Chapitre 1: introduction

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

L'administrateur doit notamment s'occuper de :
- La gestion des besoins, du budget et des priorités.
- La gestion des ordinateurs et des périphériques
- La gestion des performances des systèmes.
- La gestion des utilisateurs.
- La gestion des fichiers et des disques.
- La gestion des services.
- La gestion des problèmes.
- La gestion des sauvegardes et du stockage des données. La gestion du réseau.
- La gestion de la sécurité.

Assurer la sécurité de l'infrastructure réseau via :

- Fermer à clé toute salle contenant du matériel informatique
- Mise en place d'un pare-feu
- Fermer à clé toute armoire contenant matériel réseau
- Mots de passe cryptés sur tous les périphériques
- Politique de sécurité et sensibiliser les utilisateurs

Différents réseaux :

- Télécommunications : téléphonie fixe et mobile
- Câblo-opérateurs : télédistribution
- Informatique : internet

Les différentes tailles

- PAN (Personal Area Network)

Réseau simple permettant à des périphériques locaux de partager des fichiers
1 à 10m, exemple: bluetooth

- LAN (Local Area Network)

Principalement utilisé dans les entreprises, les terminaux s'envoient des trames et n'ont pas besoin d'accès à internet
10m à 1km, exemple: campus

- MAN (Metropolitan Area Network)

Utilise principalement de la fibre optique afin de relier des bâtiments entre eux
1km à 100km, exemple: réseau FedMAN qui relie les bâtiments des administrations fédérales

- WAN (Wide Area Network)

Réseau qui couvre une grande zone géographique.
+ 100km, exemple: Internet

Les différentes technologies de transmission

- La diffusion

Un seul support de transmission est partagé par tous les équipements connectés. Chaque message envoyé par un équipement sur le réseau est reçu par tous, mais seul le destinataire concerné le traitera.

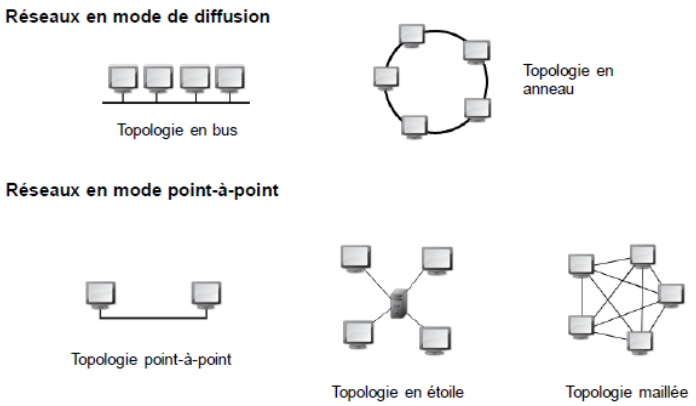
- Le point-à-point

Un seul support de transmission relie une paire d'équipements seulement.
Quand deux équipements non connectés directement entre eux veulent communiquer, ils le font par le biais des autres.
Une transmission p-à-p entre un expéditeur et un destinataire est appelée diffusion individuelle (ou envoi unicast).

Les différentes topologies

La topologie physique

Structure physique du réseau. C'est donc la forme, l'apparence, l'arrangement spatial du réseau.



La topologie logique

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

- Ethernet

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

- Token Ring

Accès par jeton: seul le poste ayant le jeton peut transmettre sur le réseau.
Si un poste veut émettre il doit attendre jusqu'à ce qu'il ait le jeton.
Topologie en anneau.

- FDDI (Fiber Distributed Data Interface)

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

Mode de fonctionnement des réseaux

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

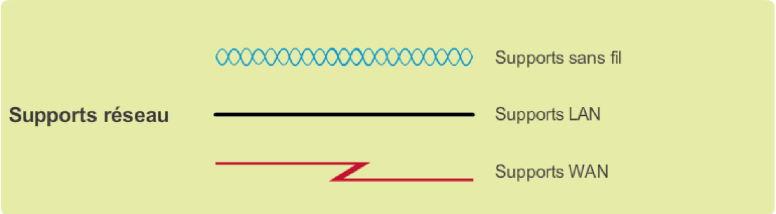
- Les serveurs fournissent des informations
- Les clients demandent des informations et les affichent

Habituellement, on utilise un modèle client-serveur où le serveur est passif et répond aux demandes des clients
Il existe également le modèle P2P (Peer to Peer) qui permet à un ordinateur d'être client et serveur simultanément

Avantages du P2P
- *Facile à configurer*
- *Coût faible*
- *Pratique pour les petits réseaux*

Désavantages du P2P
- Pas d'administration centralisée
- Peu sécurisé
- Non évolutif
- Risque de ralentissement sur le réseau lorsque beaucoup de requêtes

Symboles



Internet

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

Intranet
Réseau LAN privé d'une entreprise auquel peuvent accéder uniquement ses membres, ses employés ou des gens autorisés.
Généralement accessible uniquement depuis le site de l'entreprise.
Permet en général d'accéder aux horaires, notes de services, etc.

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

Manières d'accéder à Internet

- Par câble

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

- Par xDSL (Digital Subscriber Line)

Fonctionne sur un ligne téléphonique divisée en trois canaux

1. Appels téléphoniques
2. Download
3. Upload

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

- ADSL (Asymmetric DSL)

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

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

Permet d'atteindre d'obtenir un meilleur débit que les précédents. Jusque 34Mb/s en symétrique.

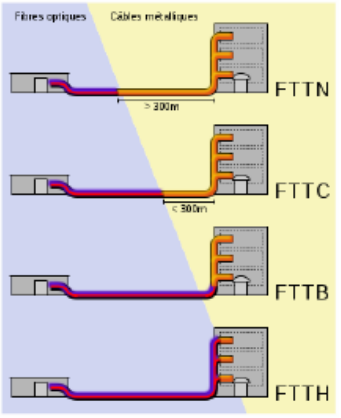
- VDSL 2 (Very-high-bit-rate DSL 2)

Encore plus que le premier. Jusque 100Mb/s en full-duplex.

- Par fibre

Plus la fibre est proche de l'utilisateur, plus la qualité de service sera meilleure.
Car les derniers mètres sont en cuivre, moins il y en a mieux c'est.

Il existe d'ailleurs différents types de réalisations possibles (en fonction du prix bien souvent) et on retrouve donc plusieurs appellations possibles :
- FTTN : *Fiber To The Neighbourhood*
- FTTC : *Fiber To The Curb* (Fibre jusqu'au trottoir)
- FTTB : *Fiber To The Building*
- FTTH : *Fiber To The Home*



- Par satellite

Idéal pour ceux qui n'ont pas accès à la DSL ou au câble. Les débits sont en général élevés comme les frais d'installation.
Déploiement au sol immédiat, dès que parabole installée, on a internet.

- Par cellulaire

On peut accéder à Internet partout où il y a un signal cellulaire via notre téléphone.
Les performances sont limitées selon le téléphone et la station de base

- Par ligne commutée

A l'époque, on téléphonait au FAI afin d'obtenir une faible bande passante.

Le WiMax (Worldwide Interoperability For Microwave Access)

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

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

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

Avant et maintenant

Aujourd'hui, grâce aux évolutions technologique, on peut regrouper tous les types de réseaux vu ci-dessous en un réseau convergent. Contrairement au passé, où chacun était un réseau ne pouvant communiquer avec les autres.

La segmentation et le multiplexage

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

Le but est d'envoyer des parties de plus petite tailles, afin de pouvoir entremêler plusieurs discussions. Cela s'appelle le **multiplexage.** On augmente la fiabilité du réseau car chaque message n'a pas besoin de parcourir le même chemin pour arriver à la destination.

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

L'architecture d'un réseau

Il y a 4 caractéristiques à prendre en compte:

- La tolérance aux pannes

Il faut que le réseaux limite l'impact des pannes => redondance.
Cela crée des chemins d'accès de substitution en cas de panne.

- L'évolutivité

Lorsqu'un utilisateur vient s'ajouter à un réseau, il faut que les performances restent inchangées pour ceux qui y étaient déjà
=> Utilisation d'un modèle hiérarchisé à plusieurs couches

- La qualité de service

L'utilisateur exige un niveau de qualité et de service ininterrompu.
=> Utilisation de niveaux de priorités (voix , vidéo, données)

- La sécurité

Avec l'évolution d'Internet comme moyen de transmission de communication, les exigeances en matière de sécu ont évoluées.
=> Mettre en place des mesures de sécurité

BYOD

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

La virtualisation

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

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

- Hyperviseur type 1

Outil qui s'interpose entre la couche matérielle et logicielle.
Il a accès aux composants de la machine et possède son propre noyau.

- Hyperviseur type 2

Application installée sur un système d'exploitation.
Les performances sont réduites mais propose une parfaite étanchéité entre les systèmes.

Le cloud computing

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

- Cloud personnalisé:

Conçus pour répondre aux besoins d'un secteur spécifique

- Cloud public:

Cloud dont les services et app. sont accessibles par tous. Ils peuvent être gratuit ou payant. (dropbox onedrive etc)

- Cloud privé:

Cloud dont les services et app. sont destinés à une entreprise ou à une entité spécifique (amazon webservices)

- Cloud hybride:

Cloud qui comporte au moins deux cloud.

Avantages du cloud computing
- Accès à tout moment via Internet
- Coûts d'infrastructure réduits,
- Permet de réagir rapidement aux besoins des clients

Le CPL (Courant Porteur de Ligne)

Permet la construction d'un réseau informatique sur le réseau électrique d'une habitation (comme le xDSL).

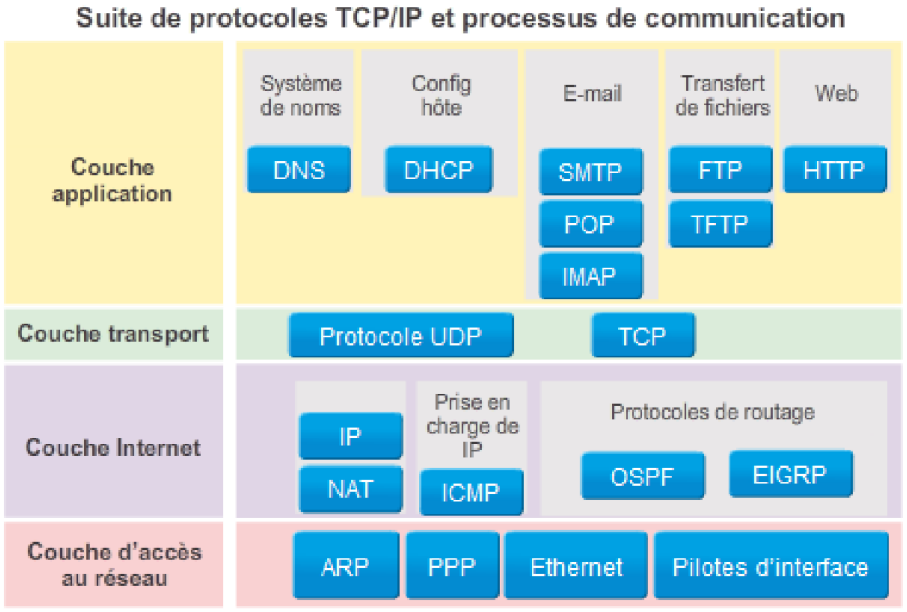
Le Big Data
Solution pour permettre à tout le monde d'accéder en temps réel à des bases de données géantes

Règles des 3V:
- Volume des données considérables à traiter,
- Variété d'informations,
- Vélocité à atteindre = Fréquence de création, collecte et partage

Chapitre 2: Communication et protocoles réseaux

Protocole

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



Codage d'un message

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

L'encapsulation et la désencapsulation

L'encapsulation est un processus permettant d'encapsuler un message dans un format spécifique appelé "trame",
Avant d'être transmis sur le réseau.

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

La désencapsulation c'est l'inverse.

Taille des messages

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

Synchronisation des messages

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

Contrôle de flux (débit de parole)

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

Option de remise des messages

Monodiffusion => un émetteur, un récepteur

Diffusion => un émetteur à tous les récepteurs

Multidiffusion => un émetteur à un groupe de récepteurs

Protocole propriétaire

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

Acronymes des protocoles à connaître

Protocoles de la couche application :

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

Protocoles de la couche transport :

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

Protocoles de la couche internet :

- IP (Internet Protocol) : Permet de recevoir des segments de message de la couche transport. Il regroupe les messages en paquets et indique leur adresse pour permettre leur acheminement de bout en bout sur un interréseau

- NAT (Network Address Translation) : Permet de convertir les adresses IP d'un privé en adresses IP globales et publiques
- ICMP (Internet Control Message Protocol) : Permet à l'hôte de destination de signaler à l'hôte source des erreurs liées aux transmissions de paquets
- OSPF (Open Shortest Path First) : Protocole de routage à états de liens permettant de faire du routage dynamique
- EIGRP (Enhanced Interior Gateway Routing Protocol) : Protocole de routage dynamique propriétaire à Cisco

Protocoles de la couche réseau :

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

Acronymes des sociétés de merde

Internet Society (ISOC) qui est chargée de promouvoir le développement, l'évolution et l'utilisation ouverte d'Internet dans le monde entier
Internet Architecture Board (IAB) qui s'occupe de la gestion et du développement général des normes sur Internet
Internet Engineering Task Force (IETF) qui a pour but de développer, de mettre à jour et d'assurer la maintenance d'Internet et des technologies TCP/IP. L'IETF se compose de différents groupes de travail qui constituent les principales entités de développement des spécifications et des recommandations de l'organisme
Internet Research Task Force (IRTF) qui se concentre sur la recherche à long terme liée à Internet, aux protocoles TCP/IP, aux applications, aux technologiques et à l'architecture
L'Institute of Electronical and Electronics Engineers (IEEE) qui est une association américaine professionnelle s'adressant aux spécialistes du génie électrique et de l'électronique qui souhaitent se consacrer à l'innovation

L'EIA (Electronic Industries Alliance) connue pour ses normes associées au câblage électrique, aux connecteurs et aux racks de 19 pouces utilisés pour monter l'équipement réseau.
La TIA (Telecommunications Industry Association) est responsable du développement des normes de communication dans un grand nombre de domaines.
L'ITU-T (secteur de la normalisation des télécommunications de l'Union Internationale des Télécommunications) définit des normes de compression, de télévision sur IP
L'ICANN (Internet Corporation for Assigned Names and Numbers) est une association a but non lucratif basée aux états unis qui coordonne l'attribution des adresses IP, la gestion des noms de domaine utilisés par le protocole DNS et les identificateurs de protocole ou numéro de ports utilisés par les protocoles TCP et UDP.
L'IANA (Internet Assigned Numbers Authority) est une composante de l'ICANN chargée de superviser et de gérer l'affection des adresses IP, la gestion des noms de domaines et les identificateurs pour le compte de l'ICANN.

Modèle OSI

7.	application	La ***couche application*** permet d'obtenir une connectivité de bout en bout entre des individus du réseau humain à l'aide de réseaux de données.	données	application
6.	présentation	La ***couche présentation*** fournit une représentation commune des données transférées entre des services de couche application.		présentation
5.	session	La ***couche session*** fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.		session
4.	transport	La ***couche transport*** définit des services pour segmenter, transférer et réassembler les données de communications individuelles entre les périphériques finaux.	segment	transport
3.	réseau	La ***couche réseau*** fournit des services permettant d'échanger des parties de données sur le réseau entre des périphériques finaux identifiés.	paquet	réseau
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.	trame	liaison de données
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. 42	bit	physique

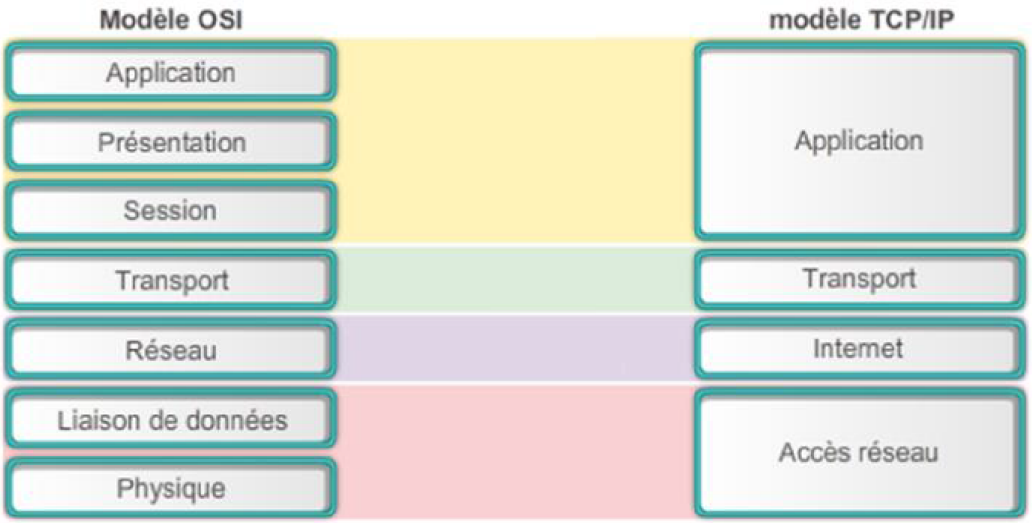
Le modèle TCP/IP

Le modèle de protocole TCP/IP pour les communications interréseau fut créé au début des années 1970 et est parfois appelé modèle Internet.

Le modèle TCP/IP est un modèle en 4 couches :

PDU		
Message	Application	Représente des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue.
Segment	Transport	Prend en charge la communication entre différents périphériques à travers divers réseaux.
Datagramme	Internet	Détermine le meilleur chemin à travers le réseau.
Trame	Accès réseau	Contrôle les périphériques matériels et les supports qui constituent le réseau.

44



Adresse réseau et adresse liaison de données

Dans un paquet IP, on retrouve deux adresses logiques: l'ip source et l'ip destination
Dans une trame de liaison de donneés on retrouve deux adresses physiques: l'adresse MAC source et l'adresse MAC destination

Les adresses MAC sont formées de 48 bits et sont physiquement intégrées à la carte réseau.

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

Normes IEE

- 802.1 protocoles LAN de couches supérieure
- 802.3 Ethernet
- 802.11 WLAN
- 802.15 WPAN (réseau sans fil personnel)

Important pour l'examen

Dans une trame liaison de données, on retrouve deux adresses physiques :

- L'adresse source : celle du périphérique qui envoie le paquet. Initialement la carte réseau de la source du paquet.
- L'adresse de destination : celle de l'interface réseau du routeur du tronçon suivant, ou si le destinataire est dans le réseau local, de celui-ci.

Communication

Lorsqu'un hôte doit communiquer avec un hôte distant, il doit utiliser le routeur, ou passerelle par défaut.

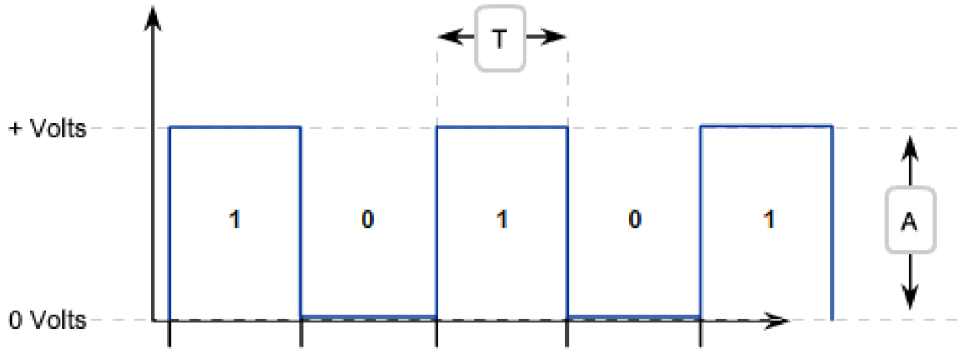
Cette adresse doit être configurée sur tous les hôtes du réseau local. Si pas d'adresse de passerelle pas défaut configurée, les messages adressés aux hôtes des réseaux distants ne peuvent être acheminés.

Lorsqu'un pc doit communiquer avec un réseau extérieur, l'adresse MAC de destination sera l'adresse du routeur (passerelle par défaut).

Chapitre 3: Accès réseau

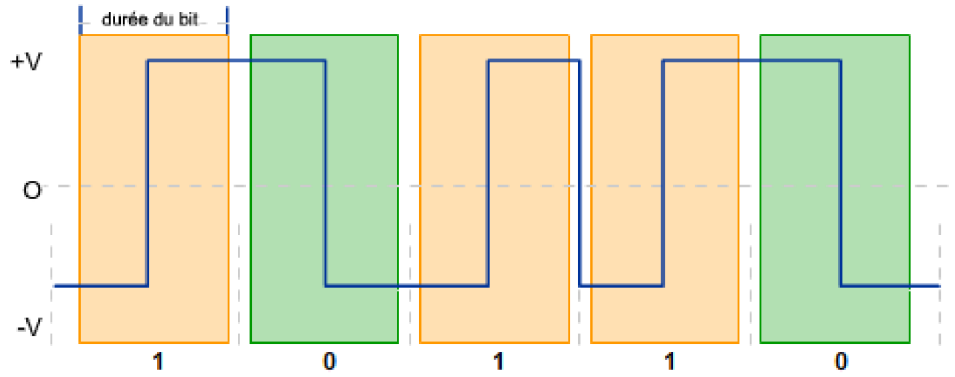
Les ≠ méthodes de codage

Le codage NRZ (Non Return To Zero)
Le flux de bits est transmis en tant que série de valeurs de tension



Dans le cas d'une plage de tension de 5V, 0V équivaut à un 0 logique, tandis que 5V équivaut à 1 logique.
Efficace uniquement à bas débit. N'utilise pas la bande passante de manière efficace.

Le codage Manchester
Représente les valeurs binaires comme des transitions de tension



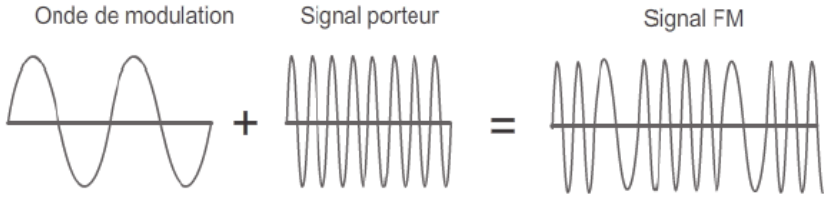
La transition d'une tension – à + équivaut à 1 logique. L'inverse à 0 logique.
Cette transition doit se produire au milieu de chaque durée de bit.

Les ≠ types de transmissions (signalisation)

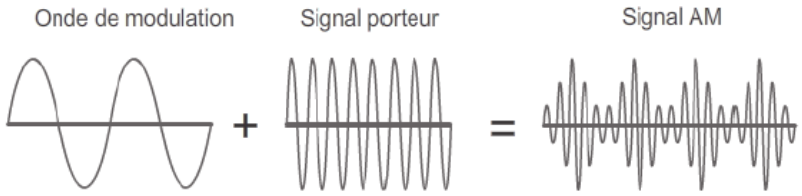
Asynchrone
L'intervalle de temps entre les caractères ou les blocs de donnés peut être défini arbitrairement
--> Les trames doivent contenir des indicateurs de début et de fin.

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

▪ **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.



La bande passante

Est la capacité d'un support à transporter des données.
Déterminée selon différents facteurs :

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

Le débit est la mesure du transfert de bits sur le support pendant une période donnée.

Les ≠ types de supports physiques

Support de cuivre
Plus souvent utilisé car bon marché, facile à installer et prés ente une faible résistance au courant électrique.
Limités par la distance et les interférences du signal.

Risques:
- Interférences électromagnétiques ou radioélectriques (EMI ou RFI)

Déforme et détériore les signaux de données => blindage, mise à la terre
Source : éclairages fluorescents, moteurs électriques)

- Diaphonie

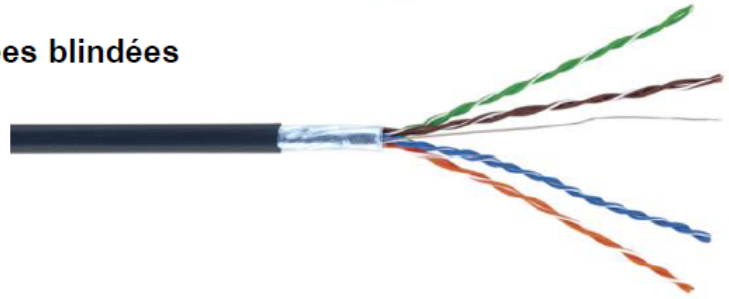
Perturbation d'un câble causée par les champs électrique ou magnétiques d'un signal d'un câble adjacent => torsader les paires de fils

Pour limiter la sensibilité des câbles de cuivre aux parasites électroniques, on peut par exemple utiliser un blindage métallique. (Nécessitant des connexions de mise à la terre).

Il existe 3 trois principaux types de supports en cuivre utilisés dans les réseaux :

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

➢ **les câbles à paires torsadées blindées**



➢ **les câbles coaxiaux**

Les câbles **UTP (Unshielded Twisted Pair)** utilisent des paires de câble torsadée poru éviter la diaphonie. Ils existent de différentes catégories :

• Catégorie 1 et 2 : correspondent à des types de câblages abandonnés. Il étaient utilisés pour les communications téléphoniques et les premiers réseaux Token Ring.

• Catégorie 3 : c'est un type de câblage permettant une bande passante de 16 MHz. Ce type de câble est en cours d'abandon également. Il ne sert principalement plus

qu'à la téléphonie sur le marché commercial ainsi que pour les réseaux Fast Ethernet.

• Catégorie 4 : c'est un type de câblage permettant une bande passante de 20 MHz. Ce standard fut principalement utilisé pour les réseaux « Token Ring » à 16 Mbps ou les réseaux 10BASE-T.

• 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 »).

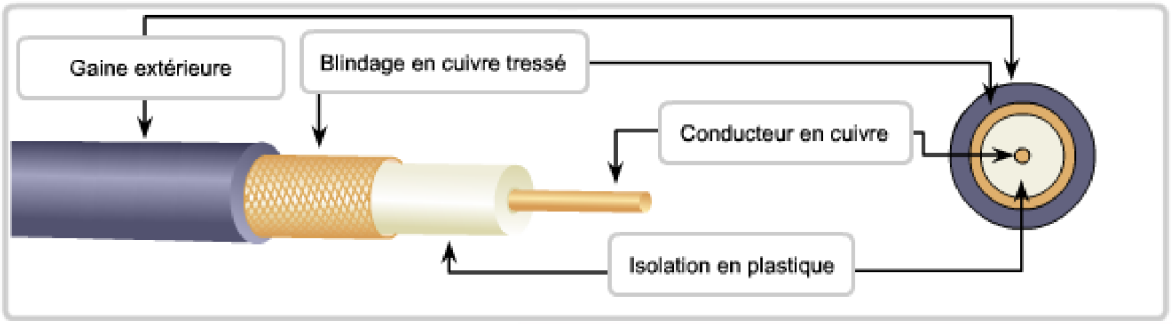
• Catégorie 5e : cette catégorie de câble est une adaptation de la catégorie 5. Elle permet une vitesse allant jusqu'à 1 000 Mbits/s et une bande passante de 100 MHz.

• Catégorie 6 : ce type de câble permet une bande passante de 250 MHz.

• Catégorie 7 : cette catégorie de câblage permet une bande passante de 1 GHz et permet un débit allant jusqu'à 10 Gbit/s !

Câbles coaxiaux

Composé d'un conducteur de cuivre entouré d'une couche de matériau isolant flexible.
Sur ce matériau isolant, il y une torsade de cuivre ou une feuille métallique.
La gaine enveloppe le tout.



Les prises BNC sont les connecteurs les plus répandus.

Fibre optique

Il s'agit d'un fil en verre très pur, transparent, flexible et très fin.
Les bits y sont codés sous forme d'impulsions lumineuses, le câble sert de guide d'ondes qui transmet de la lumière entre les deux extrémités Avec un minimum de perte de signal grâce à une différence d'indice de réfaction entre le cœur et sa gaine.

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

Désavantages: coût élevé, matériel différent, manipulation délicate

Domaine d'application: réseaux d'entreprise, FTTH, réseaux longue distance, réseaux sous-marins

Composition: coeur => enveloppe => gaine intermédiaire => renforcement => gaine générale

Il en existe deux types:

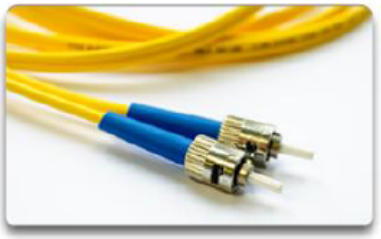
- Monomode:

Transporte un seul rayon lumineux émis par un laser, peut aller jusqu'à 100km, coeur de petit diamètre (8 à 10 microns), moins de dispersion

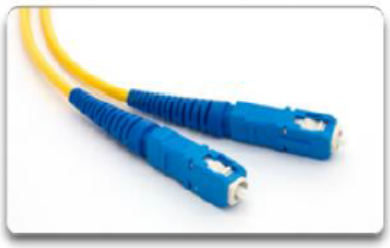
- Multimode:

Transporte plusieurs rayon lumineux incohérents, la lumière émises des DEL entre selon différents angles, coeur + large (50 à 62,5 microns), + de dispersion, 2km +-

▪ Le **connecteur ST (« Straight Tip »)** est un connecteur à baïonnette très largement utilisé avec de la fibre optique multimode.



Connecteurs ST



Connecteurs SC

▪ Le **connecteur SC (« Suscriber Connector »)** est un connecteur utilisant un mécanisme de pousser-tirer, garantissant l'insertion dans le bon sens et largement utilisé avec de la fibre optique monomode.

▪ Le **connecteur LC (« Lucent Connector »)** est un petit connecteur utilisé avec de la fibre optique monomode et multimode (bidirectionnelle ou non).

Connecteur LC

Support sans fils

Utilisent les fréquences radio ou micro-ondes

On retrouve 3 normes courantes:

- IEEE 802.11: WLAN = Wi-Fi, utilise le CSMA/CA

- IEEE 802.15: WPAN = Bluetooth, utilise un processus de jumelage
- IEEE 802.16: WiMax accès à large bande sans-fil à l'aide d'un topologie point-à-multipoints

- (802.1 = Réseaux locaux)
- Dans le futur, le LiFi: peut atteindre 45mbit/s

Comment déterminer le type d'un câble

S/FTP => Shielded Foiled Twisted Pair

Shielded -> Blindage composé de tresses métalliques
Foiled => Blindage grâce à une feuille de métal

Si S devant => Tresses métalliques entourent le tout
Sinon => Tresses métalliques entourent chaque paire

La composition d'une trame

- Une en-tête
  - Indicateur de début de trame
  - Adresses
  - Type
  - Contrôle de flux
- Fin de trame
  - Détection d'erreur
  - Indicateur de fin de trame

Méthodes d'accès

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

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

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

CSMA (Carrier Sense Multiple Access)
Amélioration de l'Aloha pour les réseaux câblés.

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

Quand la station a besoin d'émettre, elle vérifie que rien ne soit émise sur le media
- Si c'est le cas, elle commence à émettre
- Sinon elle attend la fin de la transmission en cours avant d'émettre

/!\ Ne supprime pas complètement les collisions

CSMA/CD (Collision Detection)
Amélioration du CSMA grâce à la détection de collision.

Une station prête à émettre transmet et continue à écouter le canal.
Si il y a une collision, elle interrompt sa transmission et envoie des signaux spéciaux "bits de bourrage" afin que
Toutes les stations présentes sur le réseau soit prévenus de la collision.

Elle retentera une émission ultérieurement (après un délai aléatoire)

CSMA/CA (Collision Avoidance)
Le périphérique examine le support pour établir si celui-ci comporte un signal.
Si le support est libre, le périphérique envoie une notif pour dire qu'il va transmettre
Ensuite il transmet ses données

La trame 802.11
La norme IEEE 802.11 (communément appelée Wi-Fi) utilise une méthode d'accès au support de type CSMA/CA.
Les réseaux 802.11 utilisent également les accusés de réception de liaison de données pour confirmer la bonne réception d'une trame.
Si la station de travail d'envoi ne détecte pas la trame d'accusé de réception, la trame est retransmise.

La faible congestion d'une bande (ex : 5GHz) est le fait qu'elle soit moins sujette aux interférences.

Chapitre 4: Ethernet

Ethernet

Il s'agit de la technologie réseau local prédominante dans le monde
- Fonctionne au niveau de la couche liaison de donnée et de la couche physique
- Définie par les normes 802.2 et 802.3 de IEEE

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

La couche liaison de donnée

Séparée en deux parties

- Sous-couche LLC Ethernet

Gère la communication entre les couches supérieures et inférieures.

- Sous-couche MAC Ethernet

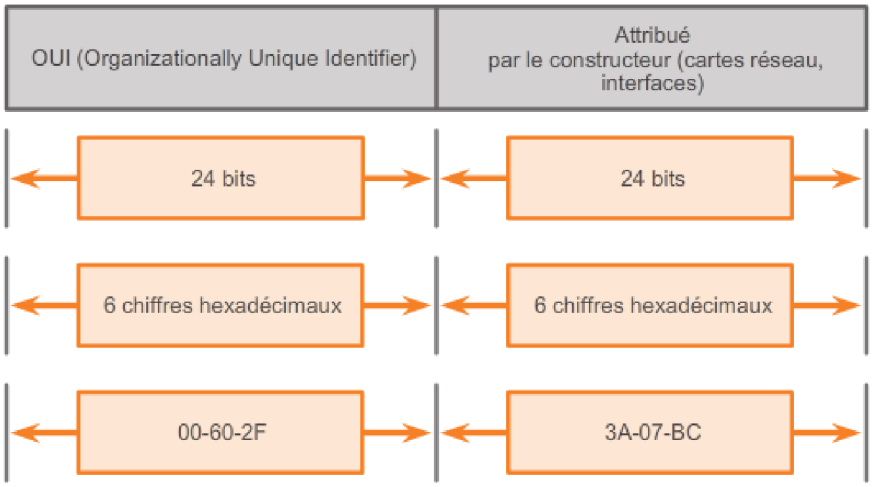
Elle encapsule les données et contrôle l'accès au support

Adresse MAC

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

Elles sont uniques au monde.

Les 24 premiers octets sont la partie OUI qui est l'identifiant du constructeur (les autres c'est la partie NIC)



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

Norme de taille d'une trame

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

Les types d'adresses MAC

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

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

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

Protocole ARP

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

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

Il existe deux façons de le faire en dynamique:
1. Quand un noeud reçoit des trames en provenance d'un support, il enregistre les IP et MAC source dans sa table ARP
2. Le périphérique envoie une requête ARP à tous les périphériques du réseau local, la requête contient l'IP destination et une adresse mac

de diffusion. Le périphérique concerné répond à la requête ARP en envoyant une trame de monodiff. contenant son adresse MAC

P174 à relire pour prérequis !!
Idem 182

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

Le concentrateur (HUB)

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

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

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

Le commutateur (SWITCH)

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

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

La table de commutation
Elle fait correspondre les adresses MAC de destination au ports utilisés pour la connexion aux noeuds.
Pour chaque trame entrante, l'adresse MAC de destination dans son en-tête est comparée à la liste d'adresses.
Lorsqu'un port répertorié dans la table est mappé à une adresse MAC, il est utilisé comme port de sortie de la trame.

Les ≠ fonctions de bases

- L'apprentissage:

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

- L'horodatage:

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

- L'inondation

Quand un commutateur ne sait pas sur quel port envoyer une trame, il fait une diffusion à l'exception du port d'arrivée
L'hôte possédant l'adresse correspondante va traiter la trame et lui répondre afin que le switch met à jour sa table MAC

- Le réacheminement sélectif

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

- Le filtrage

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

Domaine de collisions et de diffusions

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

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

La fonction auto-MDIX
Lorsque vous activez cette fonction, le commutateur détecte le type de câble requis pour les connexions Ehternet cuivre, puis configure les interfaces en conséquence

Méthodes de transmission de trames

Store and forward
Lorsqu'un switch reçoit une trame, il stocke les données dans des mémoires tampons jusqu'à ce qu'il ai tout reçu, pendant ce temps il recherche

dans la trame, des informations sur sa destination et procède à un contrôle d'erreur. Nécessaire pour l'analyse de la qualité de service sur des réseaux convergé où la classification des trames pour la priorité du trafic est importante.

Cut-through
Le switch agit sur les données au fûr et à mesure qu'il les reçoit, même si la transmission est pas finie. Il met une quantité suffisante en mémoire tampon Afin de lire l'adresse MAC de destination et déterminer ainsi le port où il faut transmettre les données. Il n'y a pas de controle d'erreur donc plus rapide qu'au-dessus, sauf que risque d'envoyer des trames endommagées => utilisation inutile de la bande passante.

Il en existe deux variantes:

- Fast-Forward

Offre le niveau de latence le plus faible. Transmet un paquet immédiatement après la lecture de l'adresse de destination
Comme il envoie avant d'avoir tout reçu, les trames peuvent comporter des erreurs.

- Fragment-Free

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

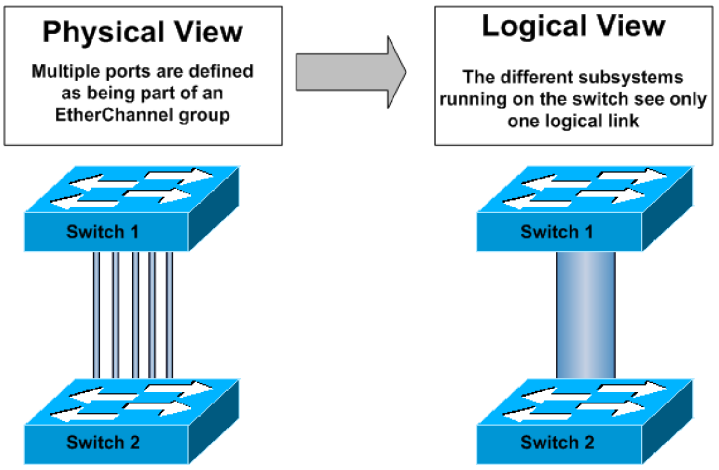
Mise en mémoire tampon

Axée sur les ports
Les trames sont stockées dans des files d'attentes liées à des ports entrants et sortants. Une trame est transmise au port sortant uniquement si
Toutes les trames qui la précèdent dans la file d'attente ont correctement été transmises. (Une seule trame peut tout retarder si un port de destination est saturé)

Partagée
Le commutateur stocke toutes les trames dans une mémoire tampon commune à tous les ports du commutateur. La capacité est allouée dynamiquement.
Les trames de la mémoire sont liées de manière dynamique au port de destination, ce qui permet de recevoir la trame sur un port et de la transmettre sur un autre sans files d'attente.

PoE : technologie permettent à un commutant de fournir une alimentation électrique à des périphériques par le biais d'un câble ethernet. Celui-ci alloue 2 paires (ou +) sur les quatre que contient un câble UTP.

EtherChannel est une technologie d'agrégation de liens utilisé principalement sur les commutateurs Cisco. Elle permet d'utiliser plusieurs liens physique comme un seul lien logique, afin d'augmenter la vitesse et la tolérance aux pannes des commutateurs.



Il existe des commutateurs de couche 3, fonctionnant comme un couche 2, mais à défaut d'exploiter les informations d'adresses MAC de couche 2, celui-ci peut également utiliser les adresses IP.
Celui-ci ne cherche pas uniquement à savoir quelle adresse MAC est associée à ses ports, mais il peut également identifier les adresses IP sur ses interfaces. Il peut donc réorienter le trafic sur bases d'adresse IP.

Ces commutateurs utilisent une méthode de transmission plus complexe appelée Cisco Express Forwarding (CEF).
Les 2 principaux composants de l'opération CEF sont :

- Base d'information de transfert (FIB pour « forwarding information base »)
- Table de contiguïté

Le principe de la FIB est très similaire à celui d'une table de routage. Cependant la structure de donnée plus avancée optimise la recherche, permettant une transmission plus efficace des paquets.

Chapitre 5: Système d'exploitation de réseau

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

DLNA définit un standard d'interopérabilité permettant la lecture, le partage,.. d'appareils multimédias, connecté à un routeur domestique. Ceux-ci regroupent 4 périphériques en 1 :

Routeur => transfère les paquets de données vers Internet et reçoit des paquets depuis Internet

Switch => Connecte des périphériques finaux à l'aide de câbles réseau
Point d'accès dans fil => émetteur radio capable de connecter des périph. finaux sans fil
Pare-feu => Sécurise le trafic sortant et controle le trafic entrant

Cisco IOS (Internetwork Operating System)

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

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

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

Accéder au CLI (Console-Line interface)

- Via le port console (ligne CTY) C'est un port de gestion permettant un accès hors réseau à un routeur. S'utilise en principal pour config initiale, reprise après sinistre, dépannage lorsqu'accès distant impossible, ou récupération de mdp
- Via telnet ou SSH (VTY) SSH est plus sécurisé quel telnet (authentification par mdp + sécurisée, chiffrement lors du transport de donnée)
- Via le port AUX (ligne téléphonique commutée) Ne s'utilise que localement comme le port console

Les périphériques réseau ont besoin de 2 types de logiciels pour fonctionner : l'OS et le logiciel de configuration.
Les fichiers de configuration contiennent les commandes du logiciel Cisco IOS utilisées pour personnaliser les fonctionnalités d'un périphérique Cisco.
Un périphérique réseau Cisco contient 2 fichiers de configuration : initiale chargé dans la mémoire vive quand le périphérique démarre, et celui en cours.

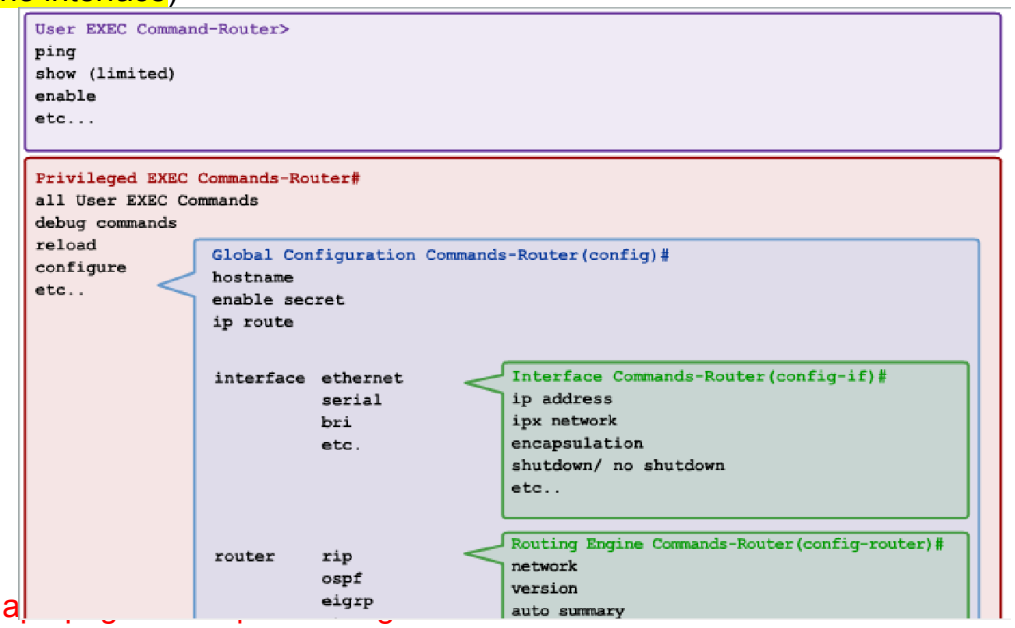
Le fichier de configuration initiale (« startup-config ») est utilisé au démarrage du système pour configurer le périphérique. Il est stocké en mémoire vive non volatile (NVRAM). Ce qui implique que ce fichier reste intact lorsque le périphérique Cisco est mis hors tension.

Lors du démarrage, les fichiers startup-config sont chargés en mémoire vive, et est considéré comme running config.

Le fichier de configuration en cours (« running config » est modifié lorsque l'administrateur réseau configure le périphérique. Les modifications de ce fichier produisent immédiatement leurs effets sur le fonctionnement du périphérique Cisco. Il faut sauvegarder ces modifications dans le startup-config, sous peine de les voir disparaître lors de l'extinction du périphérique.

Modes d'exploitation Cisco IOS dans l'ordre croissant

- Mode d'exécution utilisateur (visualisation)
- Mode d'exécution privilégié (visualisation détaillée et accès à la configuration et gestion du périphérique)
- Mode de configuration globale (commandes de configuration globale sur l'équipement)
- Modes de configuration spécifiques (commandes de configuration d'un service ou d'une interface)



Relire a

Chapitre 6: Couche réseau

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

Elle utilise pour cela, 4 processus de base:

- L'adressage

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

- L'encapsulation

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

- Le routage

Les paquets vont devoir traverser des périphériques intermédiaires connectant les réseaux (routeurs). Ils vont sélectionner les chemins afin de
Diriger les paquets vers leur destination. Chaque route empruntée par un paquet pour atteindre le périphérique suivant est appelée saut

- La désencapsulation

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

Les caractéristiques du protocole IP (Internet Protocol)

Il a été conçu pour ne pas surcharger les réseaux. Il fournit uniquement les fonctions requises pour transférer un paquet d'une source à une destination en passant par un système interconnecté de réseaux.

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

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

Le protocole IPv4

Un paquet IPv4 comporte deux parties
- En-tête IP -> indique les caractéristiques du paquet
- Données utiles -> contient les info. du segment de couche 4 et les données en elles-mêmes

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

Problèmes de l'IPv4
- Manque d'adresses IP => Il y en a 4 milliards mais c'est pas assez
- Croissance de la table de routage Internet => Ces routes IPv4 consomment beaucoup de mémoire et de ressources sur les routeurs Internet
- Manque de connectivité de bout en bout (du à la technologie d'adresse réseau NAT, permettant à plusieurs périphériques de partager une adresse ip publique unique)

Apparition de l'IPv6

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

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

Le routeur

Equipement intermédiaire opérant au niveau de la couche 3 du modèle OSI, il envoie et recevoir des paquets IP qui lui sont destinés
Chaque interface du routeur est un membre ou un hôté d'un réseau IP différent

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

Ils nécessitent:
- Un OS
- Un processeur
- De la mémoire vive => contient l'IOS, fichier de config « running-config », table de routage IP, Cache ARP, Mémoire tampon
  / !\ Mémoire volatile, perd son contenu lors mise hors tension.
- De la mémoire morte => instructions de démarrage, le POST (Power On Self Test, pour savoir si tout va bien), une version limitée (de merde) de l'IOS

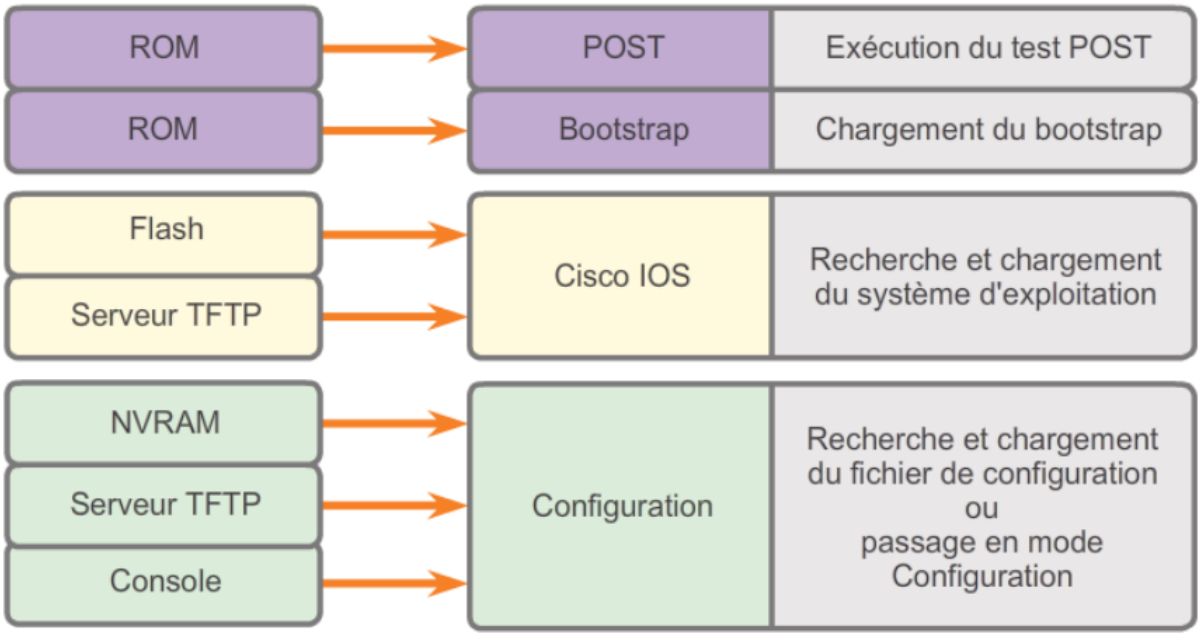
La mémoire vive non volatile est utilisé par IOS comme stockage permanent pour le fichier startup-config

La mémoire Flash est une mémoire non volative utilisée comme stockage permanent pour l'IOS et d'autres fichier associés au système, il y est copié de la mémoire Flash vers la mémoire vive lors du démarrage

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

Etapes lors du démarrage:

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



Connexion et interfaces d'un routeur

Les connexions sur un routeur Cisco peuvent être regroupées en deux catégories:
- Ports de gestion: ports console et aux utilisés pour configurer, gérer et dépanner le routeur (pas de transfert de paquets)
- Interfaces de routeur: configurée via l'adressage IP pour transporter le trafic.

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

Le routage

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

Un hôte peut envoyer un paquet à:
- Lui (via 127.0.0.1 qui est une interface de bouclage, à des fins de test)
- Un hôte local
- Un hôte distant => le routeur sera une "passerelle par défaut"

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

La table de routage

Fichier de donnée stocké dans la mémoire vive qui contient des informations de route sur le réseau connecté ainsi que les entrées de réseaux distants que le

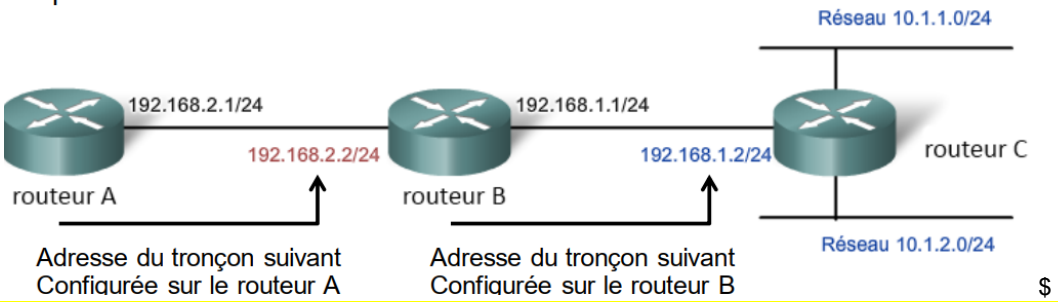
périphérique a découvertes. Le routeur utilise ces infos pour trouver le meilleur chemin.

Les routes possèdent trois caractéristiques principales:
- Le réseau de destination
- Le tronçon suivant ou la passerelle permettant d'atteindre le réseau de destination
- La métrique associée au réseau de destination

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

Un routeur peut être configuré pour posséder une route par défaut. Il s'agit d'un route qui correspond à tous les réseaux de destination.
Dans les réseaux IPv4 l'adresse 0.0.0.0 avec le masque 0.0.0.0 est utilisée à cet effet. La route par défaut est utilisée pour transférer
Les paquets pour lesquels aucune entrée ne figure dans la table de routage pour le réseau de destination.

Fonctionnement route statique
Chaque routeur doit connaitre la structure du réseau.
Une route par défaut doit être configurée pour chaque sous-réseau.
Si la structure du réseau change ou que de nouveaux réseaux deviennent disponibles, ces modifications doivent être mises à jour manuellement sur chaque routeur.



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

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

Les protocoles de routage sont:
- RIP (Routing Information Protocol)

Chaque route est associée à une métrique (nombre de sauts limité à 15)
Chaque routeur envoie à ses voisins ses info. de routage (toutes les 30 sec)
Il va calculer les meilleures routes et déduire sa table de routage selon la métrique calculée

- EIGRP (Enhanced Interior Gateway Routing Protocol)

Calcule les métriques sur base d'une formule composée du délai, de la bande passante, de la fiabilité et de la charge.
Au niveau du réseau, chaque routeur envoie un paquet "Hello" à ses voisins toutes les 5sec afin de dire qu'il est actif et que ses routes sont correctes.
Au niveau de l'échange d'info. une mise à jour concernant une table de routage n'est envoyée que lorsque celle-ci est modifiée. Cette màj contiendra que les routes modifiées et sera envoyée qu'aux routeurs concernés

- OSPF (Open Shortest Path First)

Permet d'avoir des routes de plus de 15 sauts
Utilise une métrique plus compliquée (prenant compte des débits)
Améliore le temps de convergence. (Temps nécessaire aux routeurs pour recalculer les nouvelles routes suites à un changement dans le résau)
P269 config routeur !!

Chapitre 7: Couche transport

Introduction

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

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

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

Objectifs de la couche transport

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

Fiabilité de la couche transport

Elle est basée sur 3 opérations de base:
- Effectuer le suivi des données transmises
- Accuser la réception des données
- Retransmettre toute donnée n'ayant pas fait l'objet d'un accusé de réception

Les protocoles TCP et UDP

TCP (Transmission Control Protocol)
Protocole de couche transport fiable et complet, qui garantit que toutes les données arrivent à destination.

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

En-tête TCP = 20 octets

UDP (User Datagram Protocol)
Protocole de couche transport très simple qui ne permet pas de garantir la fiabilité

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

En-tête UDP = 8 octets

Donc TCP > UDP

Les numéros de port classé par l'IANA

- Ports réservés (0 à 1023)

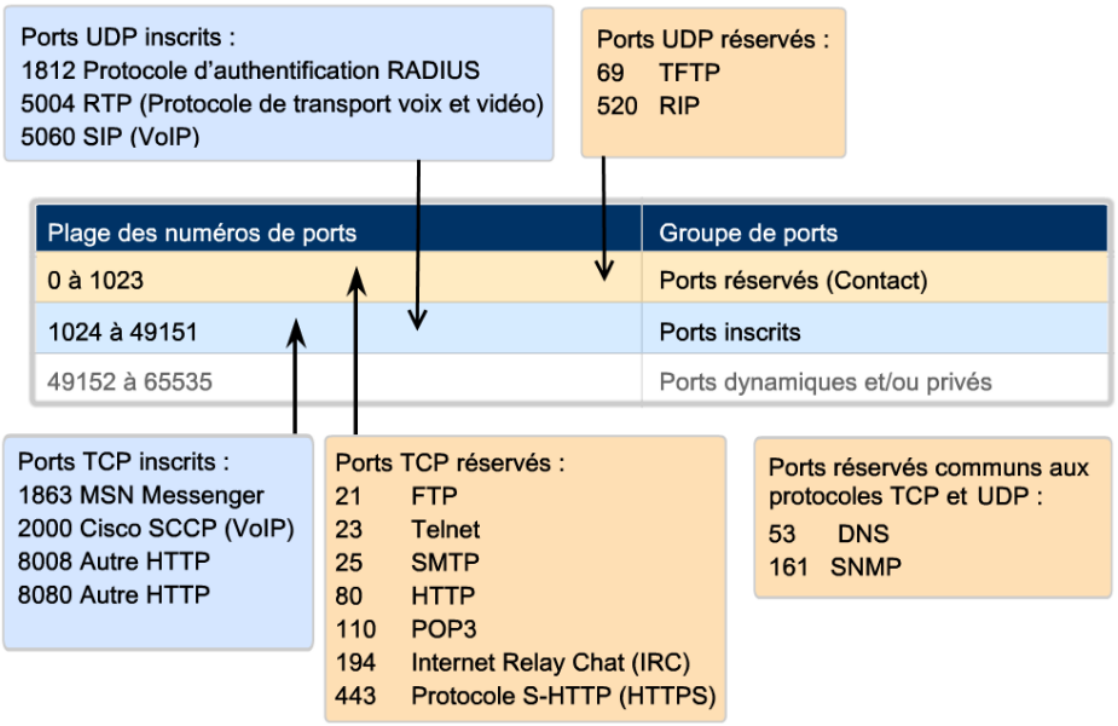
Ils sont réservés à des services ou applications

- Ports inscrits (1024 à 49151)

Affecté à des processus ou applications d'utilisateurs

- Ports privés ou dynamiques (49152 à 65535)

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



L'ensemble formé par le numéro de port et l'adresse ip s'appelle un SOCKET.

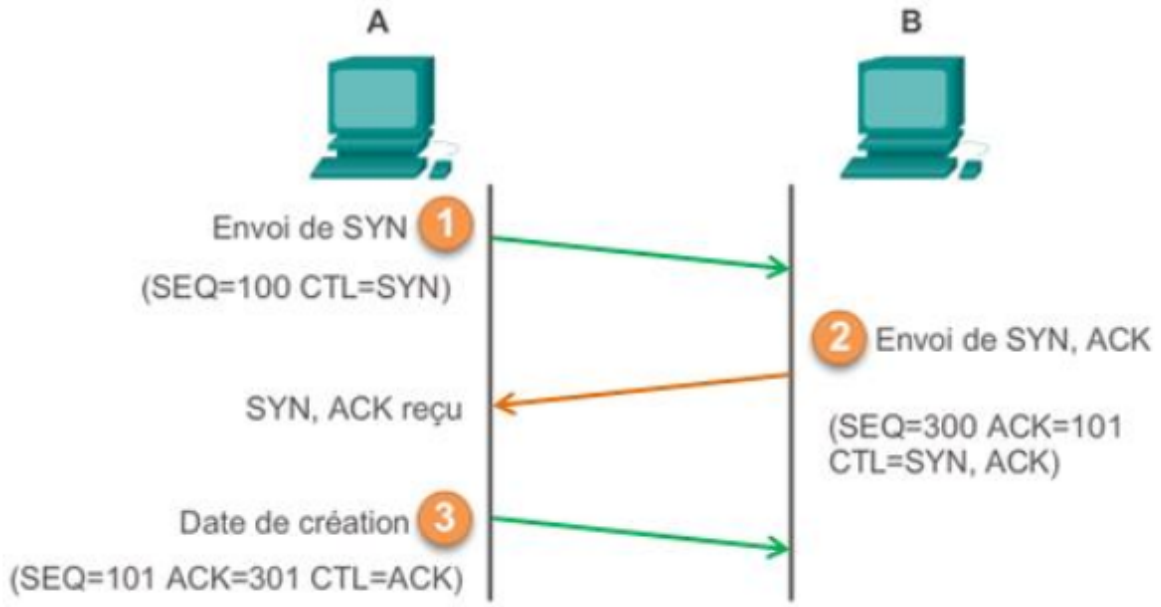
Etablissement d'une connexion TCP

1. Le client demande l'établissement d'une session client-serveur avec le serveur
Envoi d'une demande de synchronisation avec numéro de séquence
SYN avec un numéro de séquence (SEQ. Ex 100).
Champs de contrôle = SYN

2. Le serveur accuse réception de la session et demande l'établissement d'une session serveur-client
Réponse du serveur avec ACK égal au numéro d'ordre reçu +1 (ex : 101) et son numéro d'ordre de synchronisation (ex SEQ 300)

CTL = SYN

3. Le client accuse réception de la session serveur-client
Connexion établie, le client répond avec un ACK égal au numéro d'ordre reçu + 1.
SEQ = 101 ACK 301 CTL = ACK

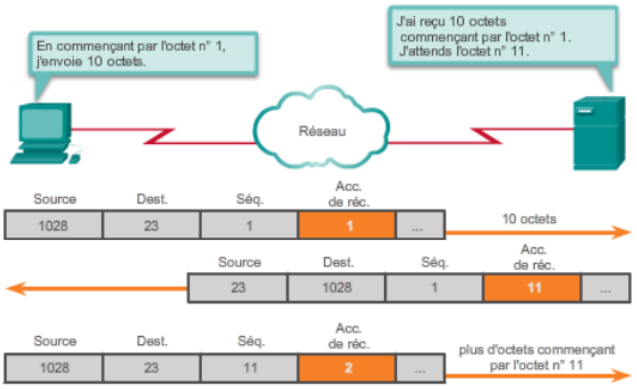


Fermeture d'une connexion TCP

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

Fiabilité de la connexion

Situation :



Le PC envoie un segment contenant 10 octets de données pour cette session et un numéro d'ordre égal à 1 dans l'en-tête.

Le serveur reçoit le segment au niveau de la couche 4 et détermine que le numéro d'ordre est 1 et qu'il y a 10 octets de données. Il renvoie alors un segment au PC pour accuser la réception de ces données. Dans ce segment, l'hôte définit le numéro ACK sur 11 pour indiquer que le prochain octet de données qu'il prévoit de recevoir dans cette session est l'octet numéro 11.

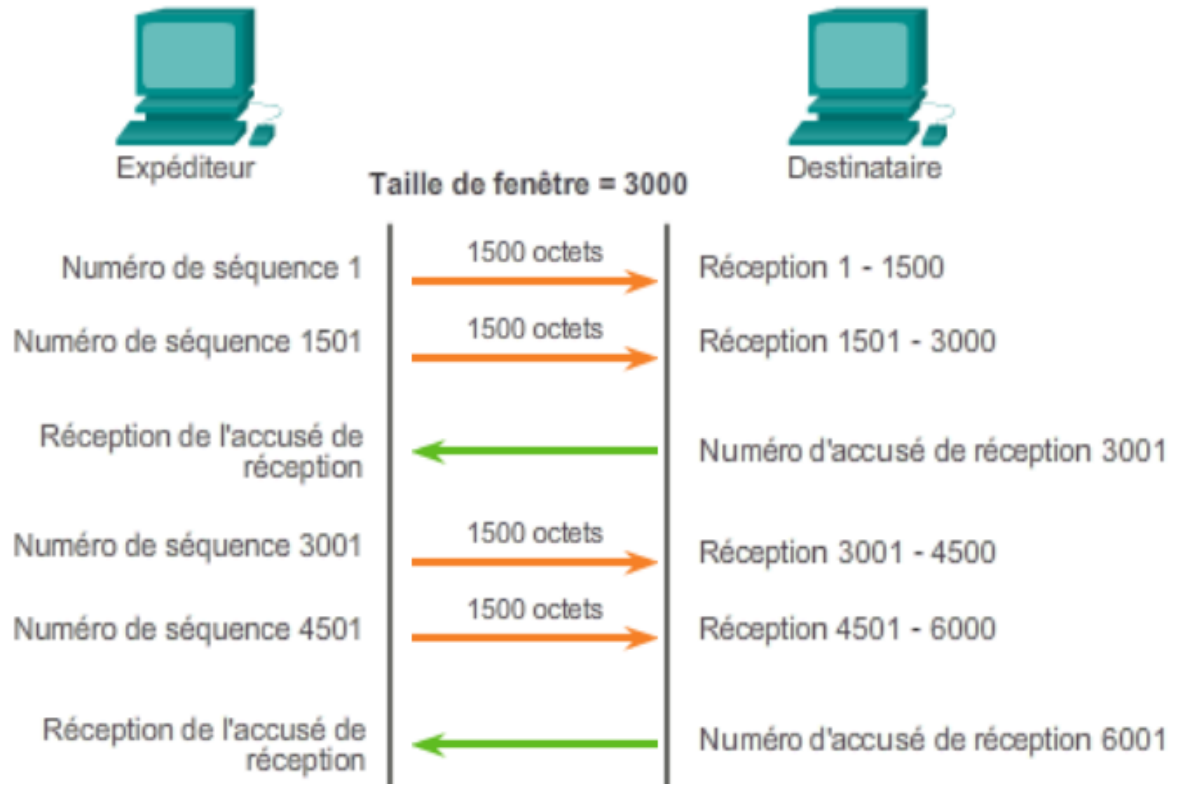
Le PC reçoit cet accusé de réception, il peut envoyer le segment suivant contenant des données pour cette session commençant par l'octet numéro 11.

La taille de fenêtre

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

Cette taille est définie lors du démarrage de la session

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

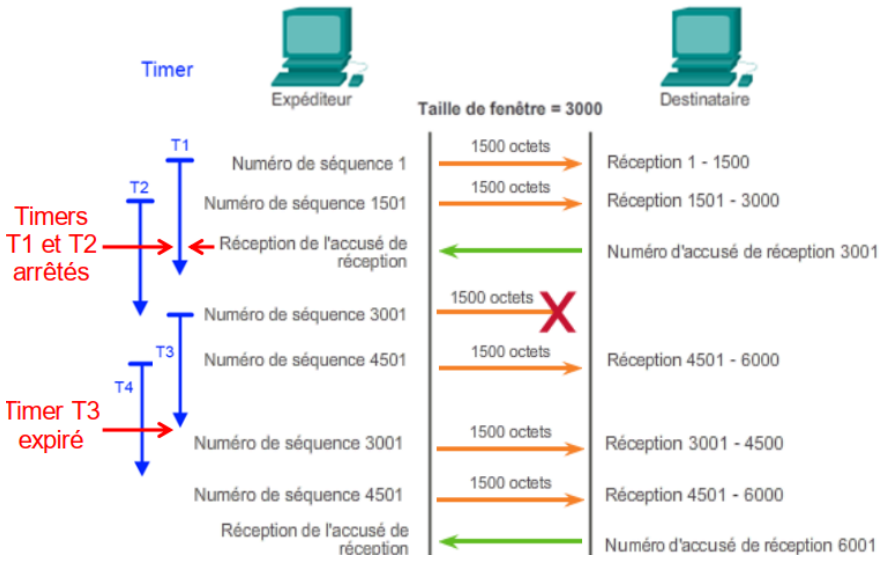


Cette valeur varie dynamiquement en fonction de la qualité de la transmission. Après une période sans perte de données ni contrainte sur les ressources, le destinataire commence à augmenter la taille de la fenêtre.

Gestion des pertes de segments du TCP

Quand le protocole TCP source envoie des segments de données, il va placer une copie du segment dans une file d'attente de retransmission
Et va déclencher en même temps un timer. Si il ne reçoit pas d'ACK avant la fin du timer, il va retransmettre à partir du dernier numéro d'accusé de réception

Il existe également des SACK (ACK sélectifs) permettant, si les 2 hôtes sont compatibles, une retransmission partielle des octets manquants.



Protocole de la couche application utilisant UDP

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

- DNS
- DHCP
- TFTP
- RIP
- VoIP

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

---

Chapitre 8: Adressage IP

Adressage IPv4

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

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

Elle contient deux parties:

- ID de réseau

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

- ID d'hôte

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

Les ≠ classes d'adresses

A: 8 bits partie réseau, 24 partie hôte
B: 16 bits réseau, 16 bits hôtes
C: 24 bits réseau, 8 hôtes
D: Réservées pour le multicast, TOUJOURS UNE ADRESSE DE DESTINATION
E: Réservées à la recherche ou à des usages futurs

Les adresses du bloc 168.254.0.0/16 sont des adresses link-local (c'est du réseau local APIPA)

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

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

Solution pour palier aux problèmes de l'IPv4

Le CIDR (Classless Inter-Domain Routing)

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

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

Technique calcul IP réseau/diffusion/hôtes

Coexistence IPv4 et IPv6

Techniques de migration vers l'IPv6

- Double pile

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

- Tunneling

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

- Traduction

Un paquet IPv6 est traduit en paquet IPv4 et inversement

Adressage IPv6

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

La notation décimale a été abandonée au profit d'une notation hexa

décimale où les 8 groupes de deux octets sont séparés par un signe ":"

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

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

La longueur de préfixe est utilisée pour indiquer la partie réseau d'une adresse IPv6, elle peut aller de 0 à 128

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

Adresse anycast
Adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques
Le périphérique le plus proche reçoit le paquet

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

Adresse de monodiffusion
Il existe 6 types mais voici les plus importants:

- Adresse de monodiffusion globale: idem que IPv4, un hôte à un destinataire
- Adresse link-local: utilisées pour communiquer avec d'autres périphériques sur la même liaison locale, uniquement utilisable en local plage FE80 ::/10

Chapitre 9: Découpage réseau

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

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

On divise un réseau selon les critères suivants:
- Taille
- Nombre d'hôtes par sous réseau
- Méthode d'attribution des adresses d'hôte
- Hôtes nécessitant des adresses IP statiques
- Hôtes pouvant utiliser le protocole DHCP

L'attribution des adresses ne doit pas être laissée au hasard, trois critères sont à prendre en compte:
- Eviter les doubles
- Assurer et contrôler l'accès
- Surveiller la sécurité et les performances

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

Comment découper un réseau correctement
- Toujours commencer par décomposer les réseaux en affectant les plages d'adresses les plus grandes en premier

- Quand on place un réseau plus grand que le précédent dans une plage, il faut sauter une certaine plage d'adresses

Exercice de découpage réseau

En tenant compte de:

Commercial

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

ASR: 195.208.192.0/25

Manufacture

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

ASR: 195.208.192.128/25

Marketing

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

ASR: 195.208.192.128/25

Info

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

ASR: 192.208.193.0/27

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

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

ASR: 195.208.193.64/27

Dirlo

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

ASR: 192.208.193.0/27

Secrétariat

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

ASR: 192.208.193.0/27

Compta

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

ASR: 192.208.193.200/29

RH

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

ASR: 192.208.193.0/27

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

Commercial: 195.208.192.0/25 => 2^(32-25) = 128 hôtes
Marketing + Manufacture: 195.208.192.128/25 => 2^(32-25) = 128 hôtes
Direction + Info + RH + Secrétariat: 192.208.193.0/27 => 2^(32-27) = 32 hôtes
R&D: 195.208.193.64/27 => 2^(32-27) = 32 hôtes
Comptabilité: 192.208.193.200/29 => 2^(32-29) = 8 hôtes

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

Segmentation IPv6

1 ère solution

2 ème solution

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

---

Chapitre 10: La couche application

Introduction

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

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

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

Le protocole HTTP

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

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

Il existe trois types de message courant:
- GET => requête cliente pour obtenir des données
- POST et PUT

Servent à uploader des fichiers de données vers le serveur Web

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

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

Caractéristiques du protocole HTTP
- Utilise TCP au port 80
- Stateless: le serveur ne maintient aucune info sur les requêtes des clients
- Non sécurisé => pas de chiffrement

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

Codes de statut
- 1xx: info
- 2xx: succès
- 3xx: redirection
- 4xx: erreurs du client
- 5xx: erreurs du serveur

Le cache
Lorsqu'une page ne subit pas de modification, elle est mise en cache
- Réduit le temps d'attente
- Réduit le trafic des réseaux

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

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

Les cookies
Permettent au serveur de mémoriser des données du côté client

Les protocoles Email
SMTP
Permet de transférer les e-mails de manière fiable et efficace.
Port:
- 25 sans chiffrement
- D'autres avec chiffrement

POP3
Port: 110
Permet à ordinateur de récupérer des e-mails à partir d'un serveur de messagerie.
L'email est téléchargé du serveur au client puis supprimé du serveur

IMAP
143 ou 220 selon la version
Des copies des mesages sont téléchargées vers l'application cliente
Les messages originaux sont conservés sur le serveur jusqu'à ce qu'ils soient supprimés manuellement.

DNS
Service de nom de domaine, associe les noms des ressources à l'adresse réseau numérique requise.
=> Associe un domaine à une IP

DHCP
Port:
- Serveur 67
- Client 68

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

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

FTP
Permet le transfert de données entre un client et un serveur, port 20 et 21
Existe en version simplifiée appelée TFTP, (pas sécurisé), port 69