INSTITUT PRIVÉ

ipSMART

Introduction aux Réseaux Informatiques

Classe : L2 DGL & IG

Année 2023 -2024

Par M. Bakary KAMISSOKO

PLAN DU COURS

Introduction aux Réseaux Informatiques

A. **Concepts fondamentaux** : modèles (OSI et TCP/IP), médias et composants

B. **Notion d'adressage IPv4 :** classes, sous-réseaux, VLSM, CIDR

C. **Introduction au routage :** statique et dynamique

CONCEPTS FONDAMENTAUX

INTRODUCTION

OSI

TCP/IP

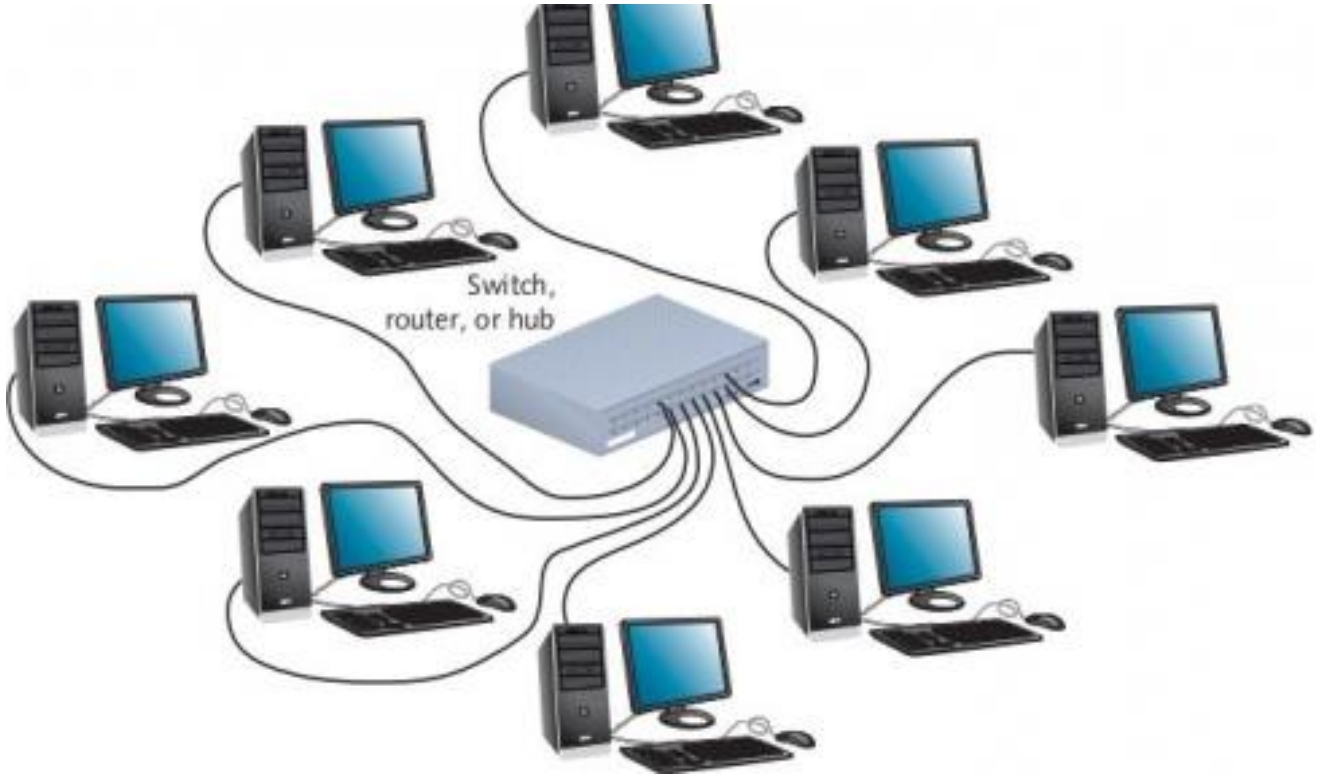
MEDIAS ET COMPOSANTS

OBJECTIF ET CONTENU

Objectifs :
Comprendre l'organisation et le fonctionnement d'un réseau informatique.

Contenu :
Étude de la topologie réseau

Qu’est ce qu’un réseau ?



Définition

- Réseau informatique : Ensemble d’ordinateurs et de périphériques connectés les uns aux autres à travers de supports de transmission.

- Un réseau informatique vise à fournir les moyens matériels et logiciels pour faire communiquer et permettre l’échange d’informations entre plusieurs équipements informatiques de manière souple et fiable.

Qu’est ce qu’un réseau ?

Définition

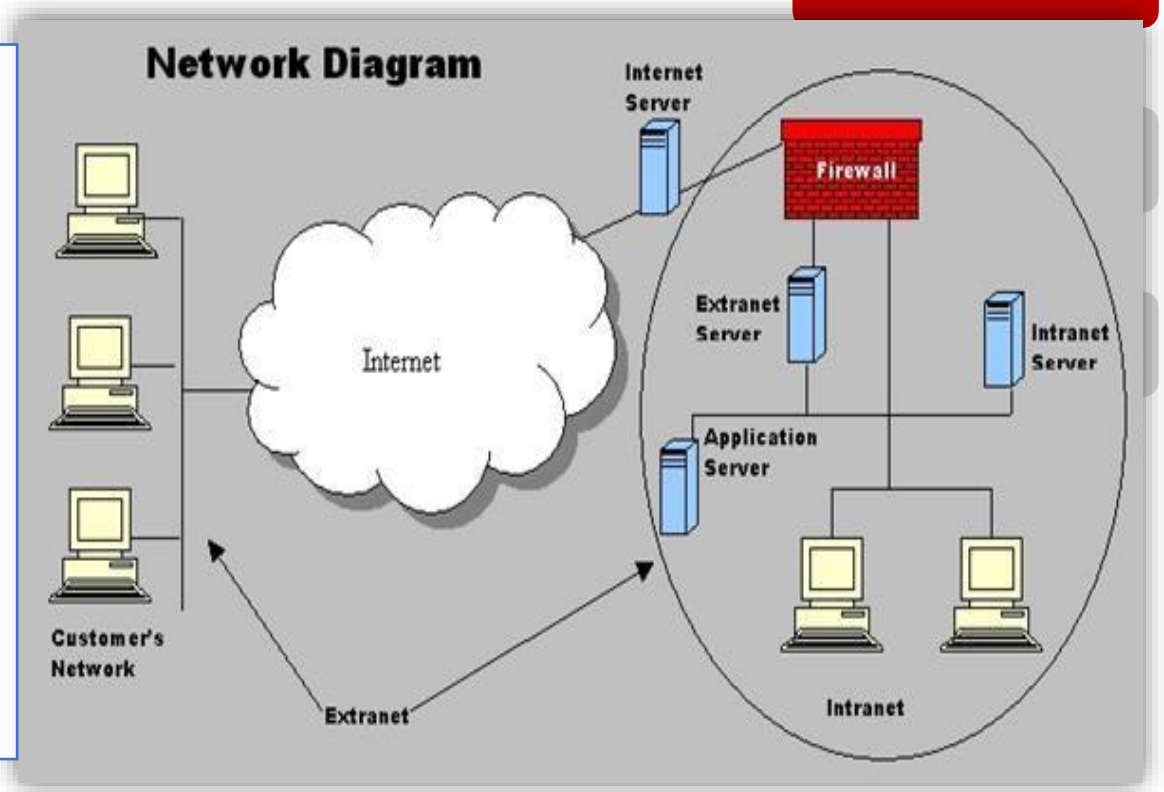
Réseau c’est un ensemble d'équipements (nœuds), reliés entre eux, grâce à divers moyens

matériels et logiciels (protocoles) pour échanger des données

CONCEPTS FONDAMENTAUX

Échelle:

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

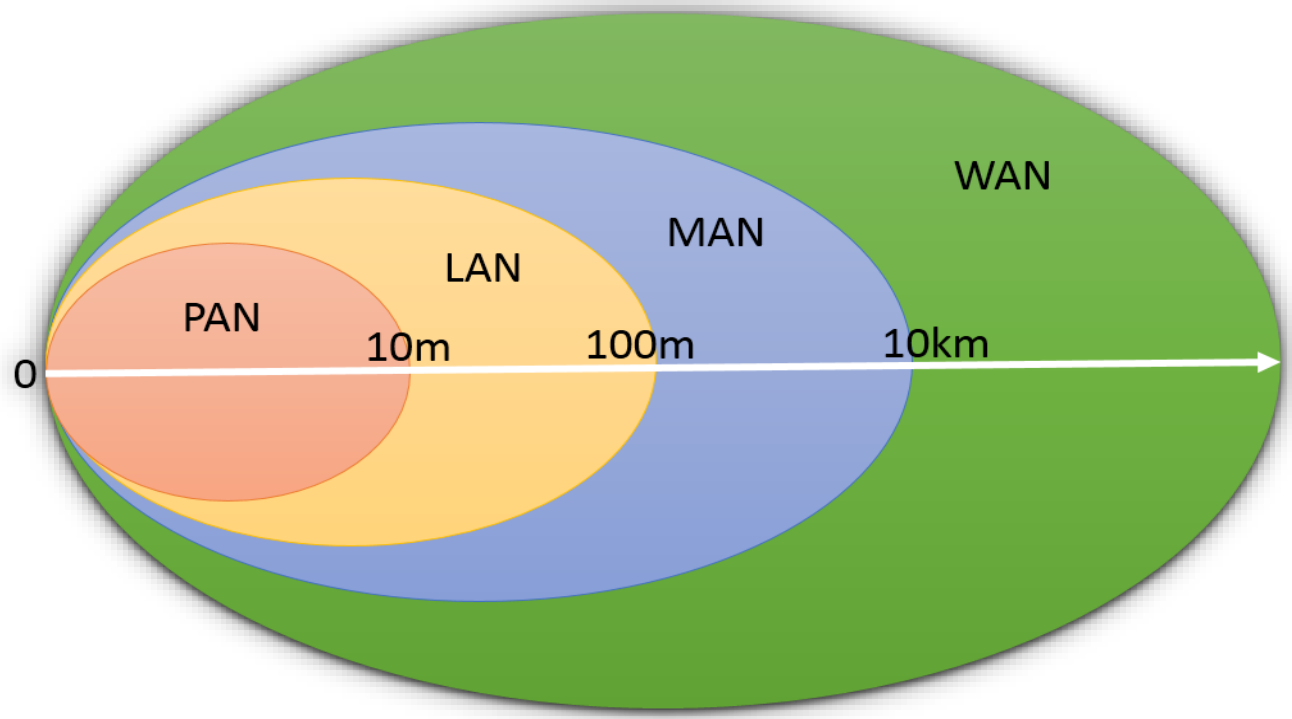


CONCEPTS FONDAMENTAUX

Classification par étendue

- Types de réseaux

  PAN, LAN, MAN, WAN



CONCEPTS FONDAMENTAUX

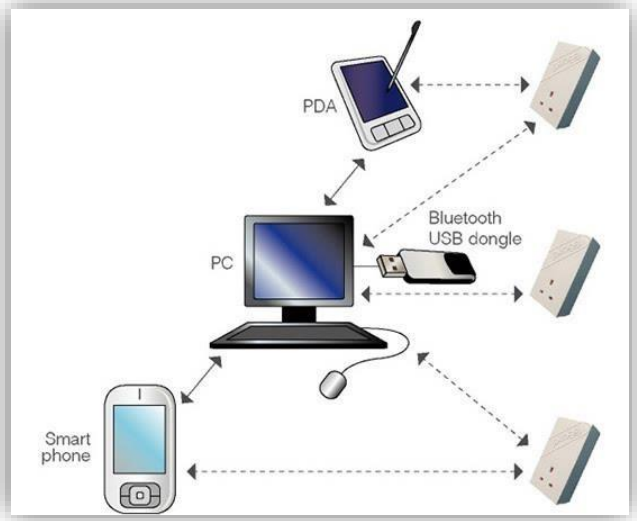
- **PAN:** Personal Area Network
  Caractéristiques:

  - réseaux de très petite dimension généralement sur 10 m ou moins;

  - pour une seule personne, ou un très petit nombre de personne;

  - un très petit nombre d'éléments (laptop+ smartphone+ appareil photo connecté);

  - via des technologies sans-fil (Wireless PAN) Wireless USB , Bluetooth,

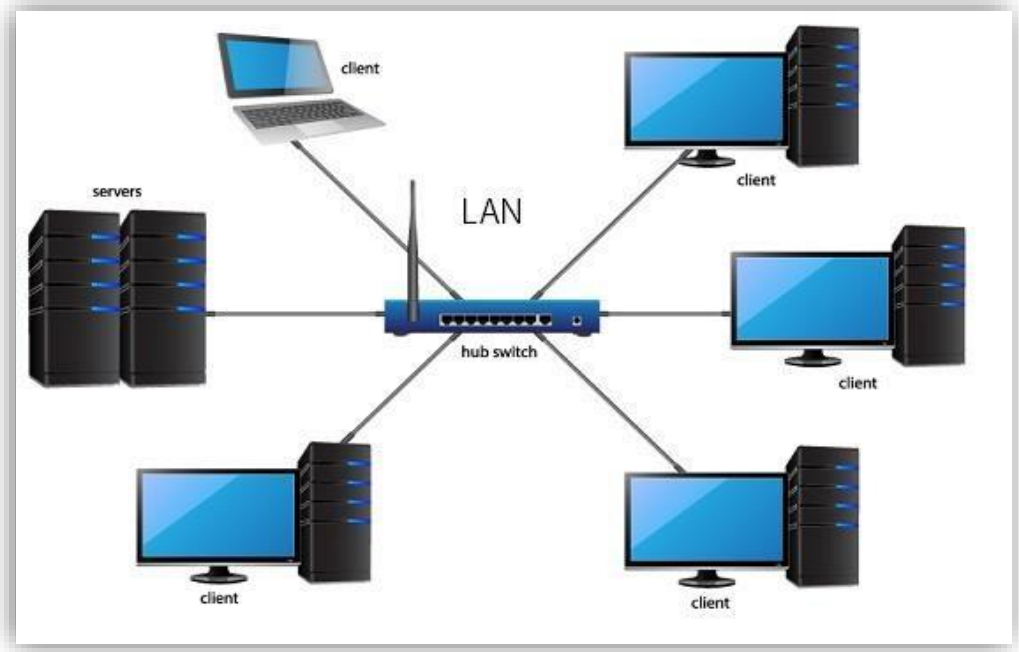


CONCEPTS FONDAMENTAUX

- **LAN:** Local Area Network

Caractéristiques:

- à l'échelle d'un bâtiment ou d'une entreprise ;
- généralement quelques centaines d'utilisateur
- distance entre 10m et 1km
- de 10Mb/s (Ethernet) à 1Gb/s (Gigabit Ethenet), voir 10Gb/s



CONCEPTS FONDAMENTAUX

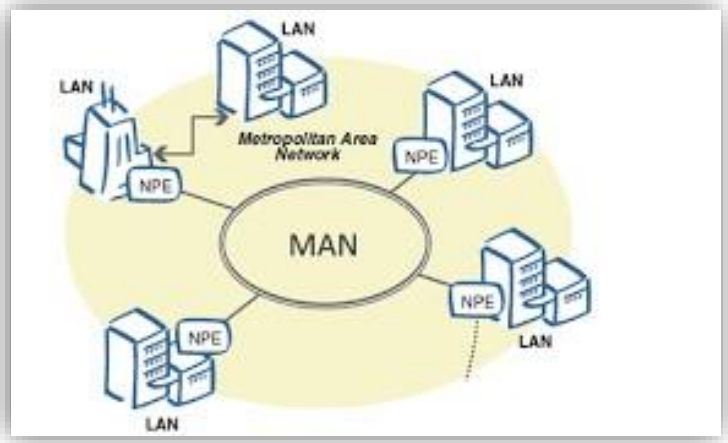
INTRODUCTION

- **MAN:** Metropolitan Area Network

  Caractéristiques:

  - à l'échelle d'un campus ou d'une ville (privé ou public) ;
  - généralement par fibre optique, par des médias identiques aux LAN , paire téléphonique ,

    WiFi étendu, Wimax
  - distance entre 5 et 50 kms voir jusqu'à 200 Kms;

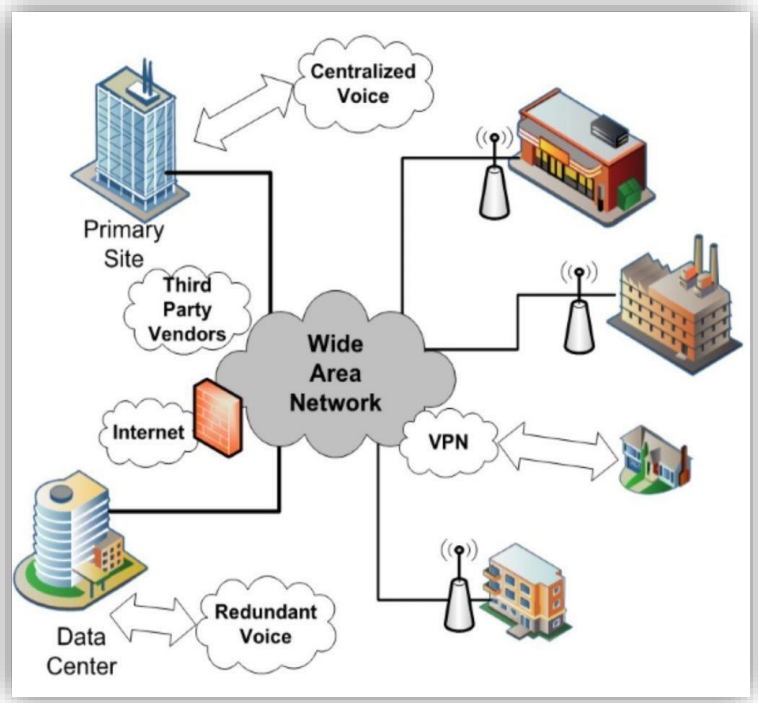


CONCEPTS FONDAMENTAUX

- **WAN**: Wide Area Network

Caractéristiques:

- très grande zone géographique (pays, continent, voir planète);
- Le plus grand et connu étant bien sûr Internet;
- Assure l'interconnexion entre LANs ou MANs
- type de connexions hétérogène, en fonction du prix et de la distance , jusqu'à 2Tb/s sur FO;
- diverses topologie,



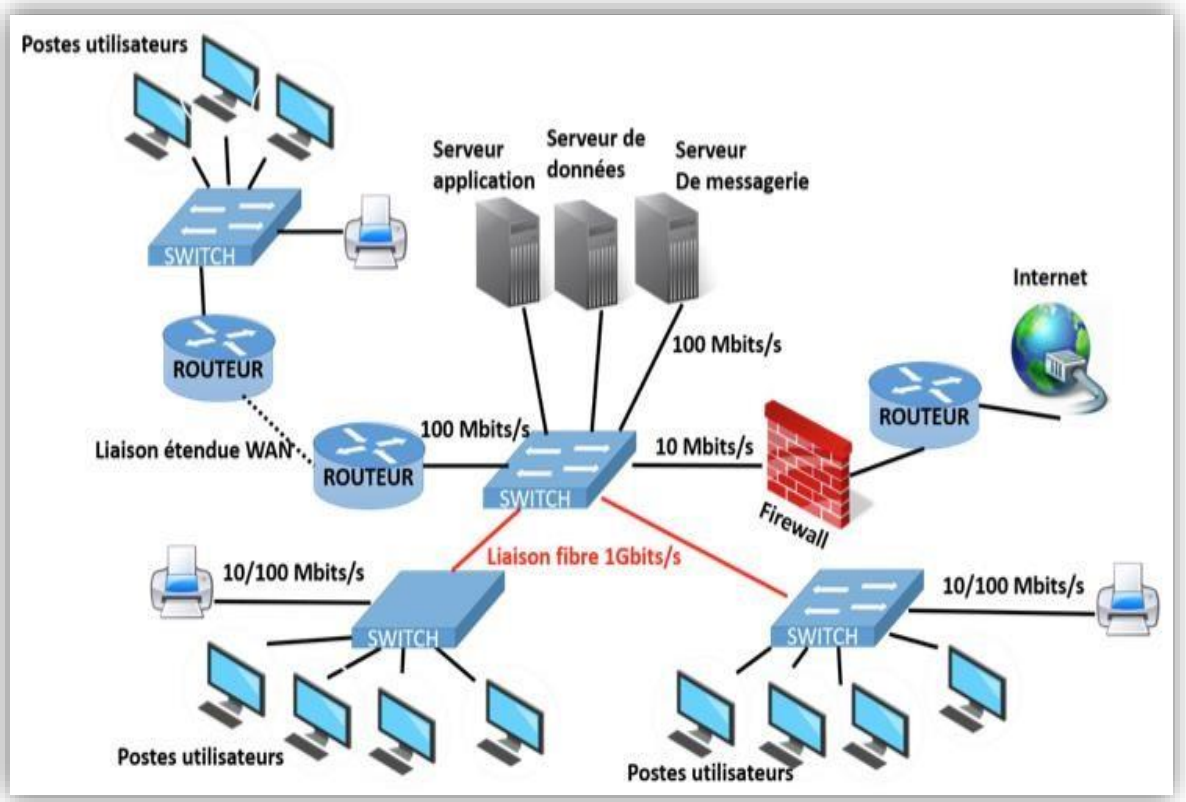
CONCEPTS FONDAMENTAUX

INTRODUCTION

Classification par topologie

Définie l'architecture d'un réseau

- relation entre composants
- via un ou plusieurs médias
- connections
- hiérarchie



CONCEPTS FONDAMENTAUX

Classification par topologie

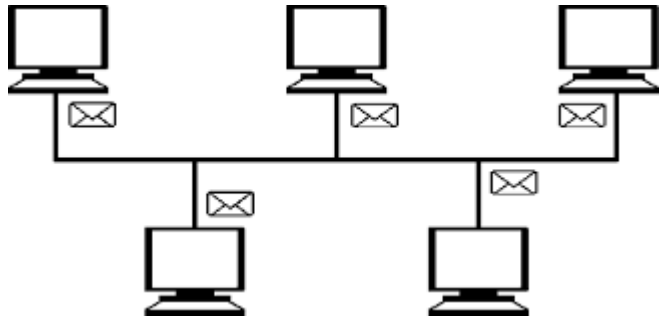
Réseaux en bus :

- ❖ câblage unique:

- ❖ inconvénients:

- panne totale en cas de dysfonctionnement du support
- bande passante partagée
- taux de collision élevé
- liaison passive par dérivation (électrique ou optique)
- uni ou bi-directionnel
- terminé à chaque extrémité par des (bouchons)

❖avantages: Simple, économique



CONCEPTS FONDAMENTAUX

Classification par topologie

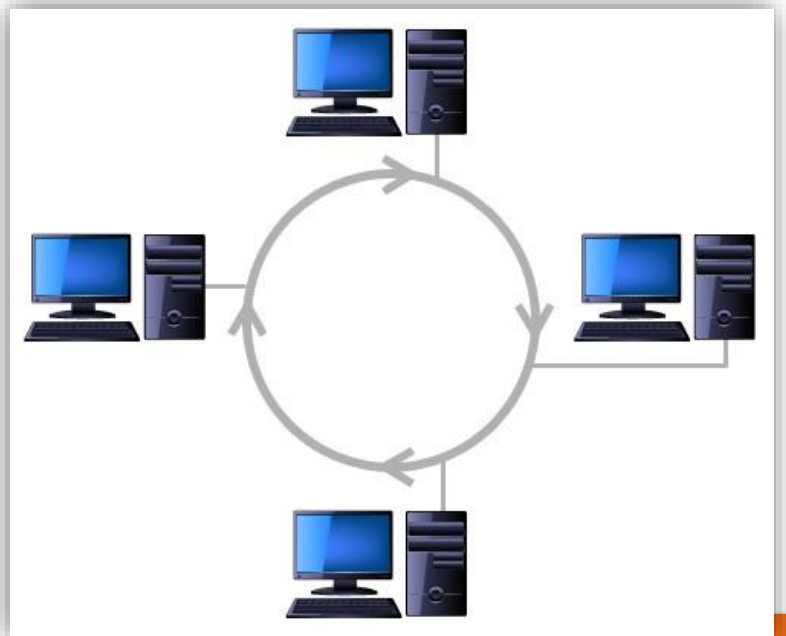
- Réseaux en anneaux (Token Ring, FDDI):
  - ❖ Chaque station joue le rôle de station intermédiaire :
- sur un connexion unique (circulaire) , souvent composé de deux anneaux à sens opposés;
- le plus souvent grâce à un répartiteur sur lequel sont connectés tout les éléments
  - ❖ avantages:

isolation de chaque nœud (bande passante dédié)

  - ❖ inconvénients:

Coût

une défaillance d'un élément entraîne une panne de tout le système taux de collision élevé



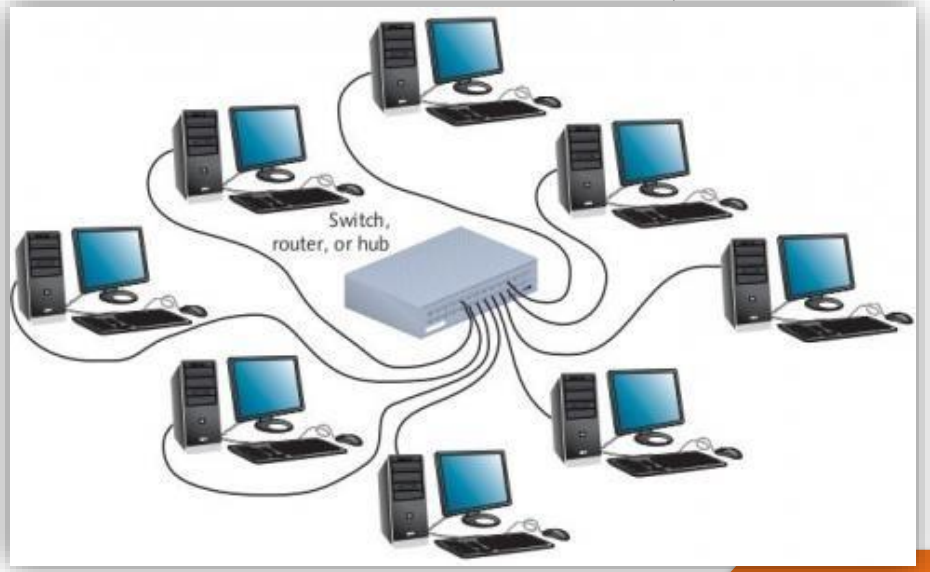
CONCEPTS FONDAMENTAUX

Classification par topologie

- Réseaux en étoile:
  - ❖ nœuds connectés grâce à un équipement d'interconnexion :
- concentrateur (hub) ou commutateur (switch) ;
  - ❖ avantages:

pas de défaillance générale en cas de dysfonctionnement d'une liaison (meilleur débit)

❖inconvénients: coût d'évolution élevé



CONCEPTS FONDAMENTAUX

Classification des réseaux

SYNTHESE

- Distinction selon un critère organisationnel :

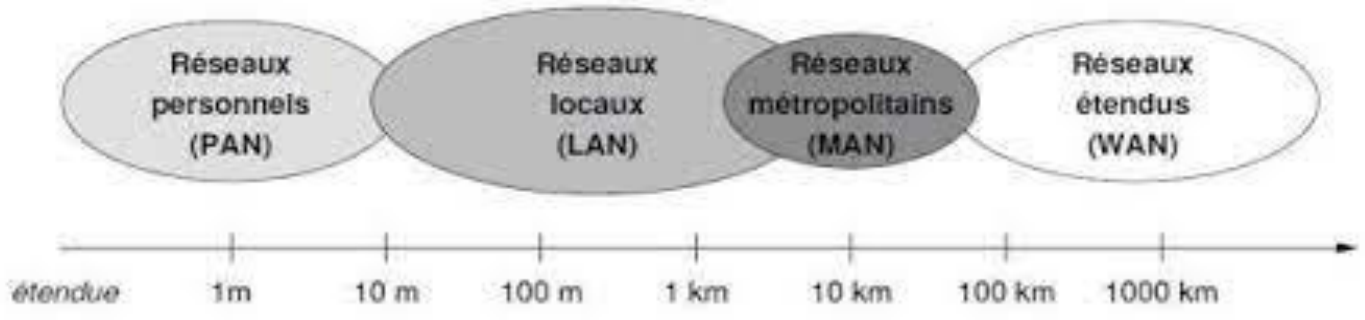
  Réseaux privés

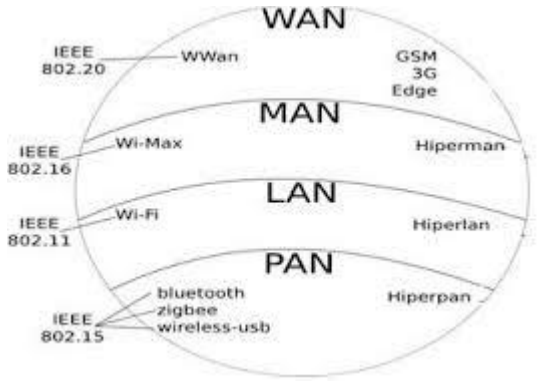
  Réseaux publics

  Réseaux virtuels (VPN)

- Distinction selon la capacité à transmettre des données

  Réseaux haut débit, réseaux multimédia





Modèle OSI et TCP/IP

INTRODUCTION

OSI

TCP/IP

MEDIAS ET COMPOSANTS

OBJECTIF ET CONTENU

Objectifs :
Comprendre l'organisation et le fonctionnement d'un réseau informatique.

Contenu :
Étude d'architectures de réseaux, incluant les modèles OSI (Open Systems Interconnection) et la pile TCP/IP (Transmission Control Protocol / Internet Protocol)

Modèle OSI et TCP/IP

INTRDOUCTION
OSI
TCP/IP
MEDIAS ET COMPOSANTS

INTRODUCTION

Aujourd'hui, dans le monde réseau, il existe deux modèles largement dominants : le modèle OSI qui définit 7 couches et le modèle TCP/IP (modèle Internet) qui définit 4 couches.

Le modèle OSI est un modèle de réseau idéalisé (modèle conceptuel), tandis que le modèle TCP/IP est une implémentation pratique.

Modèle OSI et TCP/IP

INTRODUCTION
OSI
TCP/IP
MEDIAS ET COMPOSANTS
conclusion

Le modèle théorique OSI et ses 7 couches

Le modèle OSI (Open Systems Interconnection ou Interconnexion de Systèmes Ouverts en Français) est un modèle conceptuel (théorique) dont le but est de définir des normes de communication entre différents systèmes informatiques. Il est normé en 1984.

Ce modèle propose un système de communication composé de **7 couches différentes**. L'idée derrière cette représentation est une nouvelle fois de décomposer la communication entre deux périphériques en différentes « étapes » bien définies afin qu'on puisse par la suite faire évoluer les composants de chacune des couches de manière indépendante plutôt que de devoir modifier l'intégralité du processus de communication dès le changement d'un composant.

Modèle OSI et TCP/IP

Le modèle théorique OSI et ses 7 couches

Le modèle OSI ne donne qu'une définition générale de chaque couche (on parle de couche d'abstraction) sans spécifier les services ni les protocoles utilisés par chacune d'entre elles.

C'est aux concepteurs des protocoles de les créer de façon à ce qu'ils respectent les règles et limites d'une couche en particulier.

Modèle OSI et TCP/IP

Les 7 couches définies par le modèle OSI sont les suivantes :

N° de la couche	Nom de la couche	Unité de données
7	Application	Données non transformées
6	Présentation	Données non transformées
5	Session	Données non transformées
4	Transport	Segments
3	Réseau	Paquets
2	Liaison des données	Trames
1	Physique	Bits

Modèle OSI et TCP/IP

INTRODUCTION
OSI
TCP/IP
CONCLUSION

La couche application

La couche application est la couche la plus proche de l'utilisateur. La majorité des protocoles utilisés par les utilisateurs se situent dans cette couche (HTTP, SMTP, FTP, etc.).

Cette couche interagit avec les applications logicielles qui implémentent des composants de communication. La couche application est le point d'accès aux services réseaux.

La couche application a généralement pour fonction d'identifier les interlocuteurs, de déterminer si les ressources sont disponibles et de synchroniser les communications.

La couche d'application en elle-même n'a aucun moyen de déterminer la disponibilité des ressources sur le réseau.

Modèle OSI et TCP/IP

La couche application

Pour la couche application, on peut notamment utiliser les protocoles suivants (en se limitant au monde IP) :

- Les protocoles FTP (IETF), NFS (Sun Microsystems) et AFS, SMB/CIFS (Microsoft) pour le transfert de fichiers ;
- Les protocoles Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), Internet Message Access Protocol (IMAP) pour les services de messagerie ;
- Les protocoles Telnet, rlogin, Secure Shell (SSH) pour les sessions distantes ;
- Le protocole HTTP pour le transfert de ressources hypermédia comme les documents HTML ;
- Des protocoles d'exploitation et de gestion comme Domain Name System (DNS) pour la résolution d'adresse, (SNMP) Simple Network Management Protocol pour la supervision.

Modèle OSI et TCP/IP

La couche présentation

La couche présentation est chargée du formatage des données de la couche applicative afin qu'elles puissent être envoyées à travers le réseau puis être lues à nouveau par les applications.

La couche session

La couche session contrôle les connexions entre les ordinateurs. Cette couche permet l'ouverture et la fermeture de session et gère la synchronisation des échanges ainsi que les transactions

Modèle OSI et TCP/IP

La couche transport

La couche transport fournit les moyens concrets pour transférer des données de taille variable d'une source vers une destination en conservant la qualité du service.

L'enjeu de la couche de transport est de réceptionner les données qui viennent des couches supérieures, de les découper et de la faire transiter jusqu'à la couche réseau.

Cette couche est la première à communiquer directement avec la machine de destination : elle gère les communications de bout en bout ("end to end") entre processus (programmes en cours d'exécution).

La couche réseau

La couche réseau fournit les moyens concrets pour transférer des données de taille variable (appelés "paquets") entre différents réseaux de nœuds.
On va notamment effectuer le routage et l'adressage des paquets dans cette couche, c'est-à-dire qu'on va définir la route que vont emprunter les paquets pour aller d'un point de départ à un point d'arrivée (d'un interlocuteur à l'autre).

Modèle OSI et TCP/IP

La couche liaison de données

La couche liaison des données gère les communications entre deux machines directement connectées entre elles.

On va dans cette couche découper des données brutes en trames de tailles variables puis les envoyer de manière séquentielle.

On va également dans cette couche détecter et pouvoir corriger les erreurs pouvant survenir dans la couche physique, définir le protocole pour établir et mettre fin à une connexion entre deux périphériques connectés physiquement et définir le protocole de contrôle de flux (régulation du trafic) entre eux.

La couche physique

La couche physique est chargée de la transmission des signaux entre les interlocuteurs. Son service est limité à l'émission et la réception d'un bit ou d'un train de bits continu.
La couche physique est, comme son nom l'indique, la couche dans laquelle sont définis les protocoles du monde physique (les différents câbles de transmission).

Modèle OSI et TCP/IP

Le modèle pratique TCP/IP et ses 4 couches

Le modèle TCP/IP (encore appelé « modèle Internet »), qui date de 1976, a été stabilisé bien avant la publication du modèle OSI en 1984.

Pour information, TCP/IP est un modèle dérivé de l'ARPANET dont le but était de maintenir les communications coûte que coûte en cas d'attaque nucléaire. Il en découle un réseau basé sur le routage de paquets à travers une couche appelée Internet.

Le modèle TCP/IP est une approche réaliste ou pratique d'un modèle réseau. En conséquence, c'est le modèle TCP/IP qui est utilisé comme modèle de réseau de référence pour Internet.

INTRODUCTION
OSI
TCP/IP
CONCLUSION

Modèle OSI et TCP/IP

Le modèle pratique TCP/IP et ses 4 couches

Le modèle TCP/IP tient son nom de ses deux protocoles « majeurs » : les protocoles TCP (Transmission Control Protocol) et IP (Internet Protocol).
Il présente aussi une approche modulaire (utilisation de couches) mais en contient uniquement quatre :

- **La couche application ;**
- **La couche transport ;**
- **Internet ;**
- **Accès réseau.**

N° de la couche	TCP/IP	Unité de données
4	Application	Données non transformées
3	Transport	Segments
2	Internet	Paquets
1	Accès réseau	Bits

INTRODUCTION
OSI
TCP/IP
CONCLUSION

Modèle OSI et TCP/IP

La couche application

Le modèle TCP/IP regroupe les trois couches de session, présentation et application du modèle OSI dans une seule couche application. En effet, d'un point de vue pratique, cela ne fait souvent pas beaucoup de sens de séparer ces couches.

Cette couche contient tous les protocoles de haut niveau : FTP pour le transfert de fichiers, SMTP pour les mails, HTTP pour le WWW, DNS pour les noms de domaine.

Modèle OSI et TCP/IP

La couche transport

La couche transport assure la communication logique entre processus. Cette couche détermine comment les données doivent être envoyées : de manière fiable ou pas.

Concrètement, on va pouvoir choisir entre deux protocoles dans la couche transport : TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

TCP est un protocole de transfert fiable orienté connexion. Ce protocole contrôle et s'assure qu'il n'y ait ni perte ni corruption de données. Il est donc en charge des erreurs. TCP est le protocole le plus utilisé sur le Web aujourd'hui.

UDP est un protocole de transfert non fiable et qui ne nécessite pas de connexion préalable. Ce protocole est particulièrement utilisé pour les échanges où la perte de quelques données n'est pas grave (appel vidéo, jeu en ligne, etc.) car il est plus rapide que TCP.

Modèle OSI et TCP/IP

La couche internet

Le but principal de la couche Internet est d'assurer la communication logique entre hôte, c'est-à-dire de transmettre coûte que coûte les paquets d'un hôte à un autre et de faire en sorte qu'ils arrivent à destination.

Le protocole principal de cette couche est IP (Internet Protocol ou Protocole Internet). Les paquets peuvent prendre différentes routes pour arriver à destination et arriver dans un ordre différent de l'ordre dans lequel ils ont été envoyés.

Modèle OSI et TCP/IP

La couche internet

Dans son fonctionnement, la couche Internet n'est pas responsable d'une transmission fiable.

Elle ne fournit qu'un service peu fiable et une livraison optimale (via le routage et l'adressage). Étant donné que la livraison de paquets entre divers réseaux est une opération intrinsèquement peu fiable et sujette aux pannes, la charge de la fiabilité a été placée avec les points d'extrémité d'un chemin de communication, c'est-à-dire les hôtes, plutôt que sur le réseau.

Ce sera aux protocoles de plus haut niveau d'assurer la fiabilité du service.

Modèle OSI et TCP/IP

La couche accès réseau

La couche accès réseau du modèle TCP/IP regroupe les couches physique et de liaison des données du modèle OSI. Cette couche définit comment envoyer des paquets IP à travers le réseau (via des protocoles comme Ethernet ou Wireless entre autres

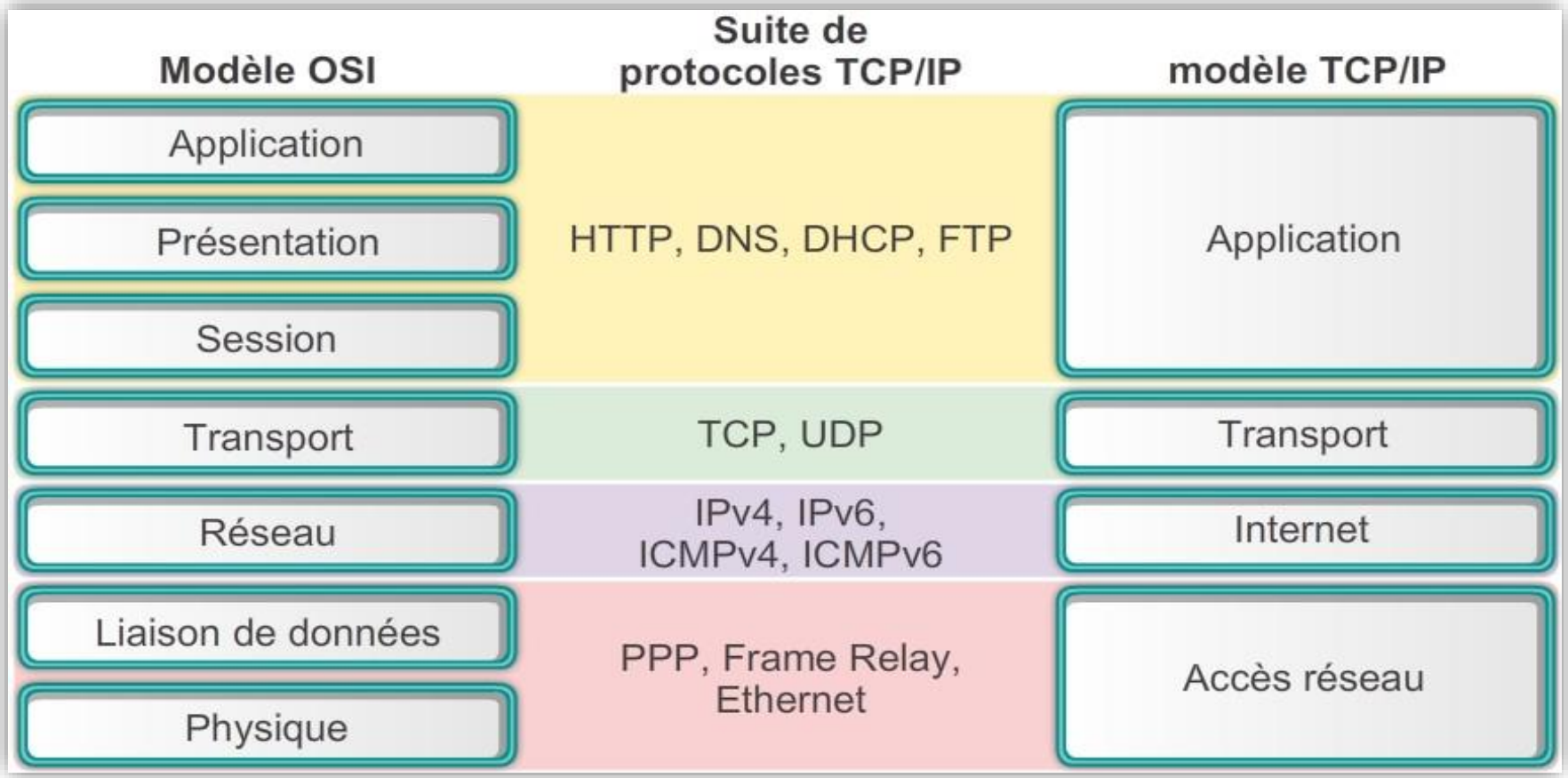
Modèle OSI et TCP/IP

La couche internet

Quels sont les éléments qui constituent un réseau de communication numérique ?

a. Une infrastructure pour l'échange d'information.
b. Les hôtes connectés à cette infrastructure.
c. Les services et applications qui communiquent.
d. Les 3 réponses ci-dessus.
e. Aucune de ces réponses.

Modèle OSI et TCP/IP



INTRODUCTION

OSI

TCP/IP

CONCLUSION

Médias et composants

COMPSANTS

MEDIA

Répéteur:

- ❑Combinaison de récepteur et d'émetteur
  - permettant de retransmettre les signaux reçus
  - permet d'augmenter la distance entre deux nœuds
- ❑Fonctionnement binaire
  - aucune interprétation du signal reçu
- couche 1 (physique) du modèle OSI

Un **répéteur** (en anglais *repeater*) est un équipement simple permettant de regénérer un signal entre deux noeuds du réseau, afin d'étendre la distance de câblage d'un réseau.

Médias et composants

COMPSANTS

MEDIA

Concentrateur (Hub):

- ❑amplifie et multiplie le signal vers plusieurs PCs
  - forme de répéteur / multiprise
- ❑Traitement binaire
  - redistribution du signal sur tout les ports
  - couche 1 du modèle OSI (physique)

Un **concentrateur** est un élément matériel permettant de concentrer le traffic réseau provenant de plusieurs hôtes, et de régénérer le signal.

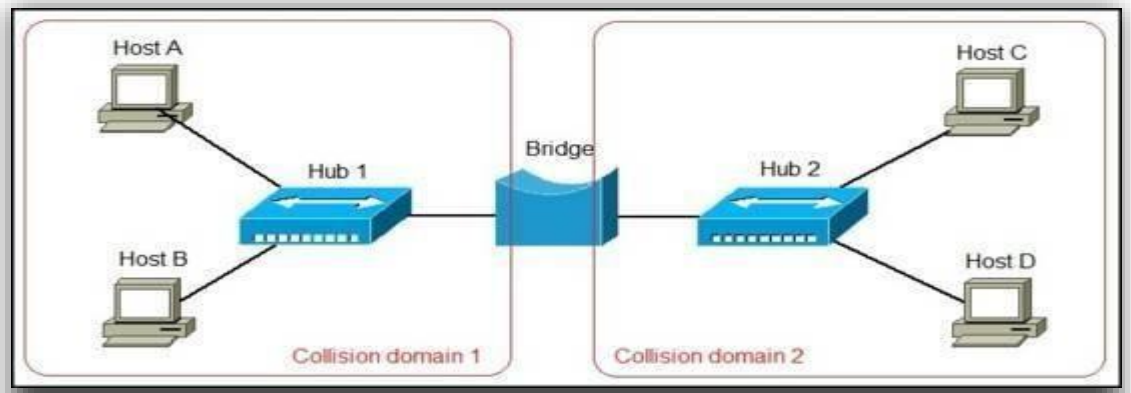
Médias et composants

COMPSANTS

MEDIA

Pont (bridge)

Un **pont** est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Ainsi, contrairement au répéteur, qui travaille au niveau physique, le pont travaille également au niveau logique (au niveau de la couche 2 du modèle OSI), c'est-à-dire qu'il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont.

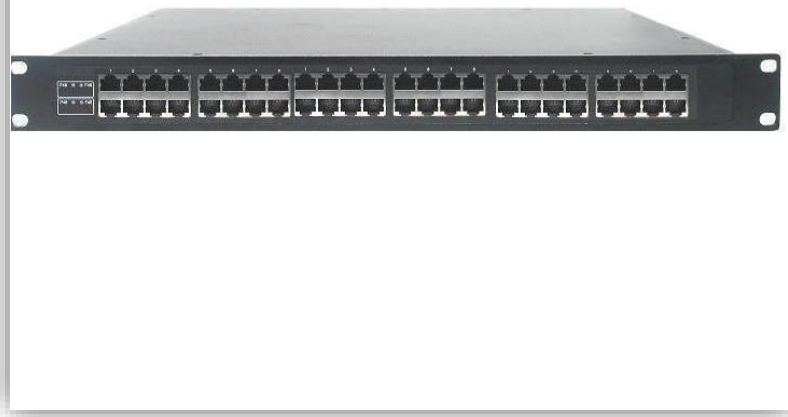


Média et composants

Un **commutateur** (en anglais *switch*) est un pont multiports, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI.

Le commutateur analyse les trames arrivant sur ses ports d'entrée et filtre les données afin de les aiguiller uniquement sur les ports adéquats (on parle de **commutation** ou de **réseaux commutés**). Si bien que le commutateur permet d'allier les propriétés du pont en matière de filtrage et du concentrateur en matière de connectivité.

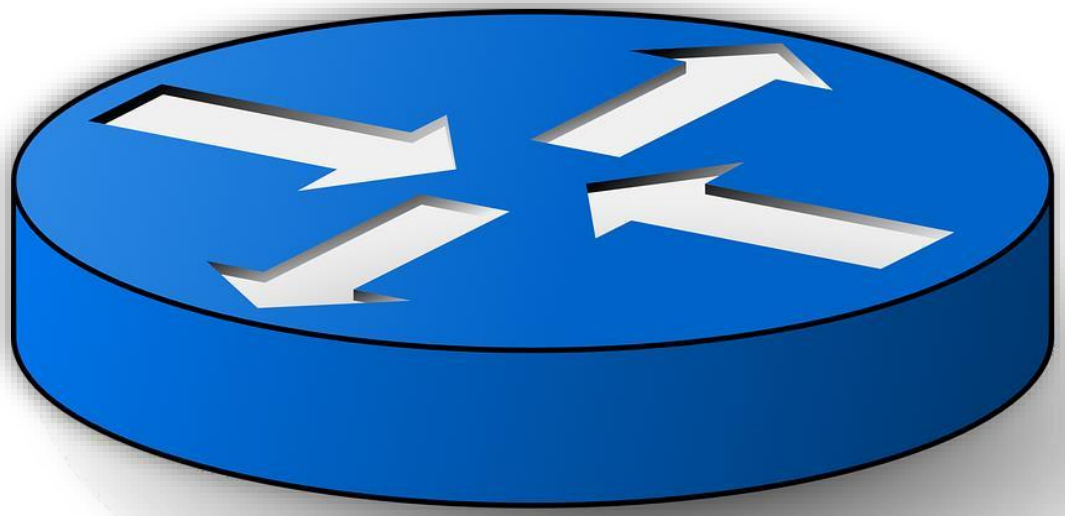
Voici la représentation d'un switch dans un schéma de principe



Médias et composants

Routeur

- niveau 3 (réseau) du modèle OSI
- fait transiter des paquets d'une interface à une autre
- permet d'interconnecter plusieurs réseaux
- le plus souvent via le protocole IP (adresse)
- plans d'adressage différents
- détermine le chemin emprunté par un paquet



Médias et composants

Les équipements d'interconnexion

Les principaux équipements matériels mis en place dans les réseaux locaux sont :

- Les répéteurs, permettant de régénérer un signal
- Les concentrateurs (hubs), permettant de connecter entre eux plusieurs hôtes
- Les ponts (bridges), permettant de relier des réseaux locaux de même type
- Les commutateurs (switches) permettant de relier divers éléments tout en segmentant le réseau
- Les passerelles (gateways), permettant de relier des réseaux locaux de types différents
- Les routeurs, permettant de relier de nombreux réseaux locaux de telles façon à permettre la circulation de données d'un réseau à un autre de la façon optimale
- Les B-routeurs, associant les fonctionnalités d'un routeur et d'un pont

COMPSANTS

MEDIAS

Médias et composants

COMPSANTS

MEDIAS

- **Médias:**

1- Câbles électriques:

- ligne de transmission éléments conducteurs métalliques, permettant d'acheminer un signal d'un émetteur vers un récepteur.

2 – Perturbations:

- les perturbations sont d'origine électromagnétiques
- ajoute une tension au signal à transmettre (le transforme) exemple signal audio: friture
- Dans le cadre d'un signal numérique, changement d'état de certains bits , fausse totalement le message

Médias et composants

Coaxiaux:

- un seul conducteur (simple ou multi-brin , cuivre).
- isolé de son blindage par un matériaux diélectrique
- débit important sur de longues distances à faible coût
- fragile, instable et vulnérable aux interférences et aux écoutes

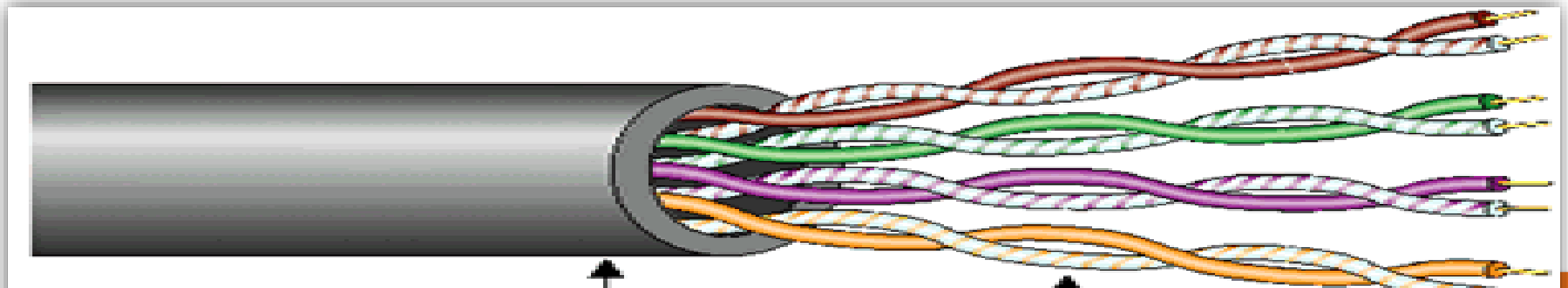
Médias et composants

COMPSANTS

MEDIAS

Paires torsadées:

- enroulement en hélice de chaque paire de fils conducteur (diminue la diaphonie)
- Chaque paire étant caractérisé par un nombre moyen de torsade par mettre augmenter le nombre de torsades permettant de diminuer les risques de diaphonie
- Un câble réseau pouvant être composé de plusieurs paires torsadées, il est important de varier leurs nombre moyen de torsades par mettre pour éviter toute diaphonie entre les paires



Médias et composants

Fibre optique:

COMPSANTS

MEDIAS

- très haut débit grâce à des rayons optiques conduits par le "cœur" du câble , entouré
  d'une gaine et d'une protection
- uni-directionnel
- insensible aux champs électromagnétiques
- types

  - monomode: 1Gb/s / km - multimode: 100Gb/s/ km
- Avantages: 1- Légèreté 2- Immunité au bruit 3- Faible atténuation Très haut débit
  4- Très haut débit 5-Quasi impossibilité d'écoute
- Inconvénients : 1- installation complexe 2- coût élevé

Médias et composants

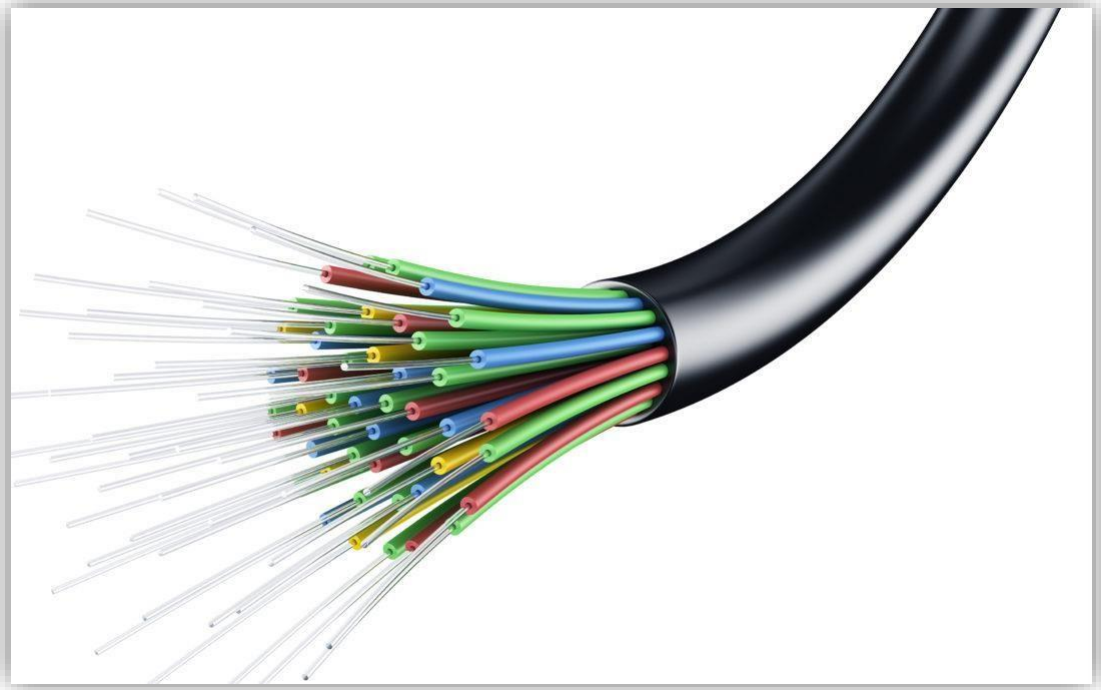
- principalement utilisé pour

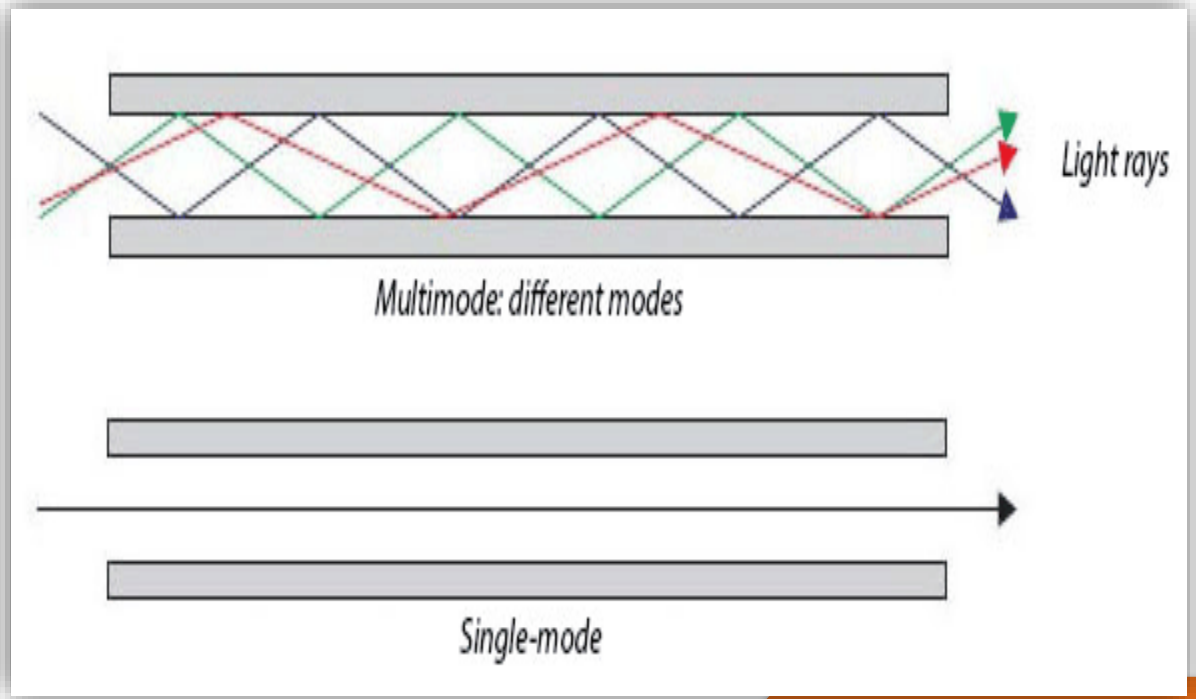
1- des connections entre répartiteurs 2- des connections très haut débit

- ne convient pas aux LAN

COMPSANTS

MEDIAS





Notion d’adressage

OBJECTIF ET CONTENU

En suivant cette activité, vous serez capable :

- de décrire le rôle d'une adresse IP dans le fonctionnement d'Internet,
- d'expliquer le principe d'adressage hiérarchique,
- de comprendre la structure d'une adresse

Notion d’adressage

INTRODUCTION

INTRODUCTION

OSI

TCP/IP

Adresse IP est un numéro d'identification de chaque appareil connecté à un réseau utilisant le protocole Internet.

ce matricule sert à identifier les machines et à leur permettre de dialoguer entre elles, en échangeant des données sur Internet.

Quel est le rôle de l'adresse IP ?

Si vous utilisez un smartphone, un ordinateur ou tout autre dispositif relié à Internet, sachez que ce dernier possède ce que l'on appelle une **adresse IP**. Sorte de carte d'identité, cette suite de chiffres permet d'identifier les appareils numériques, mais aide aussi à l'acheminement des paquets de données

Notion d’adressage

Lors d’une communication entre deux postes, le flux de données provenant de la couche transport — niveau 4 du modèle OSI — (par exemple des segments TCP) est encapsulé dans des paquets par le protocole IP lors de leur passage au niveau de la couche réseau. Ces paquets sont ensuite transmis à la couche liaison de données — niveau 2 du modèle OSI — afin d’y être encapsulés dans des trames (par exemple Ethernet).

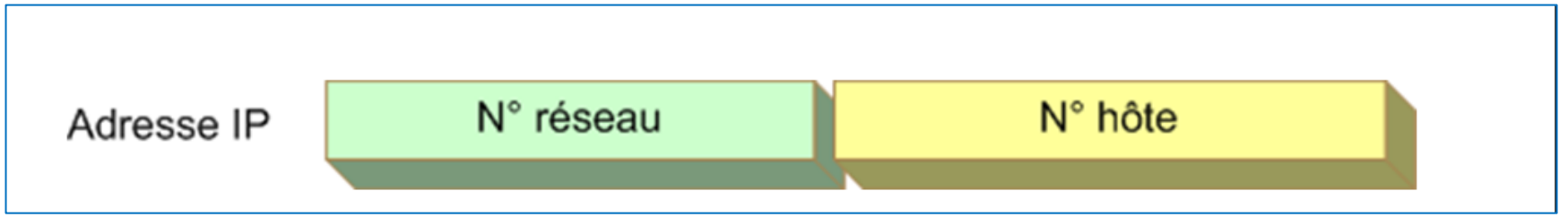
Les données traversant Internet sont divisées en morceaux plus petits, appelés paquets. Des informations IP sont attachées à chaque paquet, et ces informations aident les routeurs à envoyer des paquets au bon endroit. Chaque appareil ou domaine qui se connecte à Internet se voit attribuer une adresse IP et, comme les paquets sont dirigés vers l’adresse IP qui leur est attachée, les données arrivent là où elles sont nécessaires.

Constitution d'une adresse IP V4

- constituée de 4 octets (32 bits)
  Ex : 192 . 168 . 2 . 45

- séparée entre deux parties

  - le numéro de réseau
  - le numéro d'hôte



Les différents types d'adresses IPv4

Dans la plage d'adresses de chaque réseau IPv4, il y a trois types d'adresse :

- **L'adresse réseau** : l'adresse qui fait référence au réseau
- **L'adresse de diffusion** :une adresse spécifique, utilisée pour envoyer les données à tous les hôtes du réseau
- **Des adresses d'hôte** : des adresses attribuées aux périphériques finaux sur le réseau

Types d'adresse

Adresse réseau

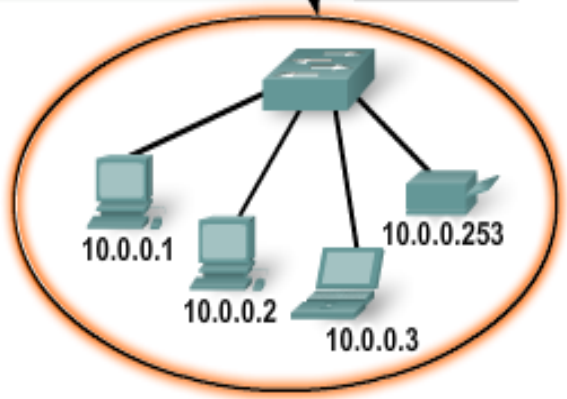
Adresse de diffusion

Adresse d'hôte

	Réseau		Hôte
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001

Placez le pointeur sur un élément pour en savoir plus.

10.0.0.0 fait référence au réseau dans son ensemble. Tous les périphériques de ce réseau partagent les mêmes bits d'adresse réseau.



Types d'adresse

Adresse réseau

Adresse de diffusion

Adresse d'hôte

Réseau			Hôte
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001

Placez le pointeur sur un élément pour en savoir plus.

L'adresse de diffusion sert à envoyer des paquets à chaque hôte du réseau partageant la même partie réseau de l'adresse.

Types d'adresse

Adresse réseau

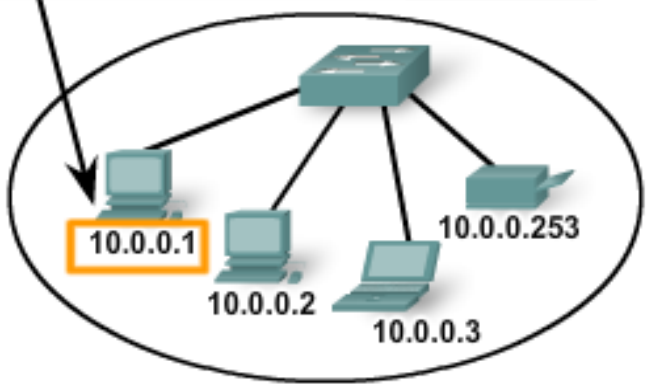
Adresse de diffusion

Adresse d'hôte

	Réseau		Hôte
10	0	0	0
00001010	00000000	00000000	00000000
10	0	0	255
00001010	00000000	00000000	11111111
10	0	0	1
00001010	00000000	00000000	00000001

Placez le pointeur sur un élément pour en savoir plus.

Chaque hôte de ce réseau a une adresse unique.



Préfixes réseau:

Comment savoir combien de bits représentent la partie réseau et combien représentent la partie hôte ?

Pour cela nous ajoutons une longueur de préfixe à l'adresse réseau. La longueur de préfixe correspond au nombre de bits de l'adresse qui représentent la partie réseau.

Par exemple, dans 172.16.4.0 /24, /24 est la longueur de préfixe. Elle nous indique que les 24 premiers bits correspondent à l'adresse réseau. Il reste donc 8 bits qui correspondent à la partie hôte.

Réseau	Adresse réseau Bits de tous les hôtes (Rouge) = 0	Plage d'hôtes Représente toutes les combinaisons de bits d'hôtes à l'exception de celles composées uniquement de 0 ou de 1	Adresse de diffusion Bits de tous les hôtes (Rouge) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
Représentation binaire 24 bits réseau	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011	10101100.00010000.00000100.11111111
		10101100.00010000.00000100.11111110	
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

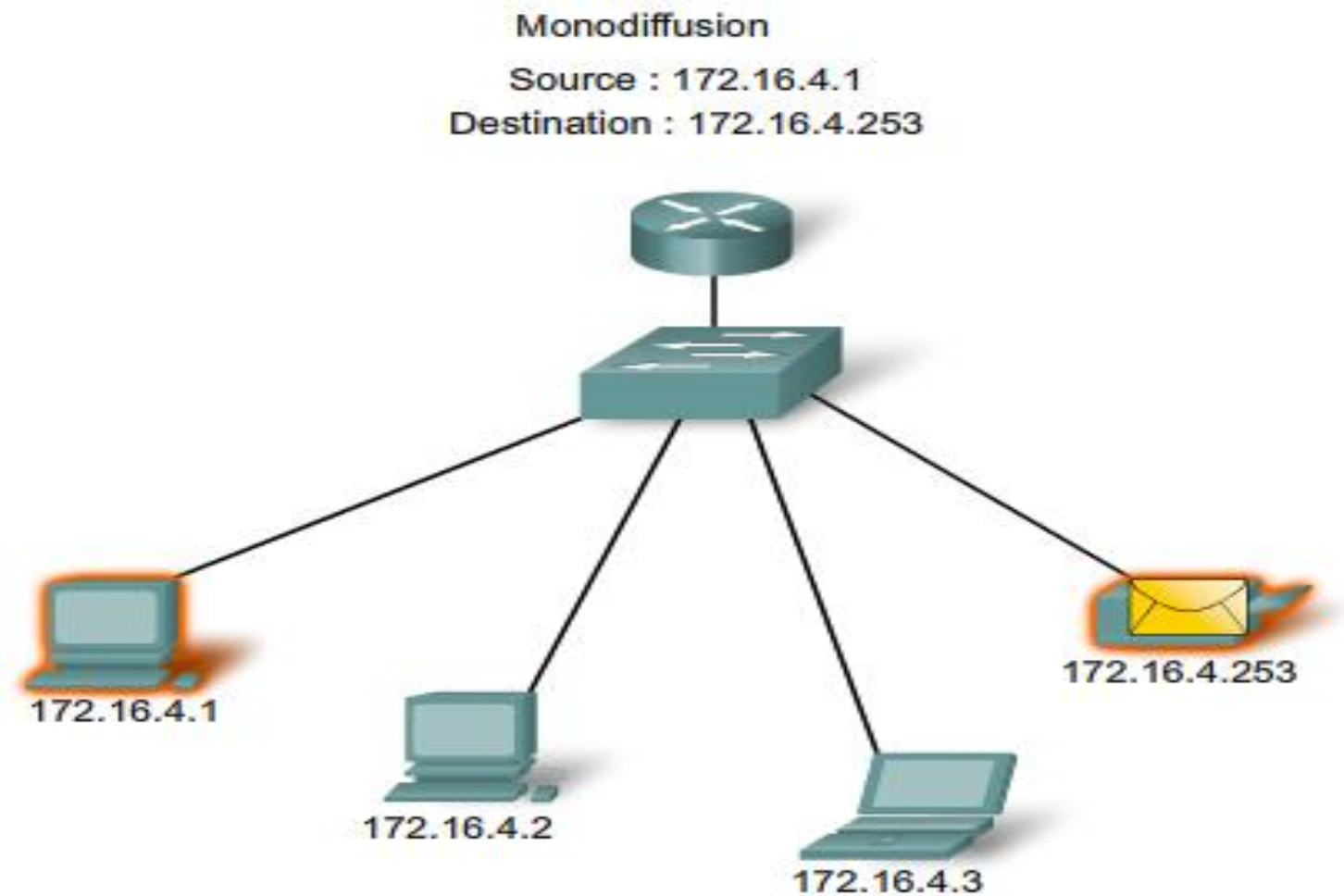
Réseau	Adresse réseau Bits de tous les hôtes (Rouge) = 0	Plage d'hôtes Représente toutes les combinaisons de bits d'hôtes à l'exception de celles composées uniquement de 0 ou de 1	Adresse de diffusion Bits de tous les hôtes (Rouge) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
Représentation binaire 25 bits réseau	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011	10101100.00010000.00000100.01111111
		10101100.00010000.00000100.01111110	
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

Réseau	Adresse réseau Bits de tous les hôtes (Rouge) = 0	Plage d'hôtes Représente toutes les combinaisons de bits d'hôtes à l'exception de celles composées uniquement de 0 ou de 1	Adresse de diffusion Bits de tous les hôtes (Rouge) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
Représentation binaire 26 bits réseau	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.00111110	10101100.00010000.00000100.00111111
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31

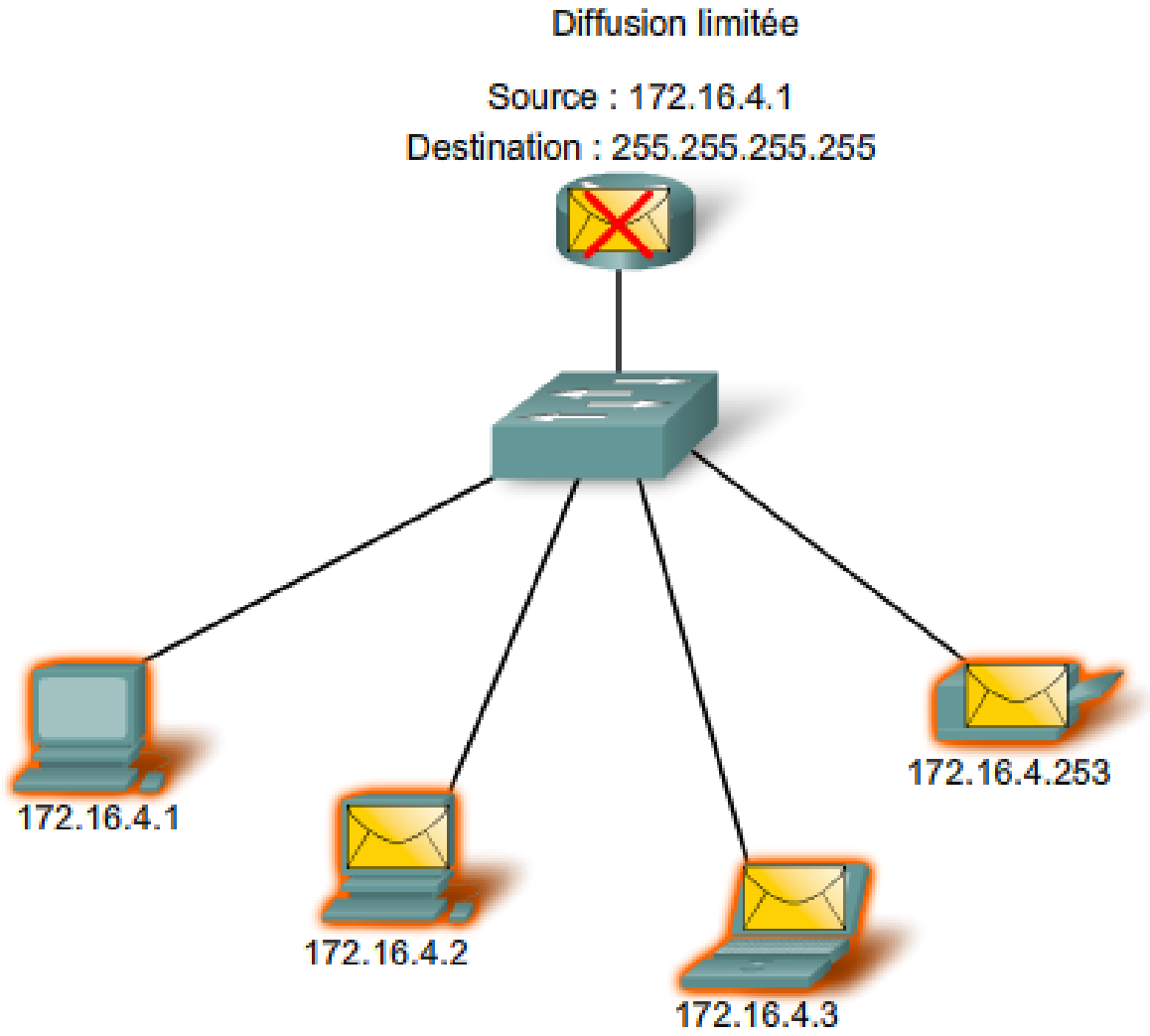
Réseau	Adresse réseau Bits de tous les hôtes (Rouge) = 0	Plage d'hôtes Représente toutes les combinaisons de bits d'hôtes à l'exception de celles composées uniquement de 0 ou de 1	Adresse de diffusion Bits de tous les hôtes (Rouge) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31
Représentation binaire 27 bits réseau	10101100.00010000.00000100.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011	10101100.00010000.00000100.00011111
		10101100.00010000.00000100.00011110	

Dans un réseau IPv4, les hôtes peuvent communiquer de trois façons :

Monodiffusion : processus consistant à envoyer un paquet d'un hôte à un autre.

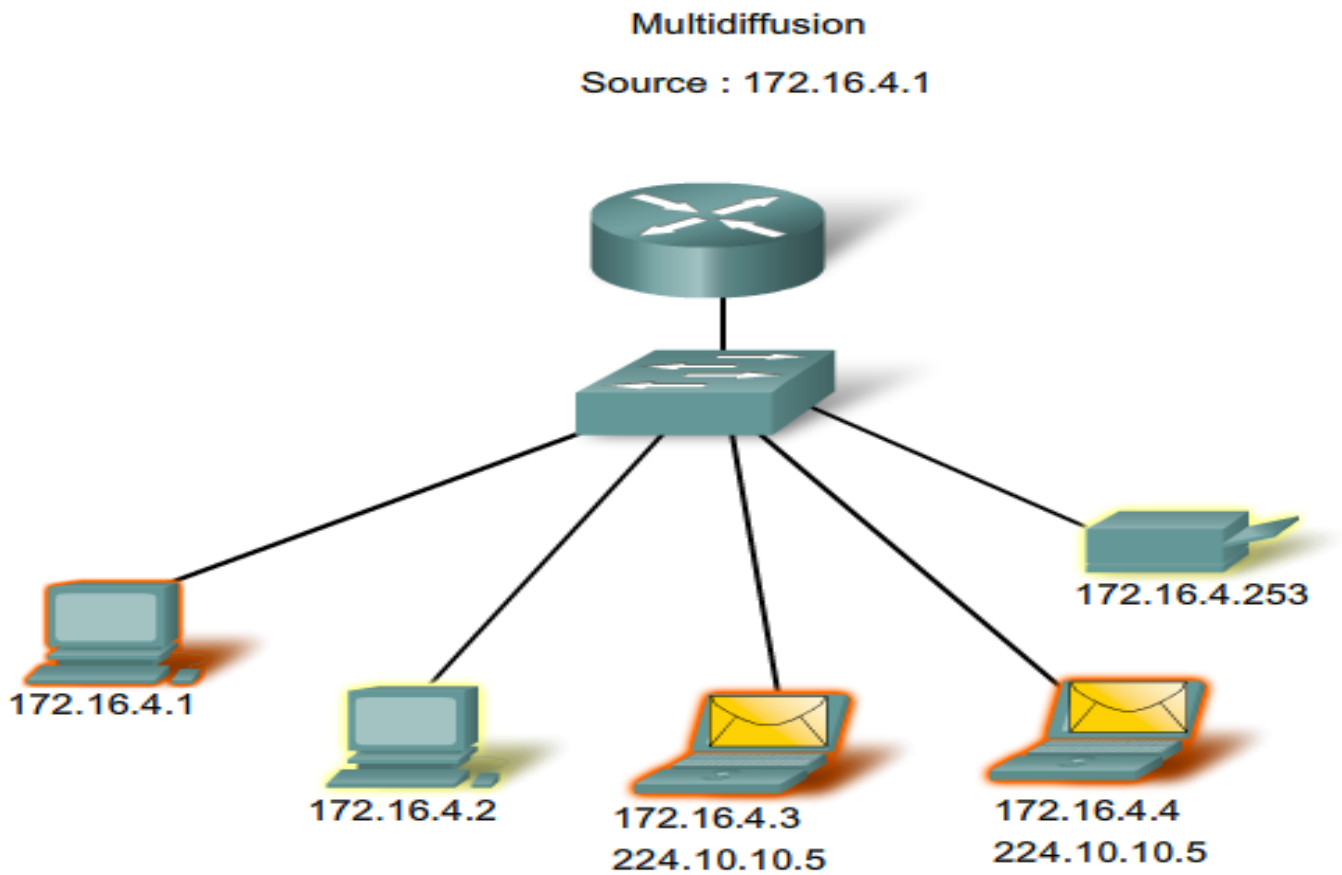


Diffusion : processus consistant à envoyer un paquet d'un hôte à tous les hôtes du réseau.



Multidiffusion : processus consistant à envoyer un paquet d'un hôte à un groupe d'hôtes en particulier.

IPv4 a réservé la plage d'adresses 224.0.0.0 - 239.255.255.255 à l'adressage des groupes de multidiffusion.



Adresses expérimentales

il s'agit de la plage d'adresses IPv4, allant de **240.0.0.0 à 255.255.255.254**. ces adresses sont répertoriées comme étant réservées .

Adresses de multidiffusion

Un autre bloc d'adresses est réservé à un usage spécifique : il s'agit de la plage d'adresses de multidiffusion IPv4, allant de **224.0.0.0 à 239.255.255.255**.

Adresses d'hôte

les hôtes IPv4 peuvent utiliser les adresses allant de **0.0.0.0 à 223.255.255.255** .

Adresses privées

de 10.0.0.0 à 10.255.255.255 (10.0.0.0 /8),
de 172.16.0.0 à 172.31.255.255 (172.16.0.0 /12),
de 192.168.0.0 à 192.168.255.255 (192.168.0.0 /16).

En règle générale, les hôtes qui ne nécessitent pas d'accès à Internet peuvent utiliser les adresses privées sans limitation.
De nombreux hôtes, sur différents réseaux, peuvent utiliser les adresses d'un même espace privé.

Grâce à des services qui traduisent les adresses privées en adresses publiques :NAT (Network Address Translation), les hôtes d'un réseau privé peuvent accéder aux ressources présentes sur Internet.

Adresses publiques

Ces adresses sont normalement attribuées à des hôtes publiquement accessibles depuis Internet.

Faire l'exercice 6.2.5

Adresses IPV4 spéciales

certaines adresses ne peuvent pas être attribuées à des hôtes.

Adresses réseau et de diffusion

Dans chaque réseau, la première et la dernière adresse ne peuvent pas être attribuées à des hôtes. Il s'agit respectivement de l'adresse réseau et de l'adresse de diffusion.

Route par défaut

0.0.0.0. : La route par défaut est utilisée comme route « dernier recours » lorsqu'aucune route plus spécifique n'est disponible. L'utilisation de cette adresse réserve également toutes les adresses de la plage **0.0.0.0 - 0.255.255.255** (0.0.0.0 /8).

Bouclage

L'adresse de bouclage IPv4 **127.0.0.1** est une autre adresse réservée. Il s'agit d'une adresse spéciale que les hôtes utilisent pour diriger le trafic vers eux-mêmes ; ex : envoyer une requête ping à l'adresse de bouclage afin de tester la configuration TCP/IP de l'hôte local.

Bien que seule l'adresse 127.0.0.1 soit utilisée, les adresses de la plage **127.0.0.0-127.255.255.255** sont réservées

Adresses locales-liens

Les adresses IPv4 de la plage **169.254.0.0 - 169.254.255.255** (169.254.0.0 /16) sont désignées en tant qu'adresses locales-liens. Elles peuvent être automatiquement attribuées à l'hôte local par le système d'exploitation, dans les environnements où aucune configuration IP n'est disponible.

Classes d’adresses IP

Classe d'adresse	Plage du premier octet (décimale)	Bits du premier octet (les bits verts ne changent pas)	Parties réseau(N) et hôte (H) de l'adresse	Masque de sous-réseau par défaut (décimal et binaire)	Nombre de réseaux et d'hôtes possibles par réseau
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 réseaux (2^7) 16 777 214 hôtes par réseau (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16 384 réseaux (2^14) 65 534 hôtes par réseau (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2 097 150 réseaux (2^21) 254 hôtes par réseau (2^8-2)
D	224-239	11100000-11101111	S.O. (multidiffusion)		
E	240-255	11110000-11111111	S.O. (expérimental)		

** Les adresses d'hôtes contenant uniquement des zéros (0) et des uns (1) ne sont pas valides.

Limites de l’adressage par classe

L’attribution par classe des adresses IP gaspillait souvent de nombreuses adresses, ce qui épuisait la disponibilité des adresses IPv4.

Par exemple, une entreprise avec un réseau de 260 hôtes devait se voir attribuer une adresse de classe B avec plus de 65 000 adresses.

Adressage réseau

Il doit être correctement préparé et documenté aux fins suivantes :

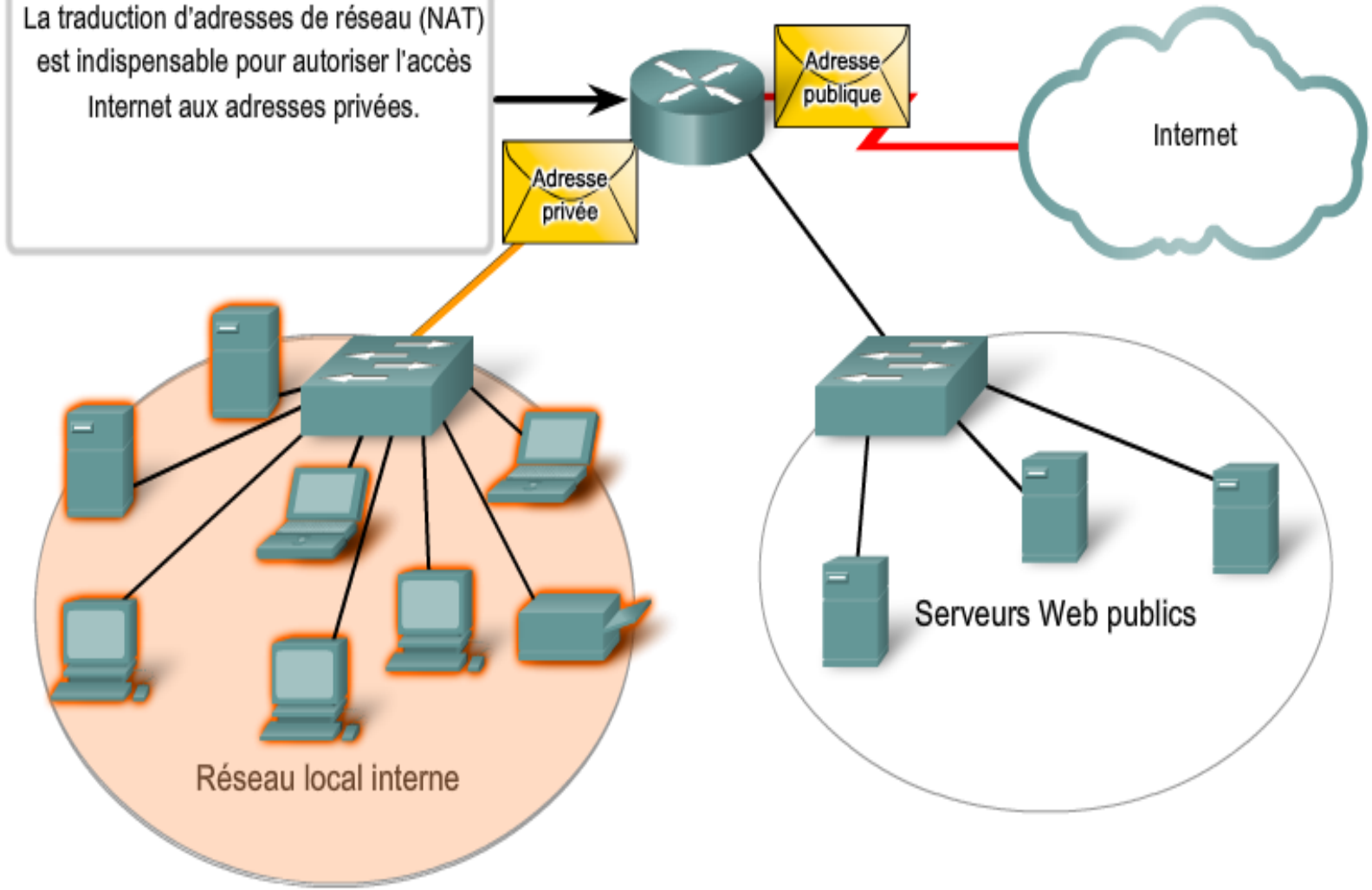
- Éviter les doublons d'adresse
- Fournir et contrôler l'accès
- Surveiller la sécurité et les performances

Dans la préparation d'un schéma d'adressage IPv4, il faut avant tout décider quand les adresses privées doivent être utilisées et où elles seront appliquées.

Planification et affectation d'adresses IPv4

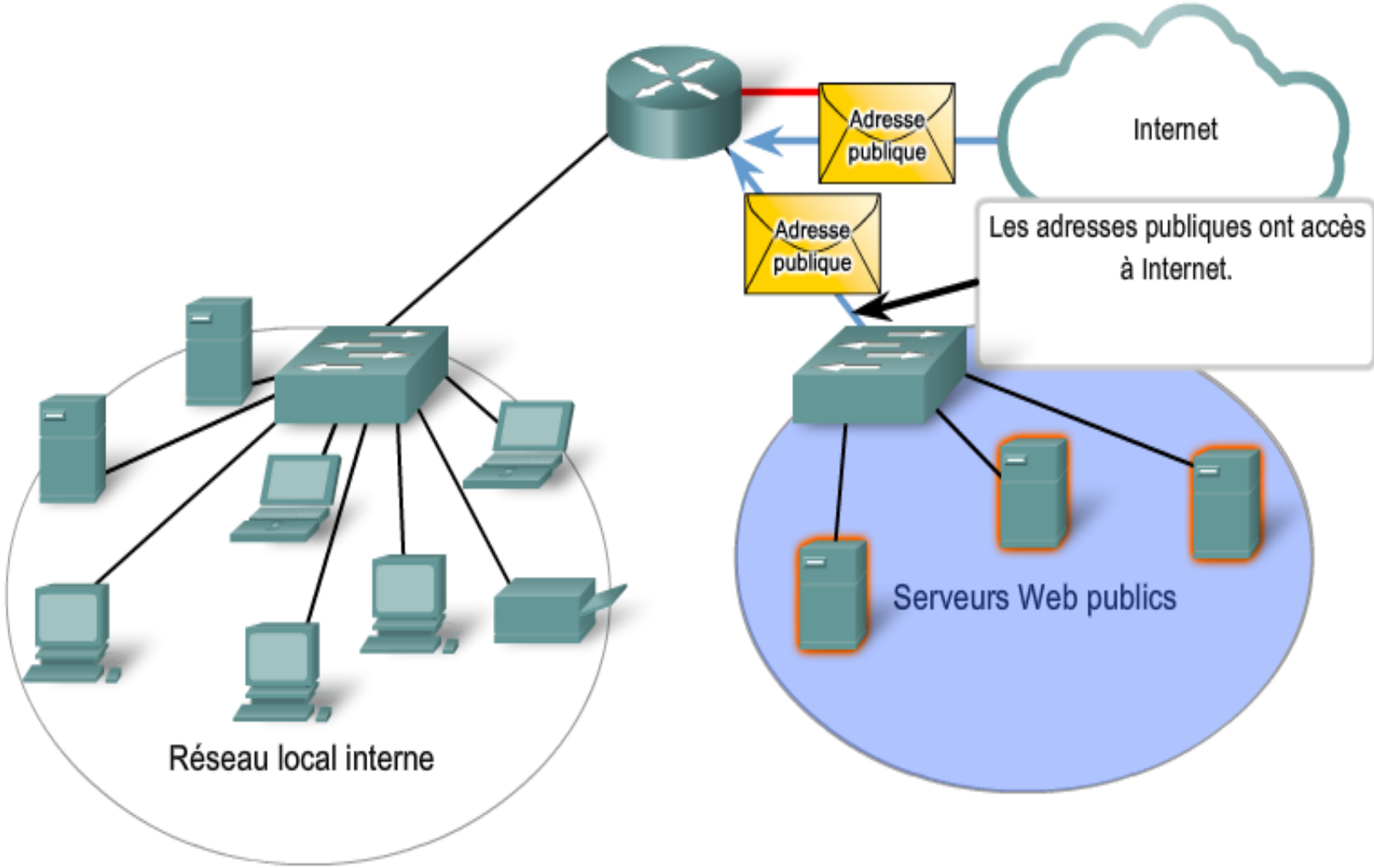
Adresses publiques et privées

La traduction d'adresses de réseau (NAT) est indispensable pour autoriser l'accès Internet aux adresses privées.



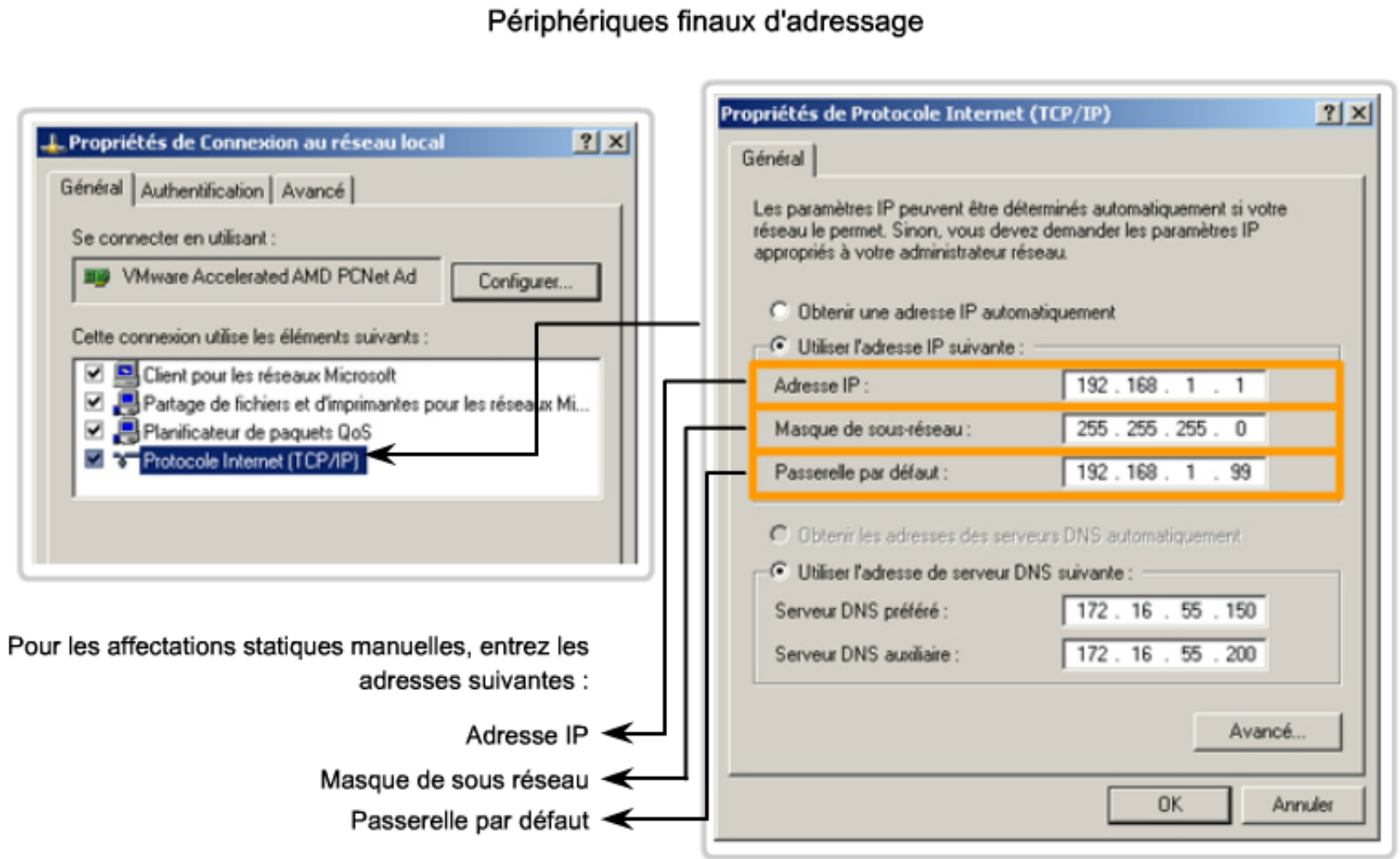
Planification et affectation d'adresses IPv4

Adresses publiques et privées



Attribution statique d’adresses

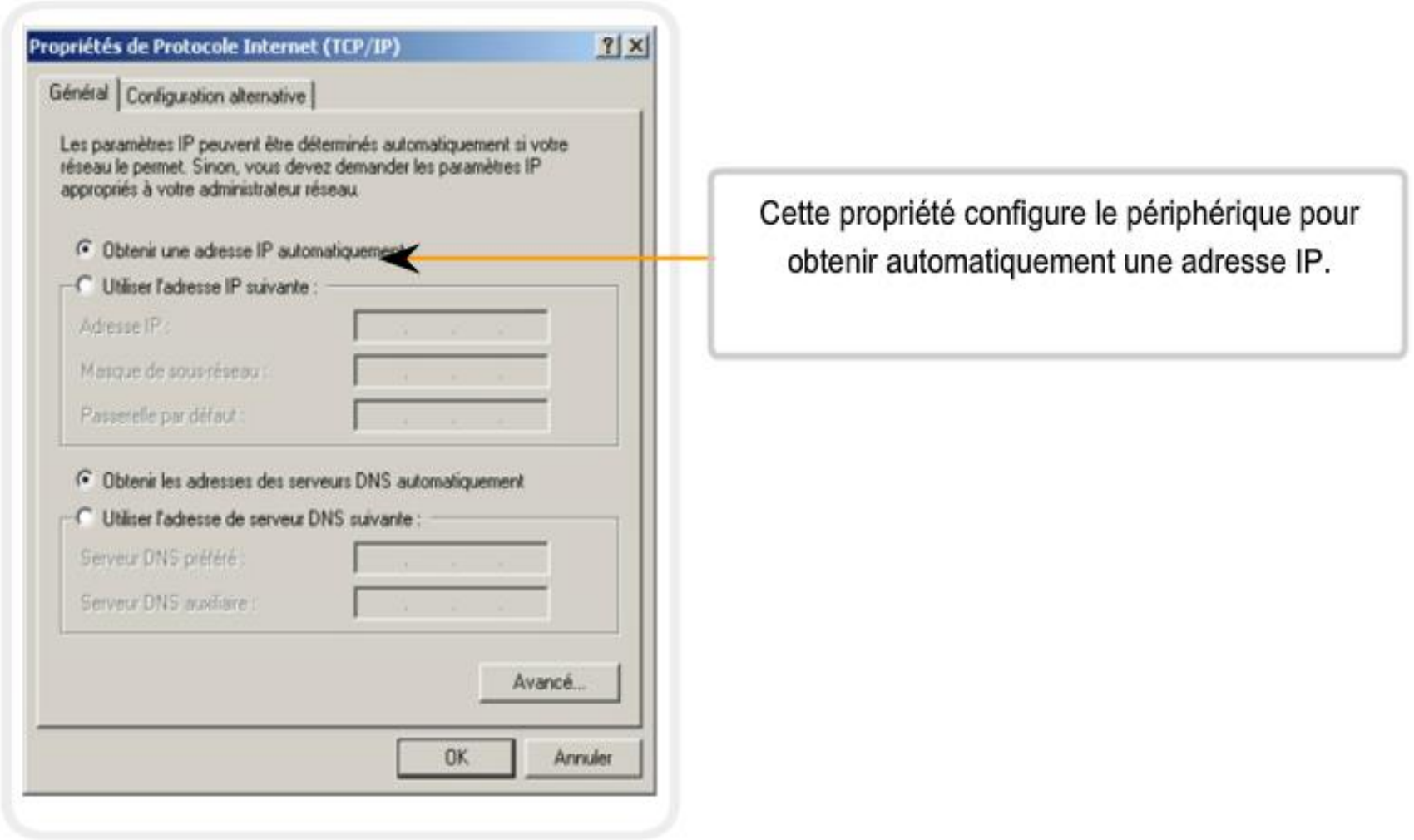
Avec ce type d’attribution, l’administrateur réseau doit configurer manuellement les informations de réseau pour un hôte . Ces informations comportent, au minimum, l’adresse IP, le masque de sous-réseau et la passerelle par défaut.



Attribution dynamique d’adresses

En raison des difficultés associées à la gestion des adresses statiques, les périphériques des utilisateurs se voient attribuer leur adresse de manière dynamique, à l’aide du protocole DCHP (Dynamic Host Configuration Protocol),

Affectation d'adresses dynamiques



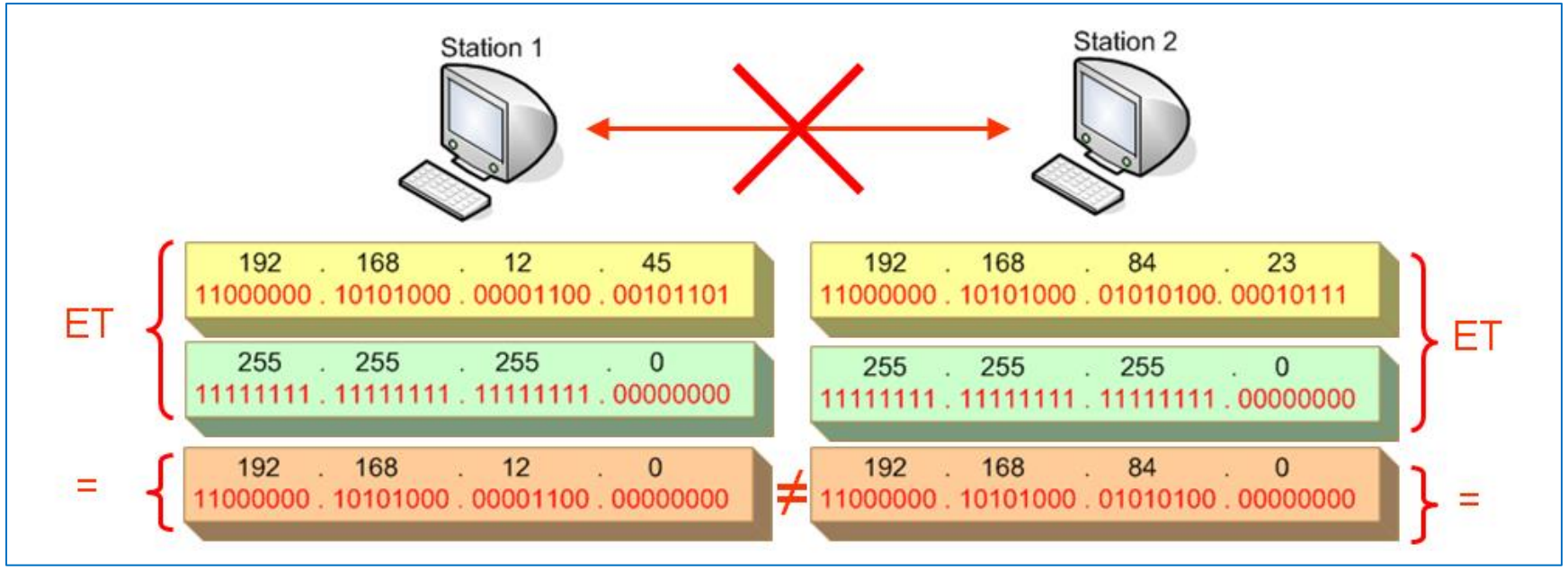
L’avantage de l’attribution dynamique des adresses réside dans le fait que les adresses ne sont pas permanentes pour les hôtes, elles sont uniquement « louées » pour une certaine durée. Si l’hôte est mis sous tension ou retiré du réseau, son adresse est renvoyée au pool et sera réutilisée.

L’autre avantage de l’attribution dynamique réside dans le fait que le personnel de support du réseau est dégagé de cette tâche et le risque d’erreur de saisie est quasiment éliminé.

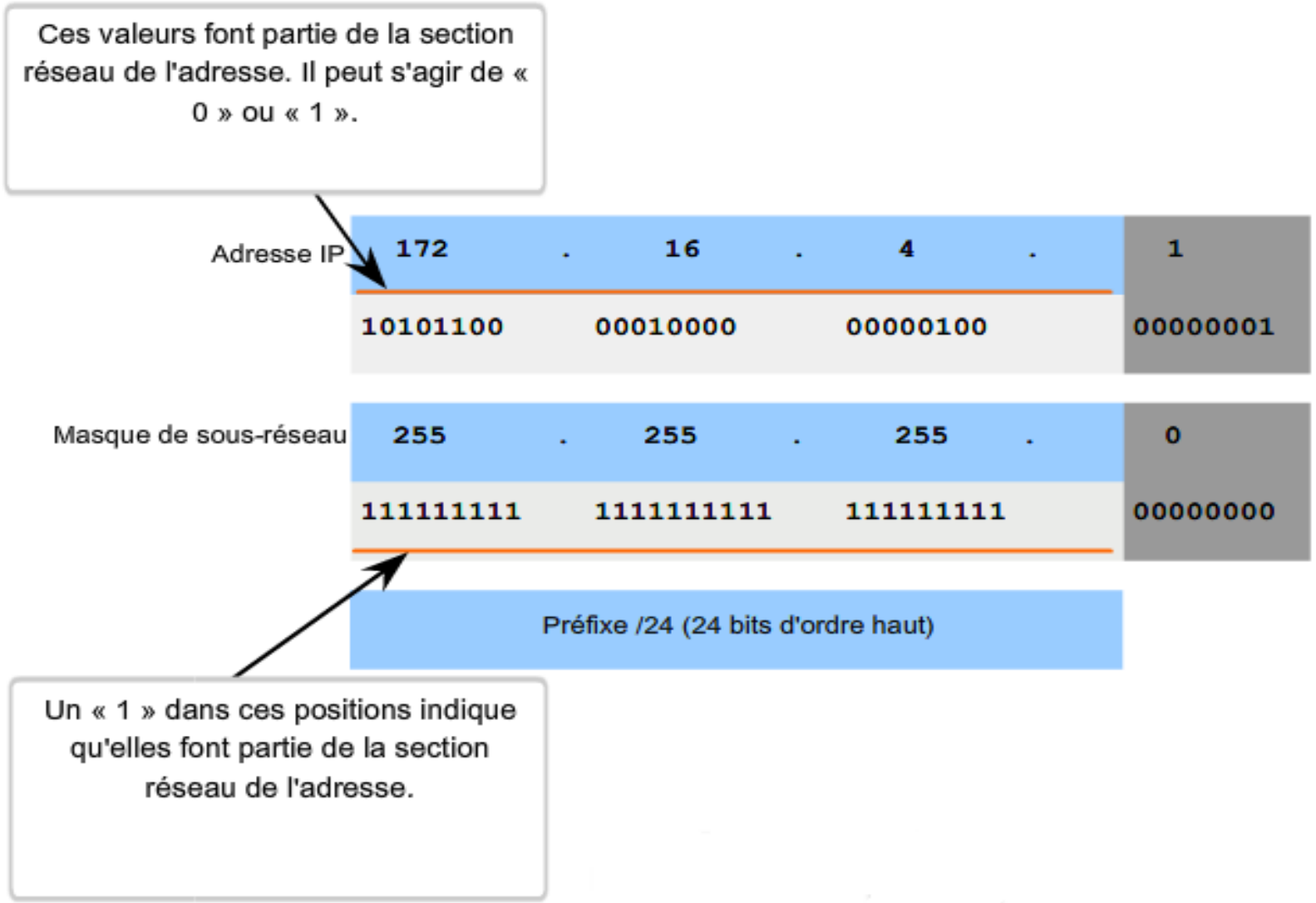
Application du masque

- Deux hôtes peuvent communiquer en direct si :
  - le résultat d'un **ET LOGIQUE** entre l'adresse IP et le masque est identique pour les deux hôtes

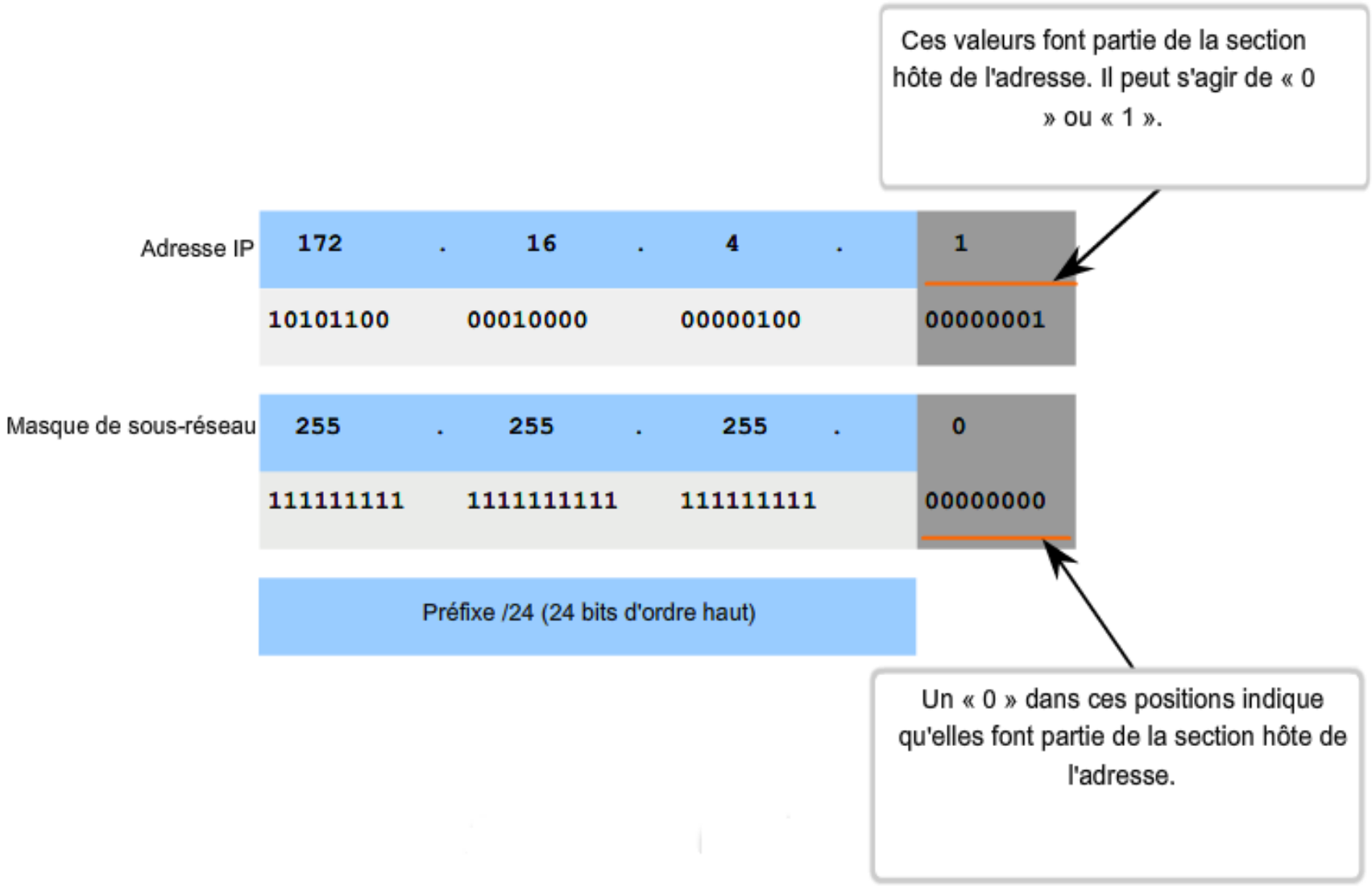
EX



Partie réseau d'une adresse IP



Partie hôte de l'adresse IP



Le préfixe et le masque de sous-réseau constituent des moyens distincts de représenter la même chose : **la partie réseau d'une adresse**.

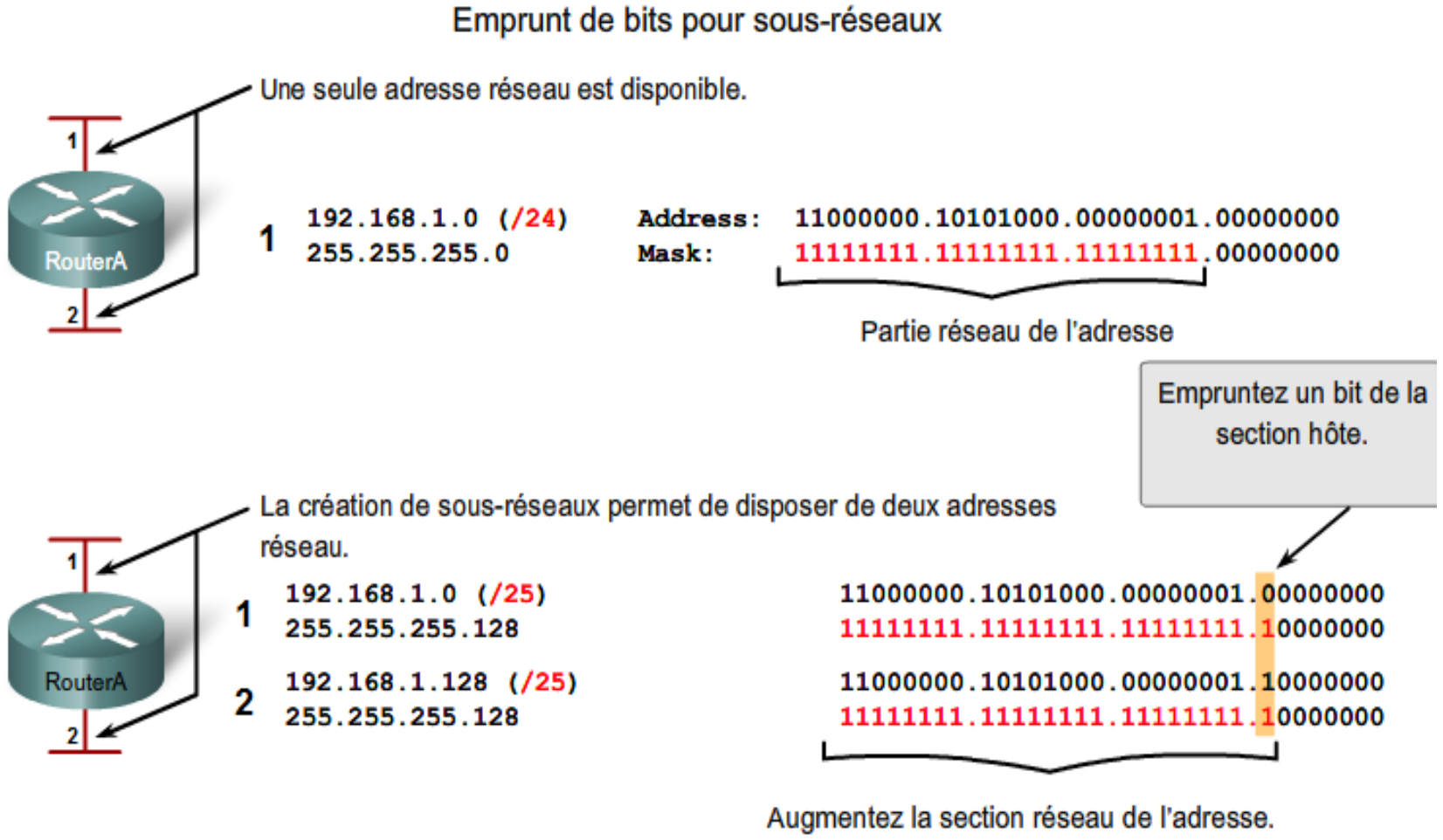
Prenons par exemple l'hôte 172.16.4.35/27 :
adresse : 172.16.4.35 10101100 . 00010000 . 00000100 . 00100011

masque de sous-réseau : 255.255.255.224 11111111 . 11111111 . 11111111 . 11100000

adresse réseau serait : 172.16.4.32 10101100 . 00010000 . 00000100 . 00100000

Soit l'adresse IPV4 suivante 172.16.132.70 /20 .
Dans quel réseau se trouve cet hôte (donner son adresse réseau)

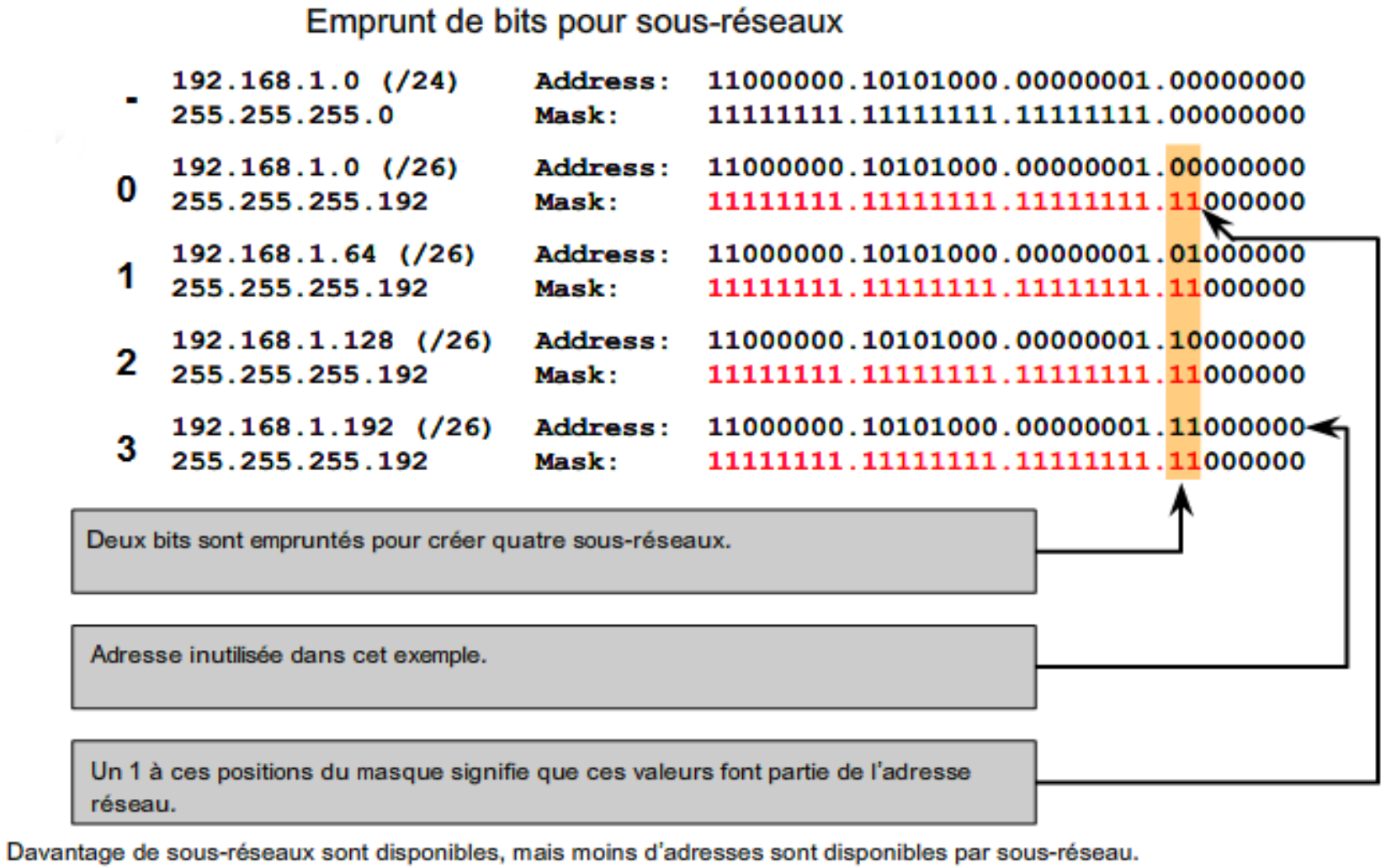
Notions de base pour la création de sous-réseaux



Sous-réseau	Adresse réseau	Plage d'hôtes	Adresse de diffusion
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

utilisons le même bloc d’adresses, à savoir 192.168.1.0 /24.pour créer 3 sous-réseau.

Pour cela ,on doit emprunter deux bits et nous obtenons ainsi quatre sous-réseaux.



Davantage de sous-réseaux sont disponibles, mais moins d'adresses sont disponibles par sous-réseau.

Sous-réseau	Adresse réseau	Plage d'hôtes	Adresse de diffusion
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

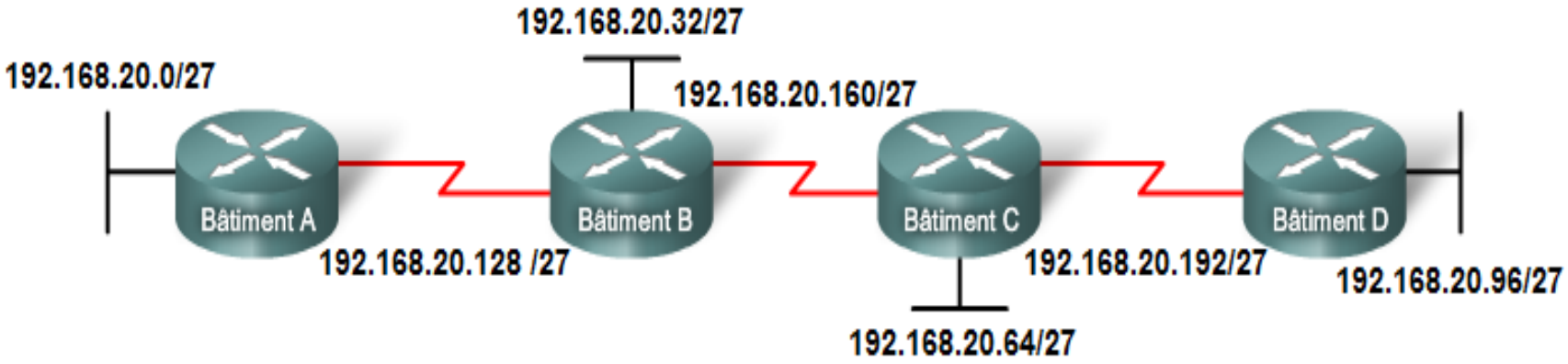
La formule qui permet de calculer le nombre d'hôtes sur un réseau est la suivante :

Nombre d'hôtes utilisables = 2^n - 2

Où n correspond au nombre de bits restants réservés aux hôtes.

Le découpage d'un sous-réseau, qui revient à utiliser un masque de sous-réseau de longueur variable **VLSM** (Variable Length Subnet Mask), permet d'optimiser l'efficacité de l'adressage.

la topologie du schéma ci-dessous démontre qu'un sous-réseau a besoin de sept sous-réseaux, un pour chacun des quatre réseaux locaux et un autre pour chacun des trois réseaux étendus.



Avec l'adresse 192.168.20.0, nous devons emprunter 3 des bits d'hôte du dernier octet afin de créer sept sous-réseaux pour le sous-réseau 192.168.20.0 .

Remarque

Bien que nous ayons réussi à diviser le sous-réseau en un nombre adéquat de sous-réseaux, nous avons gaspillé un nombre important d'adresses. Par exemple, seules deux adresses sont nécessaires dans chaque sous-réseau des liaisons de réseau étendu.

Vingt huit adresses n'ont pas été utilisées dans chacun des trois sous-réseaux du réseau étendu et sont bloquées dans ces blocs d'adresses.
Pour fournir des blocs d'adresses aux liaisons WAN avec deux adresses chacune, nous allons emprunter trois autres bits d'hôte qui seront utilisés comme bits réseau à partir du sous-réseau 6.

Numéro de sous-réseau	Adresse de sous-réseau
Sous-réseau 0	192.168.20.0/27
Sous-réseau 1	192.168.20.32/27
Sous-réseau 2	192.168.20.64/27
Sous-réseau 3	192.168.20.96/27
Sous-réseau 4	192.168.20.128/27
Sous-réseau 5	192.168.20.160/27
Sous-réseau 6	192.168.20.192/27
Sous-réseau 7	192.168.20.224/27

Numéro de sous-réseau	Adresse de sous-réseau
Sous-réseau 0	192.168.20.192/30
Sous-réseau 1	192.168.20.196/30
Sous-réseau 2	192.168.20.200/30
Sous-réseau 3	192.168.20.204/30
Sous-réseau 4	192.168.20.208/30
Sous-réseau 5	192.168.20.212/30
Sous-réseau 6	192.168.20.216/30
Sous-réseau 7	192.168.20.220/30

Avec cet adressage, nous obtenons les sous-réseaux 4, 5 et 7 qui restent disponibles pour de futurs réseaux, ainsi que d'autres sous-réseaux réservés aux liaisons WAN.

Exercices

1. Réaliser l'adressage du scénario du paragraphe **6-5-3**
2. Faire l'exercice du paragraphe **6-5-4** et celui du **6-5-5** afin de vous entraîner à déterminer l'adresse réseau et le nombre maximal d'hôtes pour un réseau.
3. Faire l'exercice du paragraphe **6-5-6** afin de vous entraîner à déterminer les hôtes et les adresses réseau et de diffusion pour un réseau.
4. Faire le **TP 6-5-7 et TP 6-5-8**

La commande ping :

C’est un utilitaire qui permet de tester une connectivité IP entre des hôtes. Elle envoie des demandes de réponse à une adresse hôte spécifiée. Elle utilise un protocole de couche 3 qui fait partie de la suite de protocoles TCP/IP appelée **ICMP** (Internet Control Message Protocol). Elle utilise un datagramme ICMP Echo Request.

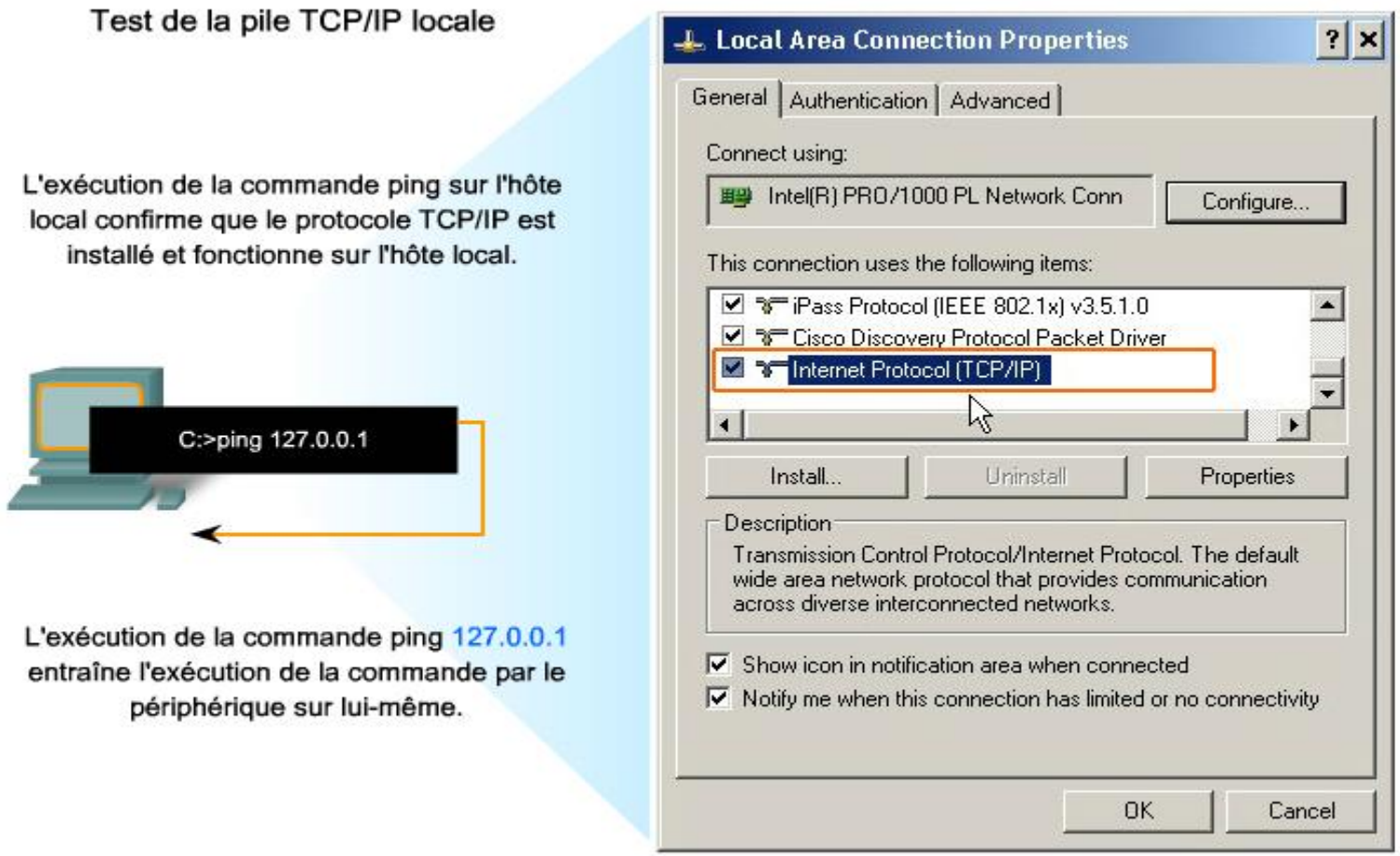
Si l’hôte, à l’adresse spécifiée, reçoit une demande Echo, il répond par un datagramme ICMP Echo Reply.

La commande ping a une valeur de délai d’attente pour la réponse. Si la réponse n’est pas reçue dans le délai imparti, la commande ping abandonne l’opération et affiche un message indiquant que la réponse n’a pas été reçue.

Une fois toutes les requêtes envoyées, l’utilitaire ping présente la sortie indiquant le taux de réussite et le délai moyen aller-retour, jusqu’à la destination.

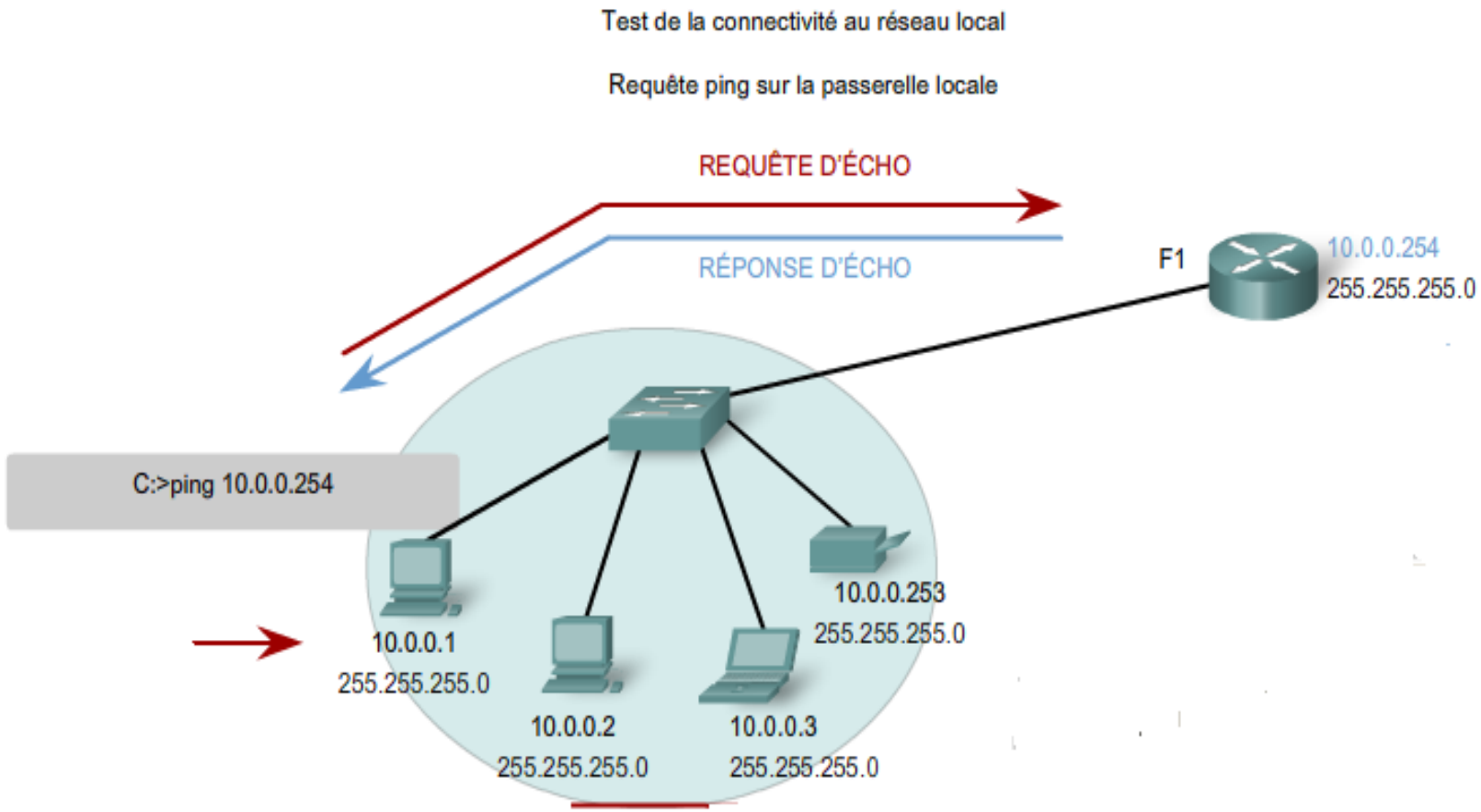
Envoi d'une requête ping sur le bouclage local ping 127.0.0.1

Une réponse de 127.0.0.1 indique que le protocole IP est correctement installé sur l'hôte. Si un message d'erreur est généré, cela indique que TCP/IP ne fonctionne pas sur l'hôte.



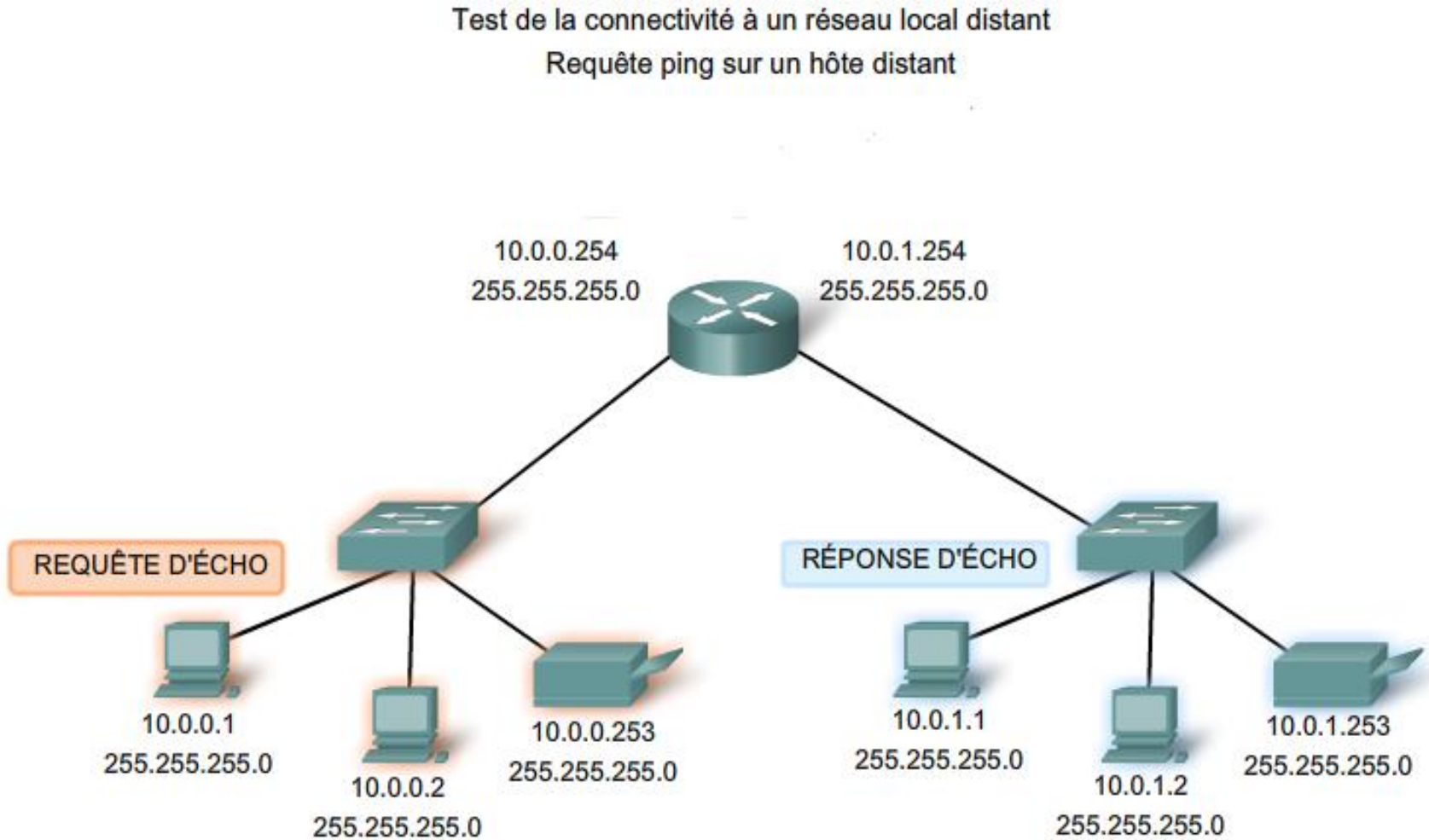
Envoi d’une requête ping sur une passerelle pour le test du réseau local

la commande ping est utilisée aussi pour tester la capacité d’un hôte à communiquer sur le réseau local.



Envoi d’une requête ping à un hôte distant

la commande ping est utilisée aussi pour tester la capacité d’un hôte IP local à communiquer sur un inter-réseau**.**



La commande traceroute (tracert)

C’est un utilitaire qui permet d’identifier le chemin entre des hôtes.

L’analyse du chemin génère une liste de sauts qui ont été traversés sur le trajet.

Si les données parviennent à destination, l’analyse du chemin répertorie tous les routeurs rencontrés sur le chemin.

Si les données n’atteignent pas un des sauts sur leur parcours, l’adresse du dernier routeur qui a répondu à l’analyse est renvoyée. Elle indique, soit l’endroit où le problème est survenu, soit l’endroit où des restrictions de sécurité s’appliquent.

Faire l’exercice 6.7.5 : configuration d’un sous-réseau et d’un routeur et réaliser le TP 6-7-5 sur packet tracer .

Quelles sont les différences entre les nombres binaires et les nombres décimaux ? (Choisissez deux réponses.)

- [ ] Les nombres décimaux sont de base 1 alors que les nombres binaires s'appuient sur la base 2.
- [ ] Les nombres binaires sont de base 2 alors que les nombres décimaux s'appuient sur la base 10.
- [ ] Les ordinateurs exploitent les nombres binaires tandis que les humains utilisent des nombres décimaux.
- [ ] Les nombres tapés sur le clavier sont saisis sous forme binaire, puis convertis en nombres décimaux par l'ordinateur.
- [ ] Les nombres binaires représentent trois états : actif, inactif, nul. Les nombres décimaux, eux, ne représentent pas d'état.

Regardez la commande ci-dessous et son résultat. Un administrateur réseau teste la configuration sur un ordinateur hôte. Quel est le type d'adresse correspondant à 127.0.0.1 ?

- Une adresse locale-lien
- Une adresse de bouclage
- Une adresse publique
- Une adresse de route par défaut

À quoi correspond la partie de l'adresse IP représentant le préfixe ?

- L'adresse de diffusion (broadcast)
- L'adresse de l'hôte
- L'adresse réseau
- L'adresse de monodiffusion (unicast)

Parmi les affirmations suivantes en matière d'adresses IP réseau, laquelle est vraie ?

- Tous les bits d'hôte valent 0.
- Tous les bits d'hôte valent 1.
- L'adresse attribuée est la plus grande possible dans une plage.
- Tous les bits de réseau valent 1.

Lorsque tous les bits hôte sont associés à la valeur 1, quel est le type d'adresse ?

- L'adresse réseau
- L'adresse de diffusion (broadcast)
- L'adresse d'hôte
- L'adresse de monodiffusion (unicast)

Combien de chiffres binaires (bits) composent une adresse IPv6 ?

- 64 bits
- 48 bits
- 128 bits
- 32 bits

Quelle est la raison principale à l'origine du développement du protocole IPv6 ?

- La sécurité
- La simplification du format des en-têtes
- L'extension des possibilités d'adressage
- La simplification de l'adressage

Faites glisser les options de gauche sur la valeur correspondante à droite.

192.168.16.192/30	Quatre bits empruntés pour créer les sous-réseaux
172.27.64.98/23	Six sous-réseaux utilisables
172.18.125.6/20	Deux hôtes utilisables par sous-réseau
10.1.167.36/13	Le réseau n'est pas scindé en sous-réseaux
192.168.87.212/24	512 adresses par sous-réseau
172.31.16.128/19	

CONFIGURATION DE BASE DU ROUTEUR

INTRODUCTION

LES PORTS

CONFIGURATION

OBJECTIF ET CONTENU

Objectifs :
Comprendre les composants et le fonctionnement d'un réseau routeur.

Contenu :
Configuration de base d'un routeur

Le fichier IOS (système d'exploitation du routeur) est stocké dans une zone de mémoire semi-permanente appelée Flash. La mémoire Flash assure un stockage non volatile.

Méthodes d'accès

Il y a plusieurs moyens d'accéder à l'environnement ILC. Les méthodes les plus répandues utilisent :

- ❑ le port de console : accès terminal ;
- ❑ le port Ethernet ou série : accès telnet ou SSH ;
- ❑ le port AUX. / accès modem

Le port de console est souvent utilisé pour accéder à un périphérique avant que les services réseau ne soient lancés ou lorsqu'ils sont défaillants.

La console s'utilise en particulier dans les circonstances suivantes :

- configuration initiale du périphérique réseau ;
- procédures de reprise après sinistre et dépannage lorsque l'accès distant est impossible ;
- procédures de récupération des mots de passe.

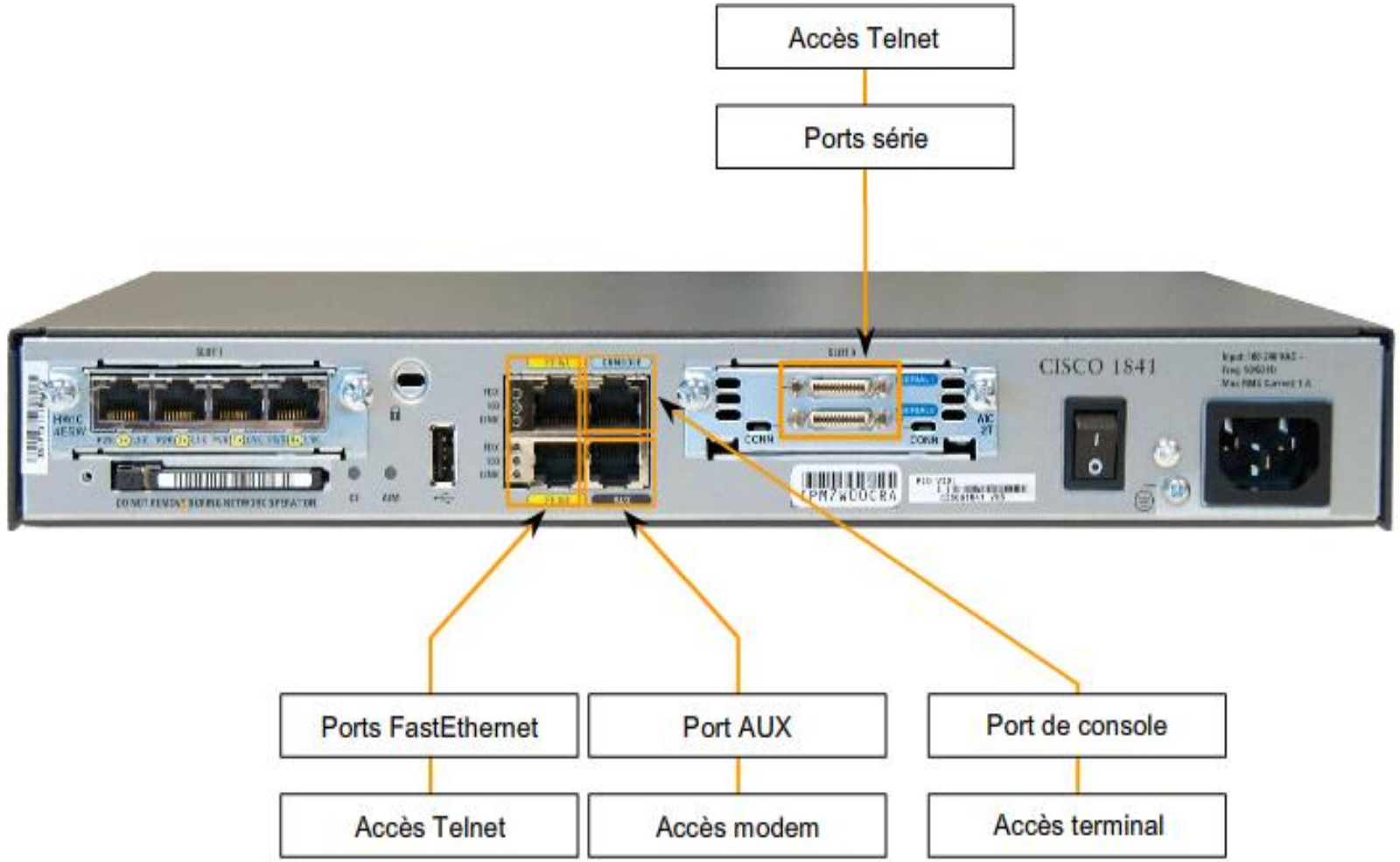
Accès telnet ou SSH

- Les sessions Telnet requièrent des services réseau actifs sur le périphérique. Le périphérique réseau doit avoir au moins une interface active configurée avec une adresse de couche 3.

Un hôte doté d'un client Telnet peut accéder aux sessions vty en cours d'exécution sur le périphérique Cisco.
IOS exige l'emploi d'un mot de passe dans la session Telnet pour une authentification minimale.

- Le protocole Secure Shell (SSH) permet un accès distant plus sécurisé aux périphériques.

SSH fournit une authentification par mot de passe plus résistante que celle de Telnet et emploie un chiffrement lors du transport des données de la session.


Accès Telnet
Ports série
CISCO 1841
Ports FastEthernet
Port AUX
Port de console
Accès Telnet
Accès modem
Accès terminal

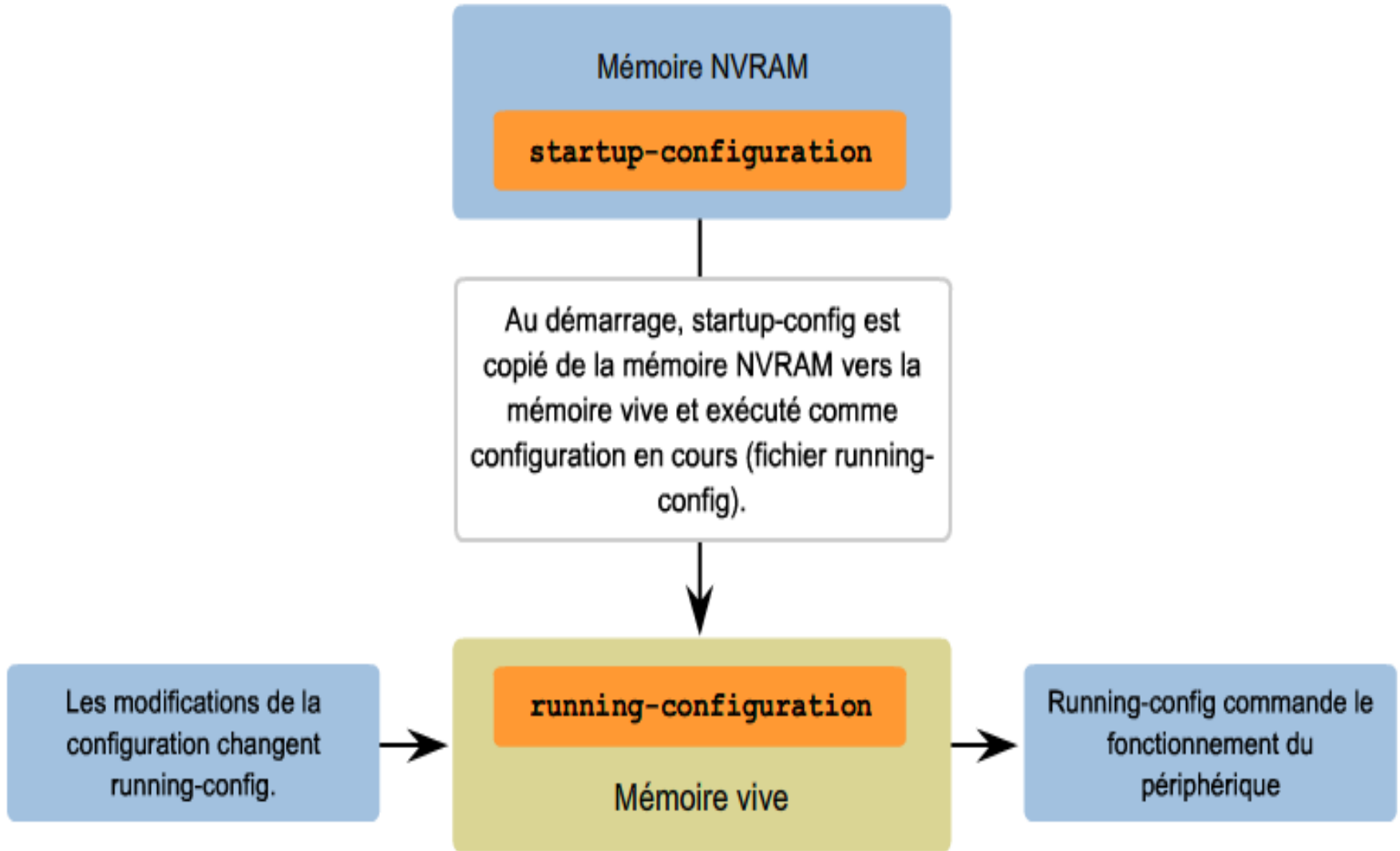
Les routeurs ont besoin de deux types de logiciels pour fonctionner : le système d'exploitation et le logiciel de configuration.

Un routeur Cisco contient deux fichiers de configuration :

- le fichier de configuration en cours, que le périphérique utilise en fonctionnement normal (**running-config)** ;

- le fichier de configuration initiale (**startup-config**) qui est chargé quand le périphérique démarre et sert de copie de sauvegarde de la configuration. Il est stocké en mémoire vive non volatile (NVRAM).

Une fois chargé en mémoire vive, le fichier de configuration initiale est considéré comme étant la configuration en cours, également appelée **running-config**.


Mémoire NVRAM
startup-configuration
Au démarrage, startup-config est copié de la mémoire NVRAM vers la mémoire vive et exécuté comme configuration en cours (fichier running-config).
Les modifications de la configuration changent running-config.
running-configuration
Mémoire vive
Running-config commande le fonctionnement du périphérique

Modes IOS Cisco :

les principaux modes sont les suivants :

- mode d’exécution utilisateur ;
- mode d’exécution privilégié ;
- mode de configuration globale ;
- autres modes de configuration spécifiques.

```
Router>ping 192.168.10.5

Router#show running-config

Router(config)#Interface FastEthernet 0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

Basculement entre mode utilisateur et mode privilégié

Les commandes **enable** et **disable** permettent d'aller et venir entre le mode d'exécution utilisateur et le mode d'exécution privilégié

La syntaxe de la commande enable est la suivante :

```
Router>enable
```

l'invite du routeur se transforme en :

```
Router#
```

L e routeur est en mode d'exécution privilégié.

Si une authentification par mot de passe a été configurée pour le mode d'exécution privilégié, IOS vous invite à fournir le mot de passe.

```
Router>enable
Password:
Router#
```

Le mode de **configuration globale.**

Router#**configure terminal**

Cette commande permet de faire passer le périphérique du mode d'exécution privilégié au mode de configuration globale

Modes de configuration spécifiques

Mode de configuration	Invite
Interface	Router(config-if)#
Ligne	Router(config-line)#
Routeur	Router(config-router)#

Pour quitter un mode de configuration spécifique et retourner au mode de configuration globale, entrez **exit** .

Pour quitter complètement le mode de configuration et retourner au mode d'exécution privilégié, entrez **end** ou utilisez **Ctrl-Z**.

Après une modification à partir du mode global, enregistrez la configuration dans le fichier de configuration initiale stocké en mémoire NVRAM.

Router#**copy running-config startup-config** ou Router#**copy r s**

Attribution de noms

Router#**configure terminal** abrev **:conf t**
Router(config)# **hostname ent** abrev **: host ent**
ent(config)#

pour supprimer le nom attribué à un périphérique, on utilise:

ent(config)# **no hostname**
Router(config)#

TP 11.2.1

Tout périphérique doit être protégé par des mots de passe configurés localement afin de limiter l'accès.

Mot de passe de console : limite l'accès au périphérique par une connexion console
Mot de passe enable : limite l'accès au mode d'exécution privilégié
Mot de passe « enable secret » : chiffré, limite l'accès au mode d'exécution privilégié
Mot de passe VTY : limite l'accès au périphérique par une connexion Telnet ou SSH .

Il est recommandé d'utiliser des mots de passe différents pour chacun de ces niveaux d'accès.

Mot de passe console
ent(config)#**line console 0**
ent(config-line)#**password cisco**
ent(config-line)#**login**

Mots de passe enable et enable secret
ent(config)#**enable password class** (une ancienne version du logiciel Cisco IOS)
ent(config)#**enable secret class** (le mot de passe est chiffré)

Mot de passe VTY
ent(config)#**line vty 0 4**
ent(config-line)#**password cisco**
ent(config-line)#**login**

Chiffrement de l'affichage des mots de passe
service password-encryption

Messages de bannière
pour déclarer que l'accès à un périphérique est réservé aux personnes autorisées.
ent(config)#**banner motd #Toute utilisation non autorisée fera l'objet de poursuites judiciaires. #**

TP 11.2.2

Restauration de la configuration d'origine du périphérique
redémarrer le périphérique en entrant la commande **reload en mode d'exécution privilégié**.
Pour abandonner les modifications, entrez n ou no.

Suppression de toutes les configurations
La commande Router#**erase startup-config** permet de supprimer la configuration initiale.

Sauvegarde des configurations hors connexion
Les fichiers de configuration peuvent être stockés sur un serveur TFTP (Trivial File Transfer Protocol) ou sur un support conservé en lieu sûr.

Sauvegarde de la configuration sur un serveur TFTP
Router#copy running-config tftp ou copy startup-config
Entrez ensuite l'adresse IP de l'hôte qui doit héberger le fichier de configuration et le nom à attribuer au fichier de configuration et confirmer l'action.

TP 11.2.3

Configuration des interfaces Ethernet d'un routeur

Les interfaces Ethernet d'un routeur servent de passerelles pour les périphériques finaux sur les réseaux locaux connectés directement au routeur.

```
Router(config)#interface FastEthernet 0/0
Router(config-if)#ip address 192.168.1.1  255.255.255.0
Router(config-if)#no shutdown
```

Configuration des interfaces série d'un routeur

Les interfaces série permettent de connecter des réseaux étendus (WAN) à des routeurs sur un site distant ou chez un fournisseur de services Internet.
Les interfaces série nécessitent un signal d'horloge pour contrôler la synchronisation des communications.
La commande **clock rate** permet d'activer l'horloge et de spécifier sa fréquence.

```
Router(config)#interface Serial 0/0/0
Router(config-if)#ip address 192.168.2.1  255.255.255.252
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
```

TP 11.5.1

Si on veut créer une description, on utilise la commande **description :**

Router(config-if)# description Connexion au commutateur principal du bâtiment A

Faire le TP 11.6.1 à remettre après les vacances

les principaux raccourcis:

Tab : Complète la commande ou le mot clé en affichant le reste
Ctrl-R : Affiche à nouveau une ligne
Ctrl-Z : Permet de passer du mode de configuration au mode d'exécution
Bas : Permet à l'utilisateur de faire défiler vers l'avant les commandes précédentes
Haut : Permet à l'utilisateur de faire défiler vers l'arrière les commandes précédentes
Ctrl-Maj-6 : Permet à l'utilisateur d'interrompre un processus IOS comme ping ou traceroute
Ctrl-C : Permet d'abandonner la commande actuelle et de quitter le mode de configuration

Il est possible d'abréger les commandes

exemple : Router#sh int