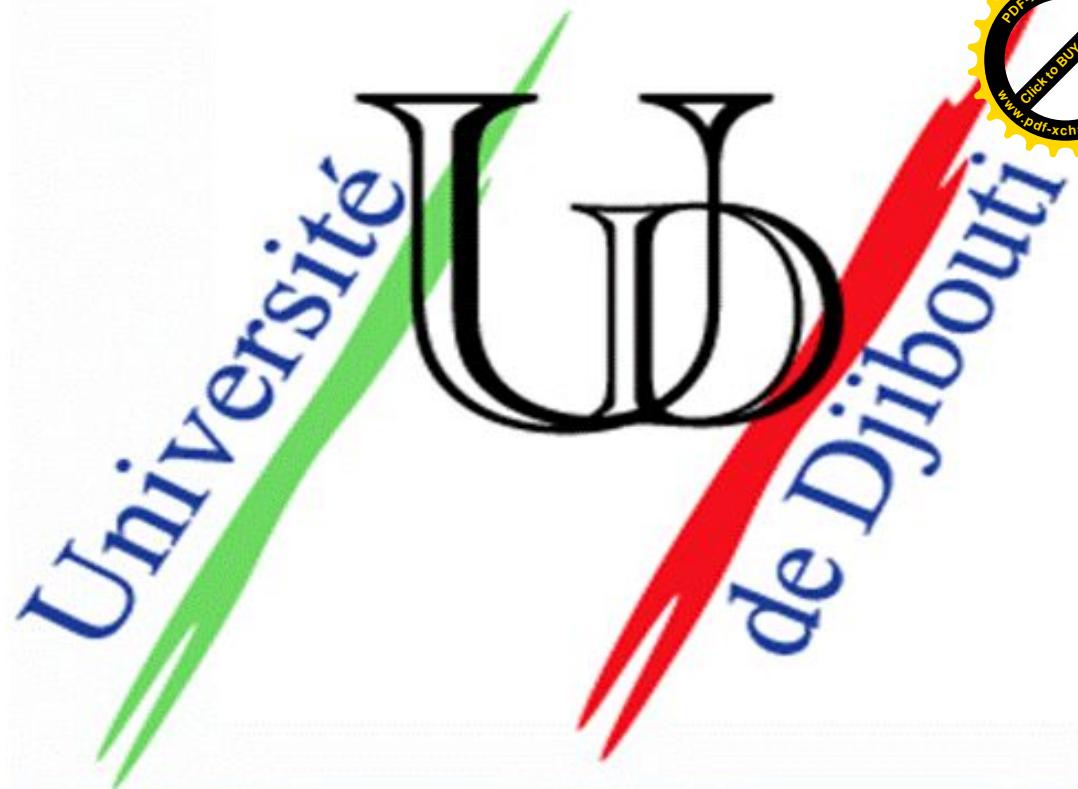




Chapitre 1:

Exploration du réseau

ISMAEL DOUKSIEH



Explorer les fonctions d'un réseau

Objectifs:

- Décrire les différents réseaux utilisés et leurs impacts dans la vie quotidienne
- Décrire les modèles de partage de ressources dans un réseau
- Expliquer les topologies et les composants utilisés dans un réseau
- Expliquer les caractéristiques de base d'un réseau prenant en charge la communication dans une PME
- Expliquer les tendances liées au réseau qui affecteront l'utilisation des réseaux dans les PME

Chapitre 1:

Exploration du réseau

ISMAEL DOUKSIEH

Un réseau

Un réseau désigne un ensemble d'équipements informatiques interconnectés pour permettre la communication de données entre applications, quelles que soient les distances qui les séparent. Un réseau s'appuie sur deux notions fondamentales :

- **L'interconnexion** qui assure la transmission des données d'un noeud à un autre.
- **La communication** qui permet l'échange des données entre processus.
- **Partager des fichiers** (images, audios, vidéos, ...)
- **Partager des ressources** (Imprimantes, Speakers,

On appelle noeud (node) l'extrémité d'une connexion. Un processus est un programme en cours d'exécution et représente le bout d'une communication dans un réseau informatique.

Interconnexion de nos vies

L'impact des réseaux dans la vie quotidienne

- Les réseaux facilitent l'apprentissage
- Les réseaux facilitent la communication
- Les réseaux facilitent notre travail
- Les réseaux facilitent le divertissement

Types de réseaux

Les réseaux informatiques peuvent être classés suivant leur portée :

- 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.
- 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.
- Autres dénominations connues : **MAN** (Metropolitan Area Network), **PAN** (Personal Area Network), **WPAN** et **WLAN** (Wireless ...), **SAN** (Storage Area Network), ...

Bourniture de ressources dans un réseau

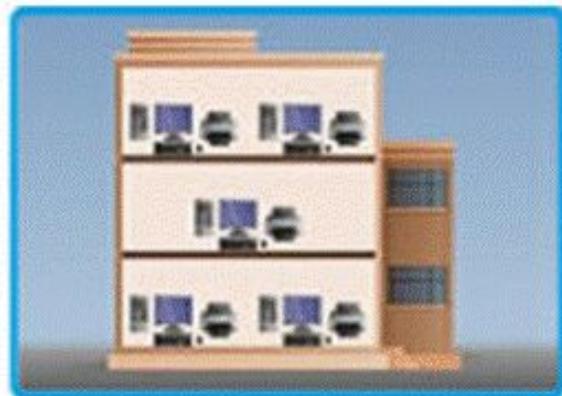
Types de réseaux



Petits réseaux domestiques



Réseaux de petits bureaux/bureaux à domicile



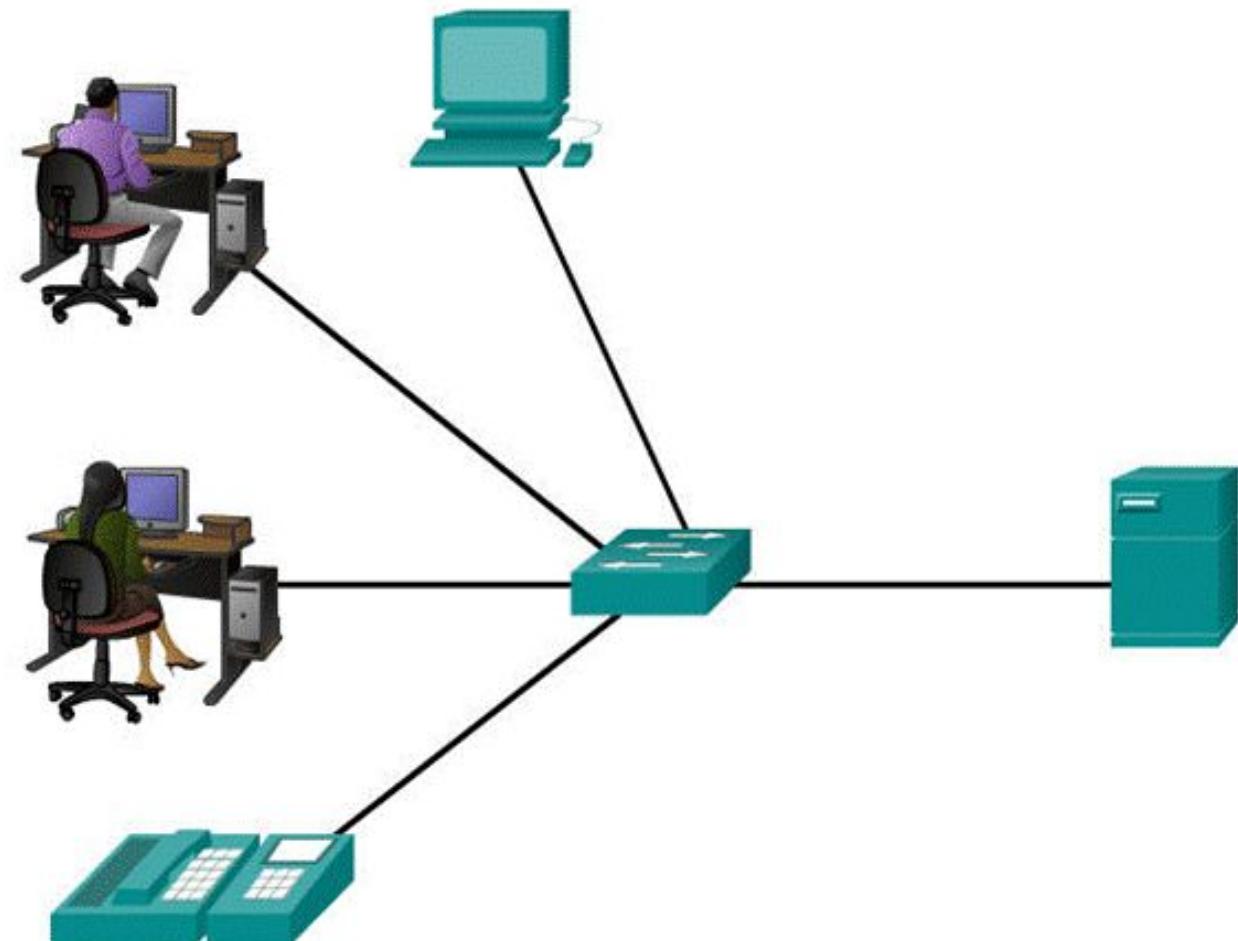
Moyens et grands réseaux



Réseaux mondiaux

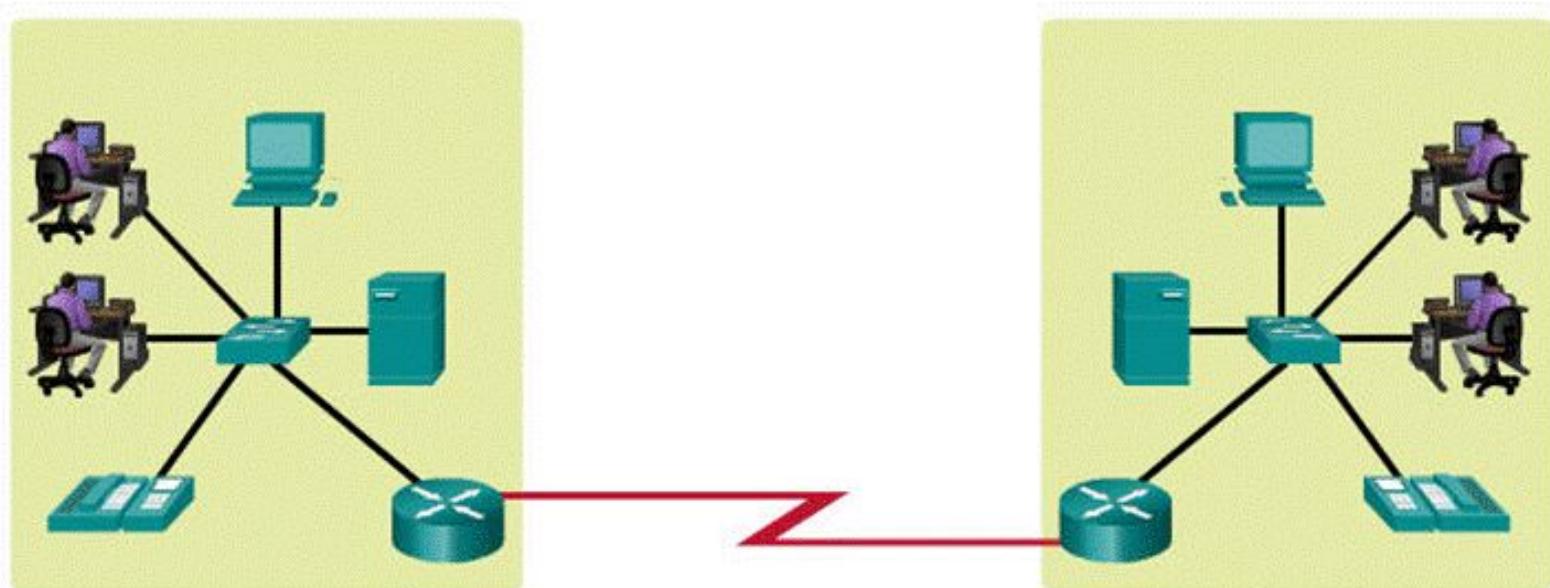
Les réseaux locaux et les réseaux étendus

Réseaux locaux (LAN)



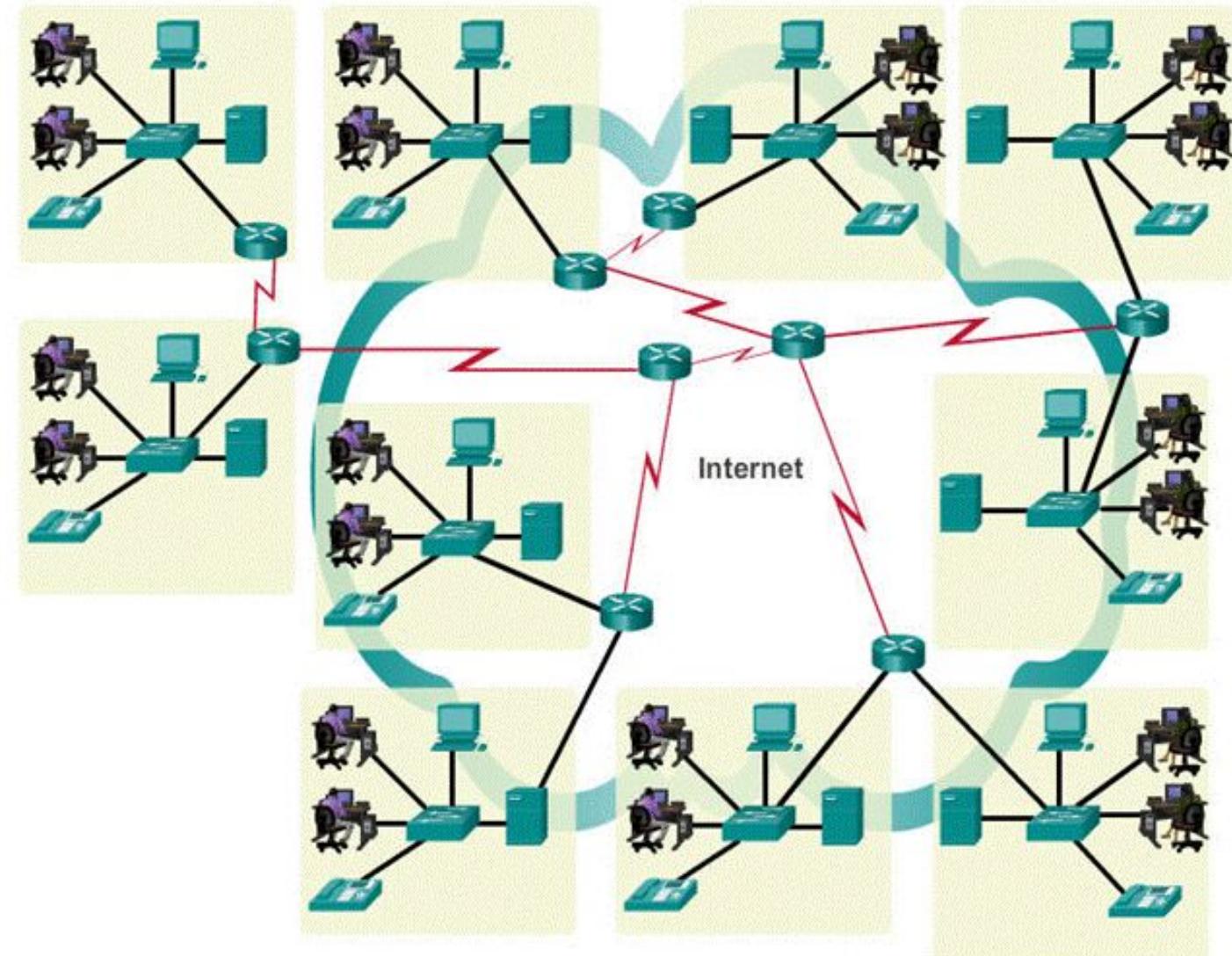
Le réseau d'une maison individuelle, d'un bâtiment ou d'un campus est appelé « réseau local ».

Les réseaux locaux et les réseaux étendus Réseaux étendus (WAN)



Les réseaux locaux séparés géographiquement sont reliés par le biais d'un réseau appelé « réseau étendu ».

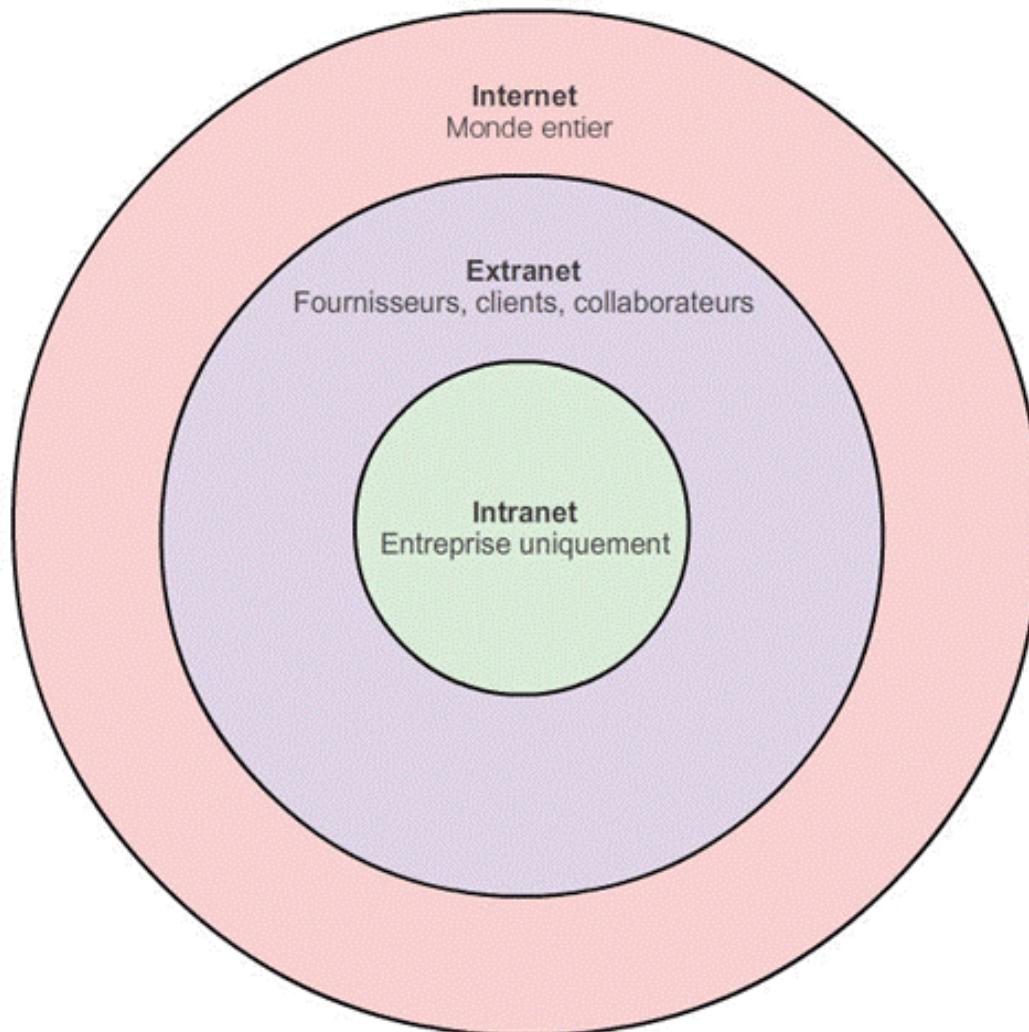
Les réseaux locaux, les réseaux étendus et Internet



Les réseaux locaux et étendus peuvent être connectés au sein d'interréseaux.

Internet

Intranet et Extranet

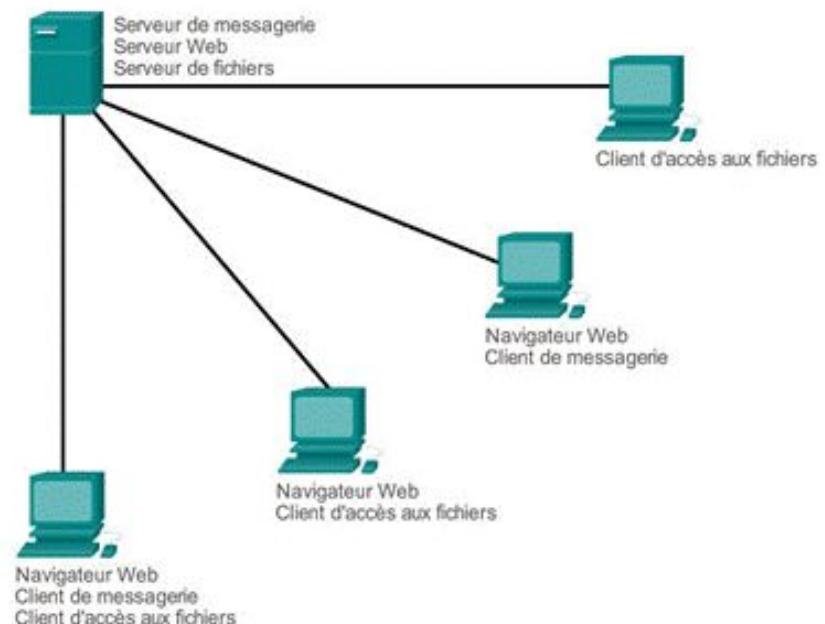
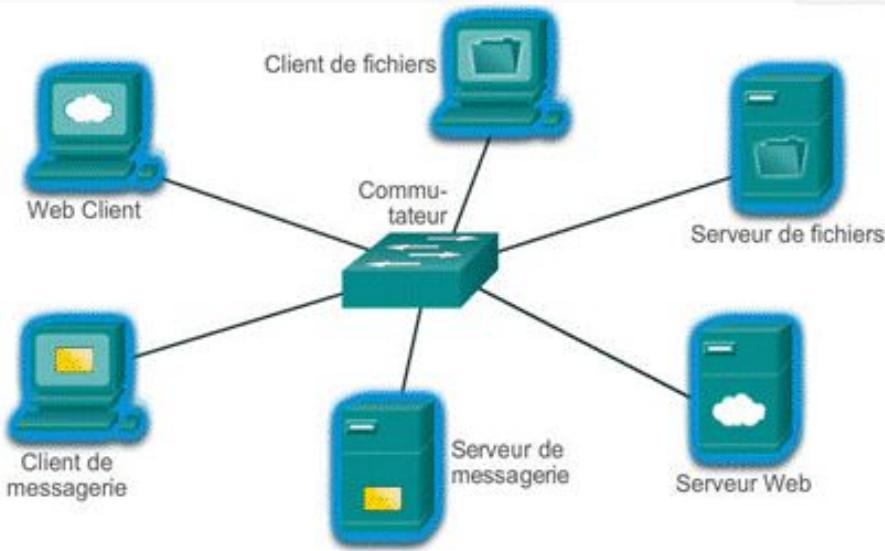


Les réseaux informatiques peuvent être classés en fonction de leurs utilisations et des services qu'ils offrent. Ainsi, pour les réseaux utilisant la famille des protocoles TCP/IP, on distingue :

- **Intranet** : le réseau interne d'une entité organisationnelle
- **Extranet** : le réseau externe d'une entité organisationnelle
- **Internet** : le réseau des réseaux interconnectés à l'échelle de la planète

Deux modèles de Fourniture de ressources dans un réseau

Serveurs/Clients



Deux modèles de Fourniture de ressources dans un réseau Peer-to-Peer (P2P)



Avantages du réseau peer-to-peer :

- Facile à configurer
- Moins complexe
- Coût inférieur étant donné que les périphériques réseau et les serveurs dédiés peuvent ne pas être nécessaires
- Peut être utilisé pour des tâches simples telles que le transfert de fichiers et le partage des imprimantes

Inconvénients du réseau peer-to-peer :

- Pas d'administration centralisée
- Peu sécurisé
- Non évolutif
- Tous les périphériques peuvent servir à la fois de client et de serveur, ce qui peut ralentir les performances



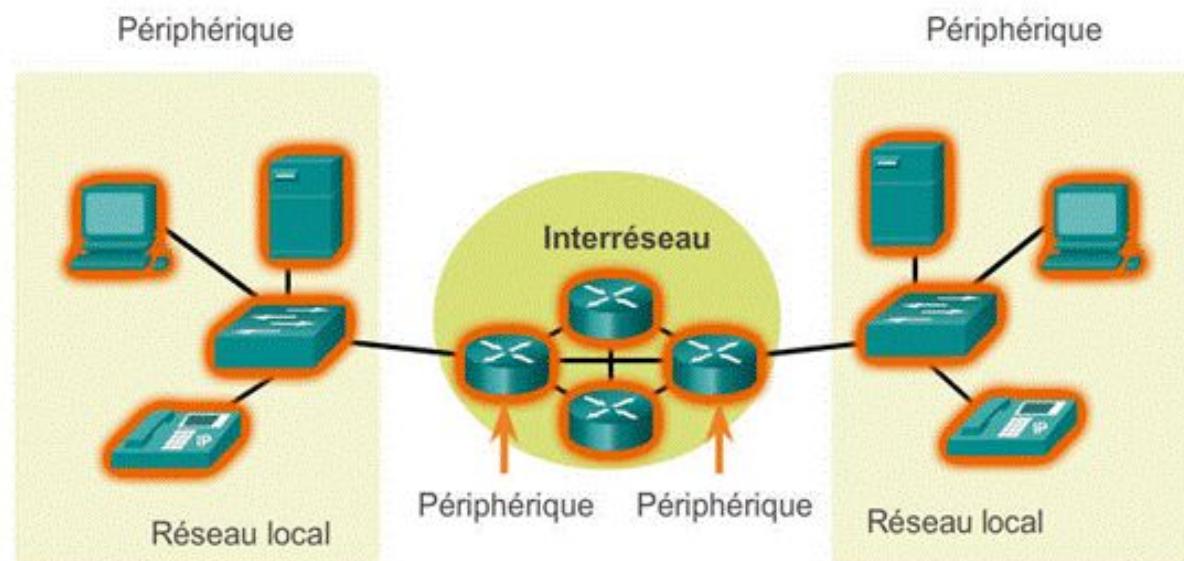
Composants d'un réseau

Les réseaux locaux, les réseaux étendus et Internet

Composants d'un réseau

Les composants d'un réseau se classent en trois catégories :

- Les périphériques
- Les équipements intermédiaires
- Les services (Protocoles, Applications)



Composants d'un réseau

Les périphériques finaux

Voici quelques exemples de périphériques finaux :

- Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs Web)
- Imprimantes réseau
- Téléphones VoIP
- Caméras de surveillance
- Appareils portatifs (smartphones, tablettes, PDA, lecteurs de carte sans fil et lecteurs de codes à barres)

Composants d'un réseau

Équipements Intermédiaires

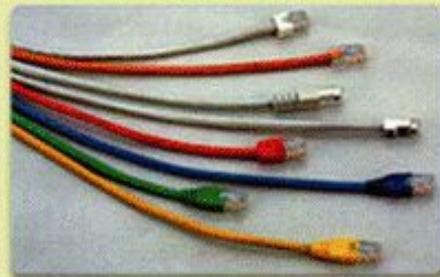
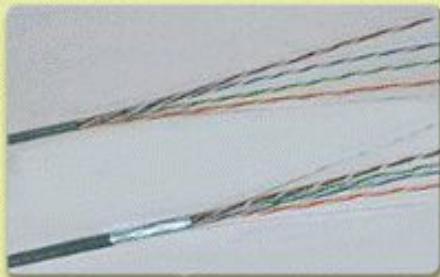
Parmi ces périphériques réseau intermédiaires, citons :

- Les périphériques d'accès réseau (commutateurs et points d'accès sans fil)
- Les périphériques inter-réseau (routeurs)
- Les dispositifs de sécurité (pare-feu)

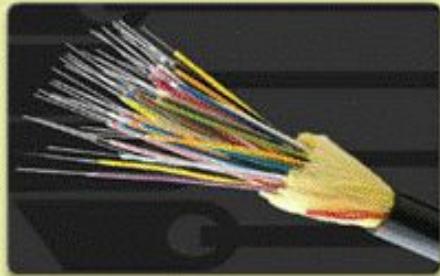
Composants d'un réseau

Supports de transmission

Cuivre



Fibre optique



Sans fil



Composants d'un réseau

Représentations graphiques des réseaux

Périphériques finaux



Ordinateur de bureau



Ordinateur portable



Imprimante



Téléphone IP



Tablette sans fil



Terminal TelePresence

Périphériques intermédiaires



Routeur sans fil



Commutateur LAN



Routeur



Commutateur multicouche

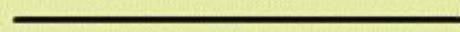


Pare-feu

Supports réseau



Supports sans fil



Supports LAN



Supports WAN

Caractéristiques d'un réseau

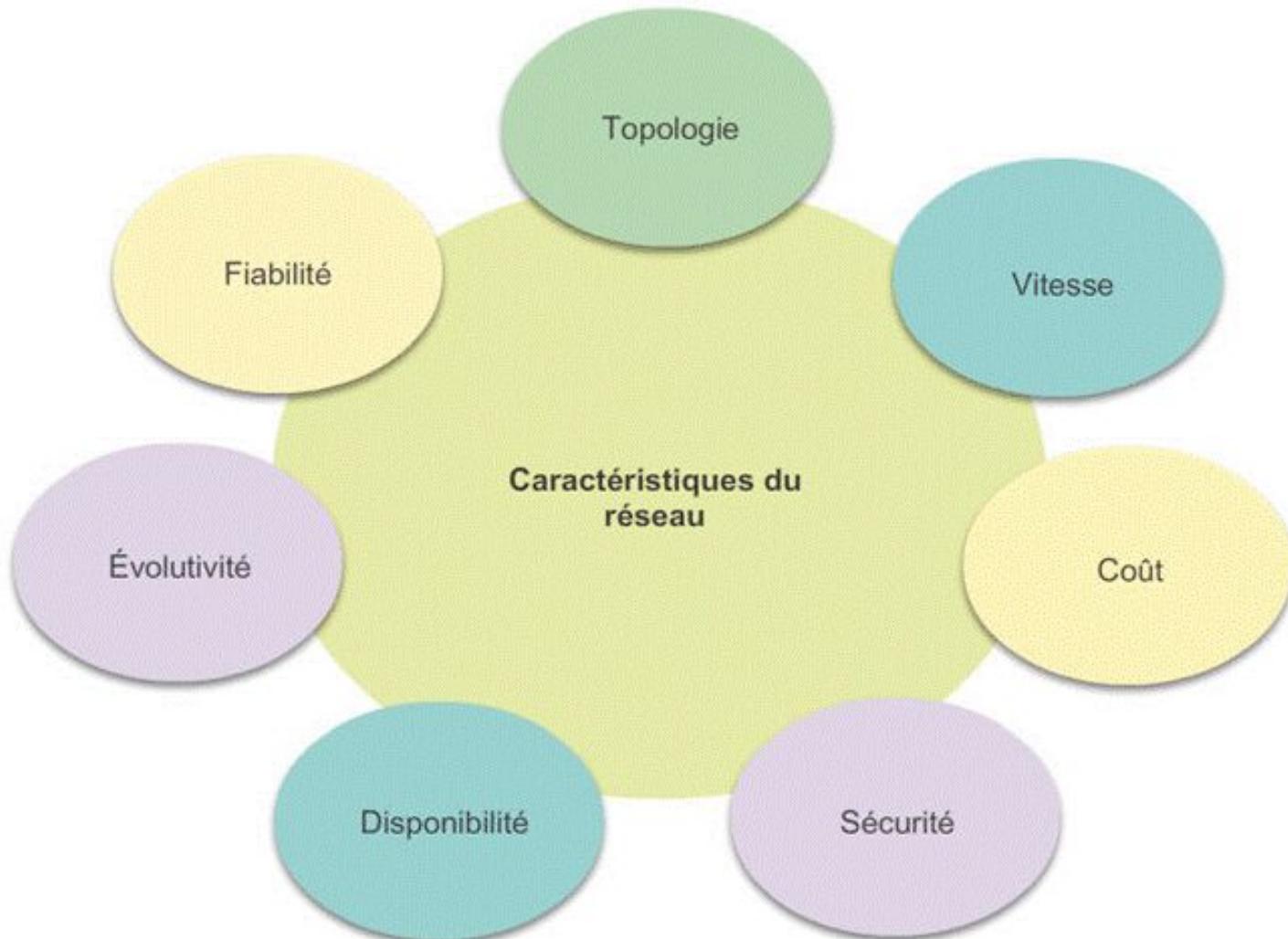
Les caractéristiques de base d'un réseau sont :

- 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 œuvre.
- Le **nombre de nœuds** maximum que l'on peut interconnecter.

Fonctions d'un routeur

Caractéristiques d'un réseau

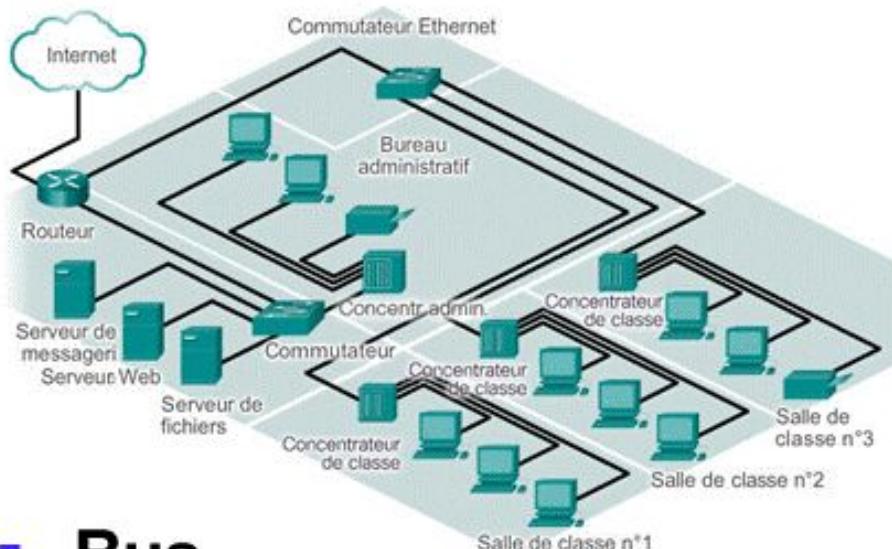
Caractéristiques du réseau



Caractéristiques d'un réseau

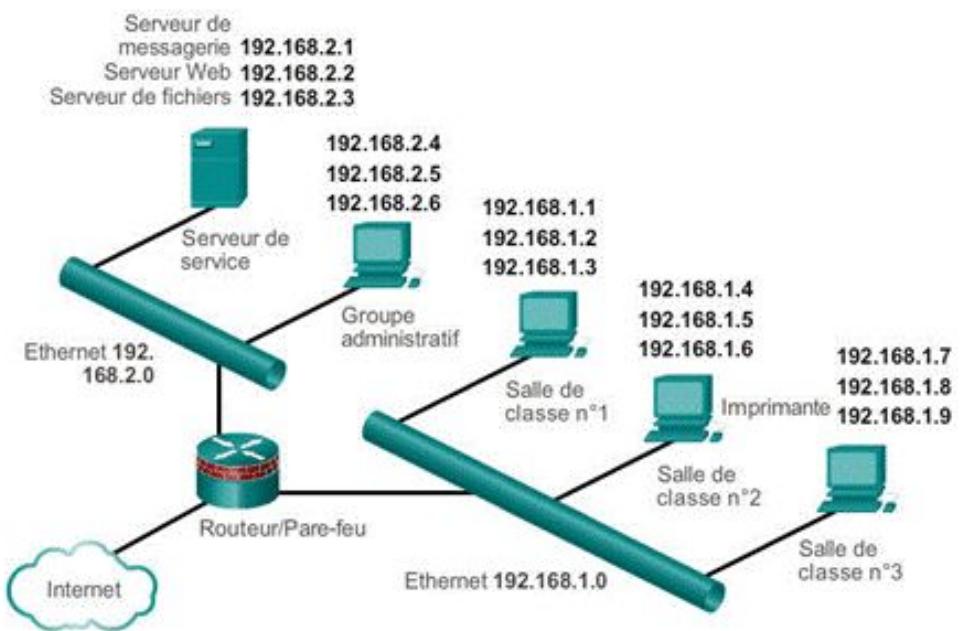
Schémas de topologie

Topologie physique



- **Bus**
- **Anneau (Ring)**
- **Maillage (Mesh)**
- **Etoile (Star)**

Topologie logique



Caractéristiques d'un réseau

Types de réseaux : par topologie

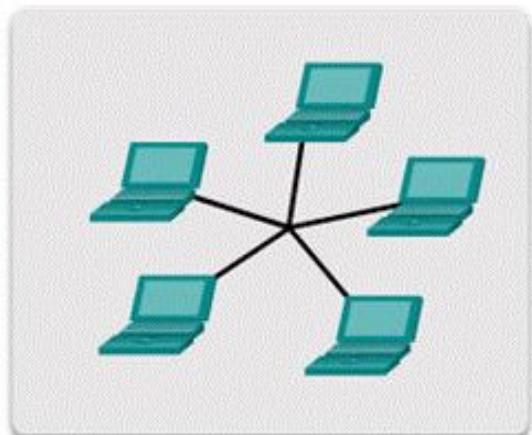
Ils peuvent également être catégorisés par topologie de réseau :

- **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.
- **Réseau en arbre** : souvent un réseau en étoile réparti sur plusieurs niveaux (étoile étendue)

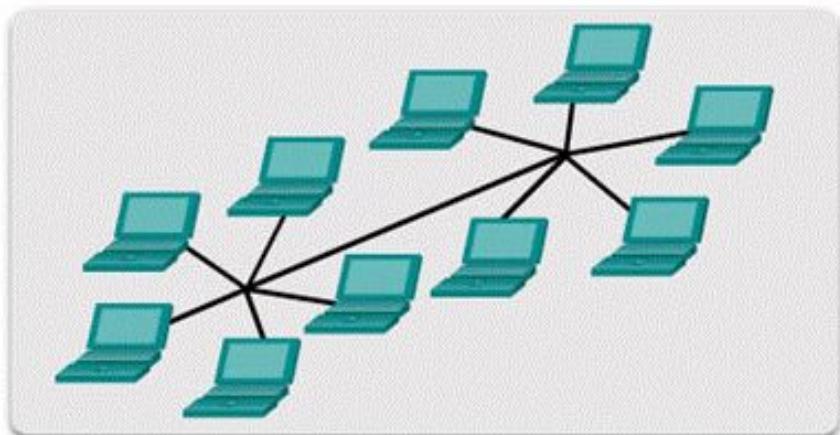
Caractéristiques d'un réseau

Topologie physique

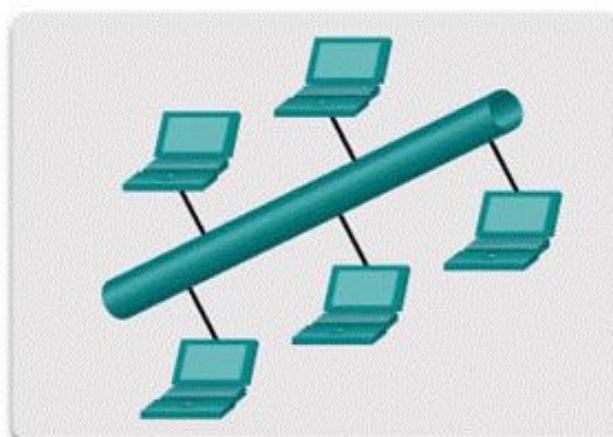
Topologies physiques



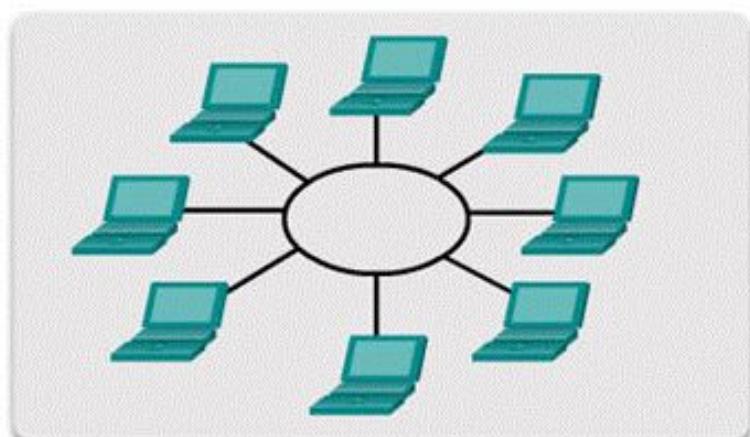
Topologie en étoile



Topologie en étoile étendue



Topologie en bus



Topologie en anneau

Caractéristiques d'un réseau

Autres caractéristiques

Alors que les réseaux évoluent, nous découvrons que les architectures sous-jacentes doivent prendre en considération des caractéristiques de base si elles veulent répondre aux attentes des utilisateurs :

- Coût
- Performance (Débit)
- Fiabilité
- Sécurité
- Disponibilité (Tolérance aux pannes)
- Évolutivité
- Qualité de service (QS)

Tendances relatives aux réseaux **Nouvelles tendances**

Les plus répandues incluent :

- Le BYOD (Bring Your Own Device)
- La collaboration en ligne
- Les vidéos
- Le cloud computing
- Les Data Centers
- Les smart homes



FIN



Chapitre 1:

Les protocoles et modèles de communication réseau



ISMAEL DOUKSIEH





Objectifs:

- Expliquer comment les règles sont utilisées pour faciliter la communication humaine
- Expliquer le rôle des protocoles et des organismes de normalisation en tant que facilitateurs de l'interopérabilité des communications réseau
- Expliquer les modèles TCP/IP et OSI
- Expliquer les processus d'encapsulation et de désencapsulation



Chapitre 2:

Les protocoles et modèles de communication d'un réseau

ISMAEL DOUKSIEH

Les règles de communication

La communication n'est certainement pas un but en soi mais bien un **instrument**, une **ressource**, au service de l'efficacité des organisations.

Un réseaux fait appel à la cohérence de l'architecture de communication.

Architecture de communication : On appelle architecture de communication l'ensemble des règles qui définissent, structurent et organisent les échanges d'informations entre les systèmes et les infrastructures de communication.

Système de communication : Un système de communication correspond à l'ensemble des composants matériels et logiciels qui assurent le traitement et le contrôle des échanges d'informations pour satisfaire un besoin de communication, au niveau d'une communauté d'usagers.

Infrastructure de communication : Quant à l'infrastructure de communication, il s'agit de l'ensemble des moyens matériels et logiciels qui assurent la transmission des informations. Elle est constituée par des équipements de réseaux, matériels et logiciels, et des éléments de liaison.

Les règles

Qu'est-ce que la communication ?

Communication humaine



Détermination des règles

- Expéditeur et destinataire identifiés
- Accord sur le mode de communication (face-à-face, téléphone, lettre, photographie)
- Même langue et syntaxe
- Vitesse et rythme d'élocution
- Demande de confirmation ou d'accusé de réception



les règles

Mise en forme, encapsulation et synchronisation des messages

Exemple – Une lettre personnelle comprend les éléments suivants :

- Le nom du destinataire
- Une formule de politesse
- Le contenu du message
- Une phrase de conclusion
- Le nom de l'expéditeur

Synchronisation des messages

- Méthode d'accès
- Contrôle de flux
- Délai d'attente de la réponse

Expéditeur
4085 rue des pins
Ocala, Floride 34471



Destinataire
1400 rue principale
Canton, Ohio 44203

Les règles

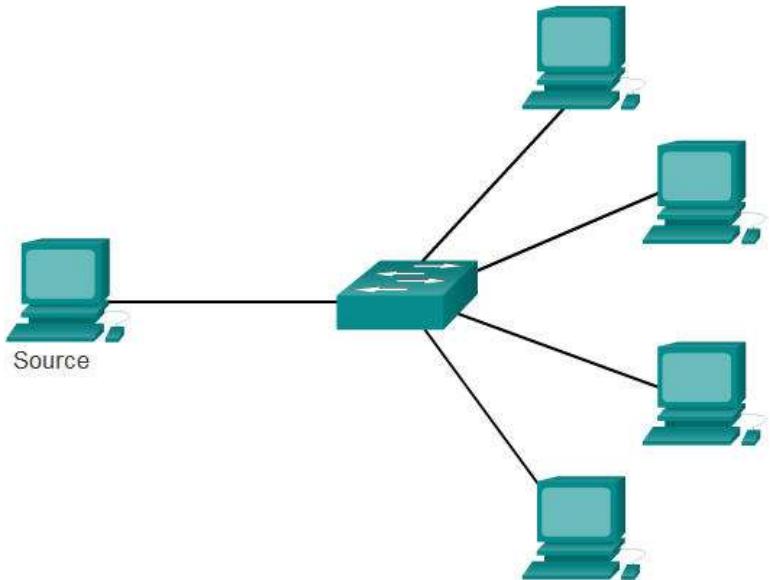
Options de remise des messages



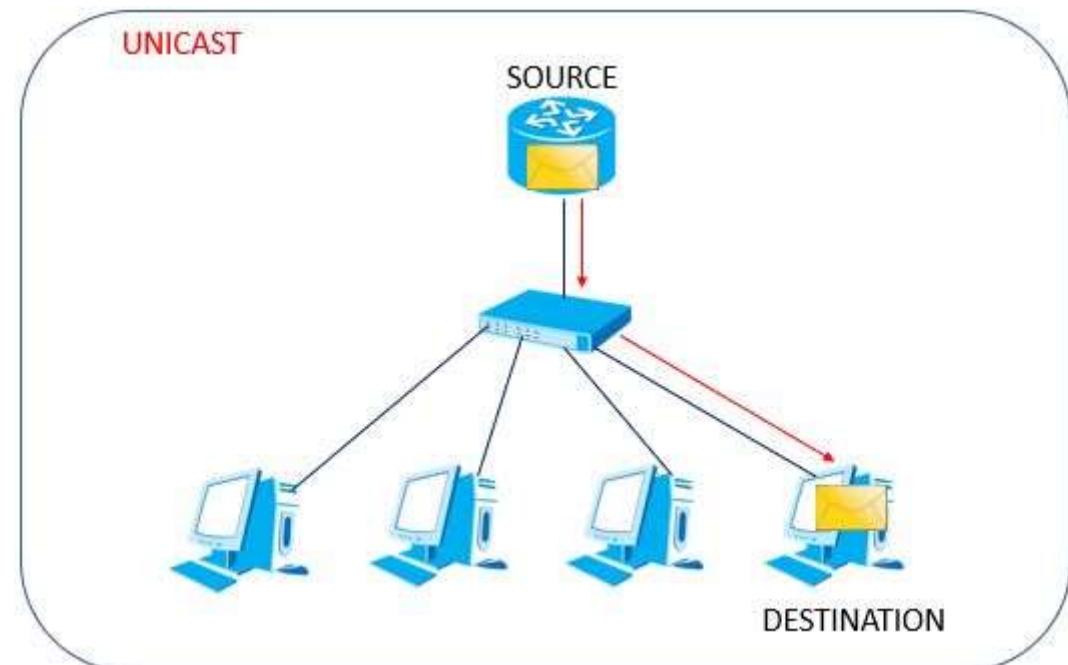
Monodiffusion

Multidiffusion

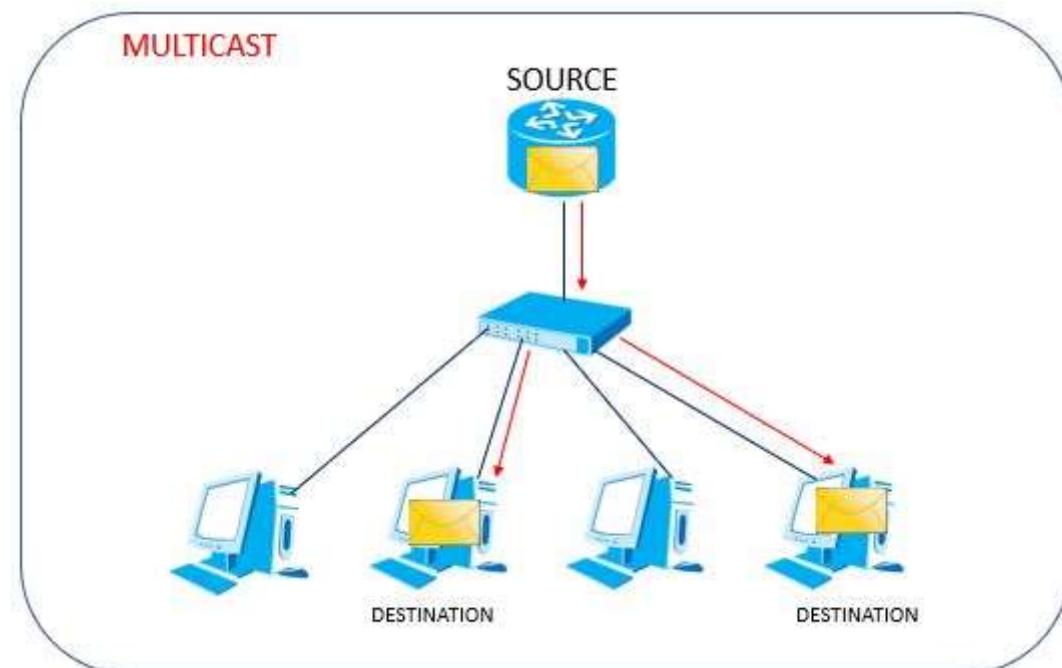
Diffusion



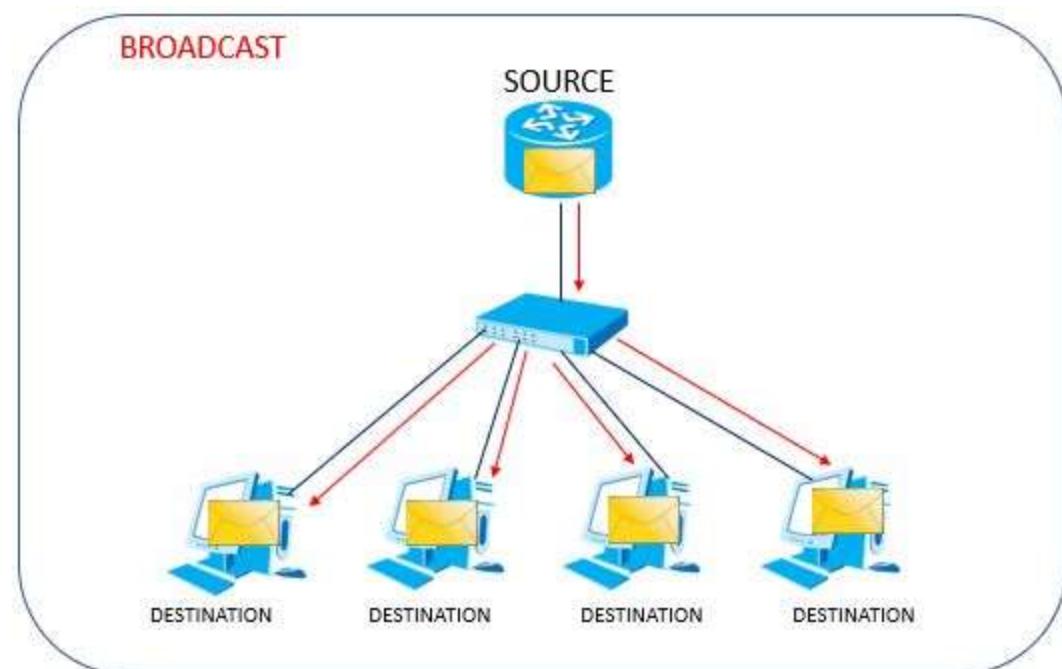
UNICAST



MULTICAST



BROADCAST



Protocoles

Règles qui régissent les communications

Protocoles : règles qui régissent les communications

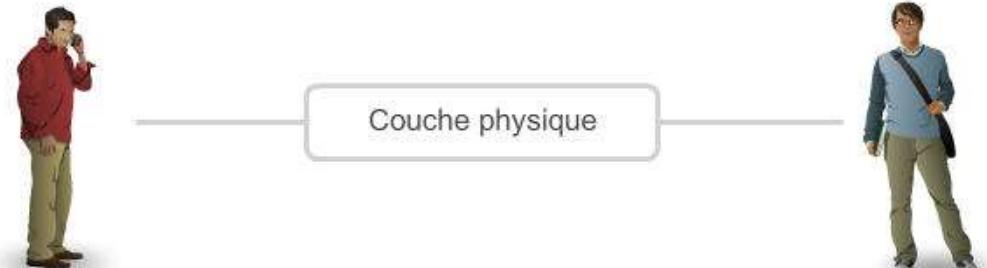
Couche contenu

Où est le café ?

Suite des protocoles de conversation

1. Utiliser une langue commune
2. Attendre son tour
3. Signaler la fin du message

Couche règles



Les suites de protocoles sont des ensembles de règles qui fonctionnent conjointement en vue de résoudre un problème.



Les protocoles du réseau

ISMAEL DOUKSIEH

Protocoles

Protocoles réseau

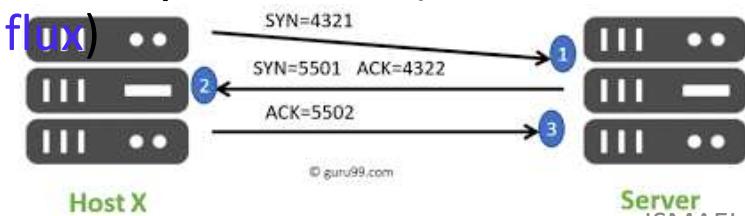
Les protocoles rendent possible le dialogue entre des machines différentes en définissant les règles pour réaliser une communication.

- Format ou structure du message
- La méthode selon laquelle les périphériques réseau partagent des informations à propos des chemins avec d'autres réseaux
- Le mode et le moment de transmission de messages d'erreur et de messages systèmes entre les périphériques
- L'établissement et la fin des sessions de transfert de données

Les protocoles TCP et UDP couche 4

Le protocole TCP

- **TCP** (Transmission Control Protocol) est un protocole de transport complexe donc lent (20 octet) mais **fiable, bidirectionnel** et utilisé en **mode connecté** qui assure la transmission des données de bout en bout (d'un processus à un autre processus). (**contrôle de flux**)



Le protocole UDP

- **UDP** (User Datagram Protocol) est un protocole simple donc **rapide** (8 octet) mais décrit comme étant **non-fiable**, utilisé en mode **non-connecté** qui assure la transmission des données de bout en bout d'un processus à un autre processus. (**voip**)

Normes et protocoles réseau

Organismes de normalisation



The Internet Corporation for Assigned Names and Numbers



LA NORMALISATION

- La normalisation existe pour :
 - Faciliter l'interconnexion et la communication entre différents utilisateurs.
 - Faciliter la portabilité d'équipements fonctionnellement, dans des applications différentes, et géographiquement, dans des régions différentes.
 - Assurer l'interopérabilité d'un équipement.
 - Garantir la pérennité donc l'amortissement des investissements (*utilisation technique valable du moment*).

Organismes de normalisation **Normes ouvertes**

- **Internet Society (ISOC):**

Une organisation non-lucrative pour soutenir financièrement l'IETF

- **Internet Architecture Board (IAB)**

Une organisation qui s'intéresse à l'évolution de l'Internet

- **Internet Engineering Task Force (IETF)**

Groupe informel ouvert participants à l'élaboration des standards sur Internet.

- **Institute of Electrical and Electronics Engineers (IEEE)**

Institut des ingénieurs électriciens et électroniciens.

- **International Organization for Standards (ISO)**

Organisation Internationale de Standardisation

Modèles de référence

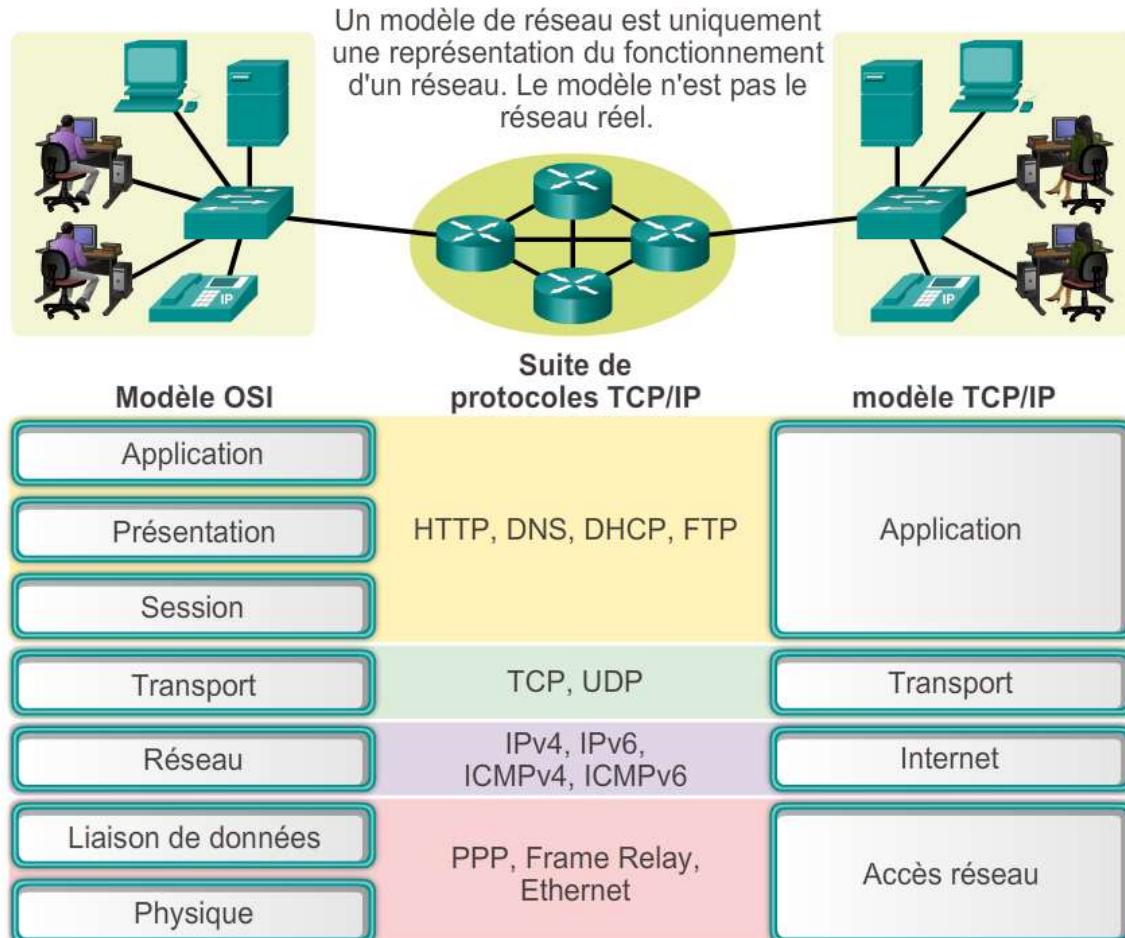
Les modèles TCP/IP et OSI

Un **modèle de référence** est utilisé pour décrire la structure et le fonctionnement des communications réseaux. On connaît deux modèles :

- Le **modèle OSI** (Open Systems Interconnect) qui correspond à une approche plus théorique en décomposant le fonctionnement en une **pile de 7 couches**.
- Le **modèle DoD** (Department Of Defense) qui répond à un problème pratique comprenant une **pile de 4 couches** pour décrire le réseau Internet (la famille des protocoles TCP/IP).

Modèles de référence

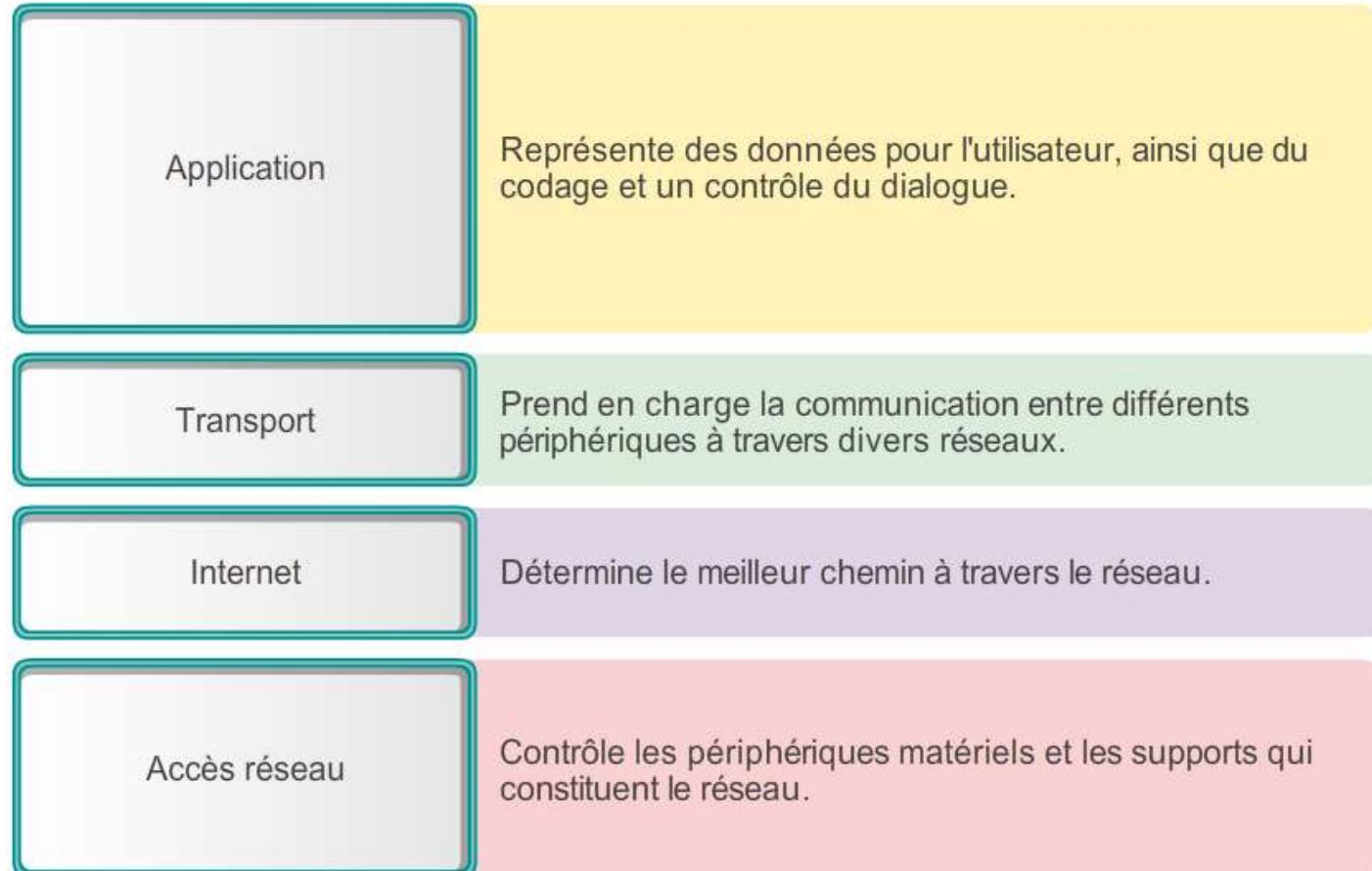
Avantages de l'utilisation d'un modèle composé de couches



Modèles de référence

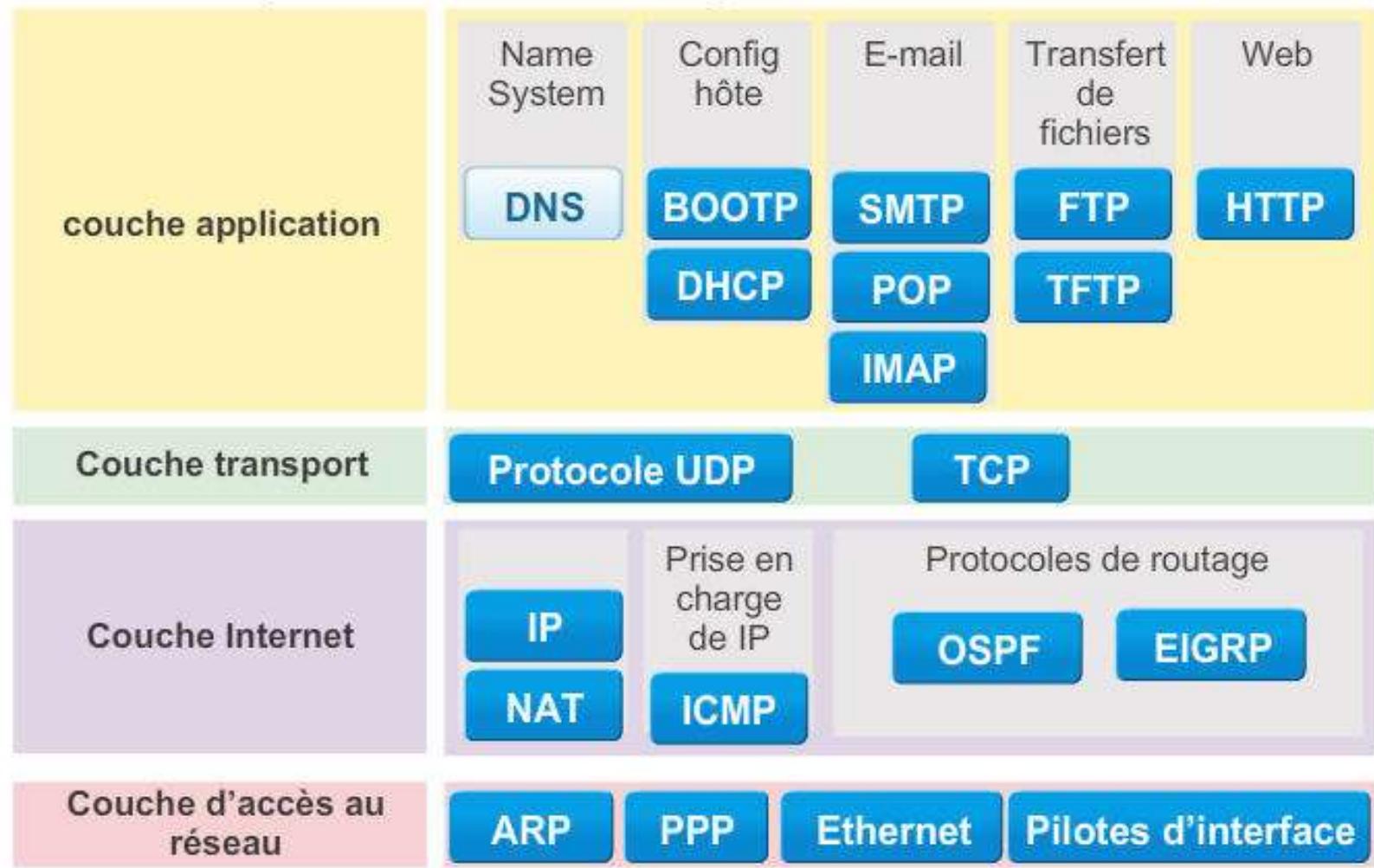
Le modèle de référence TCP/IP (DoD)

modèle TCP/IP



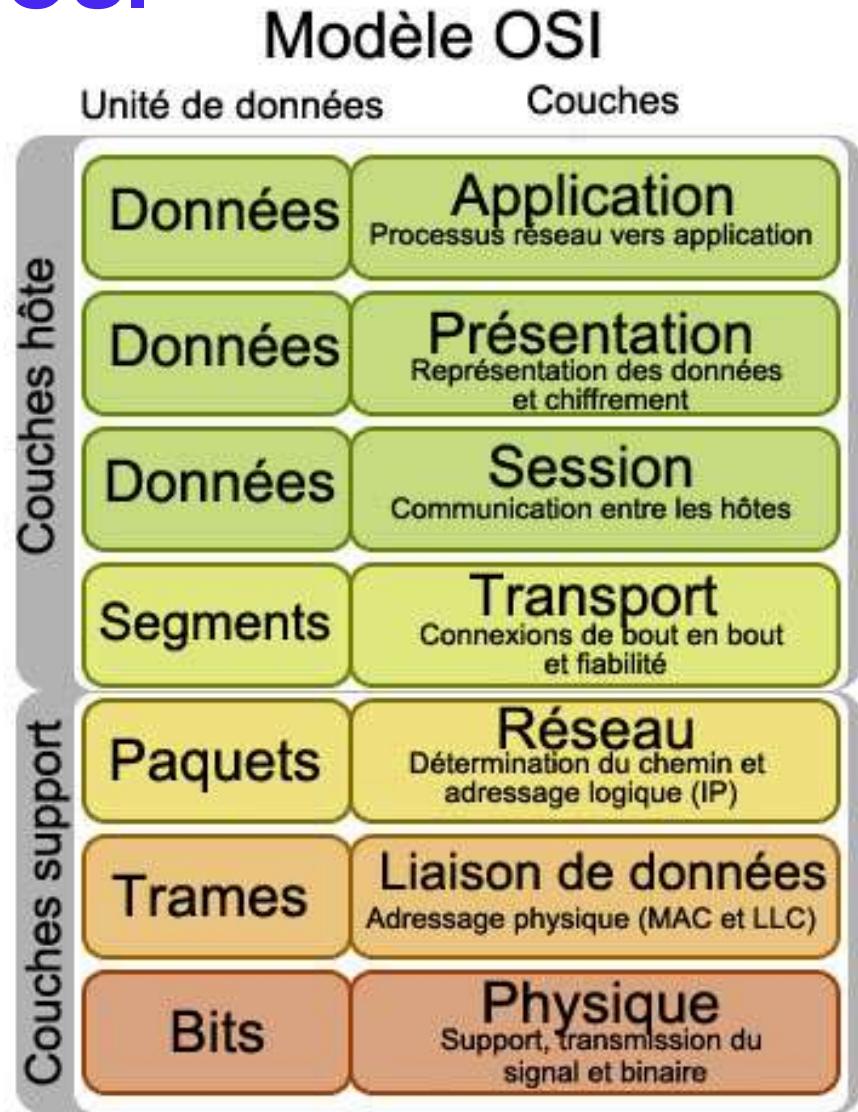
Suites de protocoles

Suite de protocoles TCP/IP et processus de communication



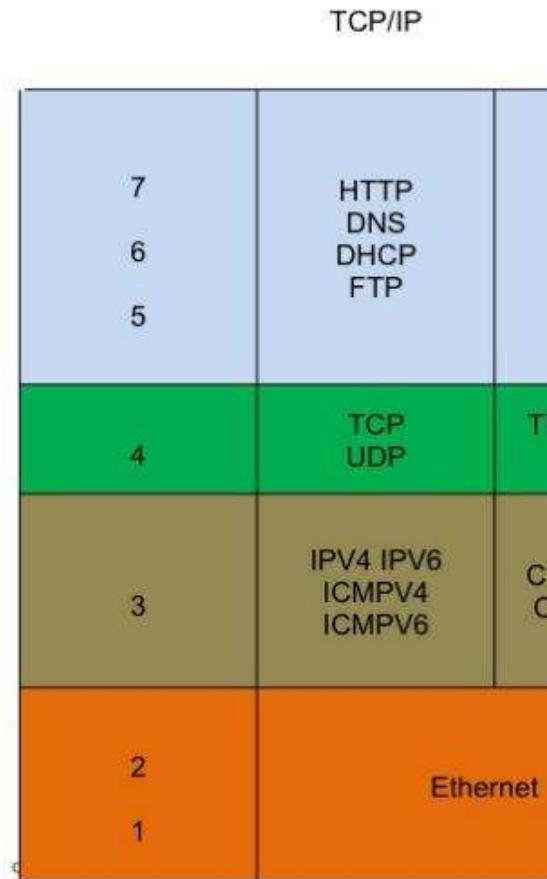
Modèles de référence

Le modèle de référence OSI



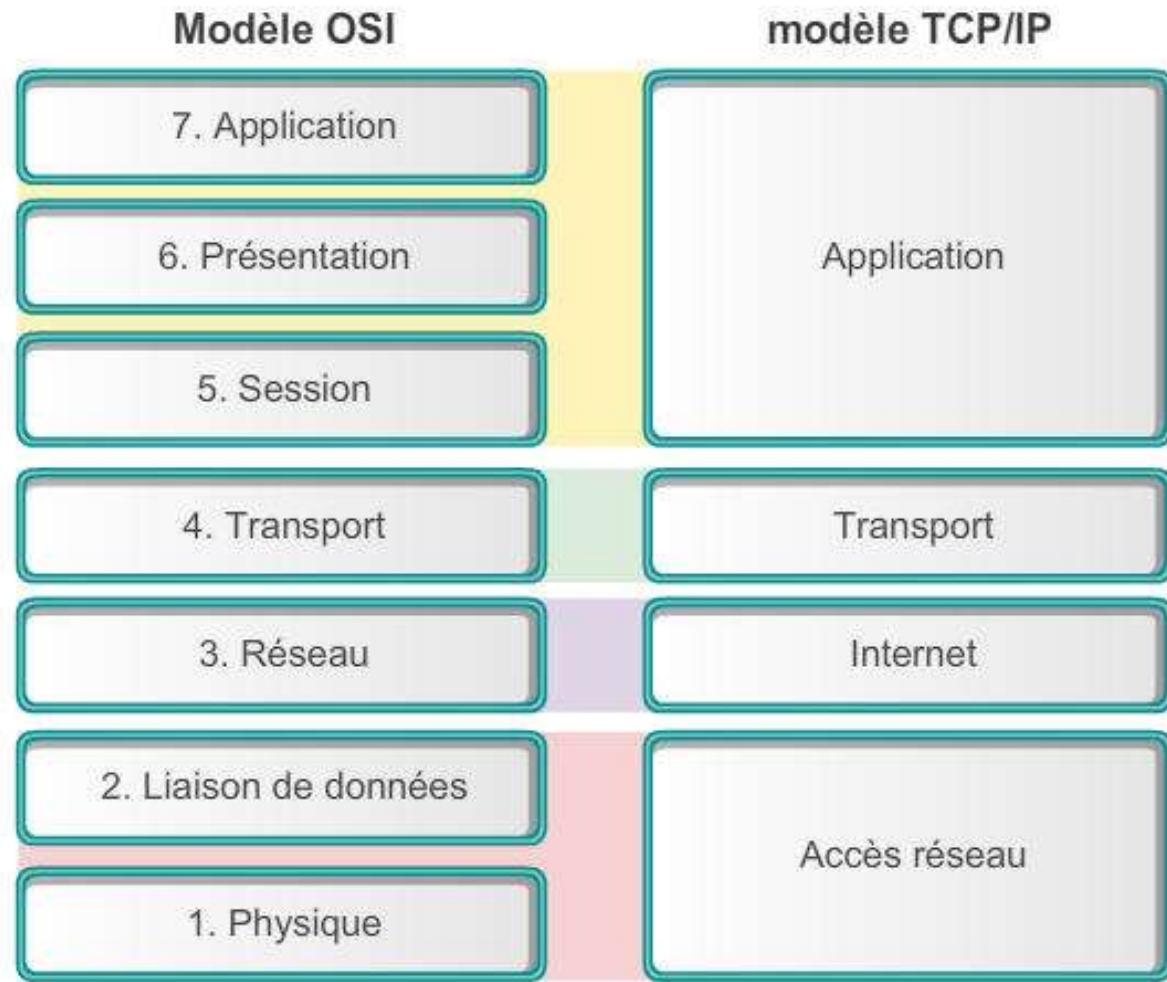
Suites de protocoles

Suites de protocoles et normes de l'industrie



Modèles de référence

Comparaison des modèles OSI et TCP/IP



La Couche 1 : La couche Physique

Transmission et réception de données entre l'appareil et le support de transmission.

Supports de Transmission:

- Signaux électriques - Ethernet, câbles coaxiaux ...
- Signaux radio (Wi-Fi)
- Signaux optiques (Fibre ...)

Fonctions: synchronisation des bits, contrôle du débit binaire, topologies physiques, mode de transmission (half-duplex, full-duplex) ...

Technologies & Protocoles: Bluetooth, USB, couche physique Ethernet (1000BASE-T ...), DSL, RNIS, infrarouge, Tl...

Périphériques: concentrateurs, répéteurs, modems, câbles ...

La Couche 2 : La couche Liaison de données

Assure le transfert de données de nœud à nœud.

Dispose de 2 sous-couches:

Couche **Contrôle d'Accès au Support** (MAC): contrôle la façon dont l'appareil accède aux supports et transfère les données

Couche **Contrôle de la Liaision Logique** (LLC): identifie et encapsule les protocoles de couche réseau, contrôle également la vérification des erreurs et la synchronisation des trames

Fonctions: Création de trames, adressage physique, contrôle d'erreur, contrôle de flux, contrôle d'accès.

Technologies et protocoles: Ethernet (802.3), WiFi (802.11), PPP, HDLC, FDDI, VTP, VLAN, DTP...

Périphériques: commutateurs L2

La Couche 3 : La couche Réseau

Responsable de la transmission des paquets, y compris le **routage** via des routeurs intermédiaires pour livrer les paquets de la source à la destination sur plusieurs liens (réseaux) ... Parce que tous les appareils ne sont pas directement connectés les uns aux autres.

IP est un protocole de couche réseau et l'adresse IP est celle qu'IP utilise pour déterminer où un paquet doit aller.

Fonctions: routage, adressage logique.

Technologies et protocoles: IP, ICMP, IPSEC, OSPF, RIP, HSRP, VRRP, NAT, ARP...

Périphériques: routeurs, commutateurs L3, pare-feu ...

La Couche 4 : La couche Transport

La couche transport fournit un transfert fiable et transparent des données entre les ordinateurs d'un réseau ou à travers différents réseaux.

Elle contrôle la fiabilité d'une liaison donnée grâce au contrôle de flux et d'erreur, à la segmentation / de-segmentation et au contrôle d'erreur...

Elle ajoute également les numéros de port source et destination dans son en-tête.

Technologies et protocoles: TCP, UDP, SCTP, AH, ESP...

La Couche: 5 et 6

Couche 5: Couche Session

Cette couche assure l'établissement, la maintenance et la fin de session entre les deux couches d'application.

Couche 6: Couche Présentation

Cette couche assure la traduction des données transférées entre les applications sur les 2 hôtes. Les données de la couche application sont extraites, manipulées et formatées selon les besoins avant d'être transmises.

Fonctions: traduction, cryptage / décryptage, compression.

La Couche 7 : La couche Présentation

Cette couche est plus proche de l'utilisateur final.

C'est là que réside l'application logicielle qui interagit avec l'utilisateur final et la couche d'application du modèle OSI.

Les services des applications de cette couche peuvent interagir avec d'autres applications telles que le traitement de texte, les bases de données ...

Technologies et protocoles: HTTP, FTP...



LECTURE

<https://www.geeksforgeeks.org/tcp-ip-model/>

<https://www.geeksforgeeks.org/layers-of-osi-model/>



Encapsulation et Désencapsulation

<https://www.techopedia.com/definition/25292/protocol-data-unit-pdu>

Encapsulation des données

Unités de données de protocole (PDU)

PDU: Unité de Données de Protocole (Protocol Data Unit)

Du point de vue de l'expéditeur, à chaque couche du modèle OSI (cela s'applique également à TCP / IP), les données provenant de la couche application sont transformées et traitées afin d'être prêtes pour leur voyage vers le récepteur.

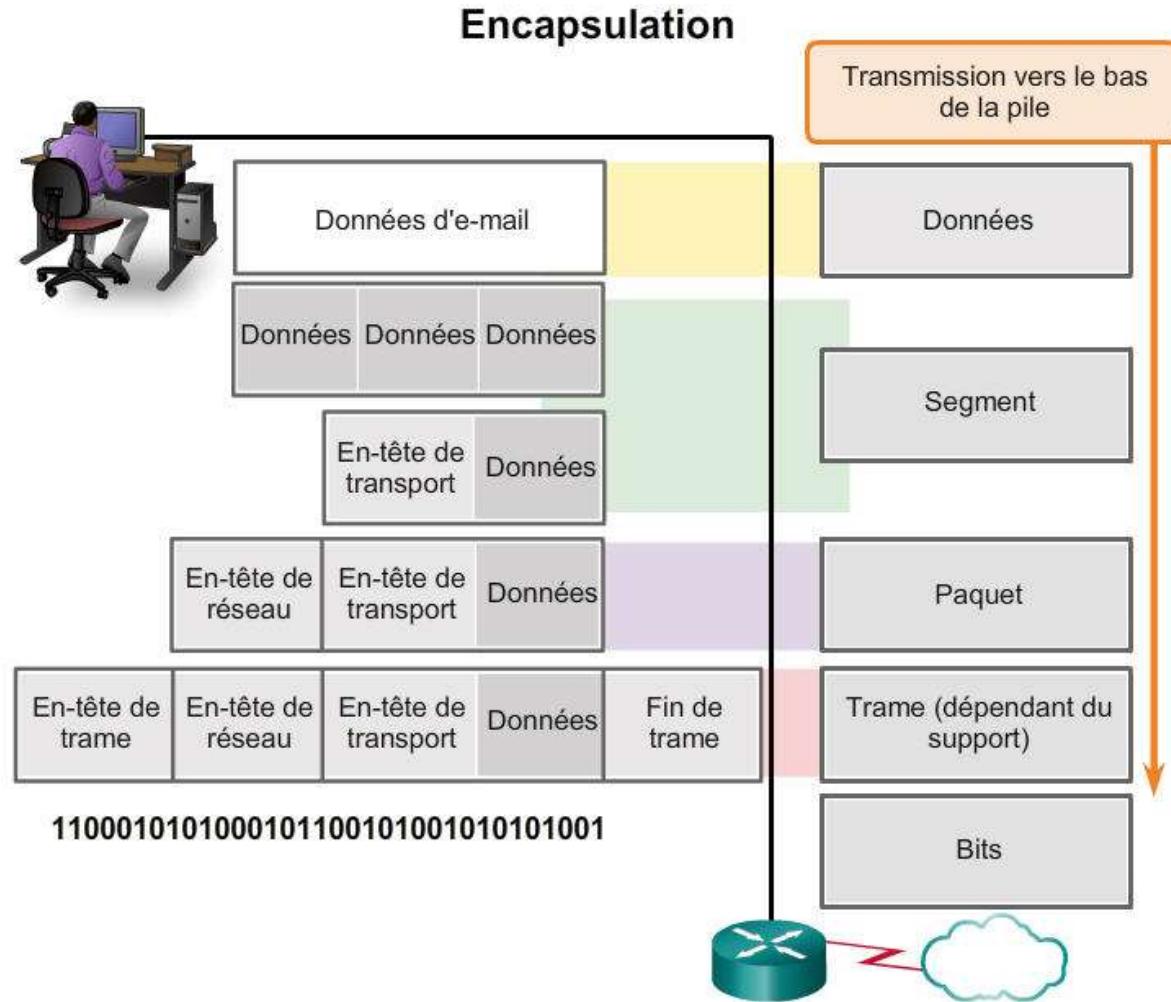
À chaque couche, plus d'informations sont ajoutées contenant des détails spécifiques pour cette couche.

Les données traitées à chaque couche sont appelées PDU ou Protocol Data Unit. Une PDU a un nom en fonction de la couche que nous considerons:

Encapsulation des données

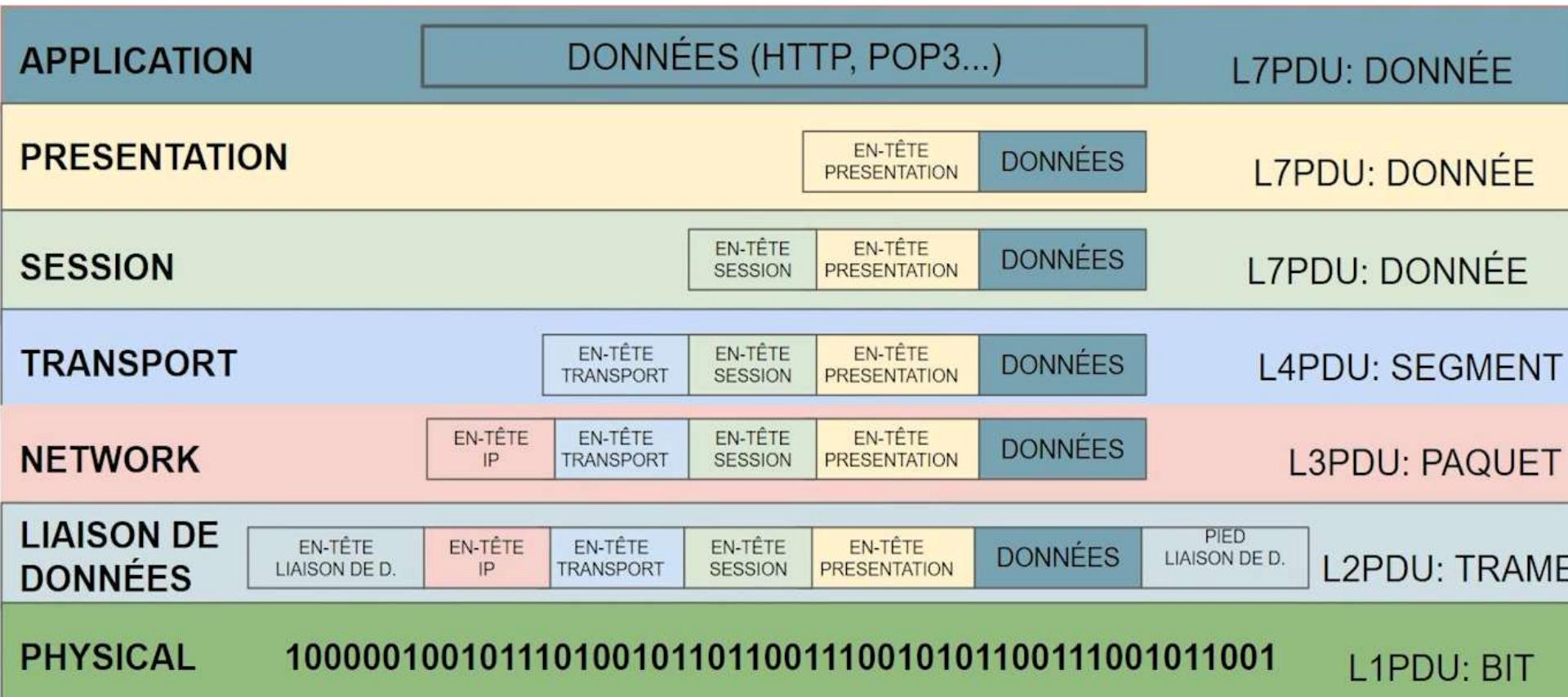
Unités de données de protocole (PDU)

- Données
- Segment
- Paquet
- Trame
- Bits



Encapsulation des données

Encapsulation | MODELE OSI



Encapsulation des données

Encapsulation | MODELE TCP/IP

APPLICATION

DATA http GET request url: xyx.com

PDU: DATA

TRANSPORT

EN-TÊTE TRANSPORT
TCP/UDP
SOURCE/DEST # PORT

DATA
html GET req.
xyx.com

PDU: SEGMENT

INTERNET

EN-TÊTE IP
IP ADRESSE
SOURCE/DEST

EN-TÊTE TRANSPORT
TCP/UDP
SOURCE/DEST # PORT

DATA
html GET req.
xyx.com

PDU: PACKET

NETWORK
ACCESS

EN-TÊTE ACCES
RESEAU
ADRESSE MAC
SOURCE/DEST

EN-TÊTE IP
IP ADRESSE
SOURCE/DEST

EN-TÊTE TRANSPORT
TCP/UDP
SOURCE/DEST # PORT

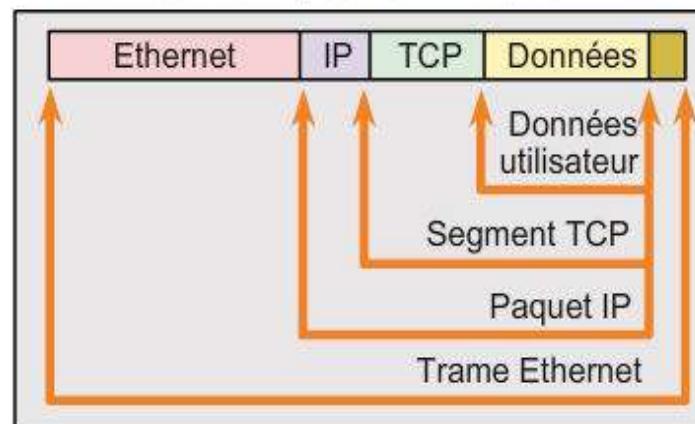
DATA
html GET req.
xyx.com

PIED ACCÈS
RÉSEAU
FCS

PDU: FRAME

Encapsulation des données Désencapsulation

Termes d'encapsulation de protocole



Serveur Web

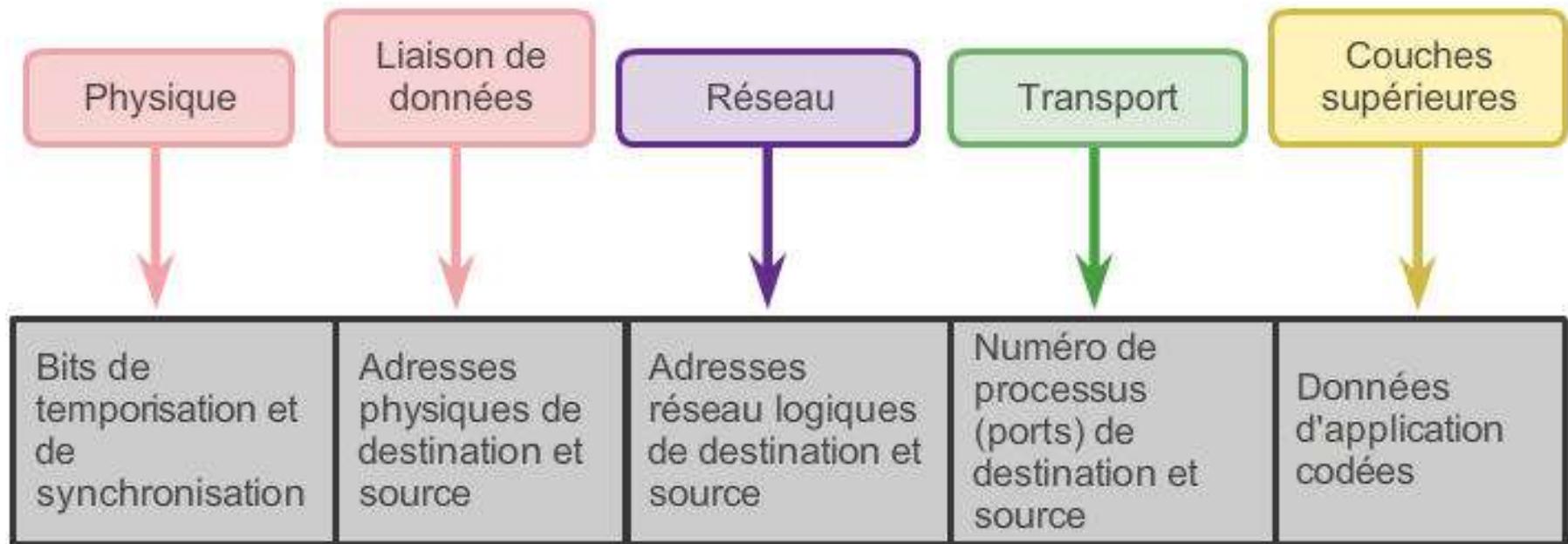


Client Web

0101011010100101111011010100100101010110110

Déplacement des données sur le réseau

Accès aux ressources locales



es aux ressources locales

Adresses d'application, de réseau et de liaison de données

■ Adresse d'application

- ✓ Numéro de Port source
- ✓ Numéro de Port destination

■ Adresse réseau

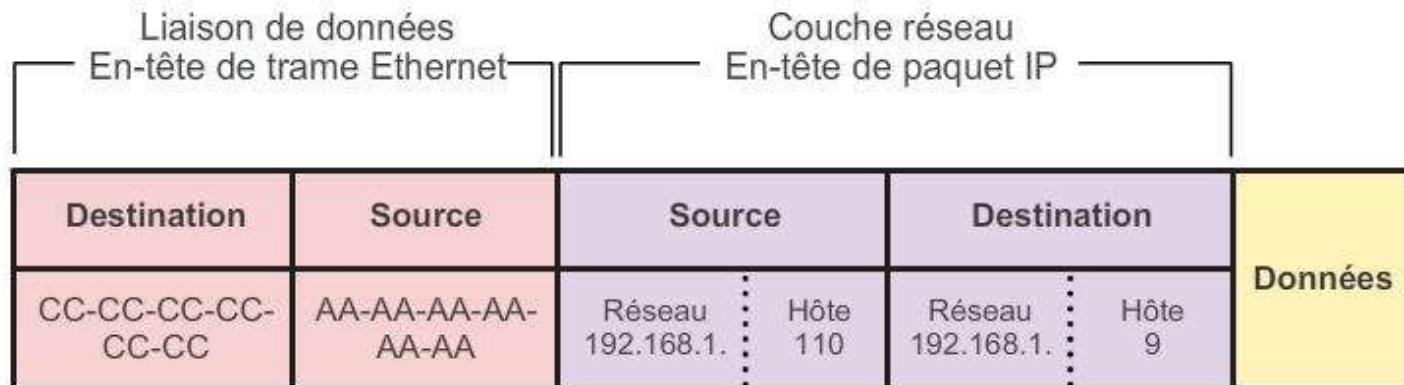
- ✓ Adresse IP source
- ✓ Adresse IP de destination

■ Adresse de liaison de données

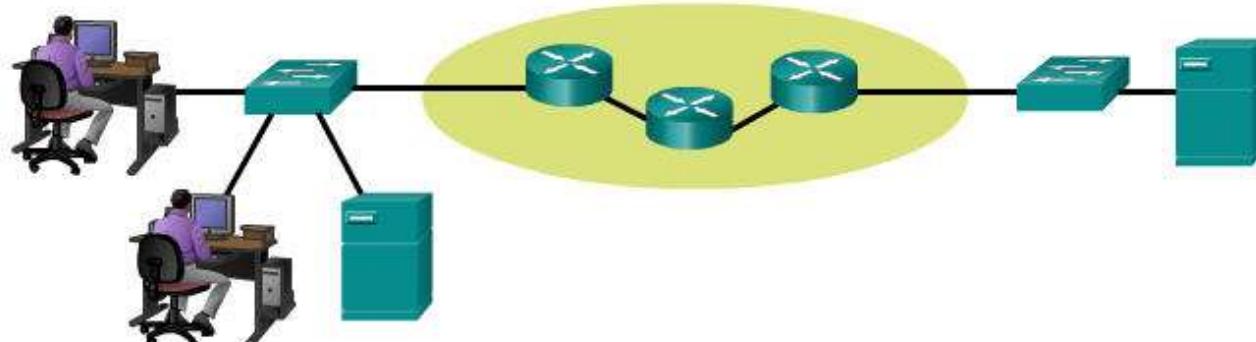
- ✓ Adresse de liaison de données source
- ✓ Adresse de liaison de données de destination

Accès aux ressources locales

Communication avec un périphérique sur le même réseau



PC1
192.168.1.110
AA-AA-AA-AA-AA-AA



Serveur FTP
192.168.1.9
CC-CC-CC-CC-CC-CC

Protocoles

Interaction des protocoles

- Protocole d'application : protocole de transfert hypertexte (HTTP, Hypertext Transfer Protocol)
- Protocole de transport : protocole de contrôle de transmission (TCP, Transmission Control Protocol)
- Protocole Internet : IP (Internet Protocol)
- Protocoles d'accès au réseau : liaisons de données et couches physiques

Protocoles

ARP : Adress Resolution Protocol

Pour envoyer des informations à un autre appareil, l'expéditeur a besoin de **l'adresse IP** de sa destination (adresse logique) et de **l'adresse MAC** (adresse physique) de son voisin.

L'adresse IP est connue, mais l'adresse MAC doit être apprise du voisin. C'est pour cela ARP existe.

ARP: Protocole de résolution d'adresse (Address Resolution Protocol)

C'est un protocole de communication utilisé pour découvrir l'adresse physique d'un périphérique ou d'un nœud dans un réseau.

Il s'agit d'un broadcast.



FIN

ISMAEL DOUKSIEH

Chapitre 4 : Les adressages du Réseau

Une adresse IP (Internet Protocol) est une identification unique pour un hôte sur un réseau IP. Une adresse IP est un nombre d'une valeur de 32 bits représentée par 4 valeurs décimales pointées ; chacune a un poids de 8 bits (1 octet) prenant des valeurs décimales de 0 à 255 séparées par des points. On distingue en fait deux parties dans l'adresse IP :

- ✓ une partie des nombres à gauche désigne le réseau et est appelée ID de réseau (en anglais *net-ID*),
- ✓ Les nombres de droite désignent les ordinateurs de ce réseau et est appelée ID d'hôte (en anglais *host-ID*).

Classes d'adresses IP

Pour faciliter l'administration des réseaux et la bonne répartition des adresses IP, l'organisme ayant la charge d'attribuer les adresses (l'IANA) a séparer les adresses IP en différentes catégories appelée classes. Il en existe 3 principales et 2 qui ne peuvent pas être attribuée à des machines. Ces 5 classes sont représentées par une lettre allant de A à E.

Classe	Masque de sous réseau par défaut	Adresse réseau	Nombre de réseaux	Nombre d'hôtes
A	255.0.0.0	1.0.0.0 à 126.0.0.0	126 (= $2^7 - 2$)	16 777 214
B	255.255.0.0	128.0.0.0 à 191.255.0.0	16 384 (= 2^{14})	65 534
C	255.255.255.0	192.0.0.0 à 223.255.255.0	2 097 152 (= 2^{21})	254
D	Non défini	224.0.0.0 à 239.255.255.0		
E	Non défini	240.0.0.0 à 255.255.255.0		

Seules les adresses de Classes A, B et C sont attribuables à des interfaces.

La classe D est utilisée pour des adresses de Multicast (adresse unique identifiant de nombreuses destinations)

La classe E est utilisée pour des besoins futurs ou des objectifs scientifiques

Les adresses spécifiques :

Pour chaque classe, il y a un pool d'adresses réservées pour l'utilisation de réseaux privés. Ces adresses ne sont pas routées sur Internet. Il faut obligatoirement utiliser ces adresses sur un réseau local privé.

Classe	Plage d'adresses	Masque
A	10.0.0.0 à 10.255.255.254	10/8 (255.0.0.0)
B	172.16.0.0 à 172.31.255.254	172.16/12 (255.240.0.0)
C	192.168.0.0 à 192.168.255.254	192.168/16 (255.255.0.0)

Les adresses commençant de 127.0.0.0 à 127.255.255.255 sont réservées pour le bouclage (loopback).

Distinction de la partie réseau de la partie hôte

Par défaut :

- ✓ La partie réseau des adresses de Classe A portera sur le premier octet et la partie hôte sur les trois derniers ($2^{24} = 16\ 777\ 216$ hôtes possibles par réseau)
- ✓ La partie réseau des adresses de Classe B portera sur les deux premiers octets et la partie hôte sur les deux derniers ($2^{16} = 65\ 536$ hôtes possibles par réseau)
- ✓ La partie réseau des adresses de Classe C portera sur les trois premiers octets et la partie hôte sur le dernier ($2^8 = 256$ hôtes possibles par réseau)

Partie Réseau	Partie Hôte
Adresse de la Classe A	100 . 150 . 25 . 3
Adresse de la Classe B	136 . 10 . 100 . 25
Adresse de la Classe C	195 . 74 . 212 . 12

Exemple d'adresses IP avec les hôtes possibles dans ce réseau, par défaut

Utilisation d'un masque

Un masque sera une suite de 32 bits divisée en 4 octets pointés composée uniquement d'abord d'une suite de 1 et, après, d'une suite de 0. La notation est aussi décimale pointée. Il sert d'identificateur de la partie réseau et de la partie hôte. Chaque classe d'adresse possède un masque par défaut :

classes	Masques
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Un masque va préciser de manière certaine dans quel réseau se trouve un adresse IP en déterminant les éléments suivants :

- L'adresse du réseau (appelée aussi numéro de réseau, non assignable)
- L'adresse de broadcast (adresse visant toutes les destinations, non assignable)
- La plage d'adresses utilisables (de la première à la dernière en dehors des adresses précitées)

Méthode par calcul binaire :

L'adresse du réseau, l'adresse de broadcast et la plage d'adresses utilisables peut être obtenu à partir d'un calcul booléen de type ET ou la conjonction logique (une proposition est vraie lorsque les deux termes sont tous les deux vrais) :



a. Obtenir l'adresse du réseau :

Pour l'adresse IP 140.159.125.25, adresse de classe B à laquelle on applique un masque par défaut de 255.255.0.0 :

10001100.10011111.0111101.00011001 140.159.125.25
11111111.11111111.00000000.00000000 255.255.0.0

10001100.10011111.00000000.00000000 140.159.0.0

L'adresse du réseau est donc 140.159.0.0

b. Obtenir l'adresse de broadcast :

On va remplacer les bits de valeur 0 de la partie hôte du résultat obtenu pour l'adresse de réseau par des bits de valeur 1 :

10001100. 10011111. 00000000. 00000000 140.159.0.0
par :
10001100. 10011111. 11111111. 11111111 140.159.255.255

c. Obtenir la plage d'adresses de ce réseau :

La plage d'adresse du réseau sera comprise entre la première adresse utilisable et la dernière utilisable, autrement dit, celle qui suit l'adresse du réseau et celle qui précède l'adresse de broadcast :

De
10001100. 10011111. 00000000. 00000001 140.159.0.1
A
10001100. 10011111. 11111111. 11111110 140.159.255.254



Chap.4

VSLM

<https://www.ciscopress.com/articles/article.asp?p=2731924>

Connectivité Inter-réseau



ISMAEL DOUKSIEH

VLSM

Nous allons couvrir:

- Ce que nous avons fait jusqu'à présent (Subnetting)
- Le problème le MSR de même longueur
- C'est quoi VLSM (Variable Length Subnet Mask)
- L'avantage de VLSM

VLSM

Ce que nous avons fait jusqu'à présent

Nous avons plongé un réseau dans des sous-réseaux de taille égale.

Le problème le MSR de même longueur

Nous ne voulons pas toujours avoir le même nombre d'hôtes dans tous les sous-réseaux. Nous pouvons avoir besoin d'avoir plus d'hôtes certains sous-réseaux que d'autres.

C'est là que VLSM entre en jeu.

VLSM

C'est quoi VLSM (Masque de Sous-Réseau de Longueur variable)

Variable Length Subnet Masking nous permet de subdiviser un réseau en utilisant différents masques de sous-réseau pour répondre au besoin en nombre d'hôtes par réseau.

Comment diviser un réseau avec VLSM

Nous attribuons des masques de sous-réseau au réseau au sous-réseau en commençant par le plus grand réseau, en descendant vers les plus petits selon le nombre d'hôtes que chaque MSR peut contenir

L'avantage de VLSM

Meilleure allocation des adresses IP à l'intérieur du réseau, principalement pour les réseaux publics



CAMPUS #3:

192.168.15.0/24

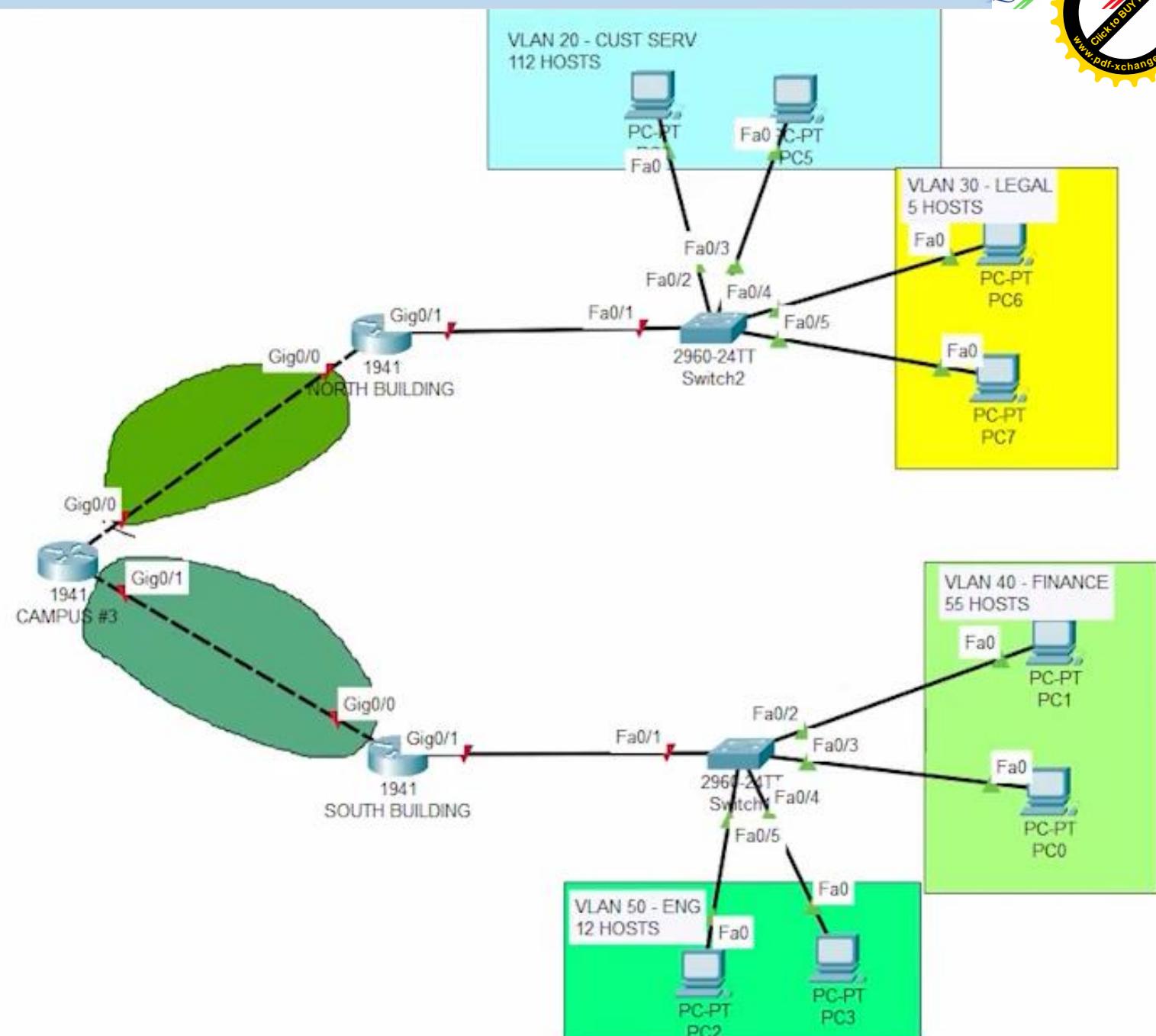
CUST SERV : 112 Hosts

FINANCE : 55 Hosts

ENG. : 12 Hosts

LEGAL : 5 Hosts

2xP2P : 2 hosts

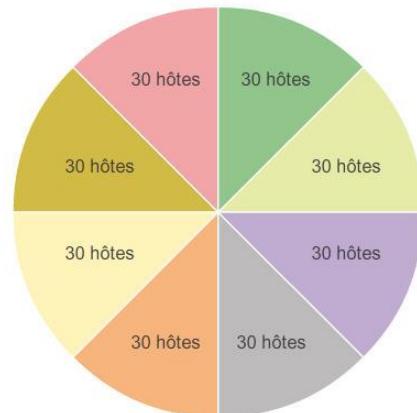


Les avantages des masques de sous-réseau de longueur variable

Les limites de la segmentation traditionnelle

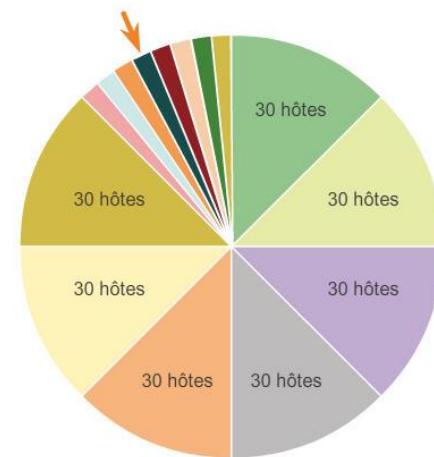
- Segmentation traditionnelle : le même nombre d'adresses est attribué à chaque sous-réseau.
- Les sous-réseaux qui n'ont pas besoin de la totalité ont des adresses inutilisées (gaspillées). Par exemple, les liaisons WAN n'ont besoin que de 2 adresses.
- Les masques de sous-réseau de longueur variable (VLSM, Variable Length Subnet Mask) ou la segmentation d'un sous-réseau optimisent l'utilisation des adresses.

La segmentation en sous-réseaux traditionnelle crée des sous-réseaux de taille égale



Sous-réseaux de tailles variables

Un sous-réseau a été à nouveau divisé pour créer 8 sous-réseaux plus petits de 4 hôtes chacun



Déterminer le masque de sous-réseau

Segmenter le réseau en sous-réseaux en fonction des besoins des hôtes (VLSM)

Deux considérations sont à prendre en compte lors de la planification de sous-réseaux :

- Nombre de sous-réseaux nécessaires
- Nombre d'adresses d'hôte nécessaires
- Formule pour déterminer le nombre d'hôtes utilisables

$$2^{n-2}$$

2^n (où n est le nombre de bits d'hôte restant) est utilisé pour calculer le nombre d'hôtes

-2 L'ID de sous-réseau et l'adresse de diffusion ne peuvent pas être utilisés sur chaque sous-réseau

Les avantages des masques de sous-réseau de longueur variable

Les masques de sous-réseau de longueur variable (VLSM)

- La technique VLSM permet de décomposer un espace réseau en parties inégales.
- Le masque de sous-réseau varie alors selon le nombre de bits ayant été empruntés pour un sous-réseau particulier.
- Le réseau est segmenté en premier, puis les sous-réseaux sont divisés à leur tour.
- Cette opération est répétée autant de fois que nécessaire pour créer des sous-réseaux de différentes tailles.



Exercice VLSM



FIN

Chapitre 3 : Les adressage Réseaux

Une adresse IP (Internet Protocol) est une identification unique pour un hôte sur un réseau IP. Une adresse IP est un nombre d'une valeur de 32 bits représentée par 4 valeurs décimales pointées ; chacune a un poids de 8 bits (1 octet) prenant des valeurs décimales de 0 à 255 séparées par des points. On distingue en fait deux parties dans l'adresse IP :

- ✓ une partie des nombres à gauche désigne le réseau est est appelée **ID de réseau** (en anglais *netID*),
- ✓ Les nombres de droite désignent les ordinateurs de ce réseau est est appelée **ID d'hôte** (en anglais *host-ID*).

Classes d'adresses IP

Pour faciliter l'administration des réseaux et la bonne répartition des **adresses IP**, l'organisme ayant la charge d'attribuer les adresses (l'IANA) a séparer les adresses IP en différentes catégories appelée classes. Il en existe 3 principales et 2 qui ne peuvent pas être attribuée à des machines. Ces **5 classes** sont représentées par une lettre allant de A à E.

Classe	Masque de sous réseau par défaut	Adresse réseau	Nombre de réseaux	Nombre d'hôtes
A	255.0.0.0	1.0.0.0 à 126.0.0.0	126 (= $2^7 - 2$)	16 777 214
B	255.255.0.0	128.0.0.0 à 191.255.0.0	16 384 (= 2^{14})	65 534
C	255.255.255.0	192.0.0.0 à 223.255.255.0	2 097 152 (= 2^{21})	254
D	Non défini	224.0.0.0 à 239.255.255.0		
E	Non défini	240.0.0.0 à 255.255.255.0		

Seules les adresses de Classes A, B et C sont attribuables à des interfaces.

La classe D est utilisée pour des adresses de Multicast (adresse unique identifiant de nombreuses destinations)

La classe E est utilisée pour des besoins futurs ou des objectifs scientifiques

Les adresses spécifiques :

Pour chaque classe, il y a un pool d'adresses réservées pour l'utilisation de réseaux privés. Ces adresses ne sont pas routées sur Internet. Il faut obligatoirement utiliser ces adresses sur un réseau local privé.

Classe	Plage d'adresses	Masque
A	10.0.0.0 à 10.255.255.254	10/8 (255.0.0.0)
B	172.16.0.0 à 172.31.255.254	172.16/12 (255.240.0.0)
C	192.168.0.0 à 192.168.255.254	192.168/16 (255.255.0.0)

Les adresses commençant de 127.0.0.0 à 127.255.255.255 sont réservées pour le bouclage (loopback).

Distinction de la partie réseau de la partie hôte

Par défaut :

- ✓ La partie **réseau** des adresses de **Classe A** portera sur le premier octets et la partie **hôte** sur les trois derniers ($2^{24} = 16\ 777\ 216$ hôtes possibles par réseau)
- ✓ La partie **réseau** des adresses de **Classe B** portera sur les deux premiers octets et la partie **hôte** sur les deux derniers ($2^{16} = 65\ 536$ hôtes possibles par réseau)
- ✓ La partie **réseau** des adresses de **Classe C** portera sur les trois premiers octets et la partie **hôte** sur le dernier ($2^8 = 256$ hôtes possibles par réseau)

Partie Réseau

Partie Hôte

Adresse de la Classe A	100 . 150 . 25 . 3	2 exp 24 = 16 777 216 hôtes possibles par sous-réseaux
Adresse de la Classe B	136 . 10 . 100 . 25	2 exp 16 = 65 536 hôtes possibles par sous-réseaux
Adresse de la Classe C	195 . 74 . 212 . 12	2 exp 8 = 256 hôtes possibles par sous-réseaux

Exemple d'adresses IP avec les hôtes possibles dans ce réseau, par défaut

Utilisation d'un masque

Un masque sera une suite de 32 bits divisée en 4 octets pointés composée uniquement d'abord d'une suite de 1 et, après, d'une suite de 0. La notation est aussi décimale pointée. Il sert d'identificateur de la partie réseau et de la partie hôte. Chaque classe d'adresse possède un masque par défaut :

classes	Masques
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Un masque va préciser de manière certaine dans quel réseau se trouve un adresse IP en déterminant les éléments suivants :



- L'adresse du réseau (appelée aussi numéro de réseau, non assignable)
- L'adresse de broadcast (adresse visant toutes les destinations, non assignable)
- La plage d'adresses utilisables (de la première à la dernière en dehors des adresses précitées)

Méthode par calcul binaire :

L'adresse du réseau, l'adresse de broadcast et la plage d'adresses utilisables peut être obtenu à partir d'un calcul booléen de type ET ou la conjonction logique (une proposition est vraie lorsque les deux termes sont tous les deux vrais) :

a. Obtenir l'adresse du réseau :

Pour l'adresse IP 140.159.125.25, adresse de classe B à laquelle on applique un masque par défaut de 255.255.0.0 :

10001100.10011111.01111101.00011001 140.159.125.25
11111111.11111111.00000000.00000000 255.255.0.0

10001100.10011111.00000000.00000000 140.159.0.0

L'adresse du réseau est donc 140.159.0.0

b. Obtenir l'adresse de broadcast :

On va remplacer les bits de valeur 0 de la partie hôte du résultat obtenu pour l'adresse de réseau par des bits de valeur 1 :

10001100. 10011111. 00000000. 00000000 140.159.0.0
par :
10001100. 10011111. 11111111. 11111111 140.159.255.255

c. Obtenir la plage d'adresses de ce réseau :

La plage d'adresse du réseau sera comprise entre la première adresse utilisable et la dernière utilisable, autrement dit, celle qui suit l'adresse du réseau et celle qui précède l'adresse de broadcast :

De
10001100. 10011111. 00000000. 00000001 140.159.0.1
A
10001100. 10011111. 11111111. 11111110 140.159.255.254

Partie 2 : L'adressage IP- Les sous-réseaux (Découpage d'un réseau IP)

Subnetting : On utilise une seule adresse IP pour créer d'autres sous-réseaux.

Pourquoi subnetting ou pourquoi le sous-réseau?

- Ils permettent aux réseaux locaux physiquement à distance d'être reliés.
- Un mélange des architectures de réseau peut être relié, comme l'Ethernet sur un segment et le Token ring sur des autres.
- Ils permettent à un nombre illimité de machines de communiquer en combinant des sous-réseaux, par contre, le nombre de machines sur chaque segment est limité par le type de réseau utilisé.
- La congestion de réseau est réduite comme les diffusions et chaque trafic local de réseau est limité au segment local.

Caractéristique

- Un réseau IP de classe A, B ou C peut être découpé en sous-réseaux.
- Chaque sous-réseau peut être découpé en sous-sous-réseaux et ainsi de suite.
- Il y a de même notion pour le réseau et le sous-réseau.
- Chaque sous-réseau a un seul identifiant réseau unique et il exige un masque de réseau pour les sous-réseaux.

Il est nécessaire de bien déterminer les points suivants avant de faire Subnetting :

- Déterminer le nombre d'identifiant réseau requis pour l'usage courant et également pour l'évolution dans le futur
- Déterminer le nombre maximum des machines de chaque sous-réseau, tenant compte encore de la croissance dans le futur
- Définir un masque de réseau pour le sous-réseau entier
- Déterminer les identifiants sous-réseau qui sont utilisables
- Déterminer les identifiants machines valides et assigner les adresses IP aux postes de travail.

Exemple :

Le réseau de classe C, NetID : 192.168.1.0 avec le masque par défaut 255.255.255.0.

On veut découper ce réseau en 4 sous-réseaux.

Calculer le nombre de sous-réseau :

Si l'on utilise 1 bit -> $2^1 = 2$ sous-réseaux,

Si l'on utilise 2 bits -> $2^2 = 4$ sous-réseaux.



Calcul du masque de sous-réseau

Le masque de chaque sous-réseau est obtenu en rajoutant 2 bits à 1 au masque initial.

Le masque de réseau par défaut est 255.255.255.0 :

Soit 11111111 11111111 11111111 00000000

En ajoutant 2 bits on obtient

11111111 11111111 11111111 11000000

En fin, on a le masque de sous-réseau : **255.255.255.192**

Calcul du NetID de chaque sous-réseau

- Le NetID de chaque sous-réseau sera constitué de 26 bits
- Les 24 premiers bits seront ceux de l'écriture en binaire de 192.168.1.
- Les 2 bits suivants seront constitués du numéro du sous-réseau 00, 01, 10,11

Les adresses des sous-réseaux

-192.168.1.**00**xxxxxx

- 192.168.1.**01**xxxxxx-

- 192.168.1.**10**xxxxxx-

-192.168.1.**11**xxxxxx-

Les 4 identifiants de sous-réseaux sont **192.168.1.0**, **192.168.1.64** et **192.168.1.128**,
192.168.1.192

Calcul des HostID des sous-réseaux

- Adresse IP de Premier sous-réseau :192.168.1.0
192.168.1.**00000000** : Non utilisable- l'adresse IP du premier sous-réseau

192.168.1.0**00000001** = 192.168.1.1

192.168.1.0**00000010** = 192.168.1.2

- . |
- . | 62machines
- . |

192.168.1.0**0111110** = 192.168.1.62

192.168.1.0**0111111** : Non utilisable- Adresse de Diffusion

La plage d'adresse IP du premier sous-réseau est de 192.168.1.1 à 192.168.1.62

- Adresses IP de Deuxième sous-réseau :192.168.1.64

192.168.1.10000000 : Non utilisable $192.168.1.10000001 = 192.168.1.129$

$192.168.1.01000001 = 192.168.1.65$

- . |
- . | 62machines
- . |

$192.168.1.01111110 = 192.168.1.126$

192.168.1.01111111 : Non utilisable- Adresse de diffusion

La plage d'adresse IP du deuxième sous-réseau est de 192.168.1.65 à 192.168.1.126

Adresses de diffusion

Pour obtenir l'adresse de diffusion dans chaque sous-réseau; on met à 1 tous les bits de HostID.

L'adresse de diffusion de premier sous-réseau est **192.168.1.00111111**, soit **192.168.1.63**.

L'adresse de diffusion de deuxième sous-réseau est **192.168.1.01111111**, soit **192.168.1.127**

Nombre de sous-réseaux/ nombre de bits

Le nombre de sous-réseaux dépend du nombre de bits qu'on emprunte à la partie Hôte pour déterminer les nombre de sous-réseaux souhaités.

Nombre de bits	Nombre de sous-réseaux
1	2
2	4
3	8
4	16
5	32
6	64
7	128
8 (impossible pour une classe C)	256

La sécurisation des informations sensibles

Partie A. Les dangers d'Internet

1. Les virus informatiques

Qu'est-ce qu'un virus informatique ?

Un virus informatique est un *programme*[des instructions écrites dans un langage de programmation] qui *effectue certaines actions* et, en général, *cherche à se reproduire*. Il peut aussi avoir comme effet, recherché ou non, de *nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté*. *Les actions effectuées dépendent du virus et sont différentes d'un virus à l'autre* : cela peut aller du simple affichage d'images ou de messages à l'écran à l'effacement complet du disque dur (dans ce cas, on parle de « *bombe logique* » ou de « *charge utile* »), en passant par la suppression de certains fichiers.

Les virus informatiques peuvent *se répandre à travers tout moyen d'échange de données numériques* comme l'Internet, mais aussi les disquettes, les cédéroms,... Son appellation provient d'une analogie avec le virus biologique puisqu'il présente des similitudes dans sa manière de se propager et de se reproduire.

Remarque :

Sachez que le nombre de virus en circulation sur PC s'élève à plusieurs dizaines de milliers. Le danger est donc bien réel et cela n'arrive pas qu'aux autres. Il faut donc *apprendre à bien identifier les risques pour ne pas se faire contaminer ni, par voie de conséquence, contaminer les autres* ; en effet, quand vous êtes victime d'un virus, outre le désagrément de la situation, la plupart du temps vous le transmettez à vos correspondants chaque fois que vous envoyez un e-mail. Raison de plus pour vous protéger !

2. Les vers

Les vers se répandent dans le courrier électronique en profitant des failles des différents logiciels de messagerie (notamment Microsoft Outlook). Dès qu'ils ont infecté un ordinateur, ils s'envoient eux-mêmes dans tout le carnet d'adresses, ce qui fait que l'on reçoit ce virus de personnes connues. Certains d'entre eux ont connu une expansion fulgurante (« *I Love You* »).

3. Les canulars (hoax)

Terme anglais qu'on peut traduire par canular, le hoax peut être défini comme une fausse information ou une rumeur. C'est une forme particulière de spam puisqu'il se base sur le courrier électronique. Il utilise la crédulité des utilisateurs pour se propager. En faisant circuler des informations qui apparaissent à l'utilisateur comme essentielles il compte sur celui-ci pour relayer (forwarder) l'information à tous ses contacts.

En général, le hoax n'est pas réellement dangereux puisqu'il ne met pas en défaut la sécurité des données de l'utilisateur et n'essaie pas de lui extorquer de l'argent.

Cependant, le hoax possède quelques côtés pervers :

- ♦ Il sert la désinformation en faisant circuler de fausses informations ou des rumeurs non fondées et décrédibilise le moyen de diffusion que représente Internet.
- ♦ Il engorge les réseaux et les boîtes aux lettres en se servant des utilisateurs crédules pour être propagé.



4. Les chevaux de Troie

Le terme *cheval de Troie* (en anglais, *trojan horse* ou simplement *trojan*) tire bien entendu son origine d'un célèbre épisode de la mythologie grecque où un cheval en bois contenant des guerriers avait été introduit, grâce à une ruse, dans la ville de Troie assiégée.

Un cheval de Troie est donc un programme qui effectue une tâche spécifique à l'insu de l'utilisateur.

À la différence d'un virus, *un cheval de Troie ne se reproduit pas*, mais de nombreux virus diffusent également un cheval de Troie sur l'ordinateur qu'ils infectent.

Un cheval de Troie peut être exécuté de manière furtive à chaque démarrage de l'ordinateur si un virus a programmé son exécution automatique en ajoutant des clés dans le registre.

Un cheval de Troie peut aussi se cacher dans un logiciel qui lui servira d'hôte.

Exemple

Quand un utilisateur croit exécuter un programme de jeu de dames qu'il a téléchargé sur Internet, il va également lancer un petit logiciel furtif qui va enregistrer toutes les touches qu'il saisit au clavier et, par conséquent, dévoiler tous ses mots de passe, son numéro de carte bancaire s'il réalise des achats sur Internet, etc. C'est ensuite un jeu d'enfant pour le cheval de Troie de stocker toutes ces informations dans un fichier qui sera ensuite transmis par protocole FTP, dès l'activation de la connexion Internet, sur un serveur situé dans un pays où la législation n'est pas trop regardante...