ni aucune autre organisation.

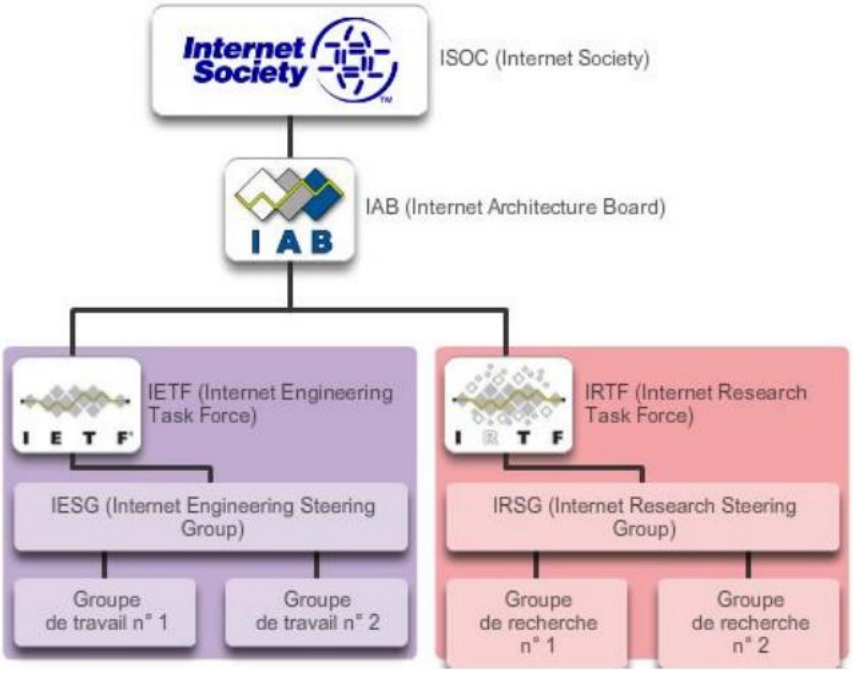
Internet Engineering Task Force (IETF)

A pour but de de développer, de mettre à jour et d'assurer la maintenance d'Internet et les technologies TCP/IP. L'une des principales responsabilités de l'IETF est de produire des documents RFC (Request for Comments), c'est-à dire des notes dérivants les protocoles, les processus et les technologies d'Internet.

Internet Research Task Force (IRTF)

Se concentre sur la recherche à long terme liée à Internet et aux protocoles TCP/IP (contrairement à l'IETF qui s'intéresse surtout aux besoins à court **terme**), aux applications, à l'architecture et aux technologies.

Hiérarchisation de ces organismes



Institute of Electrical and Electronics Engineers (IEEE)

L'IEEE est une association américaine professionnelle s'adressant aux spécialistes du génie électrique et de l'électronique qui souhaitent se consacrer à l'innovation technologique et à la création de normes.

Chaque norme IEEE correspond à un groupe de travail chargé de créer et d'améliorer des normes. Au niveaux des groupes de travail des normes 802, on retrouve notamment :

• 802.1 qui est un groupe de travail sur les protocoles LAN de couche supérieure.

• 802.3 qui est un groupe de travail sur Ethernet. (MAC)

• 802.11 qui est un groupe de travail sur les LAN sans fil (WLAN).

• 802.15 qui est un groupe de travail sur les réseaux personnels sans fil (WPAN)

Organisation internationale de normalisation (ISO)

Il s'agit du plus grand concepteur de normes internationales pour une large gamme de produits et services. ISO n'est pas l'acronyme du nom de l'organisation.

Dans le domaine des réseaux, elle est surtout célèbre pour son modèle de référence OSI (Open Systems Interconnection)

ICANN (Internet Corporation for Assigned Names and Numbers)

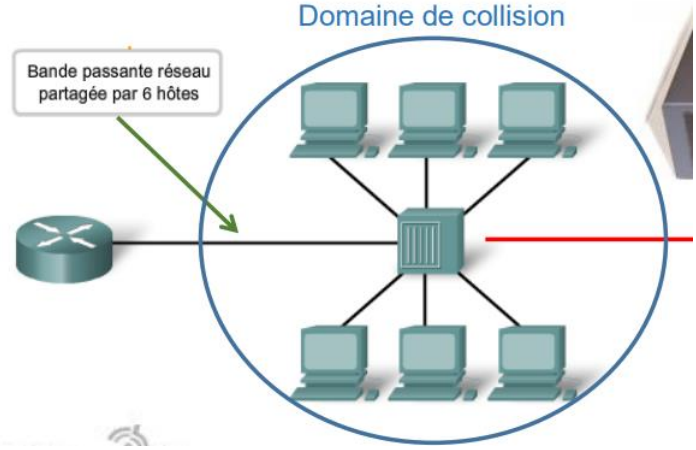
Association à but non lucratif basée aux États-Unis qui coordonne l'attribution des adresses IP, la gestion des noms de domaine utilisés par le protocole DNS et les identificateurs de protocole ou numéros de ports utilisés par les protocoles TCP et UDP. L'ICANN crée des politiques et assume la responsabilité totale de ces attributions.

Accès au réseau, infos complémentaires

- En fin de trame, détection des erreurs
- Partage du réseau..
    - Méthode d'accès basé sur le conflit (non déterministe), les nœuds ne savent pas comment réagir en cas de conflit...
        - Avec une gestion des conflits : Utilisation des CSMA/CD ou CSMA/CA (Carier sense multiple acces)
    - Méthode d'accès contrôlé (déterministe), pas de colissions et débit prévisible
        - Token ring en gros
- Méthode Aloha : années 70, devloppé par l'université d'Hawaï, sur plusieurs îles. Quand on périphérique veut communiquer, il vérifie la disponibilité du support, en attendant un « ACK » qui indique que la demande est prise en compte, s'il y a une collision, pas de ACK
- CSMA est une amélioration de la méthode Aloha, on écoute si il y a une trame émise, si pas de transmission elle envoie, sinon elle attends.
    - CSMA/CD, elle écoute et détecte les collisions.
    - CSMA/CA : Elle évite les colissions
- Protocole PPP : Acheminer des trames entre deux nœuds

Hub (concentrateur)

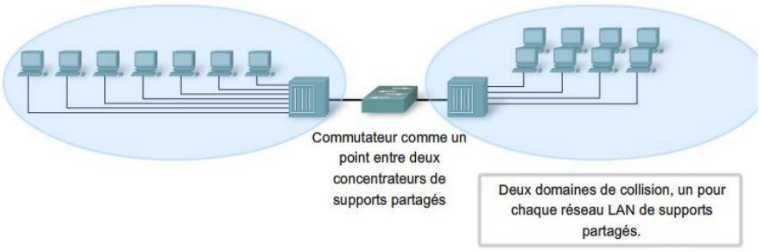
- Utilise la première couche du modèle OSI, possède 4,8,16 ou 32 ports… Renvoie le paquet à tous les périphériques connectés…
- Ces périphériques connectés à un Hub créer ensembles un domaine de collision.



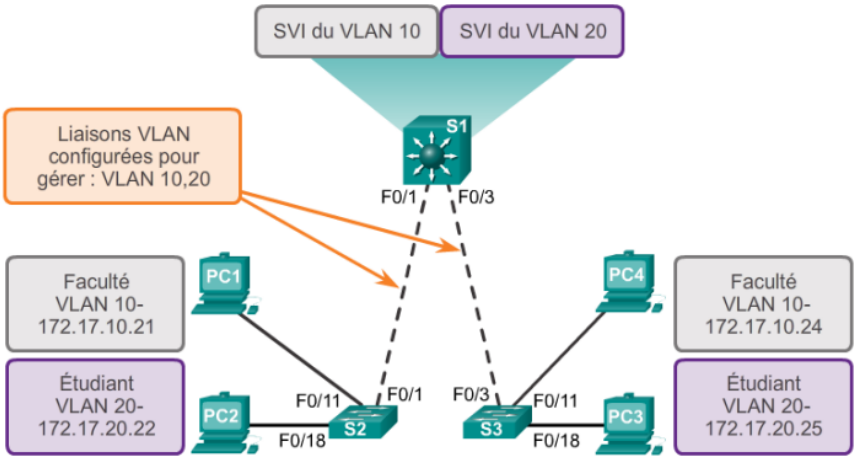
- Probléme d'évolutivité : Les performances sont inversemment proportionelles au nombre de périphériques qui partagent le support… Problème aussi de latence.
- Plus il y a de périphériques dans un domaine de collision, plus le trafique et le risque de collisions augmente.

Switch (Commutateur)

- Relie des réseaux en travaillant avec les deux premières couches du modèle OSI.
- Analyse les trames qui arrivent, filtre en fonction de l'adresse MAC et aiguille les sorites grâce à sa **table de commutation.**
- Chaque port d'un switch est un domaine de collision séparé.



- Permet d'augmenter le débit de données transmises. Donc connexion point à point entre chaque périphérique connecté aux ports du commutateur et celui-ci, avec donc des collisions evitées.
- 3 types de commutateurs (fixes, modulaires et empilables)
- Techologie PoE : fournir une alimentation via le câblage ethenet.
- Technologie EtherChannel : assemblage de plusieurs liens physiques en un lien logique. Pour augmenter la vitesse et tolérance aux pannes entre switch, routeurs, serveurs.
- Commutateur de couche 3 ➔ Utilise aussi les adresses Ip en plus des MAC. Il existe 3 types d'interfaces de couche 3 :
    - SVI : inverface virtuel (Vlan)
    - Port routé : Port phyysiquye de couche 3 d'un switch pour servir de port du routeur
    - Etherchanell couche 3 : Interface d'un périphérique cisco associé à un ensemble de ports routés.



- Configuration :

  Il suffit de configurer les ports routés en faisant passer l'interface en mode de couche 3 à l'aide de la commande de configuration d'interface **no switchport**. Il faut ensuite attribuer une adresse IP au port et activer l'interface.

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
```

Table de commutation

- Fait le lien entre le numéro de port du switch et l'adresse mac d'un périphérique

Exemple de table de commutation

Numéro de port	Adresse MAC
1	00-11-AA-BB-CC-DD
2	00-22-A1-B2-C3-D4

- Pour fonctionner, les commutateurs de couche 2 utilisent 5 fonctions de base…

  ✓ Apprentissage

  Au démarrage, la table est vide, Quand il reçoit une trame, il examine l'adresse source et l'associe avec le port de provenance de cette trame.

  ✓ Horodatage

  Heure d'apprentissage de la première utilisation d'un port

  ✓ Inondation

  Quand le switch ne connait pas le port associé à une adresse mac, il envoit à l'adresse MAC de diffusion (FF FF…) et l'envoie donc à tous les ports. Ensuite il attend la réponde, dont il associe le port d'entrée à l'adresse MAC qu'il ne connaissait pas.

- ✓ Réacheminement sélectif

  Fonction principale d'un switch, permet d'aayser les trames et d'envoyer celle-ci vers le port avec l'adresse de destination correspondante dans sa table de commutation.

- ✓ Filtrage

  Si une trame n'est pas transmise, le switch abandonne celle-ci. De plus certains filtres sont aussi associé avec certaines adresses MAC ou ports, par sécurité pour le réseau.

- *EN GROS : Si le switch ne connait pas l'adresse de destination, il envoie à tous les ports (via l'adresse de diffusion) , et capte la réponse pour l'ajouter à sa table. S'il connait, il transfère et sa table reste inchangée.*

Transmission des trames

- Méthode Store and forward : Il garde les données en mémoire (tampon), quand il a l'ensemble des données il envoie. Quand il recueille les données, il procède un contrôle d'erreur CRC, si pas d'erreur, les données sont transmises, si il y a une erreur il ignore la trame. ➔ Utilisé pour les trames avec un service de priorité importante (ex : VoIp)
- Méthode Cut-through : Il envoie directement les trames même si la transmission n'est pas terminée. Pas de contrôle d'erreur dans la trame… Mais plus rapide que store and forward. Il en existe deux type de cut-through :
  - Fast-Forward : Faible latence, transmission immédiate.
  - Fragment-Free : Stocke les 64 premiers octets de la tramme avant transmission, avec un contrôle de ceux-ci, pour faire un compromis entre la vitesse de transmission et la fiabilité de la trame.
- Pour la mise en mémoire tampon, deux méthodes :
  - Axée sur les ports : fille d'attente liées à des ports, donc une seule trame peut retarder toutes les autres derrières…
  - Partagée : Mémoire tampon partagée à tous les ports, capacité allouée dynamiquement (important pour la communication asymétrique, qui permet l'utilisation de différents débits, sur différents ports.

Routeur

- Equipement de la couche3 du modèle OSI, assurant le routage des paquets.
- Capable d'envoyer des paquets IP et recevoir ceux qui lui sont destinés. En gros c'est bpost, mais en plus fiable et rapide.
- Chaque interface du routeur, est un membre ou hôte d'un réseau IP différent. Donc elles sont toutes configurées avec des adresse IP et masque de sous réseaux différents.

Mémoire

Mémoire	Volatile/Non volatile	Données stockées
Mémoire vive (RAM)	Volatile	• Exécution de l'autotest à la mise sous tension (IOS) • Fichier de configuration en cours • TablesARP et de routageIP • Mémoire tampon de paquets
ROM	Non volatile	• Instructions de démarrage • un logiciel de diagnostic de base; • IOS limitée
NVRAM	Non volatile	• Fichier de configuration initiale
Flash	Non volatile	• IOS • Autres fichiers système

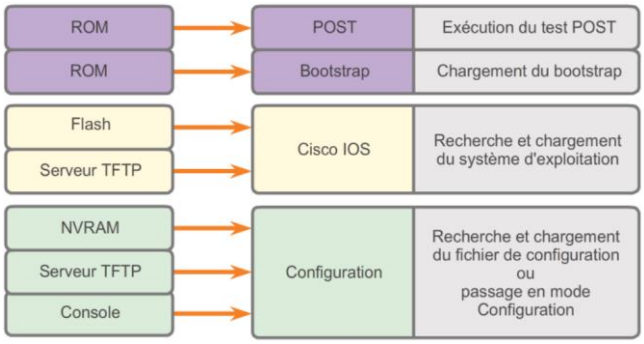
Ports et interface du routeur

- Port de gestion : Console, Aux, utilisé pour la configuration, pas utilisé pour les paquets
- Interfaces LAN et WAN, configurées sur une IP pour transporter le trafic. Interfaces Ethernet = LAN. Interface DSL = WAN.
- On peut accéder à distance au routeur via une connexion SSH ou Telnet, en accédant aux sessions vty. (SSH>Telnet car ssh sécurisé employant un chiffrement)

Démarrage d'un routeur

1) Exécution POST (power-on selft test) qui test automatiquement et diagnostique les composants matériels.
2) Programme d'amorçage (mémoire morte vers mémoire vive) qui charge l'IOS
    a. L'IOS est localisé, soit sur la mémoire flash soit sur un serveur TFTP
3) Localise et charge la configuration initiale depuis la NVRAM

EN GROS :



Routage

Un hôte peut communiquer avec lui-même, un hôte local ou un hôte distant. Si l'hôte est distant, les données sont envoyée à la passerelles par défaut du routeur.

Table de routage

Fichier stocké dans la mémoire vive qui contient les routes sur les réseaux branchés directement au routeur.

Si un paquet n'est pas destiné à une adresse du réseau, il est envoyé au routeur suivant. Jusqu'à l'arrivée du paquet (ou non)

Le nombre de sauts = nombres de routeurs parcouru par le paquet.

La table contient deux éléments :

Les routes directement connectées : interfaces du routeurs, avec l'IP
Les routes distantes : Réseaux distants et autres routeurs.

Fonctionnement général :

1) Le routeur lit l'adresse de destination, et vérifie s'il connait la route.
2) Il transfère le paquet au prochain routeur en fonction du tronçon suivant de la route. Si plusieurs routes possibles, utilisation de la ***métrique*** pour décider de la route. Possibilité de configurer une **route par défaut.**
   Exemple :

```
Gateway of last resort is 192.168.2.2 to network 0.0.0.0
    10.0.0.0/24 is subnetted, 2 subnets
R       10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R       10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.2.2
```

→ Réseaux que connait la table de routage

→ Adresse du tronçon suivant pour les réseaux distants

→ Les réseaux directement connectés n'ont pas d'adresse de tronçon suivant car il n'y a aucun périphérique de couche 3 intermédiaire entre le routeur et ce réseau.

→ Route par défaut

```
D   10.1.1.0/24   [90/2170112]   via   209.165.200.226,   00:00:05,   Serial0/0/0
```

- indique comment le réseau a été découvert par le routeur.
- indique le réseau de destination.
- indique la distance administrative (fiabilité) de la source de la route.
- indique la distance à parcourir pour atteindre le réseau distant.
- indique l'adresse IP de tronçon suivant permettant d'atteindre le réseau distant.
- indique le temps écoulé depuis la découverte du réseau.
- indique l'interface de sortie du routeur permettant d'atteindre le réseau de destination.

Types de routage

- Statique : Configuration manuelle des routes, chaque routeurs doit connaitre la structure du réseau. Une route par défaut doit être configurée sur chaque sous-réseau.
- Dynamique : Utilise des protocoles de routages pour compléter les tables de routages automatiquement.
  Utilise protocole RIP(Routing Information Protocol), EIGRP(cisco uniquement), OSPF
  Pratique mais surcharge la bande passante du réseau…

Configuration

- Commande Ip Route…

  R1(config)#**ip route** 10.1.1.0 255.255.255.0 209.165.200.226

  Adresse du réseau distant — masque du réseau distant — Adresse du tronçon suivant

- Route par défaut…

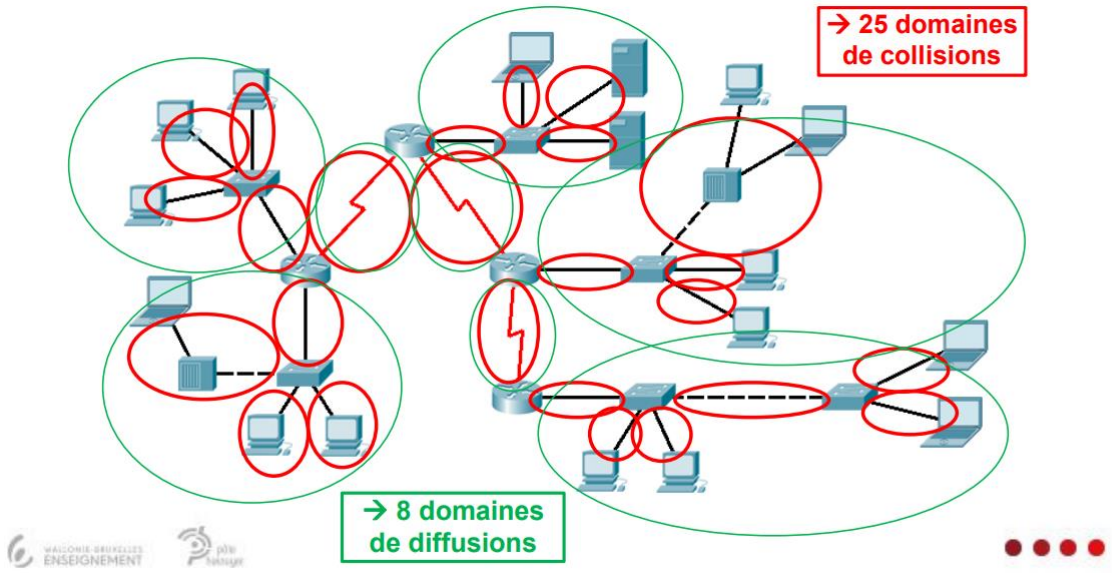
  → R1(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226

Protocole ICMP

- Internet Control Message Protocol, permet de fournir des commentaires sur les problèmes de transmission de paquet ip.
- Messages ICMP…
  1) Accessibilité de l'hôte :
     Utilisation d'un message Echo ICMP. Check si l'hôte répond au écho. Base des pings.
  2) Destination ou service inaccessible
     Permet d'avertir la source d'un message qui ne peut pas être acheminé. Avec des messages qui ont différentes significations…
  3) Délai dépassé
     Quand le champ TTL (time to live) atteint 0, message de retour. Utilisé par l'outil traceroute.

Domaines de collisions et diffusions

- Domaine de collision : région du réseau où les hôtes partagent l'accès au média
- Domaine de diffusion : zone logique où un périphérique connecté peut directement transmettre aux autres du même domaine, sans passer par un routeur.
- Règles pour la division :
  - Tous les ports d'un switch = domaines de colissions différents
  - Tous les périphériques connectés à un hub = un domaine de collision
  - Tous les ports d'un routeur = domaines de diffusions



Adressage IP

IPv4

Division ID

IPv4 est codé sur 32bits (4 octets de 8 bits)

- Binaire : xxxx xxxx . xxxx xxxx . xxxx xxxx . xxxx xxxx
- Décimale : xxx.xxx.xxx.xxx (xxx = 0-255)

ID réseau (netID) = L'adresse réseau qui ne bouge pas, référence pour l'appartenance à un réseau)

ID hôte (hostID) = Adresse du périphérique appartenant au réseau

Classes IP

- Classe A :
  netID = 8 premiers bits (/8) commençant par 0 (jusque 127)
  0xxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
- Classe B :
  NetID = 16 premiers bits (/16) commençant par 10 (de 128 à 191)
  10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
- Classe C :
  NetID = 24 premiers bits (/24) commençant par 110 (de 192 à 223)
  110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx
- Classe D :

  Les 32bits sont l'ID résea, adresse multicast (multidiffusion)

  Exemple , vidéoconférence

- Classe E : Utilisation future

Adresse privées

- 10.0.0.0 à 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 à 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 à 192.168.255.255 (192.168.0.0/16)

Types d'adresses

- Adresse réseau (AR) : Premiere adresse du réseau , identité de celui-ci
- Adresse de diffusion (Broadcast) : Dernière adresse du réseau, vers tous les hôtes du réseau
- Adresse de bouclage : 127.0.0.1 (diriger le trafic vers l'hôte même)
- Adresse Link-local : APIPA (Automatic Private IP Addressing)
- Monodiffusion (Unicast) : Un hôte à un autre
- Multidiffusion (Multicast) : Envoyer à plusieurs hôtes en même réseau

Masque de sous-réseau variable

Pour mieux adapter le nombre d'adresse du hostID par rapport au nombre de périphériques utilisés.

⇨ /x (x= nombre de bits en partant de la gauche qui ne bougent pas, valant la partie netID)

Calcul IPv4

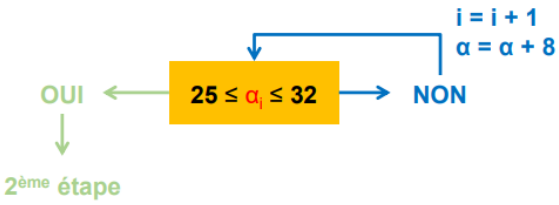
/n	Nbre hôtes
32	1
31	2
30	4
29	8
28	16
27	32
26	64
25	128
α_i	Q_i

Pour appliquer cette méthode, il suffit de connaître le tableau (ici à gauche) et puis de suivre 5 étapes :

Exemple précédent : IP_i = 192.168.10.93 /28

i = 3 2 1 0 α_i

1ère étape : Initialisation → on démarre à **i = 0**



29

/n	Nbre hôtes
32	1
31	2
30	4
29	8
28	16
27	32
26	64
25	128
α_i	Q_i

2ème étape : on regarde dans le tableau
$Q_i = f(\alpha)$

3ème étape : on trouve l'adresse réseau (**AR**)
$AR = PGM(Q_i) \leq IP_i$

4ème étape : on trouve l'adresse réseau suivant (**ARS**)
$ARS = AR + Q_i$

5ème étape : on trouve l'adresse de broadcast (**BC**)
BC = ARS - 1

Problème

Manque d'adresse publiques pour toute la planète, donc besoin de solutions :

- NAT : Conversion des adresses privées ipv4 en publique
- créer un nouveau type d'adresse (IPv6) car la toile internet évolue beaucoup

IPv6

Notation

Sur 128bits, 8 groupes de 2octets écrits en hexadécimal, séparés par des « : »

Exemple : 2A01:EF35:2421:4BE0:CDBC:C04E:A7AB:ECF3

Couche de sous réseau = « longueur de préfixe » = 64bits = /64
Donc netID=64 hostID = 64

Ecriture simplifiée

- Les zéros à gauche de chaque groupes peuvent être retirés (ex : 01AB = 1AB)
- Les groupements de « 0000 » peuvent être remplacés par « :: » une seule fois dans l'adresses, comprenant le plus possible de groupements de « 0000 » à la fois pour optimiser la longueur (ex : 0000 : 0000 : 01AB : 0000 : 0001 : 5489 : AF12 : 0000 ➔ :: 1AB : 0 : 1 : 5489 : AF12 : 0)

Types d'adresses IPv6

- Monodiffusion (toutes les adresses IPv6 sont uniques)
- Multidiffusion (envoyer vers plusieurs destinataires)
- Anycast (Adresse monodiffusion qui peut être adressé à plusieurs hôtes, paquet acheminé vers le plus proche)
- PAS D'ADRESSE DE DIFFUSION (Broadcast), mais équiavlent avec une multidiffusion globalisée

Adresses publiques

Adresse de monodiffusion globale, comme avec IPv4 sauf que pas besoin de NAT car beaucoup d'adresse IPv6, attribuées soit dynamiquement soit statique

Attribué par L'ICANN, uniquement les 2000::/3 = 1/8eme de l'espace disponible

Une adresse de monodiffusion globale se compose de trois parties :

- **Préfixe de routage global** 48
- **ID de sous-réseau** 16
- **ID d'interface** 64

Le ***préfixe de routage global*** est le préfixe ou la partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un FAI) à un client ou à un site. Pour le moment, le préfixe global de routage attribué aux clients est /48. Ces clients incluent tous les clients potentiels, des réseaux d'entreprise aux réseaux particuliers. Cet espace d'adressage est plus que suffisant pour la plupart des clients.

L'***ID de sous-réseau*** est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site.

L'***ID d'interface IPv6*** est similaire à la partie hôte d'une adresse IPv4. Le terme ID d'interface est utilisé car un hôte unique peut avoir plusieurs interfaces, chacune dotée d'une ou de plusieurs adresses IPv6.

Découpage Réseaux

- Sous diviser le réseau, ajout de niveaux de hiérarchies.
  ➔ Réseau / sous réseau / hôte
- On ajoute donc un « sous réseau » qui est un réseau plus petit au sein d'un réseau hiérarchiquement supérieur
- Faciliter l'acheminement les paquet, réduire le trafic sur le réseau global
- Réseau plat = un seul réseau (pas de sous réseaux)
- Comment segmenter ?
  - Optimisation en fonction du nombre d'hôte à attribuer dans le sous réseaux
    ➔ Combien d'adresse à attribuer
  - Eviter les doublons d'adresses (adresses uniques)
  - Contrôler les accès
  - Sécurité et performances du réseau
  - règles de base :
    - Imprimantes : adresse fixe
    - Utilisateurs : DHCP
    - Routeur : adresse fixe (dernière adresse disponible du sous réseaux = passerelle par défaut)
    - Toujours commencer par les plages de sous réseaux les plus grandes vers les plus petites
- Communication entre sous réseaux :
  - Via l'utilisation des routeurs
- Découpage :
  1) Vérifier le nombre d'hôte disponibles dans le réseau globale
  2) Calculer les masques de sous réseaux le plus proche du nombre d'adresse disponibles à attribuer (ex : 550 hôtes on fait un masque en /22
  3) On commence le premier sous réseau au début de l'adresse réseau global
     Avec 3 sous réseaux (550 / 130 / 10 hôtes)
     Exemple : AR = 192.168.160.0 / 19
     Première adresse de sous réseau : 192.168.160.0 /22
     Deuxième adresse de sous réseau : 192 168. 164. 0 /24
     Troisième adresse de sous réseau : 192.168.165.0 / 28

Imaginons, on ajoute un sous réseau pour 120 hôtes.
Adresse du quatrième sous réseau ➔
192.168.165.128 /25
(Car en /25 le PGMC de 128 est 128 (0 faisant partie du troisième sous réseau, on perd donc moins d'adresses que si l'on prenait 192.168.166.0.../25)

Sécurité du réseau

Menaces

1) Vol d'informations
2) Perte et manipulation de données
3) Usurpation d'identité
4) Interruption du service

Vulnérabilités

1) Technologique (faiblesses des protocoles)
2) Configuration (comptes non sécurisés, etc.)
3) De stratégie (mauvaise politiques de sécurités, surveillances…)

Menaces physiques

1) Matérielles (dommages physiques aux périphériques et supports)
2) Environnementales (températures, humidités)
3) Electriques (pic de tensions, bruits…)
4) Maintenance (mauvaises manipulations)

Menaces « logiciels et autres »

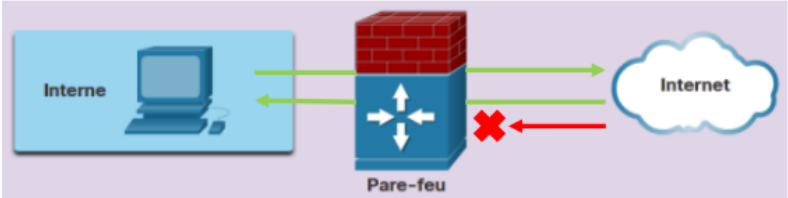
1) Virus (programme malveillant, malware.
2) Vers (Copies fonctionnelles d'eux-mêmes
3) Chevaux de Troie (partie de code qui à l'apparence légitime)

Attaques sur le réseaux…

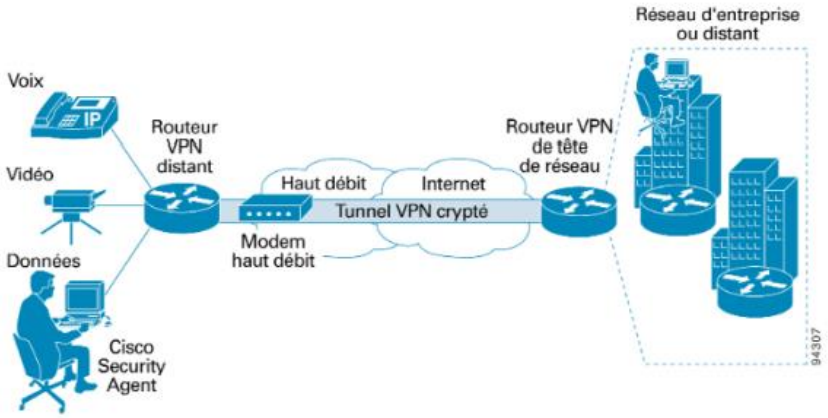
A) De reconnaissance (mappages des systèmes, services et autres)
B) Par accès (manipulation non autorisées des données) (par dictionnaire, force brute, logiciels et enregistreur de frappe, interception de trafics, ingénierie sociale)
C) Déni de service (désactivation ou corruption de réseaux..)

Systèmes de sécurités

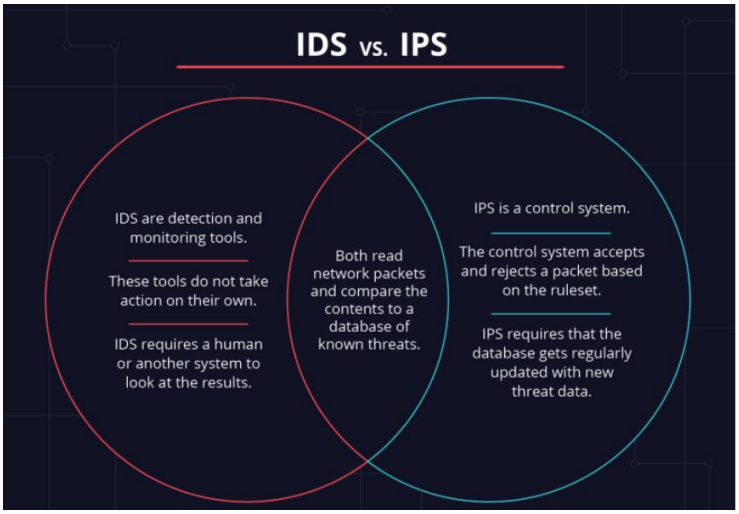
- Pare-feu : Fournir des services garantissant que le trafic peut sortir et revenir, mais le trafic externe ne peux pas arriver en interne.



- Serveur AAA : serveur d' authentification qui contient des données sécurisées.
- Routeur VPN : servir un accès à distance aux utilisateurs, créant un lien direct avec deux ordinateurs distants, en utilisant un tunnel chiffré sécurisé



- Des ESA/WSA : un esa filtre les spams, wsa les malwares connus
- IPS : outils qui surveille le trafic passant, qui recherche des logiciels maveillants.
- IDS / IPS.....



- Sauvegarder ses données.