

**Institut supérieur d'informatique et mathématique de
Monastir**

L1 info

Cours fondements des réseaux

Enseignante : Dr zeineb SADEK

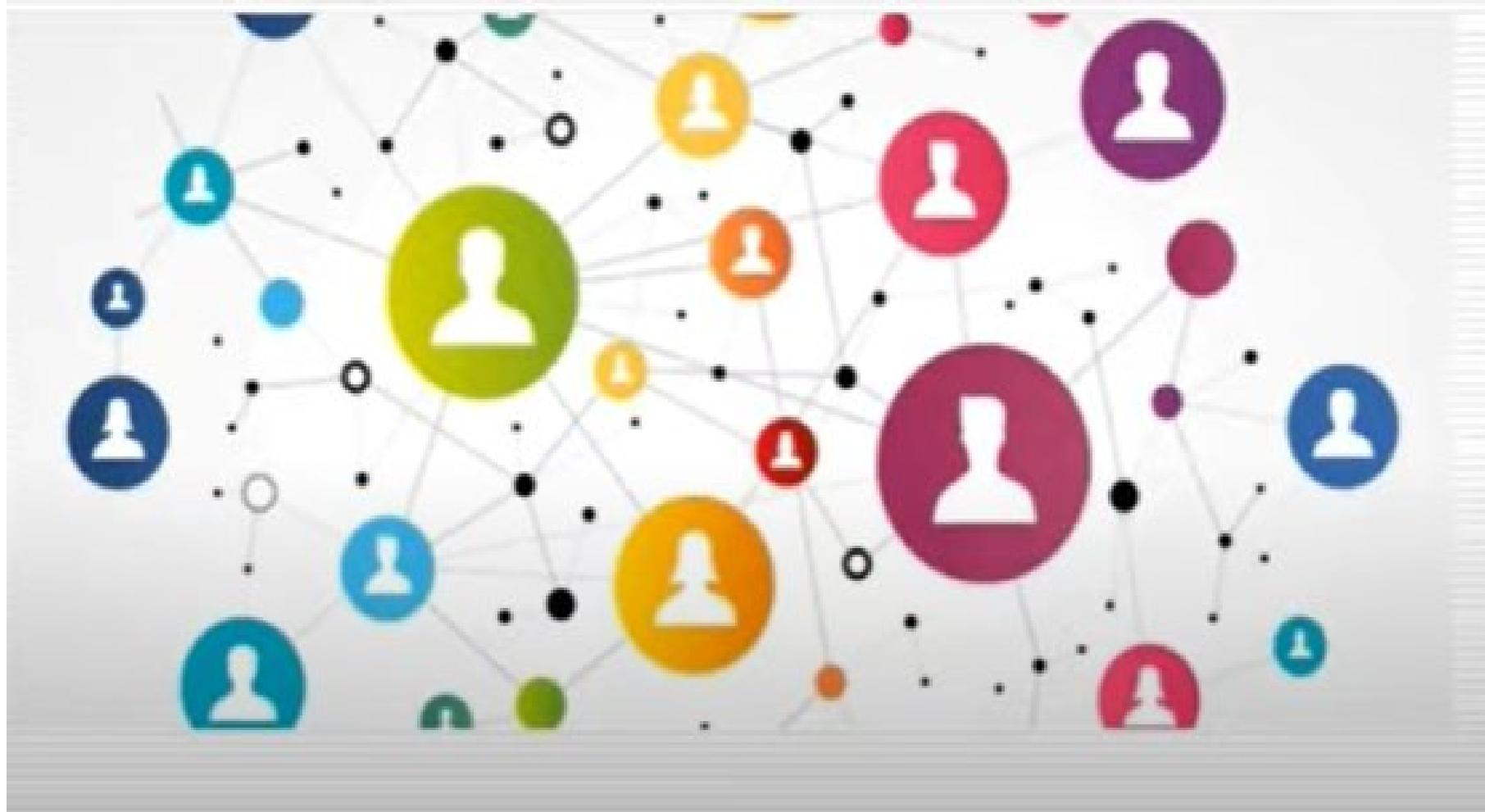
Programme : grands titres

- 1 Généralité sur réseaux informatique
- 2 Modèle de référence OSI
- 3 Modèle TCP/IP: couche accès réseau
- 4 Couche réseau (adressage et routage)

Généralité sur les réseaux informatiques

- Besoin de communication aujourd'hui
- Réseaux informatique
- Types de réseau
 - Topologie réseau
 - L'équipement réseau
 - Architecture des réseaux
 - Les Protocoles

BESOIN DE COMMUNICATION



BESOIN DE COMMUNICATION

- ✓ Industrie, militaire, médicale, chimie,, etc
- ✓ Entreprise (administration)
- ✓ Internet (le réseau des réseaux)

Industrie, militaire , médicale, chimie, ,,, etc



Militaire

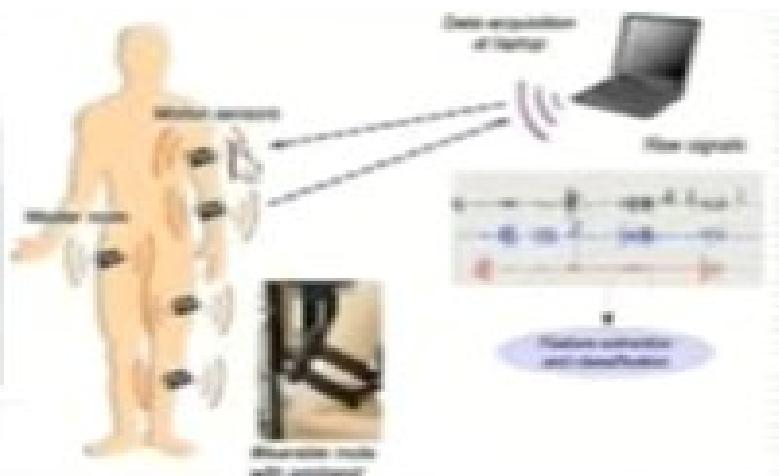


Secours



Wifi étendu

Industrie, militaire , médicale, chimie, ,,, etc



Monitoring médical



Tracking militaire



Feux de forêt



Surveillance des volcans

□ Partage des ressources

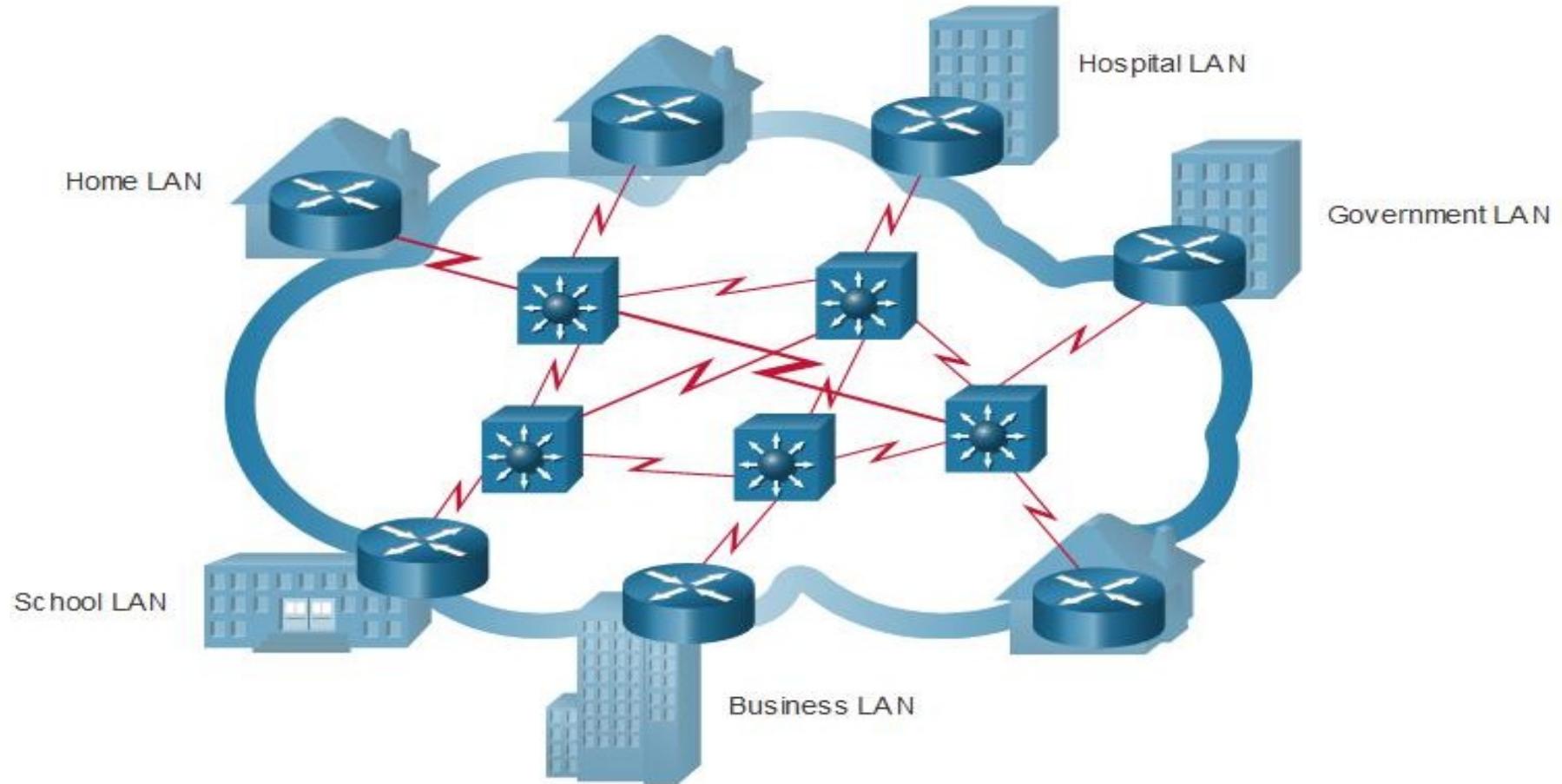
- Partager et transférer des ressources : fichier, dossier, imprimantes,.....
- Partager des applications: compilateur, système de gestion de base de données
- Partager les puissances de calcul

□ Grande fiabilité

□ Réduction de couts

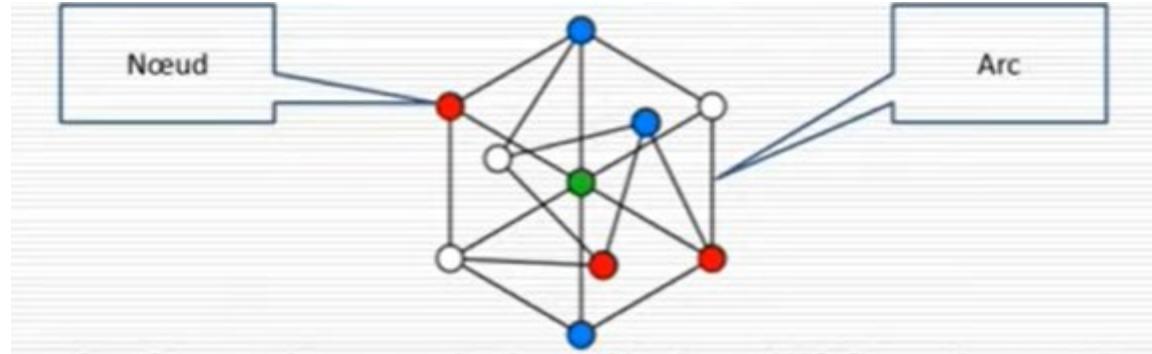


Internet



Un réseau désigne **un ensemble d'équipements interconnectés pour permettre la communication de données entre applications, quelles que soient les distances qui les séparent.**

Réseaux informatique



- **Arc** : support de transmission: cable réseau, wifi, fibre optique , satellite
- **Nœud** : peut être :
- **Equipement de communication**: pc, smartphone, capteur, puce brat robot ou
- **Equipement d'interconnexion** : répéteur, hub, switch, routeur firewall, point d'accès wifi, ect

Caractéristiques de réseau informatique

Les caractéristiques de base d'un réseau sont :

- La **topologie** qui définit l'architecture d'un réseau : on distinguera la **topologie physique** qui définit la manière dont les équipements sont interconnectés entre eux, de la **topologie logique** qui précise la manière dont les équipements communiquent entre eux.
- Le **débit** exprimé en bits/s (ou bps) qui mesure une quantité de données numériques (bits) transmises par seconde (s).
- La **distance maximale** (ou portée) qui dépend de la technologie mise en oeuvre.
- Le **nombre de noeuds** maximum que l'on peut interconnecter.

Composantes du réseau

Rôles des hôtes

Chaque ordinateur d'un réseau est appelé un hôte ou un périphérique final.

Les serveurs sont des ordinateurs qui fournissent des informations aux appareils terminaux :

- Serveurs de messagerie
- serveurs Web
- serveur de fichier

Les clients sont des ordinateurs qui envoient des demandes aux serveurs pour récupérer des informations :

- page Web à partir d'un serveur Web
- e-mail à partir d'un serveur de messagerie



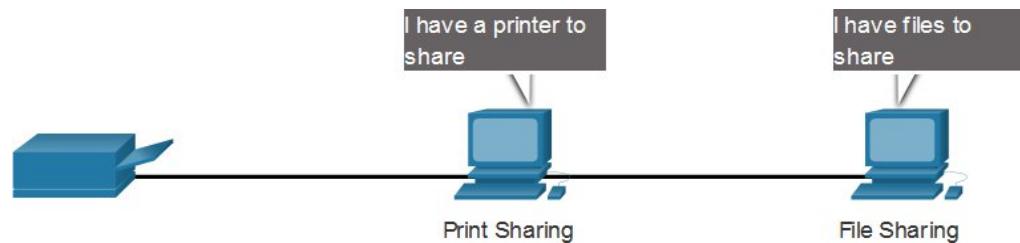
Server Type	Description
E-mail	Le serveur de courrier électronique fait fonctionner un logiciel de serveur de courrier électronique. Les clients utilisent un logiciel client pour accéder à la messagerie électronique.
Sécurité du	Le serveur Web exécute le logiciel de serveur Web. Les clients utilisent un logiciel de navigation pour accéder aux pages Web.
Fichier	Le serveur stocke les fichiers des utilisateurs et de l'entreprise. Les périphériques clients accèdent à ces fichiers.

©2021 Cisco et/ou ses filiales. Tous droits réservés. Informations confidentielles

13

Peer-to-Peer

Il est possible qu'un périphérique soit un client et un serveur dans un réseau Peer-to-Peer. Ce type de conception de réseau n'est recommandé que pour les très petits réseaux.



Avantages	Inconvénients
Facile à configurer	Pas d'administration centralisée
Moins complexe	Peu sécurisé
Réduction des coûts	Non évolutif
Utilisé pour des tâches simples : transfert de fichiers et partage d'imprimantes	Performances plus lentes

Classifications des réseaux

Deux classification:

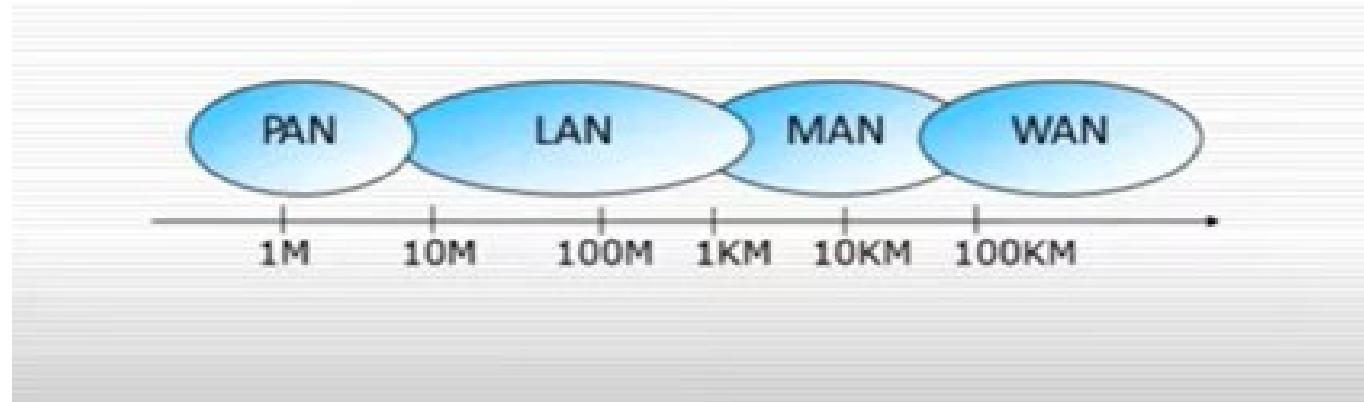
Leurs tailles :

PAN, LAN, MAN, WAN,

Leurs topologies :

Bus, anneau, étoile,

Classifications, selon la taille



Types de réseaux : par

Les réseaux informatiques peuvent être classés suivant leur portée :

Un réseau personnel ou (Personal Area Network, **PAN**) désigne un type de réseau informatique restreint en matière d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres. D'autres appellations pour ce type de réseau sont : réseau domestique ou réseau individuel.

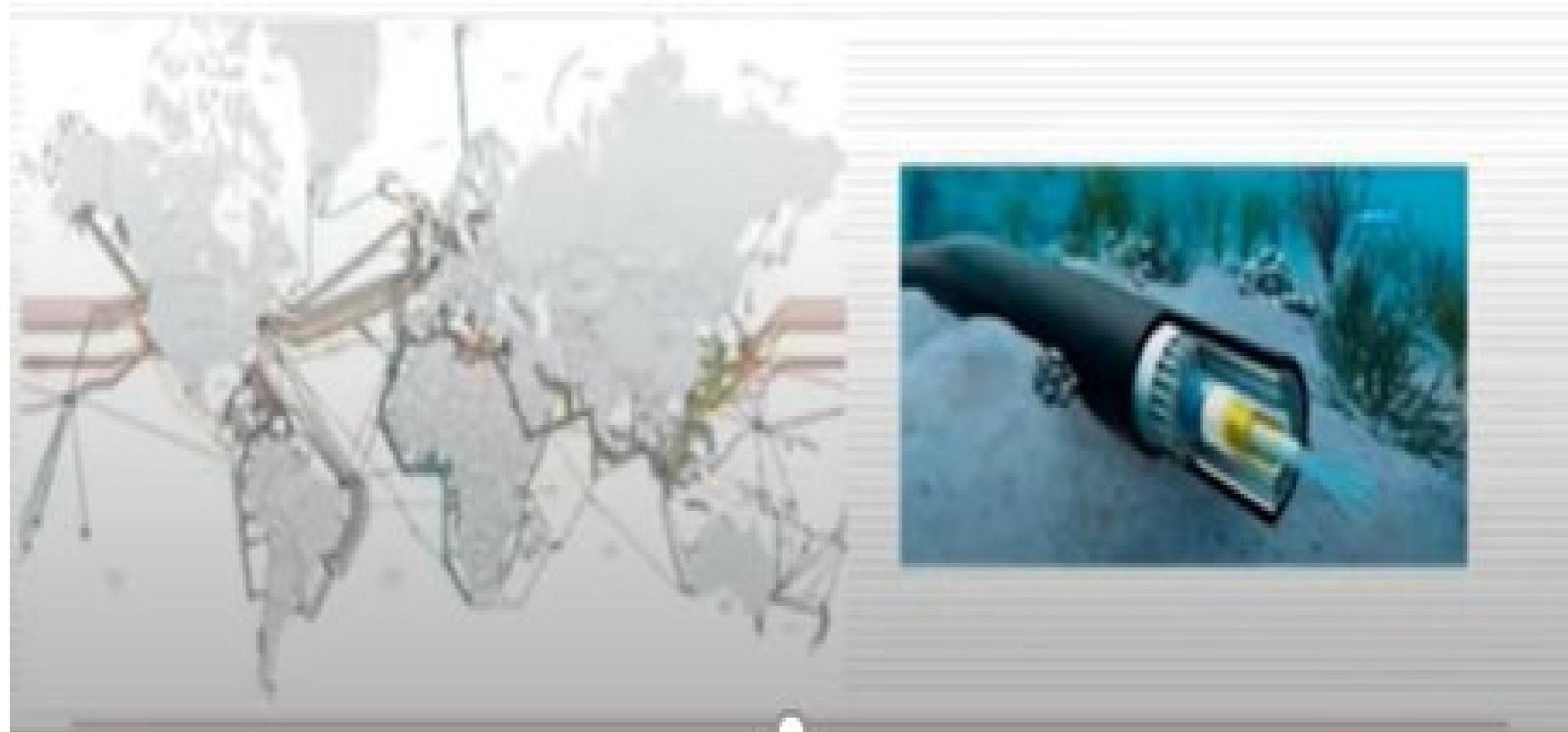
Les réseaux locaux ou **LAN** (*Local Area Network*) correspondent aux réseaux intra-entreprise (quelques centaines de mètres et n'exèdent pas quelques kilomètres), généralement réseaux dits "privés". Le réseau de votre établissement est un réseau de type LAN.

Types de réseaux : par

Un réseau métropolitain (**MAN**) est un réseau informatique qui relie des ordinateurs au sein d'une zone métropolitaine, qui peut être une seule grande ville, plusieurs villes et villages, ou toute autre grande zone comportant plusieurs bâtiments. Un MAN est plus grand qu'un réseau local (LAN) mais plus petit qu'un réseau étendu (WAN). Les MAN ne doivent pas nécessairement se trouver dans des zones urbaines ; le terme "métropolitain" implique la taille du réseau, et non la démographie de la zone qu'il dessert.

Les réseaux grandes distances ou **WAN** (Wide Area Network) sont des réseaux étendus, généralement réseaux dits "publics" (gérés par des opérateurs publics ou privés), et qui assurent la transmission des données sur des longues distances à l'échelle d'un pays ou de la planète. Internet est un réseau de type WAN.

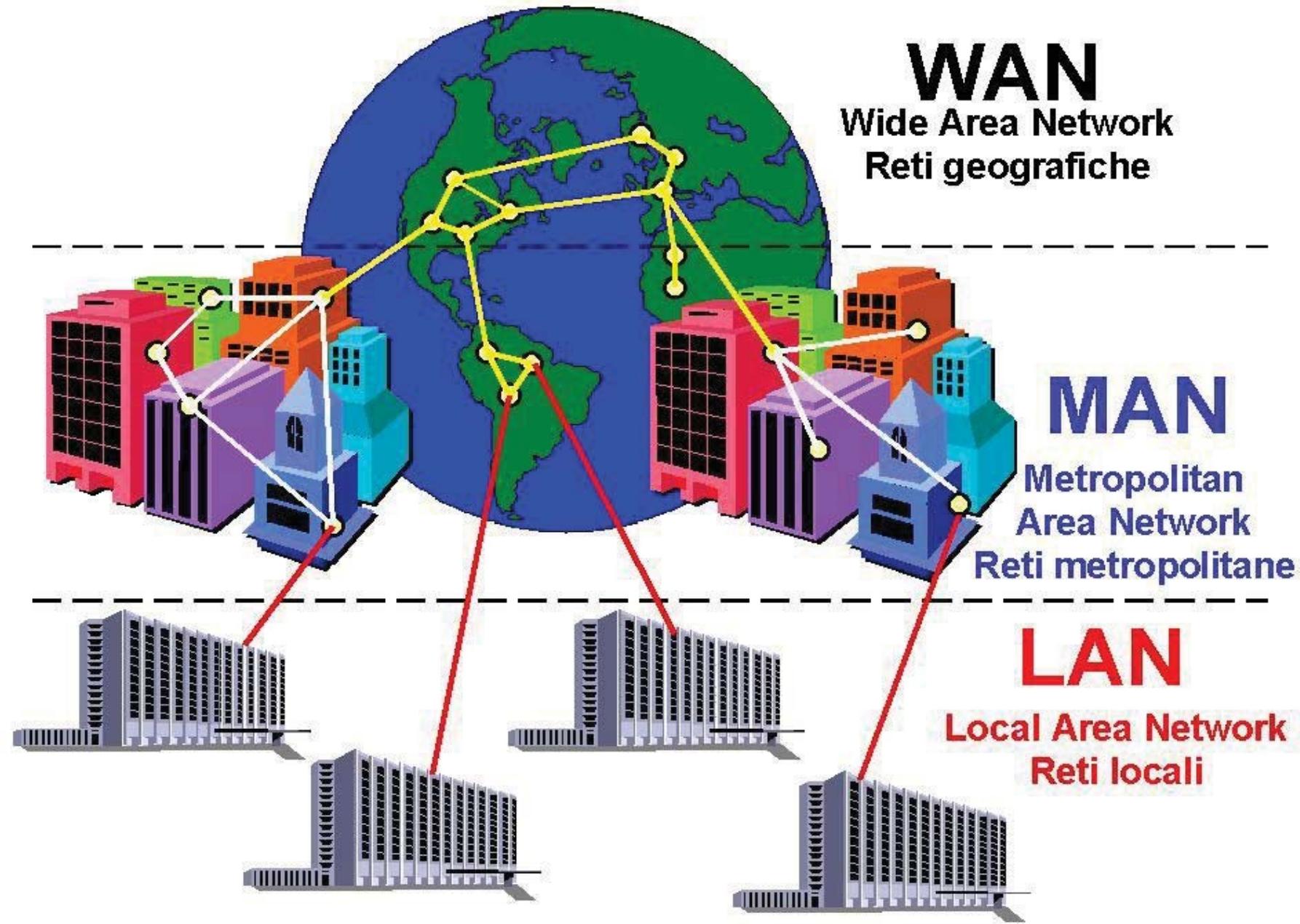
Les **GAN** utilisent les infrastructures de fibre optique des réseaux étendus (WAN) et combinent ces dernières avec des câbles sous marins internationaux ou transmissions par satellite,



WAN
Wide Area Network
Reti geografiche

MAN
Metropolitan
Area Network
Reti metropolitane

LAN
Local Area Network
Reti locali



Types de réseaux : par utilisation

Les réseaux informatiques peuvent être classés en fonction de leurs utilisations et des services qu'ils offrent.

Ainsi, pour les réseaux utilisant la famille des protocoles TCP/IP, on distingue :

Internet : le réseau des réseaux interconnectés à l'échelle de la planète, permet d'échanger des fichiers , des messages et d'accéder au web

Intranet : le réseau interne d'une entité organisationnelle (réseaux privés)

Extranet : le réseau externe d'une entité organisationnelle (une entreprise est toujours souhaité à communiquer avec des organisations qui sont extérieur de sa structure par exemple des clients , des fournisseurs , des partenaires) (accès web sécurisé)

Types de réseaux : par topologie

Ils peuvent également être catégorisés par topologie de réseau :

- **Réseau en étoile** : les équipements du réseau sont reliés à un équipement central. En pratique, l'équipement central peut être un concentrateur (hub), un commutateur (switch) ou un routeur (router).
- **Réseau en bus** : l'interconnexion est assurée par un média partagé entre tous les équipements raccordés.
- **Réseau en anneau** : les équipements sont reliés entre eux par une boucle fermée.

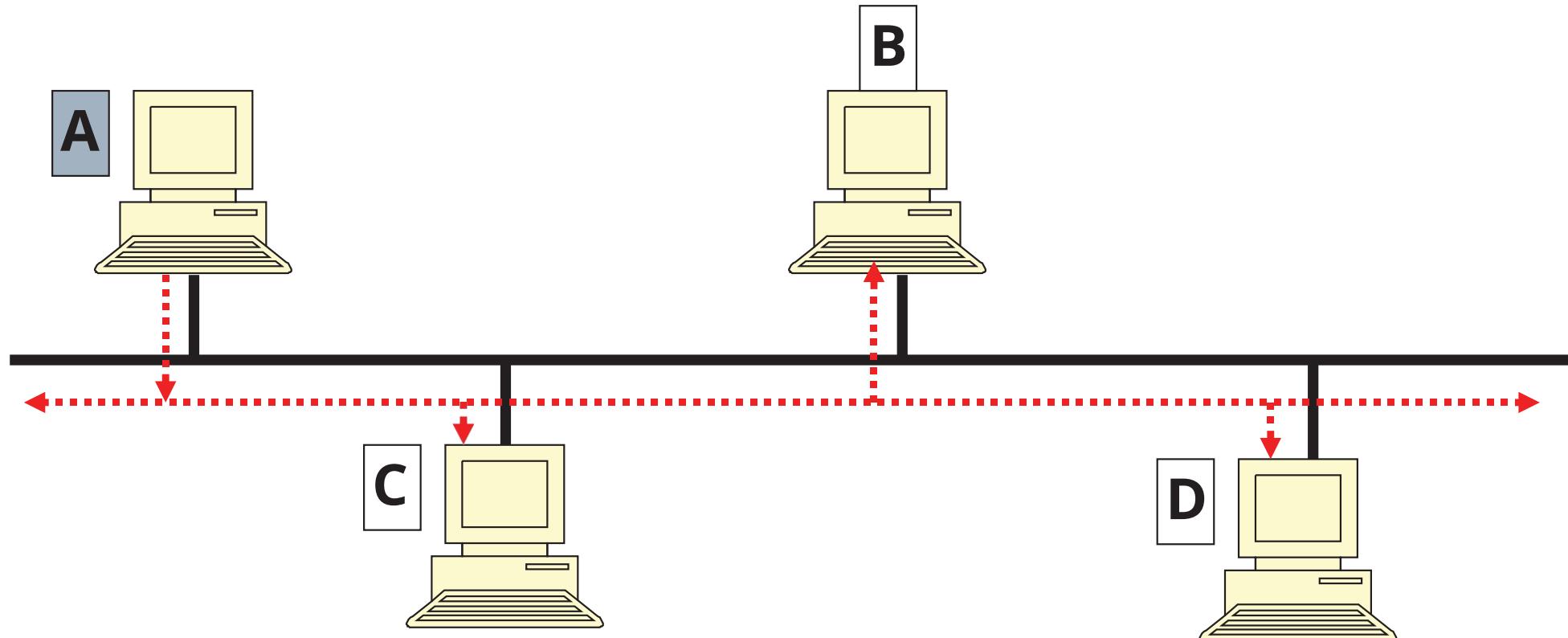
La topologie en bus

- **Les ordinateurs sont connectés les uns à la suite des autres le long d'un seul câble appelé segment**
- **Manière de communiquer basée sur les concepts :**
 - émission du signal (diffusion)
 - terminaison(bouchon) pour absorber les signaux libres



Types de réseaux : par topologie

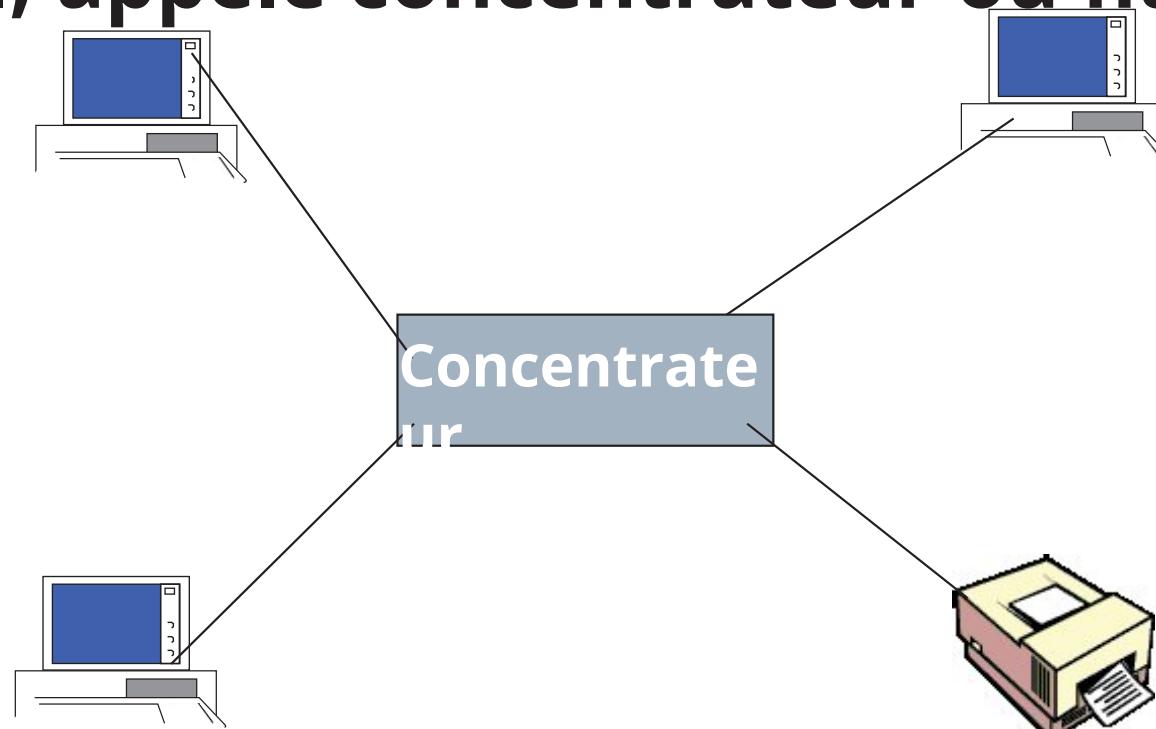
Le bus



A émet
B,C,D reçoivent

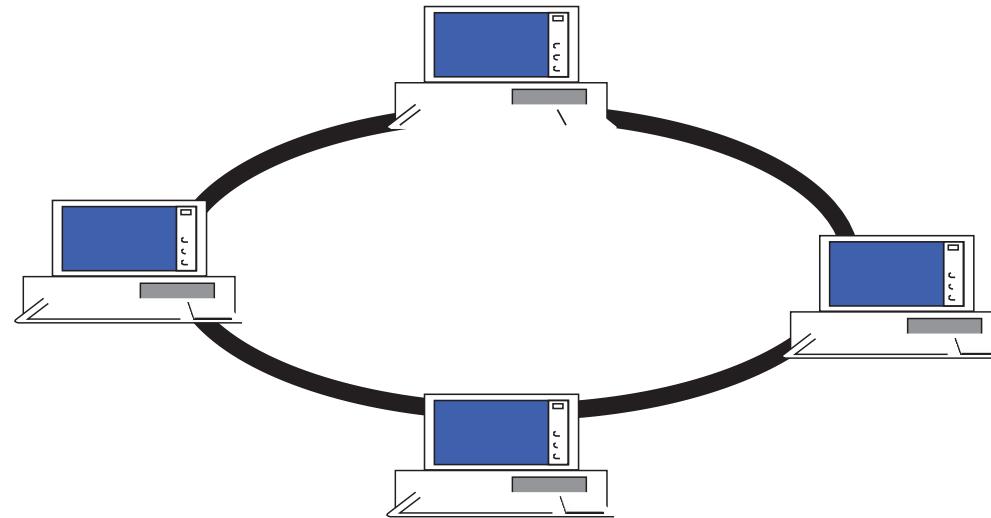
La topologie en étoile

- Les ordinateurs sont connectés par des segments de câble à un composant central, appelé concentrateur ou hub

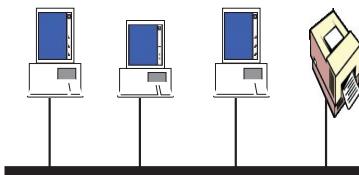
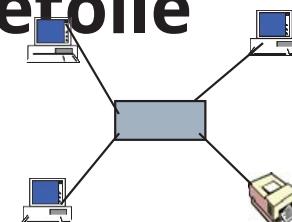
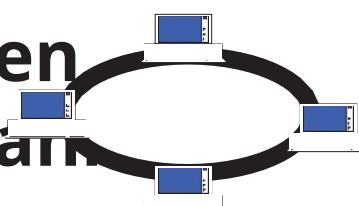


La topologie en anneau

- Dans cette architecture, les ordinateurs sont reliés sur une seul boucle de câble et communiquent chacun à leur tour



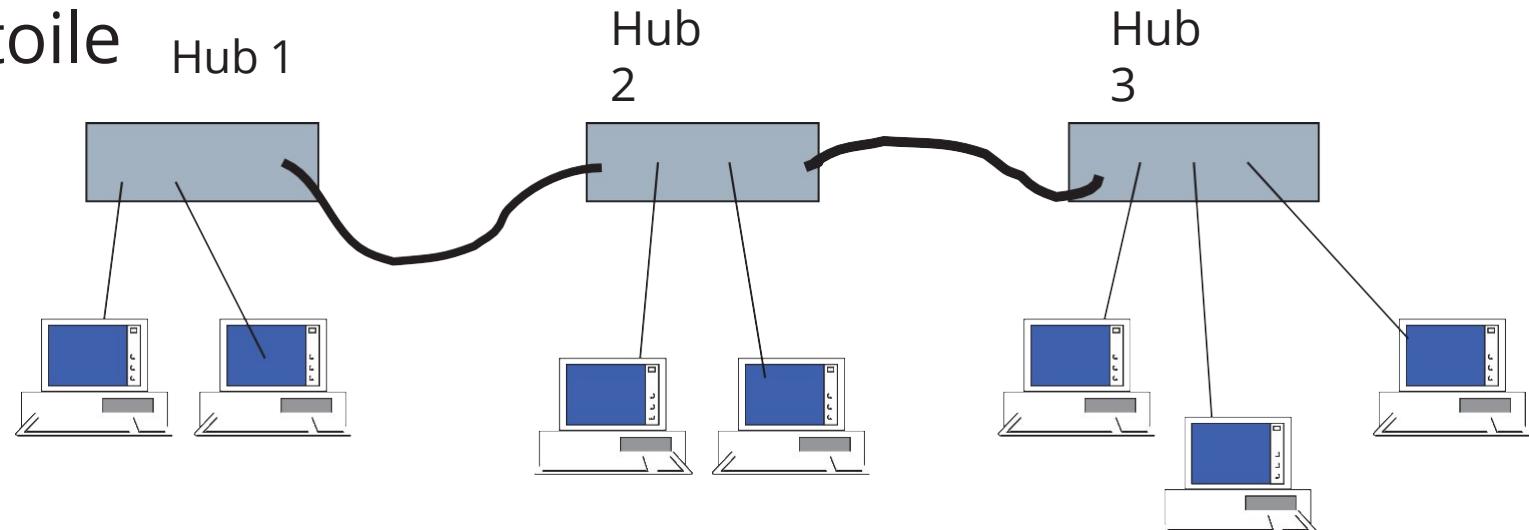
- Les signaux se déplacent le long de la boucle dans une direction et passe par chacun des ordinateurs

	avantage	inconvénients
Topologie en bus	<ul style="list-style-type: none"> - facile à mettre en œuvre - fonctionnement facile 	<p>Si l'une des connexions est déommagée l'ensemble du réseau est</p>
Topologie en étoile	<ul style="list-style-type: none"> - Si un câble tombe en panne, seul cet ordinateur est isolé du reste du réseau 	<p>plus de câbles</p> <p>- le point central</p>
Topologie en anneau	<p>Bon niveau de sécurité</p> 	<ul style="list-style-type: none"> - plus de câbles - la panne d'une seule machine isole les autres

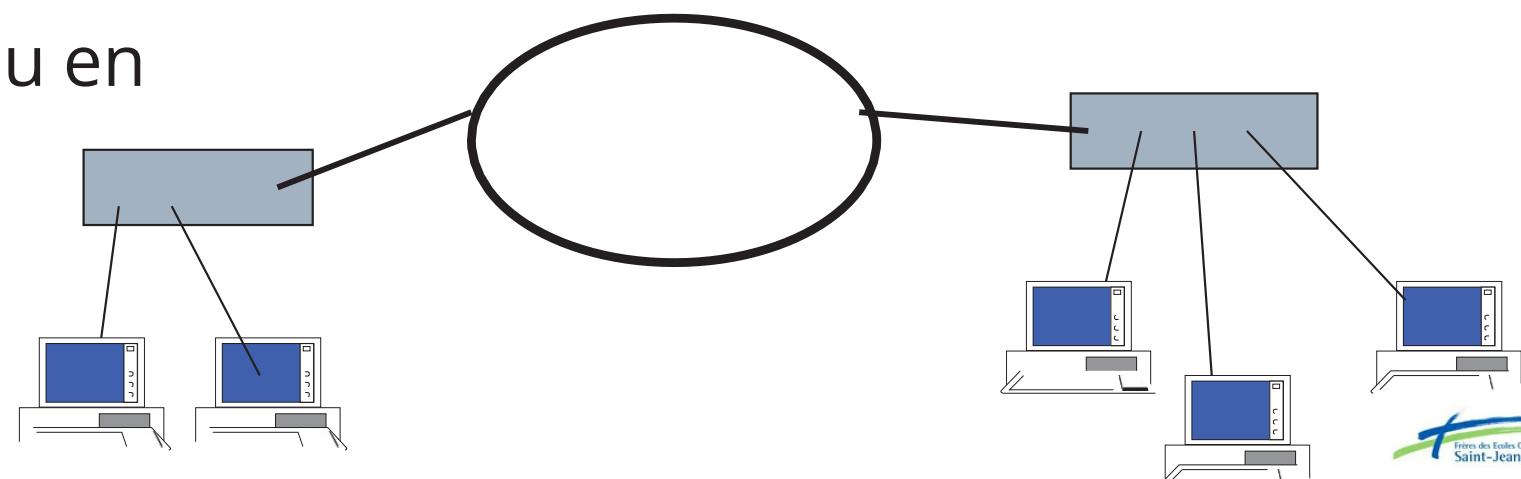
Types de réseaux : par topologie

Variantes des topologies

- Bus en étoile



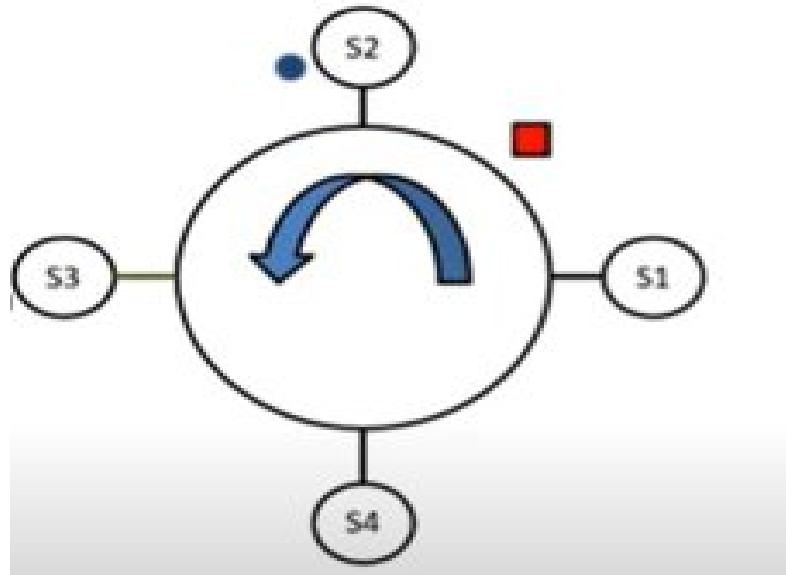
- Anneau en étoile



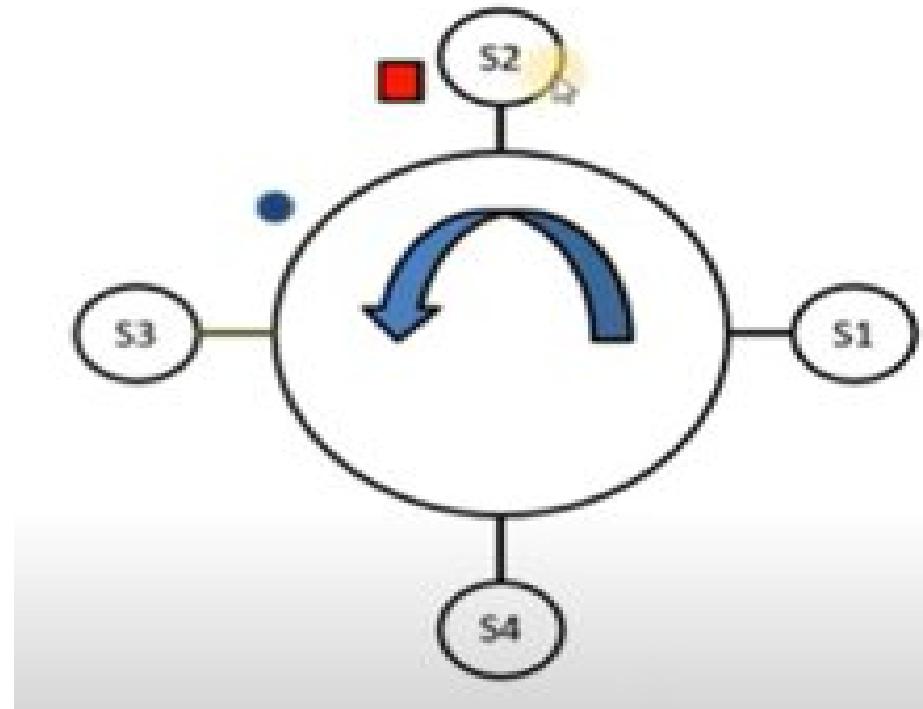
L'Ethernet classique

- Origine: crée par Xerox en 1970
- Technologie de réseau local basé sur la détection de collision
- La communication se fait à l'aide d'un protocole appelé **CSMA/CD** (*Carrier Sense Multiple Access with Collision Detect*) ce qui signifie qu'il s'agit d'un protocole d'accès multiple avec surveillance de porteuse et détection de collision
- Standard IEEE 802.3

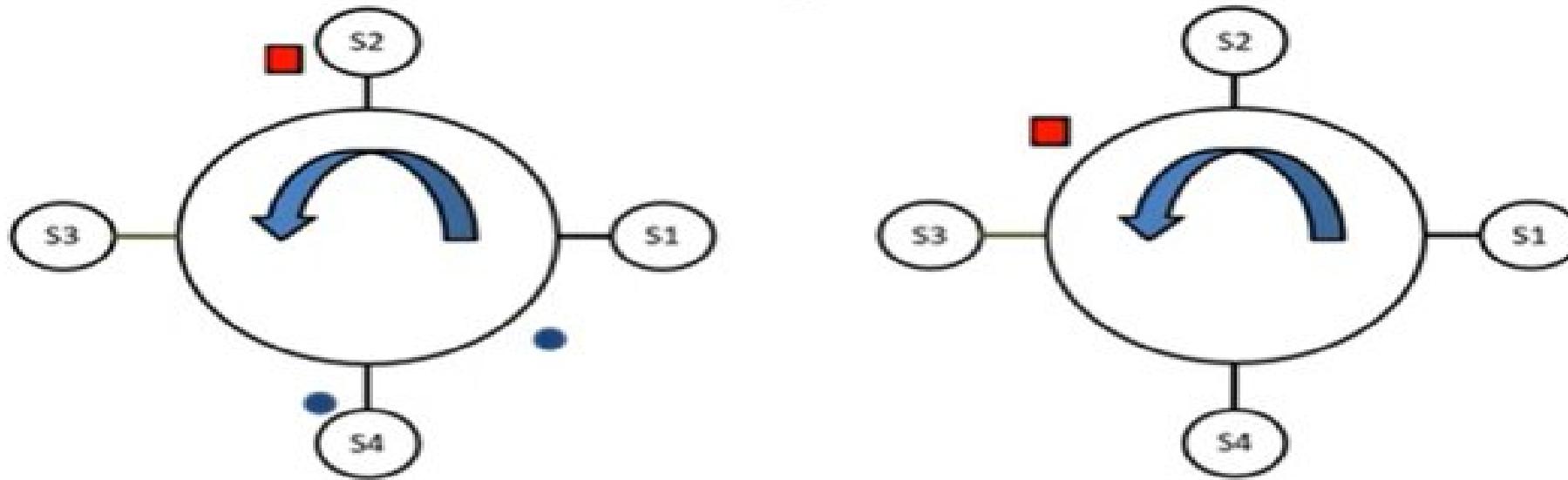
Token-Ring



la station s2 veut émmèter une trame vers la station s4, elle doit attendre la passage par jeton



la station détient le jeton et envoi le trame doit passer par la station s3, s3 doit la retransmettre à la station s4



La station s4 reçoit la trame, elle garde une copie et laisse passer une copie

La station s2 reçoit la trame qu'elle a envoyée, donc elle libère le jeton et détruit la trame,
Le jeton peut être par la suite récupéré par n'importe quelle autre station.

Token-Ring

- Origine : IBM puis normalisé 802.5
- Technologie anneau à jeton
- de 4 à 16 Mbps
- - - - :
 - Cher : coût par équipement trois à six fois plus cher
 - Sécurité

Comparaison la technologie Ethernet et la technologie token ring

Ethernet	token ring
Topologie physique de type bus et de type étoile	Topologie physique de type anneau et de type étoile
Accès CSMA/CD	Accès par jeton
Paire torsadé , câble coaxial, fibre optique	Torsadées et rarement la fibre optique
Risque de collision	Pas de collision
Débit de 10 à 100 M bit/s	Débit de 4 ou 16 M bit/s

Exercice 1

Q1 :Un employé d'une filiale établit un devis pour un client. Pour ce faire, il doit accéder à des informations confidentielles de prix sur les serveurs internes du siège. À quel type de réseau l'employé pourrait-il accéder ?

- Un réseau local
- Un intranet
- Un extranet
- sur Internet

Q2 :Quelles sont les ressources partageables dans un réseau ?

Q3 : Quelle est la différence entre la topologie logique et la topologie physique ?

Q4: Quelle est la topologie logique du hub ainsi que du commutateur ?

Q5: Répondre par vrai ou faux

L'architecture client/serveur est un mode de communication dans lequel on distingue un client parmi plusieurs serveurs.



Le réseau d'un bâtiment est appelé réseau domestique



Correction

Un employé d'une filiale établit un devis pour un client. Pour ce faire, il doit accéder à des informations confidentielles de prix sur les serveurs internes du siège. À quel type de réseau l'employé pourrait-il accéder ?

- Un réseau local
- Un intranet
- Un extranet
- sur Internet
- Quelles sont les ressources partageables dans un réseau ?

Les fichiers

Les applications

Les périphériques comme des imprimantes,
un scanner, un modem

Quelle est la différence entre la topologie logique et la topologie physique ?

Dans les réseaux locaux, on distingue la topologie physique qui indique comment les différentes stations sont raccordées physiquement (câblage), de la topologie logique qui décrit comment est distribué le droit à parole.

Quelle est la topologie logique du hub ainsi que du commutateur ?

CSMA/CD (*Carrier Sense Multiple Access with Collision Detect*) / Point-à-point

Répondre par vrai ou faux

L'architecture client/serveur est un mode de communication dans lequel on distingue un client parmi plusieurs serveurs.

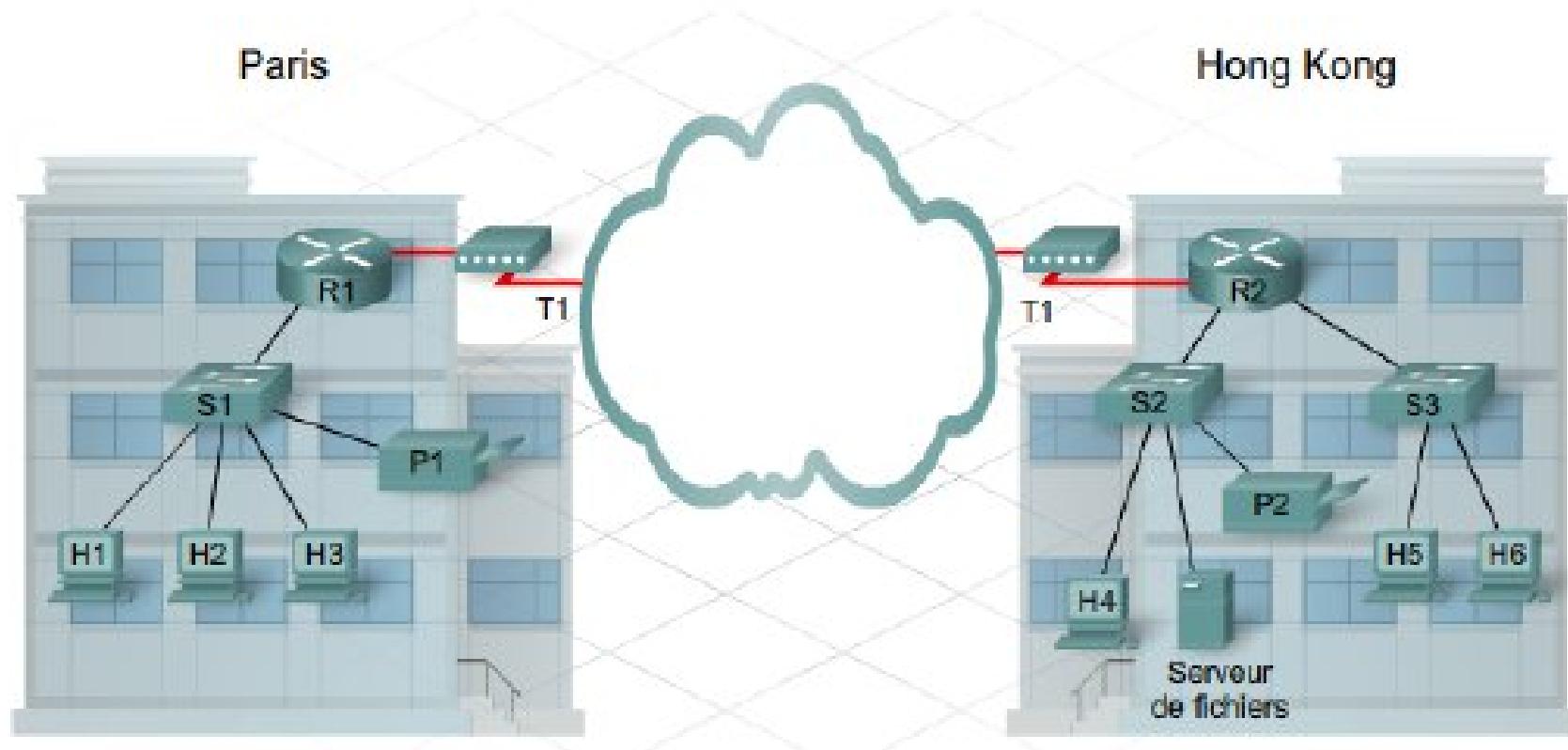
Faux

Le réseau d'un bâtiment est appelé réseau domestique

Faux

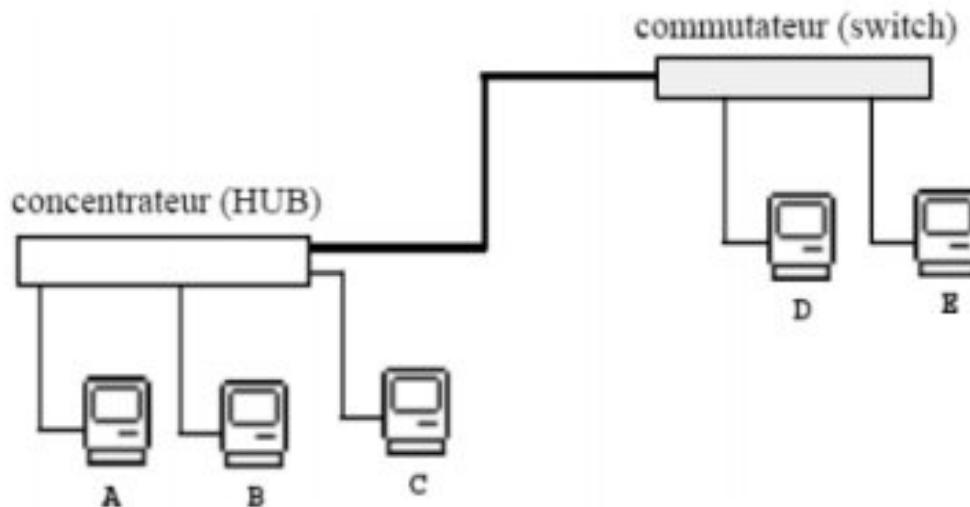
Exercice 2

Une entreprise dispose d'une agence à Paris et d'une agence à Hong-Kong. Ces deux sites communiquent entre eux (téléphone et données). Sur le schéma ci-dessous, repérer les zones LAN , WAN, et GAN .



EXERCICE 3

Soit le réseau suivant :



1. Quelles sont les topologies physiques et logiques existantes ?
2. Quelles sont les catégories de composants réseaux existants ?
3. Quel est le type de câble utilisé pour relier le concentrateur au commutateur ?
4. Si un paquet de diffusion est émis par la machine A, quelles machines recevront ce paquet ?
5. Si un paquet est émis par la machine A en direction de la machine C, quelles machines recevront ce paquet ?
6. Si un paquet est émis par la machine A en direction de la machine E, quelles machines recevront ce paquet ?

L'équipement réseau

1. Câblage réseau
2. Cartes réseau
3. Les éléments actifs

1- Câblage réseau: support physique

- **Les câbles sont destinés au transport de données numériques**
- **Le choix d'un câblage nécessite la réponse aux questions suivantes:**
 - **Quel est le volume de trafic sur le réseau ?**
 - **Quels sont les besoins en matière de sécurité ?**
 - **Quelle distance devra couvrir le câble ?**
 - **Quels câbles peuvent être utilisés ?**
 - **Quel est le budget prévu pour le câblage ?**



Câbles utilisés :

Câble coaxial

- Câble coaxial fin (Thinnet)
- Câble coaxial épais (Thicknet)

Fibre optique

Paire torsadée

- paire torsadée non blindée
- paire torsadée blindée

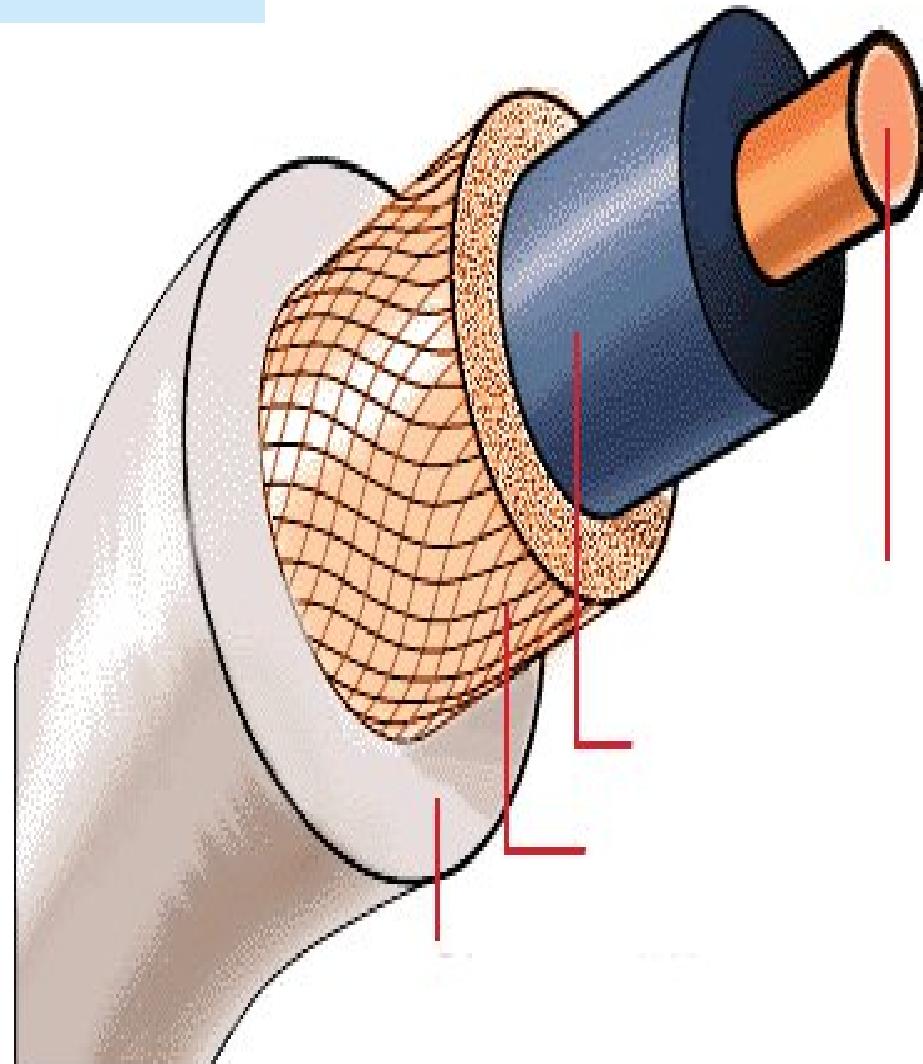
Câble coaxial

- Composé d'une partie « âme », d'une enveloppe isolante, d'un blindage métallique tressé et d'une gaine extérieure

Deux types :

- Câble coaxial fin (Thinnet)
10Base2

Câble coaxial épais (Thicknet)
10Base5





1001

BNC plug to BNC plug, moulded type,
RG-58U coaxial cable.



**Connecteur en T pour l'interconnexion
entre les
différents câbles réseau**

câble coaxial fin

- Diamètre = 6 mm
 - Distance maximale = 185 m
 - Fait partie de la famille RG-58 /U
 - Impédance = 50 ohms
 - RG-58 A/U
 - RG-58 C/U 58 A/U
 - RG-59 câble)
 - RG-6
- Brin central en Cu à un fil Brin central torsadé
- Spécification militaire du Transmission à large bande (TV par
- Diamètre plus large que RG-59

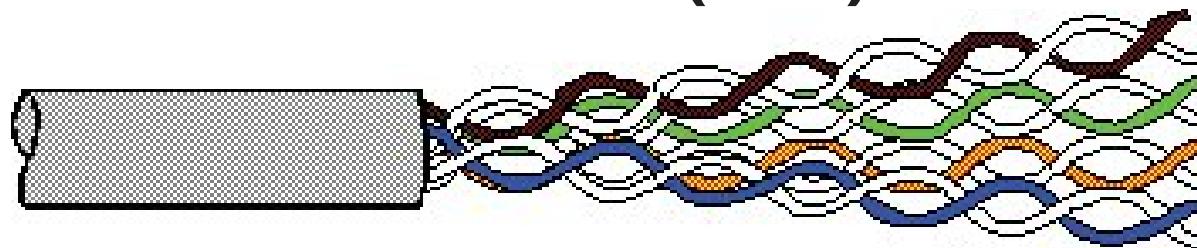


Câble coaxial épais

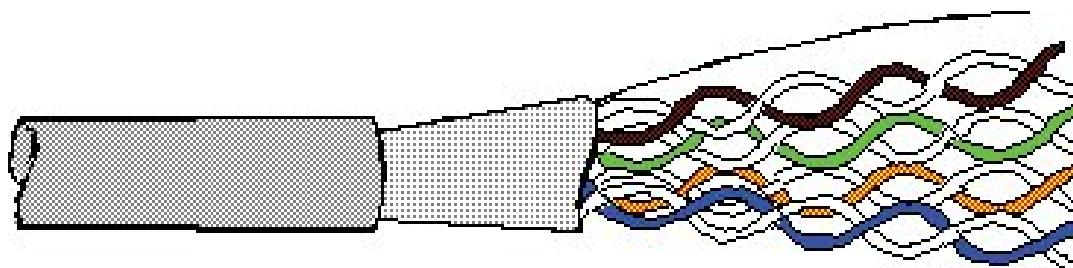
- **Diamètre = 12 mm**
- **Souvent désigné comme le standard Ethernet**
- **Longueur maximale = 500 m**
- **Il est plus difficile à plier et par conséquent à installer**

Paire torsadée

- **Une paire torsadée est constituée de deux brins torsadés en cuivre, protégés chacun par une enveloppe isolante**
- **On distingue;**
 - **paire torsadée non blindé (UTP)**
 - **paire torsadée blindée (STP)**



- **paire torsadée blindée (STP)**



les types de câbles paires torsadés:

- **10BaseT (10Mbits/s)**
- **100BaseTX (100Mbits/s)**

Les connecteurs utilisés ont la référence Rj45



**Connecteur
RJ45**

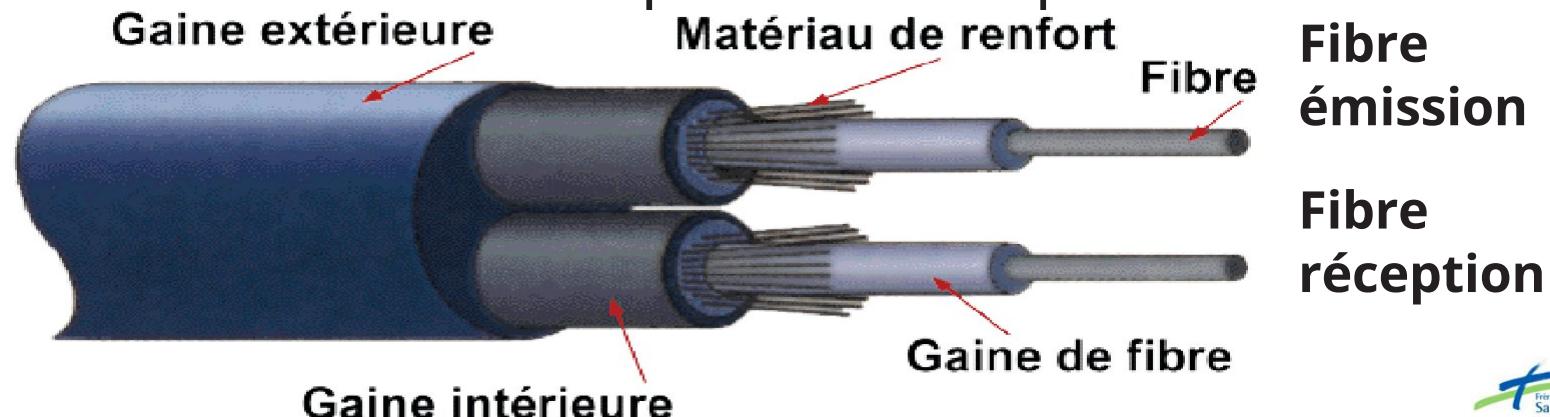
Câble UTP (10BaseT)

- Longueur maximale = 100 m
- Composition: 2 fils de cuivre recouverts d'isolant
- Normes UTP: incluent 5 catégories de câbles
 - catégorie 1: fil téléphonique standard
 - catégorie 2: quatre paire torsadées pouvant transporter des données à 4 Mb.s
 - catégorie 3: quatre paires torsadées avec 3 torsions par pied. Débit maximum = 10 Mb/s
 - catégorie 4: quatre paires torsadées. Débit maximum = 16 Mb/s
 - catégorie 5: quatre paires torsadées. Débit maximum = 100 Mb/s



Fibre Optique

- La fibre est constituée d'un cylindre en verre fin, appelé brin central, entouré d'une couche de verre appelé gaine optique.
- Elles véhiculent des signaux sous forme d'impulsions lumineuses
 - Le câble est constitué de deux fibres. Une pour l'émission et l'autre pour la réception



■ Avantage

s:

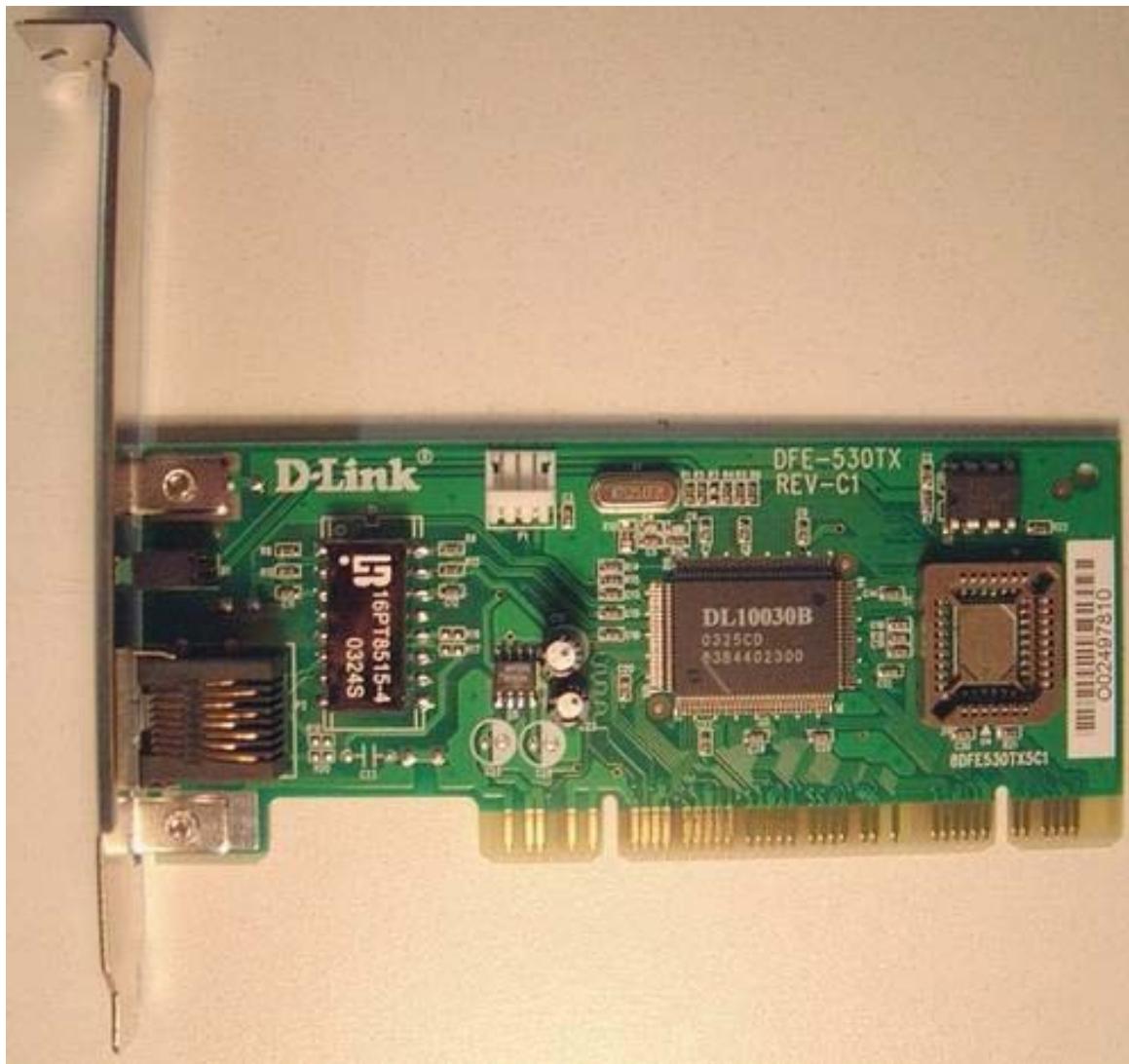
- Rapides
- Insensibles à toute interférence électromagnétique
- Génèrent très peu d'atténuation sur le signal
- Peu encombrants, plus légers
- Confidentialité des données

- Les types de câbles fibres optiques les plus utilisés: **100BaseFX** (100Mbits/s)



Type	Avantages	Inconvénient s	Mbits/ s	Lg max	Coût
Coaxial fin	coût	une coupure bloque tout le réseau	10	185 m	très faible
Coaxial épais	coût, longueur max	Coût élevé Difficulté d'installatio n	10	500 m	faible
Paires torsadées	coût, débit, une coupure ne touche pas tout le réseau	longueur max	100	100 m	faible
Fibre optique	fiabilité, débit	nécessite du personnel	1000 et +	plusieurs Km	très élevé

2- CARTES RESEAUX



- La carte réseau fait office de connexion physique entre l'ordinateur et le câble réseau
- Les cartes sont installées dans un connecteur (slot) d'extension sur chaque ordinateur et serveur du réseau
- Les fonctions de la carte réseau sont :
 - préparation pour le câble réseau des données qui seront transmises à partir de l'ordinateur
 - envoi des données vers un autre ordinateur
 - contrôle du flux de données entre l'ordinateur



3- Les éléments actifs

- Les Hubs (les concentrateurs)
- Les Switchs (les commutateurs)
- Les passerelles (Assure la communication entre réseaux de protocoles différents.)
- Les routeurs

Les hubs= concentrateur

- Élément matériel qui permet de concentrer le trafic réseau provenant de plusieurs hôtes et de régénérer le signal
- Servent à relier entre eux toutes les parties d'un même réseau physique. Lorsqu'une information arrive sur un Hub, elle est rediffusée vers toutes les destinations possibles càd vers tous les ports
- Les trames envoyées à destination d'une machine sont reçues par toutes les



Les switchs: concentrateur-commutateur

- C'est un pont multiports qui analyse les trames arrivant sur les ports d'entrée et filtre les données.
- Ils assurent le filtrage et la connectivité
- A un instant donné, ils ne laissent passer les informations que vers la destination voulue.
- # hub: les trames envoyées à une machine sont directement vers l'autre machine destinatrice



Les répéteur

Le répéteur (transceiver) est un équipement d'interconnexion de niveau 1 qui assure la répétition des bits d'un segment sur l'autre (régénération du signal pour compenser l'affaiblissement) et qui permet :

d'augmenter la distance d'un segment physique



t du support

Le pont

Dans les réseaux, un pont permet de connecter un réseau local (LAN) à un autre réseau local utilisant le même protocole (par exemple, Ethernet ou Token Ring).



Routeur

un routeur est un appareil qui connecte deux ou plusieurs réseaux ou sous-réseaux à commutation de paquets . Il remplit deux fonctions principales : gérer le trafic entre ces réseaux en transférant les paquets de données vers leurs adresses IP prévues et permettre à plusieurs appareils d'utiliser la même connexion Internet.

Programme : grands titres

- 1 Généralité sur réseaux informatique
- 2 protocole et modèle : Modèle de référence OSI et TCP/IP
- 3 Modèle TCP/IP: couche accès réseau
- 4 Modèle TCP/IP: couche internet (adressage et routage)

Chapitre 2: Protocoles et Modèles



Titre du Module: Protocoles et Modèles

Objectif du Module: Expliquer comment les protocoles réseau permettent aux périphériques d'accéder aux ressources de réseau locales et distantes.

Titre du Rubrique	Objectif du Rubrique
Les Règles efficacement.	Décrire les types de règles nécessaires pour communiquer
Protocoles	Expliquer pourquoi les protocoles sont indispensables à la communication réseau.
Suites de protocoles	Expliquer l'utilité d'adhérer à une suite de protocoles.
Organismes de normalisation	Expliquer le rôle des organismes de normalisation dans la définition des protocoles pour l'interopérabilité réseau.
Modèles de référence	Expliquer comment le modèle TCP/IP et le modèle OSI sont utilisés pour faciliter la normalisation dans le processus de communication.
Encapsulation de données	Expliquer comment l'encapsulation de données permet la transmission des
Accès aux données	Expliquer comment les périphériques locaux accèdent aux ressources locales sur un réseau.

Objectifs :

- Expliquer le rôle des protocoles et des organismes de normalisation en tant que facilitateurs de l'interopérabilité des communications réseau

2.1 Les Règles



Les Règles Fondamentaux de La Communication

La taille et la complexité des réseaux peuvent varier. Il ne suffit pas d'avoir une connexion, les appareils doivent convenir sur « comment » communiquer.

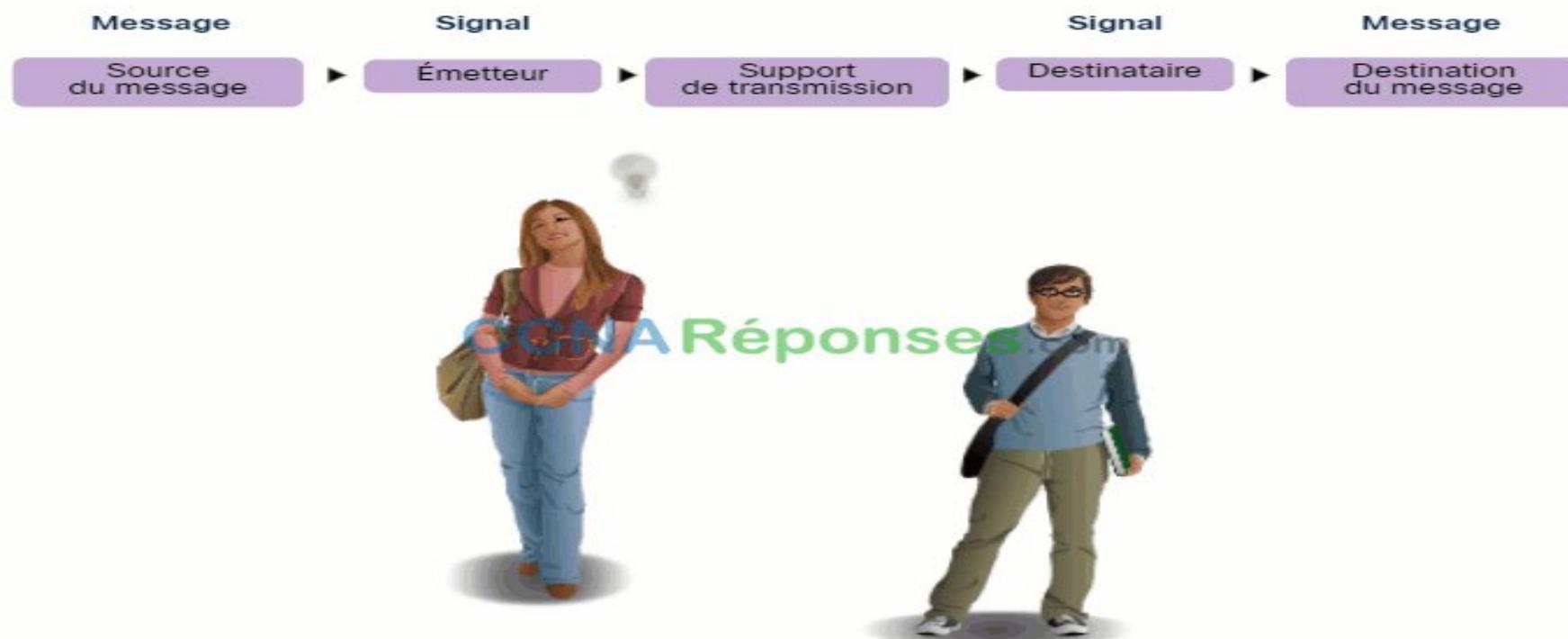
Toute communication comporte trois éléments :

- Il y aura une source (expéditeur).
- Il y aura une destination (récepteur).
- Il y aura un canal (support) qui prévoit le chemin des communications à se produire.

Les Règles

Fondamentaux de La Communication

- Toutes les communications sont régies par des protocoles.
- Les protocoles sont les règles que les communications suivront.
- Ces règles varient en fonction du protocole.



Les Règles

Établissement de la règle

- Les personnes doivent utiliser des règles ou des accords établis pour régir la conversation.
- Le premier message est difficile à lire car il n'est pas formaté correctement. La seconde montre le message correctement formaté

humans communication between govern rules. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. A estrutura da gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana comprehensivel por muitos individuos diferentes.

Rules govern communication between humans. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. The structure of the grammar, the language, the punctuation and the sentence make the configuration humanly understandable for many different individuals.



Les Règles

Établissement de la règle (Suite)

Les protocoles doivent prendre en compte les éléments suivants :

- l'identification de (source) l'expéditeur et du destinataire ;
- l'utilisation d'une langue et d'une syntaxe communes ;
- Vitesse et délais de communication ;
- la demande de confirmation ou d'accusé de réception.

Les Règles

Exigences Relatives au Protocole Réseau

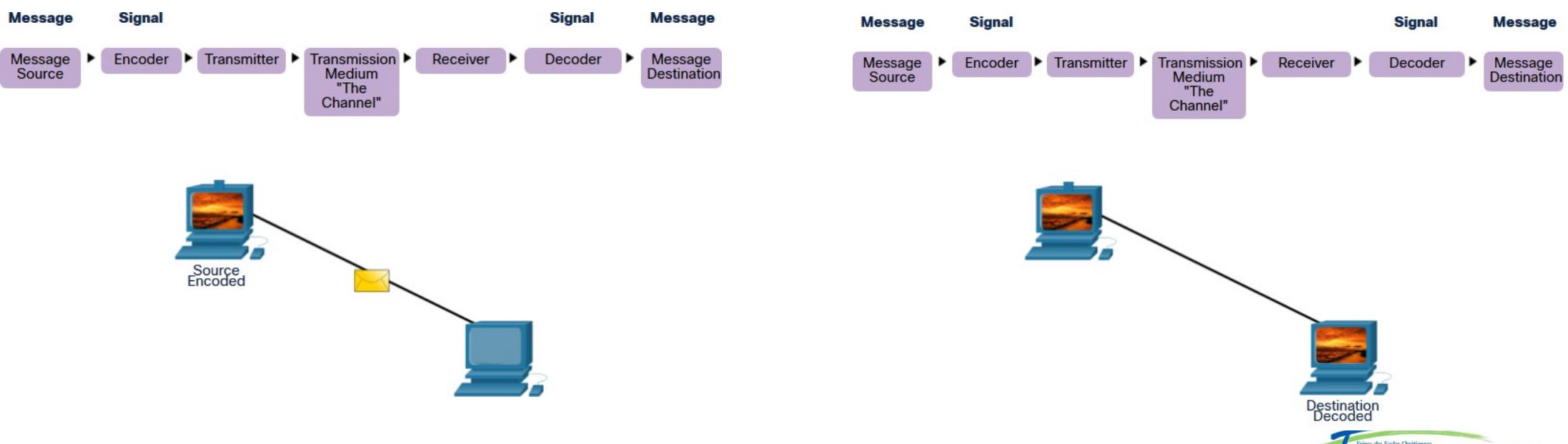
Les protocoles informatiques communs doivent être en accord et comprendre les exigences suivantes:

- Codage des messages
- Format et encapsulation des messages
- La taille du message
- Synchronisation des messages
- Options de remise des messages

Les Règles

Codage des Messages

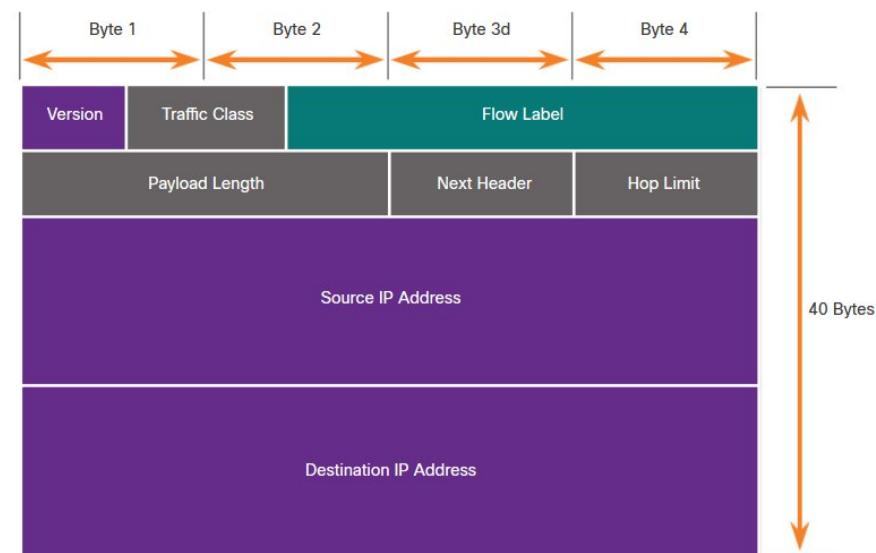
- Le codage est le processus de conversion des informations vers un autre format acceptable, à des fins de transmission.
 - Le décodage inverse ce processus pour interpréter l'information.



Les Règles

Format et Encapsulation des Messages

- Lorsqu'un message est envoyé de la source à la destination, il doit suivre un format ou une structure spécifique.
- Les formats des messages dépendent du type de message et du type de canal
 - utilisés pour remettre le message

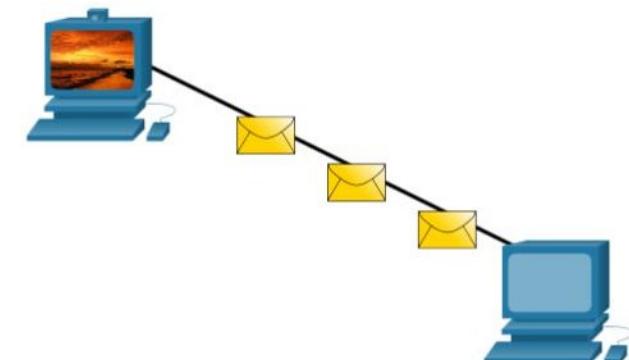
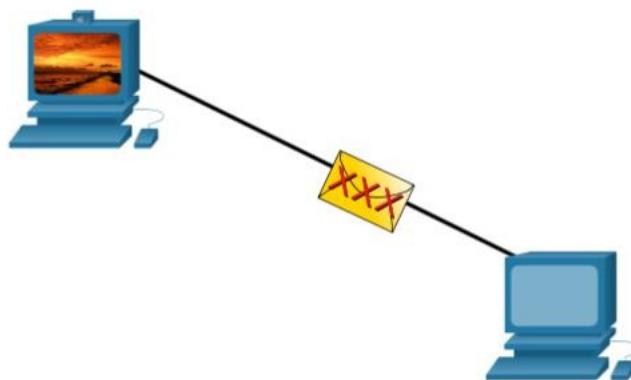


Les Règles

Taille du Message

Le format du codage entre les hôtes doit être adapté au support.

- Les messages envoyés sur le réseau sont convertis en bits
- Les bits sont codés dans un motif d'impulsions lumineuses, sonores ou électriques.
- L'hôte de destination reçoit et décode les signaux pour interpréter le message.



Les Règles

Synchronisation du Message

La synchronisation des messages comprend les éléments suivants:

- Contrôle du flux
- Délai de réponse
- Méthode d'accès

Contrôle du Flux —ceci est le processus de gestion de la vitesse de transmission des données.

Le contrôle de flux définit la quantité d'informations qui peuvent être envoyées et la vitesse à laquelle elles peuvent être livrées. Si une personne parle trop rapidement, l'autre personne éprouve des difficultés à entendre et à comprendre le message.

Dans la communication réseau, il existe des protocoles réseau utilisés par les périphériques source et de destination pour négocier et gérer le flux d'informations.



La Méthode d'Accès – Détermine le moment où un individu peut envoyer un message.

- Il peut y avoir diverses règles régissant des questions comme les « collisions ». C'est lorsque plusieurs appareils envoient du trafic en même temps et que les messages deviennent corrompus.
- Certains protocoles sont proactifs et tentent de prévenir les collisions ; d'autres sont réactifs et établissent une méthode de récupération après la collision.



CCNA Réponses.com

Délai de réponse – Si une personne pose une question et qu'elle n'entend pas de réponse dans un délai acceptable, elle suppose qu'aucune réponse n'a été donnée et réagit en conséquence.

La personne peut répéter la question ou continuer à converser.

Les hôtes du réseau sont également soumis à des règles qui spécifient le délai d'attente des réponses et l'action à entreprendre en cas de délai d'attente dépassé.

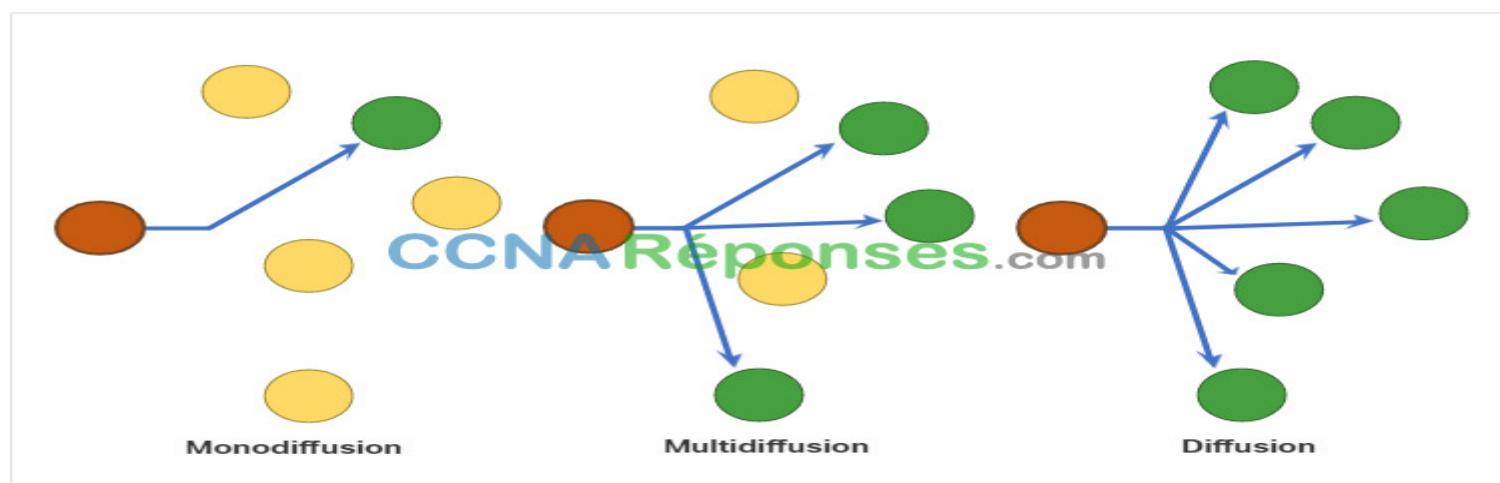
Les Règles

Options de remise du Message

La remise des messages peut être l'une des méthodes suivantes :

- **Monodiffusion** — communication un à un
- **Multidiffusion** — un à plusieurs, généralement pas tous
- **Diffusion** – un à tous

Remarque: les diffusions sont utilisées dans les réseaux IPv4, mais ne sont pas une option pour IPv6. Plus tard, nous verrons également «Anycast» comme une option de livraison supplémentaire pour IPv6.



2.2

Protocoles



Protocoles

Aperçu du Protocole

Les protocoles réseau définissent un ensemble de règles communes.

- Peut être implémenté sur les appareils dans:
 - Logiciels
 - Matériel
 - Les deux
- Les protocoles ont leur propre:
 - Fonction
 - Format
 - Règles

Type de protocole	Description
Communications de Réseau	permettre à deux ou plusieurs périphériques de communiquer sur un ou plusieurs réseaux
Sécurité des Réseaux	sécuriser les données pour fournir l'authentification, l'intégrité des données et le chiffrement des données
Routage	permettre aux routeurs d'échanger des informations sur les itinéraires, de comparer les informations sur les chemins et de choisir le meilleur chemin
Détection des Services	utilisés pour la détection automatique de dispositifs ou de services

© 2016 Cisco et/ou ses filiales. Tous droits réservés. Informations

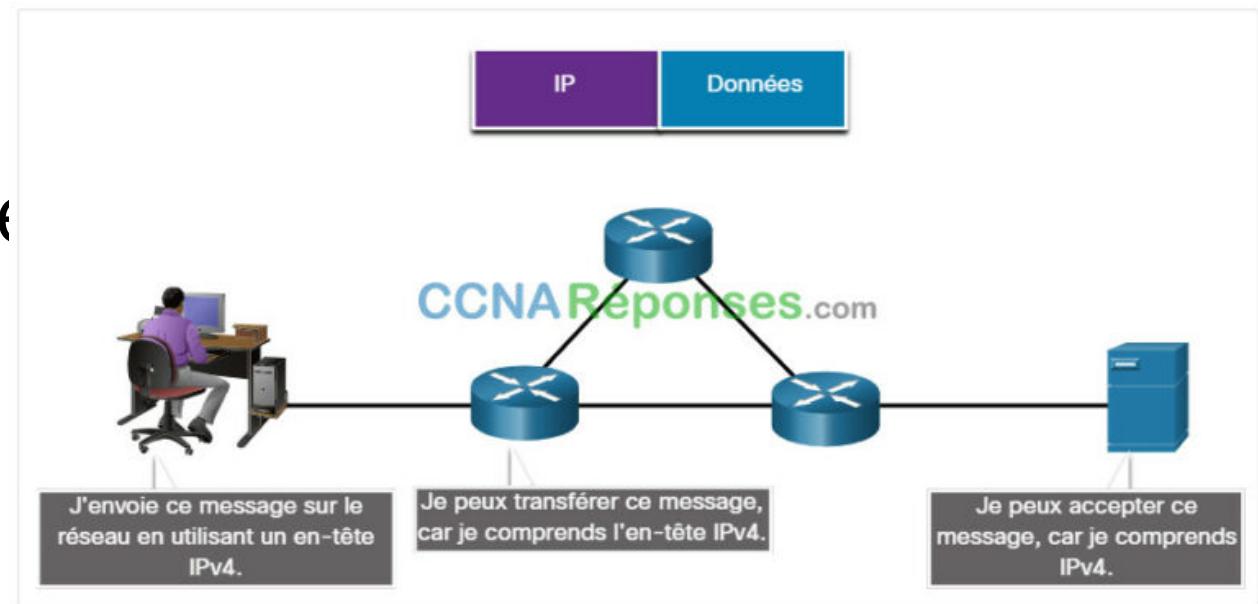
confidentielles de Cisco



Protocole

Fonctions de Protocole Réseau

- Les appareils utilisent des protocoles convenus pour communiquer.
- Les protocoles peuvent avoir



Fonction	Description
Adressage	Identifie l'expéditeur et le destinataire
Fiabilité	Offre une garantie de livraison
Contrôle de flux	Garantit des flux de données à un rythme efficace
Séquençage	Étiquette de manière unique chaque segment de données transmis
Détection des erreurs	Détermine si les données ont été endommagées pendant la transmission
Interface d'application	Communications processus-processus entre les applications réseau



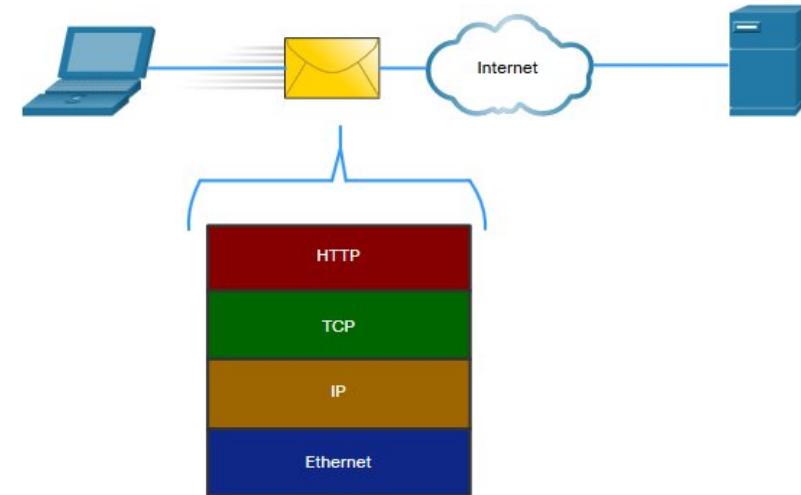
© 2016 Cisco et/ou ses filiales. Tous droits réservés.
Confidentialité de Cisco



Protocole

Interaction de Protocole

- Les réseaux nécessitent l'utilisation de plusieurs protocoles.
- Chaque protocole a sa propre fonction et son propre format.



Protocole	Fonction
Protocole HTTP (Hypertext Transfer Protocol)	<ul style="list-style-type: none">▪ Régit la manière dont un serveur web et un client web interagissent▪ Définit le contenu et le format
Protocole de Contrôle de Transmission (TCP)	<ul style="list-style-type: none">▪ Gère les conversations individuelles▪ Offre une garantie de livraison▪ Gère le contrôle du flux
Protocole Internet (IP)	Fournit des messages globalement de l'expéditeur au destinataire
Ethernet	Fournit des messages d'une carte réseau à une autre carte réseau sur le même réseau local (LAN) Ethernet

Cisco

Modèles de Référence

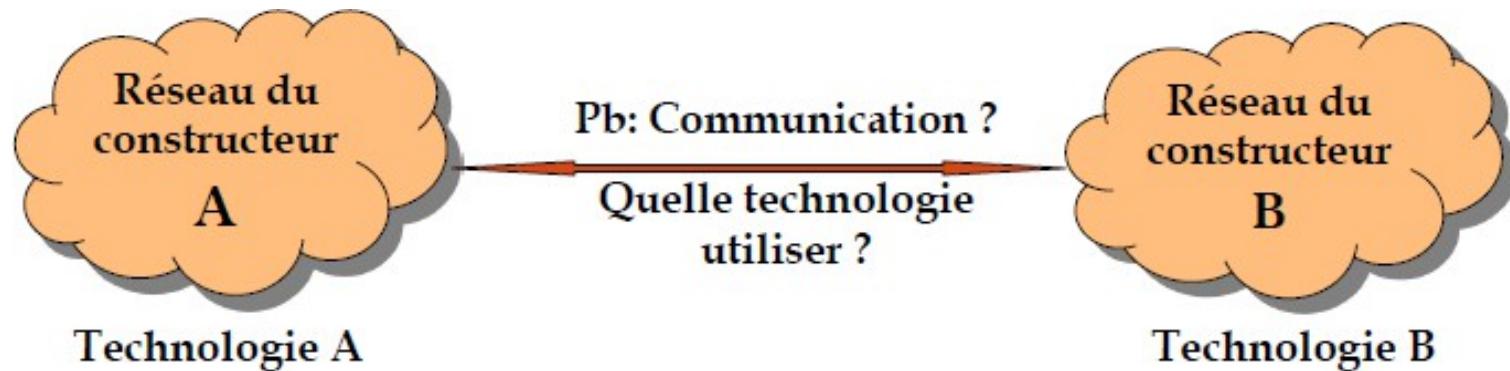


1. POURQUOI LA STANDARDISATION ?

Problématique:

- Les constructeurs informatiques ont proposé des architectures réseaux propres à leurs équipements.
 - Exemples
 - IBM a proposé SNA (System Network Architecture),
 - DEC a proposé DNA (Digital Network Architecture)...
- Ces architectures ont toutes le même défaut : du fait de leur **caractère propriétaire**, il n'est pas facile de les interconnecter, à moins d'un accord entre constructeurs.

I.Kechiche



POURQUOI LA STANDARDISATION ?

Solution:

- l'ISO (International Standards Organisation) a développé un **modèle de référence normalisé** appelé modèle OSI (Open Systems Interconnection), ou Interconnexion de systèmes ouverts en français.

Modèle OSI

- Représentation abstraite de l'interconnexion des systèmes ouverts
- Uniformisation des règles de communications réseau.
- organisé 7 couches

Ce modèle permet d'éviter :

- L'incompatibilité des architectures constructeurs entre elles,
- la complexité croissante des architectures,
- la multiplication des solutions d'interconnexion d'architectures hétérogènes,



Modèles OSI

Les couches inférieures (1 à 3) :

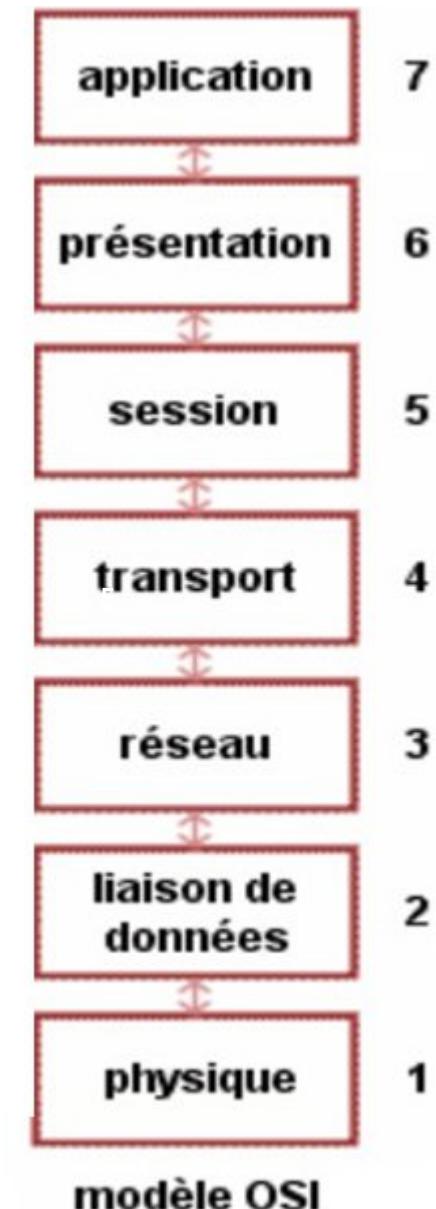
Assurent le **transport de l'information** proprement dit.

On les trouve dans les **équipements qui communiquent** via un réseau, et dans les divers dispositifs qui assurent le fonctionnement de ce réseau.

Les couches supérieures (4 à 7) du modèle OSI

Assurent le **traitement de l'information**

On les trouve dans les logiciels de communication réseau.



2. MODÈLE OSI: COMMUNICATION INTER-COUCHES 1/2

□ **Une couche:**

- est spécialisée dans un ensemble de fonctions particulières.
- utilise les fonctionnalités de la couche inférieure
- propose ses fonctionnalités à la couche supérieure.

□ **Le protocole d'une couche N**

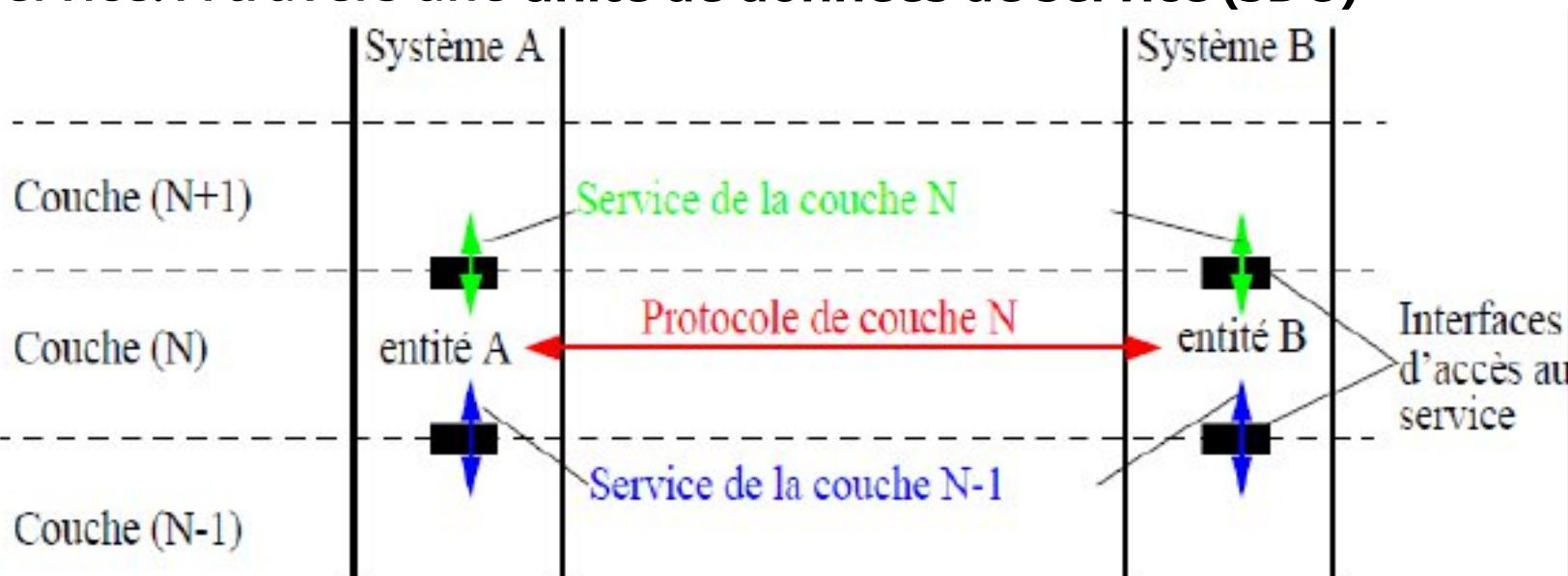
- définit l'ensemble des règles, les formats et la signification des objets échangés, qui régissent la communication entre les entités de la couche N.

□ **Le service d'une couche N**

- définit l'ensemble des fonctionnalités possédées par la couche N et fournies aux entités de la couche N+1 au niveau de l'interface N/N+1.

2. MODÈLE OSI: COMMUNICATION INTER-COUCHES 2/2

- Chaque couche du système A communique avec la couche qui lui est homologue du système B suivant un protocole
- A chaque couche correspond une **unité de données de protocole (PDU)**.
- Chaque couche fournit à la couche qui lui est inférieur un service. À travers une **unité de données de service (SDU)**



2. MODÈLE OSI : TECHNIQUE DE COMMUNICATION

Rappel: pour faire circuler l'information sur un réseau on peut utiliser principalement deux stratégies:

1. L'information est envoyée de façon complète (atomique)
 - o Monopolisation de l'infrastructure de communication,
 - o problèmes d'erreurs de communication difficiles à traiter efficacement
2. L'information est fragmentée en petits morceaux (paquets)
 - o chaque paquet est envoyé séparément sur le réseau,
 - o les paquets sont ensuite ré-assemblés sur la machine destinataire (réseau à commutations de paquets).

Le modèle OSI (Open System Interconnexion) est un modèle à 7 couches (formant une pile) qui décrit l'architecture et le fonctionnement d'un système de communication (« réseau »)

2. MODÈLE OSI : AVANTAGES

- Une couche offre un ensemble de services accomplissant un but précis.
- Chacune des couches de ce modèle représente une catégorie de problème que l'on rencontre dans un système de communication:
 - OSI permet de diviser la complexité d'un système de communication et de faciliter l'interopérabilité entre les réseaux."



2. MODÈLE OSI : COUCHES 1/4

Couche 7: Application

□ Rôle :

- C'est la couche OSI la plus proche de l'utilisateur.
- Elle fournit des services réseau aux applications de l'utilisateur tels que le courrier électronique, le transfert de fichiers ...

□ Protocoles:

- transfert de fichier (FTP)
- courrier électronique (IMAP, SMTP)

....

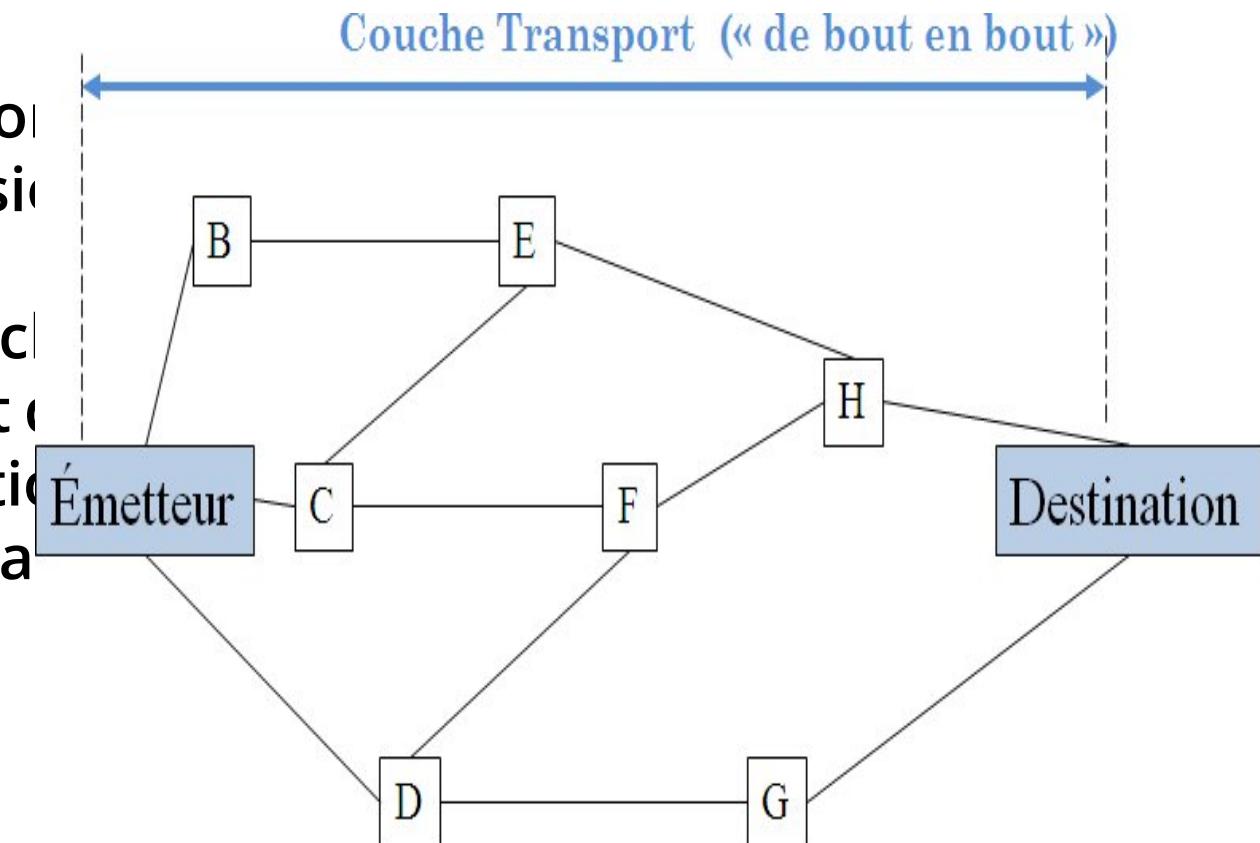
Couche 6: Présentation

- Gère le cryptage, la compression, l'autre traduction des messages

2. MODÈLE OSI : COUCHES 2/4

Couche 5: Session

- Rôle : communication
 - établir des sessions (entre utilisateurs)
 - organiser et synchroniser les sessions
 - établissement de la connectivité
 - maintien, gestion et démantèlement de la session
 - libération de la session



Couche 4: Transport

- Rôle : connexions de bout en bout
 - ne s'occupe pas des nœuds intermédiaires
 - A l'émission, découpe les messages volumineux en segments et les rassemble à la réception

MODÈLE OSI : COUCHES 3/4

UDP (User Datagram Protocol)

- Connexion non fiable mais rapide.

TCP (Transmission Control Protocol)

- Connexion fiable avec correction d'erreurs.

Couche 3: Routage

- Rôle : Adressage réseau et détermination du meilleur chemin
 - permet l'interconnexion de réseaux hétérogènes (qui n'ont pas le même plan d'adressage) et s'occupe des nœuds intermédiaires
 - assure l'adressage logique
 - le routage (aiguillage) des paquets à travers le réseau (choix du meilleur chemin)

- Protocole: ARP

2. MODÈLE OSI : COUCHES 4/4

Couche 2: Liaison de données

- Rôle : Contrôle de liaison directe, accès au média
 - assure un transfert fiable des données par le média (support physique)
 - contrôle d'erreurs (détectioп et/ou correction)
 - connectivité et sélection du chemin entre les systèmes hôtes
 - transmission des trames en séquence et gestion d'accès au support
- Protocoles:
 - Ethernet, HDLC

Couche 1: Physique

- Rôle : transfert physique
 - réalise la transmission des éléments binaires des trames sur le support de transmission

2. MODÈLE OS I :EXEMPLES D'APPLICATION

7: Couche d'application

émulation de terminal, transfert de fichiers

6: Couche de présentation

Gère le cryptage, la compression, l'autre traduction des messages

5: Couche de session

Établit et met fin aux connexions entre les applications(voir plusieurs communications simultanément)

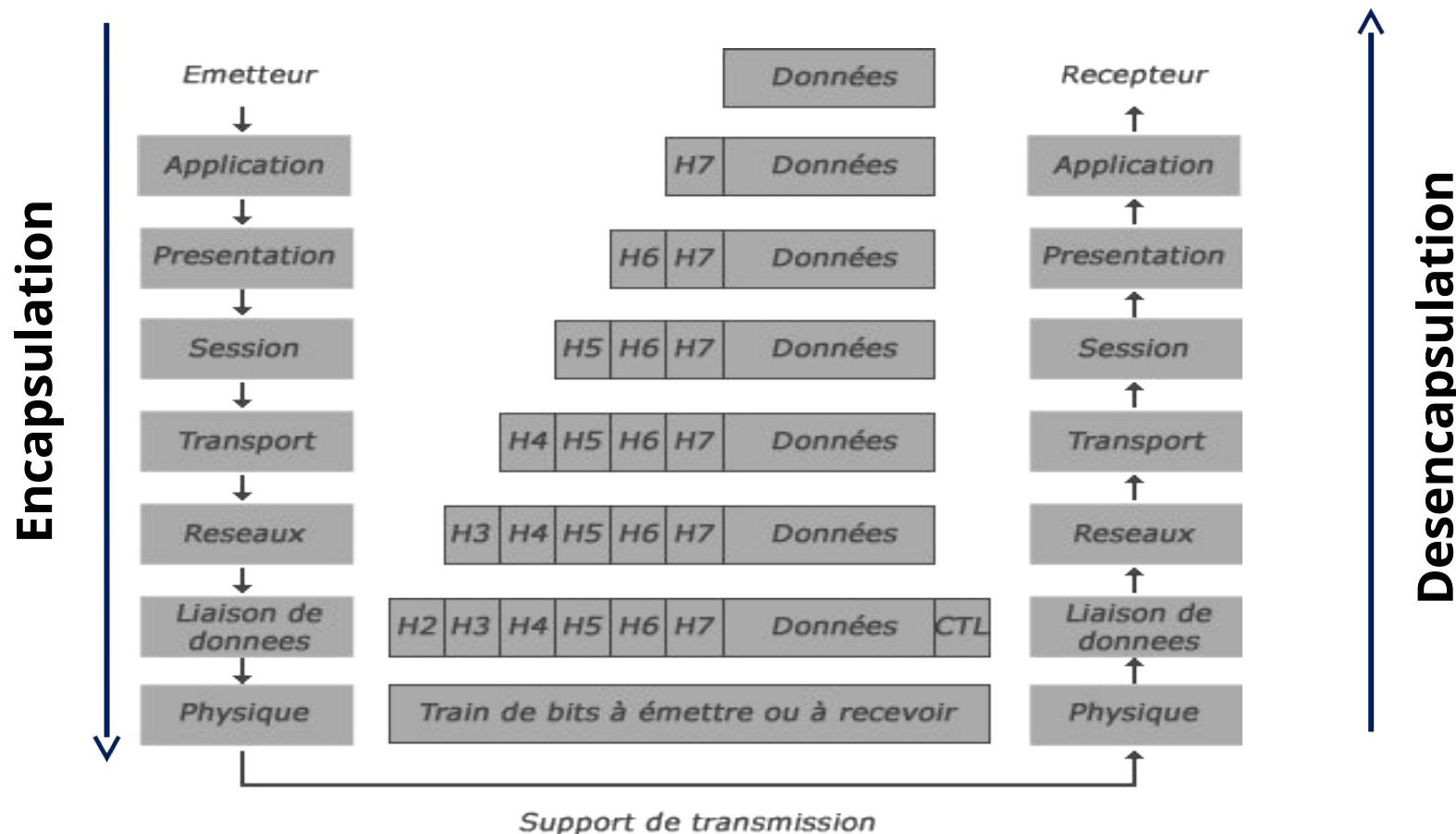
4: couche de transport

Divise les messages en paquets, assemble les paquets en messages

3: Couche réseau : assure l'ors d'une transfert à travers un ~~système~~
relai, d'acheminement les données (**paquet**) à travers differens sous réseaux (routage)



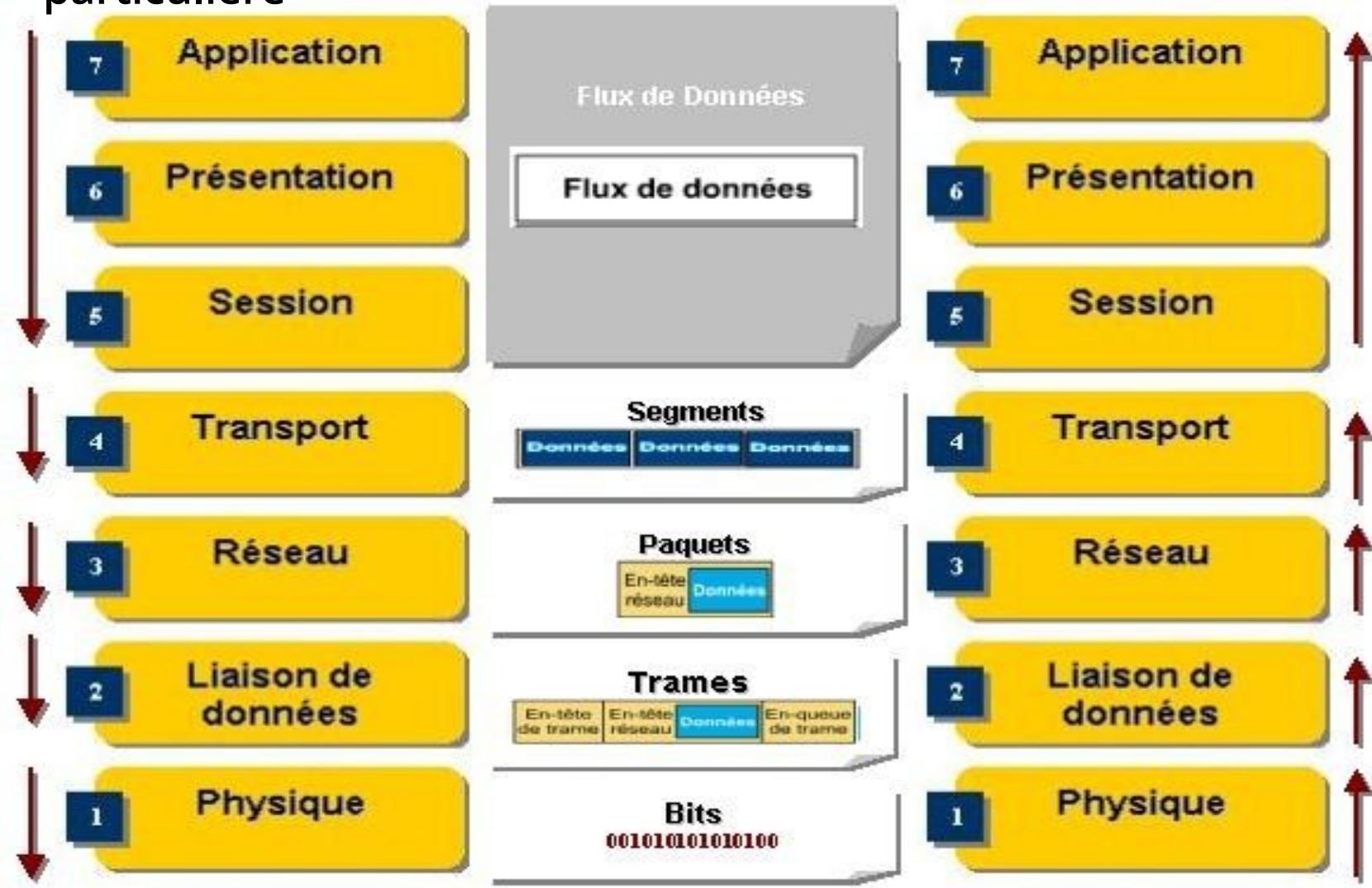
2. MODÈLE OSI : PROCESSUS D'ENCAPSULATION 1/2

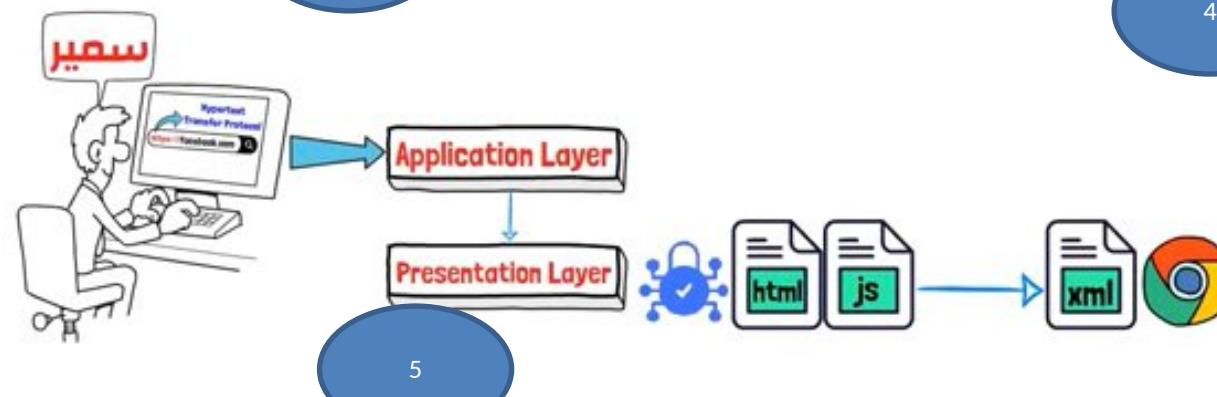
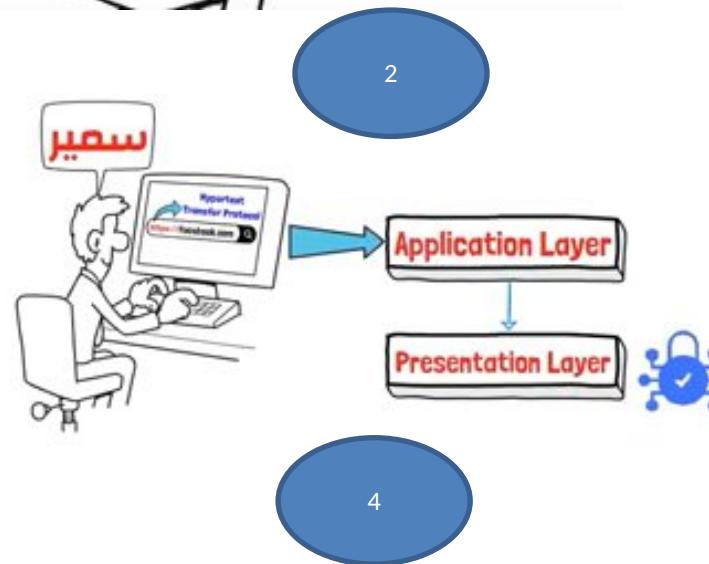
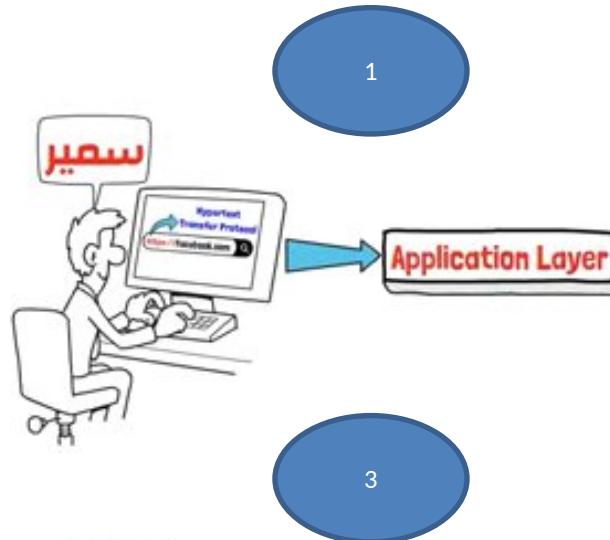


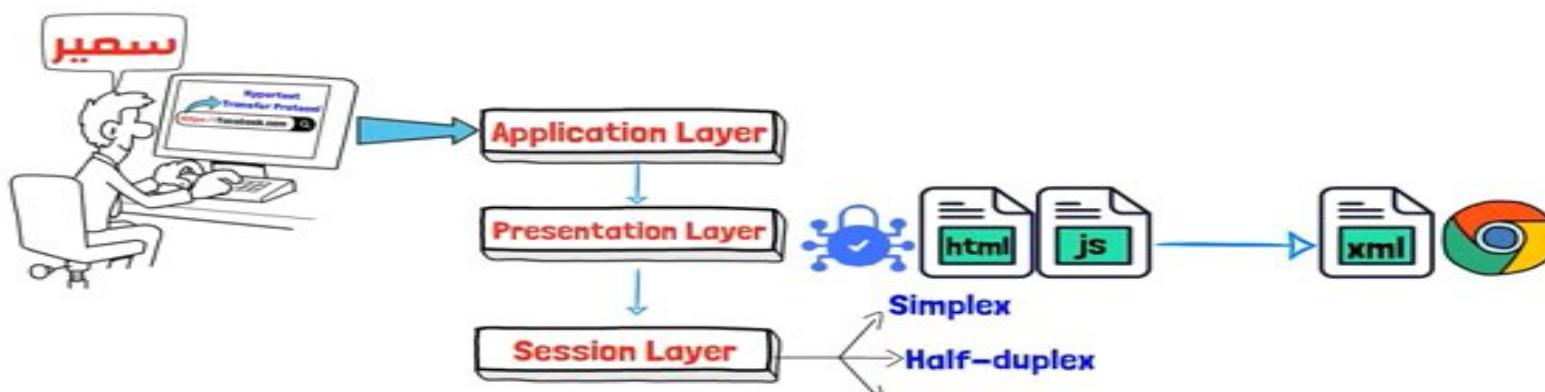
- Le passage d'une couche à la couche inférieure se fait par ajout d'informations de contrôle PCI. C'est le mécanisme **d'encapsulation**
- À la réception. Chaque couche enlève l'en-tête qui lui correspond et passe le résultat à la couche supérieure. C'est le **desencapsulation**

2. MODÈLE OSI : PROCESSUS D'ENCAPSULATION 2/2

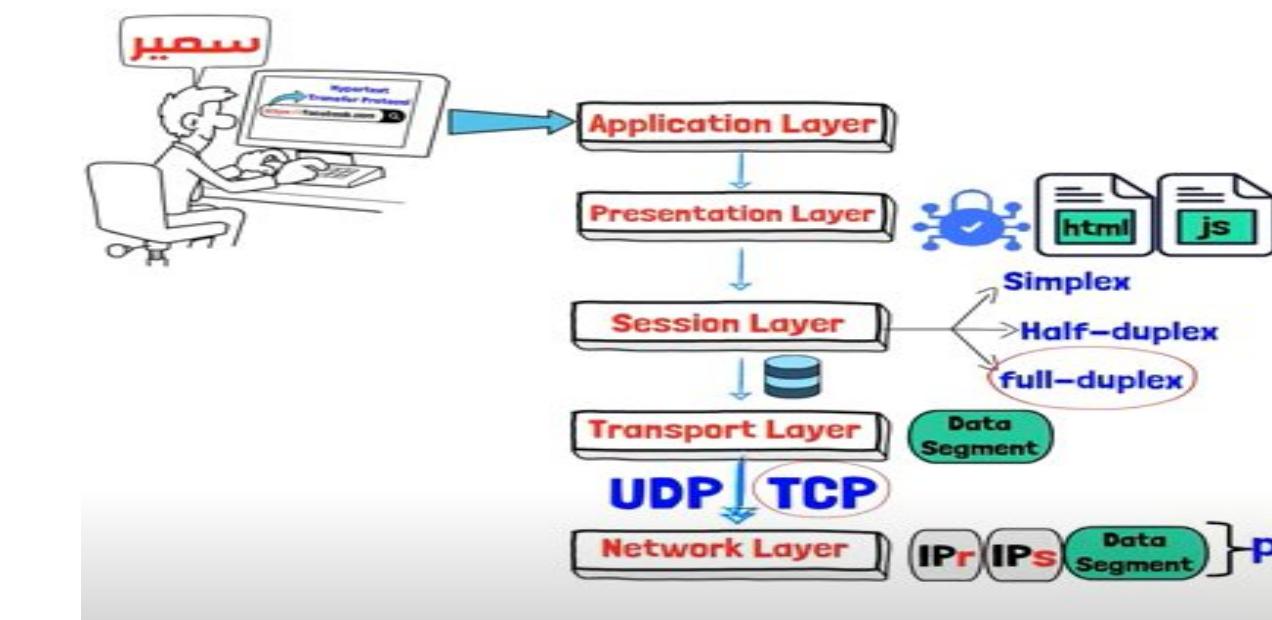
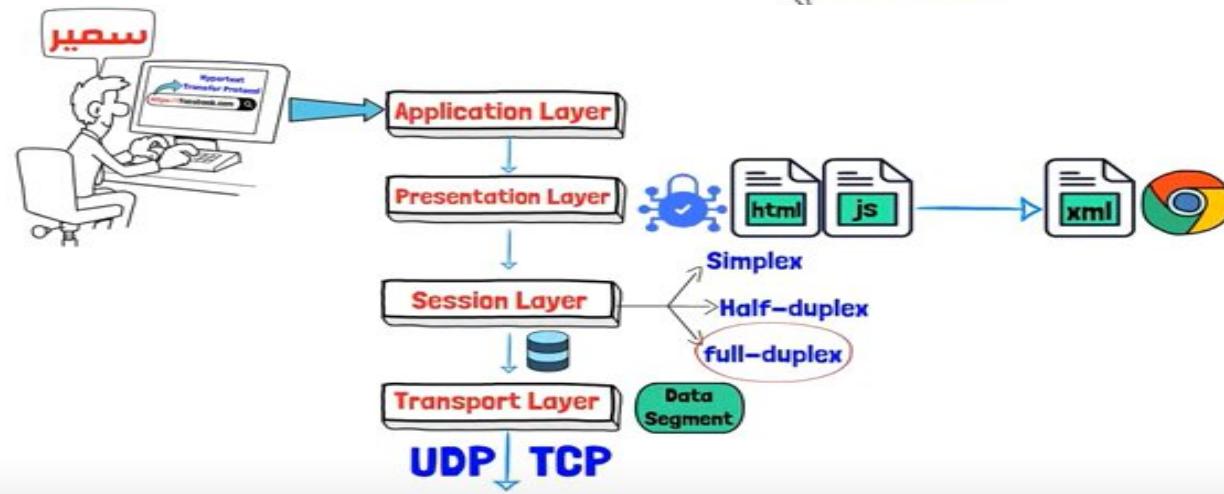
- A chaque couche correspond une structure de données bien particulière



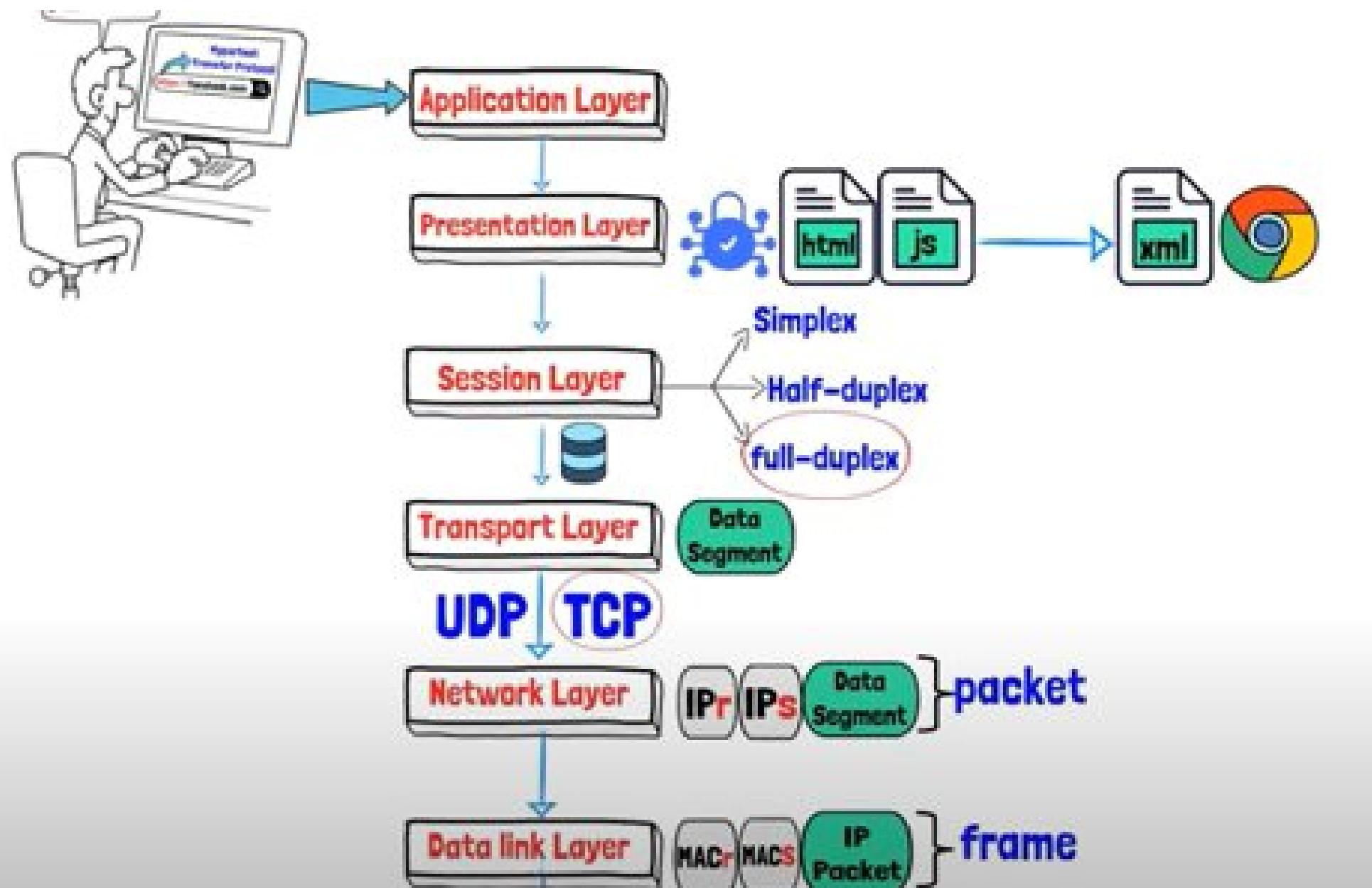


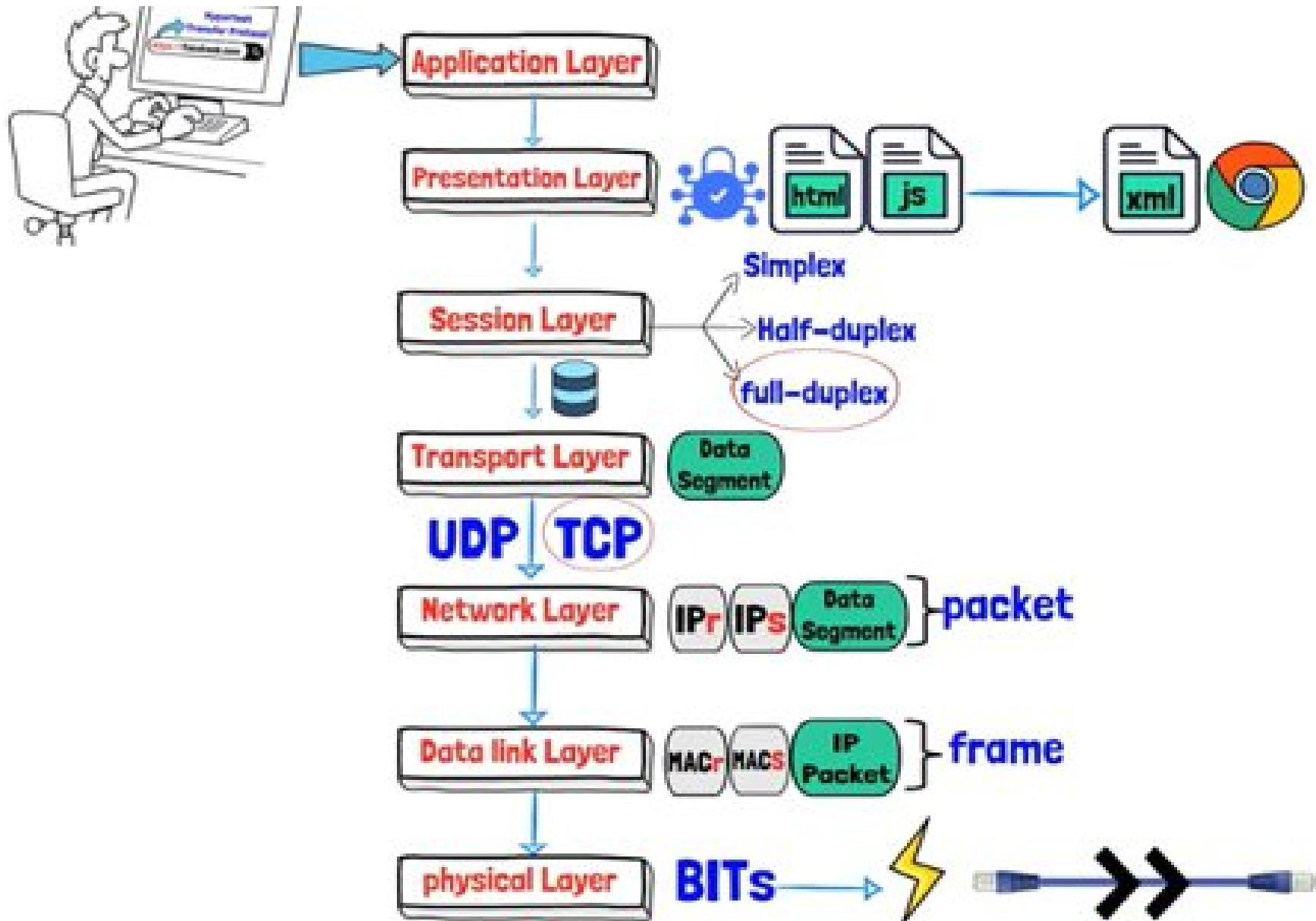


6



7





MODÈLE OSI : LIMITES

- OSI est trop **complexe** pour pouvoir être proprement et efficacement implémenté
- Le modèle OSI est **théorique** et utilisé pour comprendre les réseaux, mais il présente des limites : il n'est pas toujours applicable dans la pratique, les couches ne correspondent pas toujours aux systèmes réels (comme TCP/IP), et il peut être trop complexe pour certaines technologies modernes.
- De plus, il ne décrit pas toujours précisément les interactions dans les réseaux actuels.



Qu'est-ce que j'ai appris dans ce module?

Les Règles

- Les protocoles doivent avoir un expéditeur et un destinataire.
- Les protocoles informatiques courants comprennent ces exigences : codage, formatage et encapsulation des messages, ,,,

Protocoles

- L'envoie d'un message sur le réseau nécessite l'utilisation de plusieurs protocoles.
- Chaque protocole réseau a sa propre fonction, son format et ses propres règles de communication.



Qu'est-ce que j'ai appris dans ce module?

Modèles de référence

- Le modèle OSI compte 7 couches
- **Encapsulation de données**
- La forme que prend un élément de données à n'importe quelle couche est appelée *unité de données de protocole (PDU)*.
- Cinq PDU différentes sont utilisées dans le processus d'encapsulation des données: données, segment, paquet, frame et bits

Accès aux données

- Les couches Réseau et Liaison de données vont fournir l'adressage pour déplacer les données à travers le réseau.
- La couche 3 fournira l'adressage IP et la couche 2 fournira l'adressage MAC.
- La façon dont ces couches gèrent l'adressage dépend du fait que la source et la destination se trouvent sur le même réseau ou si la destination se trouve sur un réseau différent de la source.



Exercice

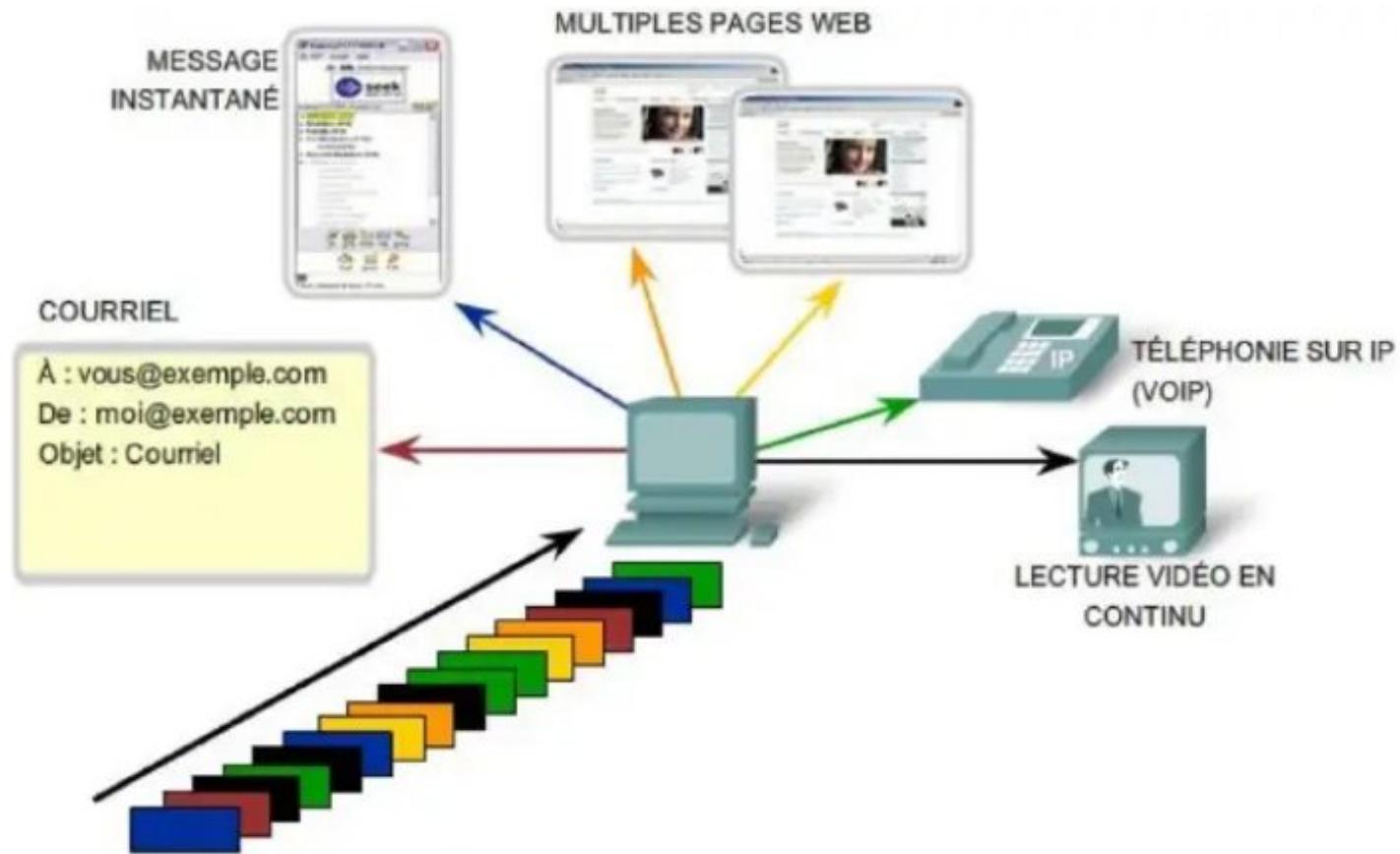
Identifier le processus présenté dans chacune des images suivantes ainsi que la couche de modèle OSI responsable de cette fonctionnalité ,



Image 1

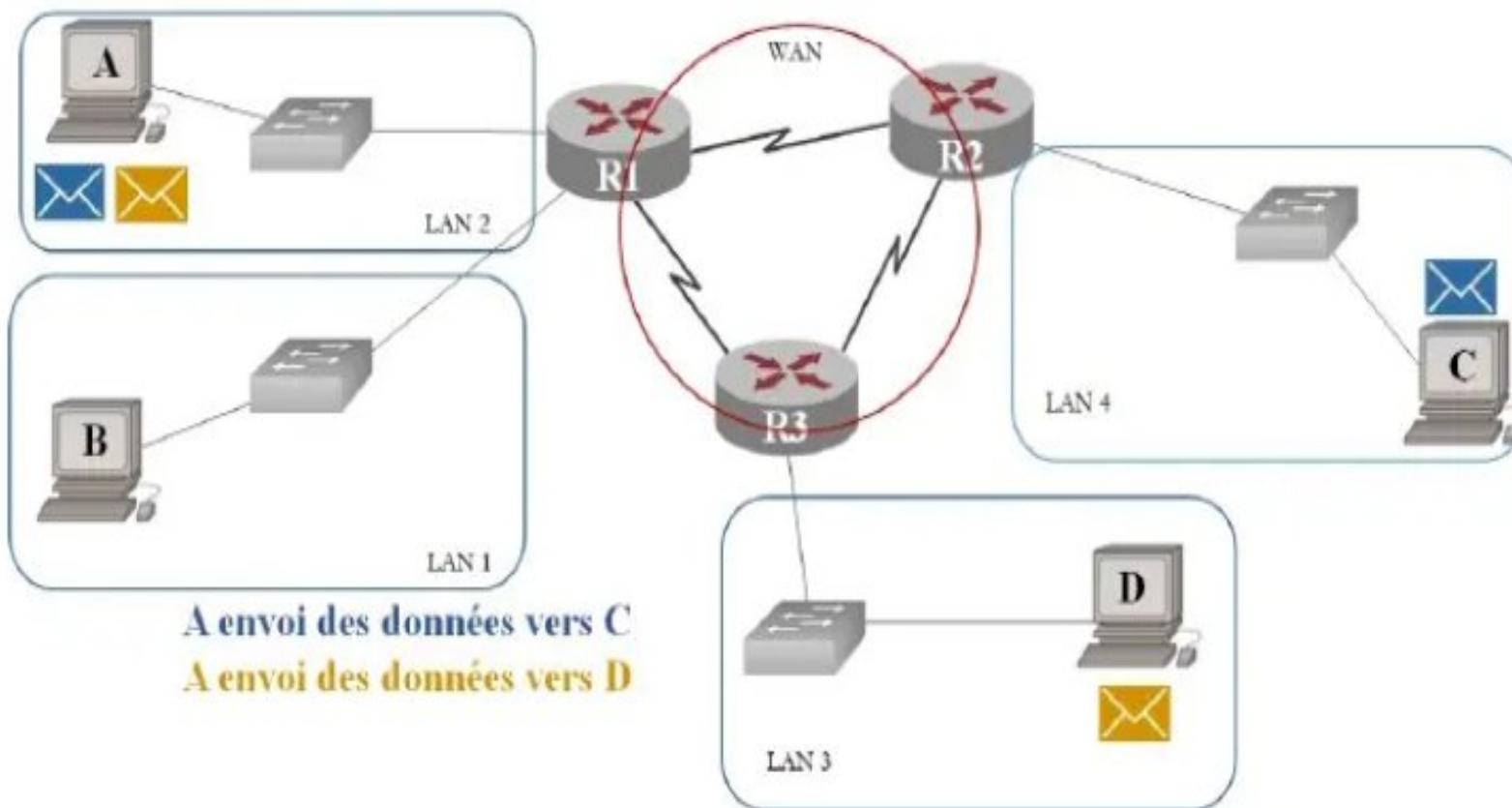
Fonctionnalité : identification des applications utilisateur

Couche : Application



Fonctionnalité : Segmentation de données

Couche : Transport



Fonctionnalité : Interconnexion des réseaux et Routage

Couche : Réseau

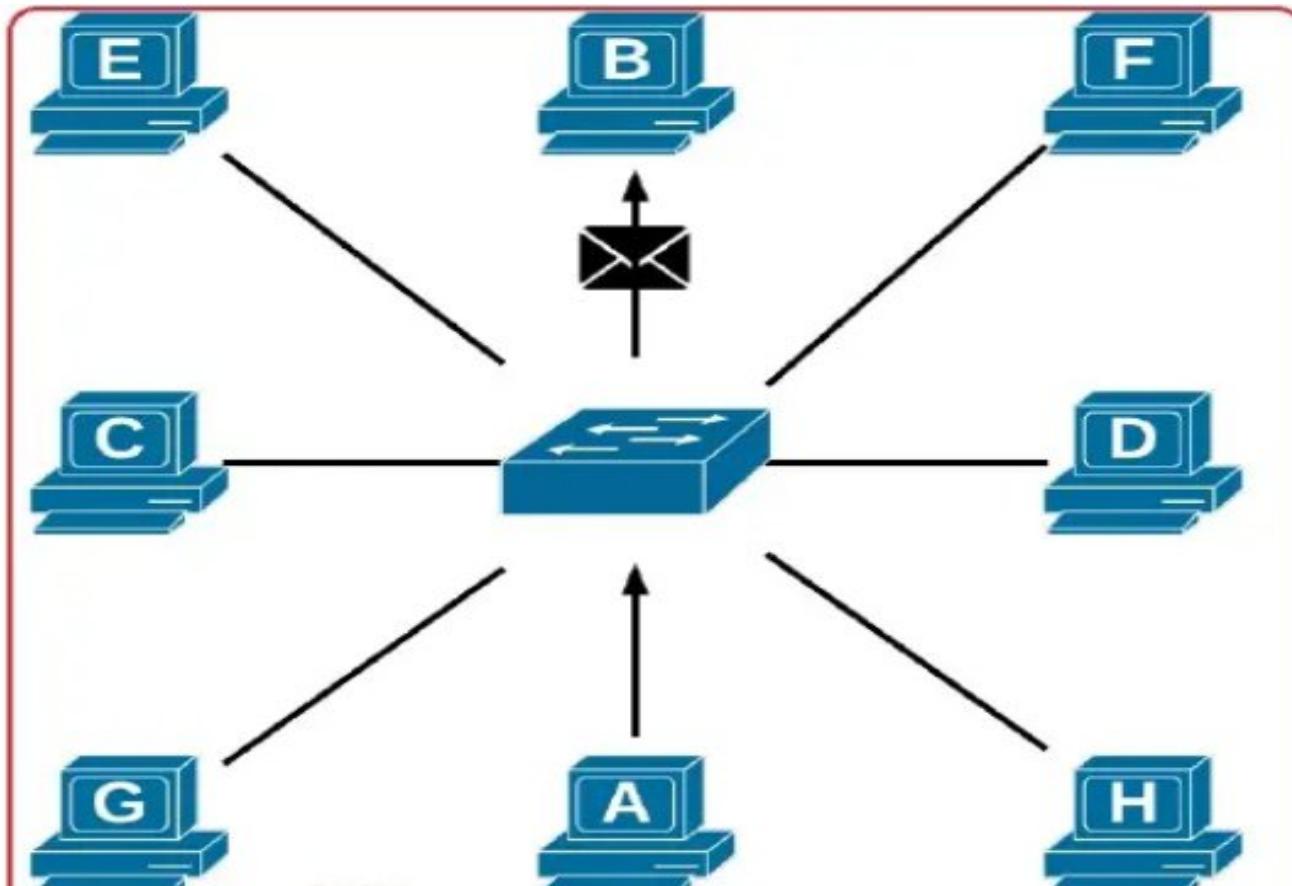
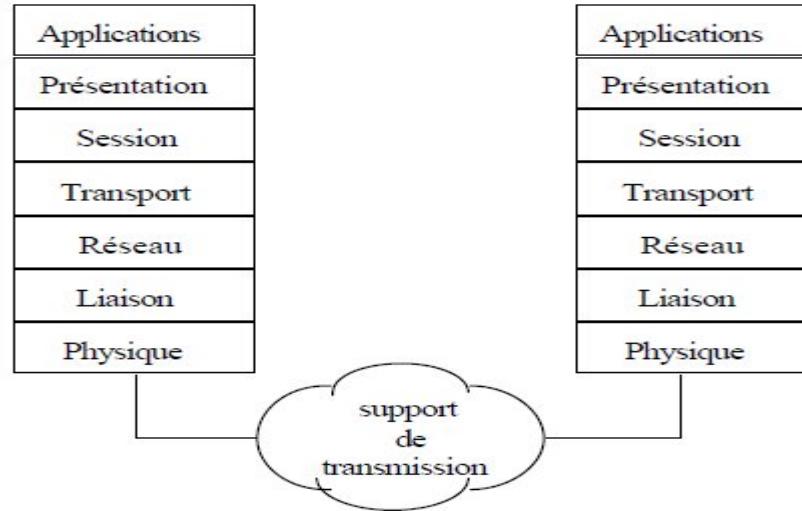


Image 3

Fonctionnalité : Commutation des données entre les machines d'un LAN

Couche : Liaison de données.



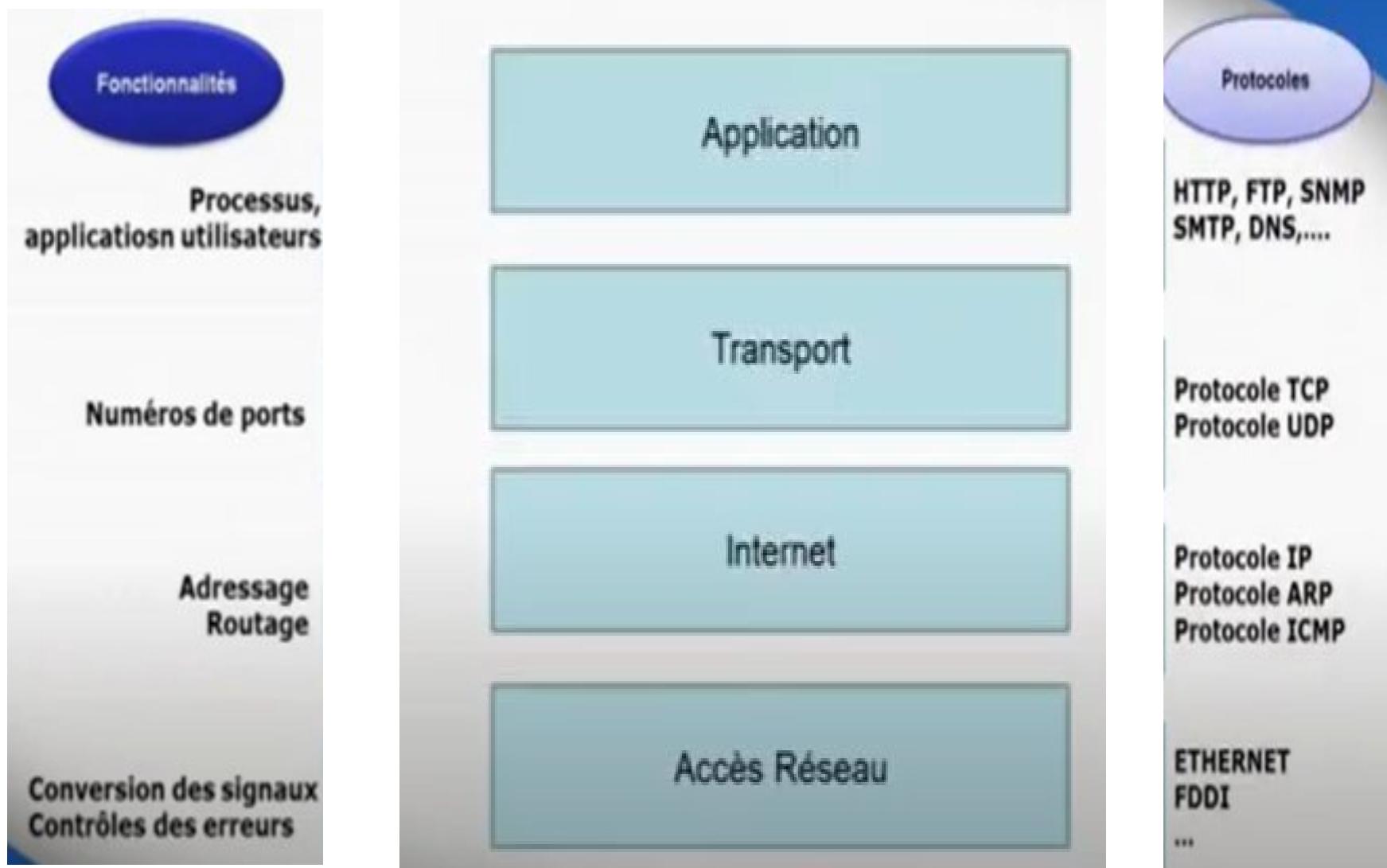
- 1. Dans le contexte du modèle OSI, qu'est qu'une PDU ?*
- 2. Quel est le nom donné aux unités de transfert pour les différentes couches ?*
3. Quelle est la caractéristique principale ajoutée dans un paquet de chacune des couches suivantes
 - o Couche transport
 - o Couche réseau
 - o Couche liaison de données

PDU (Protocol Data Unit) est une unité de données transmise entre deux couches **identiques** du modèle OSI (deux couches équivalentes du système distant). Chaque couche ajoute ses propres informations (comme des en-têtes ou des contrôles) aux données avant de les envoyer à la couche suivante, afin d'assurer une communication correcte entre les systèmes.

Etude des couches TCP /IP



Etude des couches TCP /IP



Programme : grands titres

- 1 Généralité sur réseaux informatique
- 2 Protocole et modèle : Modèle de référence OSI et TCP/IP
- 3 Modèle TCP/IP: couche accès réseau
- 4 Modèle TCP/IP: couche internet (adressage et routage)

CHAPITRE 3

Etude des couches TCP

/IP:

Couche Accès réseau



Etude des couches TCP IP :

Couche Accès réseau

N°	Nom	Description
4	Application	Couches 7 à 5 du modèle OSI
3	Transport	Qualité de transmission
2	Internet	Sélection du chemin
1	Accès Réseau	Reprend les couches 1 et 2 du modèle OSI



Application
http, ftp, pop3...

TCP/UDP

IP

Liens



Etude des couches TCP IP :

Couche Accès réseau

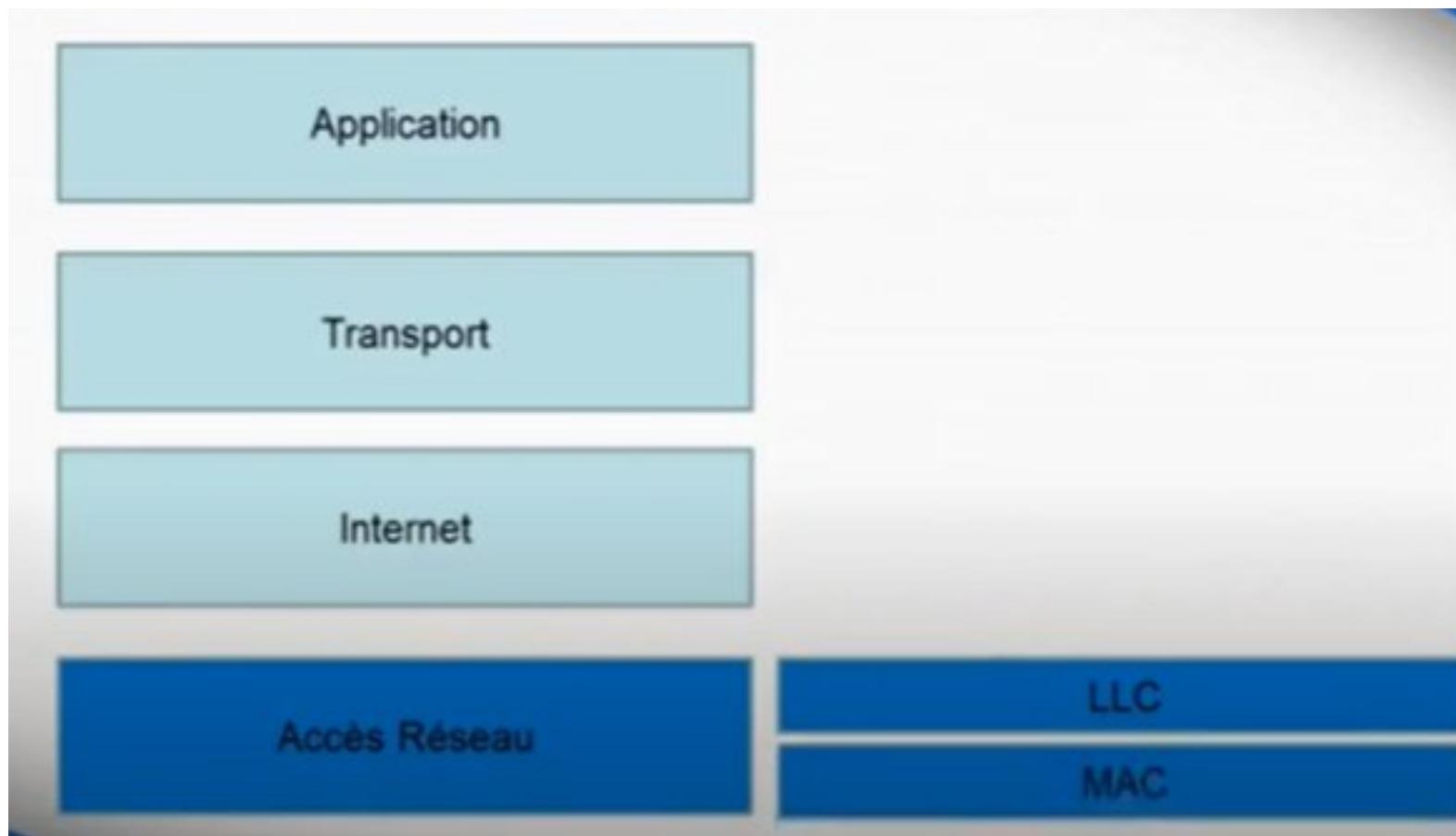
Elle contient toutes les spécificités concernant la transmission des données sur un réseau physique:
Réseau local (ethernet , ...), ligne téléphonique,

- * L'acheminement ses données sur la liaison
- * Coordination de la transmission des données (synchronisation)
- * Format des données
- * Conversion des signaux analogiques/ numériques
- * Contrôle des erreurs à l'arrivée



Etude des couches TCP IP :

Couche Accès réseau



Etude des couches TCP IP :

Couche Accès réseau

2 sous couches:

Le niveau Mac : contrôle d'accès au support

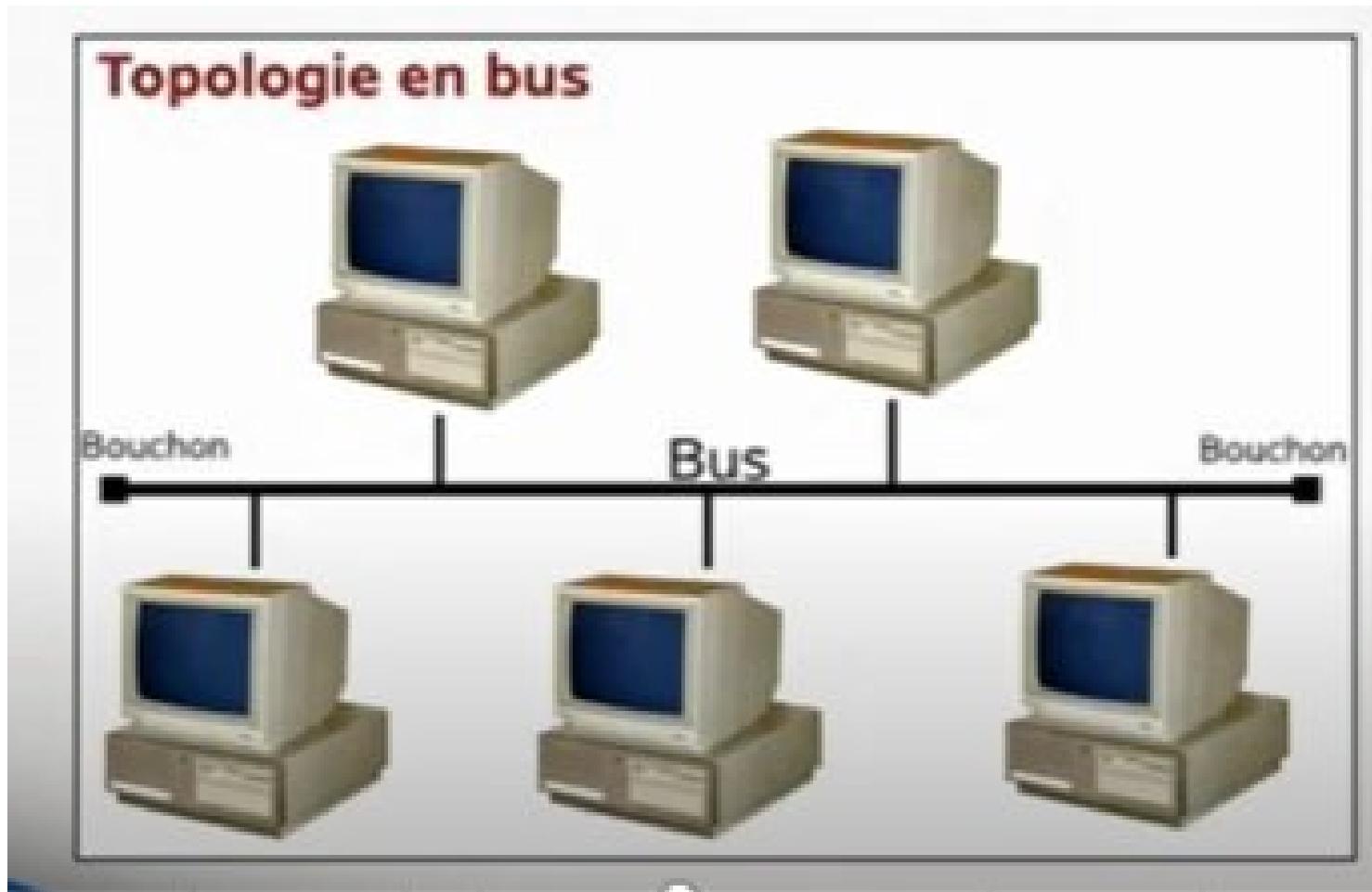
Le niveau LLC: contrôle d'erreurs et de flux



Exemple: le réseau Ethernet



Le réseau Ethernet classique



Les câble réseau



10 Base-5: câble coaxial de gros diamètre

10 Base-2: câble coaxiale de fable diamètre

10 Base-T: Paire torsadée, débit attient est d'environ 10 Mbps

100Base -TX: comme 10 Base-T avec une vitesse de 100Mbps.



On parle de catégories de câbles: CAT5 → CAT8
100 Mbit/s->40 Gbit/s

On parle aussi de différents blindages Câble U/UTP, S/FTP, SF/FTP...

Les câble réseau

Fibre optique



Représentation d'un bit

1 bit correspond à une impulsion signifiant 0 ou 1

Exemples :

Signal électrique : 0 = 0 volts et 1 = +5 volts

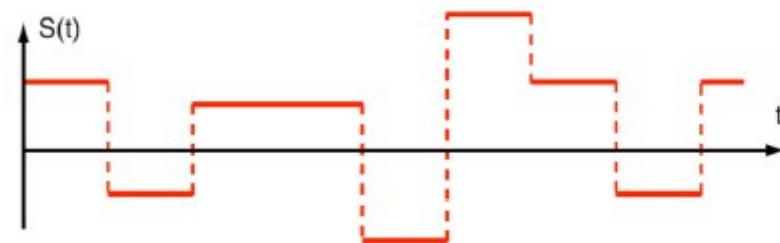
Signal optique : 0 = faible intensité et 1 = forte intensité

Transmission sans fil : 0 = courte rafale d'onde et 1 = rafale d'onde plus longue

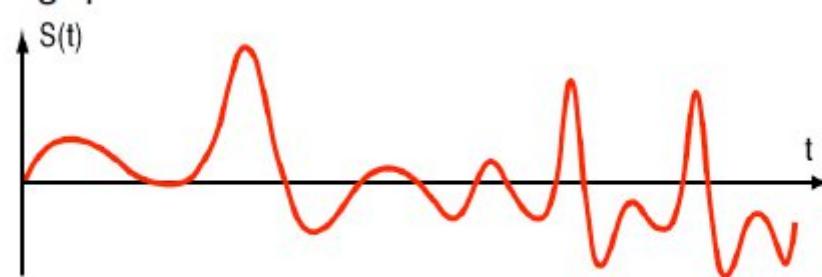
Deux techniques de transmission

Pour transmettre des données, on peut soit utiliser :

Signal numérique variant de manière
discontinue dans le temps



Signal analogique variant de manière
continue dans le temps



Affectation d'un bit lors de sa transmission

Propagation : temps mis par un bit pour se déplacer dans le média

Atténuation : perte de la force (amplitude) du signal

Bruit : ajout indésirable d'énergie à un signal causé par des sources d'énergie se trouvant à proximité

Latence : retard de transmission causé par le temps de déplacement d'un bit dans le média et la présence de circuits électroniques dans le cheminement

Collisions : lorsque deux ordinateurs utilisant le même segment de réseau émettent en même temps

Caractéristiques d'un support de transmission

- ✓ Notion de Bande Passante
- ✓ Notion de Rapidité de modulation
- ✓ Notion de Débit binaire et de Valence
- ✓ Notion de bruit

Performances temporaires

- ✓ Temps de propagation
- ✓ Temps d'émission
- ✓ Temps de transfert: Latence



Caractéristiques d'un support de transmission

- L'infrastructure d'un réseau, la qualité de service offerte, les solutions logicielles à mettre en œuvre dépendent largement des supports de transmission utilisés.
- Les supports de transmission exploitent les propriétés de conductibilité des métaux(paires torsadées, coaxial...) ou celles des ondes électromagnétiques (faisceau hertzien, fibres optiques, satellite...).
- Un support de transmission est essentiellement caractérisée par son **impédance caractéristique** et sa **bande passante**. Ces paramètres conditionnent les possibilités de transmission en termes de **débit** et de distance franchissable.



Caractéristiques d'un support de transmission

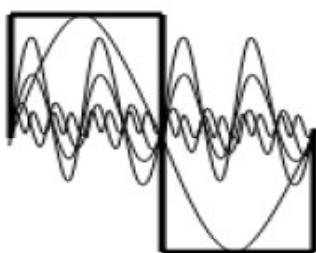
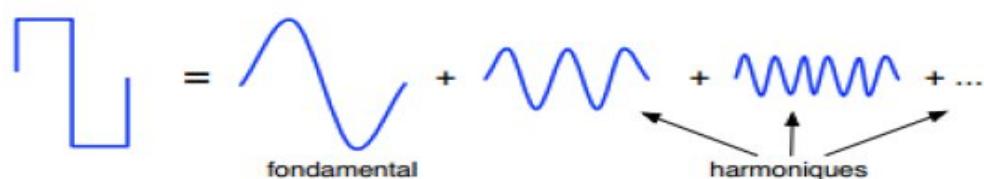
1.1. Notion de Bande Passante

Série de Fourier

Fourrier a montré que tout signal carré $s(t)$ peut s'écrire sous la forme :

$$S(t) = S_0 + \sum_{i=1}^{\infty} S_i \cos(i\omega t + \phi_i)$$

En effet, un signal non sinusoïdal peut être reconstruit en superposant un

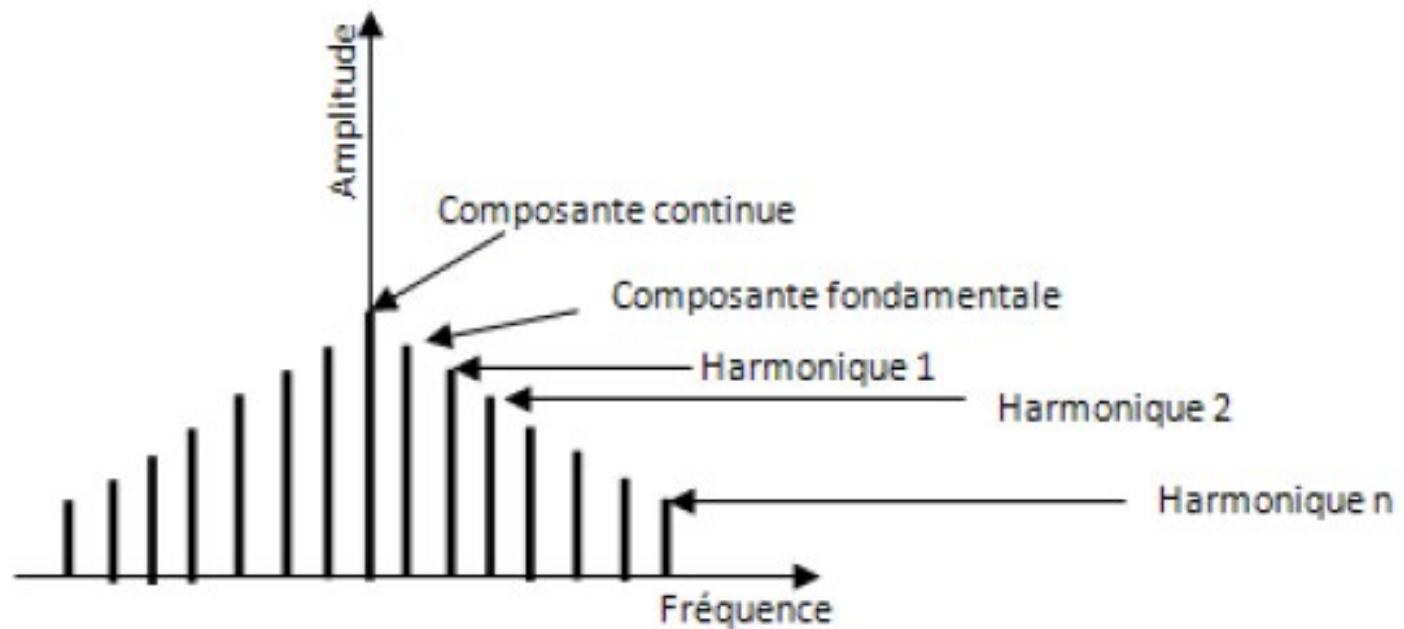


Série de Fourier

Caractéristiques d'un support de transmission

Spectre d'amplitude

- La composante centrale est dite composante continue(S_0).
- Les composantes adjacentes à la composante continue sont dites composantes fondamentales(S_1, S_{-1}).
- Toutes les autres composantes sont appelées composantes harmoniques



Caractéristiques d'un support de transmission

Fréquence de coupure

Certaines fréquences sont considérées faibles car elles seront rapidement atténuées lorsqu'elles sont utilisées. D'autres fréquences sont considérées aigues car elles sont dangereuses pour le support de transmission.

Dans le spectre de fréquence, il existe un intervalle de fréquences qu'on peut utiliser pour transmettre la donnée. La borne inférieure et la borne supérieure de cet intervalle sont notées fréquences de coupure.

Toute fréquence F_i n'appartient pas à $[F_{c_1}, F_{c_2}]$ ne sera pas utilisée.

Caractéristiques d'un support de transmission

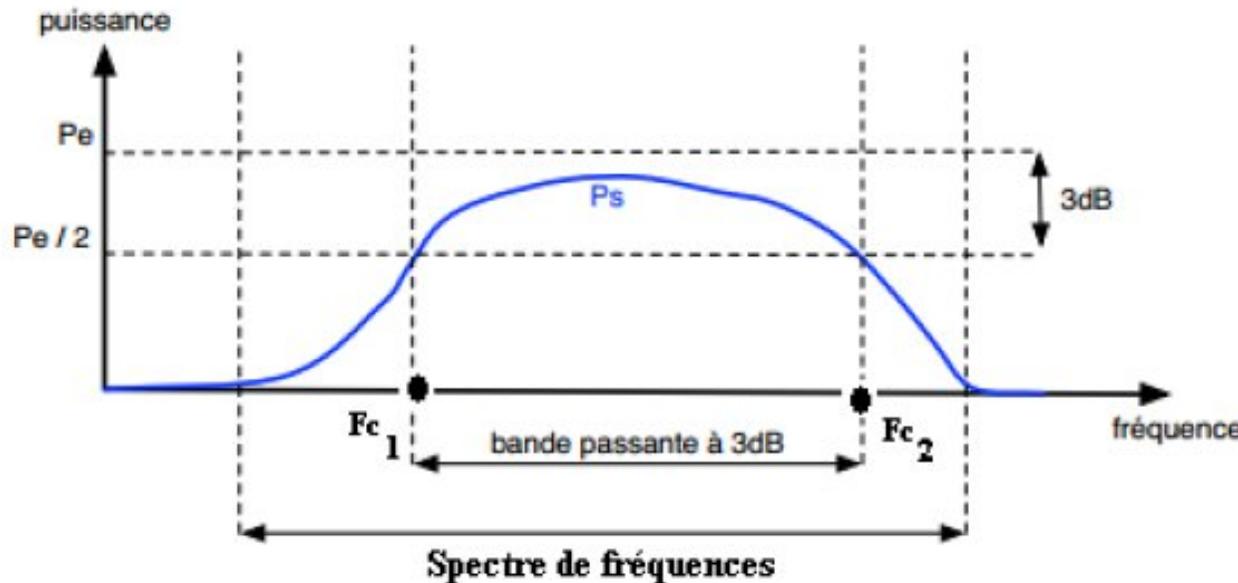
Bande passante

On appelle bande passante l'intervalle des fréquences utilisables pour la transmission des données sur un support de transmission.

Sachant que le symbole transmis est le bit, l'unité de la bande passante est le Hertz ou le bit par seconde(bps).



Caractéristiques d'un support de transmission



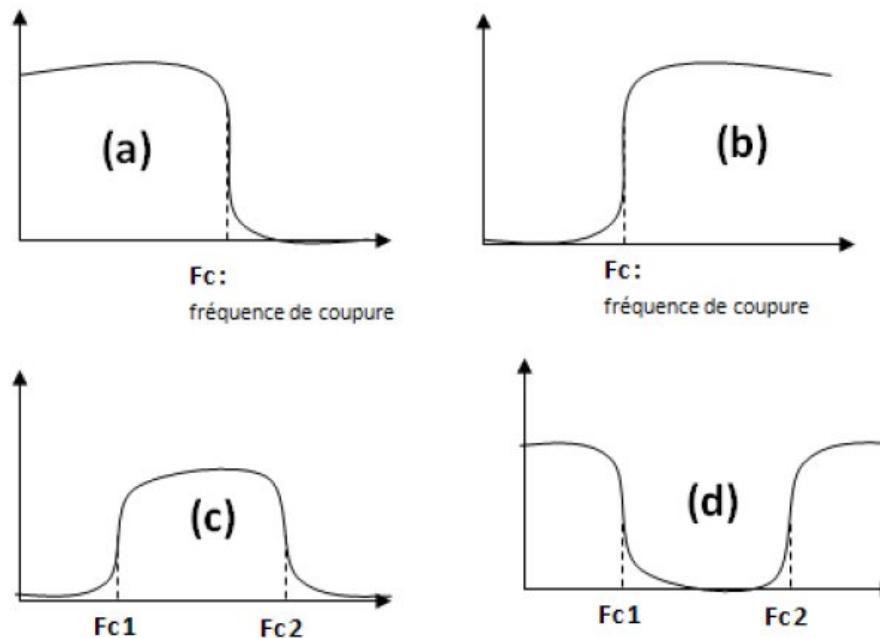
L'affaiblissement du signal électrique se mesure en décibel(db) par la formule suivante : $A = 10 \log_{10} \left(\frac{P_e}{P_s} \right)$

La bande passante est définie comme étant la plage de fréquence dans laquelle les signaux appliqués à l'entrée du support subissent un affaiblissement inférieur à 3 dB ($A < 3\text{db}$).

Caractéristiques d'un support de transmission

Filtrage des fréquences

- Pour obéir à une bande passante sur un support de transmission, il est nécessaire de filtrer les fréquences et ne laisser passer que celles faisant partie de la largeur de la bande.
- Différents types des filtres existaient :



(a) filtre passe-bas (b) filtre passe-haut (c) filtre passe-bande (d)
filtre stop-bande

Caractéristiques d'un support de transmission

Capacité

- La largeur de la bande passante de la voie de transmission est définie par :

$$W = Fc_2 - Fc_1 \text{ (Hz)}$$

où Fc_1 est la fréquence transmise la plus basse et Fc_2 la plus haute

- Lorsque l'on parle d'une bande passante, on indique une largeur d'intervalle sans préciser les bornes de cet intervalle.
- La bande passante détermine directement la capacité de transmission d'une voie :

$$C = 2 W \text{ (bauds)}$$



Caractéristiques d'un support de transmission

1.2. Notion de rapidité de modulation

- Un support de transmission se comporte comme un filtre passe-bande. Certaines composantes seront ou bien atténuerées ou retardées donnant lieu à des signaux étalés. Ces signaux entrent en conséquence en interférence et peuvent donner lieu à des symboles erronés.
- Pour éviter ces interférences, il faut limiter la bande de fréquence utilisée. Ceci implique en d'autres termes, il faut limiter les **transitions** entre les symboles.
- Soit R_{max} le nombre de transition maximum qu'un système de transmission peut supporter par unité de temps.
- On définit alors le **critère de Nyquist** par l'équation suivante :

$$R \leq 2W,$$

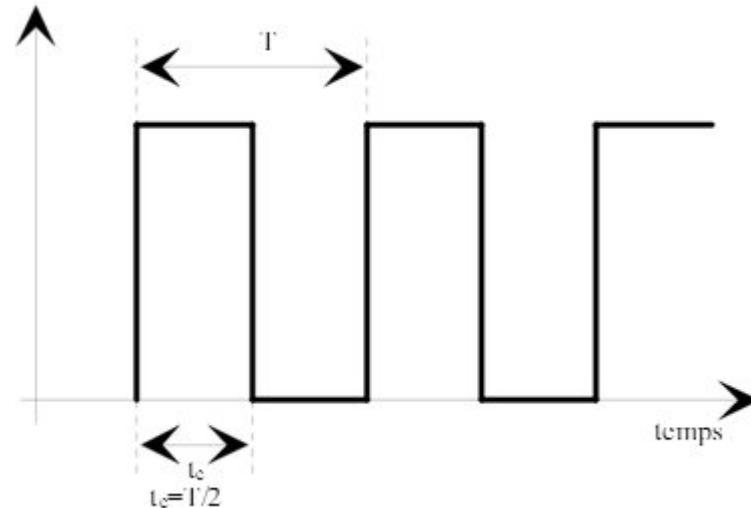
- On appelle **rapidité de modulation**, vitesse de modulation ou rapidité de transmission :

$$R = 1 / t_e = 2 * f \text{ (bauds)}$$

- On définit le **temps élémentaire** ou temps bit (durée du bit), une succession de 0 et 1 constitue un signal périodique de fréquence f et de période T tel que :

$$f = 1 / T \text{ (Hz)}$$

et $T = 2 * t_e \text{ (sec)}$



Exemple d'application

Quelle est la rapidité de modulation admissible sur une voie téléphonique ayant une bande passante allant de 300 Hz à 3400 Hz ?

Caractéristiques d'un support de transmission

1.3. Notion de Débit binaire et Valence

On appelle **débit binaire (vitesse de transmission)** le nombre de bits véhiculés par seconde sur une voie.

$$D = \frac{N}{t_e} = N * R$$

avec :

N : Nombre d'éléments binaires (bit).

t_e : Temps élémentaire (durée du bit) (s).

D : Débit binaire (bits/s) ou (bps).



Caractéristiques d'un support de transmission

- La **valence** est le nombre d'états significatifs différents que peut prendre un signal.

$$V(\text{Valence}) = 2^N \Rightarrow N = \log_2 V$$

Une valence de valeur V permet le transport de N (bits)

$$\text{On a : } D(\text{débit}) = R \ Log_2(V) \ (\text{bit/s})$$

Exemple d'application

Un système de transmission numérique fonctionne à un débit de 9600 bits/s.

1) Si un signal élémentaire permet le codage d'un mot de **4** bits, quelle est la largeur de bande minimale nécessaire de la voie ?.

Caractéristiques d'un support de transmission

1.4. Notion de Bruit

Les signaux électriques peuvent subir des modifications suites aux phénomènes suivants :

Champs électromagnétiques entraînant un changement de la polarité, on parle de bruit impulsif.

Interférences électriques donnant lieu à un changement d'amplitude, on parle de bruit blanc.

Tout bruit donne lieu à des erreurs sur le signal.

Pour exprimer l'effet de ce bruit, on mesure souvent le rapport signal/bruit (S/B). Ce rapport s'exprime en décibels

$$\frac{P_s}{P_b} \text{ dB} = 10 \log \frac{P_s}{P_b}$$

Caractéristiques d'un support de transmission

- Le théorème de Shannon (1948) exprime l'importance du facteur S/B (signal sur bruit en dB). Selon Shannon, la valence d'un signal sur un canal non idéal se mesure comme suit :

$$V = \sqrt{1 + \frac{S}{B}}$$

Ce facteur limite la Capacité maximale :

$$C_{max} = (2 W) \times N = W \log_2(1 + S/B)$$

Exemple d'application

Calculer la capacité C sur une voix téléphonique RTC ayant une bande passante allant de 300 à 3400Hz et un rapport (S/B)_{dB}= 30db.



Caractéristiques d'un support de transmission

Remarque:

- Il ne faut pas confondre le **baud** avec le **bps** ou ***bit/seconde***.
- Le baud est l'unité de mesure du nombre d'informations effectivement transmises par seconde. Il est en effet souvent possible de transmettre plusieurs bits par symbole.
- La mesure en bps de la vitesse de transmission est alors supérieure à la mesure en baud.
- Les mesures en bauds et en *bits par seconde* sont égales lorsque le signal est bivalent (seulement 2 valeurs, 0 ou 1, alors la valence vaut 2).
- Même si les mesures sont égales, la signification de baud et de bps est différente.



Caractéristiques d'un support de transmission

Taux d'erreur

Un bruit introduit des erreurs. Une erreur est une modification d'un ou plusieurs bits.

Le taux d'erreur binaire (ζ_e ou BER : Bit Error Rate) exprime le rapport entre le nombre de bits reçus en erreur par le nombre total de bits envoyés.

$$\zeta_e = \frac{\text{nbredesbitsen erreurs}}{\text{nbretotalde bits}}$$



Performances temporaires

3.1.Temps de propagation (T_p)

C'est le temps nécessaire pour envoyer un bit d'une source à une destination.

$$\text{vitesse} = \frac{\text{distance}}{\text{temps}}$$

Exemple :

Pour une ligne téléphonique, le temps de propagation respecte la loi :

$10 \mu\text{s} \leq T_p \leq 40 \mu\text{s}$ pour chaque 1 km traversé.

Pour un coaxial, $T_p \simeq 4 \mu\text{s}$ pour chaque 1 km traversé.

Exemple d'application :

La célérité (vitesse) de la lumière (onde optique) est environ $3 \times 10^8 \text{ m/s}$.

Calculer le temps de propagation pour une distance de 1km.



3.2. Temps d'émission (concerné d'un émetteur)

- Le temps d'émission est le temps nécessaire pour émettre un volume **V** de données via une interface de débit **D**.

Le temps d'émission est le temps entre le premier et le dernier bits envoyés.

$$D = \frac{V}{T_e} \quad T_e = \frac{V}{D}$$

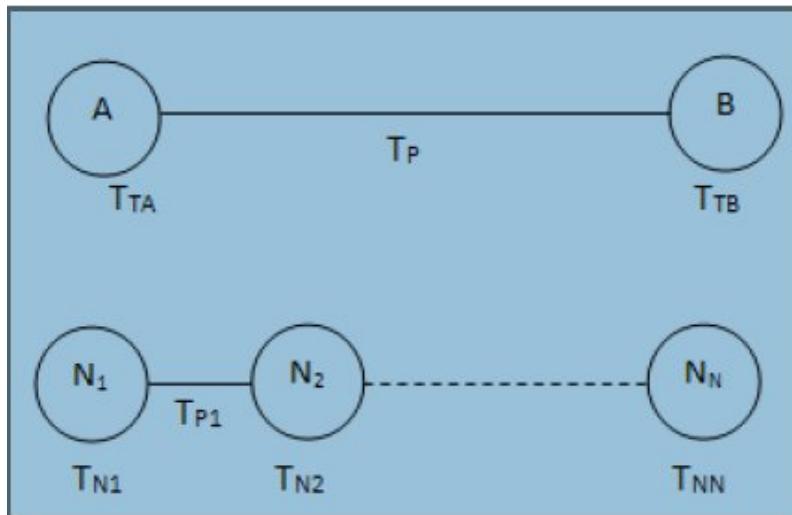
- Au niveau de chaque équipement N_i , les données subissent un traitement, pendant un temps $T_{traitement}$ avant d'être émise à la destination pendant une durée T_e .
- On note ce temps $T_{Ni} = T_e + T_{traitement}$

Performances temporaires

3.3. Temps de transfert : Latence ou Délai (concerné d'un réseau)

Le temps de transfert s'exprime alors comme suit :

$$L = \sum_{\text{node}} T_{T_i} + \sum_{\text{link}} T_{P_i}$$



Temps de transfert à travers un réseau

Performances temporaires

Exemple d'application 1:

Un message de volume $V=100$ bits est transmis sur un câble coaxial. La source a un débit d'émission de 24 kbps et est distante de 100 km de la destination.

Mesurer le temps de transfert , sachant que la vitesse de transmission est environ $5 \cdot 10^8$ m/s , et le temps de traitement est considéré négligeable.

Les codages en bande de base

Les codages usuels sont :

le code NRZ (non retour à zéro)

le code Manchester

Le codage Manchester

différentielle

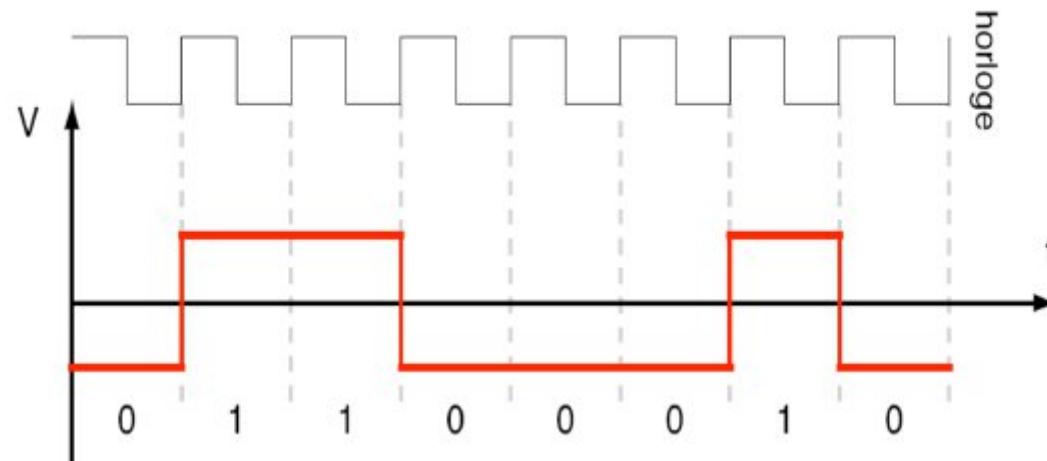
Le codage NRZI



Code NRZ (Non Return to Zero)

On code :

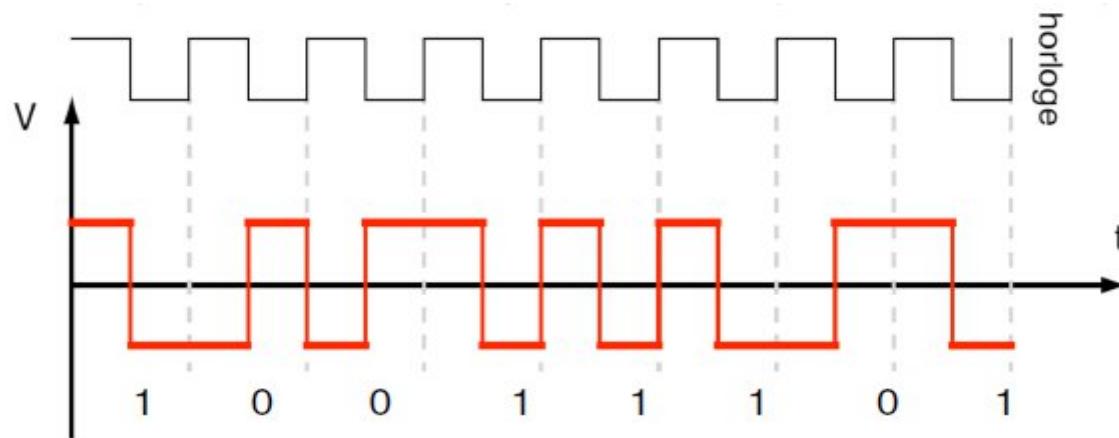
- par une tension négative le « 0 »
- par une tension positive le « 1 »



Code Biphasé ou Manchester

Le signal change au milieu de l'intervalle de temps associé à chaque bit.

Au milieu de l'intervalle il y a une transition de bas en haut pour un « 0 » (front montant) et de haut en bas pour un « 1 » (front descendant).



Principe : XOR entre les données et l'horloge
Codage utilisé pour Ethernet à 10 Mbit/s



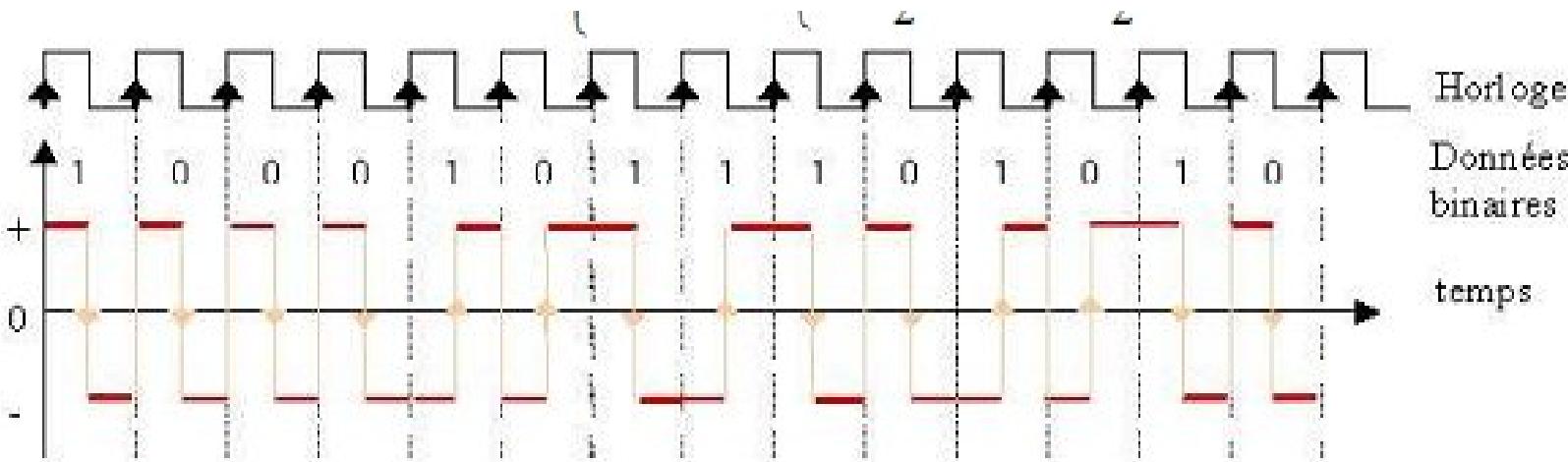
le code Manchester différentiel

- La transmission des données s'effectue toujours par l'intermédiaire de fronts placés au milieu des bits. Cependant, le choix du front s'effectue en fonction du précédent.

Ainsi:

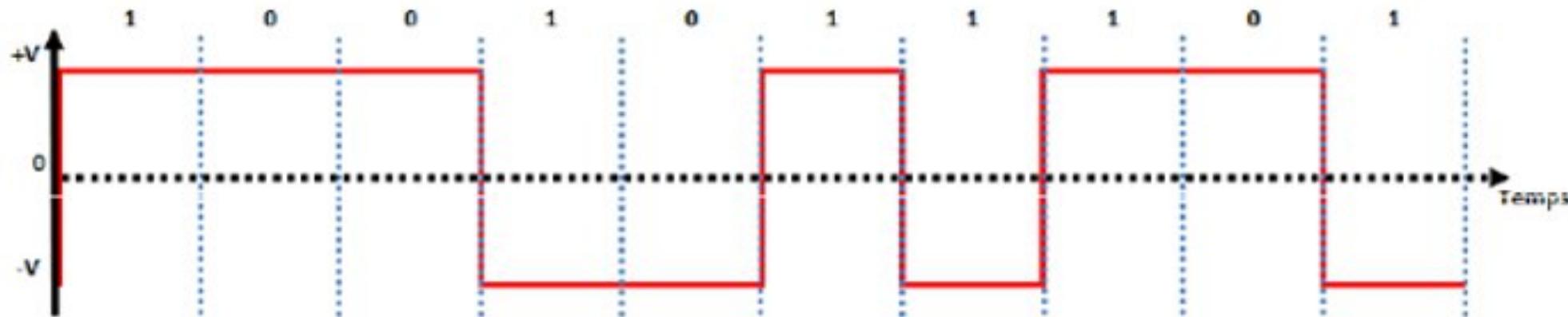
- - un état 0 produit un front identique au précédent (signaux en phase)
- - un état 1 produit un front inverse au précédent (signaux en opposition phase)

Avantage : indépendant de la polarité



— Le codage NRZI (No Return to Zero Inverted)

- Un bit à "1" entraîne un changement d'état (+V ou -V) au début du moment élémentaire
- Un bit à "0" n'entraîne aucun changement d'état et laisse le signal constant

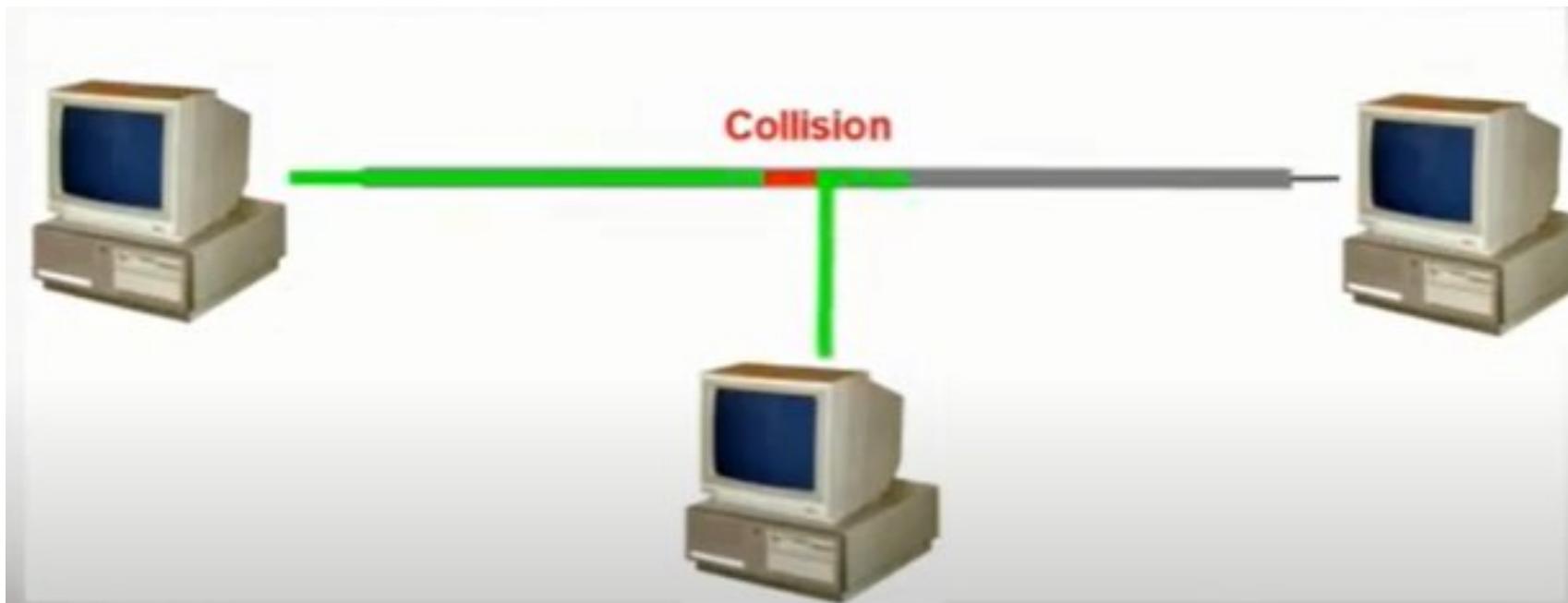


➤ Remarques :

- Améliore le codage binaire en augmentant la différence entre les "1" et les "0"
- Ne nécessite pas le repérage des fils
- Détection de la présence ou non du signal
- Nécessité d'un faible courant de transmission du signal
- De longues séries de bits identiques (à 0 ou 1), provoquant un signal sans transition, peuvent engendrer une perte de synchronisation
- Utilisé par USB, FDDI, Fast Ethernet 100BASE-FX, ...

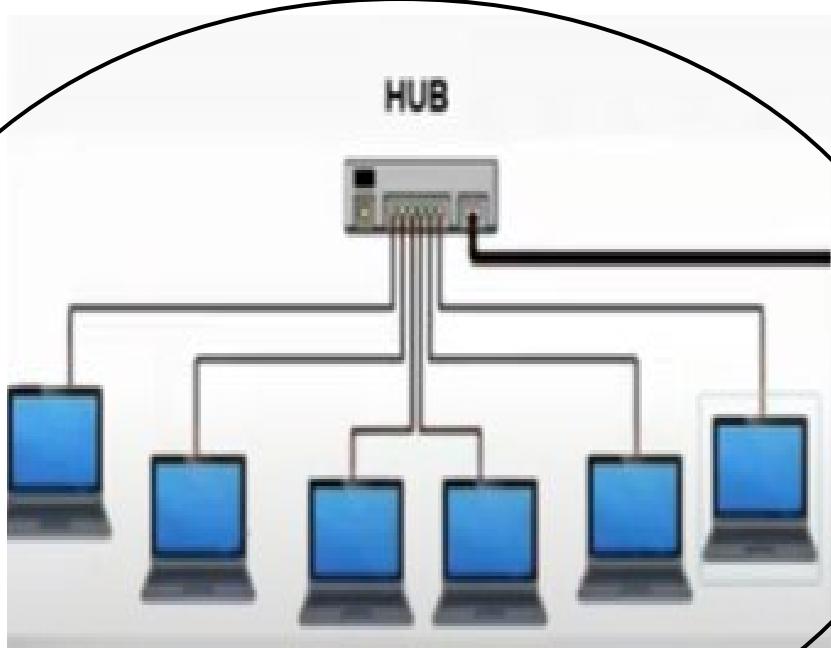
le réseau Ethernet classique

Problème de collision



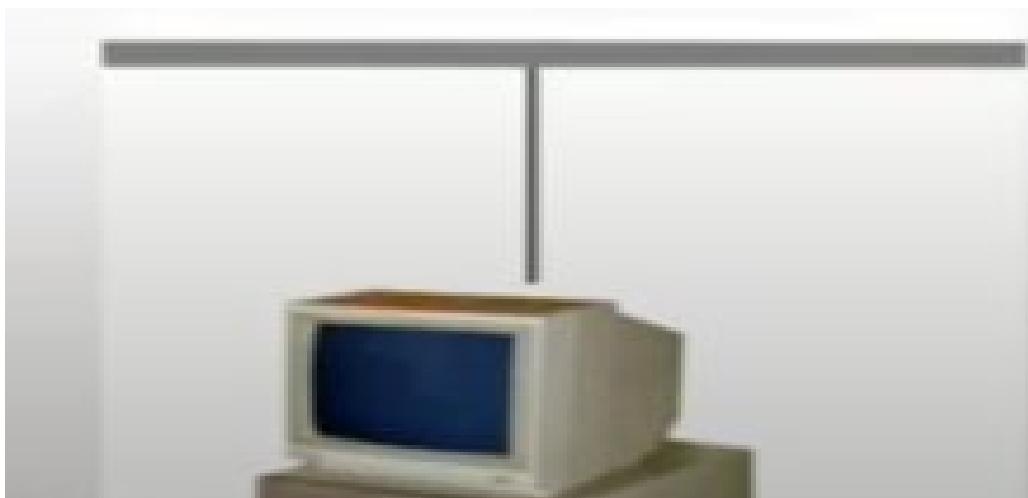
Domaine de collision

Le wifi et le bus forment aussi 01 domaine de collision



Le protocole CSMA/CD

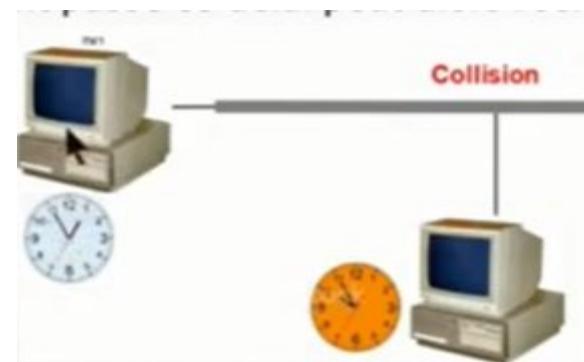
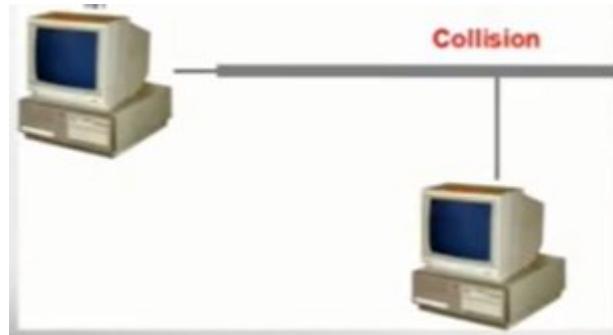
- La sous couche MAC utilise le protocole CSMA/CD: (carrier sense multiple Access with collision détection)
- Un protocole d'accès multiple avec :
 - Surveillance de porteuse (carrier sense) et
 - Détection de collision pour la transmission des trames (trains de bits)



Le protocole CSMA/CD

Chaque machine vérifie qu'il n'y a aucune communication sur la ligne avant d'émettre , Si deux machines émettent simultanément, alors il y a collision :

- 1. les deux machines interrompent leur communication**
- 2. attendent un délai aléatoire**
- 3. puis la première ayant passé ce délai peut alors réémettre**



Autres protocoles

Pour le wifi, on utilise le protocole CSMA/CA avec RTS/CTS

Principe CSMA/CA

Le CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) est un protocole utilisé dans les réseaux Wi-Fi pour éviter les collisions avant qu'elles ne se produisent.

Principe :

- 1 Écoute du canal → Si libre, passe à l'étape suivante.
- 2 Attente aléatoire → Pour éviter les envois simultanés.
- 3 Transmission des données → Si le canal reste libre.
- 4 Accusé de réception (ACK) → Si l'ACK n'est pas reçu, l'émetteur réessaie après un délai.



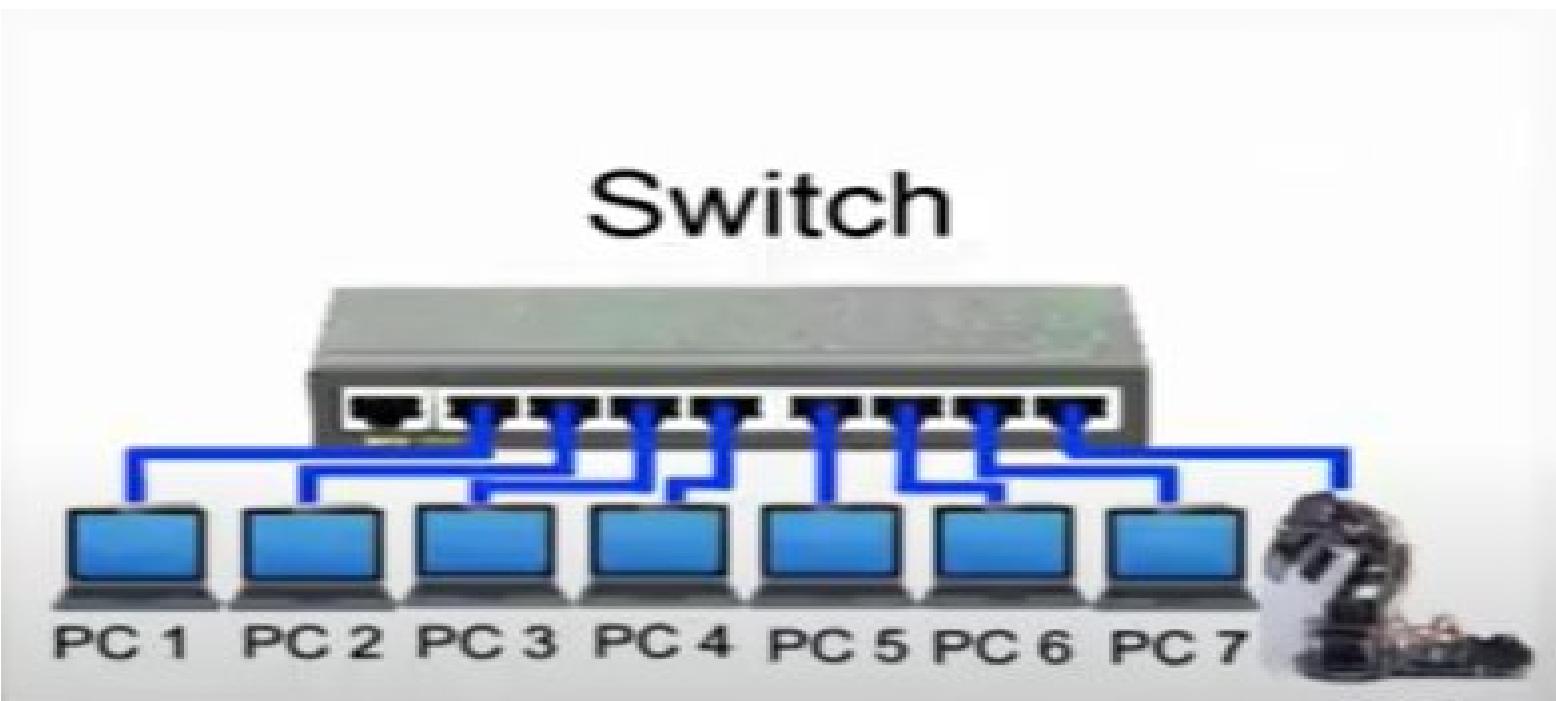
Différence entre CSMA/CA et CSMA/CD

◆ Protocole	◆ Utilisation	◆ Gestion des collisions
CSMA/CD (Collision Detection)	Réseaux filaires (Ethernet)	Déetecte la collision après qu'elle s'est produite et retransmet les données.
CSMA/CA (Collision Avoidance)	Réseaux sans fil (Wi-Fi)	Évite les collisions en écoutant le canal et en utilisant un délai aléatoire.

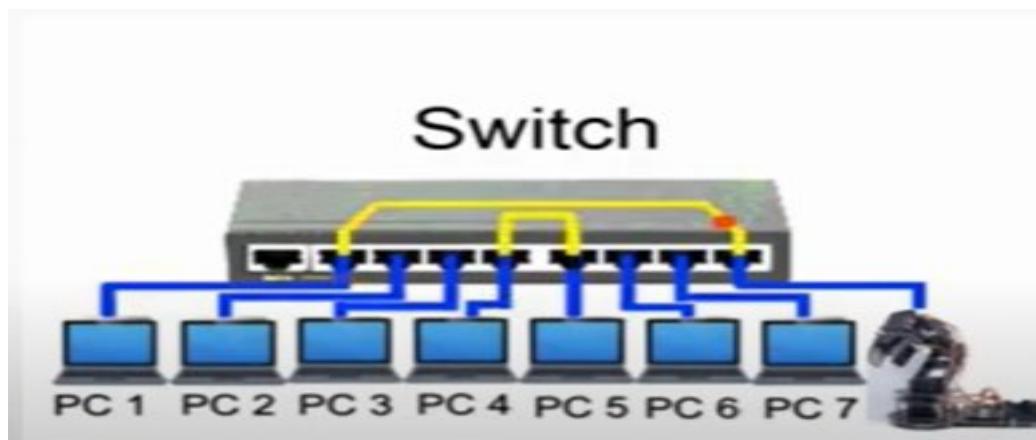


Ethernet Commuté

Switch

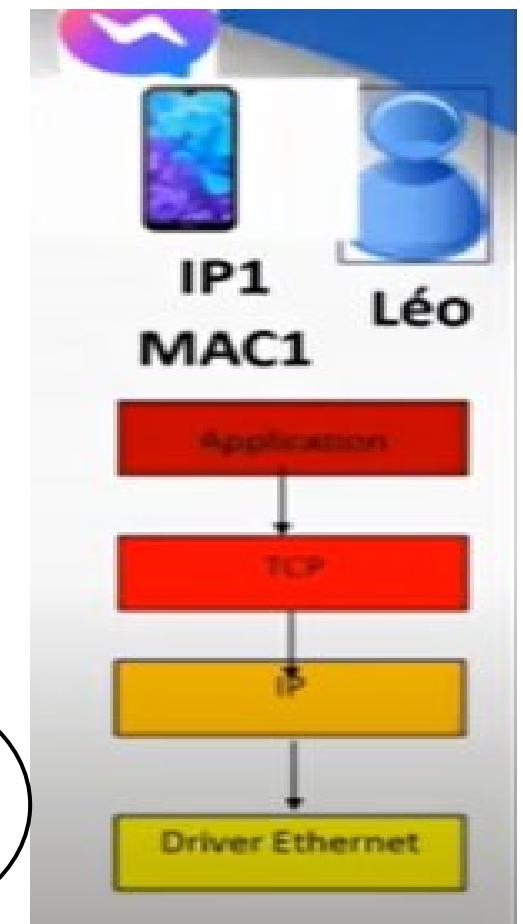
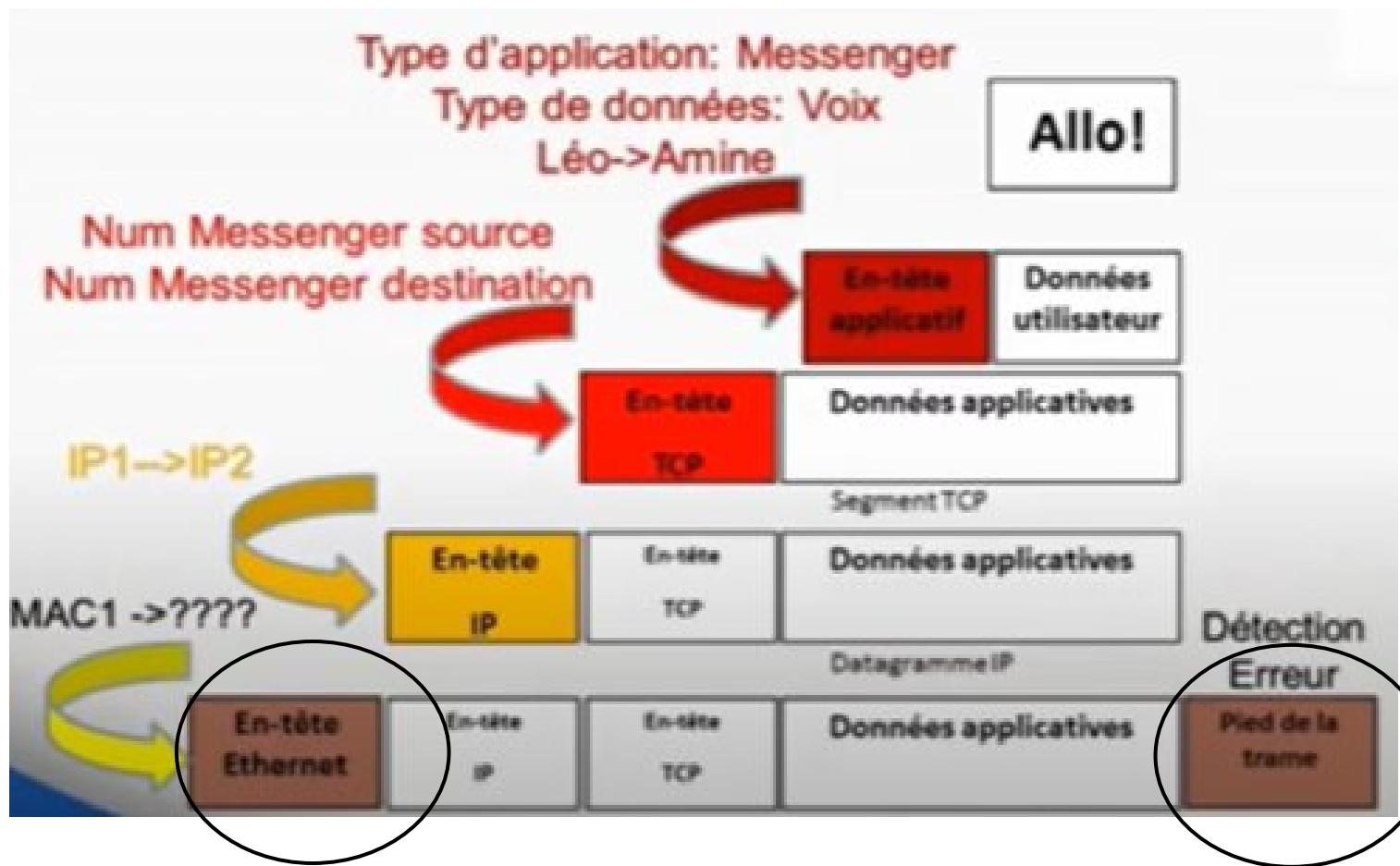


RB1

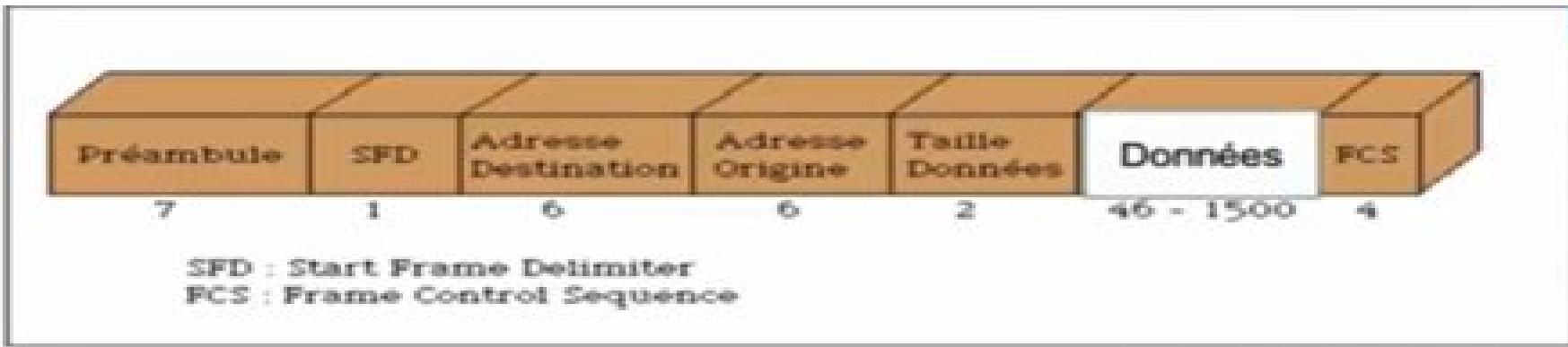


Niveau 2 Adresse MAC – Protocole Ethernet

Exemple d'encapsulation des données



La trame ETHERNET



Préambule : Annonce le début de la trame et permet aux récepteurs de se synchroniser(récepteurs sont prêts à recevoir les données sans erreurs)

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

Adresse MAC destinataire : Adresse MAC de l'interface (carte d'accès) Ethernet destinataire de la trame. On représente une adresse Ethernet comme ses 6 octets en hexadécimal séparés par des :

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

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

- Type: indique le type de protocole utilisé par la couche réseau (IPv4, IPv6, ARP, RARP...).
- Chaque protocole a sa propre structure de paquets.



La trame ETHERNET

Si le nombre de données n'atteint pas 46 octets, le champ est complété par une séquence de bourrage. Si les données sont insuffisantes pour former une trame dont la taille est supérieure ou égale à Lmin (46 octets), alors des données de bourrage sont rajoutées à l'émission et elles sont retirées à la réception avant de passer les données utiles à la couche supérieure.

Préambule 7 octets	Délimiteur de début de trame (1)	Adresse MAC Destination (généralement 6 octets)	Adresse MAC Source (généralement 6 octets)	Longueur du champ de données (2 octets)	Données	Bourrage (Complément pour obtenir 46 octets)	Code de contrôle de la trame (4 octets)

Les données de bourrage sont des octets à « 0 »



Adresse MAC

Un équipement Ethernet a une adresse unique au monde (adresse Ethernet ou adresse MAC) , les adresses IEEE 802.3 ou Ethernet sont codées sur 48bits (6 octets) , elle ont la syntaxe suivante:

.

3 octets	3 octets
Num de Constructeur	Num Série

Exemple

08:00:20:09:E3:D8 ou 8:0:20:9:E3:D8 .ou 08-
00-20-09-E3-D8 ou 08002009E3D8.



la trame HDLC (High Level Data Link Control)

Elle offre un service de transfert de données fiable et efficace entre deux systèmes adjacents. C'est un protocole utilisant le mode connecté

Format général d'une trame HDLC:

Fanion	Adresse	Commande	Données	FCS	Fanion
01111110	(8 bits)	(8 bits)	($n \geq 0$ bits)	(16 bits)	01111110

Fanion :

Chaque trame est délimitée par 2 fanions (flag) dont le rôle est d'indiquer le début et la fin d'une trame. Ils ont la valeur 01111110 (7E). Pour assurer la transparence en cas où un octet du flux de données aurait la valeur du délimiteur, un bit à 0 est inséré après 5 bits à 1. A la réception, le zéro est retiré dès qu'il se positionne derrière 5 bits.

Exemple: Données à envoyer : 111011110101011111101

Trame constituée avec fanions et bits de transparence :

01111110 11011110101011111 0 101 01111110

Programme : grands titres

- 1 Généralité sur réseaux informatique
- 2 Protocole et modèle : Modèle de référence OSI et TCP/IP
- 3 Modèle TCP/IP: couche accès réseau
- 4 couche réseau (adressage et routage)

Etude de la couche TCP/IP

Chapitre 4: couche réseau

Plan du chapitre 4

- I. Présentation de la couche IP**
- II. Définir l'adresse IP**
- III. Adresse IPv4**
- IV. Adresse IPv6**
- V. Routage**



Présentation de la couche IP

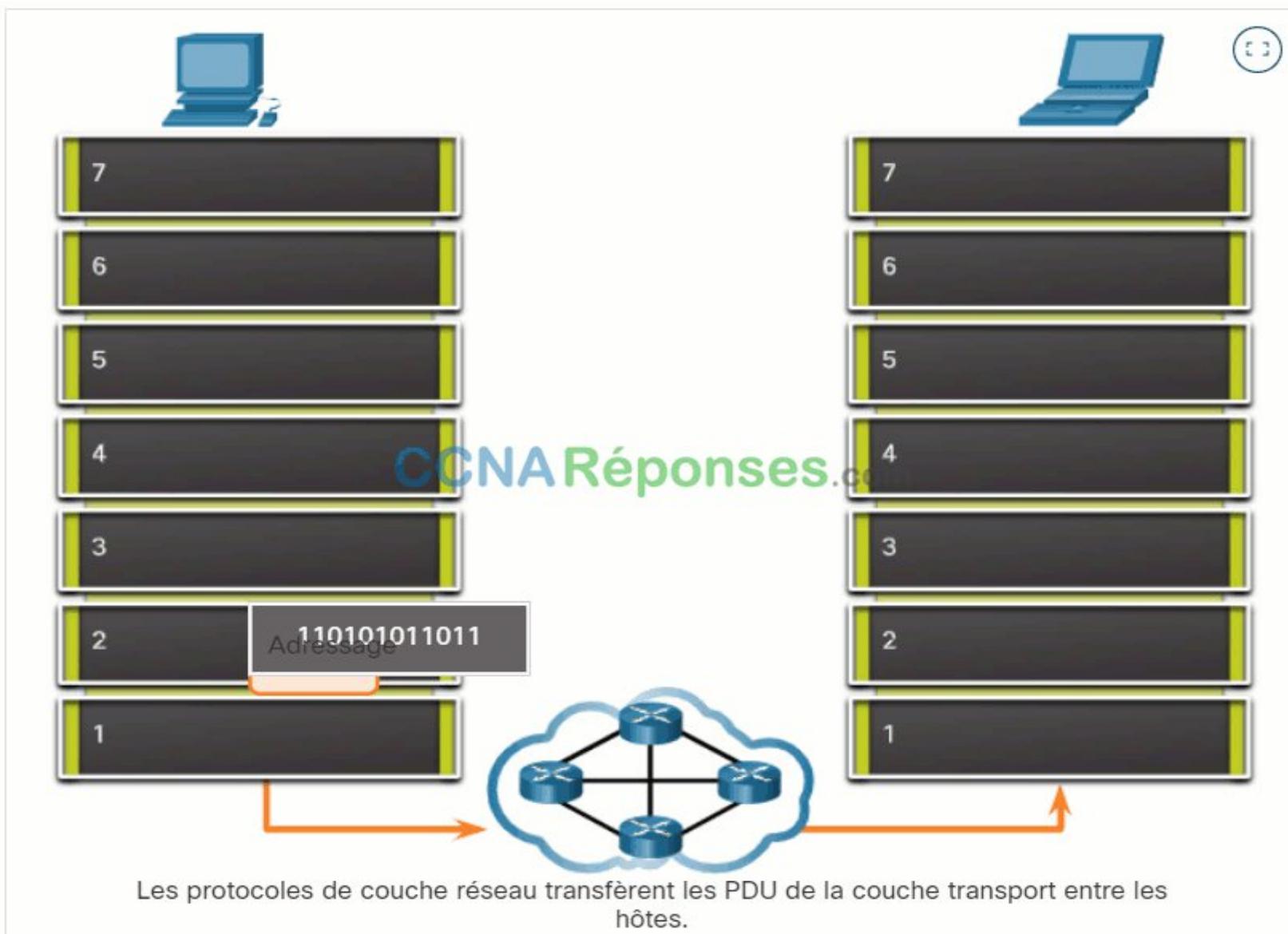
Principales fonctionnalités de la couche réseau

La couche réseau assure toutes les fonctionnalités de relai et d'amélioration de services entre entités de réseau, à savoir :

- L'encapsulation
- L'adressage
- Le routage
- La désencapsulation



Processus de communication



Transport des données via l'inter-réseau, qui est constitué de supports et de n'importe quels périphériques intermédiaires

Principales fonctionnalités de la couche réseau

L'adressage :

La couche réseau doit fournir un mécanisme pour l'adressage des périphériques finaux

Un périphérique final doit posséder une adresse **logique unique** qui permet de l'identifier sur le réseau

Le routage:

- * La couche réseau doit ensuite fournir des services pour diriger ces paquets vers leur hôte de destination

- * Les périphériques intermédiaires connectant les réseaux sont appelés **routeurs**.

- Leur rôle consiste à sélectionner les chemins afin de diriger les paquets vers leur destination => ce processus est appelé **routage**

- * Durant le routage via un inter-réseau , le paquet peut traverser de nombreux périphériques intermédiaires.



La couche réseau : protocole IP

7. Application

6. Présentation

5. Session

4. Transport

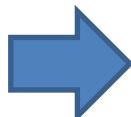
3. Réseau

2. Liaison de données

1. Physique

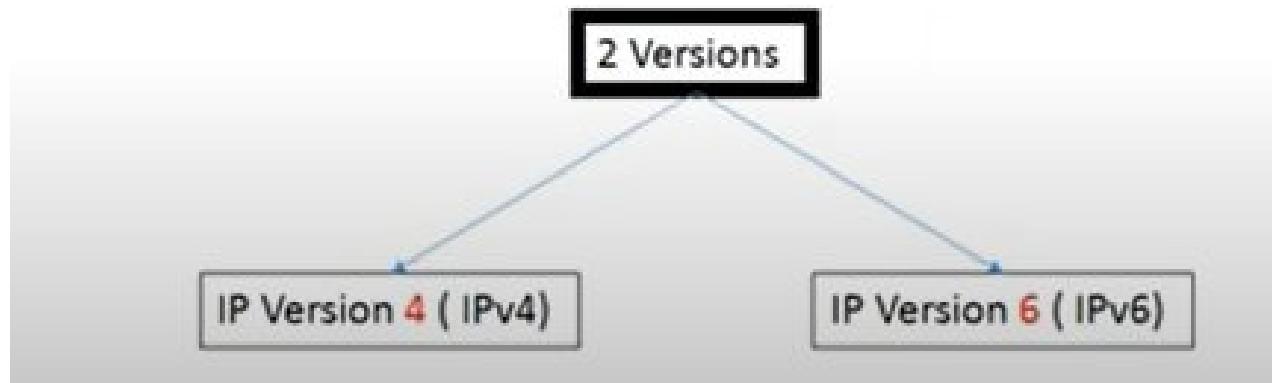
- Protocole IP version 4 (IPv4)
- Protocole IP version 6 (IPv6)
- Protocole IPX de Novell
- AppleTalk
- CLNS (Connectionless Network Service)/DECNet

Le protocole IP (IPv4 et IPv6) constitue le protocole de transport de données de couche 3 le plus répandu et fait l'objet de ce cours



C'est quoi une adresse IP ?

Une adresse IP : est un identifiant permettant le reconnaître un hôte (ordinateur en général) dans un réseau informatique

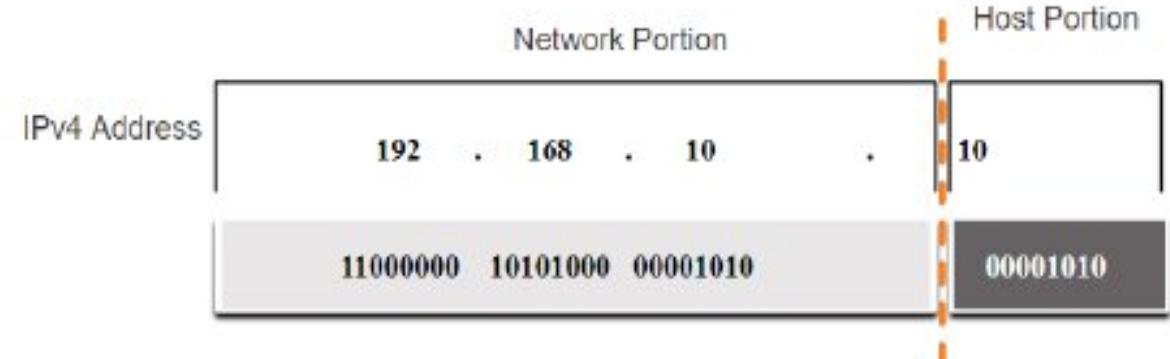
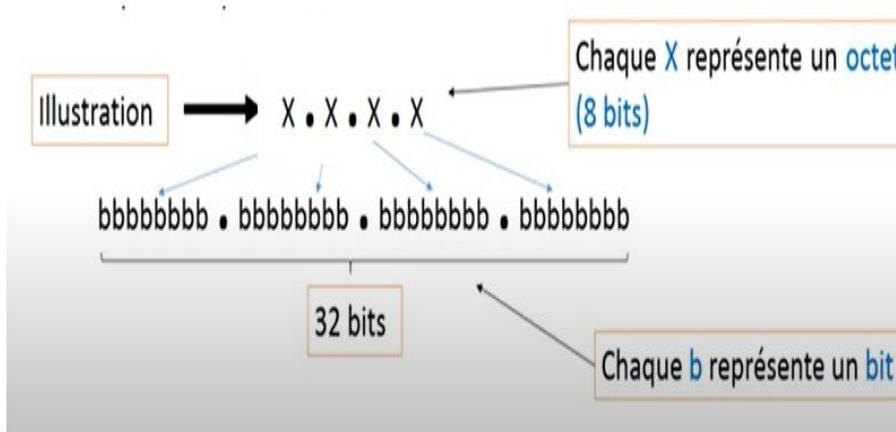


Structure de l'adresse IPv4

Les parties réseau et hôte

Une adresse IPv4 est une adresse hiérarchique de 32 bits qui se compose d'une partie réseau et d'une partie hôte.

- Lorsque vous déterminez la partie réseau et la partie hôte, il est nécessaire d'examiner le flux de 32 bits.
- Le masque de sous-réseau sert à déterminer la partie réseau d'une adresse IP.

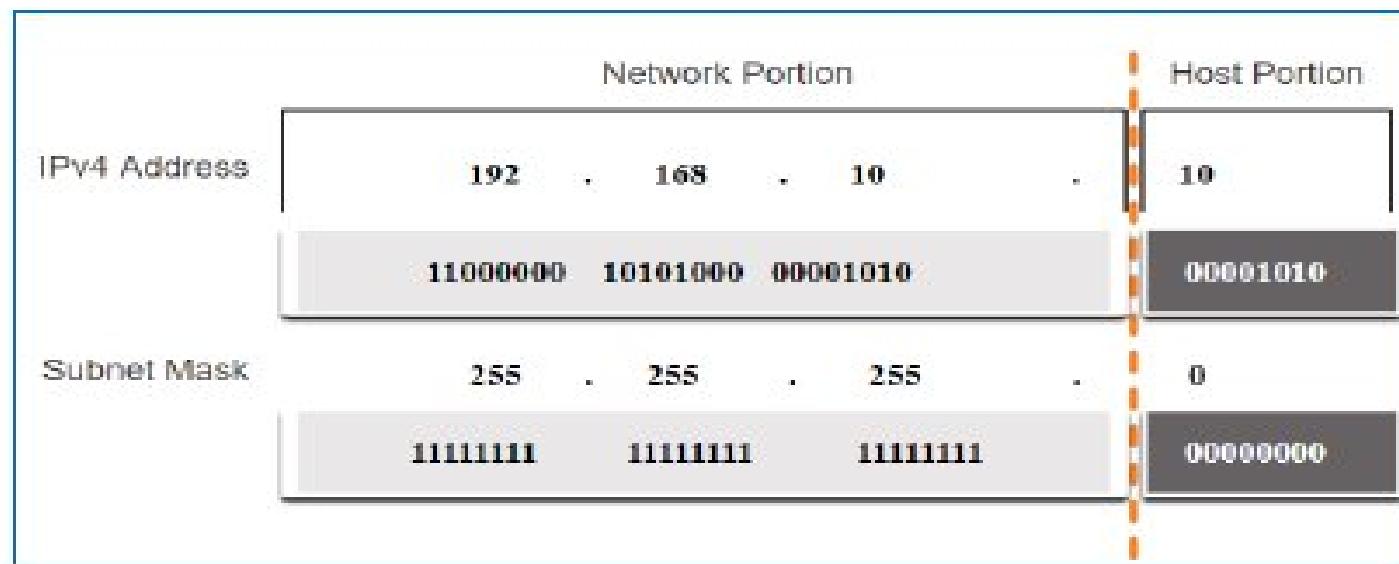


Structure de l'adresse IPv4

Le masque de sous-réseau

Pour identifier les parties réseau et hôte d'une adresse IPv4, chaque bit du masque de sous-réseau est comparé à l'adresse IPv4, de gauche à droite.

En réalité, le processus utilisé pour identifier la partie réseau
l'opération AND



Structure de l'adresse IPv4

longueur de préfixe

Une longueur de préfixe est une méthode fastidieuse d'exprimer une adresse de masque de sous-réseau.

En fait, la longueur de préfixe correspond au nombre de bit définis sur 1 dans le masque de sous-réseau.

Elle est notée au moyen de la « notation de barre oblique », il suffit donc de compter le nombre de bits du masque de sous-réseau et d'y ajouter une barre oblique.

Masque de sous-réseau	Adresse 32 bits	Préfixe Longeur
255.0.0.0	11111111.00000000.00000000.00000000	/8
255.255.0.0	11111111.11111111.00000000.00000000	/16
255.255.255.0	11111111.11111111.11111111.00000000	/24
255.255.255.128	11111111.11111111.11111111.10000000	/25
255.255.255.192	11111111.11111111.11111111.11000000	/26
255.255.255.224	11111111.11111111.11111111.11100000	/27
255.255.255.240	11111111.11111111.11111111.11110000	/28
255.255.255.248	11111111.11111111.11111111.11111000	/29
255.255.255.252	11111111.11111111.11111111.11111100	/30

Structure de l'adresse IPv4

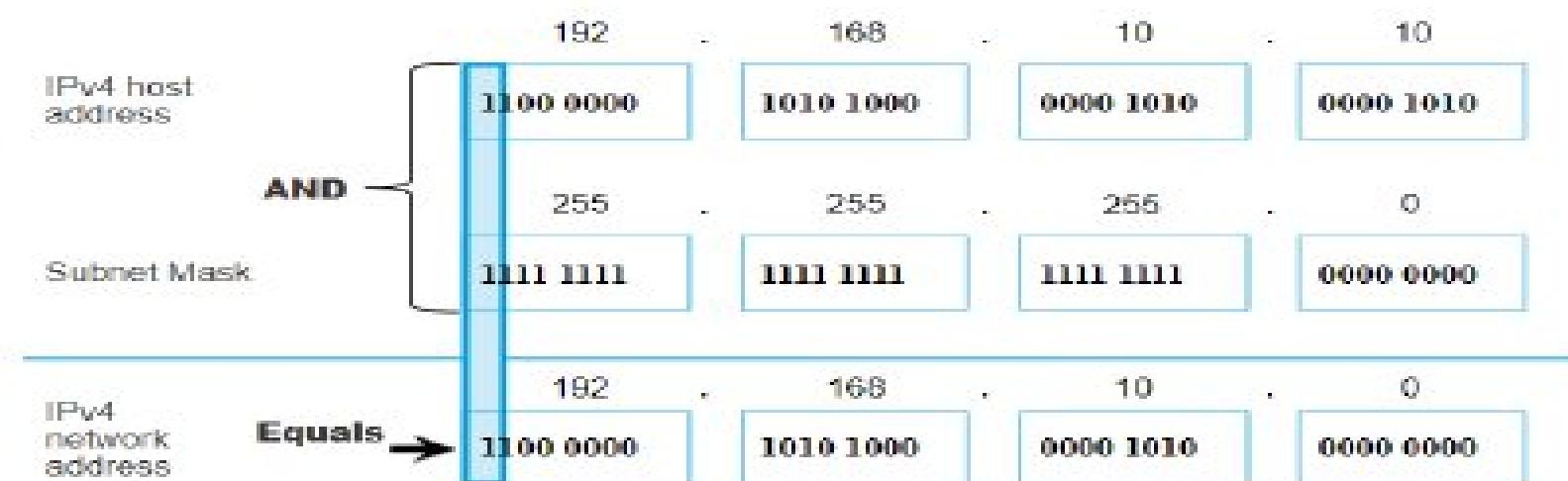
Détermination du réseau: AND (ET) logique

- Une opération logique AND est utilisée pour déterminer l'adresse réseau.
- le AND (ET) logique est la comparaison de deux bits où un 1 AND (ET) 1 produit un 1 et toutes les autres combinaisons produisent un 0.

1 AND 1 = 1, 0 AND 1 = 0, 1 AND 0 = 0, 0 AND 0 = 0

1 = Vrai et 0 = Faux

Pour identifier l'adresse réseau , l'adresse IPv4 d'un hôte est soumise bit par bit à l'opération AND de manière logique avec le masque de sous-réseau



Réseau, hôte et adresses de diffusion

- Adresse réseau
- Adresse de diffusion
- Première hôte utilisable
- Dernière hôte utilisable

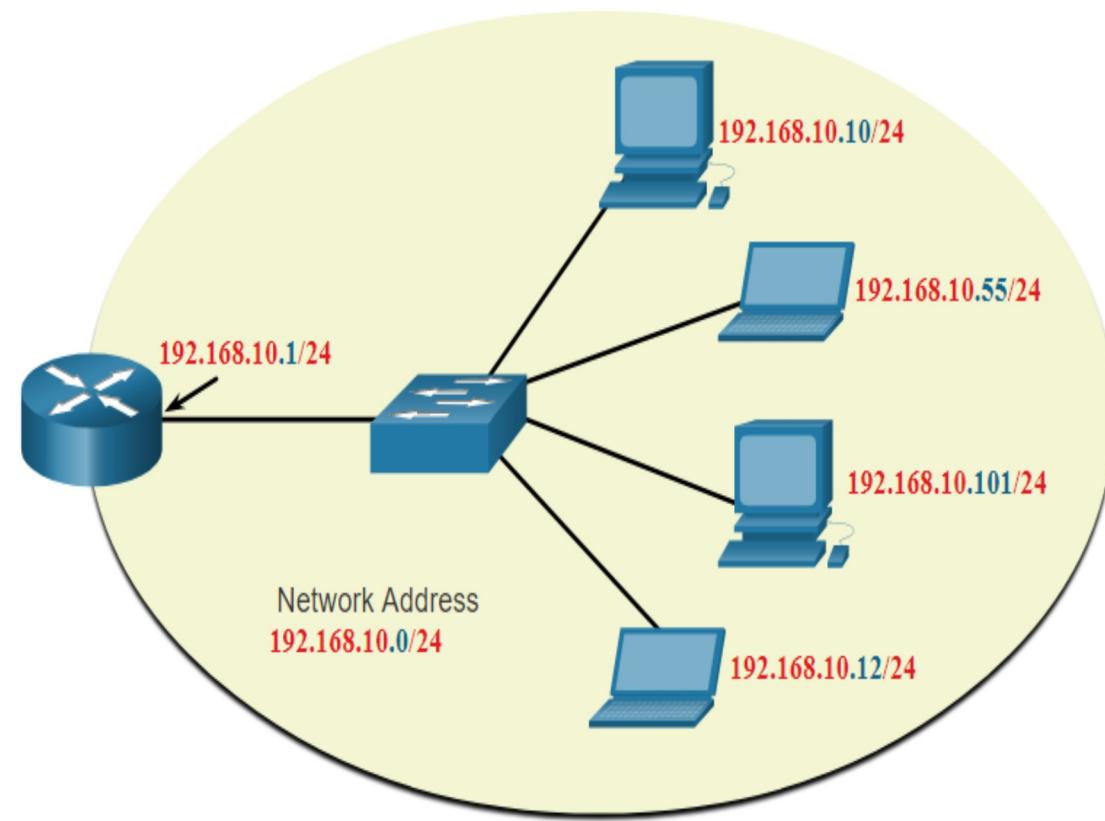
Adresses réseau, d'hôte et de diffusion

Au sein de chaque réseau se trouvent trois types d'adresses IP:

Adresse réseau

Adresses d'hôtes

Adresse de diffusion



	Partie réseau	Partie hôte	Bits d'hôte
Masque de sous-réseau . 255.255.255.0 or /24	255 255 255 11111111 111111 111111	0 00000000	
Adresse réseau 192.168.10.0 or /24	192 168 10 11000000 10100000 00001010	0 00000000	All 0s
First address 192.168.10.1 or /24	192 168 10 11000000 10100000 00001010	1 00000001	All 0s and a 1
Last address 192.168.10.254 or /24	192 168 10 11000000 10100000 00001010	254 11111110	All 1s and a 0
Adresse de diffusion 192.168.10.255 or /24	192 168 10 11000000 10100000 00001010	255 11111111	All 1s and a 0

©2021 Cisco et/ou ses filiales. Tous droits réservés. Informations confidentielles

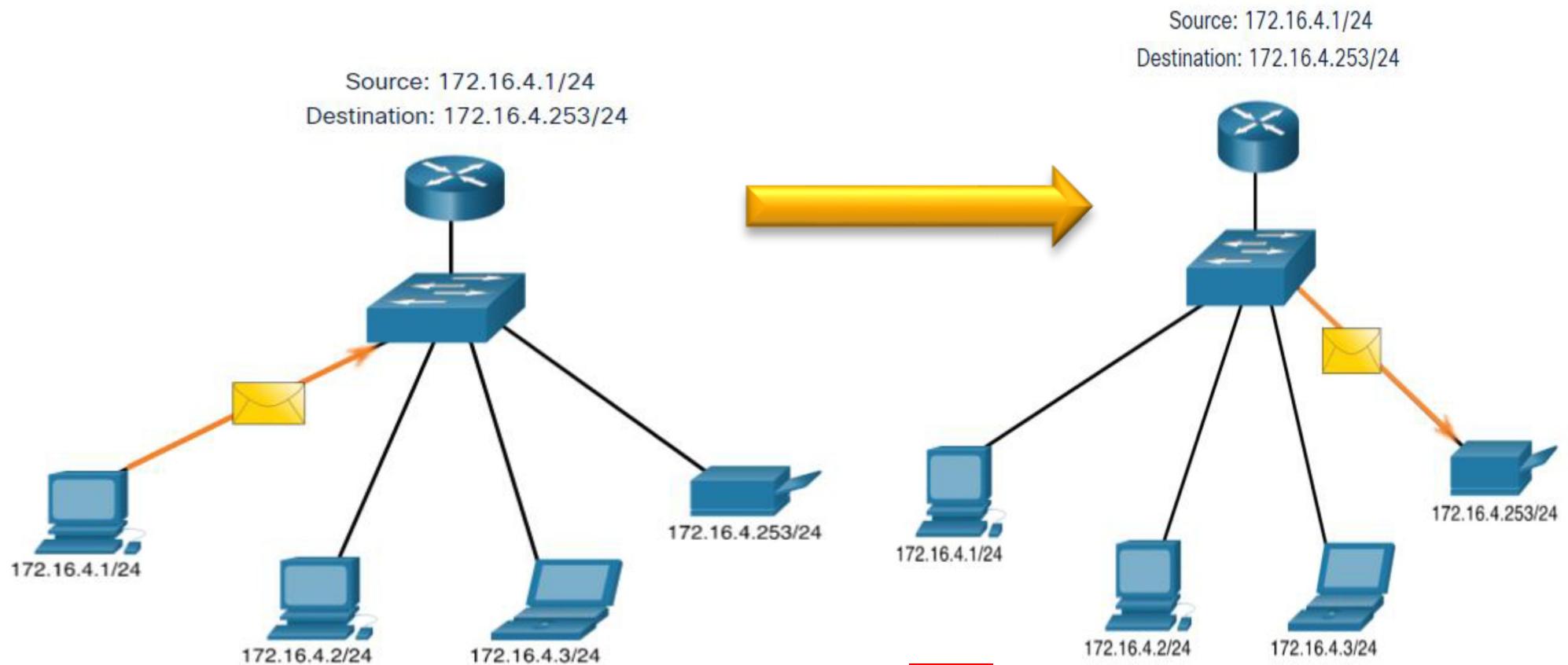
10

Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Monodiffusion

La transmission monodiffusion envoie un paquet à une adresse IP de destination.

- Par exemple, le PC à 172.16.4.1 envoie un paquet monodiffusion à l'imprimante à 172.16.4.253.

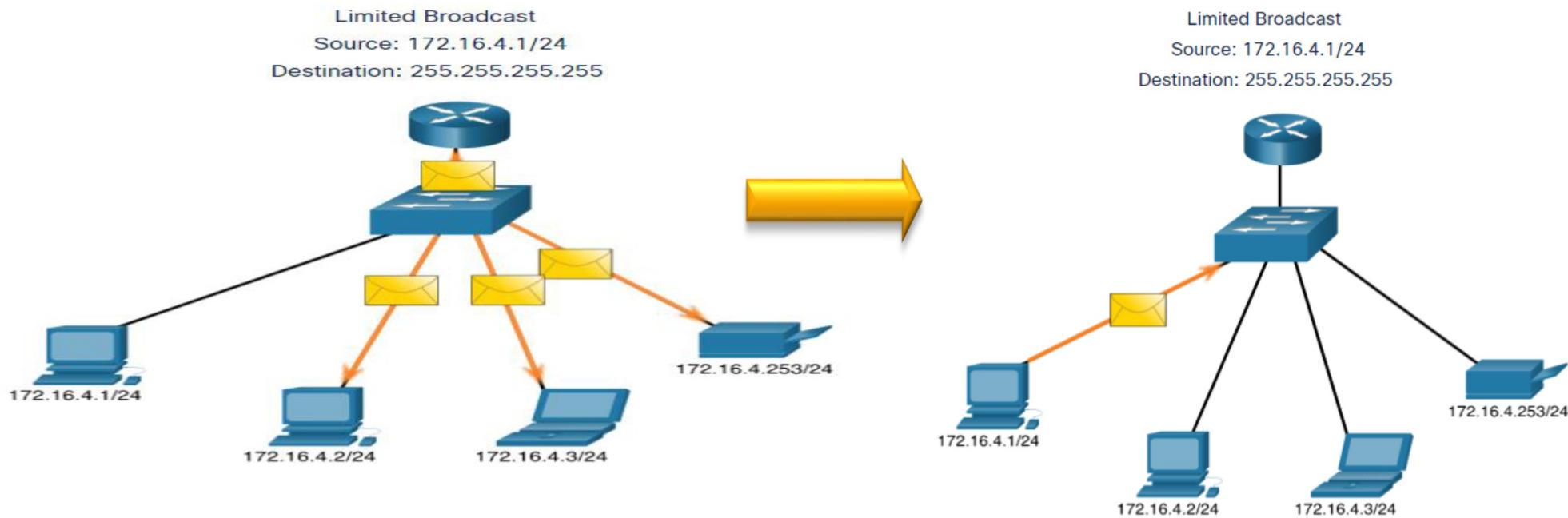


Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Diffusion

La transmission de diffusion envoie un paquet à toutes les autres adresses IP de destination.

- Par exemple, le PC à 172.16.4.1 envoie un paquet de diffusion à tous les hôtes IPv4.

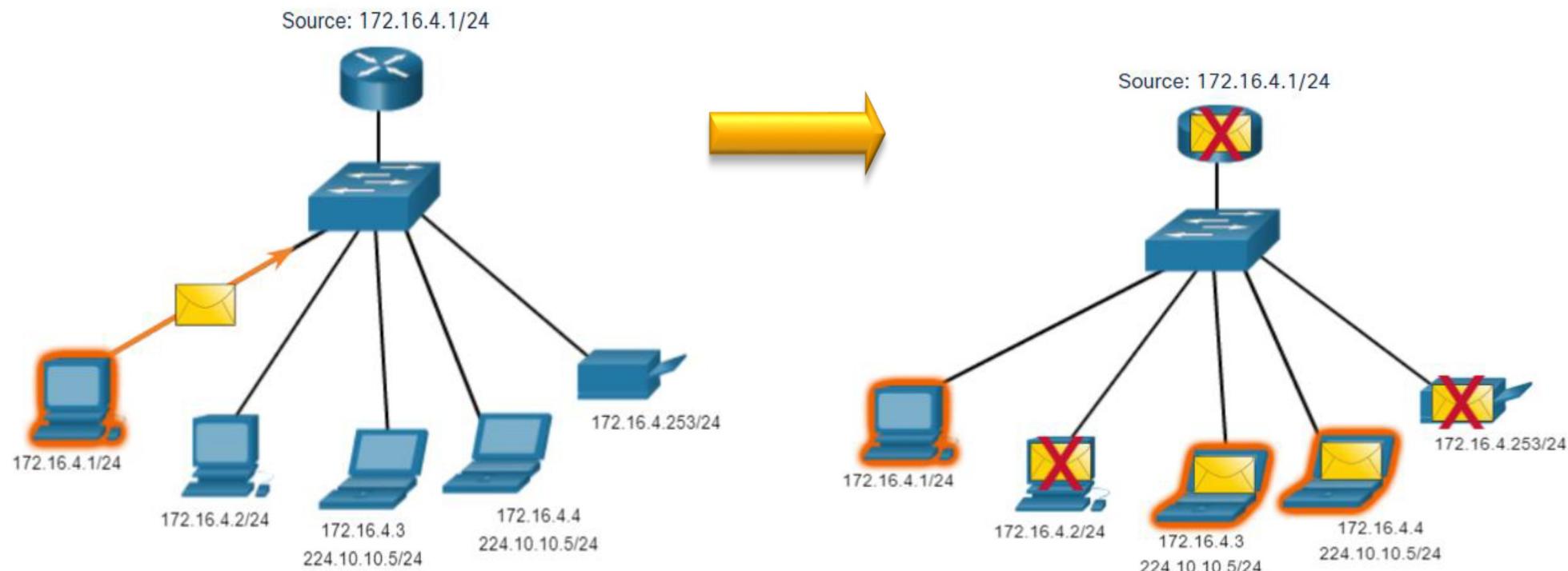


Adresses IPv4 de monodiffusion, de diffusion et de multidiffusion

Multidiffusion

La transmission de multidiffusion envoie un paquet à un groupe d'adresses de multidiffusion.

- Par exemple, le PC à 172.16.4.1 envoie un paquet de multidiffusion à l'adresse du groupe de multidiffusion 224.10.10.5.



Types d'adresses IPv4

Les adresses IPv4 publiques et privées

les adresses IPv4 publiques sont acheminées globalement entre les routeurs des FAI (fournisseurs d'accès à Internet).

- Certains blocs d'adresses appelés adresses privées sont utilisés par la plupart des **entreprises** pour attribuer des adresses IPv4 aux hôtes internes.
- Les adresses IPv4 privées ne sont pas uniques et peuvent être utilisées par n'importe quel réseau interne

Cependant, les adresses ne sont pas routables globalement.

Adresse réseau et préfixe	Gamme d'adresses privée RFC 1918
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Types d'adresses IPv4

Les adresses IPv4 des utilisateurs spéciaux

Adresses de bouclage

127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)

Généralement identifié comme 127.0.0.1

Utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

L'adresse de bouclage est une adresse IP **spéciale** utilisée par un **ordinateur pour s'adresser à lui-même**.

Elle permet à un **ordinateur de tester sa propre pile réseau** (TCP/IP) sans avoir besoin de se connecter à un autre appareil.

Les types d'adresses IPv4

Ancien système d'adressage par classe

les adresses IPv4 étaient attribuées à l'aide de l' adressage par classe tel que défini dans la RFC 790 (1981).

Classe A (0.0.0.0/8 à 127.255.255.255/8)

Classe B (128.0.0.0 /16 — 191.255.255.255/16)

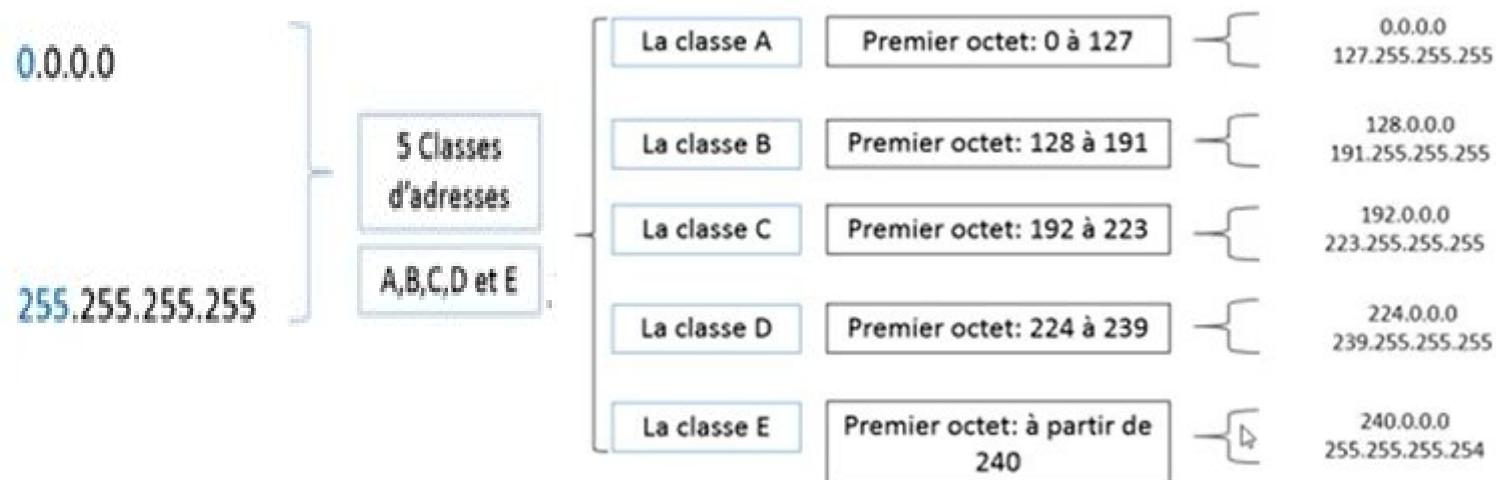
Classe C (192.0.0.0 /24 — 223.255.255.255/24)

Classe D (224.0.0.0 à 239.255.255.255)

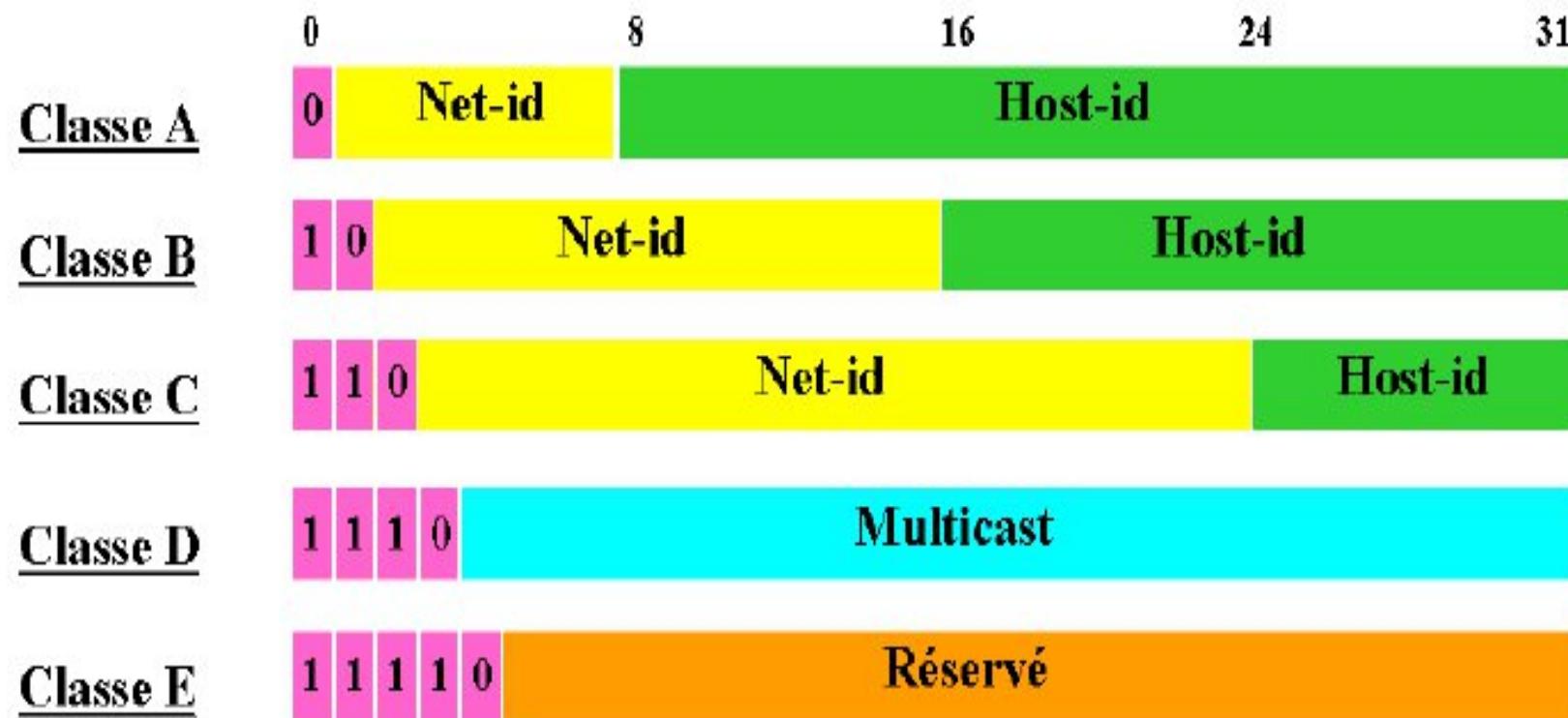
Classe E (240.0.0.0 — 255.255.255.255)

L'adressage de classe a gaspillé de nombreuses adresses IPv4.

L'allocation d'adresse par classe a été remplacée par l'adressage sans classe qui ignore les règles des classes (A, B, C).



Les adresses IP sont organisées en 5 classes



Masque de sous réseau

Les masques de sous réseau sont par défaut :

- En classe A : 255.0.0.0
- En classe B : 255.255.0.0
- En classe C : 255.255.255.0

Segmentation du réseau



Découpage en sous-réseaux

1. Utilité

Un Hôpital est composé de plusieurs services, tous connectés au réseau local de l'entreprise.

- un service d'imagerie (données volumineuses)
- un service administratif (faible volume mais disponibilité indispensable)

Un seul réseau

(-) Surcharge du réseaux

(-) un seul réseau vont prendre toute la bande passante

Une solution serait de partager le réseau en deux.

Le découpage en sous-réseau consiste à diviser une classe de réseau en petits réseaux. Mais alors comment distingue les machines = masque de réseaux

La partie de l'adresse Internet administrée localement (Host_id) peut être découpée

en deux parties :

une adresse de sous réseau

Comment structurer le réseau

La solution :

Diviser le Hôte ID en deux parties



Exercice1

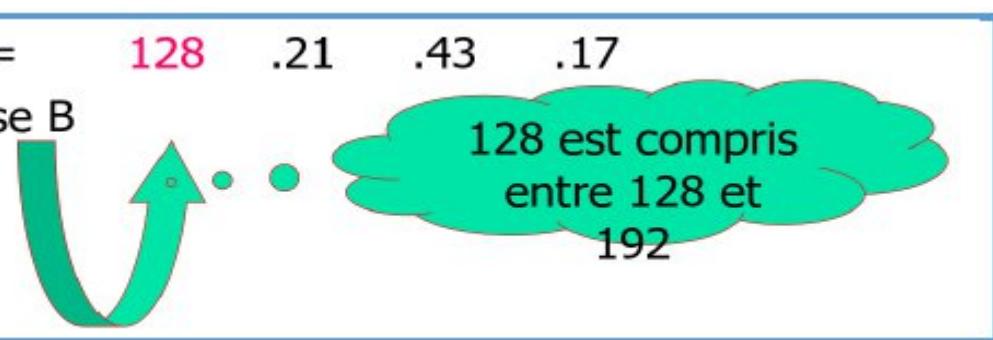
@IP = 128 .21 .43 .17

Masque = 255 .255 .255 .0

Quels sont les valeurs de :

- Numéro de sous-réseau
- Numéro d'hôte
- Adresse du sous-réseau
- Adresse de diffusion

Explication

L'adresse IP est une classe B	<p>■ @IP = 128 .21 .43 .17</p> <p>➤ Classe B</p> 
-------------------------------	--

Classe B : Donc l'@IP se trouve dans le réseau 128.21.0.0

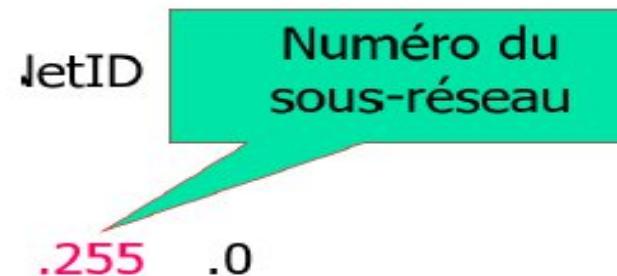
Le masque est normalement : 255.255.0.0

Or il est 255.255.255.0

L'octet en rouge est donc utilisé pour les sous-réseaux

➤ Classe B -> 16 bits de NetID

Masque = 255 .255 .255 .0



Donc l'adresse IP se trouve dans le réseau 128.21.0.0 et dans le sous-réseau 128.21.43.0

➤ L'@ du sous-réseau = **128.21.43.0**

- 128.21.43.**17**
- Masque = 255.255.255.**0**

Et le numéro de l'hôte est

➤ Numéro d'hôte = **0.0.0.17**

- Masque = 255.255.255.**0**
- 128.21.43.**17**

Conclusion

➤ Adresse du sous-réseau

- Que des 0 dans le champ de numéro de hôte

➤ Numéro d'hôte

- Masque = 255.255.255.**0**
- 128.21.43. **00**

➤ Adresse de diffusion

- Que des 1 dans le champ de numéro de hôte

➤ Numéro d'hôte

- Masque = 255.255.255.**0**
- 128.21.43. **255**

Exercice2 :

@ IP : 172.128.10.5

Masque : 255.255.192.0

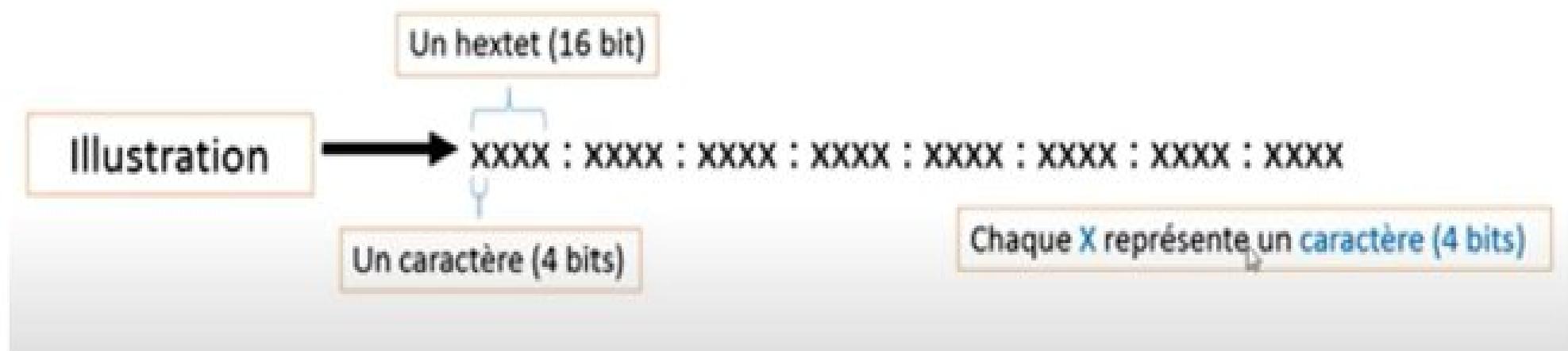
- 1. Déterminer l'adresses de réseau**
- 2. Déterminer nombre d'adresses utilisables**
- 3. Déterminer la plage adressable du réseau**

Adressage IPv6



1) Format

- L'adresse IPv6 est une adresse qui utilise le format hexadécimal
- C'est une adresse de 128 bits (16 octets ou 8 hextets)
- Chaque hextet peut aller de 0000 à FFFF



0000 (en binaire)

Adresse IPv6 minimale: 0000:0000:0000:0000:0000:0000:0000:0000

Adresse IPv6 maximale: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

1111 (en binaire)

```
graph TD; A[0000 (en binaire)] --> B[0000:0000:0000:0000:0000:0000:0000:0000]; C[1111 (en binaire)] --> D[FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF]
```

2) Les classes

Pas de classes d'adresses en IPv6

3) Type en fonction des options de remises

- **Adresses de monodiffusion** (monodiffusion globale, link-local, locale unique, non spécifiée, adresse de bouclage, Adresse IPv4 intégrée)
- **Adresses de multidiffusion**
 - * **Multidiffusion attribuée**
 - Groupe de multidiffusion à tous les nœuds (ff02::1)
 - Groupe de multidiffusion à tous les routeurs (ff02::2)
 - * **Multidiffusion de nœud sollicité (diffusion en IPv4)**
- **Adresses Anycast** (adresses attribuables à plusieurs périphériques)

Anycast est une méthode d'acheminement (routing) où plusieurs machines partagent la même adresse IP, mais le trafic est envoyé à celle la plus proche (selon le routage).



ETUDE COMPARATIVE ENTRE IPv4 et IPv6

Critères	IPv4	IPv6
Ancienneté	Ancienne version	Nouvelle version
Nombre de bits	32	128
Format utilisé	décimal	Hexadécimal
parties	<ul style="list-style-type: none"> • Partie réseau • Partie hôte 	<ul style="list-style-type: none"> • Préfixe • ID D'interface
Types	<ul style="list-style-type: none"> • Monodiffusion • Multidiffusion • Diffusion 	<ul style="list-style-type: none"> • Monodiffusion • Multidiffusion • anycast
Traitement de l'information	Moins rapide	Plus rapide
Nombre d'adresses possibles	$2^{\text{puissance } 32}$	$2^{\text{puissance } 128}$

non



Supposons que l'administrateur réseau veut subdiviser son réseau LAN dont l'adresse IP est 192.168.77.0 en plusieurs sous réseaux avec au moins 5 hôtes par sous réseau.

- a. Combien de bits devez-vous emprunter (de la partie hôte)?
- b. Quel est le nombre de sous-réseaux total dont vous disposez?
- c. Combien d'hôtes par sous-réseau avez-vous?
- d. Quel est le masque de sous-réseau obtenu?



VLSM (variable length subnet mask)



VLSM (variable length subnet mask)

La création de base de sous-réseaux est suffisante pour les petits réseaux mais n'offre pas la souplesse requise pour les grands réseaux d'entreprise.

Les masques de sous-réseau de longueur variable (VLSM) permettent une utilisation efficace de l'espace d'adressage.

Le principe de VLSM consiste à créer des sous-réseaux d'un sous-réseau. Cette technique a initialement été développée pour optimiser l'efficacité de l'adressage.

Avec l'arrivée de l'adressage privé, le principal avantage de la technique VLSM s'avère désormais être sa capacité d'organisation et de résumé (Lié à la table de routage qui est petite ou réduite).

Avantage de la technique de VLSM

- Utilisation efficace de l'espace d'adressage ;
- Utilisation de plusieurs longueurs de masque de sous-réseau ;
- Division d'un bloc d'adresses en blocs plus petits ;
- Prise en charge des résumés du routage ;
- Plus grande souplesse de conception de réseau ;
- Prise en charge des réseaux d'entreprise hiérarchiques.



EXERCICE

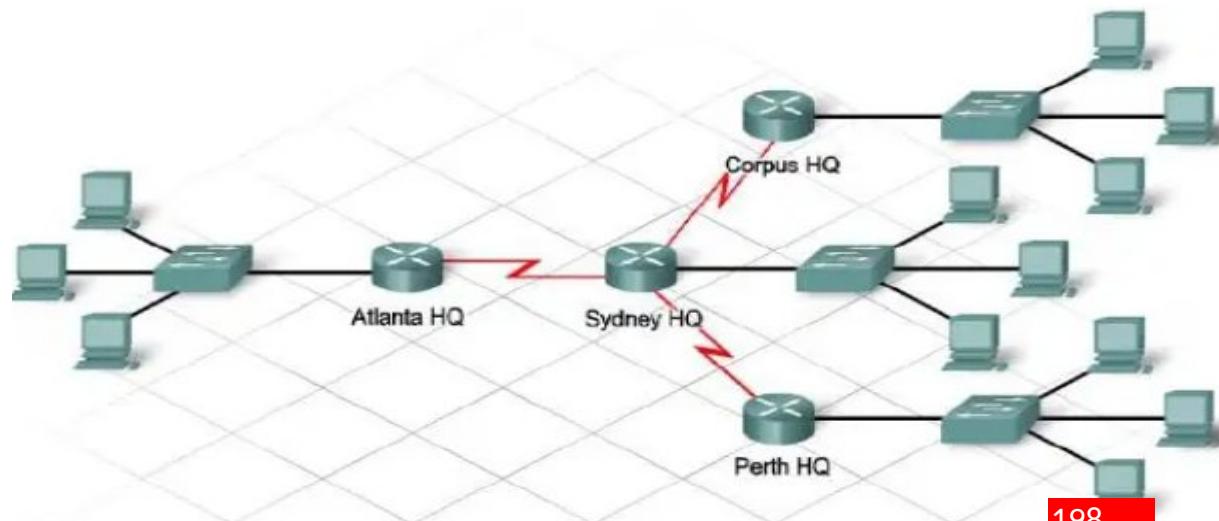
Soit le scénario suivant :

La conception d'un système d'adressage IP à l'aide de la technique VLSM nécessite entraînement et planification.

En guise d'exercice, prenons l'exemple d'un réseau qui possède les caractéristiques suivantes :

- 192.168.15.0/24
- Atlanta HQ = 58 adresses d'hôtes
- Perth HQ = 26 adresses d'hôtes
- Sydney HQ = 10 adresses d'hôtes
- Corpus HQ = 10 adresses d'hôtes
- Liaisons WAN = 2 adresses d'hôtes (chacune).

Définir le plan d'adressage pour 6 LAN en utilisant la plage d'adresse 192.168.5.0/24



Routage



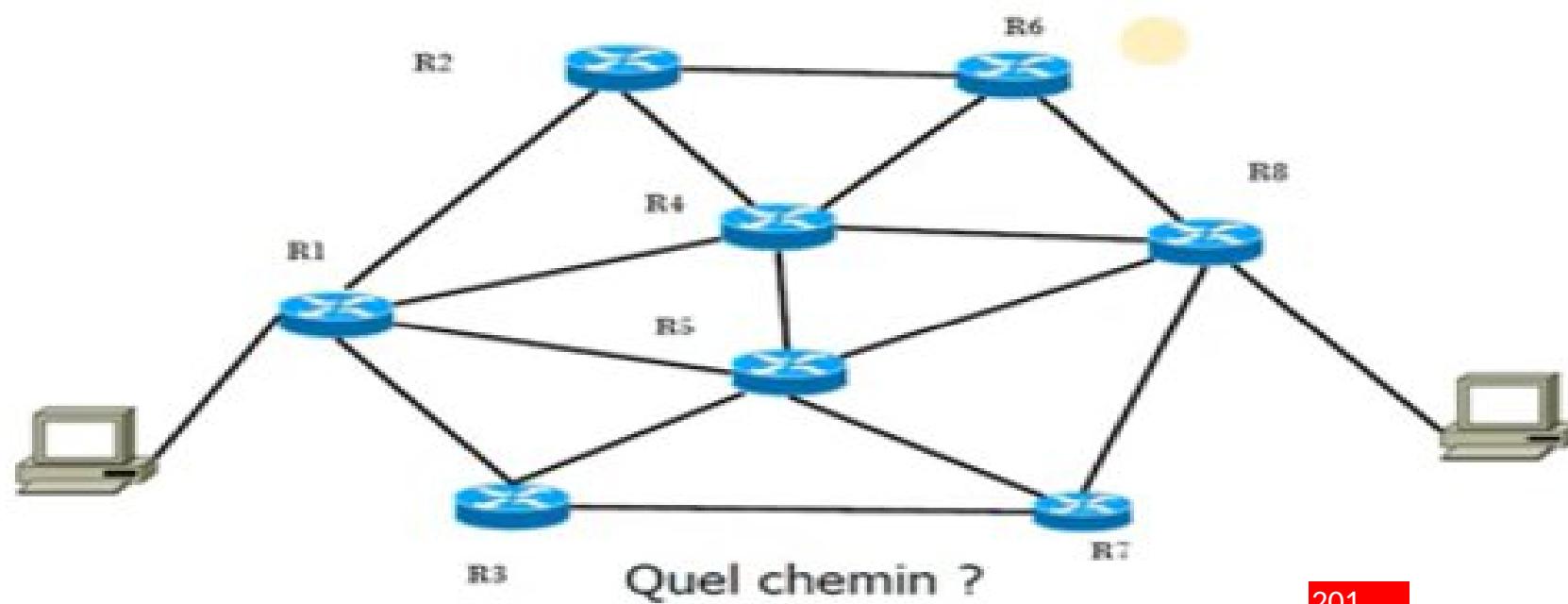
Le routage

Le routage (routage des paquets) est le processus permettant à un paquet d'être acheminé vers le destinataire lorsque celui-ci le même réseau physique que l'émetteur.

La sélection du chemin est le processus que le routeur utilise pour choisir le prochain saut (prochain routeur) du trajet que le paquet empruntera vers sa destination.

Le routage

- Les routeurs coopèrent entre eux de telle manière qu'un datagramme passe d'un routeur à un autre jusqu'à ce que l'une d'entre elles le délivre à son destinataire.
- Le routeur ne connaît pas le chemin complet pour atteindre la destination.
- Un routeur a juste une version local du réseau global.



Principe de routage

- Chaque paquet est «routé » indépendamment des autres.
- La décision du routage doit être prise pour chaque paquet.
- Des paquets successifs peuvent donc suivre des routes différentes et il peut y avoir alors déséquencement des paquets.



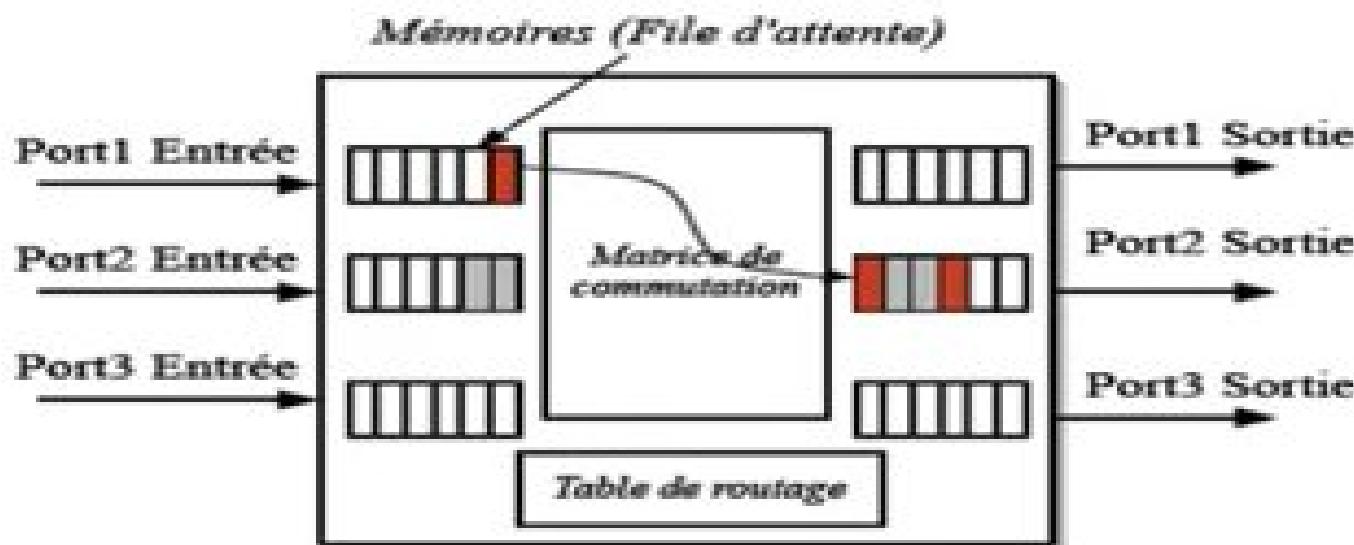
La table de routage

- Pour assurer la fonction de routage (trouver un chemin) le **routeur consulte une table** dite **table de Routage**
- Les tables de routage contiennent les informations nécessaires à la transmission des paquets sur les autres réseaux.
- Les routeurs emploient des protocoles de routage pour : Construire et gérer les tables de routage continent les informations d'acheminement.



Structure et fonctionnement d'un routeur

- Un routeur possède plusieurs interfaces d'entrée et de sortie
- Chaque interface dispose d'une mémoire
- La **table de routage** permet de choisir l'interface de sortie.



Structure de la table de routage

Une table de routage contient les informations suivantes:

- Adresse réseau destination ainsi que le masque associé à ce réseau
- Adresse IP de la passerelle : correspondant à l'adresse du prochain routeur qui va recevoir le paquet destiné au réseau de destination.

Interface de sortie: puisque le routeur possède plusieurs interfaces , donc il faut indiquer via quelle interface doit transiter le paquet.

* Généralement la table de routage IP, contient seulement les adresses réseaux et non pas les adresses machines afin de ne pas avoir une table de très grande taille

Exemple1 : un routeur et deux réseaux



Pour atteindre le réseau de destination	Prochain nœud Passerelle	Via l'interface
192.168.1.0/255.255.255.0	Direct	P1
192.168.2.0/255.255.255.0	Direct	P2

Indique que pour atteindre le réseau (192.168.1.0) passer directement via l'interface P1.

Indique que pour atteindre le réseau(192.168.2.0) passe directement via l'interface P2.

Exemple2 : deux routeurs et trois réseaux (utilisation de sous réseaux)

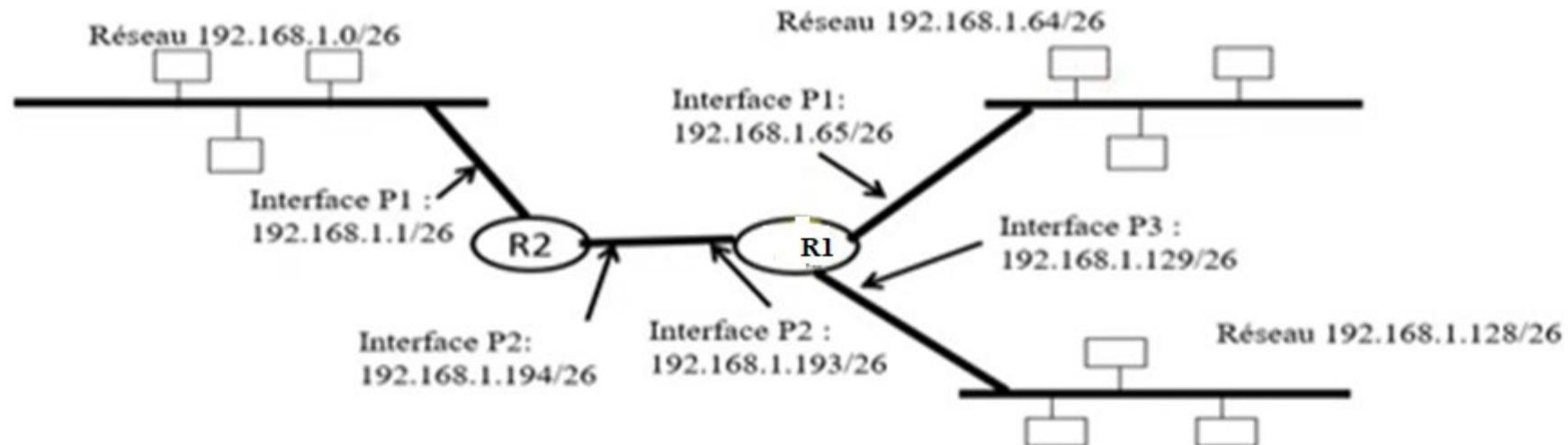


Table de routage de routeur R1

Pour atteindre le réseau de destination	Prochain nœud Passerelle	Via l'interface
192.168.1.64/26	Direct	P1
192.168.1.128/26	Direct	P3
192.168.1.192/26	Direct	P2
192.168.1.0/26	192.168.1.194	P2

Table de routage de routeur R 2

Pour atteindre le réseau de destination	Prochain nœud Passerelle	Via l'interface
192.168.1.0/26	Direct	P1
192.168.1.192/26	Direct	P2
192.168.1.64/26	192.168.1.193	P2
192.168.1.128/26	192.168.1.193	P2

Route par défaut passerelle par défaut

La route par défaut est utilisée:

- **Lorsque le chemin de destination n'est pas explicitement précisé dans la table de routage (une destination inconnue) : s'il n'y a pas une route vers le réseau de destination alors par défaut l'envoyer vers cette passerelle.**
- **Grouper la même route pour un ensemble de réseaux pour ne pas encombrer la table de routage.**



Route par défaut : exemple

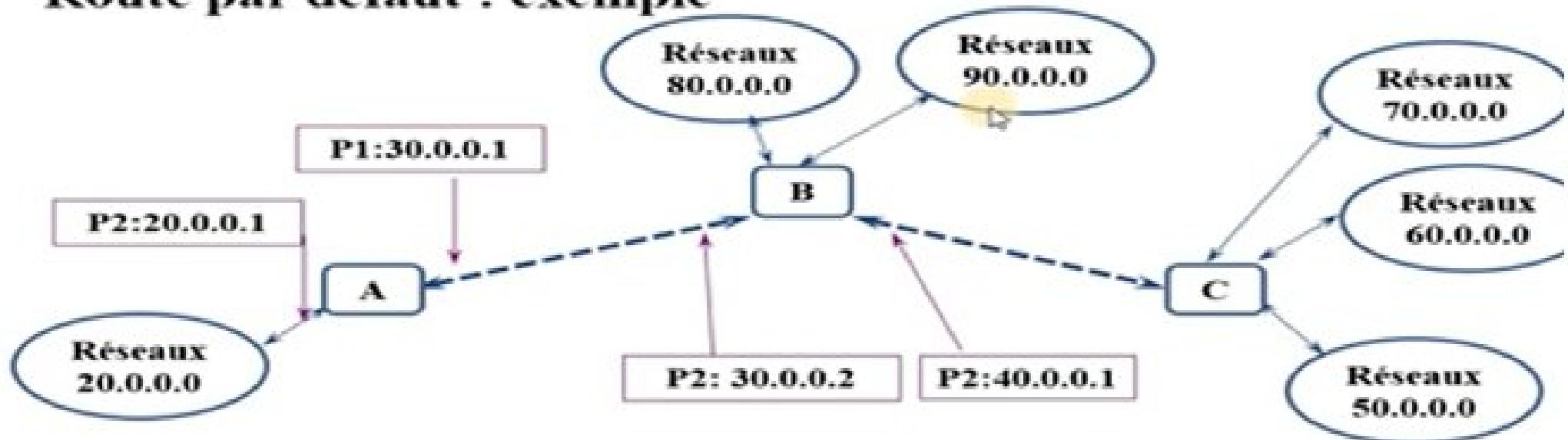


Table de routage de routeur A

Pour atteindre le réseau de destination	Prochain noeud Passerelle	Via l'interface
20.0.0.0/8	Direct	P2
30.0.0.0/8	Direct	P1
50.0.0.0/8	30.0.0.2	P1
60.0.0.0/8	30.0.0.2	P1
70.0.0.0/8	30.0.0.2	P1
80.0.0.0/8	30.0.0.2	P1
90.0.0.0/8	30.0.0.2	P1



Table de routage de routeur A

On remarque que si la même route qui est utilisée pour atteindre le réseau: 50.0.0.0 , 60.0.0.0, 70.0.0.0 , 80.0.0.0 et 90.0.0.0

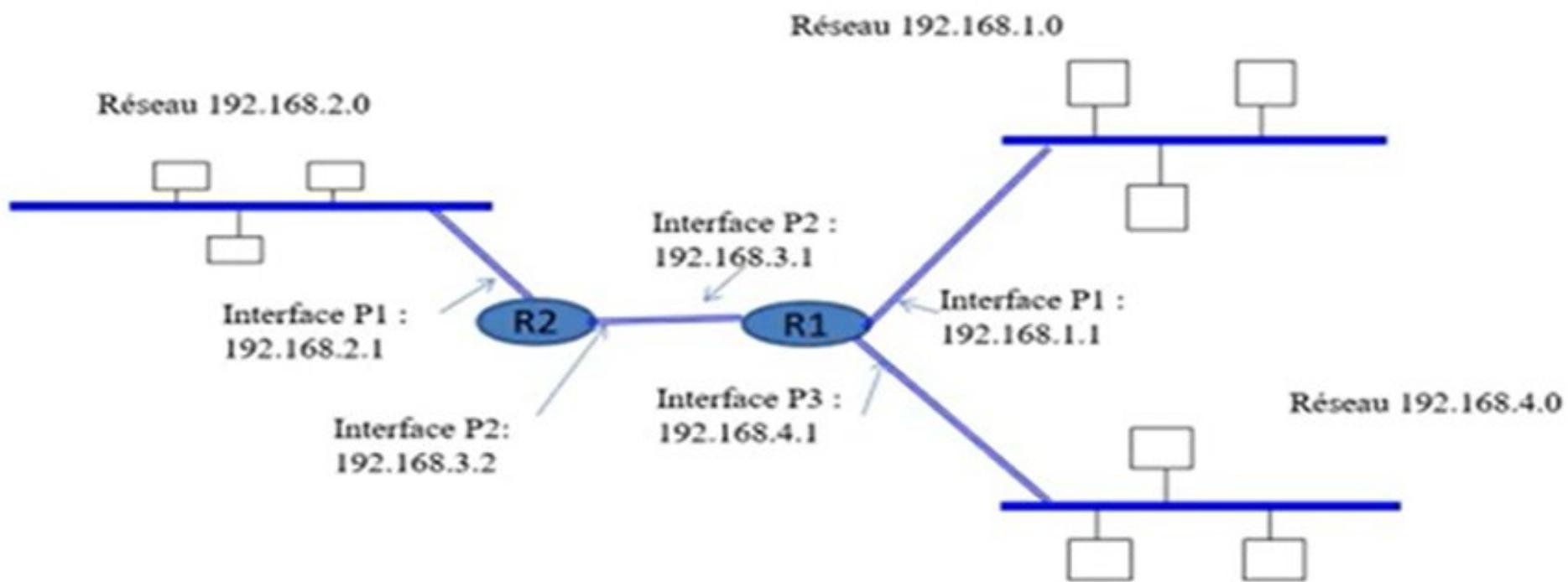
□ Utiliser une route par défaut via 30.0.0.2 (le routeur B)

Pour atteindre le réseau de destination	Prochain nœud Passerelle	Via l'interface
20.0.0.0/8	Direct (le même réseau)	P2
30.0.0.0/8	Direct (le même réseau)	P1
0.0.0.0/0.0.0.0 (tout les autres réseaux) Route par défaut	30.0.0.2	P1

Exemple table de routage d'une machine

On prend la machine M1 (@IP: 192.168.2.5) , sa table de routage

Pour atteindre le réseau de destination	Prochain nœud Passerelle	Via l'interface
192.168.2.0/24	Direct (le même réseaux)	P1
0.0.0.0/0.0.0.0	192.168.2.1	P1



Type de routage

Comment construire la table de routage ?

- + **routage statique** : les informations de routage (tables de routage) sont mises à jour **manuellement** à chaque modification topologique du réseau.
- + **Routage dynamique**: les informations table de routage relatives à la route sont mises à jour **automatiquement** entre les routeurs selon un protocole (RIP, OSPF,)

Routage statique

- + la table de routage est **mise à jour manuellement**.
- + Si la topologie change :
 - Ajout d'un réseau : ajouter la ou les règles de routage pour accéder à ce réseau sur l'ensemble des routeurs concernés
 - Pour atteindre le réseau X contacter l'adresse Z via l'interface I
 - Pour atteindre le réseau 20.0.0.0 255.0.0.0 contacter 40.0.0.1 via l'interface fa0/0
 - suppression d'un réseau : supprimer la ou les règles de routage pour accéder à ce réseau sur l'ensemble des routeurs concernés



Fonctionnement d'un routeur

Routes connectées directement, Routes apprises de manière statique:

Quand utiliser les routes statiques ?

Les routes statiques doivent être utilisées dans les cas suivants :

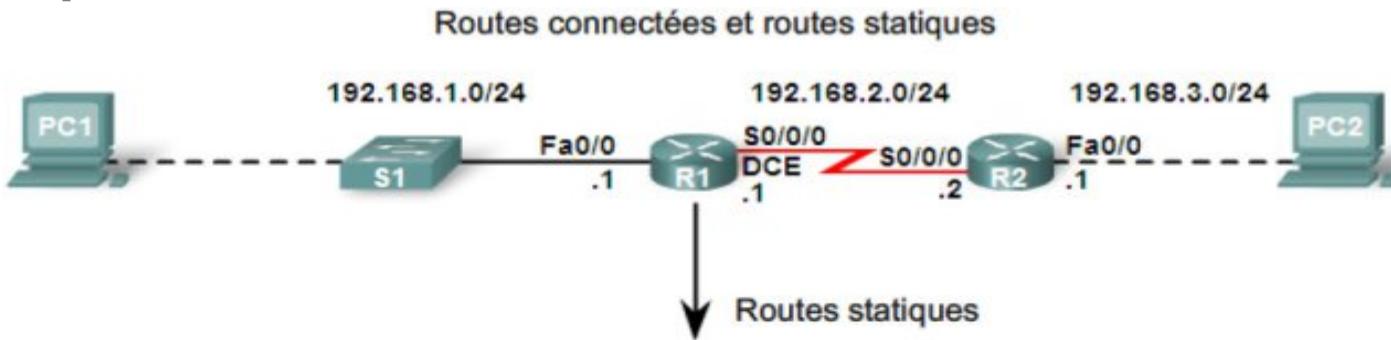
- Un réseau ne comporte que quelques routeurs. Dans ce cas, l'utilisation d'un protocole de routage dynamique ne présente aucun bénéfice substantiel. Au contraire, le routage dynamique risque d'accroître la charge administrative.

-



Fonctionnement d'un routeur

Routes connectées directement, Routes apprises de manière statique



```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
      i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
      * - candidate default, U - per-user static route, o - ODR
      P - periodic downloaded static route

Gateway of last resort is not set
```

```
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

Routes connectées directement, Routes apprises de manière statique

Routage statique:

Remarque importante : Si une route est défectueuse, le routeur continue à vouloir l'utiliser. C'est une des limites du routage statique.

AVANTAGES & INCONVÉNIENTS:

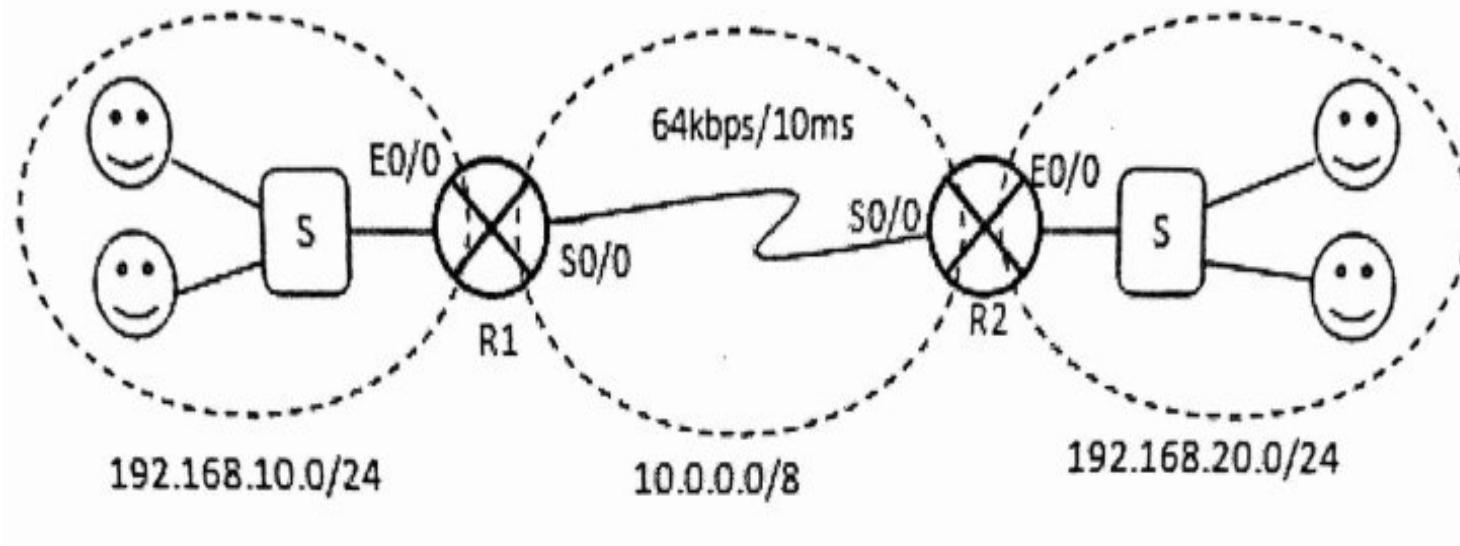
- Fournit des services de transfert sans les charges associées à la plupart des protocoles de routage dynamique.
 - Offre une sécurité plus renforcée que le routage dynamique, car aucune mise à jour de routage n'est requise.
 pirate informatique pourrait intercepter une mise à jour de routage dynamique pour obtenir des informations sur un réseau.
 - Nécessite du temps et de la précision
- **L'administrateur réseau doit entrer manuellement les informations de routage.**



Routes connectées directement, Routes apprises de manière statique

Routage statique: (configuration)

Soit l'exemple suivant:



Routes connectées directement, Routes apprises de manière statique

Routage statique: (configuration)

Utiliser la syntaxe suivante:

ip route @rd @mask @nh

@rd : adresse réseau destination

@mask : masque du réseau destination

@nh: adresse du routeur voisin

Exemple:

```
R2(config)# ip route 192.168.20.0 255.255.255.0 1 0.0.0.2
```

Fonctionnement d'un routeur

Routes connectées directement, Routes apprises de manière statique

Router#conf t

Router(config)#ip routing

Router(config)#exit

Router#

Vérifier la table de routage.

Router1# show ip route

La lettre C devant une route indique un réseau directement connecté.

La lettre S indique une route statique.

Le symbole * indique la route par défaut (si elle est déclarée)

Les bases du routage statique et dynamique ont été abordées dans le TP n°4 réalisé sur Cisco Packet Tracer. Ce TP a permis de comprendre et d'appliquer la configuration des routes statiques, ainsi que la mise en place de protocoles de routage dynamique tels que RIP , en vue d'assurer l'échange automatique des informations de routage entre les routeurs



Merci
Pour
Votre
Attention
!

