M103- Concevoir un réseau informatique

Ver : 1.0

Partie I : Maîtriser les notions de base du réseau informatique

1. Identifier les différents types de réseaux

- Description des composants d'un réseau informatique
- Différents types de réseaux
- Topologies réseau et leurs avantages et inconvénients
- Tendances des réseaux (BYOD, Collaboration en ligne, Cloud Computing, Haut débit sans fil)

1.1 Connecté au monde entier

A. Les réseaux aujourd'hui Facilitent :

- **L'apprentissage :**
- **La communication :** SMS ; Réseaux sociaux ; Outils de collaboration ; Blogs ; Wikis ; Podcast
- **Notre travail :** Les réseaux de données ont évolué pour nous aider à faciliter notre travail. Les formations en ligne à titre d'exemple.
- **Le divertissement** : Nous écoutons de la musique, regardons des films, lisons des livres et téléchargeons des éléments à consulter ultérieurement hors connexion. Les réseaux permettent de profiter de jeux en ligne qui n'auraient pas pu exister il y a 20 ans.

B. Les tailles des réseaux :

- **Les petits réseaux domestiques** : connectent plusieurs ordinateurs entre eux, ainsi qu'à Internet
- **Petits bureaux/bureaux à domicile :** permet à l'ordinateur au sein d'un bureau à domicile ou d'un bureau distant de se connecter à un réseau d'entreprise
- **Moyens et grands réseaux :** plusieurs emplacements où des centaines, voire des milliers d'ordinateurs sont reliés
- **Réseaux mondiaux :** relie des centaines de millions d'ordinateurs dans le monde, par exemple Internet.

C. Architecture des réseaux :

i. Clients et serveurs

- **Chaque ordinateur connecté à un réseau est appelé hôte ou périphérique final.**
- **Les serveurs *sont des ordinateurs qui fournissent des informations aux périphériques finaux sur le réseau*.** Par exemple, les serveurs de messagerie, les serveurs web ou les serveurs de fichiers
- **Les clients** sont des ordinateurs qui envoient des requêtes aux serveurs pour récupérer des informations comme une page web à partir d'un serveur web ou un e-mail à partir d'un serveur de messagerie.

ii. Peer-to-Peer (P2P)

- **Le logiciel client et le logiciel serveur sont généralement exécutés sur des ordinateurs distincts.** Toutefois, dans les petites entreprises ou chez les particuliers, il est typique pour un client de faire également office de serveur. Ces réseaux sont appelés des réseaux peer to peer.
- **Les avantages** des réseaux peer to peer : faciles à configurer, plus simples, moins onéreux.
- **Les inconvénients** : aucune administration centralisée, pas aussi sécurisés, pas évolutifs, des performances ralenties.

1.2 Réseaux locaux, réseaux étendus et Internet

A. Composants réseau

- **Un réseau peut être aussi simple que la connexion entre deux ordinateurs via un seul câble ou aussi complexe qu'une collection de réseaux parcourant le globe terrestre.**

- L'infrastructure de réseau comprend trois grandes catégories de composants réseau :
  - **Appareils**
  - **Supports**
  - **Services**

i. Terminaux (Equipements Finaux) :

- ***Un périphérique final*** correspond à l'équipement d'où provient un message ou d'où il est reçu.
- Les données proviennent d'un périphérique final, traversent le réseau et arrivent sur un périphérique final

ii. Périphériques réseaux intermédiaires

- **Un périphérique intermédiaire connecte entre eux les périphériques finaux dans un réseau.**

Voici quelques exemples : **les commutateurs, points d'accès sans fil, routeurs et pare-feu.**

- La gestion des données lors de leur passage à travers un réseau constitue également le rôle du périphérique intermédiaire, notamment :
  - **Régénérer et retransmettre des signaux de données.**
  - **Gérer des informations indiquant les chemins qui existent à travers le réseau et l'interréseau.**
  - **Indiquer aux autres périphériques les erreurs et les échecs de communication.**

iii. Supports Réseau :

La communication à travers un réseau s'effectue sur un support (média) qui permet à un message de se déplacer depuis la source vers la destination.

- Les réseaux utilisent généralement trois types de supports :
  - **Fils métalliques dans des câbles, comme le cuivre**
  - **Verre, tels que les câbles à fibre optique**
  - **Transmission sans fil**

B. Types de réseaux :

- Les deux types de réseaux les plus courants :
  - **Réseau local (LAN)** – s'étend sur une petite zone géographique détenue ou gérée par un individu ou un service IT.
  - **Réseau étendu (WAN)** – s'étend sur une large zone géographique, généralement impliquant un prestataire de services.
  - Autres types de réseau :
    - Réseau métropolitain (MAN)
    - Réseau local sans fil. (WLAN)
    - Storage Area Network (SAN)
    - Personnal Area Network (PAN)

i. LAN :

- Trois caractéristiques des réseaux locaux :
  - **S'étend sur une petite zone géographique** telle qu'une maison, une école, un immeuble de bureaux ou un campus.
  - **Généralement géré par une seule entreprise ou une seule personne.**
  - **Fournit une bande passante très élevée aux périphériques finaux et aux périphériques intermédiaires au sein du réseau.**

ii. WAN : Réseau Etendu

- Trois caractéristiques des réseaux étendus :
  - **Les WAN relient des LAN sur des zones étendues couvrant des villes, des états ou des pays.**
  - **Habituellement géré par plusieurs prestataires de services.**
  - **Les réseaux WAN fournissent généralement des liaisons à plus bas débit entre les réseaux locaux.**

iii. Internet

- **Internet est un ensemble de réseaux locaux et étendus interconnectés à l'échelle internationale.**
- Les réseaux locaux sont connectés entre eux par le biais des réseaux étendus.
- Les réseaux étendus sont ensuite connectés les uns aux autres à l'aide de fils de cuivre, de câbles de fibre optique ou de transmissions sans fil.

- Internet n'appartient pas à une personne ou à un groupe en particulier, toutefois, les groupes suivants ont été développés pour aider à maintenir la structure :
  - **IETF**
  - **ICANN**
  - **IAB …**

C. Connexions Internet

i. Connexions Internet des bureaux à domicile et des petits bureaux

- **Câble** : bande passante élevée, toujours disponible, connexion Internet proposée par les fournisseurs de services de télévision par câble.
- **DSL** : bande passante élevée, toujours disponible, connexion Internet qui utilise une ligne téléphonique.
- **Cellulaire** : utilise un réseau de téléphonie mobile pour se connecter à Internet ; uniquement disponible dans les endroits où il est possible de capter un signal cellulaire.
- **Satellite** : un avantage majeur pour les zones rurales dépourvues de fournisseurs d'accès à Internet.
- **Ligne commutée** : une option peu coûteuse et à faible bande passante utilisant un modem.

ii. Connexions Internet d'entreprise

Les connexions commerciales d'entreprises peuvent nécessiter une bande passante plus élevée, des connexions dédiées ou des services gérés. Options de connexion typiques pour les entreprises :

- **Lignes louées** : des circuits dédiés appartenant au réseau du fournisseur d'accès qui relient des bureaux distants avec la transmission de données et/ou de communications vocales privées.
- **WAN Ethernet** : étend la technologie d'accès des réseaux LAN au réseau étendu**.(Metro Ethernet)**
- **DSL :** la DSL d'entreprise est disponible dans divers

D. Représentations Réseaux :

- **Les schémas de réseaux, souvent appelés diagrammes de topologie,** utilisent des symboles pour représenter les périphériques au sein du réseau.
- **Diagrammes de topologie physique** : indiquent l'emplacement physique des périphériques intermédiaires et des câbles.
- **Diagrammes de topologie logique** : identifient les périphériques, les ports, et le schéma d'adressage.

i. La topologie en bus

- **Perspective physique :** Tous les hôtes sont connectés directement à une liaison
- **Perspective logique :** Tous les hôtes voient tous les signaux provenant de tous les autres équipements

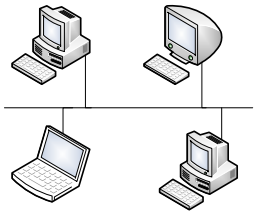


Figure 1 : La topologie en bus

ii. La topologie en anneau

- **Perspective physique :** Les éléments sont chaînés dans un anneau fermé
- **Perspective logique :** Chaque hôte communique avec ses voisins pour véhiculer l'information

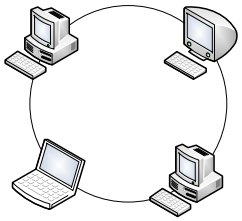


Figure 2: La topologie en anneau

iii. La topologie en étoile

- **Perspective physique :** Cette topologie comporte un nœud central d'où partent toutes les liaisons avec les autres nœuds.
- **Perspective logique :** Toutes les informations passent par un seul équipement, par exemple un concentrateur

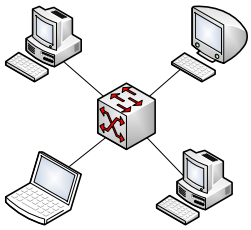


Figure 3: La topologie en étoile

iv. La topologie en étoile étendue

Cette topologie est identique à la topologie en étoile si ce n'est que chaque nœud connecté au nœud central est également le centre d'une autre étoile.

v. La topologie hiérarchique

- **Perspective physique :** Cette topologie ressemble à une topologie en étoile sauf qu'elle n'utilise pas de nœud central. Elle utilise un nœud de jonction à partir duquel elle se branche vers d'autres nœuds.
- **Perspective logique :** Le flux d'informations est hiérarchique

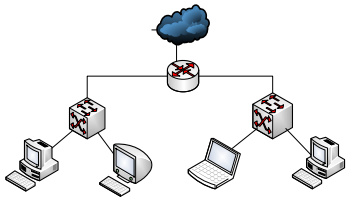


Figure 4: La topologie hiérarchique

vi. La topologie complète (maillée)

- **Perspective physique :** Chaque nœud est connecté avec tous les autres
- **Perspective logique :** Dépend des équipements utilisés

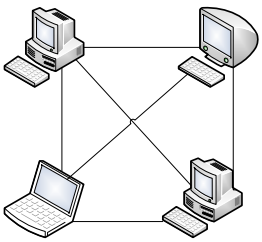


Figure 5: La topologie complète (maillée)

1.3 L'environnement réseau changeant

A. Tendances relatives aux réseaux

Le rôle du réseau doit s'adapter et se transformer continuellement afin de pouvoir suivre l'évolution des nouvelles technologies et des nouveaux périphériques qui arrivent constamment sur le marché.

Plusieurs nouvelles tendances relatives au réseau vont affecter les entreprises et les consommateurs :

- **BYOD**
- **Collaboration en ligne**
- **Communications vidéo**
- **Cloud computing**

i. BYOD

- **Bring Your Own Device (BYOD) est une tendance mondiale majeure qui permet aux utilisateurs d'utiliser leurs propres appareils en leur offrant plus de possibilités et une plus grande flexibilité.**
- BYOD permet aux utilisateurs finaux d'accéder à leurs informations et de communiquer en utilisant leurs :
  - Ordinateurs portables
  - Netbooks
  - Tablette
  - Smartphones

ii. Collaboration en ligne

- Les utilisateurs individuels souhaitent collaborer et travailler avec d'autres sur le réseau dans le cadre de projets communs.
- Les outils de collaboration, y compris Cisco Webex, illustré dans la figure ci-contre, permettent aux utilisateurs de se connecter instantanément, d'interagir et d'atteindre leurs objectifs.
- **La collaboration est une priorité pour les entreprises et le secteur de l'éducation.**

iii. Communication vidéo

- **Cisco TelePresence** offre une nouvelle façon de travailler, où tout le monde, quel que soit son lieu devient plus productif grâce à la collaboration face à face.
- Chaque jour, partout dans le monde, nous transformons les entreprises en transformant l'expérience de nos clients.

iv. Cloud computing

- **Le cloud computing est une tendance globale qui nous permet de stocker des fichiers personnels ou de sauvegarder nos données sur des serveurs via Internet.**
- **Des applications telles que le traitement de texte et la retouche photo peuvent également être accessibles par le biais du cloud.**
- **Le cloud computing permet également aux entreprises d'étendre leurs capacités à la demande et de les transmettre automatiquement à n'importe quel périphérique dans le monde entier.**
- **Le cloud computing fonctionne grâce aux data centers.** Les petites entreprises qui n'ont pas les moyens de posséder leurs propres data centers louent des serveurs et des services de stockage auprès de grandes entreprises de data centers dans le cloud.

2. A.2. Connaître les réseaux locaux (LAN)

- Différentes versions d'Ethernet
- Adresse MAC Ethernet
- Méthodes de transmission et vitesse de commutation
- Introduction aux réseaux sans fil (802.11x)

La couche physique

Types de connexions

Avant que les communications réseau puissent avoir lieu, une connexion physique à un réseau local doit être établie.

Une connexion physique peut être une **connexion filaire par câble** ou **une connexion sans fil** passant par les ondes radio.

Support de transmission de la couche physique

Trois formes élémentaires de support réseau

- **Signaux électriques : Câble en cuivre**
- **Impulsion lumineuse : Cable à fibre optique**
- **Signaux hyperfréquence : Sans fil**

Caractéristiques de couche physique

Fonctions

- Codage : Une méthode permettant de convertir un flux de bits de données en code prédéfini".
- Méthode de signalisation : Méthode de représentation des bits.

Bande passante

- La capacité d'un support à transmettre des données.
- La bande passante numérique mesure la quantité d'informations pouvant circuler d'un emplacement à un autre pendant une période donnée.
- La bande passante est parfois considérée comme la vitesse à laquelle voyagent les bits, mais cette vision n'est pas exacte. En 10 Mbit/s et en 100 Mbit/s Ethernet, les bits sont envoyés à la vitesse de l'électricité. La différence correspond au nombre de bits transmis par seconde.

Unité de bande passante	Abréviation	Equivalence
Bits par seconde	bit/s	1b/s
Kilobits par seconde	Kb/s	1kb/s=1000b/s
Mégabits par seconde	Mb/s	1Mb/s=1000 000 b/s

Débit

- Mesure du transfert de bits pendant une période donnée.
- Ne correspond généralement pas à la bande passante spécifiée dans les mises en œuvre de couche physique.
  - Quantité de trafic
  - Type de trafic
  - Latence créée par les périphériques réseau rencontrés entre la source et la destination
- Le **débit applicatif** correspond donc au débit moins la surcharge de trafic pour l'établissement de sessions, les accusés de réception et l'encapsulation.

▪ Supports de transmission

Câblage en cuivre

Caractéristiques des supports de transmission en cuivre

Transmises sur les câbles en cuivre sous forme d'impulsions électriques.

Atténuation : plus le signal voyage longtemps, plus il se détériore.

Tous les supports en cuivre doivent respecter des limites de distance strictes.

Interférences électromagnétiques (EMI) ou interférences radioélectriques (RFI) : déforment et détériorent les signaux de données transportés par les supports en cuivre.

Pour les contrer, les câbles de cuivre sont enveloppés d'un blindage.

Diaphonie : perturbation causée par les champs électriques ou magnétiques d'un signal dans un câble sur le signal traversant le câble adjacent.

Pour annuler la diaphonie, les paires de fils du circuit opposé sont torsadées ensemble.

Supports de transmission en cuivre

Trois principaux types de supports en cuivre sont utilisés dans les réseaux :

- **UTP** : Câble à paires torsadés non blindées
- **STP** : Câble à paires torsadés blindées
- **Câble coaxial**

Câble à paires torsadées non blindé (UTP)

- Le câblage à paires torsadées non blindé (UTP) est le support réseau le plus courant.
    - Il se termine par des connecteurs RJ-45.
    - Il est utilisé pour relier des hôtes réseau à des périphériques réseau, tels que des commutateurs.
    - Il se compose de quatre paires de fils à code de couleur qui ont été torsadés ensemble et qui permettent de limiter les interférences causées par les signaux d'autres fils.
    - Les codes couleur facilitent le raccordement des câbles.

Câble à paires torsadées blindées (STP)

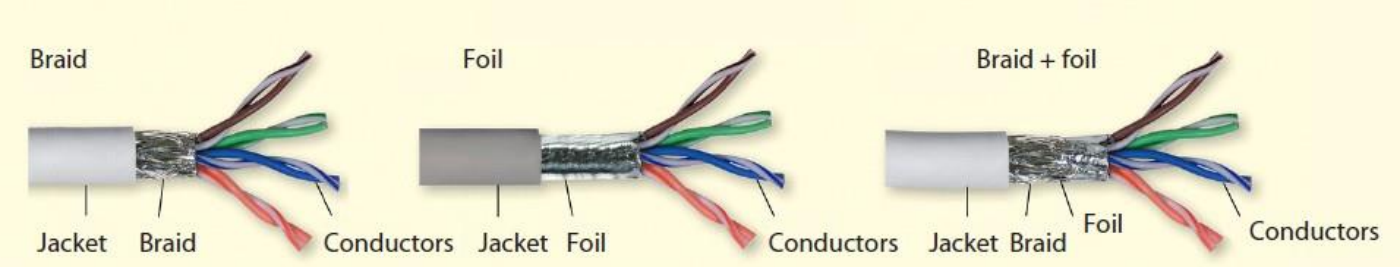
- Le STP offre une meilleure protection contre les parasites que les câbles UTP.
- Le câblage STP est bien plus onéreux et plus difficile à installer que les câbles UTP.
- Allie les techniques de blindage pour contrer les interférences électromagnétiques et radioélectriques, et les torsades pour éviter la diaphonie.
- Utilise quatre paires de fils, chacune enveloppée dans une feuille de blindage. Le tout est ensuite entouré dans une torsade ou une feuille métallique.

Câble coaxial

- Le câble coaxial est composé des éléments suivants :
    - Un conducteur en cuivre utilisé pour transmettre les signaux électroniques.
    - Un conducteur en cuivre entouré d'une couche de matériau isolant flexible en plastique.
    - Sur ce matériau isolant, une torsade de cuivre ou une feuille métallique constitue le second fil du circuit et fait office de protection pour le conducteur intérieur.
    - Le câble dans son entier est ensuite entouré d'une gaine afin d'empêcher tout dégât matériel mineur.
- Les câbles UTP ont pratiquement remplacé les câbles coaxiaux dans les installations Ethernet modernes, mais ils utilisés aux fins suivantes :
    - Installations sans fil : les câbles coaxiaux relient les antennes aux périphériques sans fil.
    - Installations de câbles Internet

Les câbles à paires torsadés :

- Le câblage UTP respecte les normes établies par la Telecommunications Industry Association (TIA) et l'Electronic Industries Association (EIA).
- La norme TIA/EIA-568 définit le câblage pour les installations de réseau local



Catégorie	Classe	Fréquence max.
Cat 5	UTP	100BASE-TX, 1000BASE-T
Cat 5e	UTP, F/UTP, U/FTP	1000BASE-T, 2.5GBASE-T
Cat 6	UTP F/UTP, U/FTP	5GBASE-T, 10GBASE-T

Connecteurs RJ45

La norme TIA/EIA-568 décrit la correspondance des codes couleur des fils avec les broches (brochage) pour les câbles Ethernet.

Types de câble Paire torsadé :

Type de câble	Standard	Application
Droit (Straight)	**T568A aux 2 extrémités ou T568B**	Connecte un hôte à un périphérique réseau (Commutateur)
Croisé (Cross-over)	**Une extrémité T568A et l'autre T568B**	Connecte 2 hôtes Connecte 2 périphériques réseau intermédiaires de même type.

	1	2	3	4	5	6	7	8
568A	BLANC-VERT	VERT	BLANC-ORANGE	BLEU	BLANC-BLEU	ORANGE	BLANC-MARRON	MARRON
568	BLANC-ORANGE	ORANGE	BLANC-VERT	BLEU	BLANC-BLEU	VERT	BLANC-MARRON	MARRON

Câblage en fibre optique

Propriétés du câblage en fibre optique

- Actuellement, les câbles à fibre optique sont utilisés dans quatre domaines d'application :
  - Réseaux d'entreprise
  - FTTH (Fiber-to-the-home)
  - Réseaux longue distance
  - Réseaux sous-marins
- Transmet les données sur de plus longues distances et avec une bande passante plus large.
- Transmet des signaux avec moins d'atténuation et sont entièrement protégés des perturbations électromagnétiques et radioélectriques.

- Utilisé pour relier des périphériques réseau.
- Un fil en verre très pur et transparent, à la fois flexible et très fin. Son diamètre n'est pas beaucoup plus grand que celui d'un cheveu humain.
- Les bits sont codés sur la fibre sous forme d'impulsions lumineuses.

Types de fibre optique

Type	Monomode (un seul signal lumineux)	Multimode
Cœur	Petit diamètre (9 microns)	Diamètre plus grand (50-60 microns)
Dispersion	Moins de dispersion	Plus de dispersion et donc perte de signal
Distance	Adapté aux applications longue distance	Adapté aux applications longue distance mais plus courte que Monomode.
Source du signal	**Laser**	**LED**

Connecteurs à fibre optique

- La lumière peut uniquement voyager dans une seule direction, deux fibres optiques sont requises pour prendre en charge le fonctionnement en mode duplex intégral.
- La gaine jaune est destinée aux câbles à fibre monomode.
- Orange (ou aqua) pour les câbles à fibre multimode.

Connecteurs ST (Straight-Tip)	L'un des premiers types de connecteur utilisés. Verrouillage en toute sécurité par vissage.
Connecteurs SC (Subscriber Connector)	Appelé connecteur carré ou standard. Utilise un mécanisme d'encliquetage pour assurer une insertion positive. Utilisé avec la fibre multimode et monomode.
Connecteurs LC (Lucent Connector) unidirectionnels	Version plus petite du SC et populaire en raison de sa taille. Connecteurs LC bidirectionnels multimodes Similaire au LC mais avec un connecteur bidirectionnel

Fibre ou cuivre

Problèmes de mise en œuvre	**UTP**	**Fibre Optique**
Bande Passante	10Mb/s – 10 Gb/s	10Mb/s – 100 Gb/s
Distance	Courte (1 à 100 mètres)	Longue (1 à 100 000 mètres)
Résistance aux perturbations	Faible	Haute
Coût des supports et des connecteurs et compétences requises pour l'installation	Moins élevé	Plus élevé

Sans-fil

Propriétés des transmissions sans fil

- Les supports sans fil transportent à l'aide de fréquences radio et micro-ondes des signaux électromagnétiques qui représentent les chiffres binaires des communications de données.
- Contraintes du sans-fil :
  - **Zone de couverture :** des matériaux de construction utilisés dans les bâtiments et structures, ainsi que le terrain local, limitent la couverture.
  - **Interférences :** perturbation par des appareils aussi courants que les éclairages fluorescents, les fours à micro-ondes et d'autres communications sans fil.
  - **Sécurité :** les périphériques et les utilisateurs non autorisés à accéder au réseau peuvent quand même accéder à la transmission.
  - **Support partagé :** un seul périphérique à la fois peut envoyer ou recevoir et le support sans fil est partagé entre tous les utilisateurs sans fil.

Types de transmissions sans fil

- **Wi-Fi : norme IEEE 802.11**
  - Utilise CSMA/CA (Carrier Sense Multiple Access Collision Avoidance)
  - La carte réseau sans fil doit attendre que le canal soit libre.
- **Bluetooth : norme IEEE 802.15**
  - Réseau personnel sans fil (WPAN)
  - Utilise un processus de jumelage de périphériques pour des distances comprises entre 1 et 100 mètres
- **WiMAX : norme IEEE 802.16**
  - Worldwide Interoperability for Microwave Access
  - Accès à large bande sans fil.

LAN sans fil (WLAN)

- Un réseau local sans fil exige les périphériques réseaux suivants :
  - **Point d'accès sans fil** : concentre les signaux sans fil des utilisateurs et se connecte à l'infrastructure réseau en cuivre existante, telle qu'Ethernet.
  - **Adaptateurs de carte réseau sans fil** : fournissent à chaque hôte du réseau la possibilité de communiquer sans fil.

Fonctionnement d'un réseau sans fil (WLAN)

Un WLAN à également besoin, tout comme un LAN, d'un média. Au lieu de câbles à paires torsadées, les WLANs utilisent des fréquences radio à 2,4 GHz et 5 GHz.

En Juin 1997, L'IEEE publie les standards 802.11 pour les réseaux locaux sans fils.

Tableau récapitulatif des fréquences et débits :

	802.11b	802.11a	802.11g	802.11n (4)	802.11ac (5)	802.11ax (6)
Bande de fréquence	2,4 Ghz	5 Ghz	2,4 Ghz	2,4 & 5 Ghz	5 Ghz	5 Ghz
Débit maximum	11 Mbps	54 Mbps	54 Mbps	300 Mbps	7000 Mbps	10 Gbps
Portée (externe)	140m	120m	140m	250 m	300 m	300 m

Les lois de la radio :

- Débit plus grand = Couverture plus faible
- Puissance d'émission élevée = Couverture plus grande mais durée de vie des batteries plus faible
- Fréquences radio élevées = Meilleur débit, couverture plus faible

Contrôle de l'accès aux supports

Contrôle d'accès au support de transmission

- Le contrôle d'accès au support est l'équivalent des règles de trafic régulant l'accès des véhicules à une autoroute.
- L'absence d'un contrôle d'accès au support serait comparable à des véhicules ignorant le trafic et accédant à la route sans se préoccuper des autres véhicules.
- Cependant, toutes les routes et tous les accès ne sont pas identiques. Un véhicule peut accéder à la route en se fondant dans la circulation, en attendant son tour à un stop ou en obéissant à des feux de circulation. Le conducteur suit des règles différentes selon chaque type d'accès à la circulation.

Topologies physiques et logiques

- **Topologie physique** : fait référence aux connexions physiques et identifie la façon dont les terminaux et les appareils d'infrastructure, tels que les routeurs, les commutateurs et les points d'accès sans fil sont interconnectés.
- **Topologie logique** : désigne la manière dont un réseau transfère les trames d'un nœud à l'autre. Ces chemins de signaux logiques sont définis par les protocoles de couche liaison de données.

Modes bidirectionnel simultané et bidirectionnel non simultané

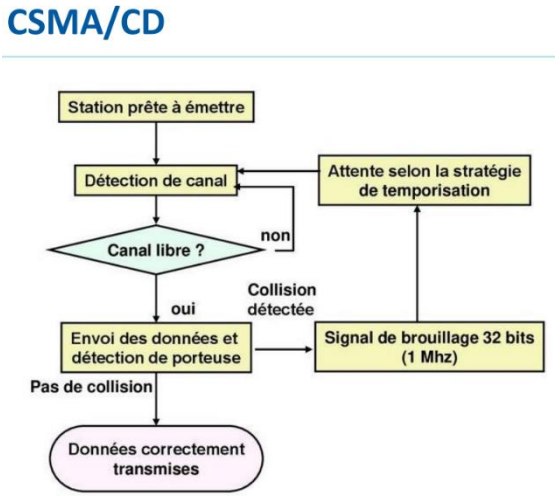
- **Communication bidirectionnelle non simultanée (half duplex)**
  - Les deux périphériques peuvent transmettre et recevoir des données sur les supports, mais pas de façon simultanée.
  - Utilisé dans les anciennes topologies en bus et avec les concentrateurs Ethernet.
  - Les réseaux locaux sans fil fonctionnent eux aussi en mode semi-duplex.
- **Communication bidirectionnelle simultanée (duplex intégral) (Full Duplex)**
  - Les deux périphériques peuvent simultanément transmettre et recevoir des données sur les supports.
  - La couche liaison de données considère que les supports sont à tout moment disponibles pour les deux nœuds en vue d'une transmission de données.
  - Par défaut, les commutateurs Ethernet fonctionnent en mode duplex intégral, mais ils peuvent adopter le mode semi-duplex s'ils se connectent à un périphérique comme un concentrateur Ethernet.

Méthodes de contrôle d'accès aux supports

- Accès avec gestion des conflits
  - Les nœuds fonctionnent eux aussi en mode semi-duplex.
  - En concurrence pour utiliser le support.
  - Un seul périphérique à la fois peut envoyer des données.
- Accès contrôlé
  - Chaque nœud dispose de son tour pour utiliser le support.
  - Les anciens réseaux locaux Token Ring en sont un exemple.

Accès avec gestion des conflits – CSMA/CD

- Le processus d'accès multiple avec écoute de porteuse et détection de collision (CSMA/CD) est utilisé sur les réseaux locaux Ethernet en mode semi-duplex.
  - Si deux périphériques transmettent en même temps, il se produit une collision.
  - Les deux périphériques détectent la collision sur le réseau.
  - Les données envoyées par les deux périphériques sont corrompues et doivent être envoyées de nouveau.



Accès avec gestion des conflits – CSMA/CA

- **CSMA/CA**
  - Utilise une méthode pour détecter si le support est libre.
  - Ne détecte pas les collisions, mais tente de les éviter en patientant avant d'effectuer la transmission.
- **Remarque** : les réseaux locaux Ethernet qui utilisent des commutateurs n'utilisent pas un système d'accès basé sur le conflit, car le commutateur et la carte réseau hôte fonctionnent en mode duplex intégral.

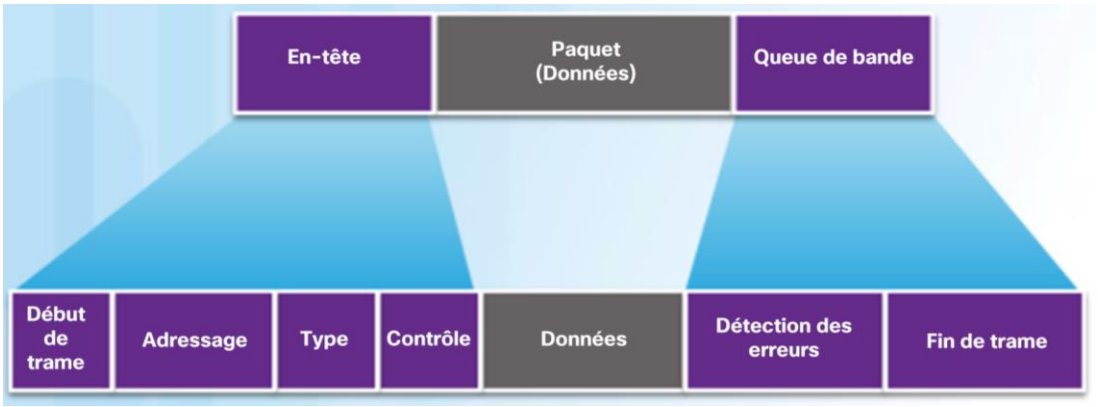
Trame liaison de données

La trame

- Chaque type de trame comprend trois éléments de base :
  - En-tête
  - Données
  - Queue de bande
- La structure de la trame et les champs contenus dans l'en-tête et dans la queue de bande dépendent du protocole de couche 3.

Champs de trame

- **Indicateurs de début et de fin de trame** : identifie les limites de début et de fin de la trame.
- **Adressage** : indique les nœuds source et de destination.
- **Type** : identifie le protocole de couche 3 dans le champ de données.
- **Contrôle** : identifie les services de contrôle de flux spéciaux comme la QoS.
- **Données** : contient les données utiles de la trame (c'est-à-dire l'en-tête de paquet, l'en-tête de segment et les données).



Adresse de couche 2

Chaque trame liaison de données contient l'adresse liaison de données source de la carte réseau qui envoie la trame, et l'adresse liaison de données de destination de la carte réseau qui la reçoit.

Trames LAN et WAN

- Le protocole de couche 2 utilisé pour une topologie dépend de la technologie.
- Les protocoles de couche liaison de données incluent :
  - Ethernet
  - 802.11 sans fil
  - PPP (Point-to-Point Protocol)
  - HDLC
  - Frame Relay

Protocole Ethernet

<table>
<tr><th colspan="2">Couches OSI</th><th></th><th colspan="4">Ethernet</th></tr>
<tr><td rowspan="2">Couche liaison de données</td><td>Sous-couche LLC</td><td rowspan="3"></td><td colspan="4">IEEE 802.2</td></tr>
<tr><td>Sous-couche MAC</td><td>IEEE 802.3</td><td>100BASE-T</td><td>Token Ring / IEEE 802.5</td><td>FDDI</td></tr>
<tr><td colspan="2">Couche Physique</td></tr>
</table>

Encapsulation Ethernet

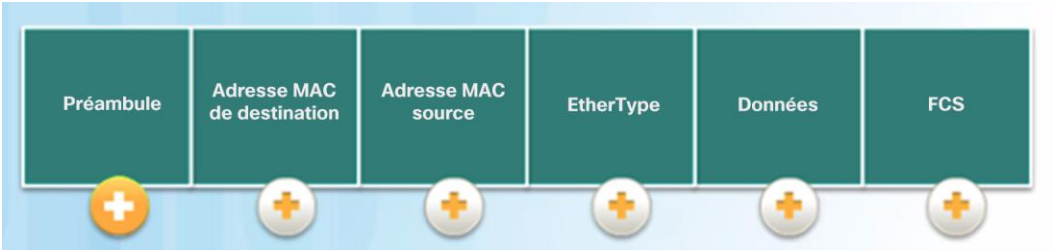
- Ethernet est la technologie LAN la plus répandue aujourd'hui.
  - Définies dans les normes IEEE 802.2 et 802.3.
  - Il prend en charge des bandes passantes de données de 10 Mbit/s, 100 Mbit/s, 1 000 Mbit/s (1 Gbit/s), 10 000 Mbit/s (10 Gbit/s), 40 000 Mbit/s (40 Gbit/s) et 100 000 Mbit/s (100 Gbit/s).
- Il fonctionne au niveau de la couche liaison de données et de la couche physique.
- Ethernet dépend de deux sous-couches distinctes de la couche liaison de données : la sous-couche de contrôle de liaison logique (LLC) et la sous-couche MAC.
- La sous-couche LLC Ethernet gère la communication entre les couches supérieures et les couches inférieures. La mise en œuvre de la sous-couche IT se fait au niveau logiciel et est indépendante du matériel.
- La sous-couche MAC est la sous-couche inférieure de la couche liaison de données. Elle est mise en œuvre au niveau matériel, généralement sur la carte réseau de l'ordinateur.

Évolution d'Ethernet

- Depuis 1973, les normes d'Ethernet se sont développées et spécifient désormais des versions plus rapides et plus flexibles.
- Les versions précédentes d'Ethernet étaient relativement lentes, de l'ordre de 10 Mbit/s.
- Les versions d'Ethernet les plus récentes fonctionnent à 10 gigabits par seconde au minimum.

Champs de trame Ethernet

- La taille minimale des trames Ethernet entre l'adresse MAC de destination et la FCS est de 64 octets et la taille maximale de 1 518 octets.
- Les trames inférieures à 64 octets sont appelées « fragment de collision » ou une « trame incomplète » et sont automatiquement rejetées par les périphériques récepteurs. Les trames de plus de 1 500 octets de données sont considérées comme des trames « jumbo » (géantes) ou « baby giant frames » (légèrement géantes).
- Si la taille d'une trame transmise est inférieure à la taille minimale ou supérieure à la taille maximale, le périphérique récepteur abandonne la trame.

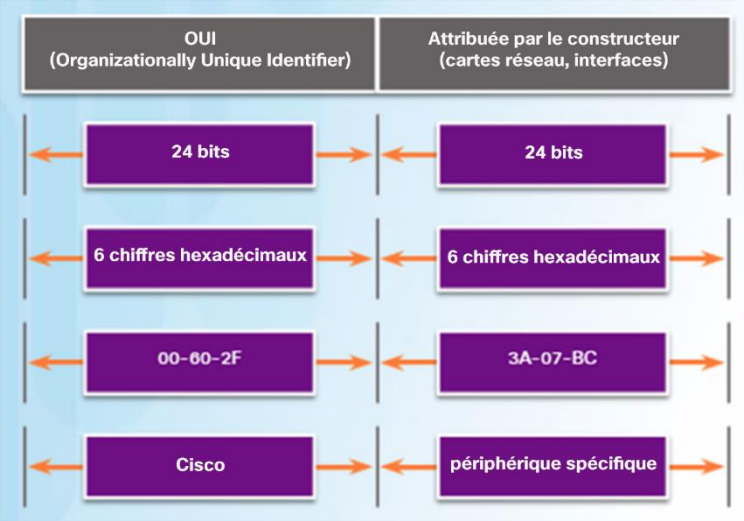


Les adresses MAC Ethernet

Adresses MAC et format hexadécimal

- Une adresse MAC Ethernet est une valeur binaire de 48 bits constituée de 12 chiffres hexadécimaux (4 bits par chiffre hexadécimal).
- Les adresses MAC ont été créées pour identifier la source et la destination réelles.

- Les règles d'adresse MAC sont établies par l'IEEE.
- L'IEEE attribue au constructeur un code de 3 octets (24 bits) appelé OUI (Organizationally Unique Identifier).



- L'IEEE demande aux revendeurs de suivre deux règles simples :
- Toutes les adresses MAC attribuées à une carte réseau ou à un autre périphérique Ethernet doivent utiliser, comme 3 premiers octets, l'identifiant OUI attribué au revendeur correspondant.
- Toutes les adresses MAC ayant le même identifiant OUI doivent utiliser une valeur unique dans les 3 derniers octets.

Traitement des trames

- Selon le périphérique et le système d'exploitation, différentes représentations des adresses MAC s'affichent.

5.2 Commutateurs LAN

La table d'adresses MAC

Notions fondamentales sur les commutateurs

- Les décisions d'un commutateur Ethernet de couche 2 du concernant la transmission de données reposent uniquement sur les adresses MAC Ethernet de couche 2.
- Un commutateur qui est sous tension aura une table d'adresses MAC vide, car il n'a pas encore appris les adresses MAC des quatre PC connectés.
- Remarque : la table d'adresses MAC est parfois appelée table de mémoire associative (CAM).

Apprentissage des adresses MAC

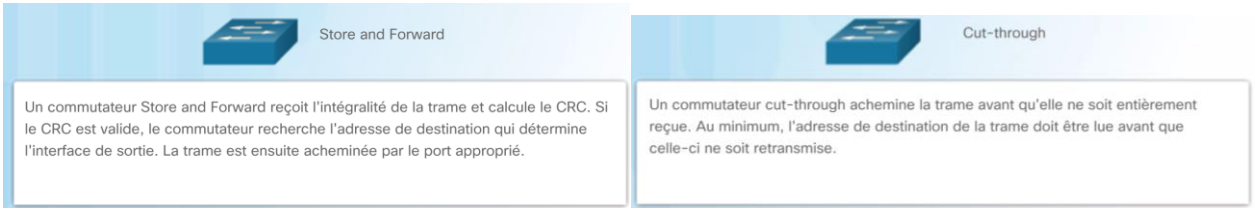
- Le commutateur crée la table d'adresses MAC de manière dynamique. Le processus pour découvrir l'adresse MAC source est le suivant :
  - Les commutateurs examinent toutes les trames entrantes à la recherche de nouvelles informations d'adresse MAC source à apprendre.
  - Si l'adresse MAC source est inconnue, elle est ajoutée à la table, tout comme le numéro du port.
  - Si l'adresse MAC source existe, le commutateur réinitialise le compteur d'obsolescence de cette entrée.
  - Par défaut, la plupart des commutateurs Ethernet conservent les entrées dans la table pendant 5 minutes.
- Le processus pour transférer l'adresse MAC de destination est le suivant :
  - Si l'adresse MAC de destination est une diffusion ou une multidiffusion, la trame est également envoyée sur tous les ports à l'exception du port entrant.
  - Si l'adresse MAC de destination est une adresse de monodiffusion, le commutateur recherche une correspondance dans sa table d'adresses MAC.
  - Si l'adresse MAC de destination se trouve dans la table, le commutateur transfère la trame par le port spécifié.
  - Si l'adresse MAC de destination ne se trouve pas dans la table (par ex., adresse de monodiffusion inconnue), le commutateur transfère la trame sur tous les ports sauf celui d'entrée.

- À mesure qu'un commutateur reçoit des trames de différents périphériques, il remplit sa table d'adresses MAC en examinant l'adresse MAC source de chaque trame.
- Si la table d'adresses MAC du commutateur contient l'adresse MAC de destination, il peut filtrer la trame et la diffuser sur un sol port.

Les méthodes de transmission du commutateur

Méthodes de transmission de trames sur les commutateurs Cisco

- Les commutateurs utilisent l'une des méthodes suivantes de transmission des données entre des ports réseau :



La commutation à la volée (Cut-Through)

- Dans le cas de la commutation cut-through, le commutateur met une quantité juste suffisante de la trame en tampon afin de lire l'adresse MAC de destination et déterminer ainsi le port auquel les données sont à transmettre. Le commutateur ne procède à aucun contrôle d'erreur dans la trame.
- Il existe deux variantes de la commutation cut-through :
    - ce mode de commutation offre le niveau de latence le plus faible. Le commutateur transmet un paquet immédiatement après la lecture de l'adresse de destination. Il s'agit de la forme la plus classique de commutation de bout en bout.
    - La commutation Fragment-Free, dans laquelle le commutateur stocke les 64 premiers octets de la trame avant la transmission. Il s'agit d'un compromis entre la commutation Store and Forward et la commutation Fast-Forward.

Mise en mémoire tampon sur les commutateurs

- Un commutateur Ethernet peut utiliser une technique de mise en mémoire tampon pour stocker des trames avant de les transmettre. La mise en mémoire tampon peut également être une solution lorsque le port de destination est saturé suite à un encombrement et que le commutateur stocke la trame jusqu'à ce qu'il puisse la transmettre.
- Il existe deux types de techniques de mise en mémoire tampon :

Méthode de mise en mémoire tampon	Description
Mémoire axée sur les ports	• Les trames sont stockées dans des files d'attente liées à des ports entrants et sortants spécifiques. • Une trame est transmise lorsque toutes les trames qui la précèdent ont été transmises.
Mémoire partagée	• Toutes les trames sont déposées dans un tampon commun qui est partagé par tous les ports du commutateur.

Paramètres du mode duplex et de vitesse

- Deux types de paramètres bidirectionnels sont employés pour les communications dans un réseau Ethernet :
  - **Mode duplex intégral** : les deux extrémités de la connexion peuvent envoyer et recevoir des données simultanément.
  - **Mode semi-duplex** : une seule extrémité de la connexion peut envoyer des données à la fois.
  - La plupart des périphériques utilisent la négociation automatique qui permet à deux périphériques d'échanger automatiquement des informations sur le débit et les fonctionnalités duplex et de choisir le mode le plus performant.
- Le **conflit de mode duplex** est une cause fréquente de problèmes de performance avec les liaisons Ethernet. Il se produit lorsqu'un port sur la liaison fonctionne en semi-duplex tandis que l'autre port fonctionne en mode duplex intégral.

A.3. Mettre en œuvre l'adressage IP

- Systèmes numériques
- Adressage IPv4 / Adressage IPv6
- Segmentation d'un réseau IPv4 / IPv6 en sous-réseau VLSM

Adresse IPv4

1. Introduction :

Les adresses IPv4 sont exprimées en 32 bits binaires divisés en 4 octets de 8 bits

*Format d'écriture : **A.B.C.D** sont comprises entre 0 et 255*

L'***Internet Assigned Numbers Authority*** (***IANA***) est un département de l'ICANN supervise l'allocation globale des adresses IPv4 et IPv6, etc.

2. Conversion binaire –décimale :

Pour faciliter la conversion (sans faire des divisions ni équations) :

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

128+32+16+2=178

ou

255-(64+8+4+1)=255-77=178

Méthode pour convertir de la décimale vers binaire (8bits)

204-128=76

76-64=12

12-8=4

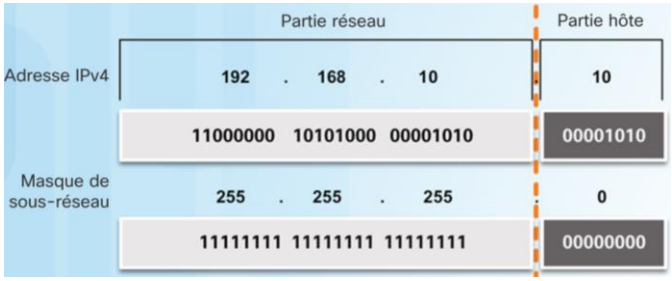
4-4=0

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

3. La hiérarchie de l'adresse IPv4 :

- ***Une adresse IPv4 est hiérarchique :*** *Elle est composée d'une partie réseau et d'une partie hôte.*
- **La partie réseau de tous les équipements d'un même réseau doit être identique.**
- ***Le masque de sous-réseau*** *permet aux périphériques d'identifier la partie réseau et la partie hôte ; il est constitué* ***de série de «1 » : Partie Réseau et se termine par une série de « 0 » : Partie Hôte.***
  S'écrit comme l'adresse IP : 255.255.255.0 ou /24 : 24 nombre des « 1 »

- *Pour calculer l'adresse Réseau : On fait une opération AND entre l'adresse IP et le Masque par bit.*



*192.168.10.10**/24***

4. Les différents types d'adresse IP dans un réseau :

Dans chaque réseau, les adresses IP peuvent être attribué aux hôtes sauf 2, l'adresse réseau et l'adresse diffusion.

- **Adresse réseau : la partie hôte** contient uniquement des « **0** » (00…000)
- **Première adresse hôte : la partie hôte** contient uniquement des 0 sauf un 1 en dernière position (00…0001)
- **Dernière adresse hôte : la partie hôte** contient uniquement des 1 sauf un 0 en dernière position (11….110)
- **Adresse diffusion : la partie hôte** contient uniquement des « **1** » (11….11)

5. Types d'adresses :

- ✓ **Monodiffusion** : communication un à un.
- ✓ **Diffusion** : communication un à tous.
- ✓ **Multidiffusion** : communication un à un groupe sélectionné.

6. Plages des adresses IPv4 :

Monodiffusion	**0./8 au 223./8**
Multidiffusion	**224./8 au 239./8**
Non utilisé	**240./8 au 255./8**

NB : toutes les adresses monodiffusion sont des adresses publiques, cad routable sur Internet sauf les adresses Privé et Spéciaux (voir la suite)

- **Adresses privées**
  - ❖ Non routables
  - ❖ Introduites au milieu des années 1990 en raison du manque d'adresses IPv4
  - ❖ Utilisées uniquement dans les réseaux internes.
  - ❖ Doivent être traduites en adresse IPv4 publique pour être routées.
  - ✓ **Blocs d'adresses privées**
    - ✓ **10.0.0.0 /8** ou 10.0.0.0 à 10.255.255.255
    - ✓ **172.16.0.0 /12** ou 172.16.0.0 à 172.31.255.255
    - ✓ **192.168.0.0 /16** ou 192.168.0.0 à 192.168.255.255
- **Adresses Spéciaux :**
  - ✓ Adresse Identification local **(0.0.0.0/8)**
  - ✓ **Adresses de bouclage** (**127.0.0.0 /8**)
    - ❖ Utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle.
  - ✓ **Adresses link-local** (**169.254.0.0 /16**)
    - ❖ Communément appelées adresses APIPA (Automatic Private IP Addressing)
    - ❖ Utilisées par le client DHCP pour se configurer automatiquement si aucun serveur DHCP n'est disponible.
  - ✓ **Adresses TEST-NET** (**192.0.2.0 /24**) : Utilisées pour l'enseignement et l'apprentissage.

7. L'ancien adressage par classe :

- Les adresses réseau reposaient sur 3 classes :
  - **Classe A** (**0.0.0.0/8** à **127.0.0.0/8**) : créée pour prendre en charge les réseaux de très grande taille, comportant plus de 16 millions d'adresses d'hôte.
  - **Classe B** (**128.0.0.0 /16** à **191.255.0.0 /16**) : créée pour répondre aux besoins des réseaux de taille moyenne ou de grande taille comportant jusqu'à 65 000 adresses d'hôtes environ.
  - **Classe C** (**192.0.0.0 /24** – **223.255.255.0 /24**) : créée pour répondre aux besoins des réseaux de petite taille comportant 254 hôtes maximum.
- **L'adressage par classe a gaspillé des adresses et a épuisé le nombre d'adresses IPv4.**
- **L'adressage sans classe a été introduit dans les années 1990**
  - **Routage inter domaine sans classe (CIDR)**
  - **Permet aux opérateurs d'allouer les adresses IPv4 sur n'importe quelle limite binaire (longueur de préfixe) au lieu d'utiliser uniquement les classes A, B ou C.**

Adresse IPv6

1. *Introduction :*

- Espace d'adressage de 128 bits plus grand, 340 sextillions d'adresses (340 10^{36})
- Résout les limites d'IPv4 (max. théorique 4 10^{9}) qui ne nous permet pas de connecter tous les hôtes sur internet.
- Apporte des améliorations comme la configuration automatique des adresses.

2. *Adresses IPv6:*

- ✓ *Sa longueur est de 128 bits.*
- ✓ *Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique*
- ✓ ***Hextet** : terme officieux qui désigne un segment de 16 bits ou de quatre valeurs hexadécimales.*

3. *Format privilégié pour la représentation des IPv6 :*

2001 :0DB8 :0000 :1111 :0000 :0000 :0000 :0000 :0200
2001 :0DB8 :0000 :1111 :00A3 :ABCD :0000 :EF98 :1234
FE80 :0000 :0000 :0000 :0123 :4567 :89AB :CDEF
0000 :0000 :0000 :0000 : 0000 :0000 :0000 :0001
0000 :0000 :0000 :0000 : 0000 :0000 :0000 :0000

4. *Pour compresser le format privilégié*

- **Règle n° 1 – Omettre les zéros en début de segment**

2001 :0DB8 :0000 :1111 :0000 :0000 :0000 :0000 :0200

R1 :2001 :DB8 :0 :1111 :0 :0 :0 :0 :200

- **Règle n° 2 – Omettre les séquences composées uniquement de zéros :** *Une suite de deux deux-points (::) peut remplacer toute chaîne unique et continue d'un ou plusieurs segments de 16 bits (hextets) comprenant uniquement des zéros.*

R2 :2001 :DB8 :0 : 1111 :: 200

Donc le format compressé de l'adresse IPv6 est : 2001 :DB8 :0 :1111 ::200

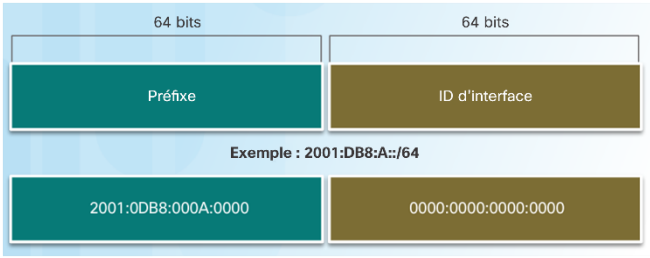
5. *Les types des adresses IPv6 :*

- ***Monodiffusion** : une seule source d'adresse IPv6.*
- ***Multidiffusion** : une adresse de multidiffusion IPv6 est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations.*

6. *Le préfixe et La longueur de préfixe :*

La longueur du préfixe IPv6 est utilisée pour indiquer la partie réseau de l'adresse IPv6 :

- *La longueur de préfixe peut être comprise entre 0 et 128. (masque pour IPv4)*
- *La longueur de préfixe IPv6 standard pour la plupart des LAN est /64*



7. *Les adresses de monodiffusion IPv6 :*

***Monodiffusion globale** : ces adresses sont uniques au monde et routables sur Internet. (publiques IPv4)*	**2000 ::/3**
***Link-local** : utilisées pour communiquer avec d'autres équipements sur la même liaison locale. Limitées à une seule liaison. (169.254.0.0/16)*	**FE80 ::/10**
***Locale unique** : utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites. (comme les adresses Privés dans ipv4)*	**FC00 ::/7**
Adresse de bouclage : attribuée à l'interface de bouclage du routeur ou hôte.	**::1/128**
Adresse non spécifiée !	**::/128**

8. Adresses IPv6 Multidiffusion :

Exemples des adresses IPv6 Multicast

- ***Groupe de multidiffusion à tous les nœuds***
  ***FF02::1** – il s'agit d'un groupe de multidiffusion que tous les périphériques IPv6 peuvent rejoindre. Similaire à une diffusion IPv4*
- ***FF02::2** Groupe de multidiffusion à tous les routeurs il s'agit d'un groupe de multidiffusion que peuvent rejoindre tous les routeurs IPv6.*

9. *Affectation Des adresses ipv6 aux hôtes :*

SLAAC : *Un périphérique peut obtenir son préfixe, la longueur de préfixe, l'adresse de la passerelle par défaut et d'autres informations à partir d'un routeur IPv6.*

« Utilise des messages d'annonce de routeur ICMPv6 (RA) du routeur local

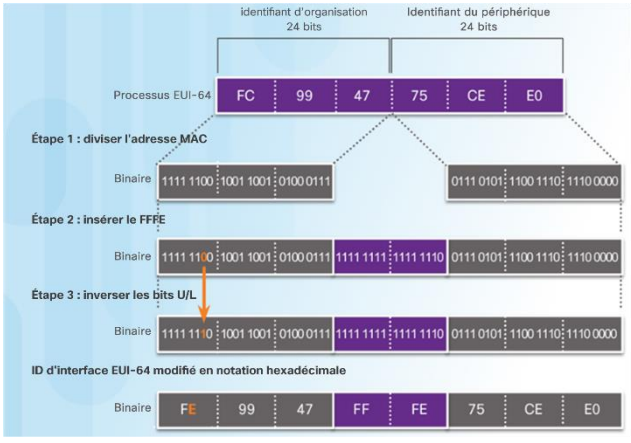
SLAAC et DHCP : *utilise SLAAC pour obtenir adresse IP et longueur de préfixe et adresses de passerelle et pour les autres options on obtiendra depuis le serveur DHCP*

DHCP : *Toutes les informations sont obtenues depuis serveur DHCP sauf l'adresse de passerelle.*

10. *Génération aléatoire et à l'aide de la méthode EUI-64*

La partie ID interface est obtenu soit de façon aléatoire ou avec la méthode EUI-64

- *Un ID d'interface EUI-64 est représenté au format binaire et comprend trois parties :*
  - *Le code OUI sur 24 bits, provenant de l'adresse MAC du client, mais dont le septième bit (universellement/localement, U/L) est inversé.*
  - *La valeur de 16 bits FFFE intégrée (au format hexadécimal).*
  - *ID de périphérique de 24 bits de l'adresse MAC du client.*



Segmentation des réseaux :

1. Segmentation des réseaux IP en sous-réseaux et Domaine de diffusion :

- Les hôtes peuvent générer un nombre excessif de diffusions, ce qui peut avoir une incidence négative sur le réseau.
  - Un fonctionnement ralenti du réseau en raison de la quantité importante de trafic généré.
  - Le ralentissement du fonctionnement de l'équipement dans la mesure où chaque périphérique doit accepter et traiter les paquets de diffusion un à un.
- **Solution** : réduire la taille du réseau en créant de plus petits domaines de diffusion. Ces espaces réseau plus petits sont appelés des ***sous-réseaux*.**
  - **Réduit le trafic global et améliore les performances réseau.**
  - **Permet aux administrateurs de mettre en œuvre des politiques de sécurité, notamment pour définir si les différents sous-réseaux sont autorisés ou non à communiquer entre eux.**

2. Segmentation à masque Fixe :

Si on veut diviser un réseau à **N** sous réseaux de taille fixe ; **càd le masque est fixe**. (tous les sous réseaux auront le même masque)

Méthode de calcul du masque et les adresses réseaux des sous-réseaux.

Prenons un exemple : soit l'adresse réseau **172.30.0.0/20** ; et on veut le diviser en **5** sous réseaux

Calcul du nouveau masque :

On cherche $X=2^m$ tel que $X \geq N$

Dans notre exemple : **$2^3 = 8 \geq 5$** donc **m=3** cad le masque des sous réseaux est : **20+m=16+3 =23 Le masque des sous réseau est : /23 = 255.255.254.0**

Pour l'adresse Réseau :

On écrit en binaire les bits qu'on vient les ajouter à la partie Réseau, et on donnant toutes les combinaisons possibles :

	Adresse Réseau			
Sous-Réseau	Partie réseau	PARTIE HOTE		
SR1	172.30. 0000 **000**	0. 0000 0000	→	**172.30.0.0**
SR2	172.30. 0000 **001**	0. 0000 0000	→	**172.30.2.0**
SR3	172.30. 0000 **010**	0. 0000 0000	→	**172.30.4.0**
SR4	172.30. 0000 **011**	0. 0000 0000	→	**172.30.6.0**
SR5	172.30. 0000 **100**	0. 0000 0000	→	**172.30.8.0**

NB : dans cette exemple, il est demandé seulement **5 SR** ; mais on peut créer **8 SR** ; vu que le division se fait seulement sur **2^x.**

3. Segmentation à masques variables (VLSM) :

La segmentation des réseaux avec masque fixe, suppose qu'on a le même nombre des hôtes sur chaque sous réseau ; ce qui est peut gaspiller les adresses IP, surtout si on n'a pas le même nombre des hôtes dans chaque sous réseau, c'est pour cela on a adopté une autre méthode qui est basé sur la division du réseau selon le nombre des hôtes dans chaque réseau ce qui introduit des masques variables pour chaque sous réseau == VLSM.

Méthode VLSM :

- **Etape** 01 : Trier les sous réseaux par ordre décroissant selon le nombre des hôtes.
- **Etape02** : ajouter à chaque sous réseau **+2** (adresse réseau + adresse diffusion)
- **Etape03** : chercher $X=2^n$ avec **X≥ (Nombre des hôtes du SR +2)**
- **Etape04** : Masque du SR /**M' = 32-n** ; (la taille de l'adresse IPv4 : 32 bits)
- **Etape05** : 1er SR aura l'adresse Réseau de départ, le 2eme SR aura l'adresse réseau du **1er SR + X** ; la valeur à ajouter dans le dernier octet de la partie Hôte.

  NB : si $X \geq 2^8$ on fait diviser $X/2^8 = r$, et on ajoute **r.0** au deuxième octet à droite. **Etape06 :**

L'adresse diffusion est **l'adresse Réseau du SR suivant -1**.

Exemple : l'adresses réseau 172.30.0.0/20

SR	Nombre des hôtes	N+2	$X=2_n$ **X≥** N+2	n	M'=32-n	@ Réseau =@Rezo précédant précèdent	@ Diffusion
SR1	300	302	512=2.0	9	/23	**172.30.0.0**	**172.30.1.255**
SR2	120	122	128	7	/25	**172.30.2.0**	**172.30.2.127**
SR3	102	104	128	7	/25	**172.30.2.128**	**172.30.2.255**
SR4	60	62	64	6	/26	**172.30.3.0**	**172.30.3.63**
SR5	22	24	32	5	/27	**172.30.3.64**	**172.30.3.95**
SR6	16	18	32	5	/27	**172.30.3.96**	**172.30.3.127**
SR7	2	4	4	2	/30	**172.30.3.128**	**172.30.3.131**
						172.30.3.132	

A savoir : **A.B.C.0 - 1 = A.B.C-1.255**

NB :

- **Le nombre des hôtes dans un réseau = 2^{32-M} -2**
- **Pour la première Adresse = @ réseau +1** • **Pour la dernière Adresse = @diffusion -1**

Astuces:

- Le dernier octet à droite de **l'adresse Réseau** et la **dernière adresse pour les hôtes** sont toujours « **PAIR** »
- Le dernier octet à droite de **l'adresse diffusion** et de la **première adresse disponible pour les hôtes** sont toujours « **imPAIR** »

A.4. Comprendre les modèles et les protocoles

- Modèle OSI et ses couches
- Modèles TCP/IP et ses couches
- Comparaison entre OSI et TCP/IP
- Protocoles et services réseaux (DNS, DHCP, FTP, messagerie et protocoles SMTP, POP, IMAP)

Règles de communication

Notions de base sur les communications

- Toutes les méthodes de communication ont en commun trois éléments :
  - Source ou expéditeur
  - Destination ou destinataire
  - Canal ou médias
- Des règles ou des protocoles régissent toutes les méthodes de communication.

Définition des règles

- Les protocoles sont nécessaires pour une communication efficace et comprennent :
  - l'identification de l'expéditeur et du destinataire ;
  - l'utilisation d'une langue et d'une syntaxe communes ;
  - la vitesse et le rythme d'élocution ;
  - la demande de confirmation ou d'accusé de réception.
- Les protocoles utilisés dans les réseaux de communication définissent également :
  - Codage des messages
  - Options de remise des messages
  - Format et encapsulation des messages
  - Synchronisation des messages
  - Taille des messages

Options de remise des messages

Message de monodiffusion	Message de multidiffusion	Message de diffusion
Livraison un à un	Livraison un à plusieurs	Livraison un à tous

Normes et protocoles réseau

Règles qui régissent les communications

- Les suites de protocoles sont mises en œuvre par les hôtes et les périphériques réseau dans le logiciel, le matériel ou les deux.
- Les protocoles sont représentés par des couches et chaque service de niveau supérieur dépend de la fonctionnalité définie par les protocoles constituant les niveaux inférieurs.

Protocoles réseau

- Les protocoles réseau définissent un format et un ensemble communs de règles d'échange des messages entre les périphériques.
- Les protocoles réseau les plus courants sont le protocole HTTP (Hypertext Transfer Protocol), le protocole TCP (Transmission Control Protocol) et le protocole IP (Internet Protocol).

Interaction entre les protocoles

- La communication entre un serveur
  web et un client web est un exemple d'interaction entre plusieurs protocoles :
  - **HTTP** : protocole d'application qui régit la manière dont un serveur web et un client web interagissent.

- **TCP** : protocole de transport qui gère les conversations individuelles.
- **IP** : encapsule les segments TCP en paquets, attribue les adresses et les livre à l'hôte de destination.
- **Ethernet** : permet la communication sur une liaison de données et la transmission physique des données sur le support réseau.

Suites de protocoles et normes de l'industrie

- Une suite de protocoles est un ensemble de protocoles qui fonctionnent ensemble pour fournir des services de communication réseau complets.
  - Peut être définie par un organisme de normalisation ou développée par un constructeur.
- La suite de protocoles TCP/IP est une norme ouverte, les protocoles peuvent être utilisés gratuitement et que tous les constructeurs ont la possibilité de les mettre en œuvre sur leur matériel ou leurs logiciels.

Suite de protocoles TCP/IP

Couche Application	HTTP FTP SMTP POP3 SMTP
Couche Transport	UDP TCP
Couche Internet	IPv4 IPv6 ICMP OSPF EIGRP
Couche Accès Réseau	ETHERNET ARP

Processus de communication TCP/IP

- Lors de l'envoi de données d'un serveur web à un client, la procédure d'encapsulation est la suivante :
  - Le serveur web prépare la page HTML (Hypertext Markup Language). Le protocole de couche d'application HTTP envoie les données à la couche transport.
  - La couche de transport divise les données en segments et identifie chacun d'eux.
  - Ensuite, les adresses IP source et de destination sont ajoutées, créant un paquet IP.
  - Les informations Ethernet sont ensuite ajoutées pour créer la trame Ethernet, ou trame de liaison de données.
- Lors de la réception des trames de liaison de données du serveur web, le client traite et supprime chaque en-tête de protocole dans l'ordre inverse dans lequel il a été ajouté :
  - Tout d'abord l'en-tête Ethernet est supprimé
  - Puis, l'en-tête de l'IP
  - Puis, l'en-tête de la couche transport
  - Enfin, les informations HTTP sont traitées et envoyées au navigateur web du client

Organismes de normalisation

Normes ouvertes

- Les normes ouvertes favorisent l'interopérabilité, la concurrence et l'innovation.
- Les organismes de normalisation sont généralement des associations à but non lucratif qui ne sont liées à aucun constructeur. Leur objectif est de développer et de promouvoir le concept des normes ouvertes.

Normes Internet

- **ISOC (Internet Society) :** société chargée de promouvoir le développement, l'évolution et l'utilisation libres d'Internet dans le monde entier.
- **IAB (Internet Architecture Board)** : comité en charge de la gestion et du développement des normes Internet.
- **IETF (Internet Engineering Task Force)** : groupe de travail chargé de développer, mettre à jour et gérer les technologies Internet et TCP/IP.
- **IRTF (Internet Research Task Force)** : groupe de travail axé sur la recherche à long terme liée aux protocoles Internet et TCP/IP.
- **ICANN (Internet Corporation for Assigned Names and Numbers) :** coordonne l'attribution des adresses IP et la gestion des noms de domaine.
- **IANA (Internet Assigned Numbers Authority)** : gère l'attribution des adresses IP, la gestion des noms de domaine et les identificateurs de protocole pour le compte de l'ICANN.

Organismes de normalisation des communications électroniques

- **IEEE (Institute of Electrical and Electronics Engineers)** : association qui se consacre à l'innovation technologique et à la création de normes dans de nombreux domaines, dont les réseaux.
- **EIA (Electronic Industries Alliance) :** normes relatives au câblage électrique, aux connecteurs et aux racks réseau.
- **TIA (Association des industries des télécommunications) :** normes pour les équipements radio, les antennes-relais, les périphériques VoIP (voix sur IP) et les communications par satellite.
- **ITU-T (Secteur de la normalisation des télécommunications de l'Union internationale des télécommunications)** : normes relatives à la compression vidéo, à la télévision sur IP (IPTV) et aux communications haut débit.

Modèles de référence

Avantages de l'utilisation d'un modèle composé de couches

- Avantage de l'utilisation d'un modèle en couches :
    - Aide à la conception de protocoles puisque les protocoles de chaque couche ont des fonctions définies.
    - Encourage la concurrence, car les produits de différents fournisseurs peuvent fonctionner ensemble.
    - Empêcher les changements de technologie d'une couche d'affecter les autres couches.
    - Fournit un langage commun pour décrire des fonctions et des fonctionnalités réseau.

Le modèle de référence OSI

- 7-**Application** : contient des protocoles utilisés pour les communications de processus à processus.
- 6-**Présentation** : permet une représentation commune des données.
- 5-**Session** : fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.
- 4-**Transport** : définit les services pour segmenter, transférer et réassembler les données.
- 3-**Réseau** : fournit des services pour échanger les parties de données individuelles sur le réseau entre des périphériques finaux identifiés.
- 2-**Liaison de données** : décrit des méthodes d'échange de trames de données entre des périphériques sur un support commun.
- 1-**Physique** : décrit les moyens mécaniques, électriques, fonctionnels et procéduraux de transmission des bits entre les connexions physiques.

Le modèle de protocole TCP/IP

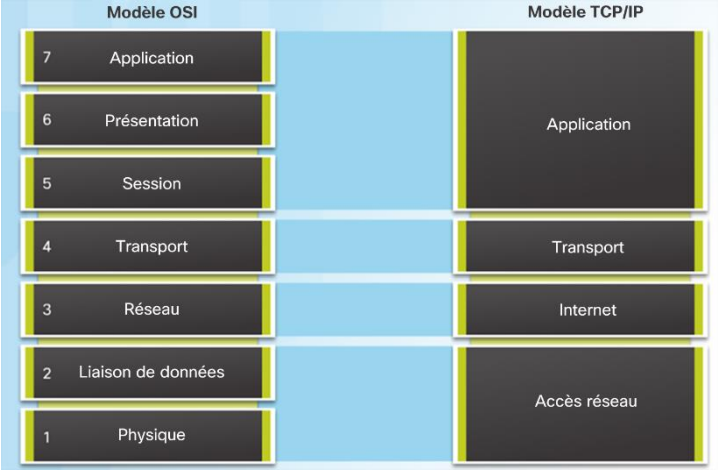
Le modèle de référence TCP/IP

- Créé au début des années 1970 pour les communications interréseau.
- Normes ouvertes.
- Aussi appelé le modèle TCP/IP ou le modèle Internet.

Les couches du modèle TCP/IP :

- **Application :** Représente des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue
- **Transport :** Prend en charge la communication entre plusieurs périphériques à travers divers réseaux.
- **Internet :** Détermine le meilleur chemin à travers le réseau.
- **Accès Réseau :** Contrôle les périphériques matériels et les supports qui constituent le réseau.

Dans le modèle OSI, la couche d'accès réseau et la couche application du modèle TCP/IP sont subdivisées pour décrire les fonctions distinctes qui doivent intervenir sur ces couches.



3.3 Transfert de données sur le réseau

Encapsulation des données

Segmentation des messages

Les flux de données importants sont divisés en parties de taille moins importante et plus facilement gérables pour les envoyer sur le réseau.

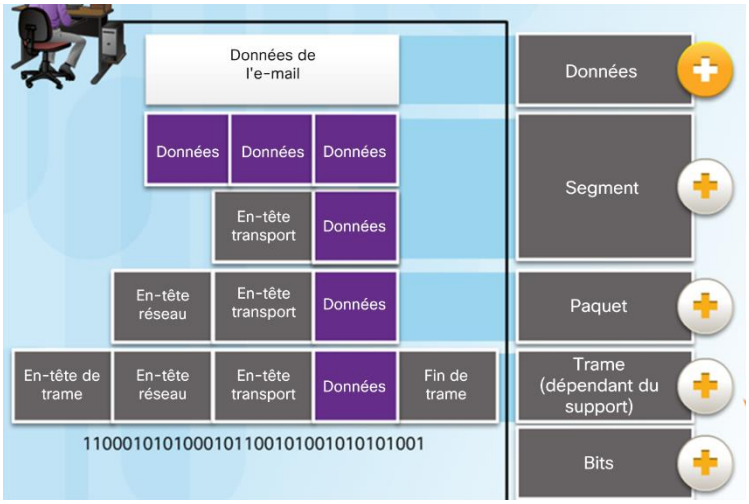
- L'envoi d'éléments de plus petite taille permet d'entremêler de nombreuses conversations différentes sur le réseau. C'est ce que l'on appelle le **multiplexage**.
- Chaque partie doit être étiquetée.
- Si une partie du message ne parvient pas à sa destination, seuls les morceaux manquants doivent être transmis à nouveau.

Unités de données de protocole

À mesure que les données d'application franchissent les piles de protocoles, des informations sont ajoutées à chaque niveau. Il s'agit du processus d'**encapsulation.**

La forme que prend une donnée sur chaque couche est connue sous le nom d'unité de données de protocole (PDU).

- **Données** : unité de données de protocole de la couche ***application***
- **Segment** : unité de données de protocole de la couche transport
- **Paquet** : unité de données de protocole de la couche réseau
- **Trame** : unité de données de protocole de la couche liaison de données
- **Bits** : unité de données de protocole de la couche physique



Couche 4 : Couche transport

La couche transport segmente les données et se charge du contrôle nécessaire au réassemblage de ces blocs de données dans les divers flux de communication. Pour ce faire, il doit :

- 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.

Suivi des conversations individuelles

Tout hôte peut héberger plusieurs applications qui communiquent sur le réseau. Chacune de ces applications communique avec une ou plusieurs applications hébergées sur des hôtes distants. Il incombe à la couche transport de gérer les nombreux flux de communication entre ces applications.

Segmentation des données

Chaque application crée un flux de données à envoyer vers une application distante ; ces données doivent donc être préparées pour être expédiées sur le support sous forme de blocs faciles à gérer. Les protocoles de la couche transport décrivent les services qui segmentent les données provenant de la couche application.

Reconstitution des segments

L'hôte recevant les blocs de données peut les diriger vers l'application appropriée. Il faut en outre que ces blocs de données individuels puissent être réassemblés dans un flux de données complet utile à la couche application.

Identification des applications

Pour que les flux de données atteignent les applications auxquelles ils sont destinés, la couche transport doit identifier l'application cible. Pour cela, la couche transport affecte un identificateur à chaque application. Les protocoles TCP/IP appellent cet identificateur un numéro de port.

Établissement d'une session

La couche transport est en mesure d'orienter la connexion en créant des sessions entre les applications. Ces connexions préparent les applications à communiquer entre elles avant le transfert des données. Dans ces sessions, il est possible de gérer avec précision les données d'une communication entre deux applications.

Acheminement fiable

Bien des circonstances peuvent entraîner la corruption ou la perte d'un bloc de données lors de son transfert sur le réseau. La couche transport veille à ce que tous les blocs atteignent leur destination en demandant au périphérique source de retransmettre les données qui ont pu se perdre.

Livraison dans un ordre défini

Étant donné que les réseaux fournissent une multitude de routes dont les délais de transmission varient, il se peut que les données arrivent dans le désordre. En numérotant et en ordonnant les segments, la couche transport s'assure que ces segments sont réassemblés dans le bon ordre.

Contrôle du flux

Les hôtes du réseau disposent de ressources limitées, par exemple en ce qui concerne la mémoire ou la bande passante. Quand la couche transport détermine que ces ressources sont surexploitées, certains protocoles peuvent demander à l'application qui envoie les données d'en réduire le flux. Ceci s'effectue au niveau de la couche transport en régulant la quantité de données que la source transmet sous forme de groupe. Le contrôle du flux contribue à prévenir la perte de segments sur le réseau et à rendre inutiles les retransmissions.

Ces services vous seront expliqués plus en détail quand nous étudierons les protocoles dans un chapitre ultérieur.

TCP et UDP

La pile de protocoles TCP/IP comprend 2 protocoles de couche 4 : TCP et UDP

TCP est un protocole orienté connexion, c'est-à-dire qu'il associe au transport des informations la notion de qualité en offrant les services suivants :

- Fiabilité
- Division des messages sortants en segments
- Réassemblage des messages au niveau du destinataire
- Ré-envoi de toute donnée non reçue

Segments : PDU de couche 4

UDP est lui un protocole non orienté connexion, c'est-à-dire qu'il n'offre pas de fonction de contrôle du bon acheminement :

- Aucune vérification logicielle de la livraison des messages
- Pas de réassemblage des messages entrants
- Pas d'accusé de réception
- Aucun contrôle de flux

Cependant, UDP offre l'avantage de nécessiter moins de bande passante que TCP. Il peut donc être intéressant d'utiliser ce protocole pour l'envoi de messages ne nécessitant pas de contrôle de qualité.

Les ports sont attribués de la manière suivante :

Plage de ports	***Utilisation***
0 à 1023	réservés aux applications publiques
1023 à 65535	attribué aux entreprises pour les applications commerciales et utilisé par le système d'exploitation pour l'attribution dynamique des ports source.

Numéros de ports

Afin que plusieurs communications puissent circuler en même temps, TCP et UDP utilisent des numéros de ports. Des conventions ont été établies pour des applications :

Protocole	Nº de port	Description
FTP data	20	File Transfer (données par défaut)
FTP	21	File Transfer (contrôle)
SSH	22	Secure SHell
Telnet	23	Telnet
SMTP	25	Simple Mail Transfer
DNS	53	Domain Name System
HTTP	80	World Wide Web HTTP
POP3	110	Post Office Protocol - Version 3
NNTP	119	Network News Transfer Protocol
IMAP	143	Interactive Mail Access Protocol v2
HTTPS	443	Protocole HTTP sécurisé (SSL)

Méthode de connexion TCP

Un service orienté connexion comportent 3 points importants :

- Un chemin unique entre les unités d'origine et de destination est déterminé
- Les données sont transmises de manière séquentielle et arrivent à destination dans l'ordre
- La connexion est fermée lorsqu'elle n'est plus nécessaire

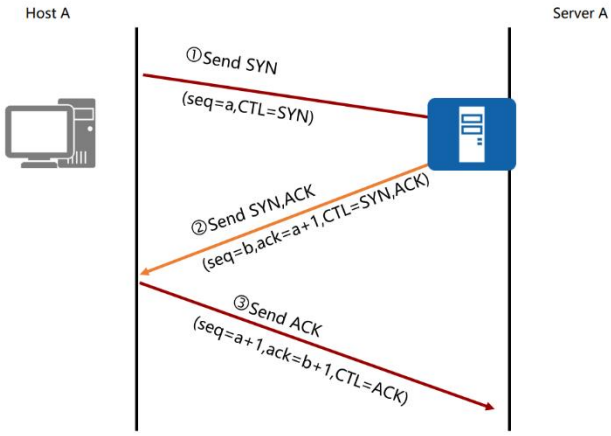
Connexion ouverte/échange en 3 étapes

Les hôtes TCP établissent une connexion en 3 étapes, appelée aussi « connexion ouverte » :

A. L'émetteur envoie un paquet avec un numéro de séquence initial (x) avec un bit dans l'en-tête pour indiquer une demande de connexion.

B. Le destinataire le reçoit, consigne le numéro de séquence initial, répond par un accusé de réception «x+1 » et inclut son propre nº de séquence (y).

C. L'émetteur reçoit x+1 et renvoie y+1 pour dire au destinataire que la réception s'est bien passée.



Fenêtrage

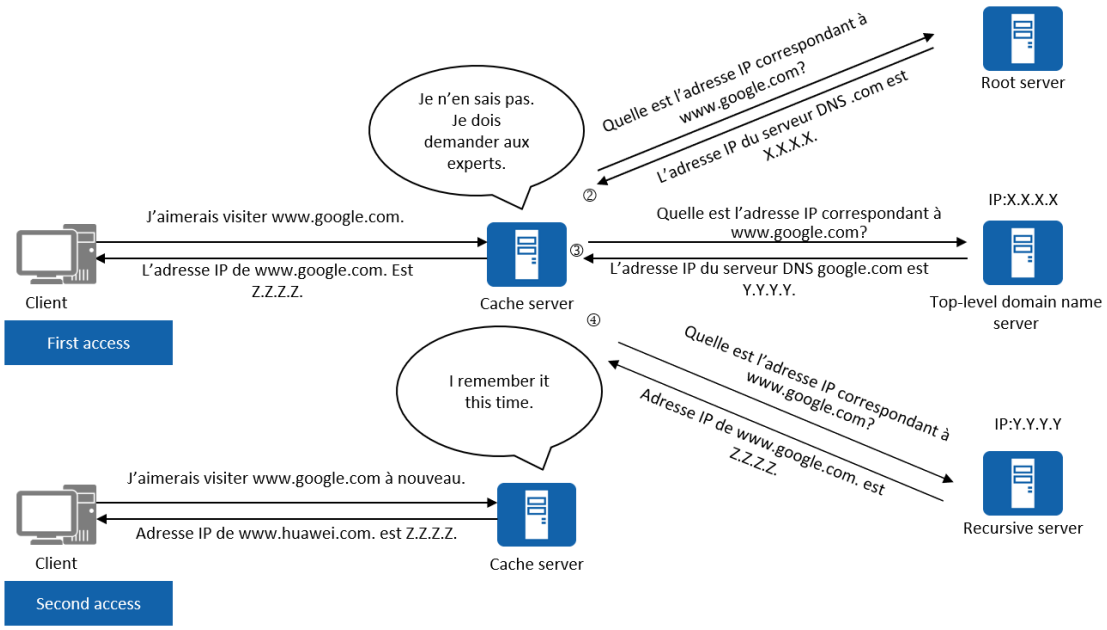
Le Fenêtrage est un mécanisme dans lequel le récepteur envoi un accusé de réception après avoir reçu un certain nombre de données. Si le destinataire n'envoi pas d'accusé, cela signifie pour l'émetteur que les informations ne sont pas parvenues correctement et dans ce cas sont retransmises.

La taille de la fenêtre détermine la quantité de données que l'on peut transmettre avant de recevoir un accusé de réception.

Protocoles et services réseaux (DNS, DHCP, FTP, messagerie et protocoles SMTP, POP, IMAP)

DNS : Domain Name System (Système de nom de domaine.)

Dans le monde de l'Internet, les machines du réseau sont identifiées par des adresses IP. Néanmoins, ces adresses ne sont pas très agréables à manipuler, c'est pourquoi, on utilise les noms. L'objectif a alors été de permettre la résolution des noms de domaines qui consiste à assurer la conversion entre les noms d'hôtes et les adresses IP. La solution actuelle est l'utilisation des DNS (Domain Name System).



Un système plus centralisé de gestion des noms.

Ce système consiste en une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente.

On appelle nom de domaine, le nom à deux composantes, dont la première est un nom correspondant au nom de l'organisation ou de l'entreprise, le second à la classification de domaine. (.fr, .com, ...).

Chaque machine d'un domaine est appelée hôte. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré (le serveur Web d'un domaine porte généralement le nom WWW).

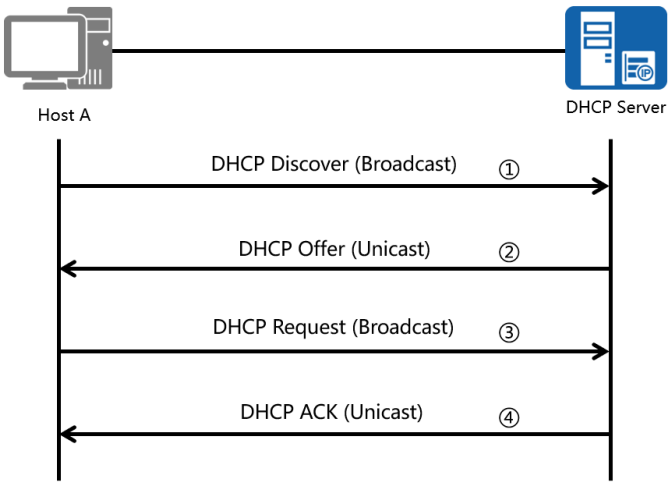
L'ensemble constitué du nom d'hôte, d'un point, puis du nom de domaine est appelé adresse FQDN (Fully Qualified Domain, soit Domaine Totalement Qualifié). Cette adresse permet de repérer de façon unique une machine. Ainsi, www.cisco.com représente une adresse FQDN.

Les machines appelées serveurs de nom de domaine permettent d'établir la correspondance entre le nom de domaine et l'adresse IP sur les machines d'un réseau.

DHCP

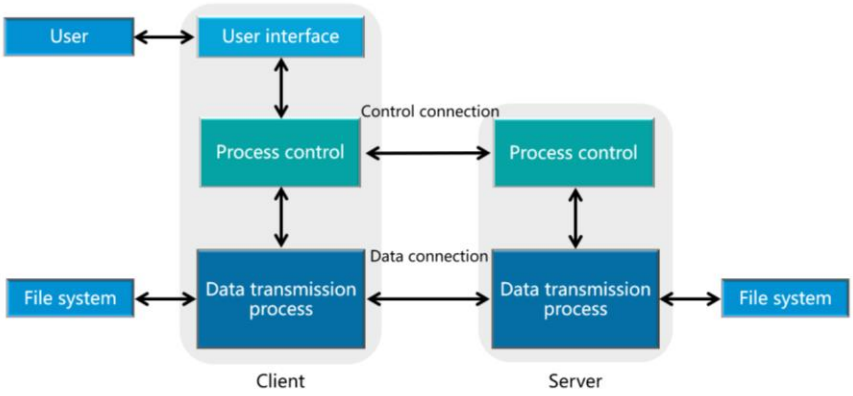
DHCP (Dynamic Host Configuration Protocol). Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP.

Le but principal étant la simplification de l'administration d'un réseau.



FTP : (File Transfer Protocol)

FTP est un protocole fiable et orienté connexion qui emploie TCP pour transférer des fichiers entre les systèmes. Le but principal du ftp est de transférer des fichiers à partir d'un ordinateur à un autre en copiant et/ou en déplaçant des fichiers des serveurs aux clients, et des clients vers les serveurs. Le protocole FTP est assigné au port 21 par défaut.



Quand des fichiers sont copiés d'un serveur, FTP établit d'abord une connexion de contrôle entre le client et le serveur. Alors une deuxième connexion est établie, qui est un lien entre les ordinateurs par lequel les données sont transférées.

TFTP

TFTP est un service non orienté connexion qui emploie UDP. TFTP (Trivial FTP) est employé sur un routeur pour transférer des dossiers de configuration et des images d'IOS de Cisco et aussi pour transférer des fichiers entre les systèmes qui supportent TFTP. TFTP est conçues pour être léger et simple à utiliser. Néanmoins TFTP peut lire ou écrire des fichiers sur un serveur à

distance mais il ne peut pas lister les répertoires et ne supporte pas une authentification utilisateur. Il est utile dans certains LANs parce qu'il fonctionne plus rapidement que le ftp.

HTTP

Le protocole de transfert hypertexte (HTTP) fonctionne avec le World Wide Web, qui est la partie la plus utilisée et la plus importante d'Internet. Une des raisons principales de cette croissance extraordinaire est la facilité avec laquelle il permet l'accès à l'information.

Un navigateur web est une application client/serveur, qui implique l'existence d'un client et d'un serveur, composant spécifique installé sur les 2 machines afin de fonctionner.

Un navigateur web présente des données dans un format multimédia, c'est-à-dire un contenu réagissant aux actions de l'utilisateur. Le contenu peut être du texte, des graphiques, du son, ou de la vidéo.

Les pages web sont écrite en utilisant l'HTML (HyperText Markup Language) : un navigateur web reçoit la page au format HTML et l'interprète de manière à afficher la page d'une manière beaucoup plus agréable qu'un document texte.

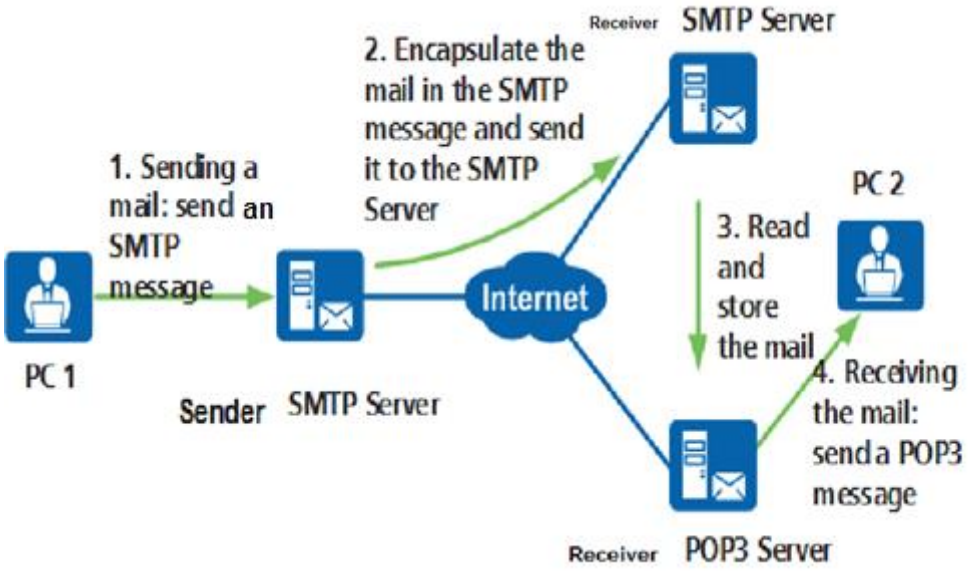
Pour déterminer l'adresse IP d'un serveur HTTP distant, le navigateur utilise le protocole DNS pour retrouver l'adresse IP à partir de l'URL. Les données qui sont transférées au serveur HTTP contiennent la localisation de la page Web sur le serveur.

Le serveur répond à la requête par l'envoi au navigateur du code html ainsi que des différents objets multimédias qui agrémente la page (son, vidéo, image) et qui sont indiqués dans les instructions de la page HTML. Le navigateur rassemble tous les fichiers pour créer un visuel de la page Web, et termine la session avec le serveur. Si une autre page est demandée, le processus entier recommence.

SMTP ; POP3 et IMAP

Les serveurs d'email communiquent entre eux en employant le Simple Mail Transfer Protocol (SMTP) pour envoyer et recevoir du courrier. Le protocole SMTP achemine des messages email dans le format Ascii en utilisant TCP. On l'utilise souvent en tant que protocole d'envoi de mail, rarement en tant que protocole de récupération d'email, car il est peu sécurisé et surtout n'offre aucune authentification.

- SMTP définit la façon dont les PC envoient le courrier à un serveur SMTP et le transfert du courrier entre les serveurs SMTP.
- Post Office Protocol 3 (POP3) et IMAP (Internet Mail Access Protocol) spécifient comment les PC gèrent et téléchargent le courrier sur le serveur de messagerie via un logiciel client.
- SMTP et POP3 (ou IMAP) sont déployés sur le serveur de messagerie par un administrateur et un logiciel client de messagerie (tel que Microsoft Outlook ou Foxmail) est installé sur le PC d'un utilisateur.



Telnet

Le protocole Telnet est un protocole standard d'Internet permettant l'interfaçage de terminaux et d'applications à travers Internet. Ce protocole fournit les règles de base pour permettre de relier un client à un interpréteur de commande (côté serveur).

Le protocole Telnet s'appuie sur une connexion TCP pour envoyer des données au format ASCII codées sur 8 bits entre lesquelles s'intercalent des séquences de contrôle Telnet.

Ce protocole est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite TCP/IP (FTP, SMTP, POP3, etc.).

En outre, le protocole Telnet est un protocole de transfert de données non sûr, c'est-à-dire que les données qu'il véhicule circulent en clair sur le réseau (de manière non chiffrée). Lorsque le protocole Telnet est utilisé pour connecter un hôte distant à la machine sur lequel il est implémenté en tant que serveur, ce protocole est assigné au port 23.