

# Réseaux informatiques

- ▶ Présentation des réseaux
- ▶ Principes de communication sur un réseau informatique
- ▶ Communication via un réseau local câblé
- ▶ Création de la couche d'accès d'un réseau Ethernet
- ▶ Création de la couche de distribution du réseau

# Présentation des réseaux

## ► Objectifs

- Expliquer le concept des réseaux et leurs avantages
- Expliquer le concept des protocoles de communication
- Expliquer comment la communication a lieu sur un réseau Ethernet
- Décrire les périphériques de la couche d'accès et les méthodes de communication sur un réseau Ethernet local
- Décrire les périphériques de la couche de distribution et les méthodes de communication dans les réseaux
- Organiser, implémenter et vérifier un réseau local

# Présentation des réseaux

## ► Qu'est-ce qu'un réseau ?

- **Dans la vie de tous les jours**

- un ensemble d'objets ou de personnes connectées ou maintenues en liaison.

- ✓ les objets ou personnes reliées sont appelées nœuds du réseau.

- peut s'appliquer à divers domaines

- ✓ le réseau social désigne un ensemble de personnes qui se connaissent et restent en contact entre elles, le réseau ferroviaire désigne les lignes de chemin de fer ainsi que les gares.

- ✓ Ainsi, il existe des réseaux électriques, téléphoniques, ou informatiques.

- **Les réseaux informatiques**

- C'est un ensemble de matériels et de logiciels permettant à des équipements (ordinateurs et autres périphériques) de communiquer entre eux.

- ✓ L'objectif d'un réseau est le partage des ressources matérielles (disques durs, imprimantes) et des ressources logicielles (fichiers, applications)

# Présentation des réseaux

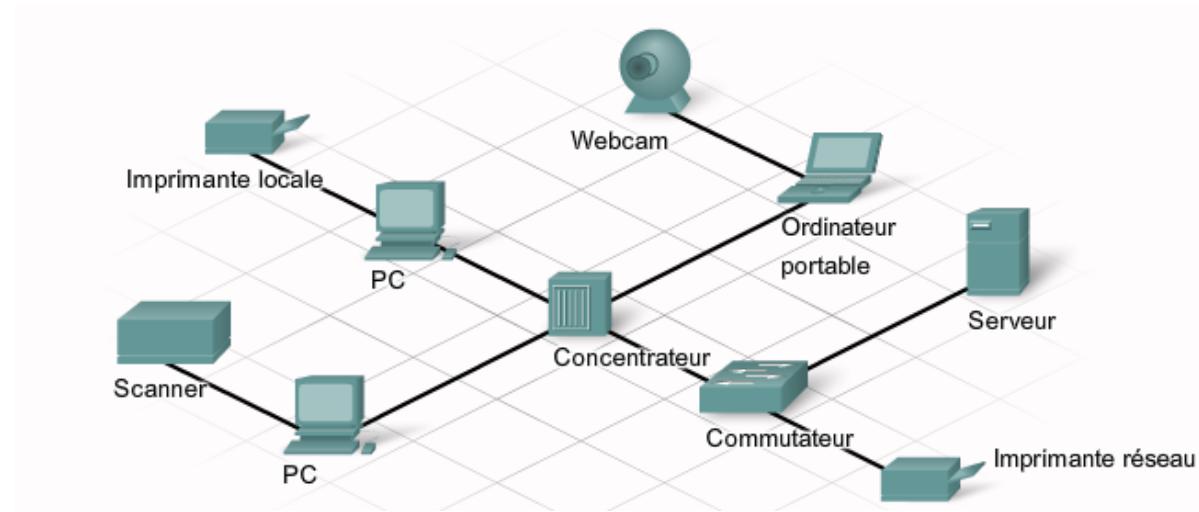
## ► Avantages des réseaux

- Les réseaux installés chez les particuliers ou les petites entreprises
  - partager des ressources, telles que des imprimantes, des documents, des images et de la musique, entre quelques ordinateurs locaux
- Dans les grandes entreprises, des réseaux de grande taille
  - publier et vendre des produits, effectuer des achats auprès de fournisseurs et communiquer avec les clients.
- Les communications via un réseau sont généralement plus efficaces et plus économiques que les formes de communication classiques telles que le courrier postal ou les appels téléphoniques interurbains ou internationaux.
  - Les réseaux mettent en œuvre des moyens de communication rapides, comme le courriel et la messagerie instantanée, ainsi que la consolidation, le stockage et l'accès aux informations sur des serveurs réseau.

# Présentation des réseaux

## ► Composants d'un réseau de base

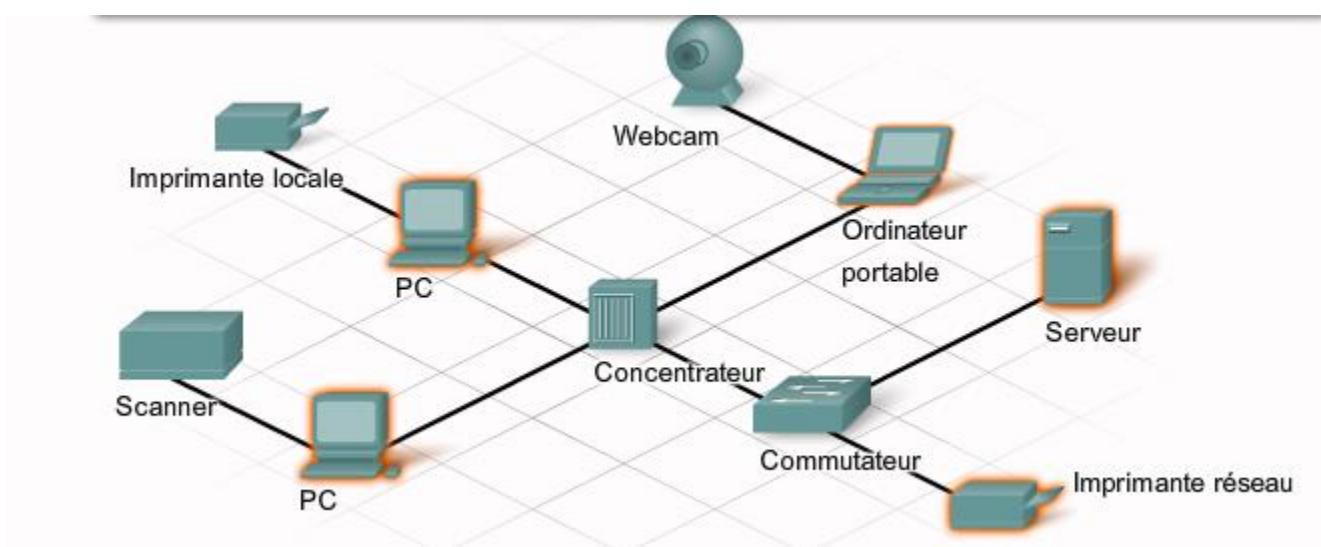
- De nombreux composants entrent dans la configuration d'un réseau : ordinateurs, serveurs, périphériques réseau, câbles, etc



- Ces composants peuvent être classés en quatre catégories principales

# Présentation des réseaux

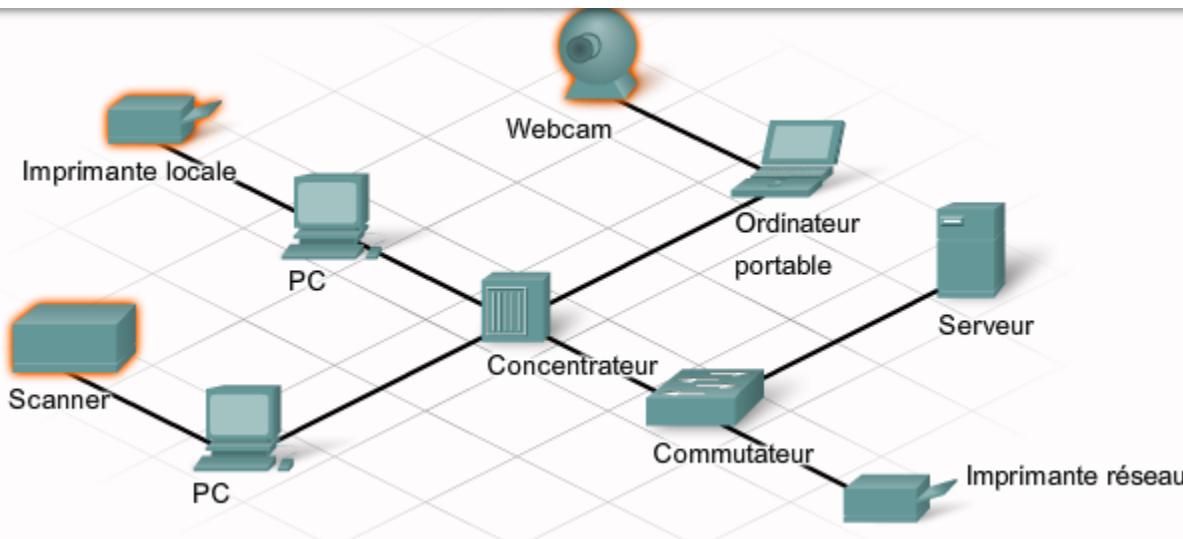
- ▶ Composants d'un réseau de base
  - Hôtes



- Les hôtes sont des périphériques qui envoient et reçoivent des messages directement sur le réseau. Un hôte a une adresse IP.

# Présentation des réseaux

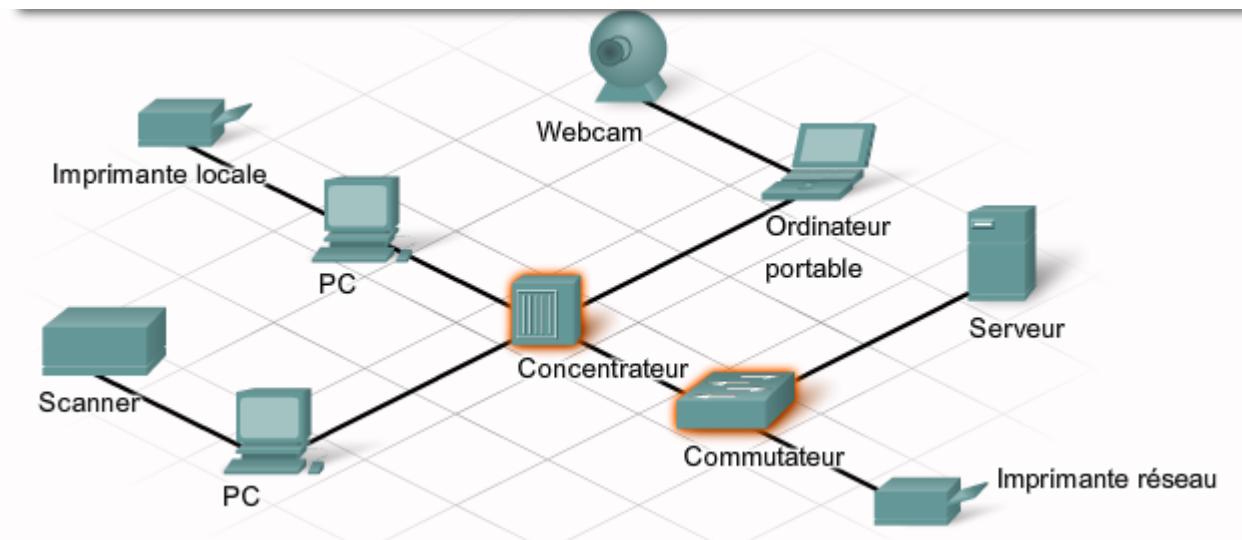
- ▶ Composants d'un réseau de base
  - Périphériques partagés



- Les périphériques partagés ne sont pas directement connectés au réseau, mais aux hôtes. L'hôte assure donc le partage de périphériques sur le réseau. Les hôtes sont équipés de logiciels configurés pour permettre aux utilisateurs du réseau d'exploiter les périphériques connectés.

# Présentation des réseaux

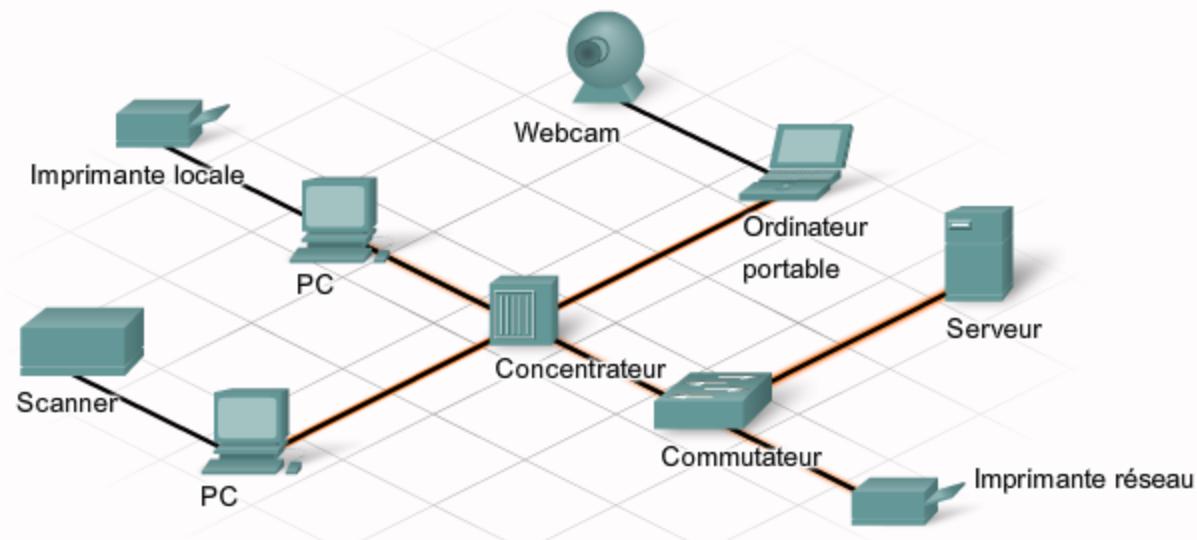
- ▶ Composants d'un réseau de base
  - Périphériques réseau



- Les périphériques réseaux relient d'autres périphériques, en particulier des hôtes. Ces périphériques alimentent et contrôlent le trafic du réseau.

# Présentation des réseaux

- ▶ Composants d'un réseau de base
  - Supports réseau

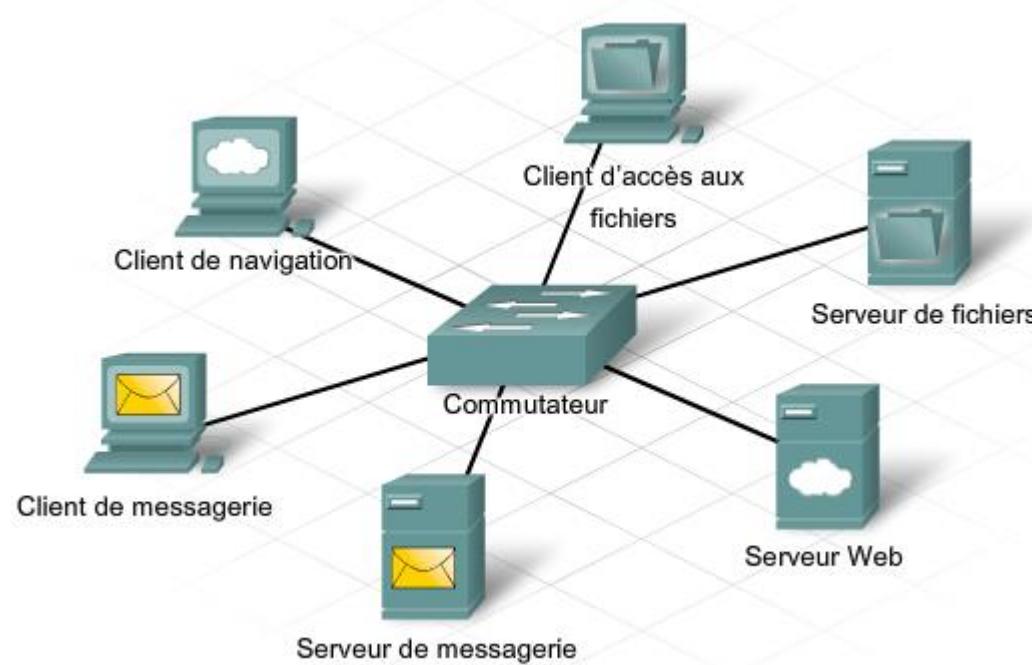


- Un support réseau permet de connecter des hôtes à des périphériques réseau. Il peut être câblé avec du cuivre ou des fibres optiques, ou utiliser des technologies sans fil.

# Présentation des réseaux

## ► Rôles des ordinateurs au sein d'un réseau

- Dans les réseaux actuels, les ordinateurs hôtes peuvent jouer le rôle de client, de serveur ou les deux. Les logiciels installés sur l'ordinateur déterminent le rôle qu'il tient au sein du réseau.



# Présentation des réseaux

## ► Rôles des ordinateurs au sein d'un réseau

- **Serveur**

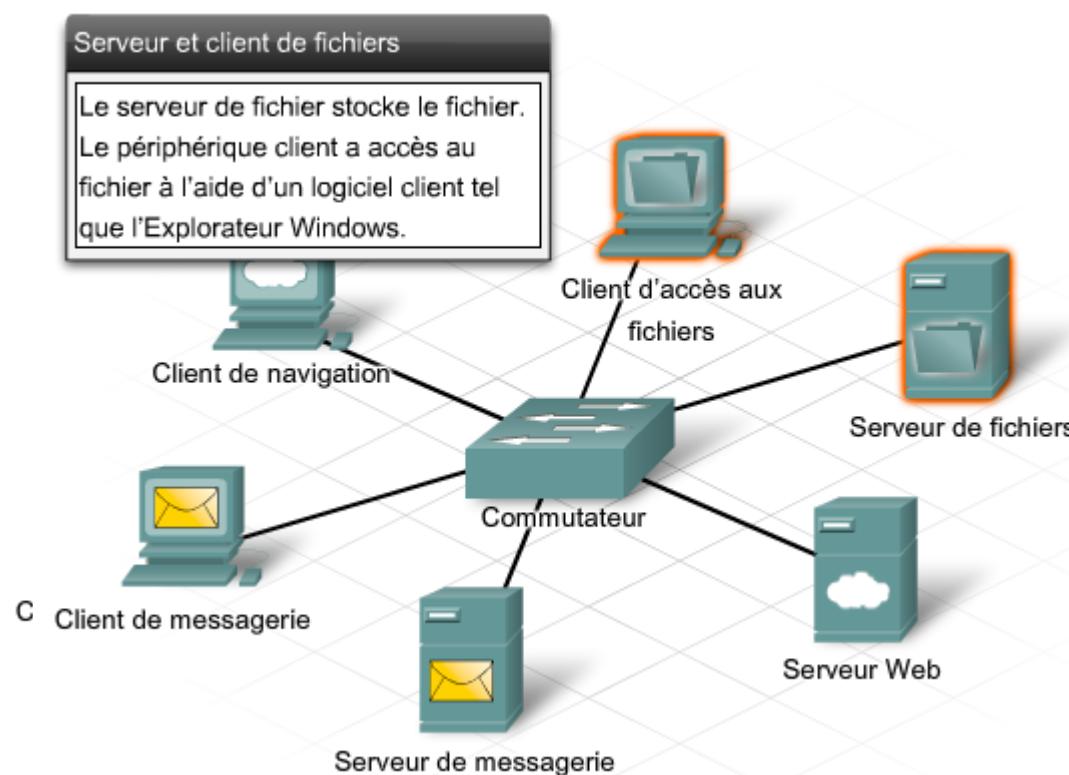
- Les serveurs sont des hôtes équipés des logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages Web, à d'autres hôtes sur le réseau. Chaque service nécessite un logiciel serveur distinct.

- **Client**

- Les clients sont des ordinateurs hôtes équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les afficher

# Présentation des réseaux

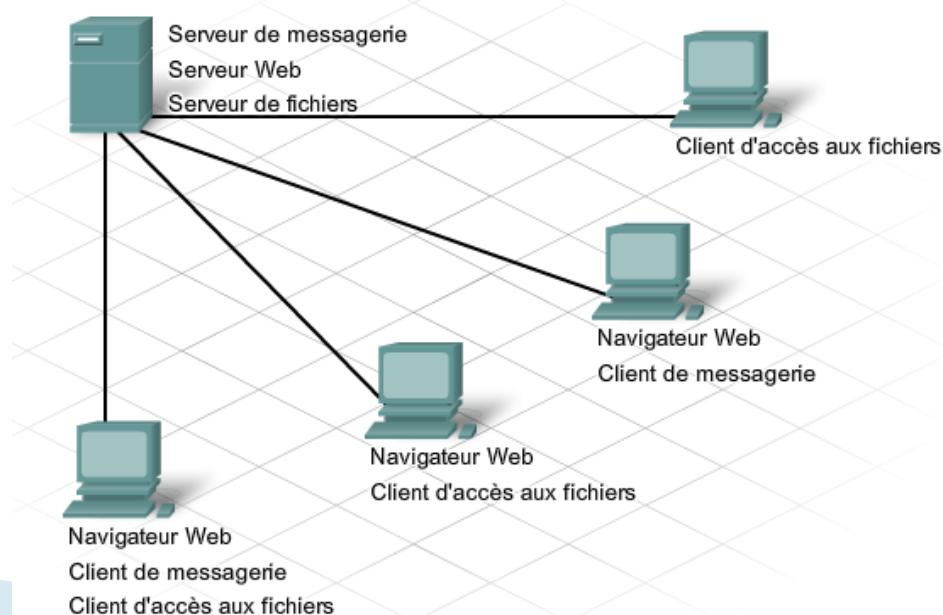
- ▶ Rôles des ordinateurs au sein d'un réseau
  - Exemples



# Présentation des réseaux

## ► Rôles des ordinateurs au sein d'un réseau

- Un ordinateur équipé d'un logiciel serveur peut fournir des services à un ou plusieurs clients en même temps.
- De plus, un seul ordinateur peut exécuter différents types de logiciel serveur. Chez les particuliers et dans les petites entreprises, il peut arriver, par nécessité, qu'un ordinateur fasse office à la fois de serveur de fichiers, de serveur Web et de serveur de messagerie.
- Un seul ordinateur peut également exécuter différents types de logiciels clients. Un logiciel client doit être installé pour chaque type de service requis. Un hôte équipé de plusieurs clients peut se connecter à plusieurs serveurs en même temps

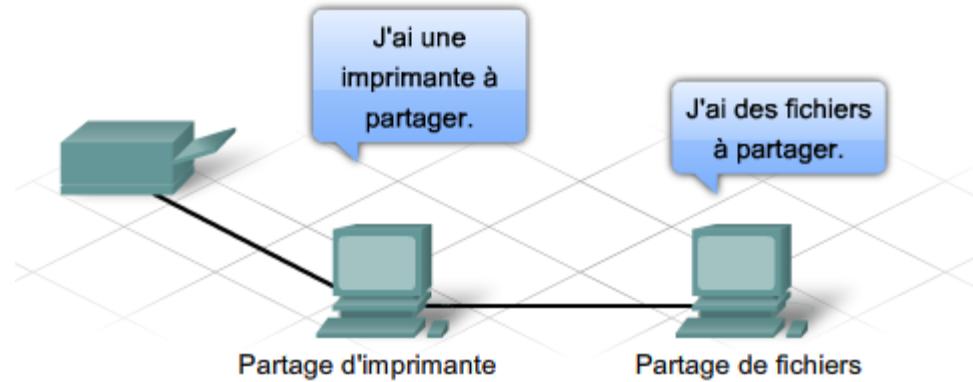


# Présentation des réseaux

## ► Réseaux peer to peer

### ◦ Définition

- Dans le cas des réseaux de particuliers et de petites entreprises, il arrive souvent que les ordinateurs fassent à la fois office de serveur et de client sur le réseau. Ce type de réseau est appelé réseau peer to peer.
- Le réseau peer to peer le plus simple est constitué de deux ordinateurs interconnectés à l'aide d'une connexion câblée ou sans fil.



- Il est également possible d'interconnecter plusieurs PC pour créer un réseau peer to peer plus important, mais cela nécessite un périphérique réseau, tel qu'un concentrateur.

# Présentation des réseaux

## ► Réseaux peer to peer

- Avantages et inconvénients

Avantages d'un réseau peer to peer :

- facile à configurer ;
- plus simple ;
- coûte moins cher car les périphériques réseau et les serveurs dédiés peuvent ne pas être nécessaires ;
- peut servir pour des tâches simples, telles que le transfert de fichiers et le partage d'imprimantes.

Inconvénients d'un réseau peer to peer :

- aucune administration centralisée ;
- n'est pas aussi sécurisé ;
- n'est pas extensible ;
- tous les périphériques peuvent servir à la fois de client et de serveur, ce qui peut ralentir leurs performances.

# Présentation des réseaux

- ▶ **Réseaux peer to peer**
  - TP: création d'un réseau Peer to Peer simple

# Présentation des réseaux

## ► Topologie des réseaux

- **Topologie physique**
  - décrit la manière dont les équipements sont reliés par des médias
- **Topologie logique**
  - décrit la manière dont les équipements communiquent.

# Présentation des réseaux

## ► Topologie des réseaux

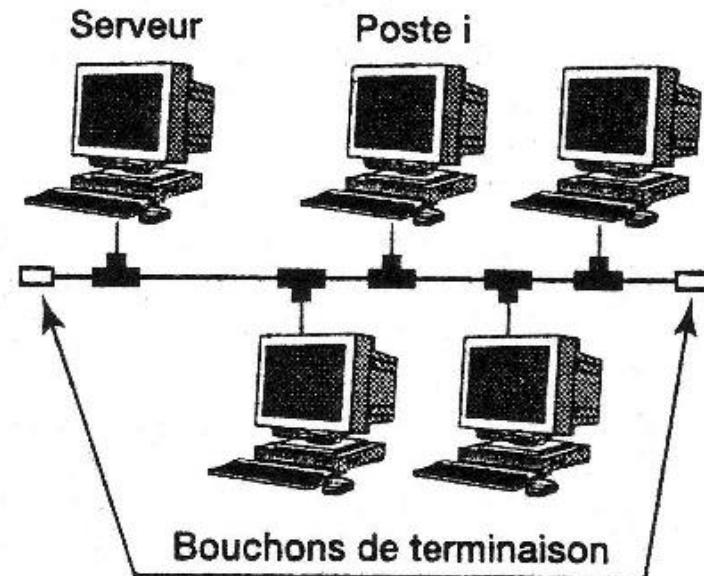
### ◦ Bus

#### • Topologie physique

- Tous les ordinateurs sont connectés entre eux par le biais d'un seul câble réseau (bus) débuté et terminé par des terminateurs (bouchons)

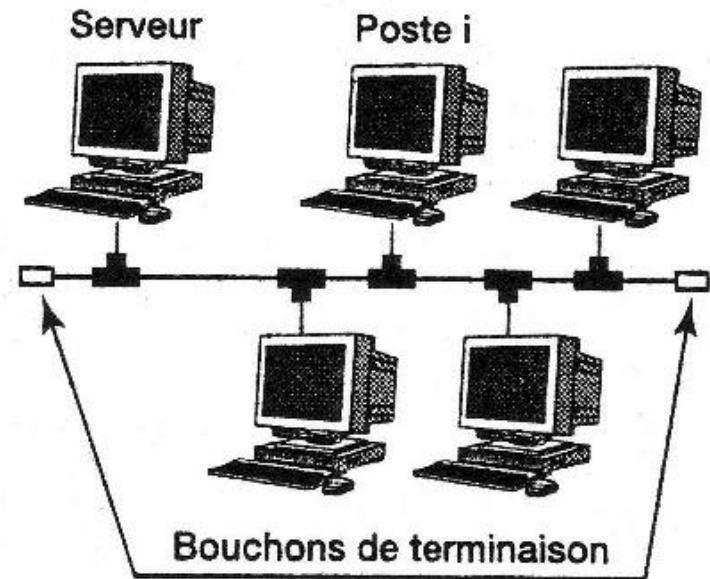
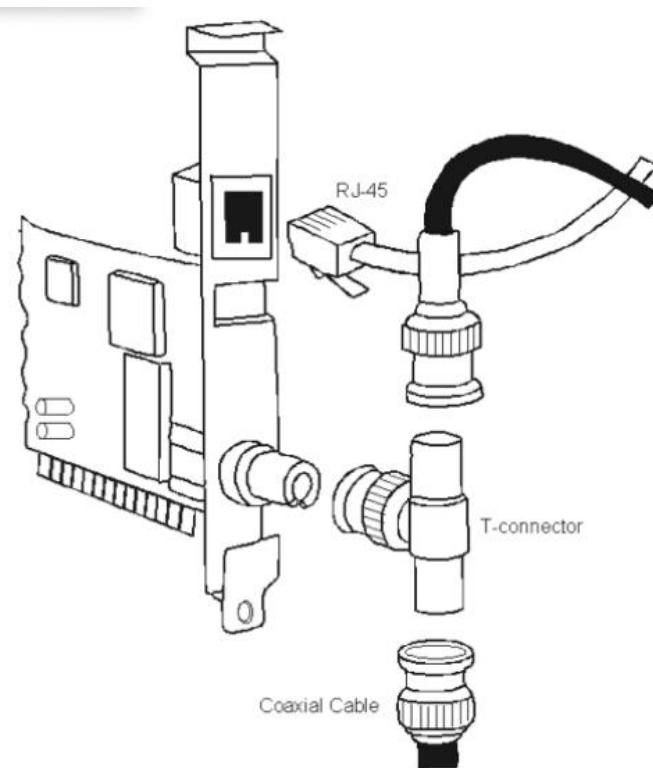
#### • Topologie logique

- Tous les hôtes voient tous les signaux provenant de tous les autres équipements



# Présentation des réseaux

- ▶ Topologie des réseaux
  - Bus



# Présentation des réseaux

## ► Topologie des réseaux

- **Bus**

- ✓ **Avantages**

- la longueur du câble est moins importante que pour les autres topologies.
    - défaillance d'un terminal n'affecte pas le reste du réseau
    - extension aisée de câble

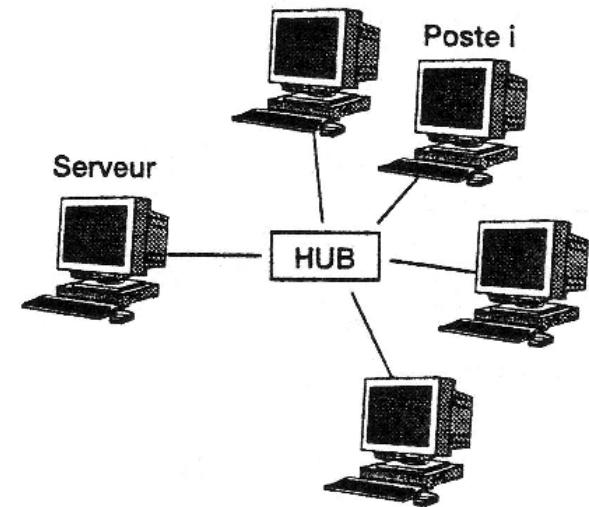
- ✓ **Inconvénients**

- temps d'attente imprévisible due à la méthode d'accès utilisée,
    - défaillance du réseau en cas de panne du support (80% des pannes du réseau),
    - performances réduites en cas de charges importantes (bande passante partagée),

# Présentation des réseaux

## ► Topologie des réseaux

- Etoile
- Topologie physique
  - Tous les câbles sont raccordés à un point central. Ce point est habituellement un concentrateur(hub) ou un commutateur (switch).
- Topologie logique
  - Toutes les informations passent par un seul équipement, par exemple un concentrateur.



# Présentation des réseaux

## ► Topologie des réseaux

### ◦ Etoile

#### ✓ Avantages

- chaque station possède sa propre ligne: absence de collisions;
- administration du réseau facilitée grâce au nœud central;
- robustesse car pas de panne réseau en cas de défaillance des terminaux et des supports.

#### ✓ Inconvénients

- l'ajout d'un poste nécessite un lien jusqu'au serveur d'où une grande longueur de câble.
- repose entièrement sur la fiabilité du nœud central et coût élevé
- le serveur doit posséder autant de connexions qu'il y a de postes de travail (24 max.),
- la panne du serveur entraîne une paralysie totale du réseau.

# Présentation des réseaux

## ► Topologie des réseaux

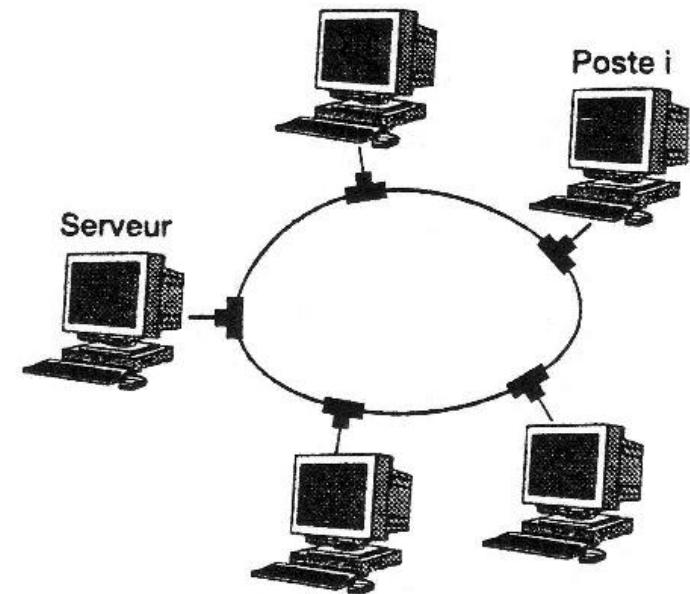
- Anneau

- Topologie physique

- Les éléments sont chaînés dans un anneau fermé..

- Topologie logique

- Les données circulent dans le même sens; ce qui évite les collisions.



Une variante de cette topologie est le double anneau où chaque hôte est connecté à 2 anneaux. Ces deux anneaux ne communiquent pas entre eux. Le deuxième anneau est utilisé comme lien redondant en cas de panne sur le premier.

# Présentation des réseaux

## ► Topologie des réseaux

### ◦ Anneau

#### ✓ Avantages

- performance fonction du nombre de nœuds et extension aisée,
- bonne performance avec une forte charge.
- le temps d'accès est déterminé (une machine sait à quel moment elle doit parler).

#### ✓ inconvénients

- rupture de l'anneau ou détection d'un nœud actif paralyse le réseau,
- les défaillances de terminaux peuvent causer une panne de réseau (récepteurs inhibés),
- doublage du support et des organes critiques pour la sécurité (courts circuits),
- chaque nœud supplémentaire dérive les performances.

# Présentation des réseaux

## ► Topologie des réseaux

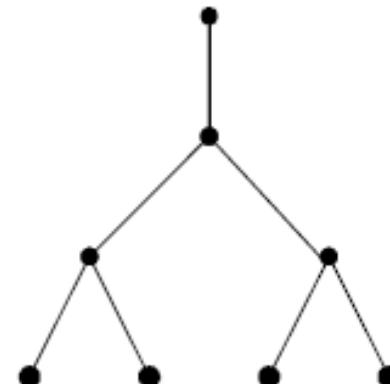
- Hiérarchique

- Topologie physique

- Cette topologie ressemble à une topologie en étoile sauf qu'elle n'utilise pas de nœud central. Elle utilise un nœud de jonction à partir duquel elle se branche vers d'autres nœuds.

- Topologie logique

- Le flux d'informations est hiérarchique



# Présentation des réseaux

## ► Topologie des réseaux

- Maillée

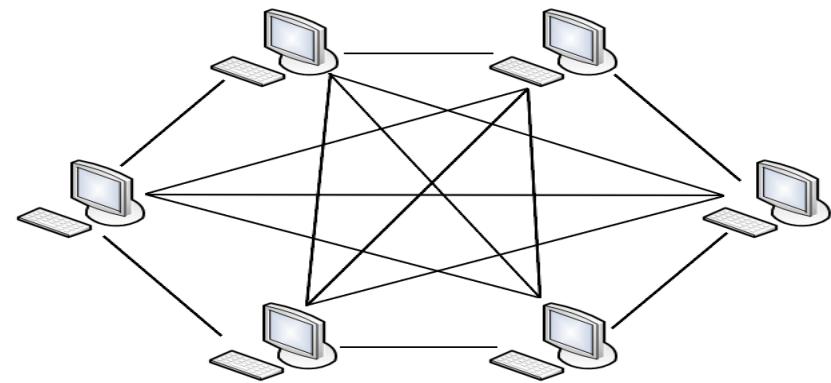
- Topologie physique

- Chaque noeud est connecté avec tous les autres.

- La formule pour connaître le nombre de câbles est  $n(n-1)/ 2$ , avec  $n$  le nombre d'ordinateurs. Donc rien qu'avec 8 ordinateurs par exemple, ça nous donnera  $8(8-1)/ 2$ , soit 28 câbles !

- Topologie logique

- Dépend des équipements utilisés



Les réseaux de zéro - siteduzero.co

Cette topologie reste peu utilisée vu la difficulté à mettre en place une telle infrastructure.

# Présentation des réseaux

## ► Typologie des réseaux

- **PAN - Personal Area Network - réseau personnel**
  - 1m,
  - liaison sans fil ordinateur/souris, clavier, imprimante...  
contrôleur d' appareil auditif, stimulateur cardiaque...
- **LAN - Local Area Network - réseau local**
  - 10m/1Km,
  - salle/immeuble/campus
- **MAN - Metropolitan Area Network – réseau métropolitain**
  - 10 Km,
  - ville

# Présentation des réseaux

## ► Typologie des réseaux

- **WAN - Wide Area Network - réseau longue distance**
  - **100Km/1000Km,**
  - **pays/continent**
- **Internet - Interréseau**
  - **10 000Km,**
  - **planète, interconnexion de réseaux**

# Principes de communication sur un réseau informatique

## ► Source canal et destination

### ◦ Message

- Ensemble d'informations qui doit être envoyé par un individu (ou un périphérique) à un autre.
- Toute forme de communication commence par un message
- Les méthodes employées pour envoyer, recevoir et interpréter un message évoluent avec les avancées technologiques.

### ◦ Eléments communs d'un moyen de communication

#### • **source du message ou l'expéditeur:**

- individus ou des périphériques électroniques qui doivent communiquer un message à d'autres individus ou périphériques

#### • **destination du message, ou son récepteur:**

- Le destinataire (ou destination) reçoit le message et l'interprète.

#### • **« canal de communication »:**

- fournit un chemin que le message empruntera pour se rendre de la source à la destination.

# Principes de communication sur un réseau informatique

## ► Règles de communication

### ◦ Protocoles

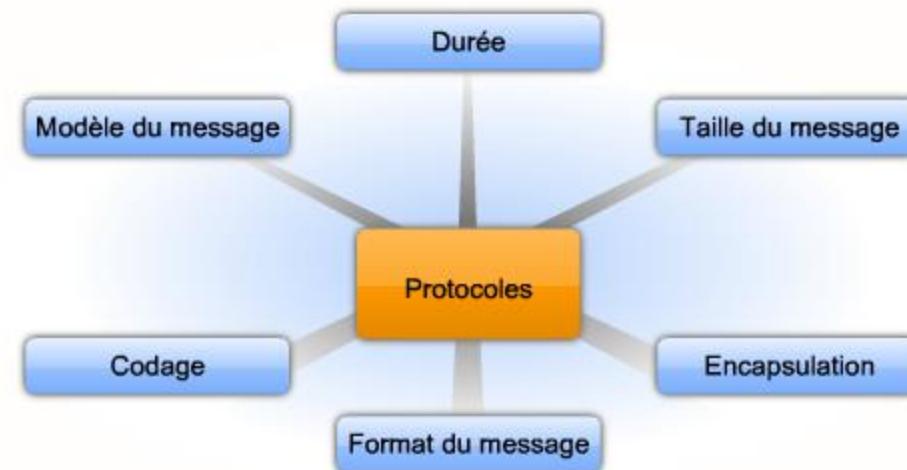
- Dans toute conversation entre deux individus, il existe de nombreuses règles (ou protocoles) que les deux doivent respecter pour que le message soit livré et compris.
- Exemples des règles:
  - l'identification de l'expéditeur et du destinataire,
  - le support ou le canal de communication convenu (face-à-face, téléphone, lettre, photo),
  - un mode de communication approprié (oral, écrit, illustré, interactif ou à sens unique),
  - une langue commune,
  - la grammaire et la syntaxe,
  - la vitesse et la date de remise du message.

# Principes de communication sur un réseau informatique

## ▶ Règles de communication

### ◦ Protocoles

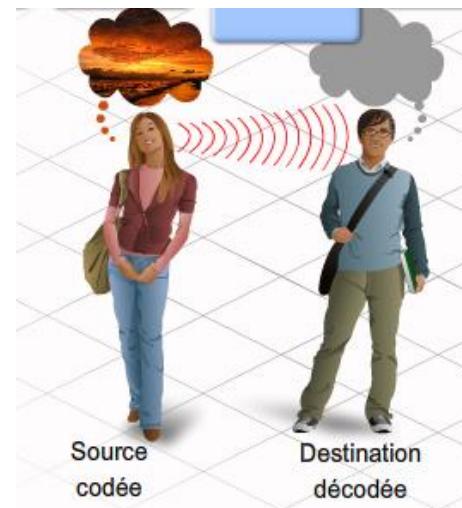
- Dépendent des caractéristiques de la source, du canal de communication et de la destination du message
- Définissent tout ce qui paramètre la façon dont un message est transmis et remis.



# Principes de communication sur un réseau informatique

## ▶ Codage des messages

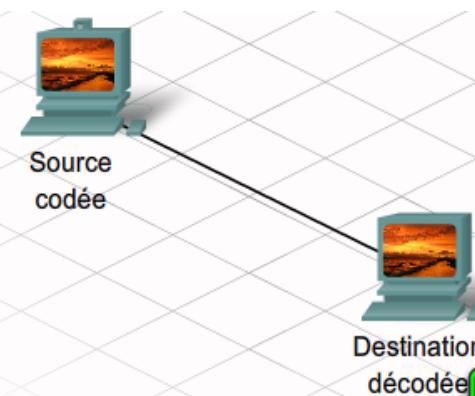
- Chez les humains
  - Codage
    - processus de conversion des pensées sous la forme d'un langage, de symboles ou de sons, en vue de leur transmission.
  - Décodage
    - processus inverse ; il permet d'interpréter ce qui est exprimé.



# Principes de communication sur un réseau informatique

## ▶ Codage des messages

- En communication informatique
  - Codage
    - Dépend du support de transmission;
    - Chaque bit émis est codé en modèle de sons, d'ondes lumineuses ou d'impulsions électriques, selon le support du réseau sur lequel les bits sont transmis.
  - Décodage
    - L'hôte de destination reçoit et décode les signaux pour interpréter le message.



# Principes de communication sur un réseau informatique

## ▶ Formatage des messages

- Lettres personnelles

- Format du contenu

- l'identification du destinataire,
    - des salutations,
    - le contenu du message,
    - une phrase de conclusion,
    - l'identification de l'expéditeur.

- Format du contenant

- L'enveloppe comporte:
    - l'adresse de l'expéditeur et celle du destinataire,
    - chacune étant écrite à l'endroit prévu.

- Encapsulation

- processus consistant à placer un format de message (la lettre) dans un autre (l'enveloppe) s'appelle « encapsulation ».
    - Une désencapsulation a lieu lorsque le processus est inversé par le destinataire et que la lettre est retirée de l'enveloppe.

ChèreJane

Je viens de revenir de voyage. J'ai pensé que tu aimerais peut-être voir mes photos.

John

Expéditeur :  
4085 SE Pine Street  
Ocala, Floride 34471



Destinataire :  
1400 Main Street  
Canton, Ohio 44203

# Principes de communication sur un réseau informatique

## ▶ Formatage des messages

- Lettres personnelles



Adresse de l'emplacement du destinataire (destination)	Adresse de l'emplacement de l'expéditeur (source)	Salutation (indicateur de début du message)	Identificateur du destinataire (destination)	Contenu de la lettre (données encapsulées)	Identificateur de l'expéditeur (source)	Fin de la trame (indicateur de fin du message)
Adressage de l'enveloppe		Lettre encapsulée				
1400 Main Street Canton, Ohio 44203	4085 SE Pine Street Ocala, Floride 34471	Chère	Jane	Je viens de revenir de voyage. J'ai pensé que tu aimerais peut-être voir mes photos.	John	

# Principes de communication sur un réseau informatique

## ▶ Formatage des messages

### ◦ Messages informatiques

- Chaque message informatique est encapsulé dans un format spécifique, appelé **trame**, avant d'être transmis au réseau.
- La trame fait office d'enveloppe.
- Elle fournit l'adresse de la destination souhaitée et celle de l'hôte source.
- Le format et le contenu de la trame sont déterminés par le type de message envoyé et par le canal sur lequel ce dernier est transmis.
- Les messages qui ne sont pas correctement formatés ne sont ni livrés ni traités par l'hôte de destination.

# Principes de communication sur un réseau informatique

## ▶ Formatage des messages

- Messages informatiques

Destination (adresse matérielle/physique)	Source (adresse matérielle/physique)	Indicateur de début (indicateur de début du message)	Destinataire (identificateur de destination)	Expéditeur (identificateur de la source)	Données encapsulées (bits)	Fin de la trame (indicateur de fin du message)
Adressage des trames		Message encapsulé				

# Principes de communication sur un réseau informatique

## ▶ Taille des messages

- Communications humaines
  - Une conversation personnelle peut être composée de plusieurs petites phrases pour que chaque partie du message soit reçue et comprise.
- Communications informatiques
  - Les restrictions en termes de taille des trames requièrent de l'hôte source qu'il décompose les longs messages en parties répondant aux impératifs de taille maximale.
  - Les règles qui régissent la taille des parties ou « trames » transmises au réseau sont très strictes.
    - Les trames trop longues ou trop courtes ne sont pas livrées.
  - Chaque partie est encapsulée dans une trame distincte, avec les informations d'adresse, puis est transmise au réseau
  - Au niveau de l'hôte destinataire, les messages sont désencapsulés et recomposés pour être traités et interprétés.

# Principes de communication sur un réseau informatique

## ► Synchronisation des messages

- - Utilisée pour déterminer le moment de la prise de parole (**méthode d'accès**), le débit de la parole (**contrôle de flux**) et le temps d'attente d'une réponse.
  - Méthode d'accès
    - Les hôtes d'un réseau ont besoin d'une méthode d'accès pour savoir à quel moment ils doivent commencer à envoyer des messages pour éviter des collisions.
  - Contrôle de flux
    - La synchronisation affecte également la quantité d'informations à envoyer, ainsi que leur vitesse de livraison.
    - il arrive que l'hôte émetteur transmette des messages plus rapidement que l'hôte de destination ne peut en recevoir et traiter. L'hôte de destination doit demander à l'hôte source de diminuer la vitesse d'envoi
  - Délai d'attente de réponse
    - Les hôtes du réseau sont également soumis à des règles qui spécifient le délai d'attente de réponses et l'action à entreprendre en cas de délai d'attente dépassé

# Principes de communication sur un réseau informatique

- ▶ **Modèles de message**
  - **Monodiffusion**
    - Un modèle de message un à un est appelé monodiffusion, ce qui signifie qu'il n'existe qu'une seule destination pour le message.
  - **Multidiffusion**
    - Lorsqu'un hôte doit envoyer des messages à l'aide d'un modèle un à plusieurs, il est appelé multidiffusion. La multidiffusion est la livraison simultanée du même message à un groupe d'hôtes de destination.
  - **Diffusion**
    - Si tous les hôtes du réseau doivent recevoir le message en même temps, une diffusion est utilisée. La diffusion représente un modèle de message un à tous. De plus, les hôtes requièrent des messages avec accusés de réception.

# Communication via un réseau local câblé

## ▶ Importance des protocoles

- Dans un environnement câblé, un réseau local se définit comme une zone où tous les hôtes doivent « parler la même langue » ou, en termes informatiques, « partager un protocole commun ».
- Le protocole définit de nombreux aspects de la communication sur le réseau local, dont : le format et la taille des messages, la synchronisation, le codage et les modèles des messages.

# Communication via un réseau local câblé

## ► Normalisation des protocoles

- Définition

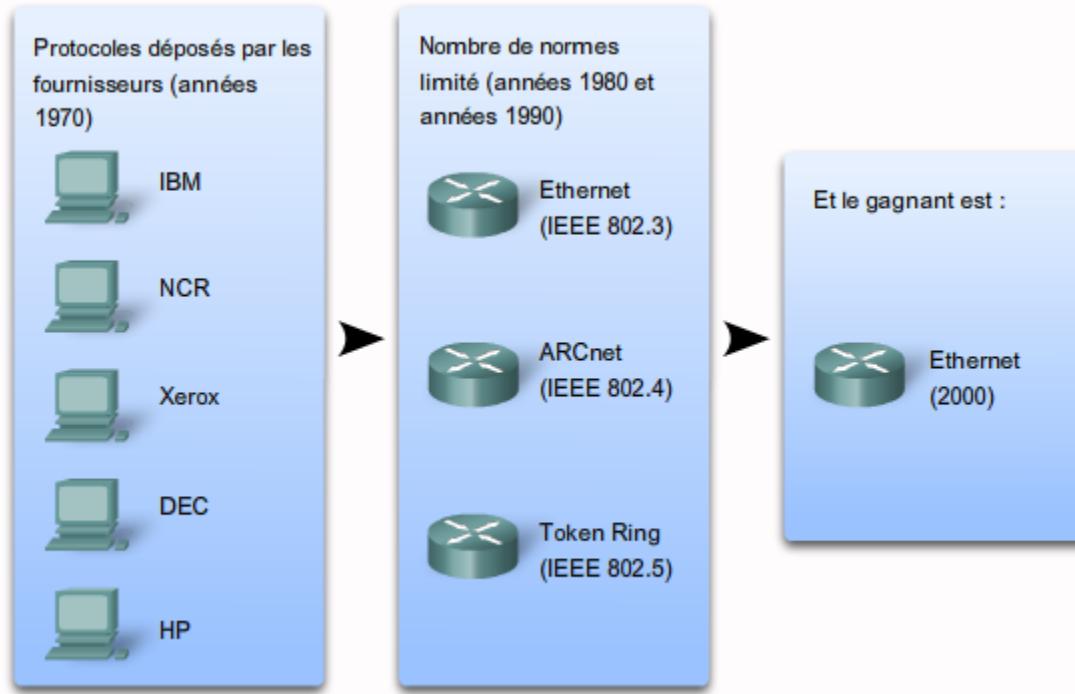
- Normes = protocoles standard
- établie pour définir des règles d'utilisation des périphériques réseau de différents fournisseurs.

- Avantages

- facilitent la conception,
- simplifient le développement de produits,
- incitent à la concurrence,
- fournissent des interconnexions cohérentes,
- facilitent la formation,
- fournissent aux clients un plus grand choix de fournisseurs.

# Communication via un réseau local câblé

- ▶ Normalisation des protocoles
  - Normes des réseaux locaux



# Communication via un réseau local câblé

## ▶ Normalisation des protocoles

### ○ IEEE

- L'IEEE (Institute of Electrical and Electronic Engineers) gère les normes relatives aux réseaux, y compris Ethernet, ainsi que les normes de la technologie sans fil.
- Les comités IEEE approuvent et tiennent à jour les normes relatives
  - aux connexions,
  - aux supports requis
  - et aux protocoles de communication
- Le comité responsable des normes Ethernet est le 802.3.
- Chaque version d'Ethernet comporte une norme.
  - Par exemple, 802.3 100BASE-T
    - 100 est la vitesse en Mbit/s.
    - BASE désigne la transmission de la bande de base.
    - T désigne le type de câble, dans ce cas, les paires torsadées.

# Communication via un réseau local câblé

## ► Adressage physique

- Toutes les formes de communication nécessitent un moyen d'identifier la source et la destination.
- **Communication humaine:**
  - la source et la destination sont représentées par des noms.
  - Lorsqu'un nom est prononcé, la personne qui le porte écoute le message et y répond. Les autres personnes présentes dans la pièce peuvent entendre le message, mais l'ignorent car il ne leur est pas adressé.

# Communication via un réseau local câblé

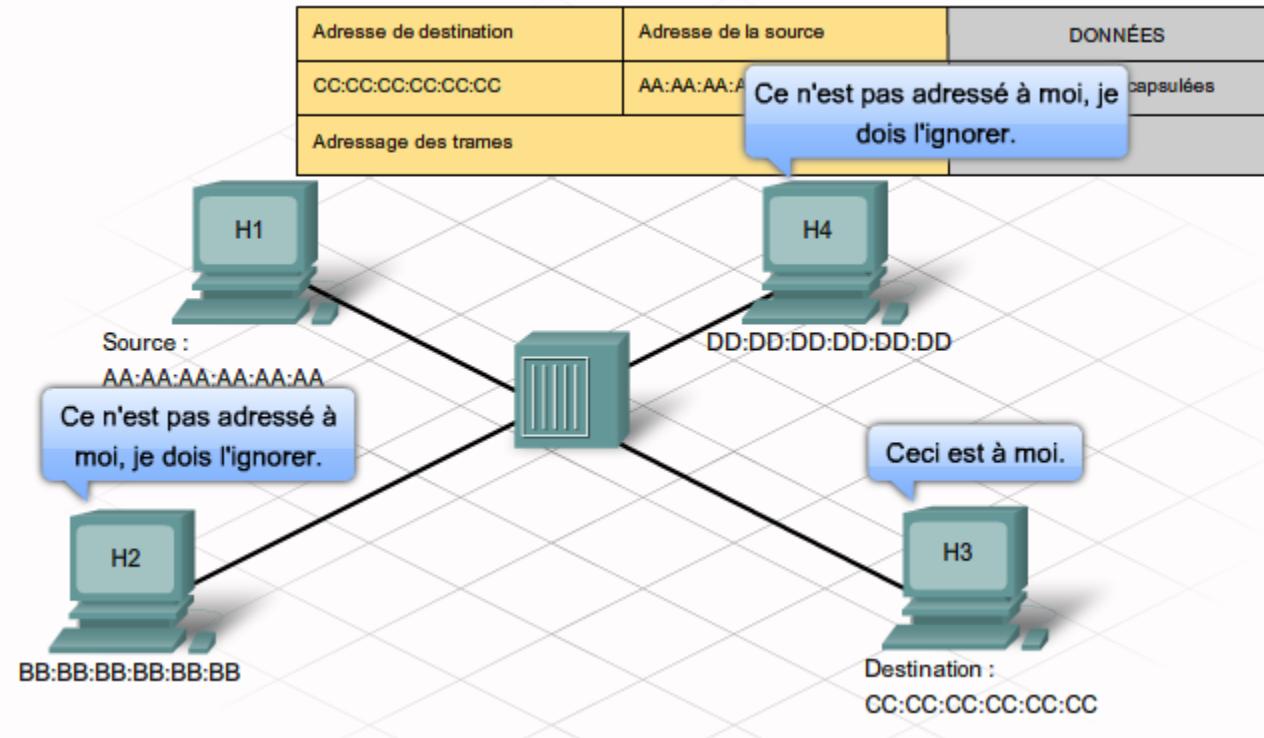
## ▶ Adressage physique

### ◦ Réseaux Ethernet:

- Chaque hôte connecté à un réseau Ethernet possède une adresse physique qui sert à identifier l'hôte sur le réseau.
- Chaque interface réseau Ethernet est dotée d'une adresse physique qui lui est attribuée lors de sa fabrication. Il s'agit de l'adresse **MAC** (**Media Access Control**).
- L'hôte source envoie des trames contenant sa propre adresse MAC comme source, ainsi que l'adresse MAC du destinataire souhaité.
- Les hôtes qui reçoivent la trame la décodent et lisent l'adresse MAC de destination.
  - Si l'adresse MAC de destination correspond à celle de la carte réseau, elle traite le message et l'enregistre pour que l'application hôte puisse l'utiliser
  - Sinon, la carte réseau ignore le message.

# Communication via un réseau local câblé

- ▶ Adressage physique
  - Réseaux Ethernet:



# Communication via un réseau local câblé

- ▶ **Adressage physique**
  - Travaux pratiques: détermination de l'adresse MAC de votre ordinateur

# Communication via un réseau local câblé

## ▶ Communication Ethernet

- Format de la trame Ethernet

Préambule	SFD	Adresse MAC de destination	Adresse MAC source	Longueur/Type	Données encapsulées	Séquence de contrôle de trame (FCS)
7	1	6	6	2	De 46 à 1500	4

- 
- **SFD, délimiteur du début de trame:** marque la fin des informations de durée et le démarrage de la trame;
- **Champ Longueur/Type**
  - Le Type indique le protocole qui reçoit les données
  - La Longueur indique le nombre d'octets de données qui suivent ce champ
  - la séquence de contrôle des trames, pour détecter les erreurs de transmission.

# Communication via un réseau local câblé

## ▶ Communication Ethernet

- Tailles des trames Ethernet
  - La taille des trames Ethernet doit être comprise entre 64 et 1518 octets. Les trames qui n'entrent pas dans ces limites ne sont pas traitées par les hôtes récepteurs

# Communication via un réseau local câblé

## ▶ Structure hiérarchique des réseaux Ethernet

- Il s'agit de plusieurs petits groupes plus gérables qui permettent au trafic local de rester local. Seul le trafic destiné aux autres réseaux est déplacé vers une couche supérieure.
- Une structure de couches hiérarchiques permet d'optimiser l'efficacité, la vitesse et les performances des réseaux. Elle permet aux réseaux d'évoluer selon les besoins, dans la mesure où il est possible d'ajouter des réseaux locaux sans amoindrir les performances des réseaux existants.

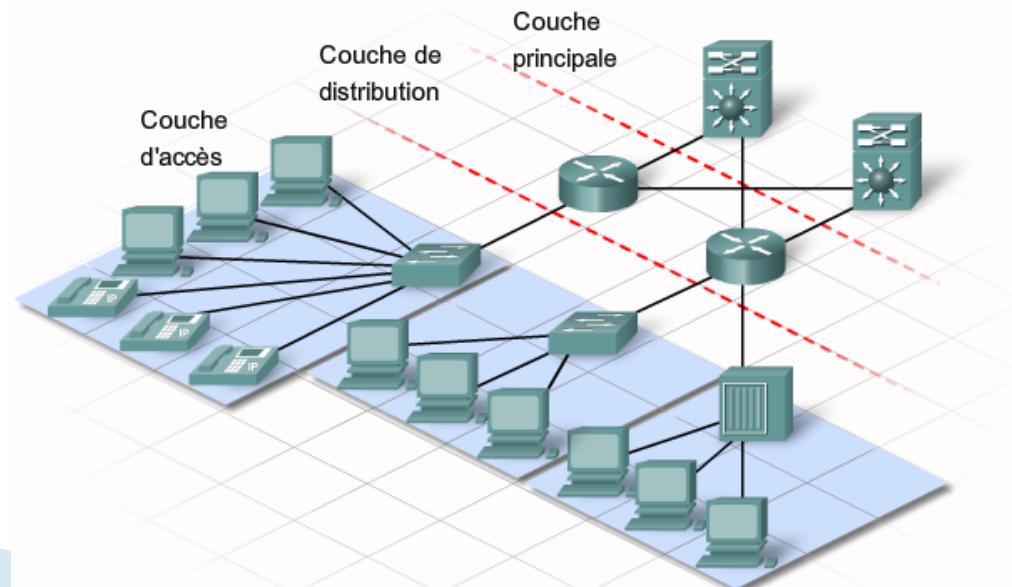
# Communication via un réseau local câblé

## ▶ Structure hiérarchique des réseaux Ethernet

La structure hiérarchique comporte trois couches de base :

- **Couche d'accès** : fournit des connexions aux hôtes sur un réseau Ethernet local.
- **Couche de distribution** : permet d'interconnecter les petits réseaux locaux.
- **Couche cœur de réseau** : connexion haut débit entre les périphériques de la couche de distribution.

Avec cette nouvelle structure hiérarchique, un système d'adressage logique est nécessaire pour identifier l'emplacement d'un hôte. Il s'agit du système d'adressage IP (Internet Protocol).



# Communication via un réseau local câblé

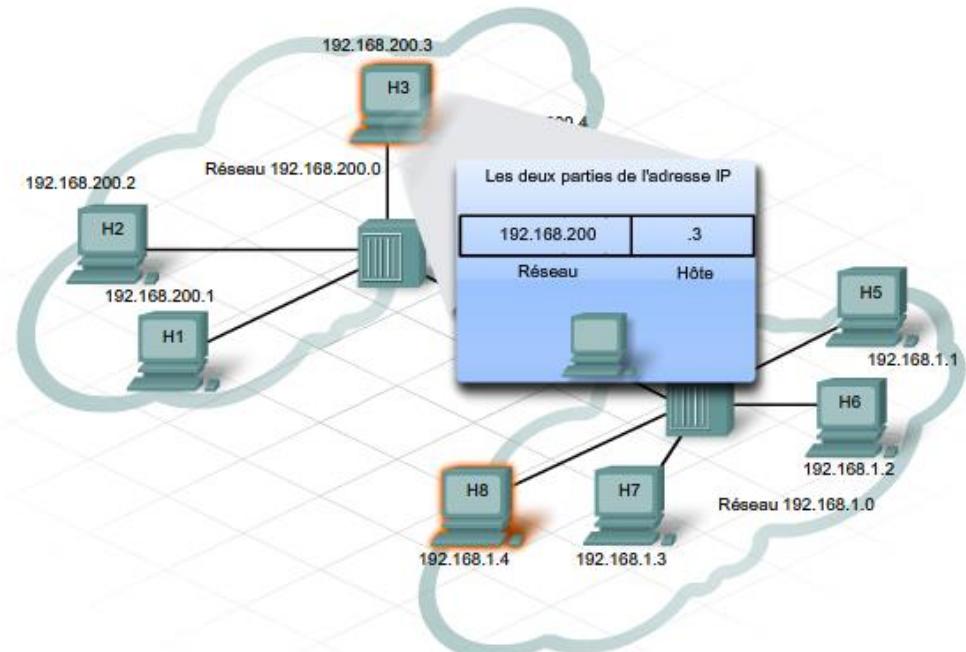
## ► Adressage logique

- En règle générale, une personne ne change pas de nom. En revanche, son adresse postale peut changer. Sur un hôte, l'adresse MAC ne change pas. Elle est physiquement attribuée à la carte réseau de l'hôte et est désignée sous le terme d'adresse physique. L'adresse physique reste la même, quel que soit l'emplacement de l'hôte sur le réseau.
- L'adresse IP est similaire à l'adresse d'une personne. Elle est appelée adresse logique car elle est affectée de façon logique, en fonction de l'emplacement de l'hôte. L'adresse IP ou adresse réseau est attribuée à chaque hôte par un administrateur réseau, selon le réseau local.

# Communication via un réseau local câblé

## ► Adressage logique

Les adresses IP se composent de deux parties. *Une partie identifie le réseau local.* La partie réseau de l'adresse IP est la même pour tous les hôtes connectés à un réseau local. *La deuxième partie de l'adresse IP identifie l'hôte individuel.* Dans le même réseau local, la partie hôte de l'adresse IP est unique pour chaque hôte.

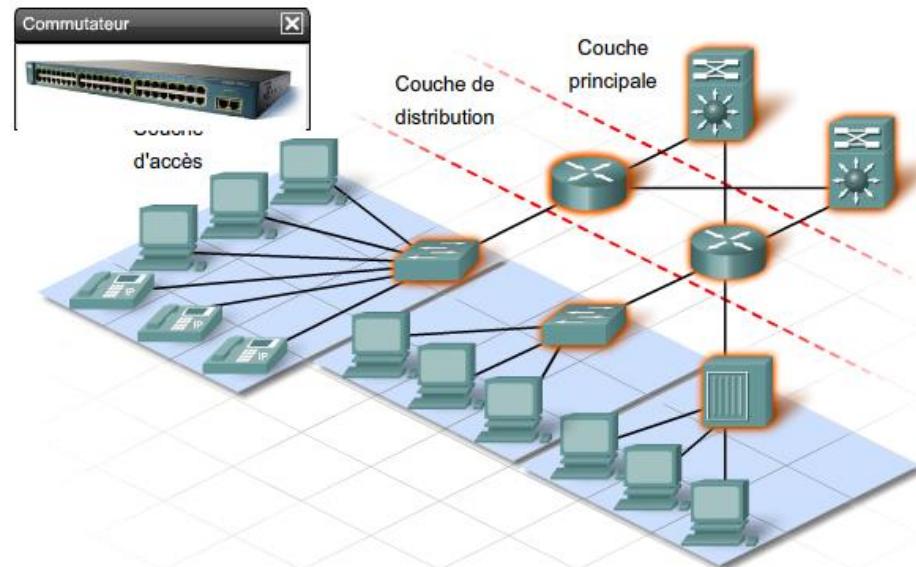


L'adresse MAC physique et l'adresse IP logique sont toutes deux requises pour que l'ordinateur communique sur un réseau hiérarchique, tout comme le nom et l'adresse d'une personne le sont pour envoyer une lettre.

# Communication via un réseau local câblé

- ▶ Périphériques et couches d'accès/de distribution
  - Couche d'accès

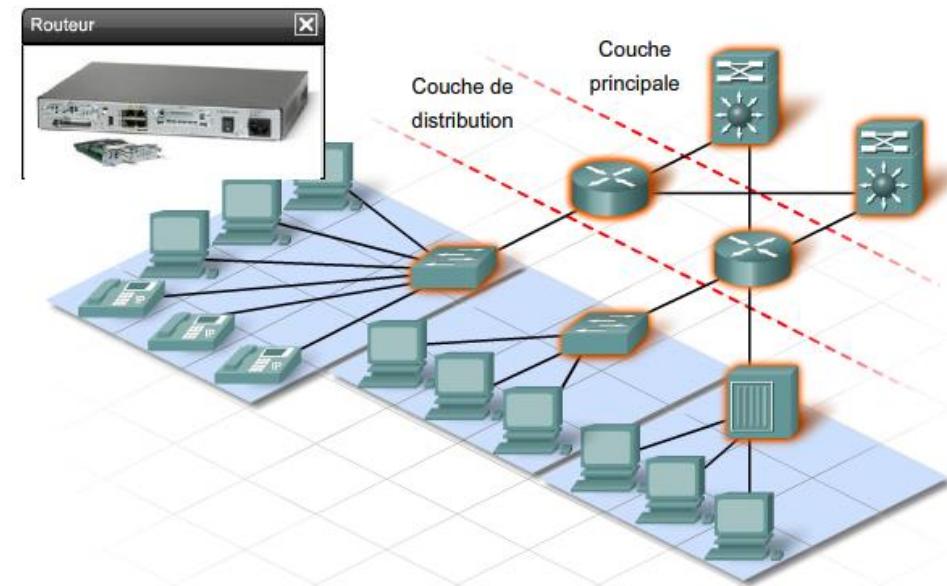
La couche d'accès fournit un point de connexion au réseau pour les périphériques des utilisateurs et permet à plusieurs hôtes de se connecter à d'autres, via un périphérique réseau (en principe un concentrateur ou un commutateur). En règle générale, tous les périphériques d'une seule couche d'accès ont, dans leur adresse IP, la même partie réseau.



# Communication via un réseau local câblé

- ▶ Périphériques et couches d'accès/de distribution
  - Couche de distribution

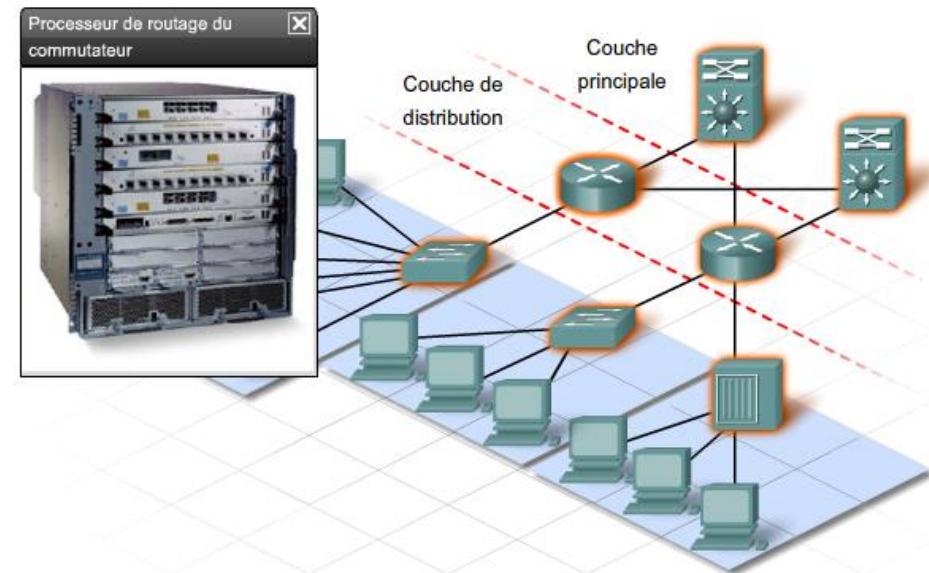
La couche de distribution établit un point de connexion pour les réseaux distincts et contrôle le flux d'informations entre eux. Elle comprend généralement des commutateurs plus puissants que ceux de la couche d'accès, ainsi que des routeurs pour le routage entre les réseaux.



# Communication via un réseau local câblé

- ▶ Périphériques et couches d'accès/de distribution
  - Couche principale (ou cœur)

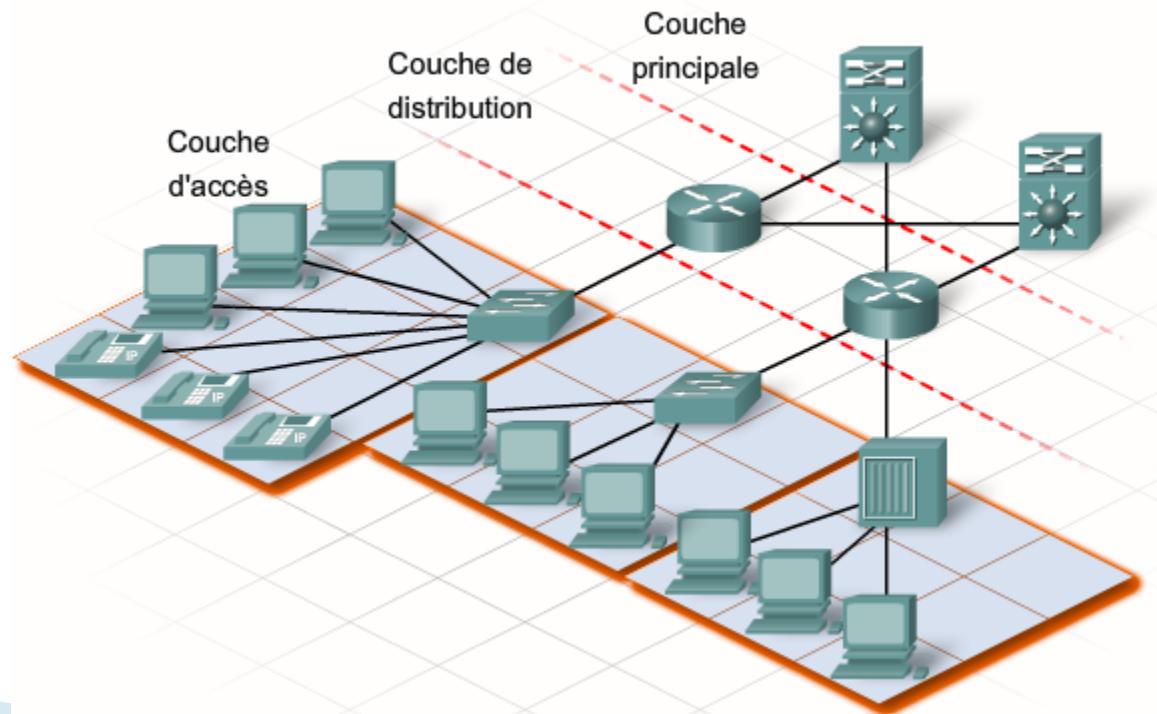
La couche principale est une couche fédératrice haut débit avec des connexions redondantes (de sauvegarde). Elle permet le transport de grandes quantités de données entre plusieurs réseaux finaux. Les périphériques de la couche principale comprennent en général des commutateurs et des routeurs haut débit, très puissants. La première fonction de la couche principale est de transporter rapidement les données.



# Création de la couche d'accès d'un réseau Ethernet

## ▶ Couche d'accès

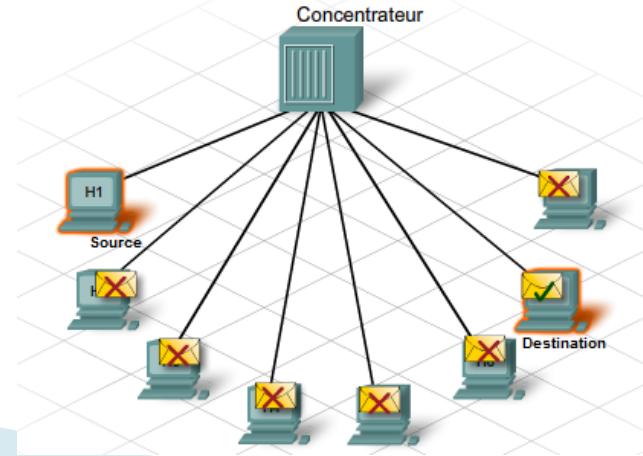
Plusieurs types de périphériques réseau permettent de connecter des hôtes au niveau de la couche d'accès, y compris des commutateurs et des concentrateurs Ethernet



# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des concentrateurs

- Les concentrateurs sont dotés de plusieurs ports, utilisés pour connecter les hôtes au réseau
- Ils ne peuvent pas déterminer les hôtes qui doivent recevoir un message particulier.
- Un concentrateur reçoit tout simplement les signaux électroniques d'un port et génère de nouveau (ou répète) le même message pour tous les autres ports.
- Les hôtes ignorent les messages qui ne leur sont pas adressés. Seul l'hôte spécifié dans l'adresse de destination du message traite le message et répond à l'expéditeur.
  - Un seul message à la fois peut être envoyé via un concentrateur Ethernet.



# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des concentrateurs

### ◦ Collision

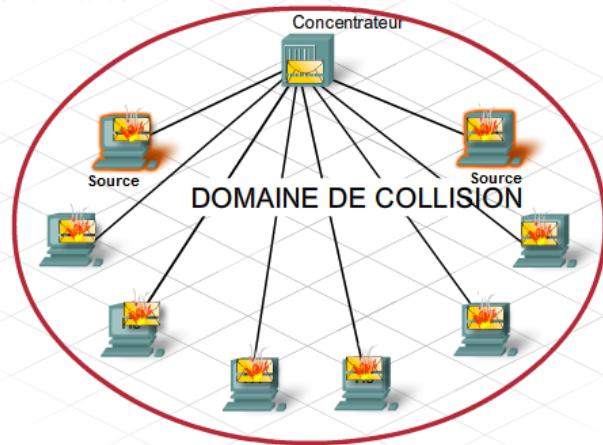
- Deux ou plusieurs hôtes connectés à un concentrateur peuvent tenter d'envoyer simultanément un message. Si c'est le cas, les signaux électroniques qui composent les messages entrent en collision au niveau du concentrateur.
- Si deux ou plusieurs hôtes connectés à un concentrateur envoient simultanément un message, les signaux électroniques qui composent les messages entrent en collision au niveau du concentrateur.
- Un concentrateur ne décode pas les messages. Par conséquent, il ne détecte pas que le message est endommagé et le répète sur tous les ports.

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des concentrateurs

### ◦ Domaine de collision

- La zone du réseau où l'hôte peut recevoir un message endommagé suite à une collision est appelée un domaine de collision.



- Au sein d'un domaine de collision, lorsqu'un hôte reçoit un message endommagé, il détecte qu'une collision s'est produite. Chaque hôte émetteur attend un laps de temps, puis tente d'envoyer ou de transmettre à nouveau le message. Plus le nombre d'hôtes connectés au concentrateur est important, plus les risques de collisions augmentent. Un grand nombre de collisions entraîne de nombreuses retransmissions. Un nombre excessif de retransmissions peut paralyser le réseau et ralentir le trafic. C'est pour cette raison qu'il est nécessaire de limiter la taille d'un domaine de collision.

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des concentrateurs

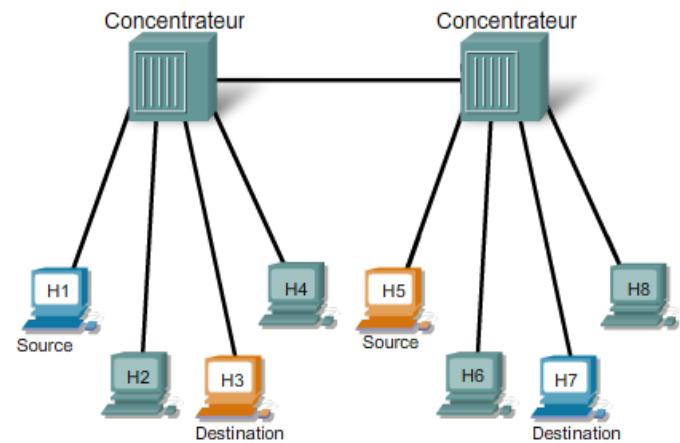
### ○ Exercices

Si l'hôte 3 envoie un message à l'hôte 6, quels périphériques hôtes reçoivent le message ?

- L'hôte 6 uniquement.
- Tous les hôtes sont connectés au concentrateur A uniquement.
- Tous les hôtes sont connectés au concentrateur B uniquement.
- Tous les hôtes sur le réseau.

Sur ce réseau, combien existe-t-il de domaines de collision ?

- Il y a 1 domaine de collision.
- Il y a 2 domaines de collision.
- Il y a 8 domaines de collision.
- Il n'y a pas de domaine de collision.



# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des commutateurs

- Contrairement au concentrateur, le commutateur peut transférer un message vers un hôte particulier. Lorsqu'un hôte envoie un message à un autre hôte sur le commutateur, ce dernier accepte et décode les trames pour lire la partie adresse physique (MAC) du message.
- Sur le commutateur, une table, appelée « table d'adresses MAC », contient une liste de tous les ports actifs et des adresses MAC hôtes correspondantes
- Lorsqu'un message est envoyé entre les hôtes, le commutateur vérifie si l'adresse MAC de destination est dans la table.
  - Si c'est le cas, le commutateur établit une connexion temporaire, appelée circuit, entre les ports source et de destination. Ce nouveau circuit fournit un canal dédié sur lequel les deux hôtes peuvent communiquer. Les autres hôtes reliés au commutateur ne partagent pas la bande passante sur ce canal et ne reçoivent pas les messages qui ne leur sont pas adressés

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des commutateurs

- Crédit de la table MAC

- Un commutateur crée la table d'adresses MAC en examinant l'adresse MAC source de chaque trame qui est envoyée entre les hôtes. Lorsqu'un nouvel hôte envoie un message ou répond à un message diffusé, le commutateur enregistre immédiatement son adresse MAC et le port auquel l'hôte est connecté. La table est mise à jour de manière dynamique chaque fois que le commutateur lit une nouvelle adresse MAC source. De cette manière, un commutateur enregistre rapidement les adresses MAC de tous les hôtes connectés.

Table MAC

fa0/1	fa0/2	fa0/3	fa0/4
260d.8c01.0000	260d.8c01.1111	260d.8c01.2222	260d.8c01.3333
fa0/5	fa0/6	fa0/7	fa0/8
260d.8c01.4444	260d.8c01.5555	260d.8c01.6666	260d.8c01.7777

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des commutateurs

- Connexion d'un concentrateur à un port de commutateur

### Objectif

- augmenter le nombre d'hôtes pouvant être connectés au réseau.

### Table d'adresse MAC

- le commutateur associe les adresses MAC de tous les hôtes connectés à ce concentrateur au port unique du commutateur.
- Lorsqu'un hôte du concentrateur connecté envoie un message à un autre hôte connecté au même concentrateur, le commutateur rejette le message.

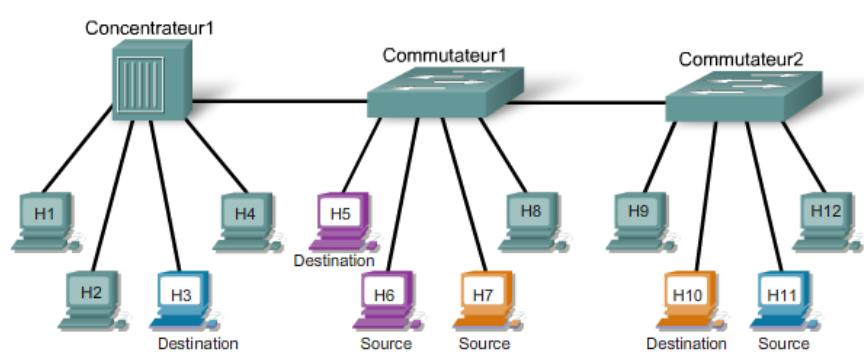
### Domaine de collision

- En cas de collision sur le concentrateur, le commutateur reçoit le message altéré, mais contrairement à un concentrateur, un commutateur ne transfère pas les messages endommagés suite à des collisions.
- Par conséquent, chacun des ports d'un commutateur crée un domaine de collision distinct.
- Moins le nombre d'hôtes est important dans un domaine de collision, moins le risque de collision est élevé.

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Fonction des commutateurs

- Exercice



Si l'hôte 9 envoie un message à l'hôte 6 et que l'adresse MAC de destination se trouve dans la table MAC pour le commutateur 1 et le commutateur 2, quels périphériques hôtes reçoivent le message ?

- Seulement l'hôte 6
- Tous les hôtes connectés au commutateur 1
- Tous les hôtes connectés au concentrateur 1 et les hôtes connectés au commutateur 1
- Tous les hôtes sur le réseau

Sur ce réseau, combien existe-t-il de domaines de collision ?

- Il y a 1 domaine de collision.
- Il y a 2 domaines de collision.
- Il y a 3 domaines de collision.
- Il y a 10 domaines de collision.
- Il y a 12 domaines de collision.

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Messagerie de diffusion

### Définition

- Envoyer un message à tous les hôtes d'un réseau local

### Causes

- lorsqu'un hôte doit trouver des informations sans savoir exactement ce qu'un autre hôte peut lui fournir,
- ou lorsqu'un hôte souhaite fournir rapidement des informations à tous les autres hôtes sur le même réseau.

### Adresse MAC de diffusion

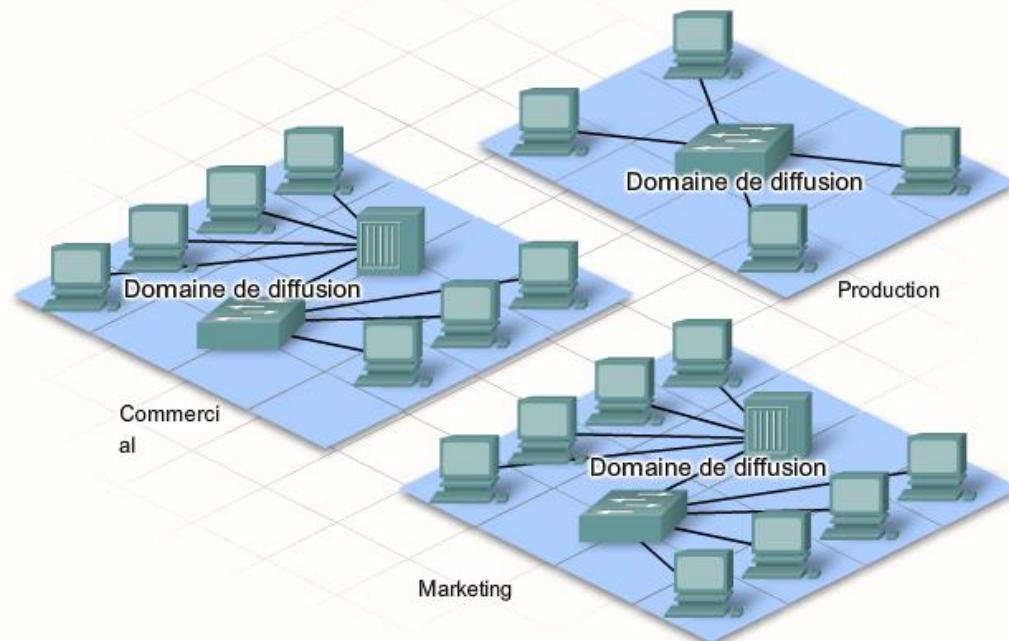
- L'adresse MAC de diffusion en notation hexadécimale est FFFF.FFFF.FFFF.

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Messagerie de diffusion

### Domaine de diffusion

- Lorsqu'un hôte envoie un message de diffusion, les concentrateurs et les commutateurs acheminent le message jusqu'à chaque hôte connecté sur le même réseau local. Par conséquent, un réseau local est également appelé **domaine de diffusion**.



# Création de la couche d'accès d'un réseau Ethernet

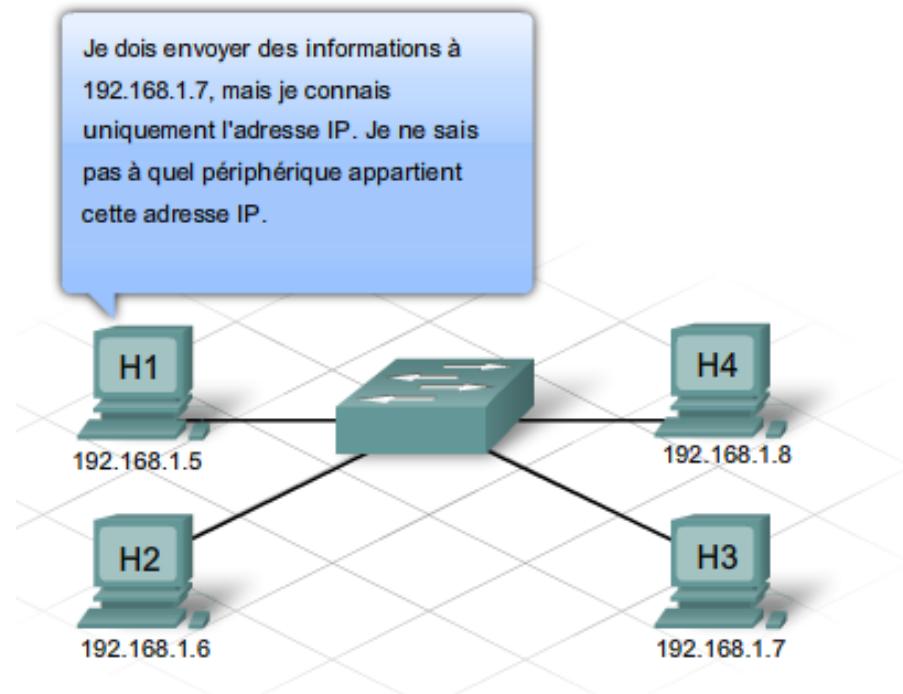
## ▶ Messagerie de diffusion

### Domaine de diffusion

- Si les hôtes connectés au même domaine de diffusion sont trop nombreux, le trafic de diffusion peut devenir disproportionné.
- Au fur et à mesure que le réseau s'étend et que d'autres hôtes sont ajoutés, le trafic du réseau, notamment le trafic de diffusion, augmente. Il est souvent nécessaire de scinder un réseau local, ou un domaine de diffusion, en plusieurs réseaux afin d'améliorer ses performances.

# Création de la couche d'accès d'un réseau Ethernet

## ▶ Protocole ARP (Adress Resolution Protocol)

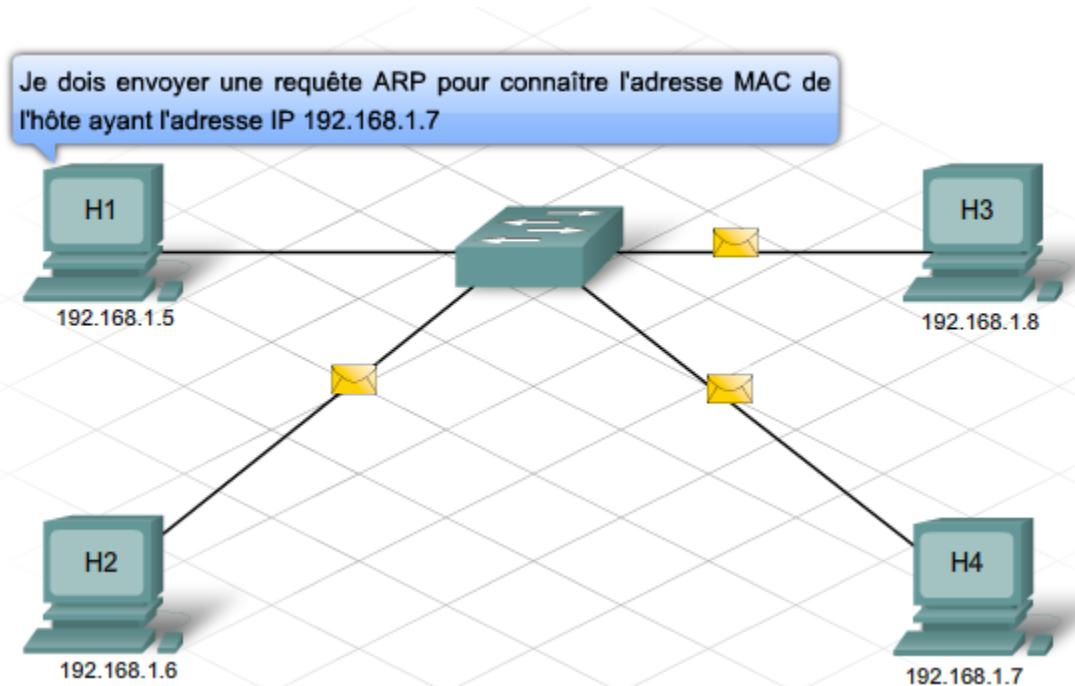


L'hôte émetteur peut utiliser un protocole IP appelé « protocole ARP » pour connaître l'adresse MAC d'un hôte sur le même réseau local.

# Création de la couche d'accès d'un réseau Ethernet

- ▶ Protocole ARP (Adress Resolution Protocol)
  - Fonctionnement

**Etape 1:** L'hôte émetteur crée et envoie une trame adressée à une adresse MAC de diffusion. La trame contient un message avec l'adresse IP de l'hôte de destination souhaité.

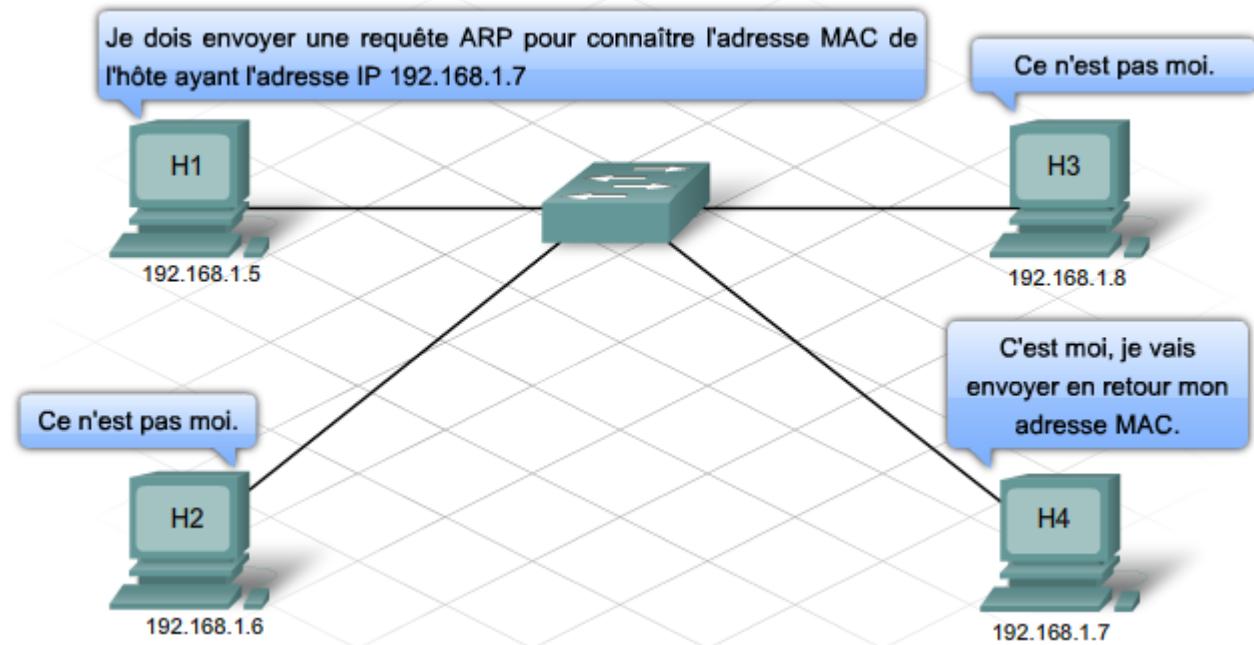


# Création de la couche d'accès d'un réseau Ethernet

## ▶ Protocole ARP (Address Resolution Protocol)

- Fonctionnement

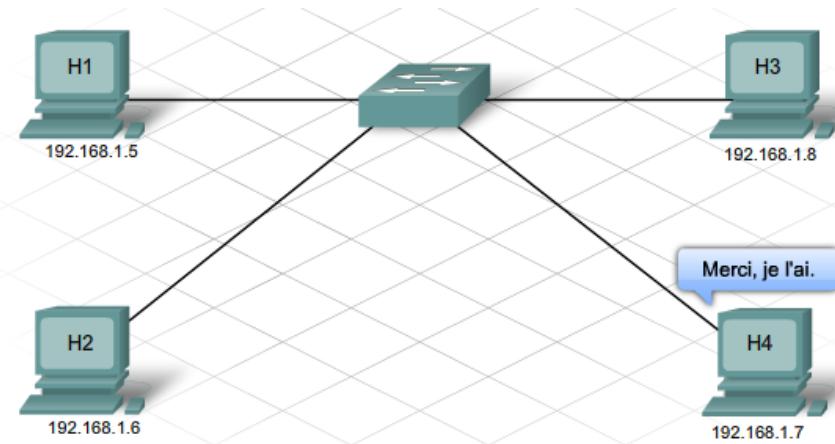
**Etape 2:** Chaque hôte du réseau reçoit la trame de diffusion et compare l'adresse IP du message à son adresse IP configurée. L'hôte dont l'adresse IP correspond renvoie son adresse MAC à l'hôte émetteur initial.



# Création de la couche d'accès d'un réseau Ethernet

- ▶ Protocole ARP (Adress Resolution Protocol)
  - Fonctionnement

**Etape 3:** L'hôte émetteur reçoit le message et enregistre l'adresse MAC et l'adresse IP dans une table appelée « table ARP ».



Une fois que l'hôte émetteur dispose de l'adresse MAC de l'hôte de destination dans sa table ARP, il peut envoyer directement des trames à l'adresse de destination, sans effectuer de requête ARP.

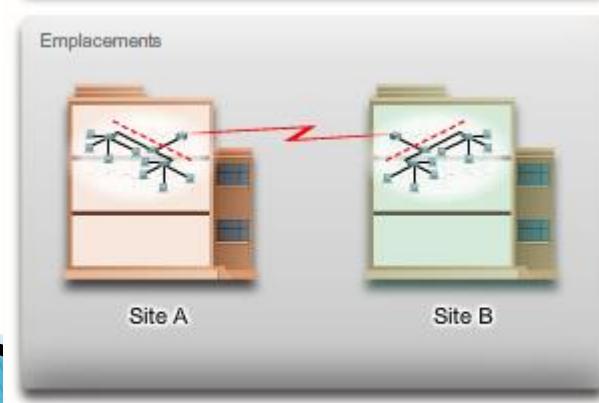
# Création de la couche de distribution du réseau

## ▶ Couche de distribution

- Segmenter un réseau local de couche d'accès

Au fur et à mesure de l'extension des réseaux, il est souvent nécessaire de diviser un réseau local en plusieurs réseaux de couche d'accès. Les réseaux peuvent être divisés en fonction de plusieurs critères, notamment les suivants :

### L'emplacement physique

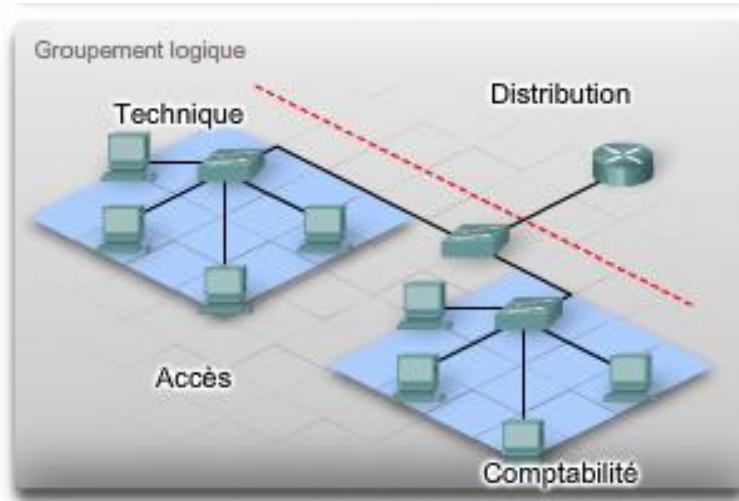


Les routeurs de la couche de distribution peuvent servir à relier des réseaux locaux à plusieurs endroits d'une entreprise séparée au niveau géographique.

# Création de la couche de distribution du réseau

- ▶ **Couche de distribution**
  - Segmenter un réseau local de couche d'accès

## □ La fonction logique

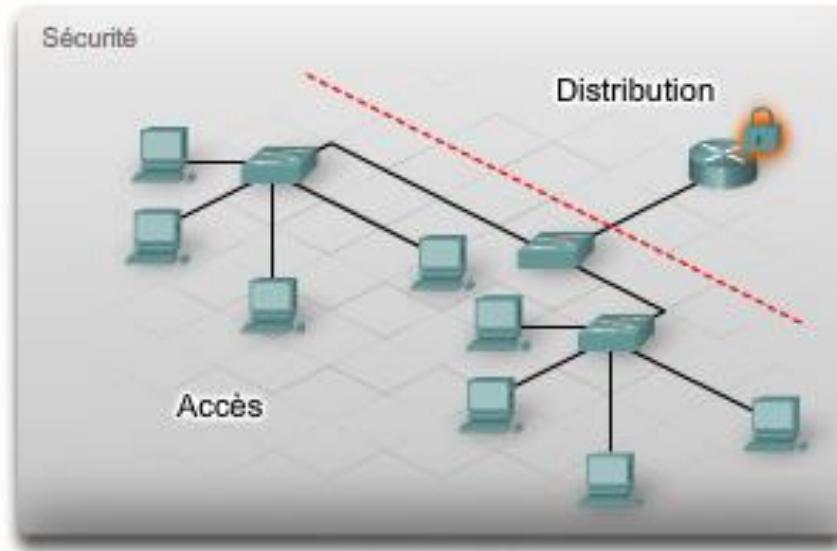


Les routeurs de la couche de distribution peuvent servir à grouper des utilisateurs d'une façon logique, tels les services d'une entreprise, qui ont des besoins communs ou qui doivent accéder à des ressources.

# Création de la couche de distribution du réseau

- ▶ **Couche de distribution**
  - Segmenter un réseau local de couche d'accès

## □ les besoins en matière de sécurité

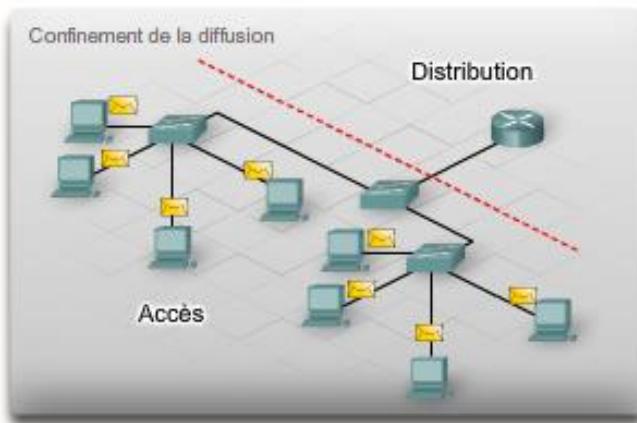


Les routeurs de la couche de distribution peuvent séparer et protéger certains groupes d'ordinateurs où se trouvent des informations confidentielles. Les routeurs peuvent également masquer les adresses des ordinateurs internes à partir de l'extérieur pour permettre d'éviter les attaques et pour contrôler qui peut entrer et sortir du réseau local.

# Création de la couche de distribution du réseau

- ▶ Couche de distribution
  - Segmenter un réseau local de couche d'accès

## □ Le confinement de la diffusion



Les routeurs de la couche de distribution peuvent limiter les diffusions au réseau local où elles doivent être entendues. Bien que les diffusions soient nécessaires, trop d'hôtes reliés sur le même réseau local peut générer un trafic de diffusion excessif et ralentir le réseau.

## □ les besoins en matière d'applications.

# Création de la couche de distribution du réseau

## ▶ Couche de distribution

### ◦ Rôle de la couche de distribution

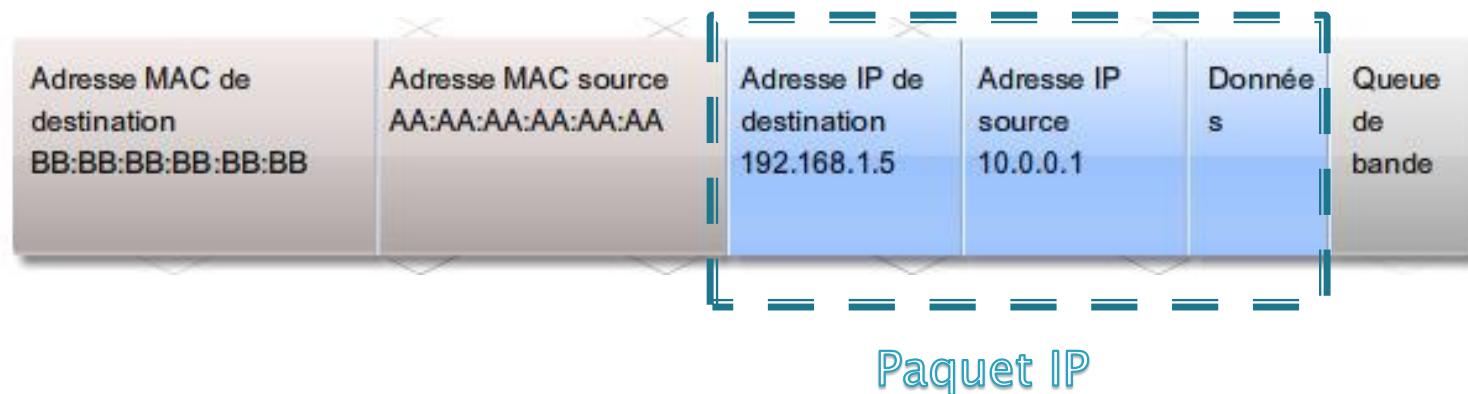
- connecte ces réseaux locaux indépendants et contrôle le trafic entre eux.
- garantir que le trafic entre les hôtes du réseau local reste local. Seul le trafic destiné à d'autres réseaux est transmis.
- filtrer le trafic entrant et sortant pour la sécurité et la gestion du trafic.

### ◦ Périphériques de la couche de distribution

- Les périphériques de la couche d'accès sont connectés les uns aux autres via les périphériques de la couche de distribution, tels que les routeurs.

# Création de la couche de distribution du réseau

- ▶ Fonction des routeurs
  - Paquet IP encapsulé dans la trame



Le format de paquet contient les adresses IP des hôtes source et de destination, ainsi que les données des messages qu'ils s'envoient.

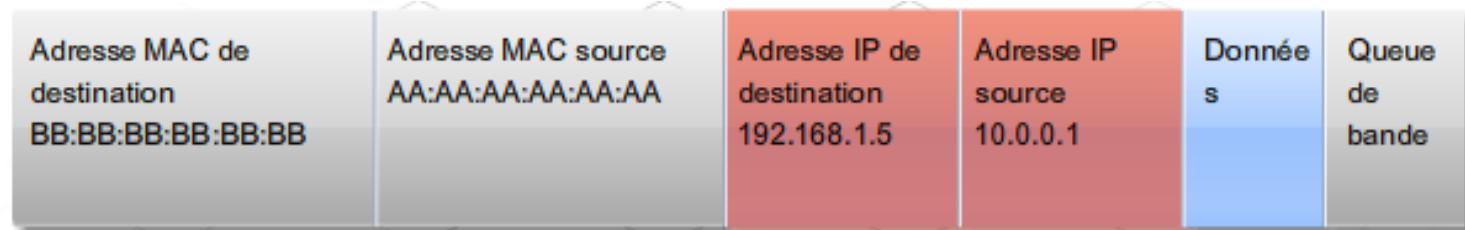
# Création de la couche de distribution du réseau

## ▶ Fonction des routeurs

- Comment sont utilisés les adresses MAC et IP



Un commutateur examine les adresses MAC.



Un routeur examine les adresses IP.

# Création de la couche de distribution du réseau

## ▶ Fonction des routeurs

- Utilisation du routeur

Un routeur est un périphérique réseau qui connecte un réseau local à d'autres réseaux locaux.

les routeurs décodent le paquet encapsulé dans la trame. Le routeur lit la partie réseau de l'adresse IP de destination et l'utilise pour déterminer le réseau connecté qui est le plus intéressant pour envoyer le message vers sa destination. À chaque fois que la partie réseau des adresses IP des hôtes source et de destination ne correspond pas, un routeur doit être utilisé pour acheminer le message.

Le routeur reçoit le message et le décapsule pour lire l'adresse IP de destination. Il détermine ensuite l'emplacement vers lequel le message doit être acheminé. Il encapsule à nouveau le paquet en une trame et achemine la trame jusqu'à sa destination.

# Création de la couche de distribution du réseau

- ▶ **Fonction des routeurs**
  - Utilisation du routeur
    - TP: adressage IP et communication réseau

# Création de la couche de distribution du réseau

## ▶ Fonction des routeurs

- Table de routage

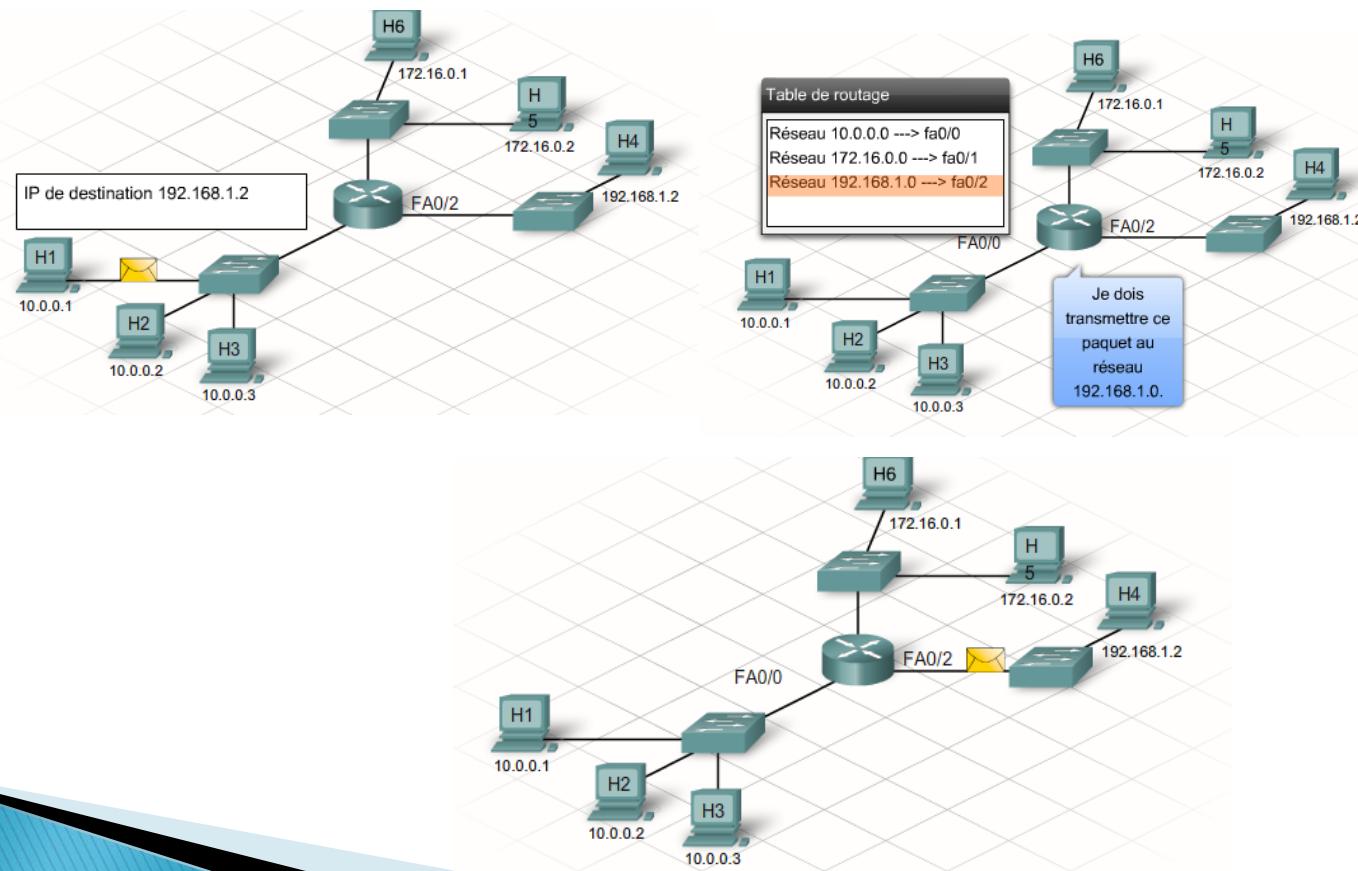
Chaque port ou interface d'un routeur permet de se connecter à un réseau local différent. Chaque routeur comporte une table de tous les réseaux connectés localement, et des interfaces qui s'y connectent. Ces tables de routage peuvent également contenir des informations sur les routes (ou chemins), que le routeur utilise pour atteindre les réseaux distants qui ne sont pas connectés localement.

Lorsqu'un routeur reçoit une trame, il la décode pour atteindre le paquet contenant l'adresse IP de destination. Il compare l'adresse de destination avec tous les réseaux contenus dans la table de routage. Si l'adresse du réseau de destination figure dans la table, le routeur encapsule le paquet dans une nouvelle trame afin de l'envoyer. Il achemine la nouvelle trame, de l'interface associée au chemin au réseau de destination. Le processus d'acheminement des paquets vers leur réseau de destination est appelé « routage ».

# Création de la couche de distribution du réseau

## ▶ Fonction des routeurs

- Table de routage

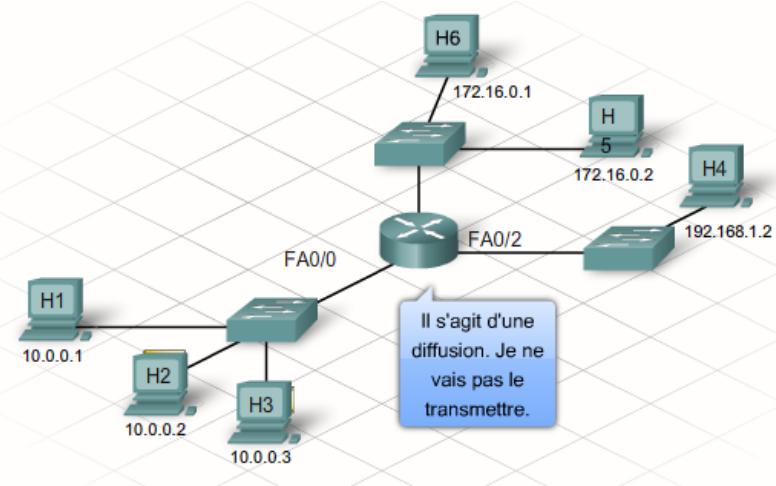
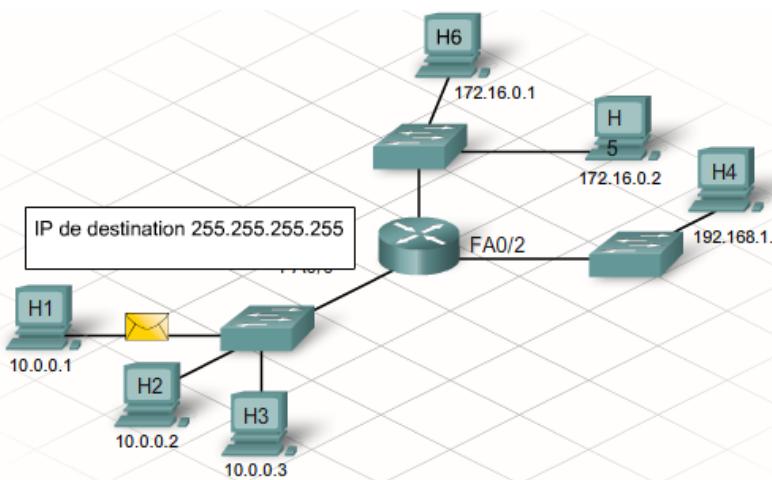


# Création de la couche de distribution du réseau

## ▶ Fonction des routeurs

- Table de routage

Les interfaces de routeur ne transfèrent pas les messages adressés à l'adresse MAC de diffusion. Par conséquent, les messages de diffusion des réseaux locaux ne sont pas transférés via les routeurs vers d'autres réseaux locaux.

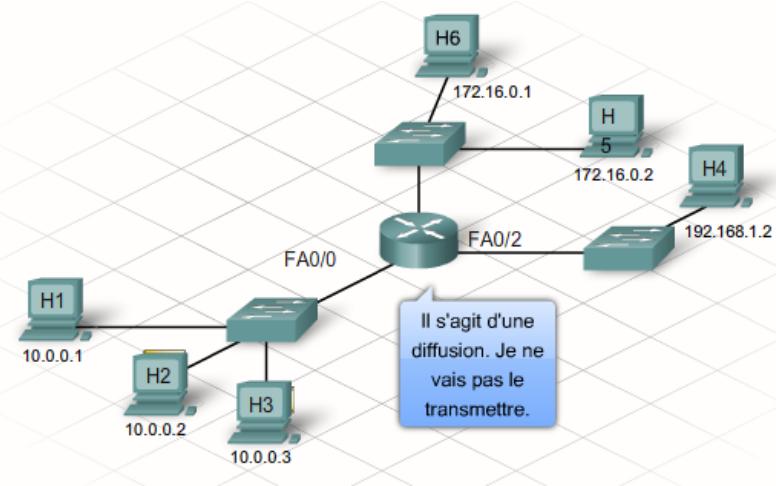
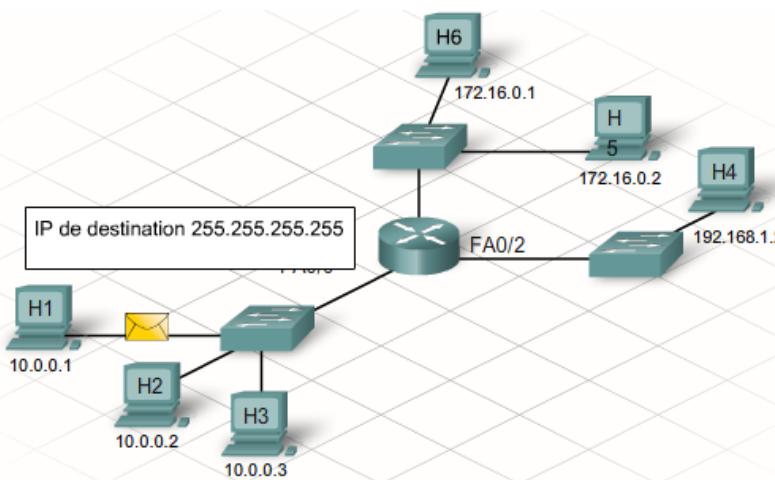


# Création de la couche de distribution du réseau

## ▶ Fonction des routeurs

- Table de routage

Les interfaces de routeur ne transfèrent pas les messages adressés à l'adresse MAC de diffusion. Par conséquent, les messages de diffusion des réseaux locaux ne sont pas transférés via les routeurs vers d'autres réseaux locaux.



# Création de la couche de distribution du réseau

## ▶ Passerelle par défaut

### ◦ Routeur utilisé comme passerelle

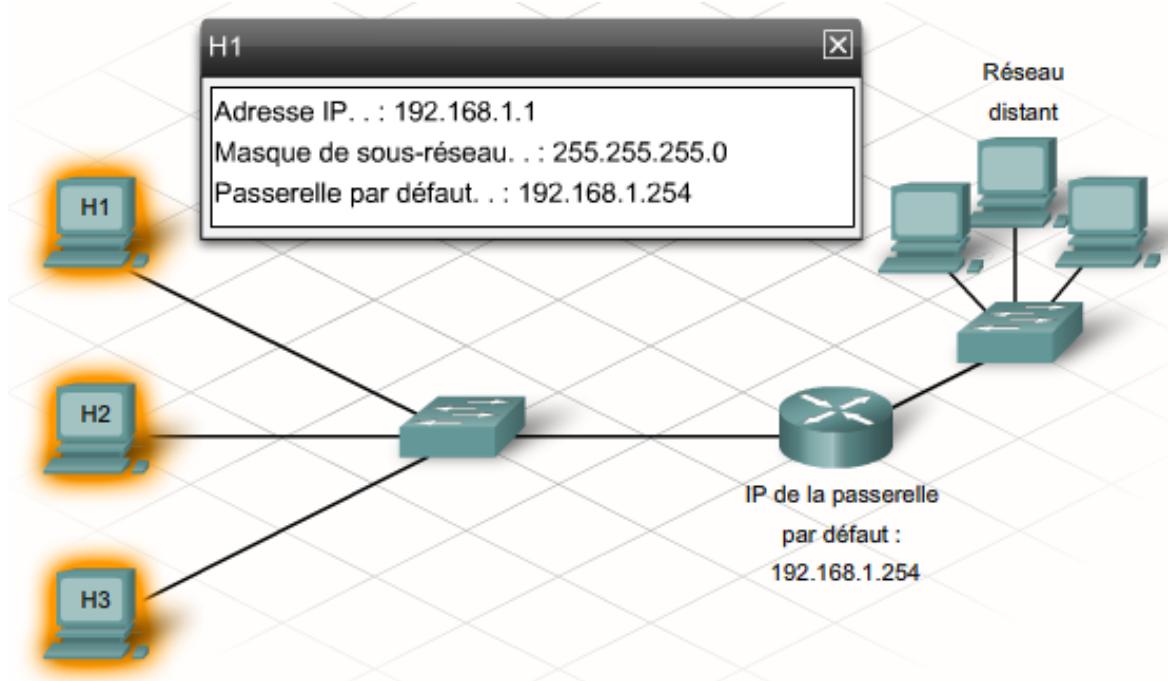
- lorsqu'un hôte doit envoyer un message à un réseau distant, il doit utiliser le routeur.
- L'hôte inclut l'adresse IP de l'hôte de destination dans le paquet
- Cependant, lorsqu'il encapsule le paquet dans une trame, il utilise l'adresse MAC du routeur comme destination de la trame. De cette façon, le routeur reçoit et accepte la trame contenant l'adresse MAC.

### ◦ Adresse de la passerelle par défaut

- Un hôte reçoit l'adresse IP du routeur par l'intermédiaire de l'adresse de la passerelle par défaut configurée dans ses paramètres TCP/IP.
- L'adresse de la passerelle par défaut est l'adresse de l'interface de routeur connectée au même réseau local que l'hôte source.

# Création de la couche de distribution du réseau

- ▶ Passerelle par défaut
  - Adresse de la passerelle par défaut



# Création de la couche de distribution du réseau

- ▶ **Passerelle par défaut**
  - **Adresse de la passerelle par défaut**

**Comment l'hôte détermine-t-il l'adresse MAC du routeur?**

Une fois que l'hôte connaît l'adresse IP de la passerelle par défaut, il peut utiliser le protocole ARP pour déterminer l'adresse MAC. L'adresse MAC du routeur est ensuite incluse dans la trame, destinée à un autre réseau.

# Création de la couche de distribution du réseau

## ▶ Tables tenues à jour par les routeurs

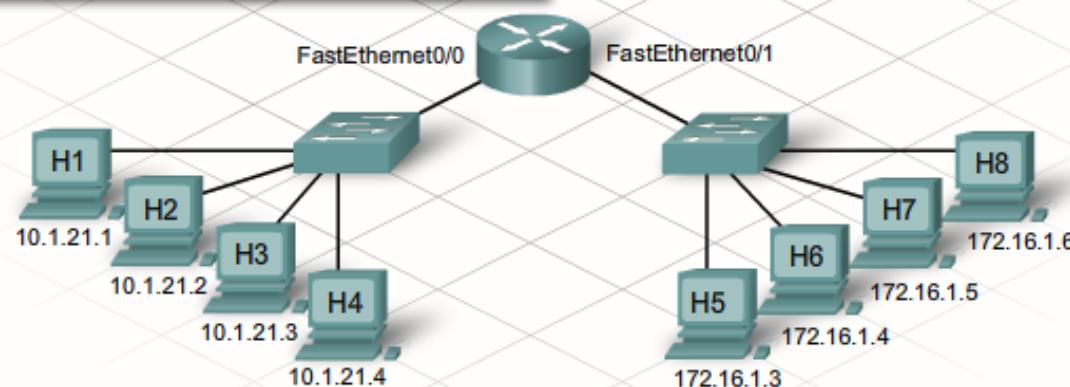
Les routeurs font circuler les informations entre les réseaux locaux et distants. Pour ce faire, les routeurs doivent utiliser à la fois le protocole ARP et les tables de routage pour enregistrer les informations

Table ARP

Adresse	Adresse matérielle	Interface
10.1.21.1	0002.a5ec.c7f9	FastEthernet0/0
10.1.21.2	0012.3fec.fb0d	FastEthernet0/0
10.1.21.3	0014.222e.dac5	FastEthernet0/0
10.1.21.4	00c0.8f4b.8b78	FastEthernet0/0
172.16.1.3	0ac3.a58c.d7f5	FastEthernet0/1
172.16.1.4	0a2f.4fed.dd0d	FastEthernet0/1
172.16.1.5	0b03.3002.ea2d	FastEthernet0/1
172.16.1.6	0d00.a94b.8caa	FastEthernet0/1

Table de routage

Type	Réseau	Port
C	10.0.0.0/8	FastEthernet0/0
C	172.16.0.0/16	FastEthernet0/1



# Création de la couche de distribution du réseau

## ▶ Tables tenues à jour par les routeurs

Les tables de routage incluent les adresses des réseaux et le meilleur chemin pour atteindre ces réseaux.

Les routeurs utilisent les tables de routage pour déterminer l'interface à utiliser pour acheminer un message jusqu'à sa destination.

Si le routeur ne peut pas déterminer où envoyer un message, il le supprime.

Les administrateurs réseau configurent une table de routage avec une route par défaut pour empêcher la suppression d'un paquet, si le chemin jusqu'au réseau de destination n'est pas indiqué dans la table de routage.

Une route par défaut est l'interface que le routeur utilise pour acheminer un paquet contenant une adresse IP de réseau de destination inconnue. Cette route par défaut se connecte généralement à un autre routeur, qui peut acheminer le paquet jusqu'à son réseau de destination final.

# Création de la couche de distribution du réseau

## ▶ Tables tenues à jour par les routeurs

Un routeur achemine une trame jusqu'à un de ces deux emplacements : un réseau directement connecté, contenant l'hôte de destination réel, ou un autre routeur du chemin, menant à l'hôte de destination

Il s'agit de l'adresse MAC de l'hôte de destination réel, si ce dernier fait partie d'un réseau connecté localement au routeur. Si le routeur doit acheminer le paquet vers un autre routeur, il utilisera l'adresse MAC du routeur connecté. Les routeurs obtiennent ces adresses MAC via les tables ARP.

Chaque interface de routeur fait partie du réseau local auquel il est connecté et tient à jour sa propre table ARP pour ce réseau. Les tables ARP contiennent les adresses MAC et les adresses IP de tous les hôtes de ce réseau.

# Création de la couche de distribution du réseau

## ▶ Tables tenues à jour par les routeurs

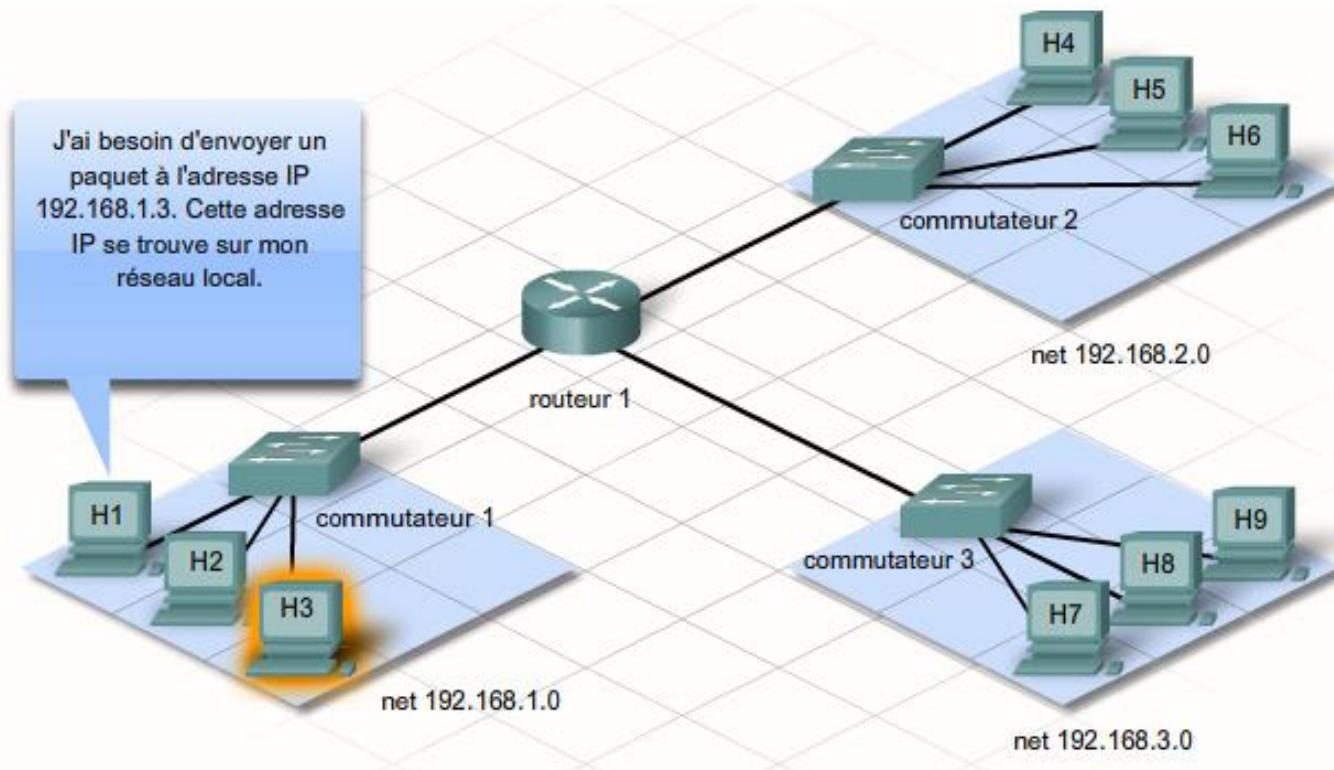
Un routeur achemine une trame jusqu'à un de ces deux emplacements : un réseau directement connecté, contenant l'hôte de destination réel, ou un autre routeur du chemin, menant à l'hôte de destination

Il s'agit de l'adresse MAC de l'hôte de destination réel, si ce dernier fait partie d'un réseau connecté localement au routeur. Si le routeur doit acheminer le paquet vers un autre routeur, il utilisera l'adresse MAC du routeur connecté. Les routeurs obtiennent ces adresses MAC via les tables ARP.

Chaque interface de routeur fait partie du réseau local auquel il est connecté et tient à jour sa propre table ARP pour ce réseau. Les tables ARP contiennent les adresses MAC et les adresses IP de tous les hôtes de ce réseau.

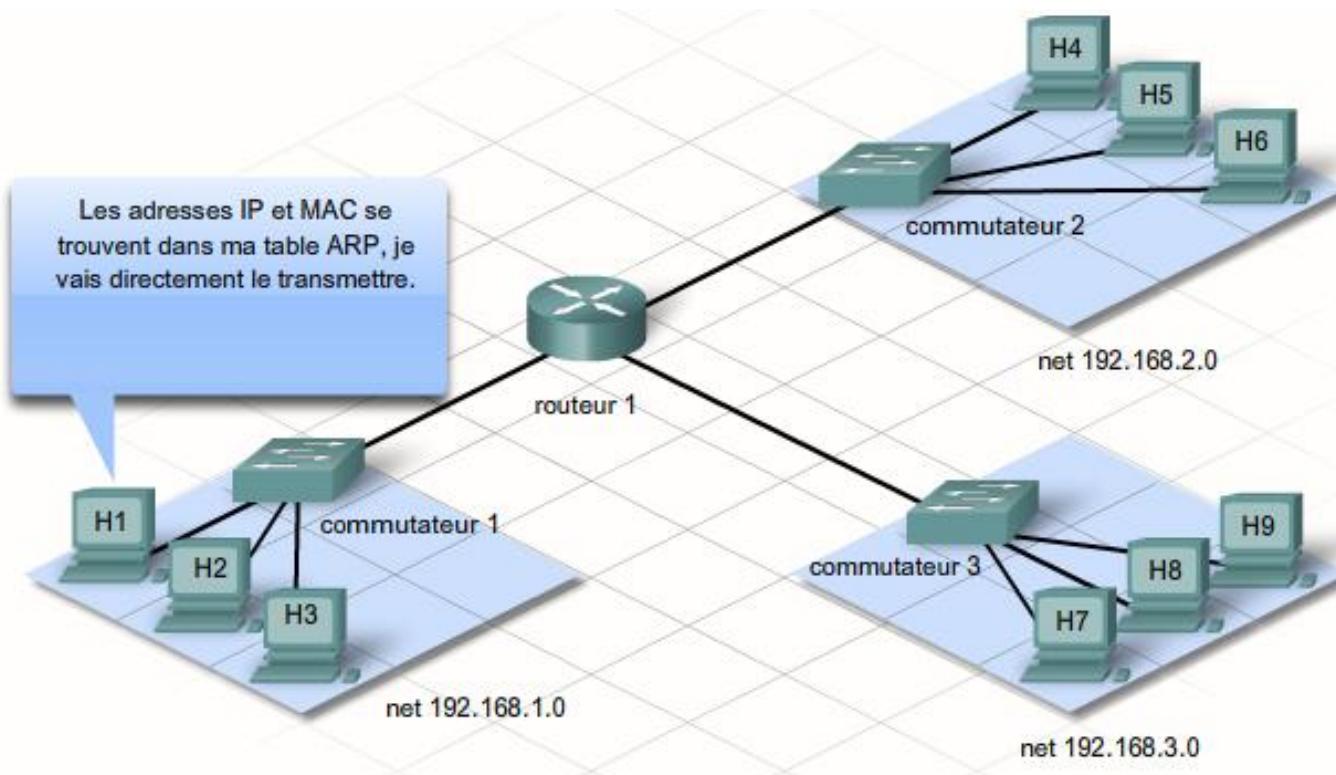
# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



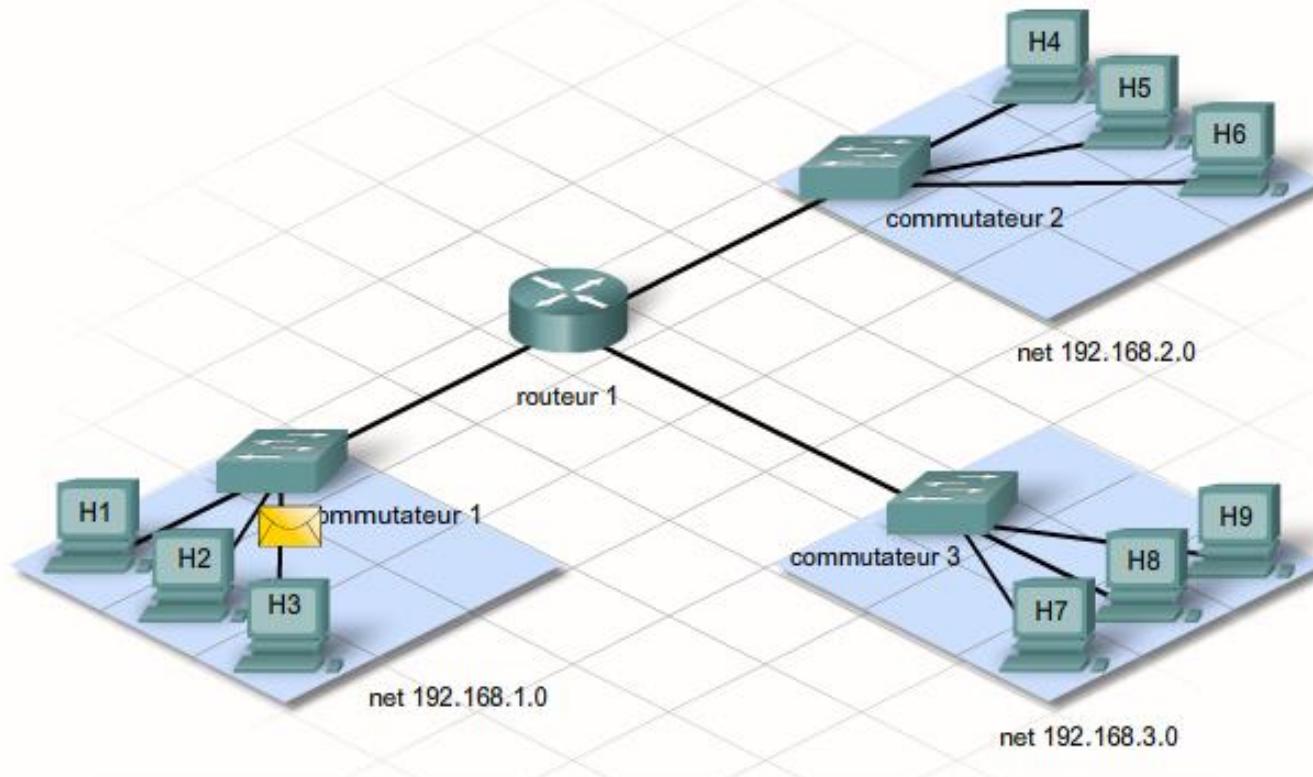
# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



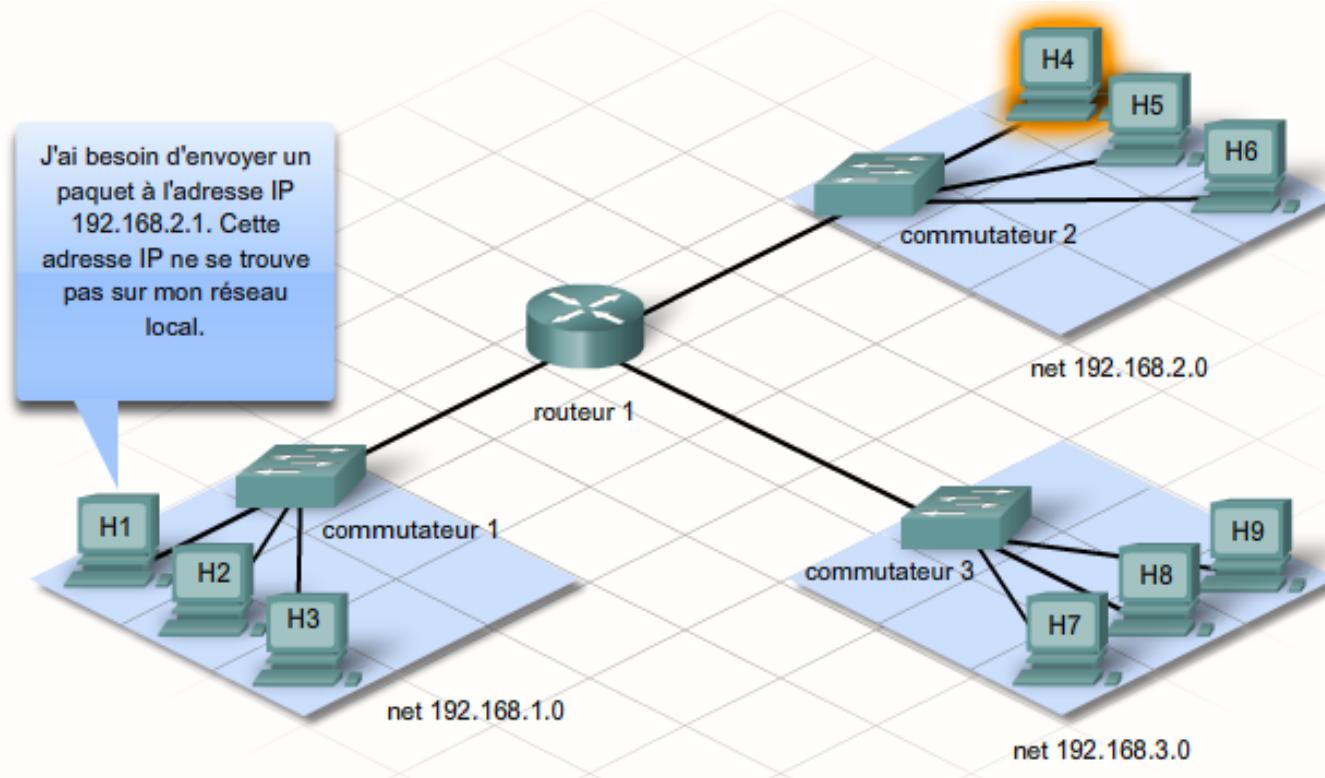
# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



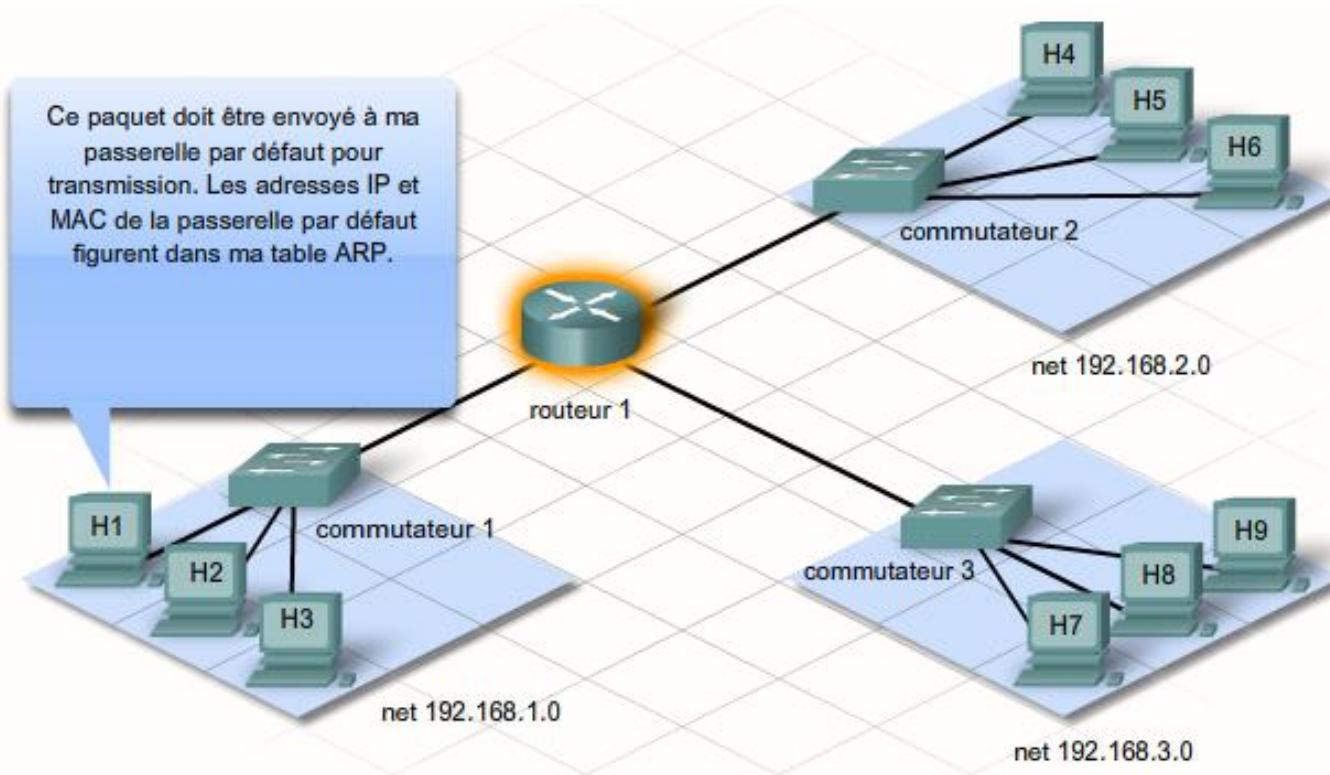
# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



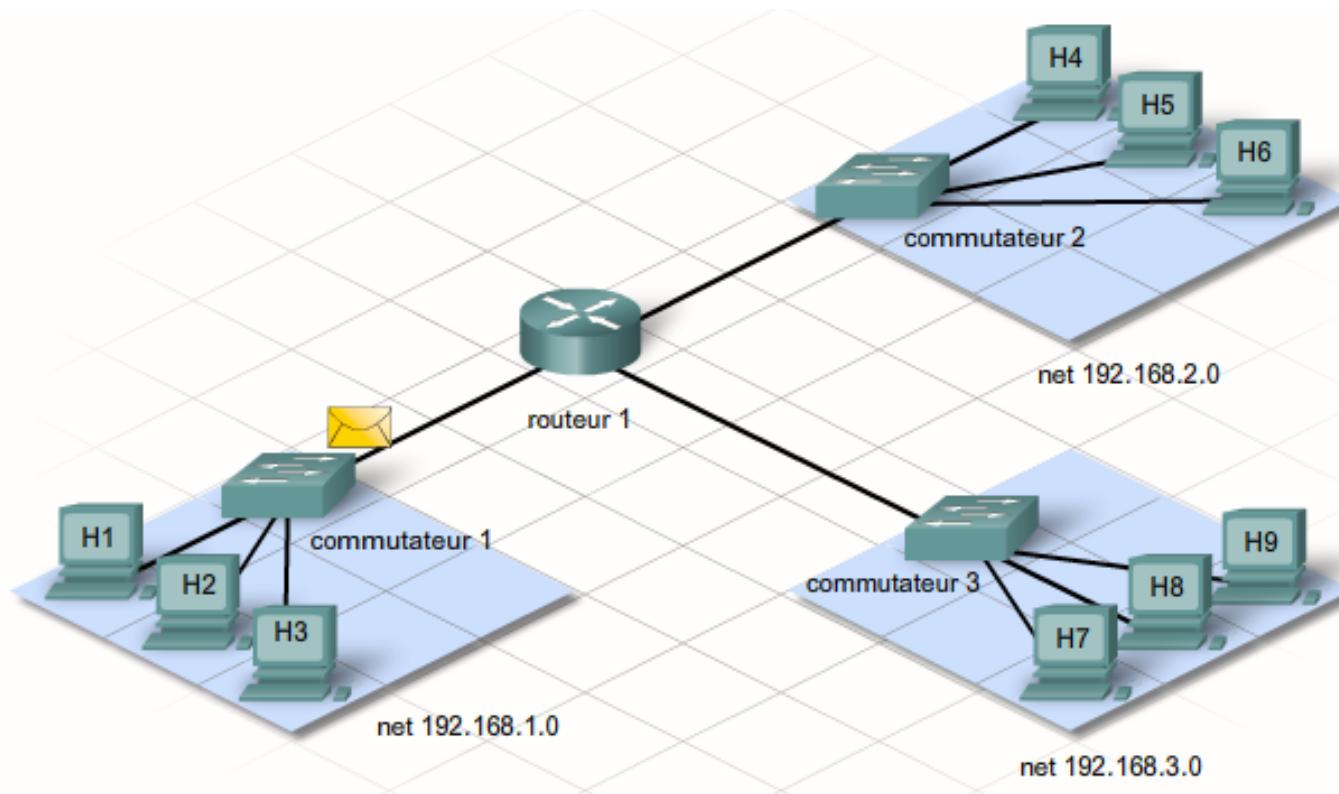
# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



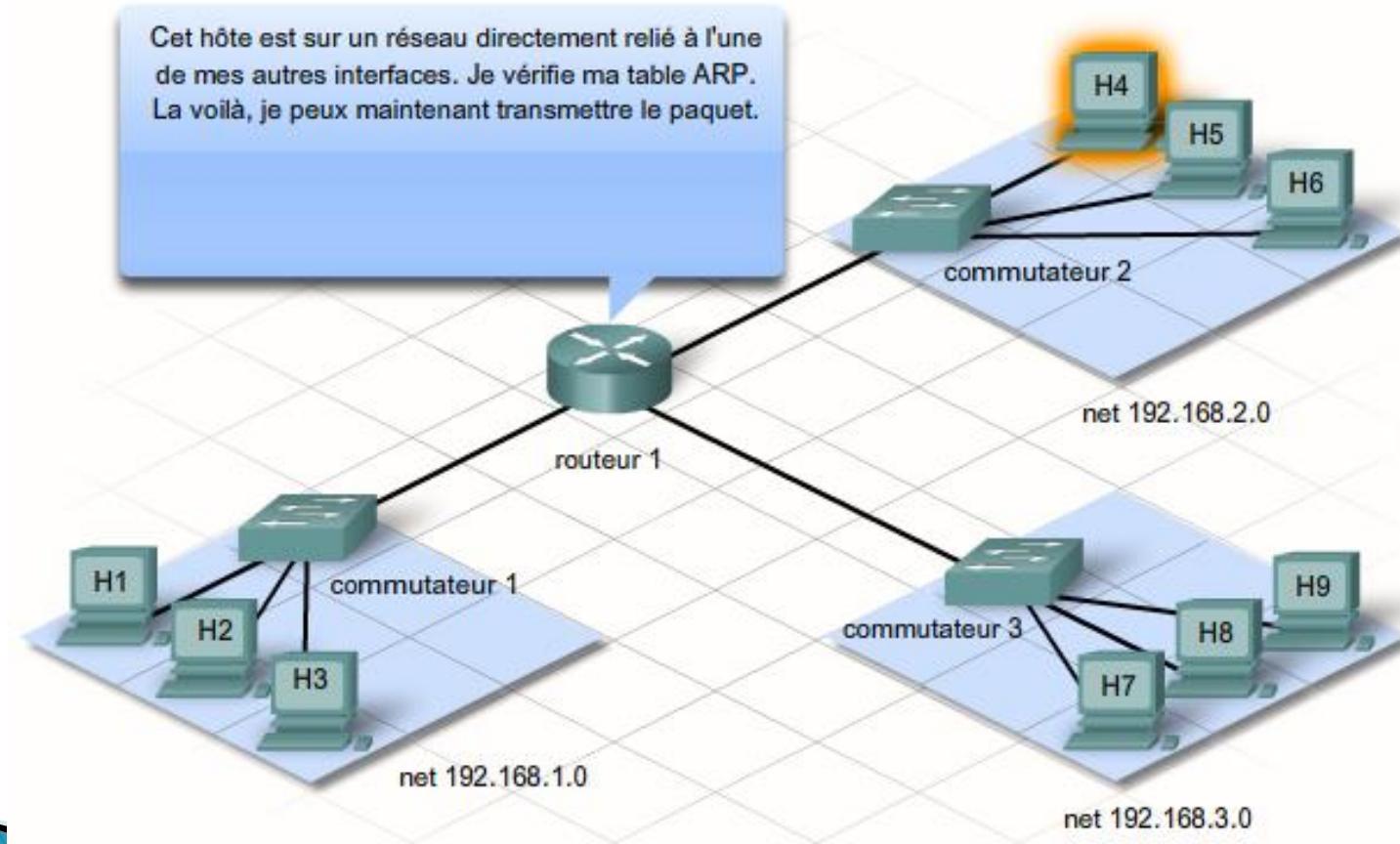
# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



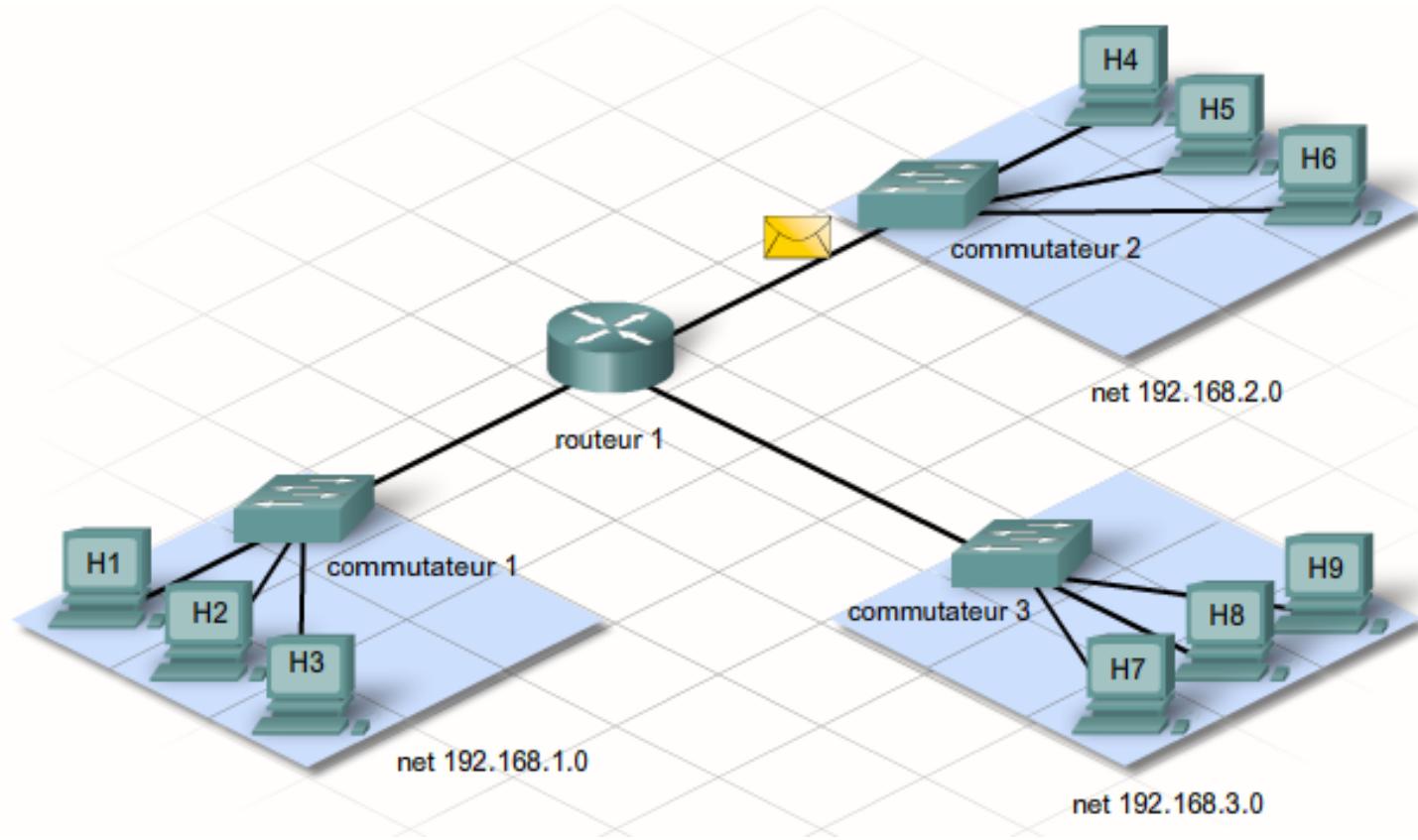
# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



# Création de la couche de distribution du réseau

- ▶ Tables tenues à jour par les routeurs



# Création de la couche de distribution du réseau

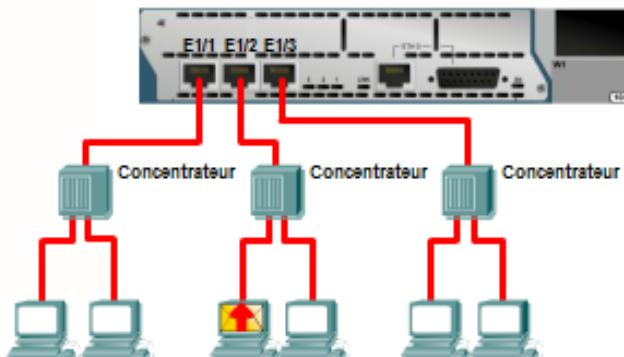
## ▶ Tables tenues à jour par les routeurs

### Exercice

Déterminez comment le routeur transmet un paquet en fonction des adresses source et de destination et des informations de la table de routage.

Répondez aux questions en fonction des informations contenues dans l'image.

Table de routage				
Type	Réseau	Port	Prochaine	Mesure
C	192.168.3.0/24	Ethernet1/1	---	0/0
C	172.16.1.0/24	Ethernet1/2	---	0/0
C	10.5.5.0/24	Ethernet1/3	---	0/0



Trame				
Ballise de démar	Destination	Source	Données encapsulées	
	10.5.5.8	172.16.1.2		

1. Quelle est l'adresse de la passerelle par défaut utilisée pour transmettre ce paquet au routeur ?

- 192.168.3.1
- 172.16.1.1
- 10.5.5.1

2. Lorsque le routeur reçoit ce paquet, vers quelle interface le transmet-il ?

- Ethernet1/1
- Ethernet1/2
- Ethernet1/3

# Création de la couche de distribution du réseau

## ► Réseau LAN (Local Area Network)

Le terme LAN fait référence à un réseau local ou à un groupe de réseaux locaux interconnectés, placés sous le même contrôle administratif. Au tout début des réseaux, les réseaux LAN étaient définis comme de petits réseaux, installés dans un seul emplacement physique. Si un réseau LAN peut être un réseau local unique, installé chez un particulier ou une petite entreprise, sa définition a évolué jusqu'à inclure les réseaux locaux interconnectés constitués de centaines d'hôtes, installés dans plusieurs bâtiments et dans plusieurs zones géographiques.

Il est important de retenir que tous les réseaux locaux d'un réseau LAN sont placés sous un même contrôle administratif. Les autres caractéristiques communes des réseaux LAN sont les suivantes : ils utilisent généralement des protocoles Ethernet ou sans fil et prennent en charge des débits de données élevés.

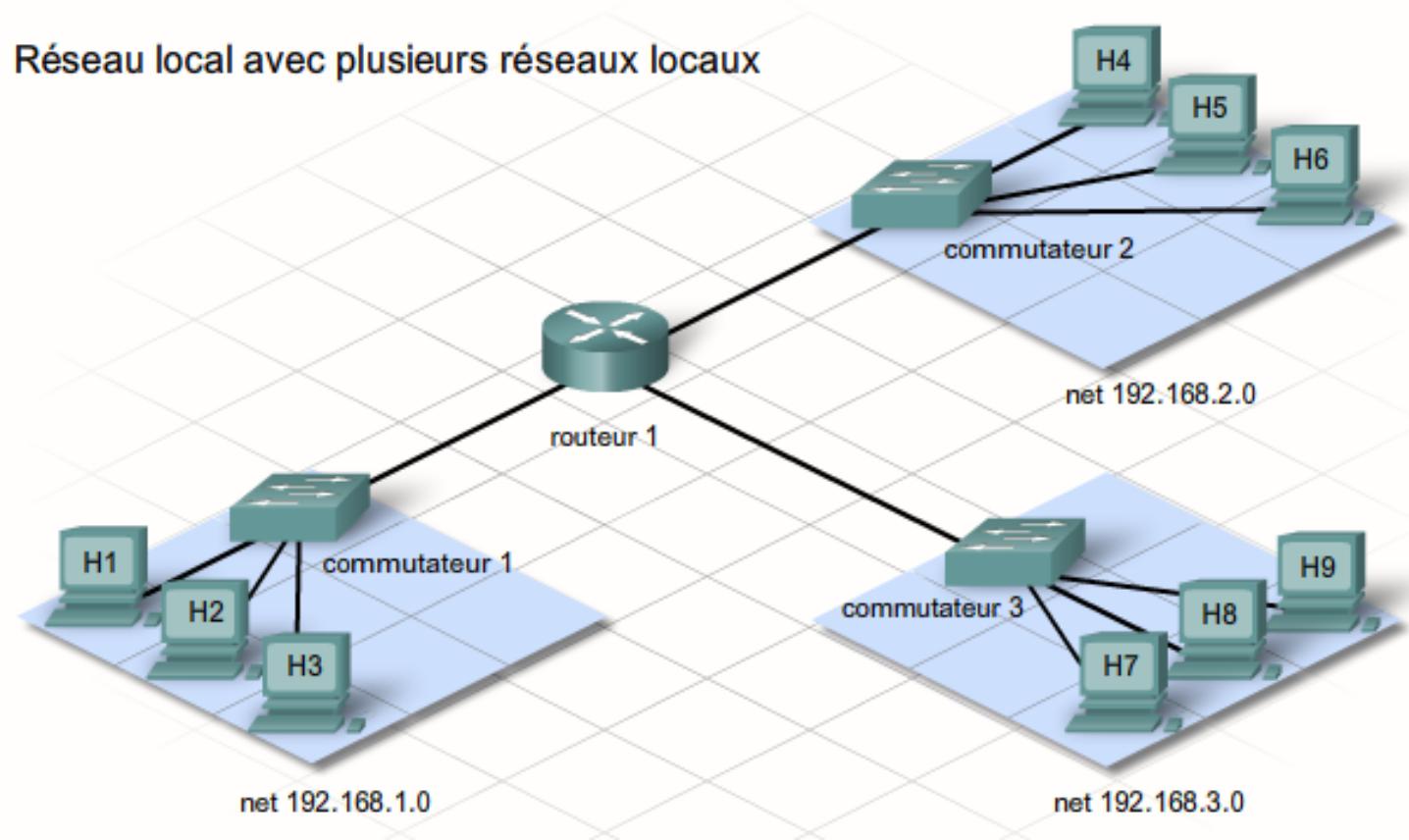
# Création de la couche de distribution du réseau

## ▶ Réseau LAN (Local Area Network)

Le terme Intranet est souvent utilisé pour faire référence à un réseau LAN privé qui appartient à une entreprise ou une administration et auquel peuvent accéder uniquement ses membres, ses employés ou des tierces personnes autorisées.

# Création de la couche de distribution du réseau

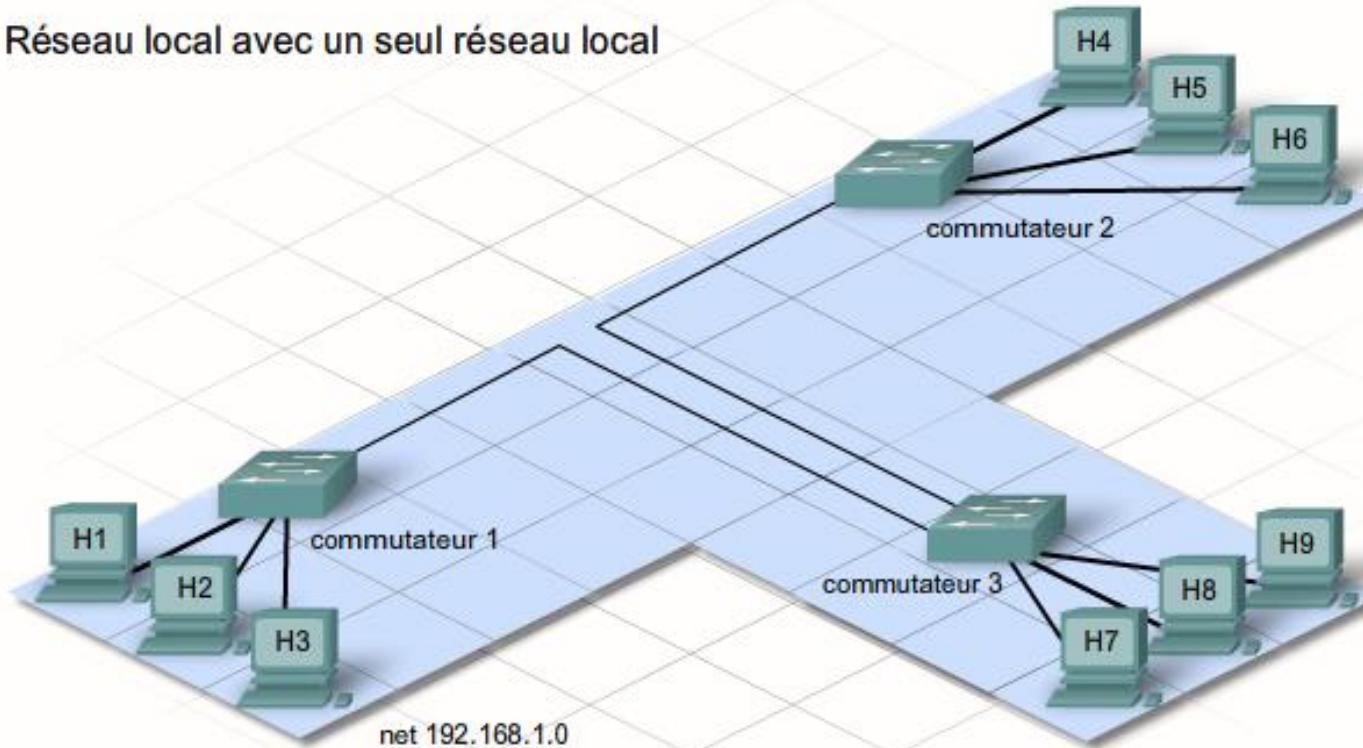
## ▶ Réseau LAN (Local Area Network)



# Création de la couche de distribution du réseau

## ▶ Réseau LAN (Local Area Network)

Réseau local avec un seul réseau local



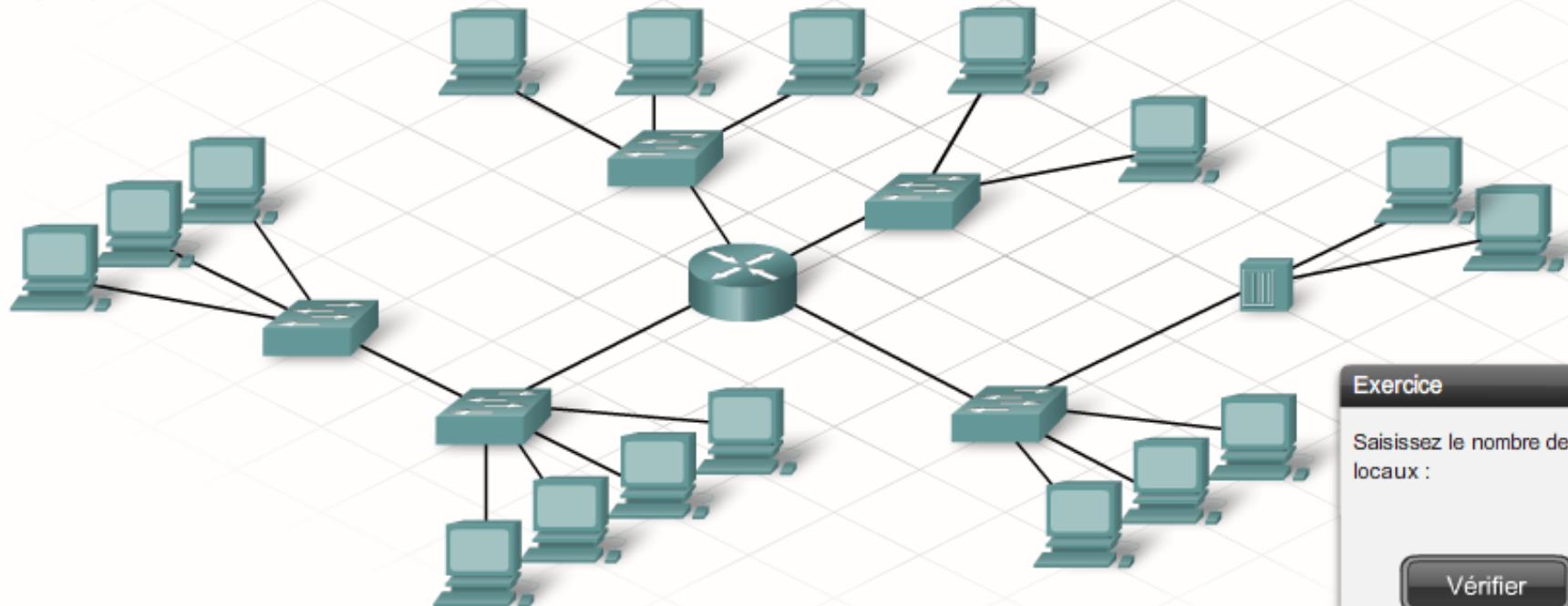
# Création de la couche de distribution du réseau

## ▶ Réseau LAN (Local Area Network)

### Exercice

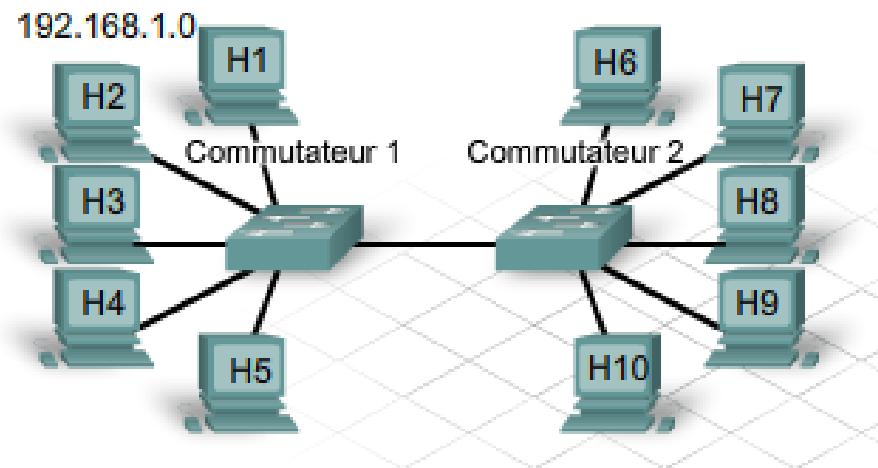
Identifiez le nombre de réseaux locaux sur le réseau local.

Comptez les réseaux locaux et saisissez leur nombre dans l'espace prévu à cet effet.



# Création de la couche de distribution du réseau

- ▶ Ajout d'hôtes aux réseaux locaux et distants
  - Positionnement de tous les hôtes sur un segment du réseau local



## Avantages :

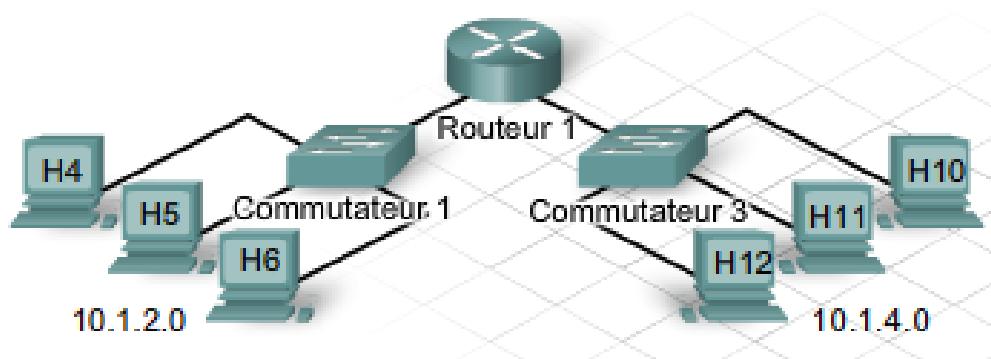
- convient aux réseaux plus simples ;
- plus de simplicité et un réseau moins coûteux ;
- permet aux périphériques d'être vus par d'autres périphériques ;
- transfert de données plus rapide : communication plus directe ;
- accès au périphérique facile.

## Inconvénients :

- tous les hôtes se trouvent dans un domaine de diffusion, ce qui augmente le trafic sur le segment et risque ainsi de ralentir les performances du réseau.

# Création de la couche de distribution du réseau

- ▶ Ajout d'hôtes aux réseaux locaux et distants
  - Positionnement de tous les hôtes sur des segments de réseau distant



## Avantages :

- convient davantage aux réseaux plus grands et plus complexes ;
- divise les domaines de diffusion et diminue le trafic ;
- peut améliorer les performances de chaque segment ;
- rend les machines invisibles pour celles qui se trouvent sur d'autres segments de réseau local ;
- peut accroître la sécurité ;
- peut améliorer l'organisation du réseau.

## Inconvénients :

- nécessite d'utiliser le routage (couche de distribution) ;
- le routeur peut ralentir le trafic entre les segments ;
- plus complexe et plus cher (nécessite un routeur).

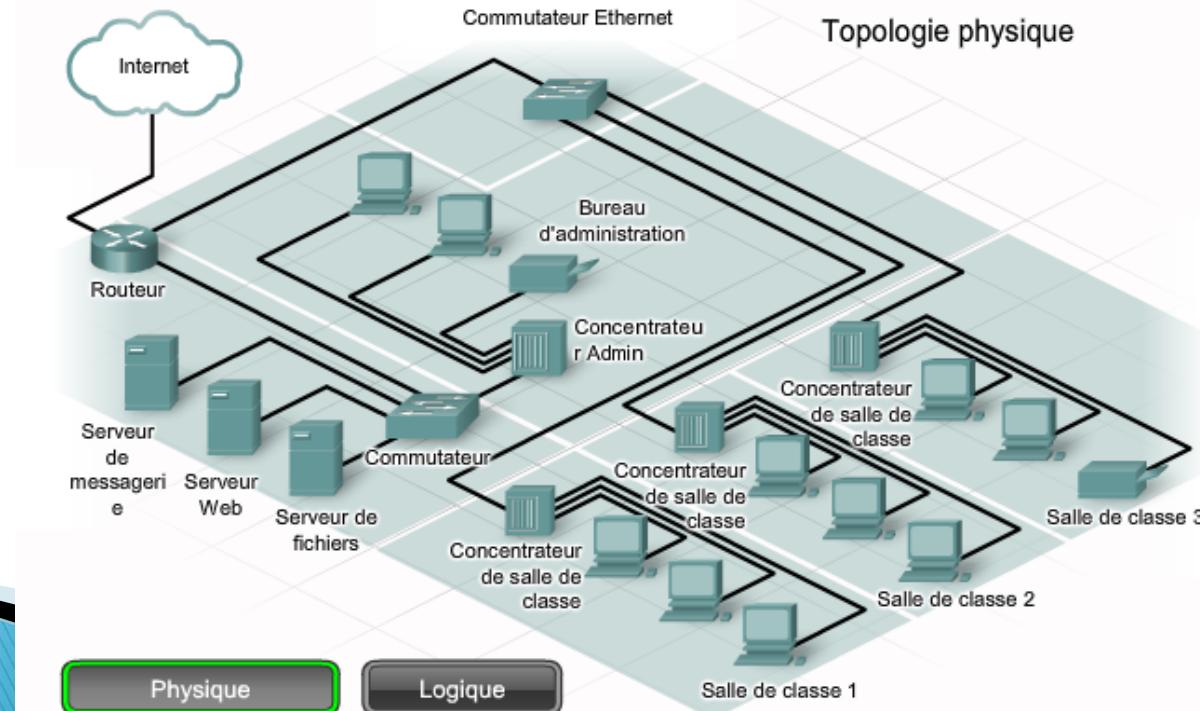
# Création de la couche de distribution du réseau

## ► Topologie de réseau

### ◦ Topologie physique

Configuration physique du réseau :

- Emplacement physique des périphériques tels que les routeurs, les commutateurs et les hôtes
- Interconnexion de tous les périphériques
- Emplacement et longueur de tous les parcours de câbles
- Configuration matérielle des périphériques finaux tels que les hôtes et les serveurs



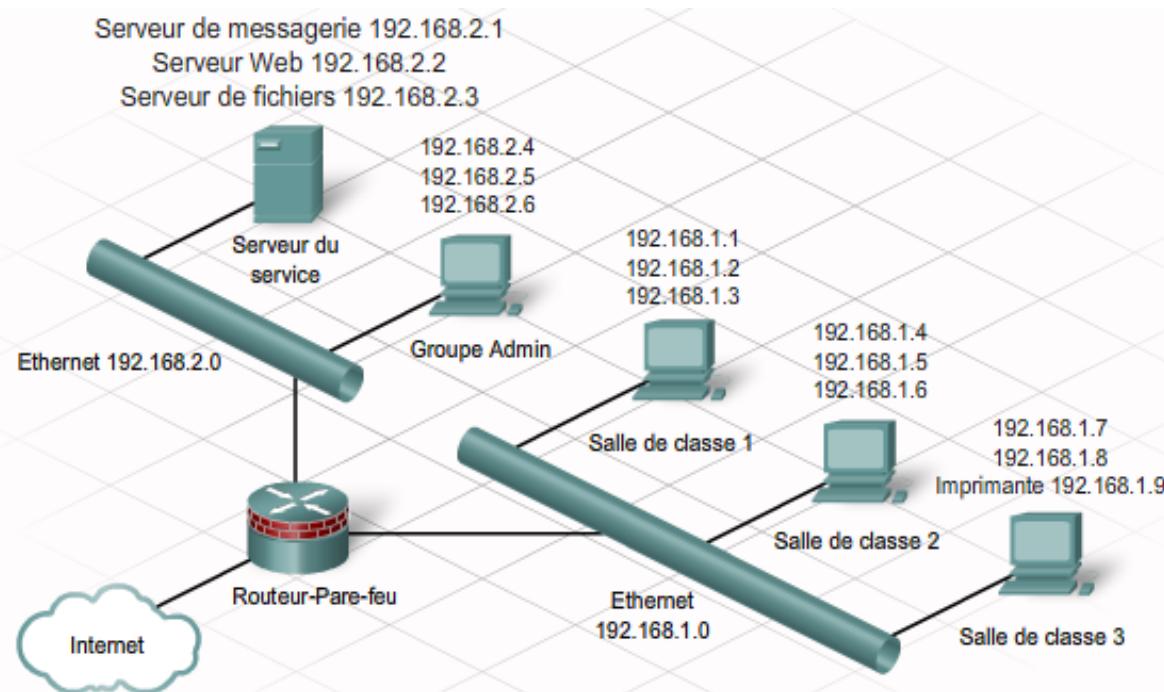
# Création de la couche de distribution du réseau

## ► Topologie de réseau

### ◦ Topologie logique

Configuration logique du réseau :

- Emplacement et taille des domaines de diffusion et de collision
- Système d'adressage IP
- Convention d'attribution de nom
- Configuration du partage
- Autorisations



# Création de la couche de distribution du réseau

## ▶ Partage de ressources

L'un des objectifs les plus courants de la mise en réseau est le partage de ressources telles que fichiers et imprimantes. Windows permet aux utilisateurs distants d'accéder à un ordinateur local et à ses ressources, par l'intermédiaire de ce que l'on appelle le partage.

Le partage de fichiers simple peut être désactivé pour définir des niveaux de sécurité plus précis. Après la désactivation, il est possible d'attribuer aux ressources les droits d'accès suivants :

- Contrôle total
- Modification
- Lecture et exécution
- Affichage du contenu du dossier
- Lecture
- Écriture

# Création de la couche de distribution du réseau

## ▶ Partage de ressources

L'un des objectifs les plus courants de la mise en réseau est le partage de ressources telles que fichiers et imprimantes. Windows permet aux utilisateurs distants d'accéder à un ordinateur local et à ses ressources, par l'intermédiaire de ce que l'on appelle le partage.

Le partage de fichiers simple peut être désactivé pour définir des niveaux de sécurité plus précis. Après la désactivation, il est possible d'attribuer aux ressources les droits d'accès suivants :

- Contrôle total
- Modification
- Lecture et exécution
- Affichage du contenu du dossier
- Lecture
- Écriture

# Création de la couche de distribution du réseau

## ▶ Partage de ressources

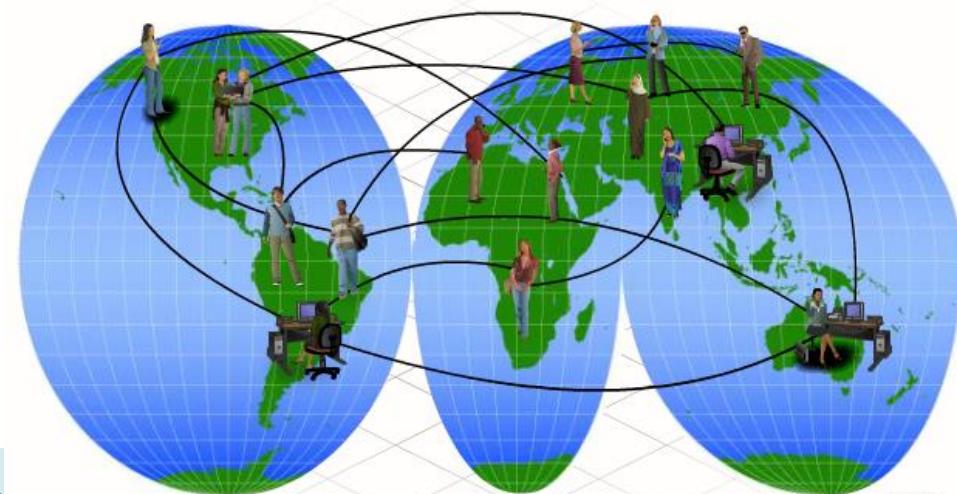
Lorsqu'un utilisateur accède à un fichier stocké sur un périphérique distant, l'Explorateur Windows permet à l'utilisateur d'associer un lecteur à une ressource ou un dossier distant. Cela permet d'associer une lettre de lecteur spécifique, par exemple M:, à la ressource distante. L'utilisateur peut alors interagir avec la ressource comme si elle était connectée localement.

- Travaux pratique: partage de ressources

# Connexion à Internet via un fournisseur d'accès

## ▶ Qu'est-ce que Internet

- Internet est un ensemble de **réseaux informatiques internationaux** qui coopèrent pour échanger des informations en respectant des **normes communes**.
- Via des **fils téléphoniques**, des **câbles à fibres optiques**, des **transmissions sans fil** et des **liaisons satellitaires**, les utilisateurs d'Internet peuvent échanger des informations dans une variété de formats.



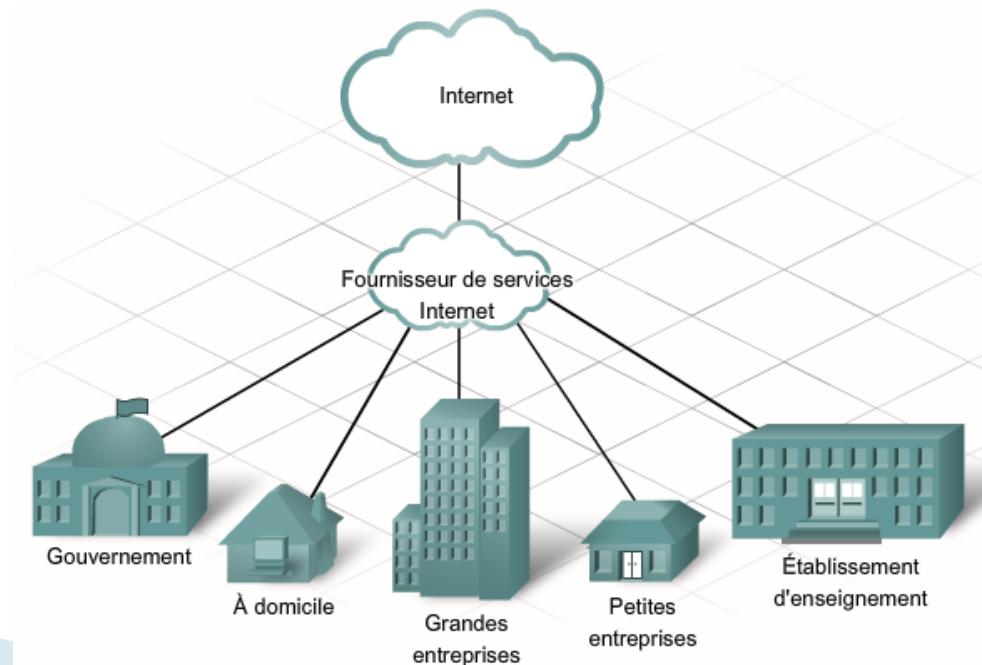
# Connexion à Internet via un fournisseur d'accès

- ▶ Qu'est-ce que Internet
  - Internet est un « **réseau de réseaux** » qui connecte les utilisateurs dans tous les pays du monde. Actuellement, il y a plus d'un milliard d'utilisateurs **Internet dans le monde.**
  - Jusqu'à présent, nous avons parlé de **réseaux** gérés par un **particulier**, une **administration** ou une **entreprise**. Internet est un ensemble de réseaux dont **personne n'est propriétaire.**
  - Cela étant, plusieurs **grandes sociétés internationales** participent à la **gestion d'Internet** pour que tous les utilisateurs appliquent les mêmes règles.

# Connexion à Internet via un fournisseur d'accès

## ▶ Fournisseurs de services Internet

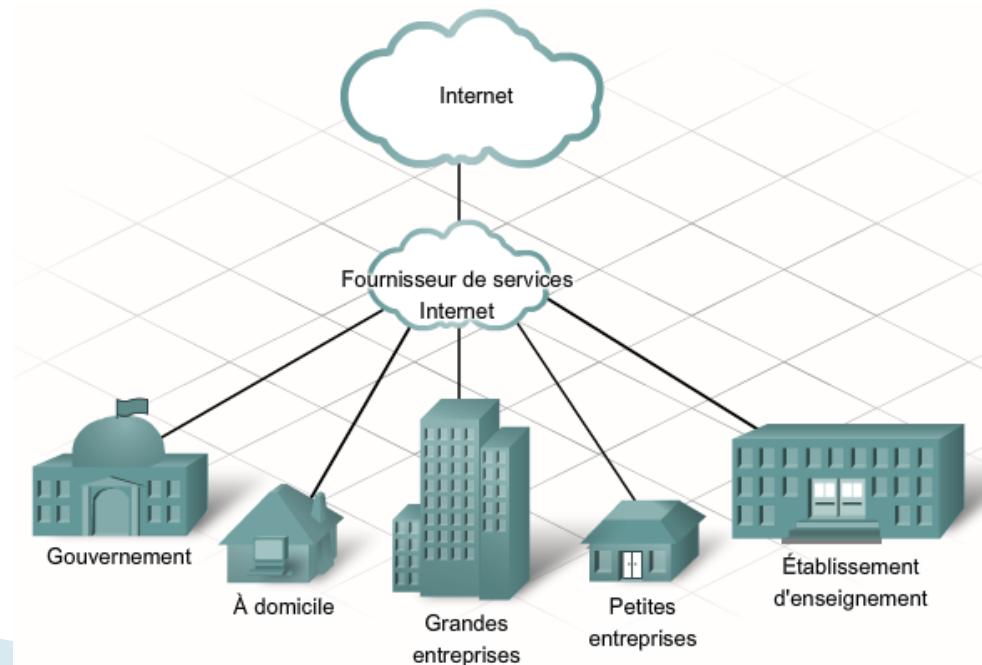
- Tout particulier, entreprise ou administration qui souhaite se connecter à Internet, doit passer par **un fournisseur de services Internet (ou FAI, *Fournisseur d'Accès à Internet, ISP, Internet Service Provider* en anglais).**



# Connexion à Internet via un fournisseur d'accès

## ▶ Fournisseurs de services Internet

- Tout particulier, entreprise ou administration qui souhaite se connecter à Internet, doit passer par **un fournisseur de services Internet (ou FAI, *Fournisseur d'Accès à Internet, ISP, Internet Service Provider* en anglais).**

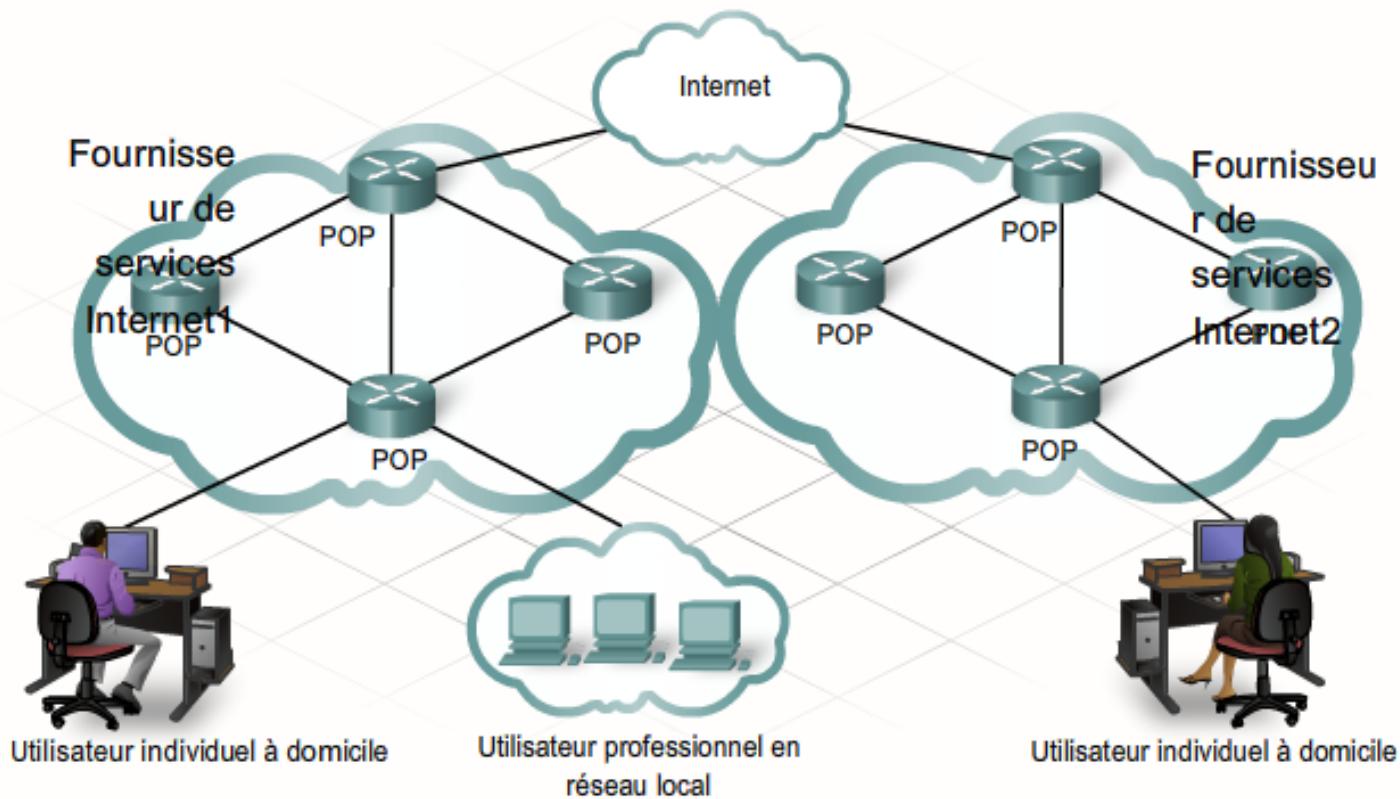


# Connexion à Internet via un fournisseur d'accès

- ▶ Fournisseurs de services Internet
  - Un **FAI** est une société qui fournit les **connexions** et la **prise en charge d'un accès Internet**.
  - Il peut également proposer des **services complémentaires**
    - messagerie électronique et hébergement Web.
  - Pour accéder à Internet, un **FAI** est indispensable.
    - Personne ne peut accéder à Internet sans ordinateur hôte ni FAI.
  - Les FAI se distinguent par le type de technologie et de vitesse de connexion qu'ils offrent.

# Connexion à Internet via un fournisseur d'accès

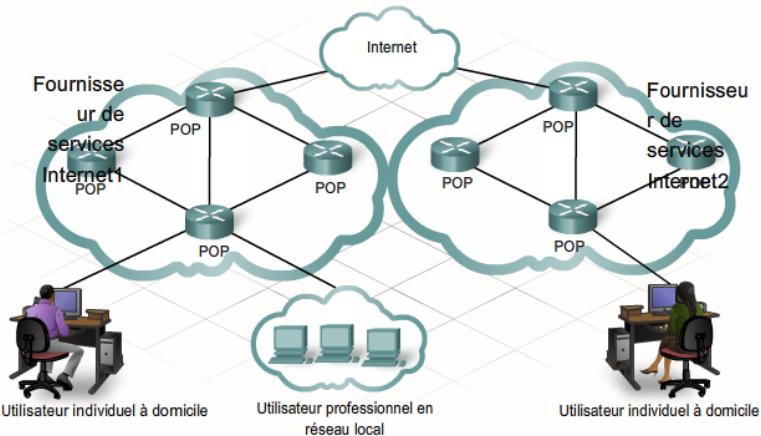
## ► Liens entre les FAI et Internet



# Connexion à Internet via un fournisseur d'accès

## ▶ Liens entre les FAI et Internet

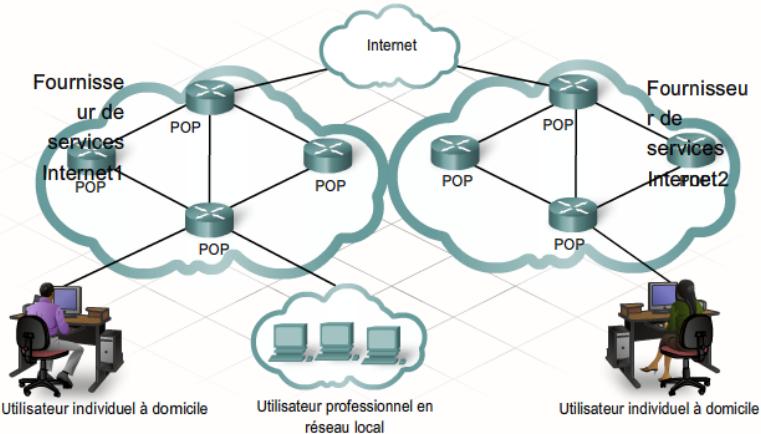
- Les ordinateurs et les réseaux locaux se connectent au FAI par le biais d'un **point de présence (POP)**.
- Un POP est un **point de connexion entre le réseau du FAI et la zone géographique que les services du POP couvrent.**



# Connexion à Internet via un fournisseur d'accès

## ► Liens entre les FAI et Internet

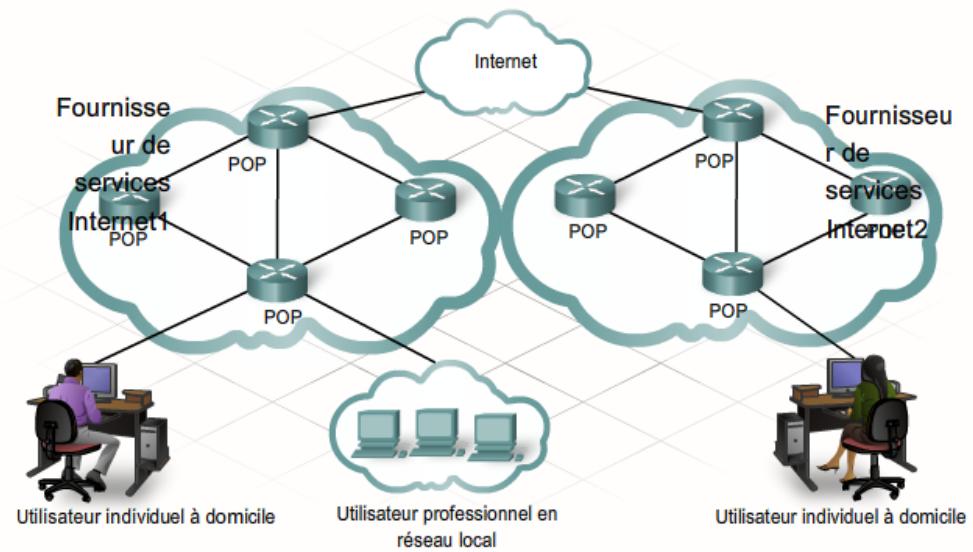
- Un FAI peut avoir **plusieurs POP** selon sa **taille** et la **zone** qu'il prend en charge
- Chez un FAI, **un réseau de routeurs** et de **commutateurs haut débit** transportent les données entre les différents POP



# Connexion à Internet via un fournisseur d'accès

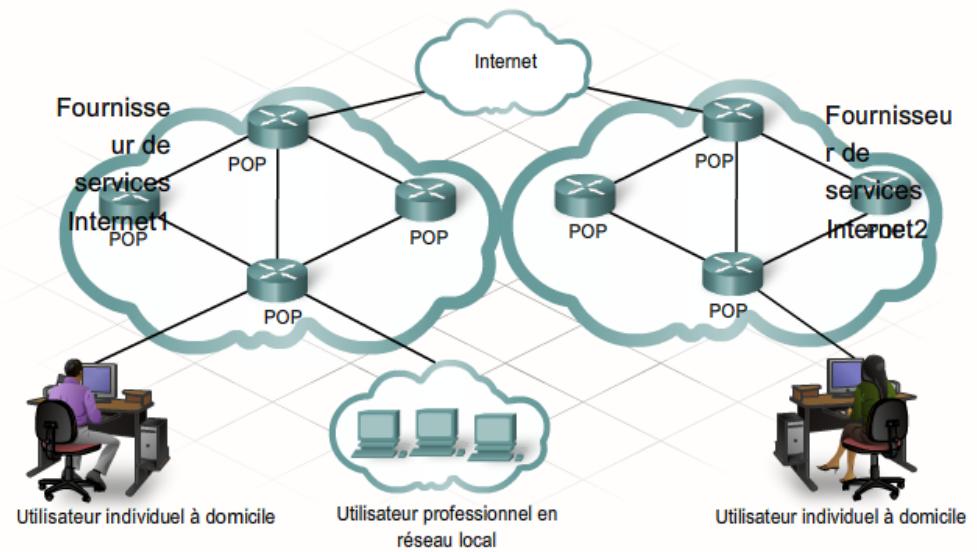
## ► Liens entre les FAI et Internet

- Les FAI se **connectent à d'autres FAI pour envoyer les informations au-delà des frontières de leur propre réseau.**
- **Internet est composé de liaisons de données haut débit qui interconnectent les POP des FAI et les FAI.**



# Connexion à Internet via un fournisseur d'accès

- ▶ Liens entre les FAI et Internet
  - Ces interconnexions font partie d'un **immense réseau haute capacité**, appelé le « **Réseau fédérateur Internet** ».
- ▶ La connexion au FAI par le biais du POP fournit aux utilisateurs **un accès aux services du FAI et à Internet**.



# Connexion à Internet via un fournisseur d'accès

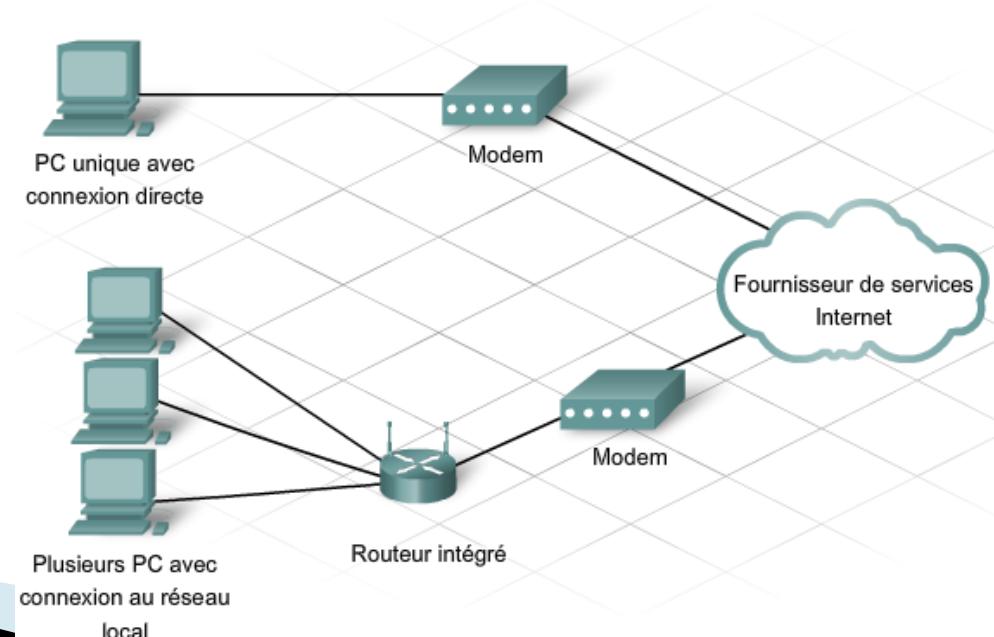
## ► Liens entre les FAI et Internet



# Connexion à Internet via un fournisseur d'accès

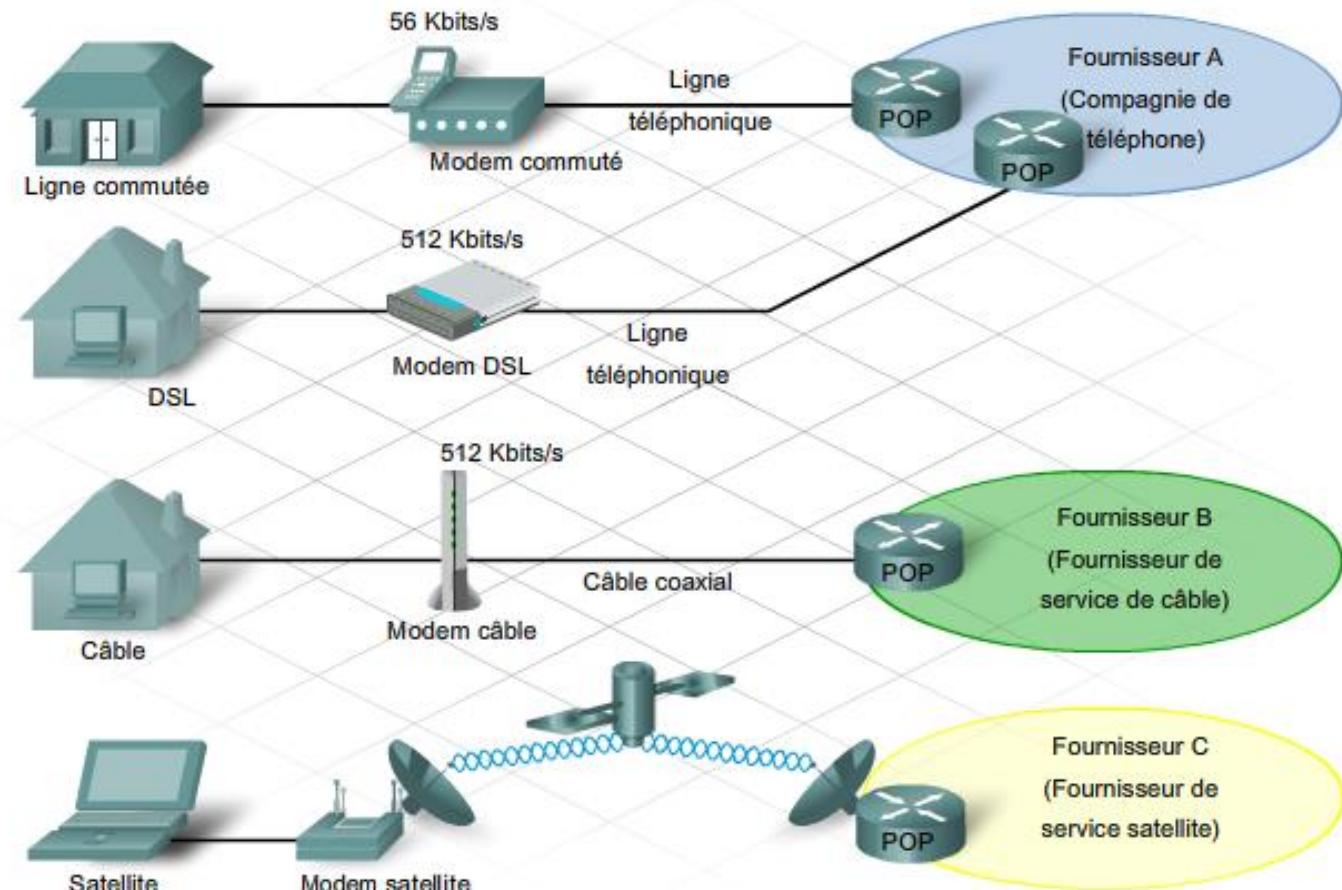
## ▶ Options de connexion au FAI

- Pour se connecter au FAI, chaque technologie d'accès Internet fait appel à un périphérique d'accès réseau, tel qu'un **modem**. Il peut être intégré à l'ordinateur ou fourni par le FAI.



# Connexion à Internet via un fournisseur d'accès

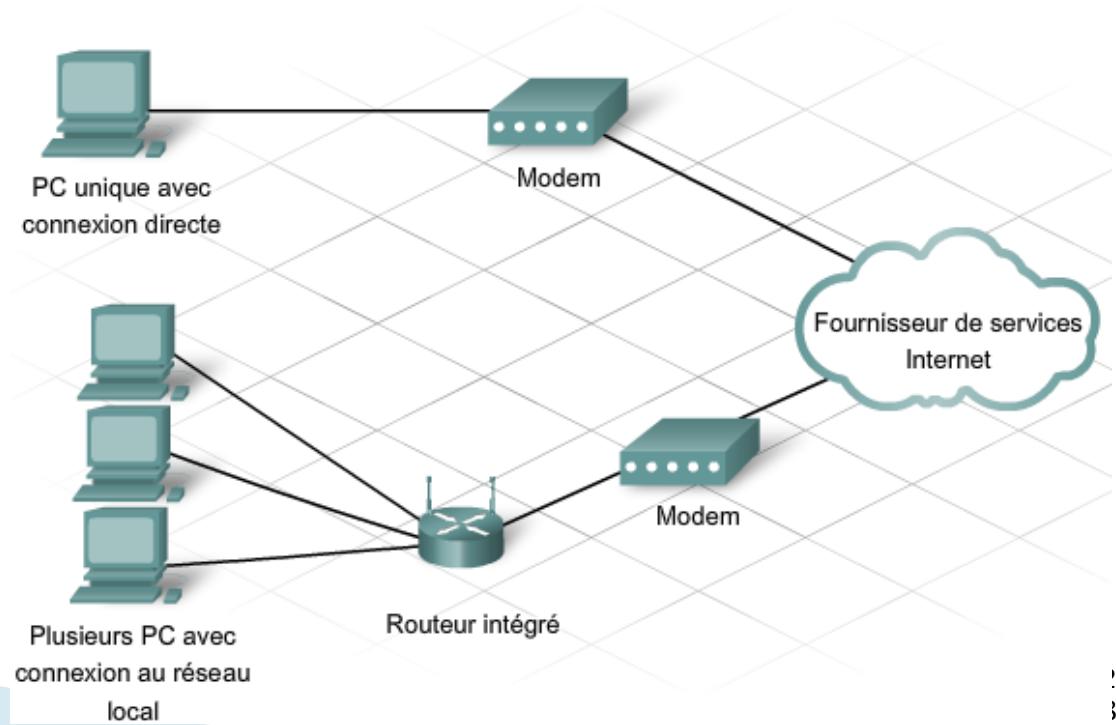
## ▶ Options de connexion au FAI



# Connexion à Internet via un fournisseur d'accès

## ▶ Options de connexion au FAI

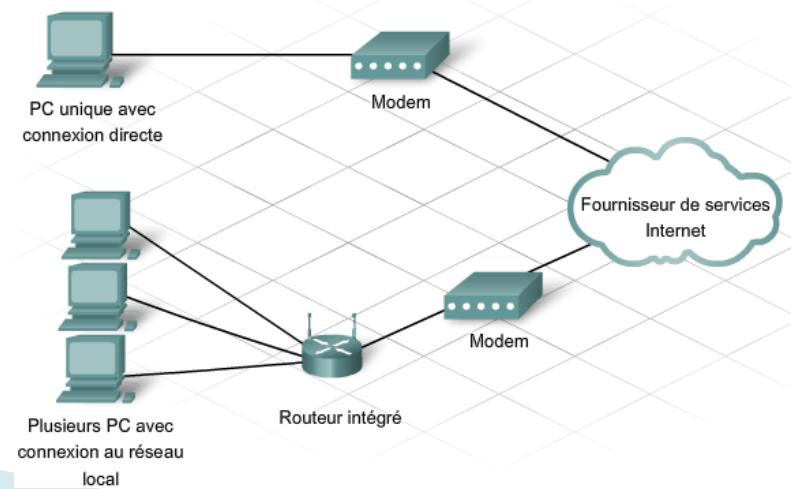
- **Pc unique avec connexion directe**
  - Le **modem** fournit une **connexion directe** entre un ordinateur et le FAI.



# Connexion à Internet via un fournisseur d'accès

## ▶ Options de connexion au FAI

- Plusieurs PC dans un réseau local
  - Un **commutateur** pour connecter plusieurs hôtes sur un réseau local, et un **routeur**, pour déplacer les paquets entre le réseau local et le réseau du FAI.
  - Ou un périphérique réseau domestique, tel qu'un **routeur intégré**, peut fournir à la fois ces fonctions, ainsi qu'une capacité sans fil.



# Connexion à Internet via un fournisseur d'accès

- ▶ Options de connexion au FAI
  - Routeur de Service Intégré (ISR)



- Conçu pour les utilisateurs à domicile et dans les petits bureaux
- 1 connexion WAN (port de routeur)
- 4 ports de commutateurs 10/100 Mbit/s
- Association des services de données, de sécurité et de sans fil
- Prestation de services à des débits large bande

# **Création de la couche de distribution du réseau**

- ▶ **Fonction des routeurs**
- ▶ **Tables tenues à jour par les routeurs**
- ▶ **Réseau LAN**
- ▶ **Ajout d'hôtes au réseaux et distants**
- ▶ **Utilisation du logiciel Packet Tracer**

# **Eléments de base de la sécurité des réseaux**

# Sécurité

- ▶ **Ne pas être exposé au danger**
- **Sentiment de n'être pas attaqué**

## Pour sécuriser

- **Répondre aux questions suivantes**
  - **Que cherche-t-on à protéger?**
  - **Contre quoi cherche-t-on à se protéger ?**
  - **De qui cherche-t-on à se protéger ?**

# **Vous avez dit «sécurité»?**

- ▶ **La sécurité au cœur des préoccupations ?**
  - **1 entreprise sur 3 a été victime d'une attaque en 2001**
  - **Pourtant 2,7% du budget informatique consacré à la sécurité**
- **L'absence de sécurité mène à :**
  - **L'espionnage industriel**
  - **La détérioration de l'image de marque**
  - **L'arrêt ou dégradation des services réseaux**
  - **Des pertes financières**
  - **Perte/manipulation de données**

# Que faut-il protéger?

- ▶ L'information stockée
- L'accès aux services externes
  - Site web, messagerie
- L'accès aux services internes
  - Intranet, Extranet, bases de données, ...
- La confidentialité des données
  - Qui peut accéder aux données ?
  - Comment peut-on y accéder ?

# De qui faut-il se protéger?

- **Menaces externes**
  - Proviennent de personnes travaillant à l'extérieur d'une organisation.
  - Elles ne disposent pas d'un accès autorisé aux systèmes informatiques ou au réseau.
- **Menaces internes**
  - Proviennent d'une personne disposant d'un accès autorisé au réseau (au moyen d'un compte utilisateur) ou d'un accès physique à l'équipement réseau.
  - Toutefois, toutes les attaques internes ne sont pas délibérées.
    - Dans certains cas, une menace interne provient d'un employé loyal qui, infecté par un virus ou une menace de sécurité en dehors de l'entreprise, introduit cette menace dans le réseau interne sans le savoir.

# De qui faut-il se protéger?

## ► Des pirates informatiques

- Les «scripts kiddies» qui utilisent des logiciels d'attaque trouvés sur Internet
- Les vrais pirates qui connaissent les protocoles et les systèmes

## • Les intrus criminels

- Ils ont plus de moyens que les pirates

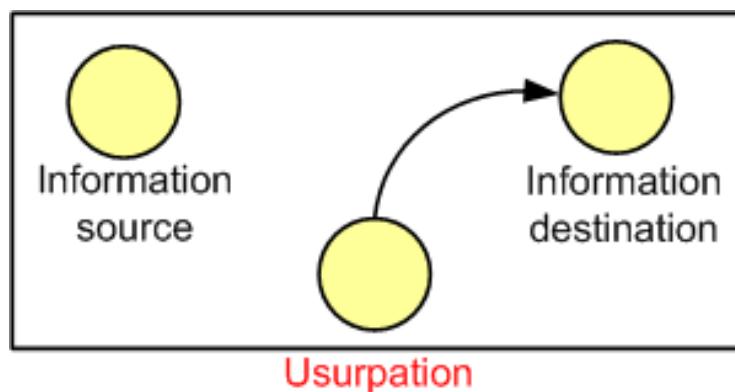
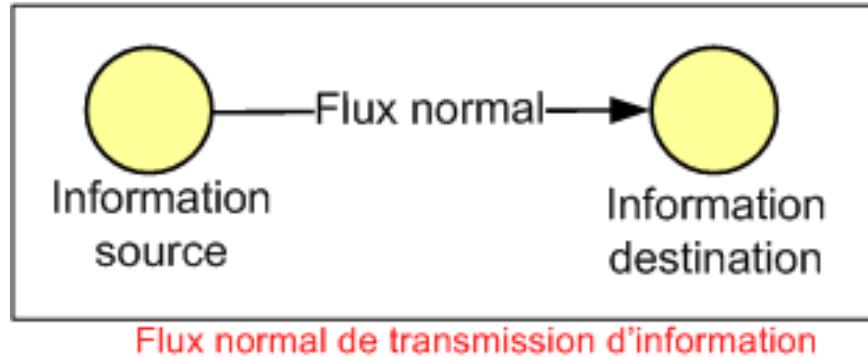
## • Terroristes industriels

- Ils ont d'énormes ressources

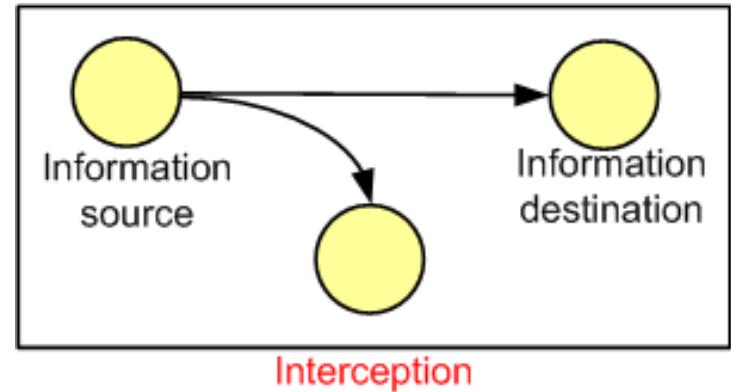
## • Employés ou fournisseurs

- Où comment la faille peut-elle venir de l'intérieur ?

# Les modèles d'attaques (1)

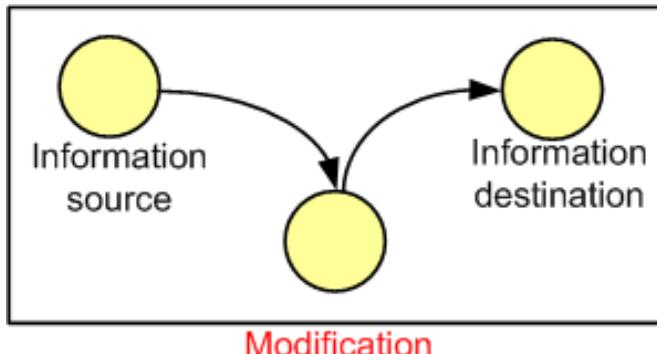


vise l'authenticité des informations



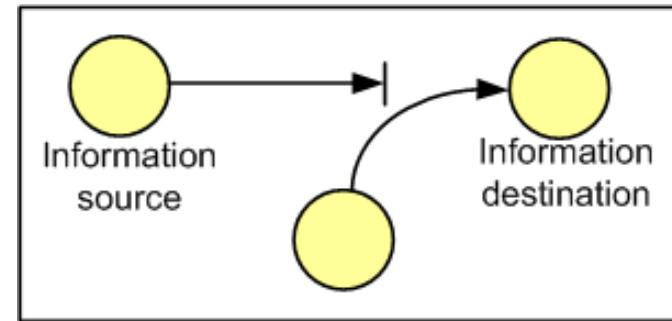
vise la confidentialité des informations

# Les modèles d'attaques (2)



Modification

vise l'intégrité des informations



Déni de service

vise l'authenticité et la disponibilité des informations

- Les parades aux 4 modèles d'attaques :
  - Authentification
  - Intégrité des données
  - Confidentialité des données
  - Disponibilité des données

# Comment se protéger ? (1)

## ▶ Authentification

- C'est le processus de vérification de l'identité
  - Interdire l'accès aux données à des tiers non autorisés
  - Interdire la modification des configurations des machines par des tiers non autorisés

## ▶ Confidentialité

- C'est l'assurance qu'une information n'est pas mise à disposition pour des individus, des entités ou des traitements non autorisées
  - Interdire l'interception ou la découverte d'informations par des tiers non autorisés

# Comment se protéger ? (2)

## ▶ Intégrité des données

- L’assurance qu’une information n’a pas été modifiée, détruite ou perdue de façon accidentelle ou intentionnelle
  - Ressources des systèmes et informations transmises doivent être modifiables uniquement par les parties autorisées

## ▶ Disponibilité

- L’assurance d’être disponible et joignable pour toute requête d’une entité autorisée
  - Sans doute la plus difficile à mettre en œuvre

# Gérer les autorisations

- ▶ **Il s'agit du point clé de la sécurité**
  - Qui est autorisé à faire quoi ?
- ▶ **L'autorisation est le droit ou la permission d'accéder à une ressource**
  - Par utilisateur ou groupe d'utilisateurs
- ▶ **Nécessité d'authentifier l'utilisateur**
  - Permet de déterminer ce à quoi l'utilisateur est autorisé
  - Permet également de garder une trace de son activité
- ▶ **Cas d'autorisations sans authentification**
  - Par exemple, un site web public

# La stratégie de sécurité

- ▶ **Ce que doit contenir la stratégie de sécurité :**
  - Répertorier qui est autorisé à faire quoi ?
  - Définir les dispositions à prendre en cas de violation
  - Comprendre parfaitement les risques encourus
  - Accepter ou diminuer les risques
- ▶ **Qui définit la stratégie de sécurité ?**
  - DSI (Directeur du Système d'Information) ou RSSI (Responsable de la Sécurité des Systèmes d'Information)
  - L'équipe technique

# Les approches sur la sécurité

- ▶ **Chaque entreprise n'a pas les mêmes besoins**
  - Les risques, les menaces et les coûts sont différents
- ▶ **Quatre approches génériques sont possibles**
  - Tout est autorisé
  - Tout ce qui n'est pas explicitement interdit est autorisé
  - Tout ce qui n'est pas explicitement autorisé est interdit
  - Tout est interdit
- ▶ **Pour réduire les risques, il faut :**
  - Choisir la bonne approche
  - Éliminer tous les risques qui ne concernent pas votre entreprise

# Analyse des risques

- ▶ **Le risque «zéro» n'existe pas**
- ▶ **On peut donc :**
  - **Ignorer les risques (Ne pas les traiter)**
    - Partir du principe que «ça n'arrivera jamais»
  - **Accepter les risques**
    - C'est pouvoir agir afin de limiter leur portée
    - Les risques existeront toujours mais avec une portée limitée
- ▶ **Deux facteurs influencent le fait d'ignorer ou d'accepter**
  - La probabilité qu'ils se produisent est vraiment très faible
  - Le coût pour limiter les risques est trop élevé

# Accepter les risques

- ▶ **Qu'est-ce qu'un risque acceptable ?**
  - **Un risque dont le coût de l'antidote est minime**
  - **Un risque induit par la nature même de l'activité de l'entreprise**
    - Exemple : Un site web marchand
- ▶ **Savoir lutter contre le risque**
  - **Éviter qu'un évènement se produise**
    - Interdire l'utilisation d'Internet !!!?
  - **Mettre en œuvre des solutions techniques**
    - Firewall par exemple

# Exemple d'analyse

- ▶ **Une inondation se produit**
  - Cela peut nuire gravement à l'activité de l'entreprise
- ▶ **Vous pouvez espérer que cela n'arrive jamais**
  - Vous ignorez alors le risque
- ▶ **Vous prenez une bonne assurance**
  - On ne traite pas le risque mais on en limite les conséquences
- ▶ **On peut installer une salle étanche**
  - On lutte contre le risque
- ▶ **Il y a toujours des risques résiduels**
  - Quelqu'un laisse la porte ouverte
  - On prend quand même une assurance

# Méthodes d'attaques

- ▶ **Le piratage psychologique**
  - Cela peut nuire gravement à l'activité de l'entreprise
- ▶ **Vous pouvez espérer que cela n'arrive jamais**
  - Vous ignorez alors le risque
- ▶ **Vous prenez une bonne assurance**
  - On ne traite pas le risque mais on en limite les conséquences
- ▶ **On peut installer une salle étanche**
  - On lutte contre le risque
- ▶ **Il y a toujours des risques résiduels**
  - Quelqu'un laisse la porte ouverte
  - On prend quand même une assurance

# Méthodes d'attaques

- ▶ **Le piratage psychologique**
  - Exploite les vulnérabilités humaines
- ▶ **Virus, vers et chevaux de Troie**
  - Exploitent les vulnérabilités logicielles
- ▶ **Attaques par déni de service et attaques en force**
- ▶ **Logiciels espion, cookies traceurs, logiciels de publicité et fenêtres intempestives**
- ▶ **Courriers indésirables**

# Le piratage psychologique

- ▶ **Fait référence à un ensemble de techniques utilisées pour**
  - **tromper des utilisateurs internes**
    - **leur faire effectuer des actions spécifiques**
      - ou révéler des informations confidentielles.
- ▶ **le pirate profite d'utilisateurs légitimes confiants pour accéder**
  - **à des ressources internes et à des informations privées,**
    - **telles que des numéros de comptes bancaires ou des mots de passe.**
- ▶ **Les trois techniques les plus souvent employées par le piratage psychologique sont :**
  - **l'usurpation, l'hameçonnage et l'hameçonnage vocal.**

# Usurcation

- ▶ **Le scénario inventé (le prétexte) est utilisé sur une victime afin d'obliger celle-ci**
  - à fournir des informations
  - ou à effectuer une
- ▶ **En général, la cible est contactée par téléphone.**
- ▶ **Par exemple, si un pirate connaît le numéro de sécurité sociale de la cible,**
  - il peut utiliser cette information pour gagner sa confiance.
  - La victime fournit alors des informations supplémentaires plus facilement.

# Hameçonnage

- ▶ Le pirate prétend représenter une organisation extérieure légitime.
- ▶ En général, il contacte la personne ciblée par courriel.
- ▶ Le pirate demande des informations de vérification, telles que des noms d'utilisateur ou des mots de passe, afin d'empêcher de prétendues conséquences terribles.

# Hameçonnage vocal/téléphonique

- ▶ Exploite la **voix sur IP**.
- ▶ Un message vocal est envoyé à un utilisateur sans méfiance,
  - lui demandant d'appeler un numéro qui semble accéder à un service bancaire téléphonique légitime.
- ▶ L'appel est ensuite intercepté par un voleur.
  - Les **numéros de comptes bancaires** ou les **mots de passe** saisis par téléphone pour vérification sont alors **volés**.

# Virus, vers et chevaux de Troie

- ▶ Ces types d'attaques exploitent les **vulnérabilités des logiciels informatiques**
- ▶ Elles introduisent du **logiciel malveillant** dans un hôte.
- ▶ Ce logiciel peut
  - **endommager** un système,
  - **détruire** des données
  - et **interdire l'accès** à des réseaux, des systèmes ou des services.
  - également **transférer à des pirates** les données et les informations personnelles d'utilisateurs de PC confiants
- ▶ Dans de nombreux cas,
  - ce logiciel peut se **dupliquer** et se **répandre** sur d'autres hôtes connectés au réseau.

# Virus

- ▶ Programme qui s'exécute et se répand en **modifiant d'autres programmes ou d'autres fichiers**.
- ▶ Un virus **ne peut pas démarrer de lui-même**. Il doit être activé.
- ▶ Une fois activé, un virus peut limiter son activité à se **dupliquer et se répandre**.



# Virus

- ▶ **il peut rapidement**
  - utiliser toute la mémoire disponible
  - et arrêter le système,
  - être programmé pour supprimer ou altérer des fichiers spécifiques avant de se répandre.
- ▶ **Les virus peuvent être transmis par**
  - des pièces jointes aux courriels,
  - des fichiers téléchargés,
  - des messages instantanés
  - ou bien par des disquettes, des CD ou des périphériques USB.

# Vers

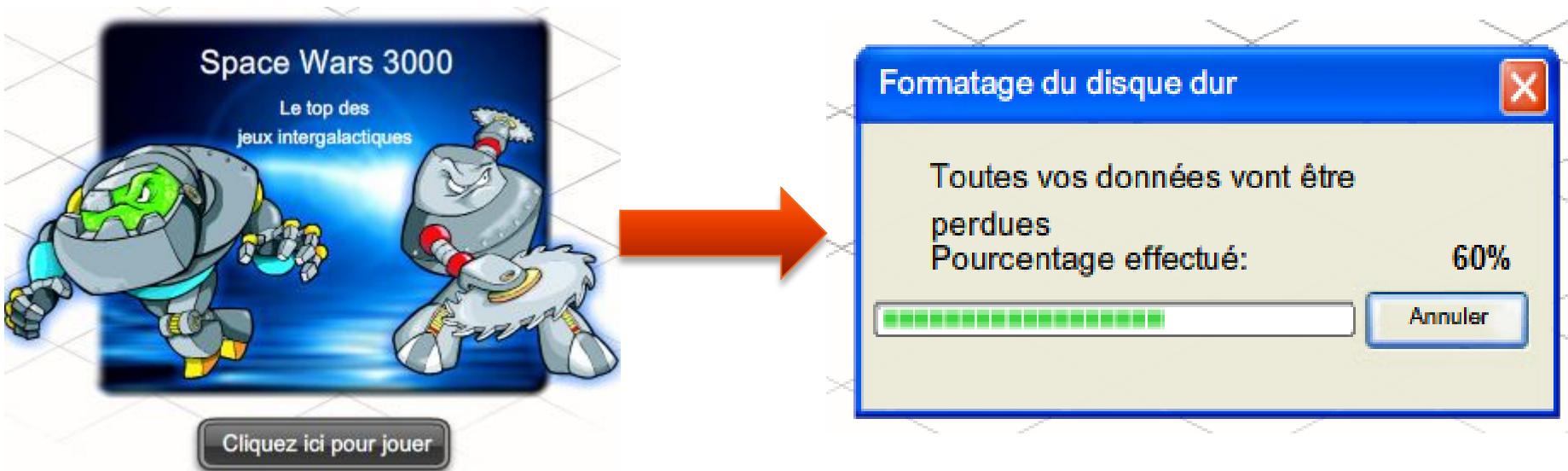
- ▶ **Similaires à un virus,**
  - mais il n'a pas besoin **de se lier à un programme existant.**
- ▶ **Utilisent le réseau pour envoyer ses propres répliques à tout hôte connecté.**
- ▶ **Ils ne nécessitent pas toujours une activation ou une intervention humaine.**
- ▶ **Les vers de réseau qui s'autopropagent peuvent**
  - **avoir un impact beaucoup plus important qu'un virus unique**
  - **et infecter rapidement de grandes parties d'Internet.**

# Cheval de Troie

- ▶ **Un cheval de Troie est un programme**
  - qui ne se duplique pas automatiquement
  - et qui est codé pour présenter l'apparence d'un programme légitime,
  - alors qu'il s'agit en fait d'un outil d'attaque.
- ▶ **Un cheval de Troie compte sur son apparence légitime**
  - pour tromper la victime afin qu'elle démarre ce programme.

# Cheval de Troie

- Il peut être relativement inoffensif ou contenir du code capable d'endommager le contenu du disque dur de l'ordinateur.



# Cheval de Troie

- ▶ Les chevaux de Troie peuvent également ouvrir une porte dérobée dans un système pour donner accès à des pirates informatiques

# Attaques par déni de service et attaque en force

- ▶ Un pirate a parfois pour objectif
  - **d'arrêter le fonctionnement normal d'un réseau.**
- ▶ Il souhaite, par une telle attaque,
  - **perturber les fonctions d'une organisation.**

# Déni de service (DoS, Denial of Service)

- ▶ **Attaques agressives**
  - sur un **ordinateur individuel**
  - ou sur des **groupes d'ordinateurs**
    - visant à **refuser des services aux utilisateurs prévus.**
- ▶ **Les attaques DoS peuvent cibler**
  - les **systèmes d'utilisateurs finaux,**
  - les **serveurs,**
  - les **routeurs**
  - et les **liaisons réseau.**

# Déni de service (DoS, Denial of Service)

- ▶ En général, les attaques DoS tentent :
  - d'inonder de trafic
    - un système ou un réseau
    - pour bloquer le trafic réseau légitime ;
  - de perturber
    - les connexions entre un client et un serveur
    - pour interdire l'accès à un service.

# Déni de service (DoS, Denial of Service)

- ▶ Exemples d'attaque DOS
  - Inondation SYN
    - un très grand nombre de paquets, demandant une connexion client, sont envoyés à un serveur.
    - Les paquets contiennent des adresses IP sources non valides.
    - Le serveur tentant de répondre à ces fausses requêtes devient trop occupé pour répondre aux requêtes légitimes.

# Déni de service (DoS, Denial of Service)

- ▶ Exemples d'attaque DOS
  - Inondation SYN

