

# **Les Réseaux Informatiques**

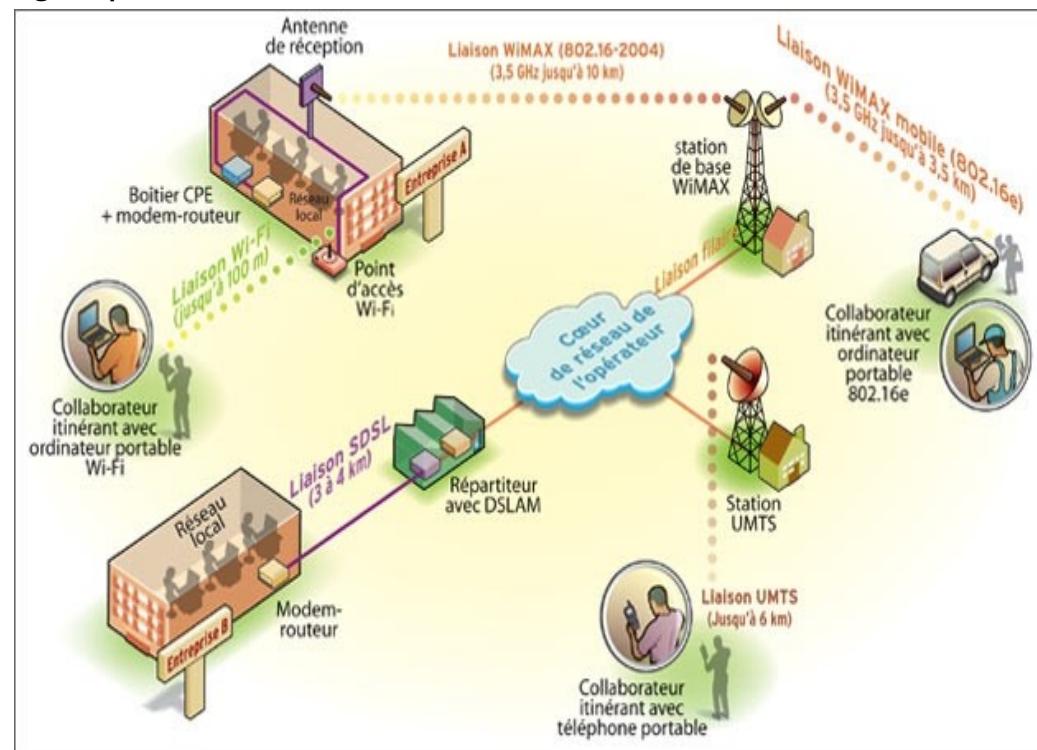
# Introduction

## • Qu'est ce qu'un réseau de télécommunications?

- Un réseau de télécommunications est un ensemble de nœuds connectées entre eux par des liens, mis en place de telle sorte que des messages puissent être transmis d'un bout à l'autre du réseau.

Exemples :

- réseau informatique
  - réseau de téléphonie mobile
  - réseau téléphonique commuté ...
- 
- Ces réseaux sont principalement formés de quatre éléments :
    - Les périphériques finaux
    - Les périphériques intermédiaires
    - Les médias
    - Les services



# Périphériques finaux

- Un périphérique final, appelé aussi hôte, est la source ou la destination d'un message transmis sur le réseau. Pour qu'il soit possible de distinguer les périphériques finaux, chaque périphérique final présent sur un réseau est identifié à l'aide d'une adresse. Lorsqu'un périphérique final initie une communication, il utilise l'adresse du périphérique final de destination afin de spécifier l'emplacement où le message doit être envoyé.

Exemple de périphériques finaux :

- PC Client
- Serveur
- Imprimante
- Tablette
- Téléphone IP
- ...



# Périphériques intermédiaires

- Les périphériques intermédiaires connectent les périphériques finaux au réseau et peuvent connecter plusieurs réseaux afin de former un inter-réseau. Ils utilisent l'adresse du périphérique final de destination, ainsi que les informations concernant les interconnexions réseau, pour déterminer le chemin que doivent emprunter les messages à travers le réseau.
- Parmi les fonctions qu'ils effectuent :
  - Régénération de signal et retransmission des messages
  - Déterminer les meilleurs chemin pour délivrer les messages
  - Déetecter et indiquer les erreurs de communication
  - Gérer les priorités des messages
  - Bloquer ou autoriser des messages selon des règles de sécurité
  - ...
- Exemple d'équipement intermédiaires :
  - Modem, commutateur, routeur, point d'accès sans fil, pare-feu ...

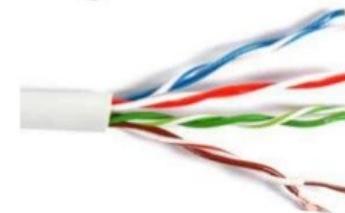


# Les médias

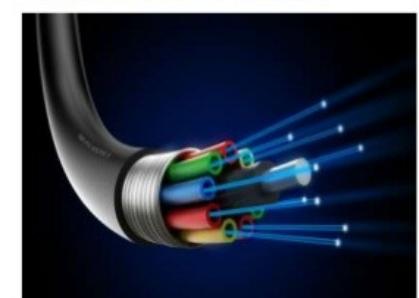
- La communication à travers un réseau s'effectue sur un support de transmission de données (média). Ce support fournit le canal via lequel le message se déplace de la source à la destination.
- Les réseaux modernes utilisent principalement trois types de supports pour interconnecter des périphériques et fournir le chemin par lequel des données peuvent être transmises :
  - Les câbles électriques  
(paire torsadées non blindée,  
paire torsadée blindée,  
câble coaxial).
  - La fibre optique (monomode,  
multimode)
  - Les ondes électromagnétiques  
(WIFI, WIMAX, Bluetooth, ...)



**COAXIAL CABLE**



**UNSHIELDED TWISTED-PAIR (UTP) CABLE**



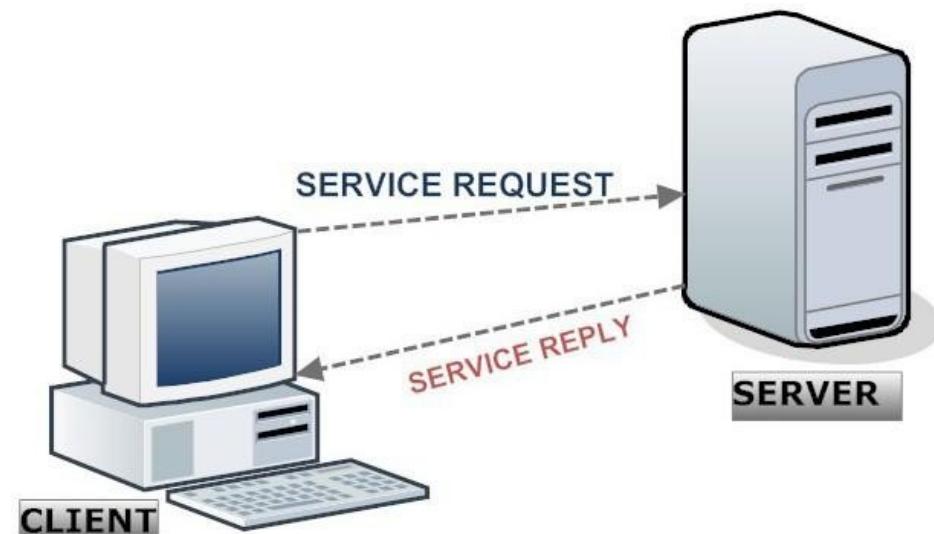
**FIBER OPTIC CABLE**



**SHIELDED TWISTED-PAIR (STP) CABLE**

# Les services

- Il existe une grande variété de logiciels serveurs appelés services en fonction des besoins à servir : un serveur web (HTTP), par exemple, publie des pages web demandées par des navigateurs web; un serveur de messagerie électronique (SMTP, POP, IMAP) gère les échanges des mails entre les clients de messagerie; un serveur de fichiers (FTP) permet de stocker et consulter des fichiers sur le réseau..
- Caractéristiques d'un processus serveur :
  - il attend une connexion entrante sur un ou plusieurs ports réseaux locaux;
  - à la connexion d'un client sur le port en écoute, il ouvre un socket local au système d'exploitation;
  - à la suite de la connexion, le processus serveur communique avec le client suivant le protocole prévu par la couche application du modèle OSI.



# Quelques types de réseaux

- Les réseaux peuvent être classifiés selon leur taille ou selon leurs fonctionnalités. Ainsi on peut citer dans la première catégorie les types de réseaux suivants :
- **LAN** (Local Area Network) ou réseau local : infrastructure réseau reliant les utilisateurs et les périphériques finaux dans une zone géographique peu étendue ; il s'agit généralement d'un réseau de petite ou moyenne entreprise ou d'un réseau domestique, dont le propriétaire et le gestionnaire sont un individu ou un service IT.
- **WAN** (Wide Area Network) ou réseau étendu : infrastructure réseau permettant d'accéder à d'autres réseaux au sein d'une zone géographique étendue, qui appartient généralement à un prestataire de services et dont la gestion est assurée par ce dernier.
- **MAN** (Metropolitan Area Network) ou réseau intermédiaire : infrastructure réseau qui couvre une zone plus vaste qu'un LAN, mais moins étendue qu'un WAN (par exemple, une ville). Les MAN sont généralement gérés par une seule entité, comme une grande entreprise.
- **PAN** (Personal Area Network) ou réseau personnel : désigne un type de réseau informatique restreint en terme d'équipements, généralement mis en œuvre dans un espace d'une dizaine de mètres. D'autres appellations pour ce type de réseau sont: réseau domestique ou réseau individuel. Exemple : l'USB, Bluetooth, l'infrarouge (IR)...

# Réseaux selon leur fonctionnalités

- **LAN sans fil (WLAN)** : infrastructure similaire à un réseau local, mais sans fil. Elle relie des utilisateurs et des terminaux situés dans une zone peu étendue.
- **SAN (Storage Area Network - Réseau de stockage)** : infrastructure réseau conçue pour prendre en charge des serveurs de fichiers et pour fournir des fonctionnalités de stockage, de récupération et de réPLICATION de données.
- **VPN (Virtual Private Network – Réseau Privé Virtuel)** : Solution permettant l'échange sécurisé de données à travers un réseau public tel qu'Internet, en utilisant des techniques de cryptographie.
- **VLAN (Virtual LAN – Réseau Local Virtuel)** : Solution permettant de créer plusieurs réseaux LAN virtuels au sein d'un même réseau LAN physique, afin de permettre d'isoler le trafic de différents services entre eux.
- **Intranet** : Le terme intranet est souvent utilisé pour faire référence à une connexion privée de réseaux LAN et WAN qui appartient à une entreprise ou une administration, et à laquelle peuvent accéder uniquement ses membres, ses employés ou des tierces personnes autorisées.
- **Extranet** : Une entreprise peut utiliser un extranet pour fournir un accès sécurisé aux personnes qui travaillent pour une autre entreprise, mais qui ont besoin d'accéder aux données de l'entreprise en question.

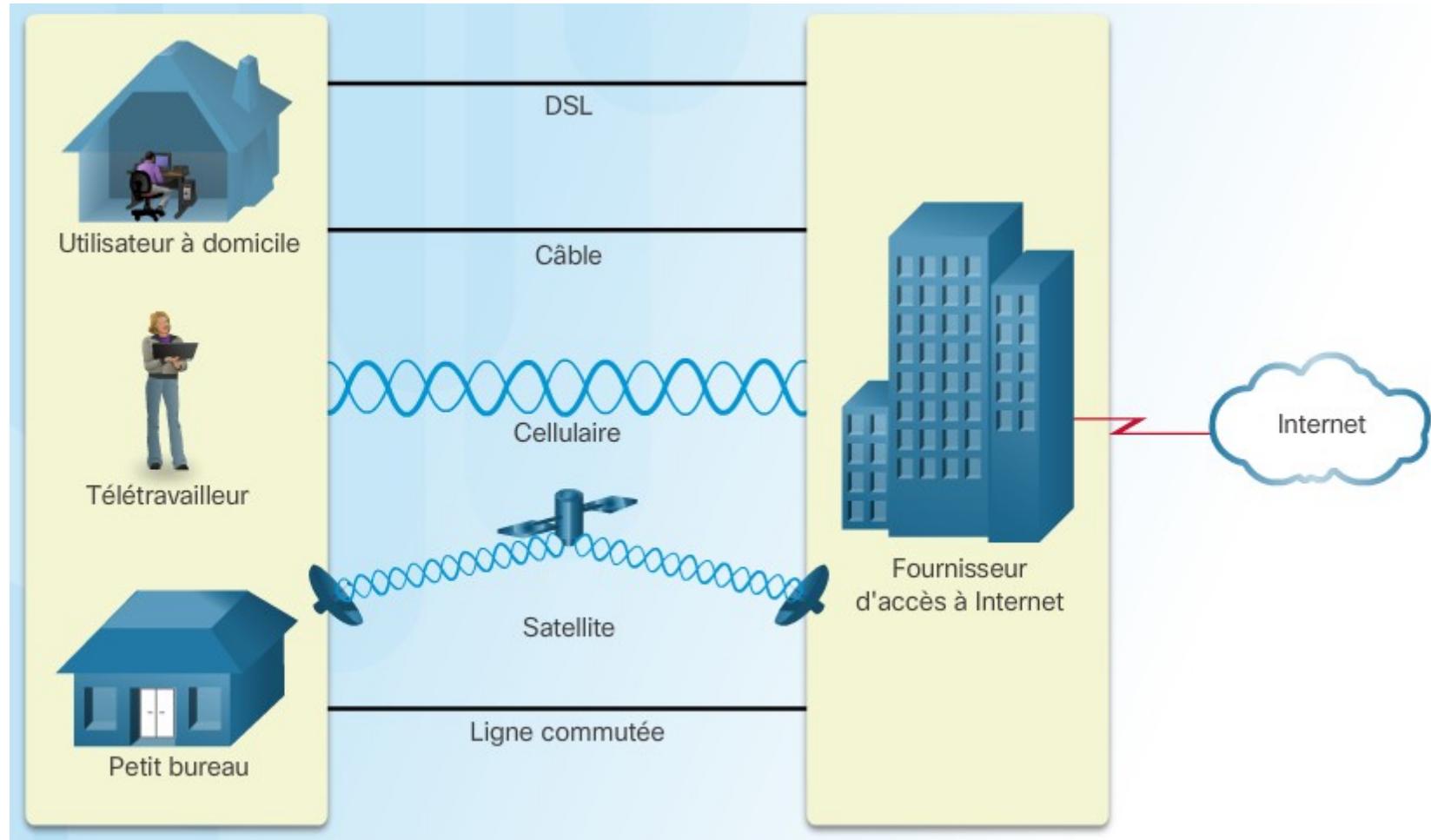
# Technologies d'accès

- Il existe plusieurs manières de connecter des utilisateurs et des entreprises à Internet.
- Les utilisateurs à domicile, les télétravailleurs (travailleurs à domicile) et les PME ont généralement besoin d'un fournisseur d'accès à Internet (FAI) pour se connecter à Internet. Les options de connexion varient considérablement d'un FAI et d'une région à l'autre. Cependant, les options les plus utilisées sont le câble haut débit, la technologie DSL (Digital Subscriber Line) haut débit, les WAN sans fil et les services mobiles.
- Les entreprises ont généralement besoin d'un accès aux autres sites professionnels et à Internet. Des connexions rapides sont requises pour prendre en charge les services d'entreprise, notamment les téléphones IP, la vidéoconférence, ainsi que le stockage dans des data centers.
- Les connexions professionnelles sont généralement fournies par des prestataires de services. Les services professionnels les plus courants sont la DSL, les lignes louées et les solutions Metro Ethernet.

# Bureaux à domicile et petits bureaux

- **Câble** : généralement proposé par les fournisseurs de services de télévision par câble, le signal de données Internet est transmis grâce au câble utilisé pour la télévision par câble. Il offre une connexion permanente à Internet haut débit.
- **DSL** : les lignes d'abonné numérique offrent une connexion permanente à Internet haut débit. La technologie DSL utilise une ligne téléphonique. En général, un utilisateur de bureau à domicile ou de petit bureau se connecte à l'aide d'une ligne ADSL (Asymmetric Digital Subscriber Line), sur laquelle la vitesse descendante est supérieure à la vitesse ascendante.
- **Cellulaire** : l'accès Internet cellulaire utilise un réseau de téléphonie mobile. Partout où vous captez un signal cellulaire, vous pouvez accéder à Internet. Les performances sont cependant limitées par les fonctionnalités du téléphone et de la station de base à laquelle l'appareil est connecté.
- **Satellite** : la disponibilité de l'accès Internet par satellite constitue un réel avantage dans les régions qui n'ont aucune autre possibilité d'accéder à Internet. Les paraboles nécessitent une visibilité directe sur le satellite.
- **Ligne commutée** : option peu onéreuse nécessitant une ligne téléphonique et un modem. La faible bande passante des connexions par ligne commutée n'est généralement pas suffisante pour les transferts de données importants, mais cette solution reste utile pour accéder à Internet lors d'un déplacement.

# Bureaux à domicile et petits bureaux



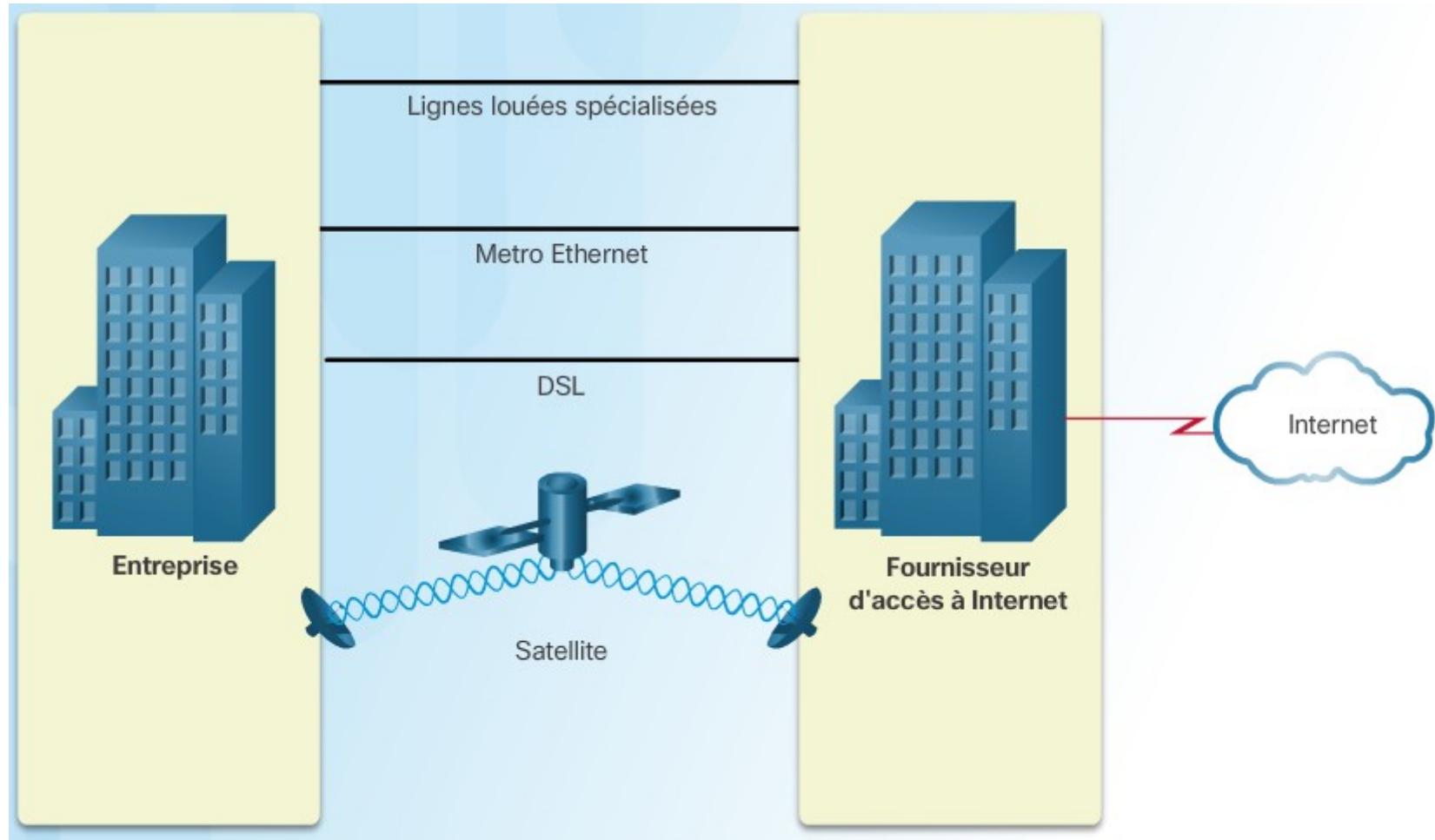
# Normes de téléphonie mobile

- Evolution des normes de téléphonie mobiles :
  - **1G (Radiocom 2000)** : Analogique
  - **2G (GSM)** : Numérique, débit = 9.05 kbit/s
  - **2.5G (GPRS)** : Numérique, débit = 171.2 kbit/s
  - **2.75G (EDGE)** : Numérique, débit = 384 kbit/s
  - **3G (UMTS)** : Numérique, débit = 1.9 Mbit/s
  - **3.5G (HSPA)** : Numérique, débit = 14.4 Mbit/s
  - **3.75G (HSPA+)** : Numérique, débit = 21 Mbit/s
  - **4G (LTE)** : Numérique, débit = 150 Mbit/s
  - **4G+ (LTE Advanced)** : Numérique, débit = 1 Gbit/s
  - **4.5G (LTE-A)** : Numérique, débit = 3 Gbit/s
  - **5G (LTE-B)** : Numérique, débit = 50 Gbit/s

# Solutions pour les entreprises

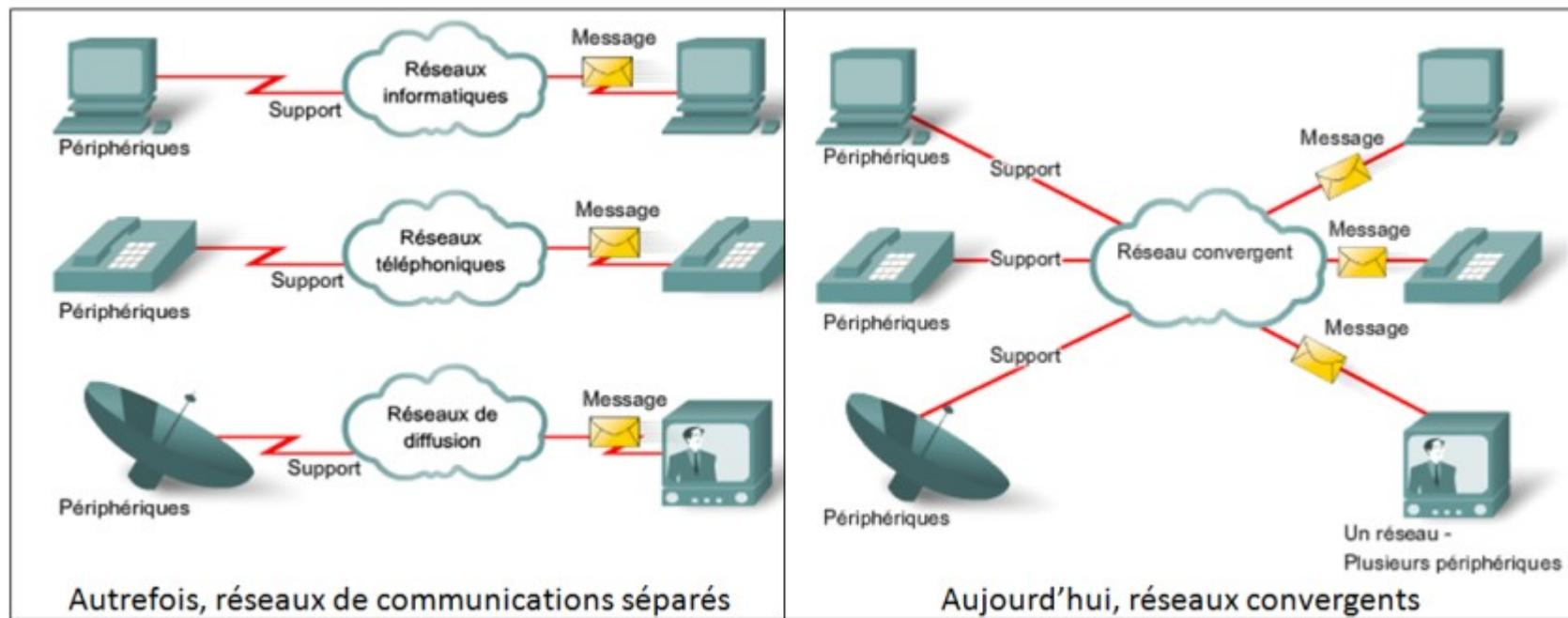
- **Lignes louées** : les lignes louées sont des circuits dédiés appartenant au réseau du fournisseur d'accès qui relient des bureaux distants pour permettre la transmission de données et/ou de communications vocales privées. Les circuits sont généralement loués sur une base mensuelle ou annuelle. Cette solution peut être onéreuse.
- **WAN Ethernet** : les réseaux WAN Ethernet étendent la technologie d'accès des réseaux LAN au réseau étendu.
- **DSL** : la DSL d'entreprise est disponible dans divers formats. La SDSL (ligne d'abonné numérique à débit symétrique) est largement utilisée. Cette solution est similaire à la version grand public de la technologie DSL, mais elle offre les mêmes débits de téléchargement ascendant et descendant.
- **Satellite** : comme c'est le cas pour les utilisateurs de bureau à domicile et de petits bureaux, le service par satellite peut fournir une connexion lorsqu'aucune solution par câble n'est disponible.

# Solutions pour les entreprises



# Réseaux convergents

- Actuellement, les réseaux de données, téléphoniques et de vidéo distincts sont en train de converger. Contrairement aux réseaux spécialisés, les réseaux convergents peuvent transmettre des données, de la voix et des flux vidéo entre différents types d'appareil, par le biais d'une même infrastructure réseau.



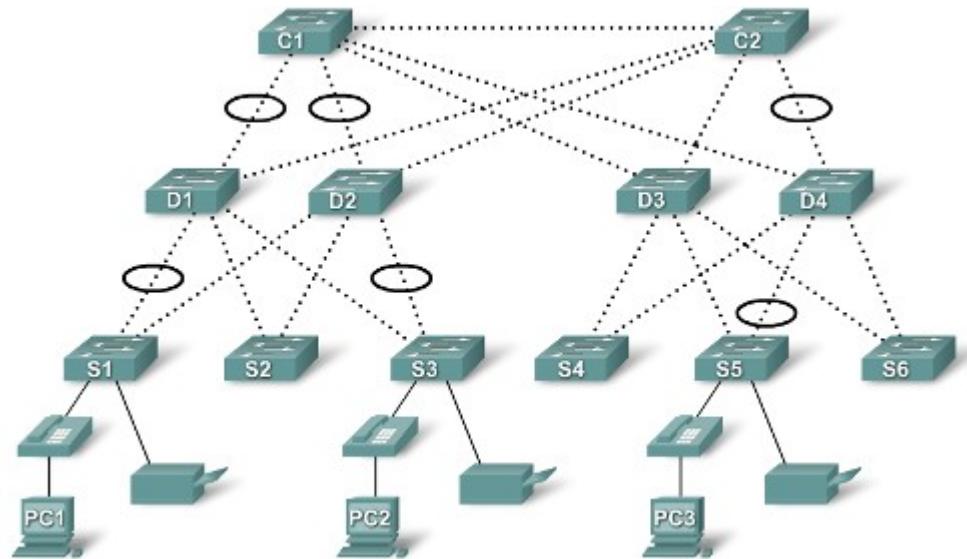
# Exigences des réseaux d'entreprise

- À mesure que les réseaux évoluent, les architectures qui en résultent doivent prendre en considération quatre caractéristiques de base si elles veulent répondre aux attentes des utilisateurs : la tolérance aux pannes, l'évolutivité, la qualité de service (QoS), et la sécurité.



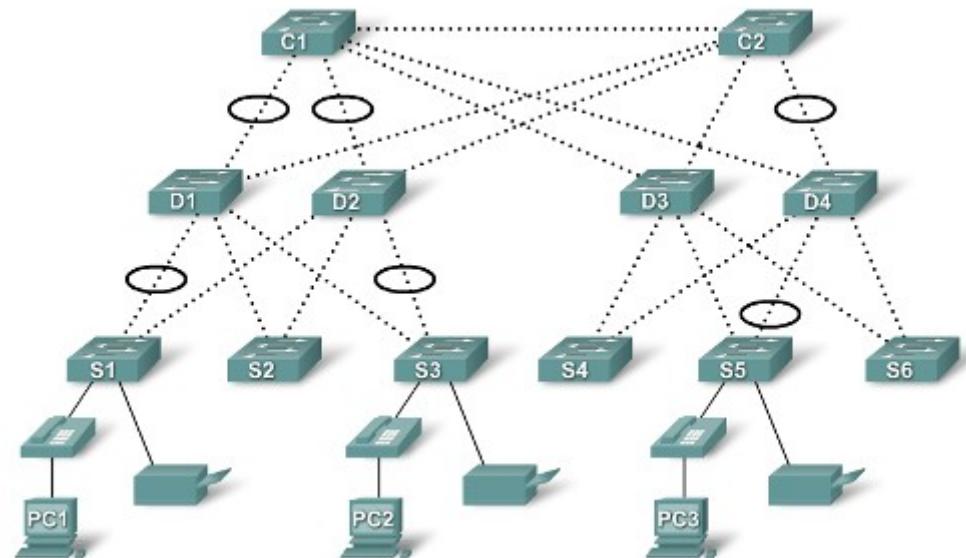
# Tolérance aux pannes

- Un réseau tolérant aux pannes est un réseau qui limite l'impact des pannes, de telle sorte que le nombre de périphériques affectés soit le plus faible possible. Il est également conçu de façon à permettre une récupération rapide en cas de panne. De tels réseaux s'appuient sur plusieurs chemins entre la source et la destination d'un message. Si l'un des chemins est défaillant, le message peut instantanément être envoyé par le biais d'une autre liaison. Le fait de disposer de plusieurs chemins vers une destination s'appelle la redondance.



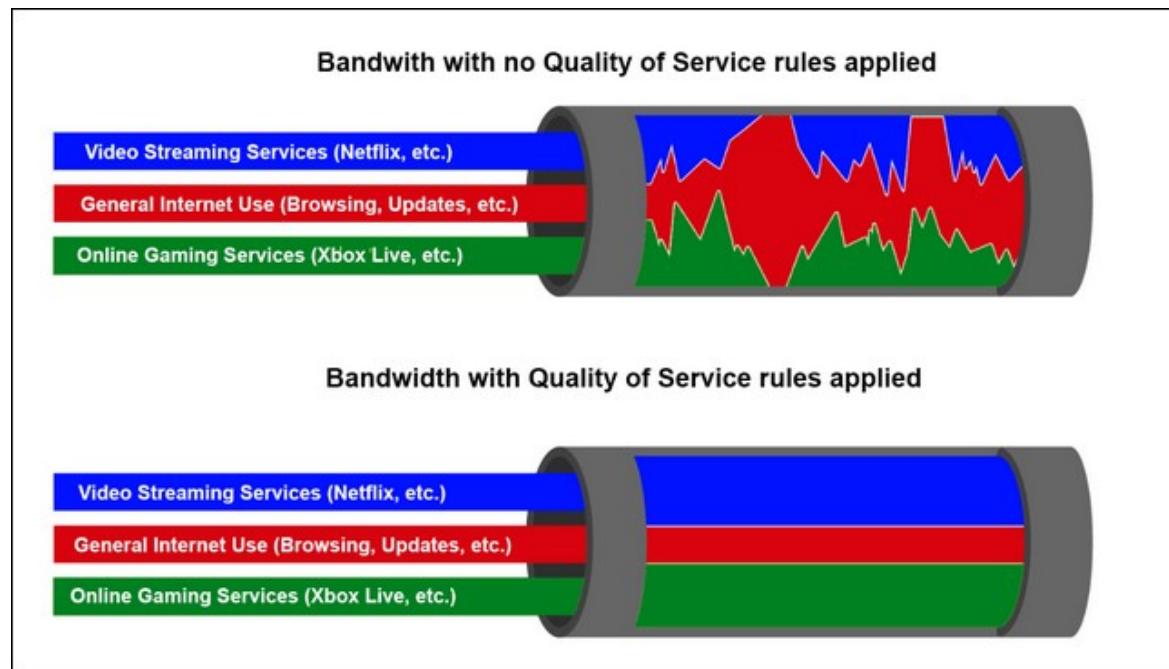
# Évolutivité

- Un réseau évolutif est en mesure de s'étendre rapidement afin de prendre en charge de nouveaux utilisateurs et applications sans que cela n'affecte les performances du service fourni aux utilisateurs existants.



# Qualité de service (QoS)

- Tandis que les données, les communications voix et le contenu vidéo convergent sur le même réseau, la QoS constitue un mécanisme essentiel pour gérer l'encombrement et assurer une fourniture fiable et rapide des contenus prioritaires.
- Lorsqu'une politique de Qualité de service (QoS) est mise en œuvre, les routeurs peuvent gérer le flux de données et le trafic de la voix et la vidéo en donnant la priorité aux communications voix et vidéo en cas de congestion du réseau.



# Sécurité

- Deux aspects de la sécurité du réseau doivent être pris en compte : la sécurité de l'infrastructure réseau et la sécurité de l'information.
- Sécuriser l'infrastructure réseau implique de sécuriser matériellement les périphériques qui assurent la connectivité du réseau et d'empêcher tout accès non autorisé au logiciel de gestion qu'ils hébergent.
- Sécuriser l'information consiste à protéger les informations contenues dans les paquets transmis sur le réseau, ainsi que les informations stockées sur les périphériques reliés au réseau.

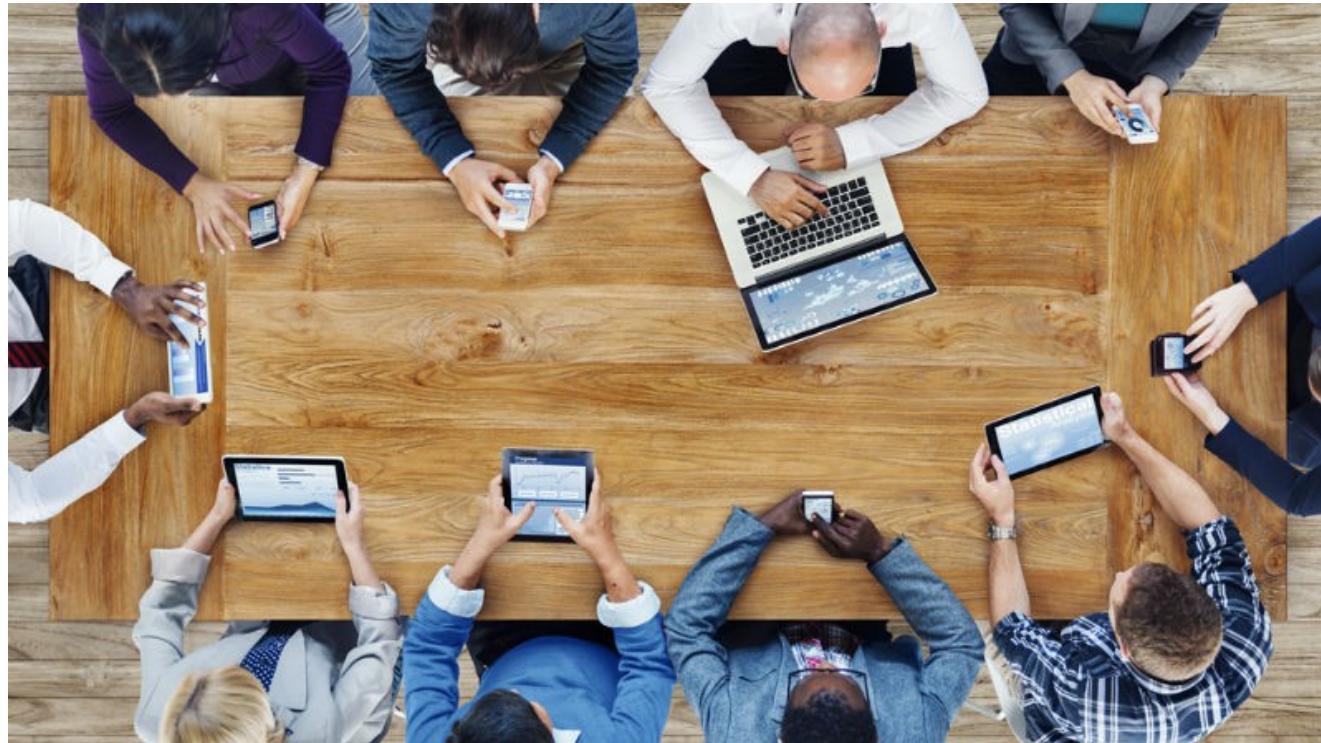


# Nouvelles tendances

- Il existe plusieurs nouvelles tendances relatives au réseau qui vont affecter les entreprises et les consommateurs. Les plus répandues sont les suivantes :
  - BYOD (Bring Your Own Device)
  - Collaboration en ligne
  - Communications vidéo
  - Cloud computing

# BYOD (Bring Your Own Device)

- Le BYOD consiste à donner aux utilisateurs finaux la liberté d'utiliser leurs propres périphériques pour accéder aux informations et communiquer au sein d'un réseau d'entreprise ou de campus universitaire. Ces outils personnels incluent notamment des ordinateurs portables, des netbooks, des tablettes, des smartphones ...



# Collaboration en ligne

- La collaboration est définie comme «le fait de travailler avec une ou plusieurs autres personnes sur un projet commun». Pour les entreprises, la collaboration est une priorité vitale et stratégique qui leur permet de rester compétitives.



# Communication vidéo

- La vidéoconférence est un outil puissant pour communiquer avec d'autres utilisateurs à distance, tant au niveau régional qu'international. La vidéo devient une condition essentielle pour collaborer efficacement à mesure que les entreprises se développent au-delà des frontières géographiques et culturelles.



# Cloud computing

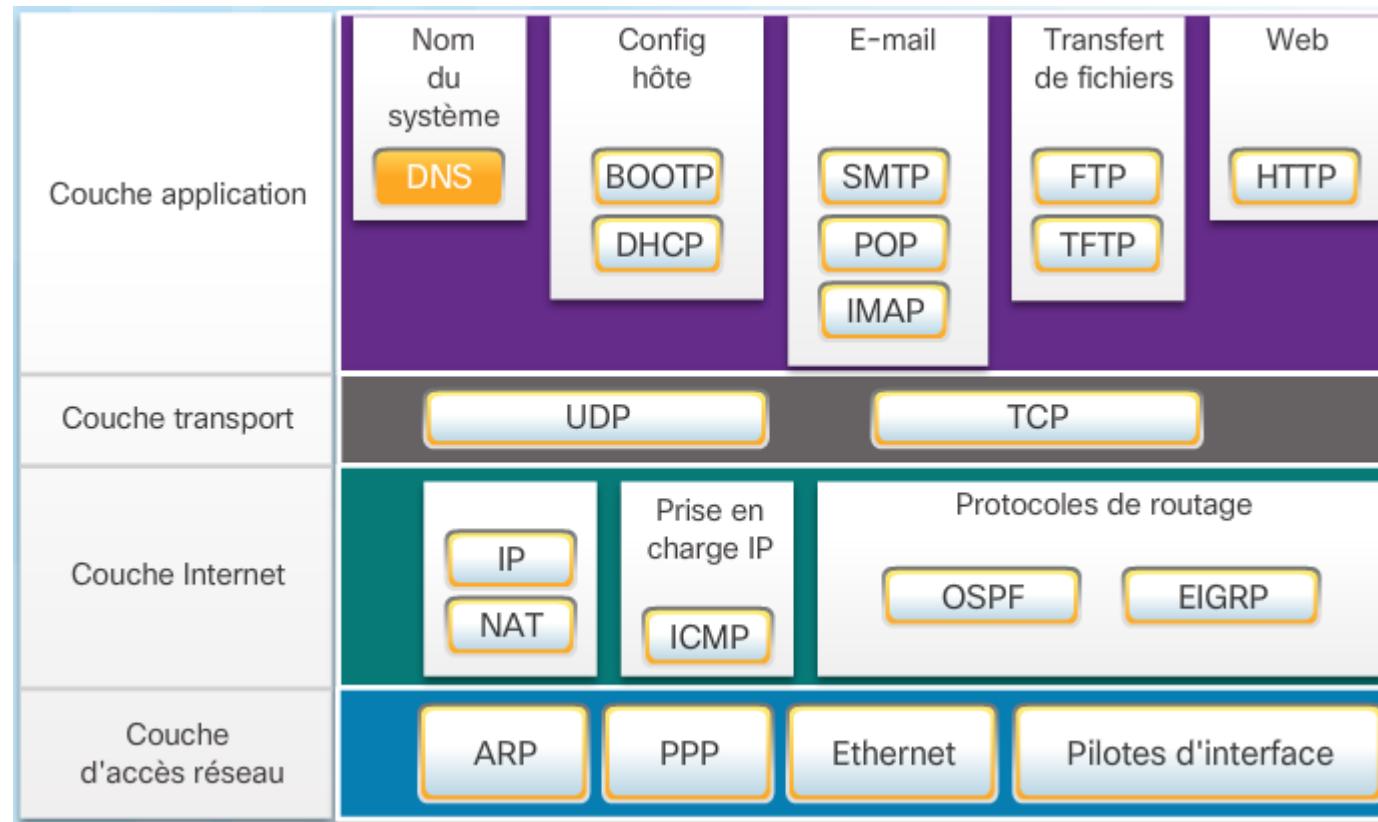
- Le cloud computing nous permet de stocker des fichiers personnels, voire de sauvegarder tout le contenu d'un disque dur sur des serveurs via Internet. Des applications telles que le traitement de texte et la retouche photo peuvent être accessibles par le biais du cloud.
- Le cloud computing fonctionne grâce aux data centers. Un data center héberge des systèmes informatiques et les composants associés. La construction et l'entretien des data centers sont en général très coûteux. Les entreprises de plus petite taille, qui ne peuvent pas se permettre de posséder leur propre data center privé, peuvent réduire le coût total de possession en louant des services de stockage et de serveur cloud à une grande entreprise proposant des data centers.



# Quelques définitions

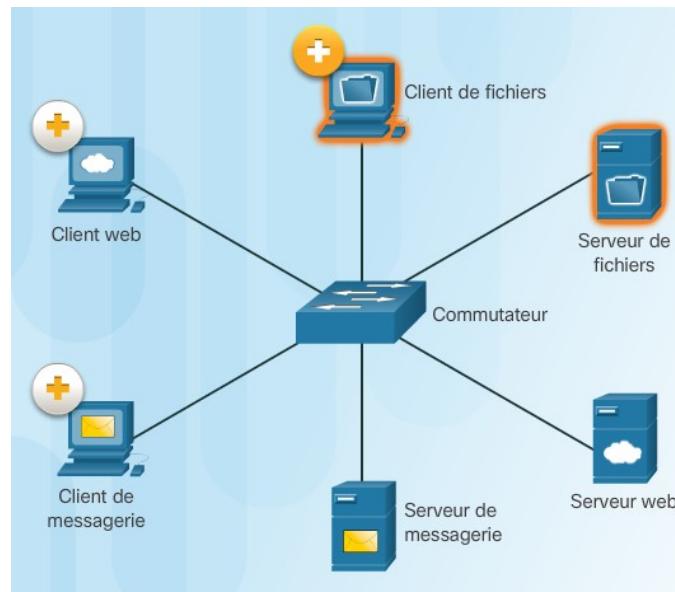
# Protocoles de communication

- Les protocoles réseau définissent un format et un ensemble communs de règles d'échange des messages entre les périphériques. Les protocoles suivants sont des exemples de protocoles de la suite de protocoles TCP/IP :



# Modèle Client/Serveur

- Les serveurs sont des ordinateurs équipés de logiciels leur permettant de fournir des informations, comme des messages électroniques ou des pages web, à d'autres périphériques finaux sur le réseau. Chaque service nécessite un logiciel serveur distinct (exemple : Apache, Filezilla Server, ...).
- Les clients sont des ordinateurs équipés d'un logiciel qui leur permet de demander des informations auprès du serveur et de les traiter (exemples : Google Chrome, Mozilla Firefox, Filezilla client, ...).



# Modèle Peer To Peer

- 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.

- **Avantages :**

- Facile à configurer, moins de complexité, coût réduit, peut être utilisé pour des tâches simples telles que le transfert de fichiers et le partage des imprimantes...

- **Inconvénients :**

- Pas d'administration centralisée, peu sécurisé, non évolutif ...



# Bandé passante et débit

- **La bande passante**

La bande passante est la capacité d'un support à transporter des données. La bande passante numérique mesure la quantité d'informations pouvant circuler d'un emplacement à un autre pendant une période donnée. Elle est habituellement exprimée en kilobits par seconde (kbit/s), en mégabits par seconde (Mbit/s) ou en gigabits par seconde (Gbit/s).

- **Le débit**

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

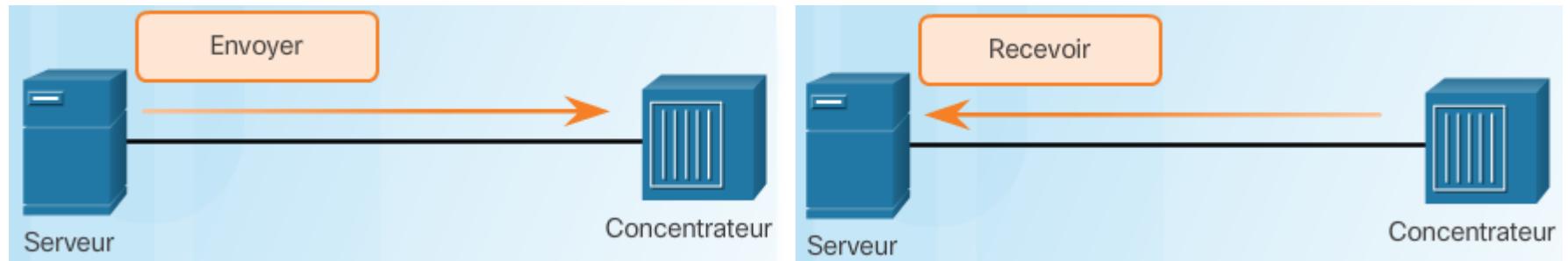
En raison d'un certain nombre de facteurs, le débit ne correspond généralement pas à la bande passante spécifiée dans les mises en œuvre de couche physique. De nombreux facteurs influencent le débit, notamment :

- La technologie utilisée pour l'accès au réseau
- L'instant où est effectué le transfert
- la latence créée par le nombre de périphériques réseau rencontrés entre la source et la destination.

# Les types de communications

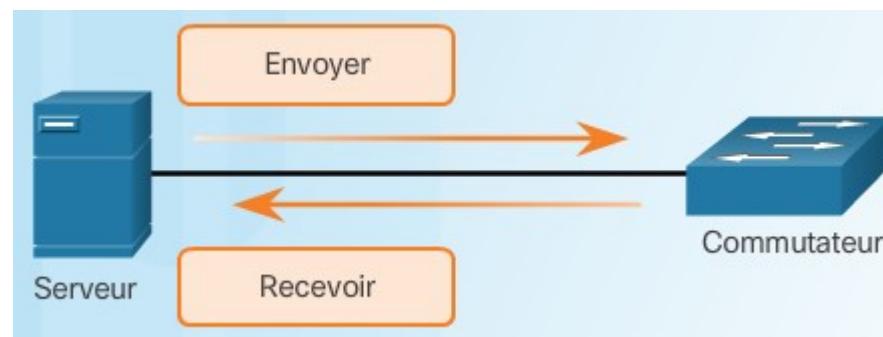
- **Communication Half duplex (semi duplex)**

les deux périphériques peuvent transmettre et recevoir des données sur les supports, mais pas de façon simultanée.



- **Communication Full duplex (duplex intégral)**

les deux périphériques peuvent simultanément transmettre et recevoir des données sur les supports.



# Les types de messages

- **Message de mono-diffusion (Unicast)**

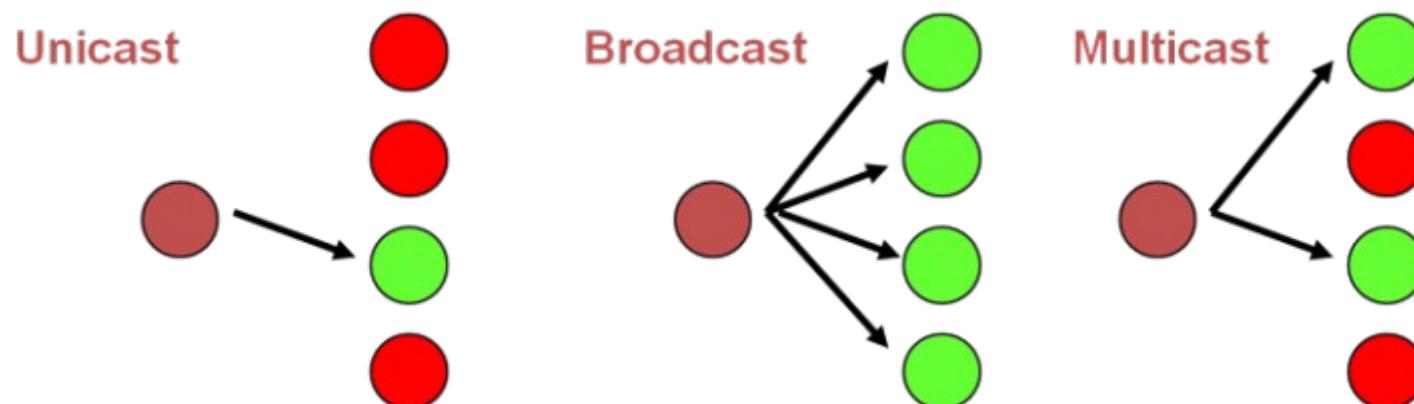
le message est envoyé d'un hôte à un seul hôte du réseau.

- **Message de diffusion (Broadcast)**

le message est envoyé d'un hôte à tous les hôtes du réseau.

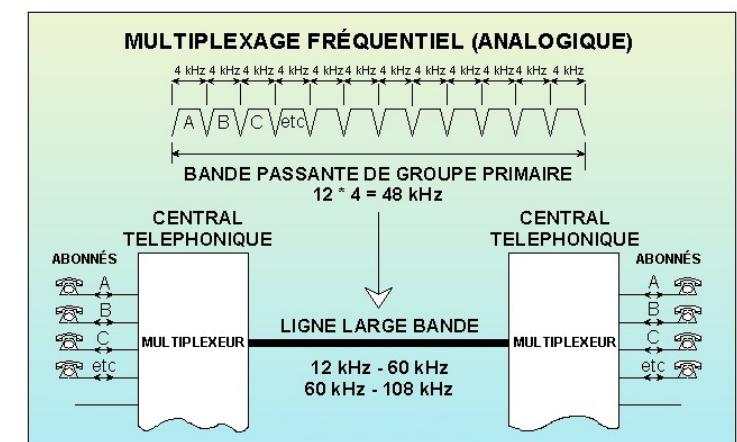
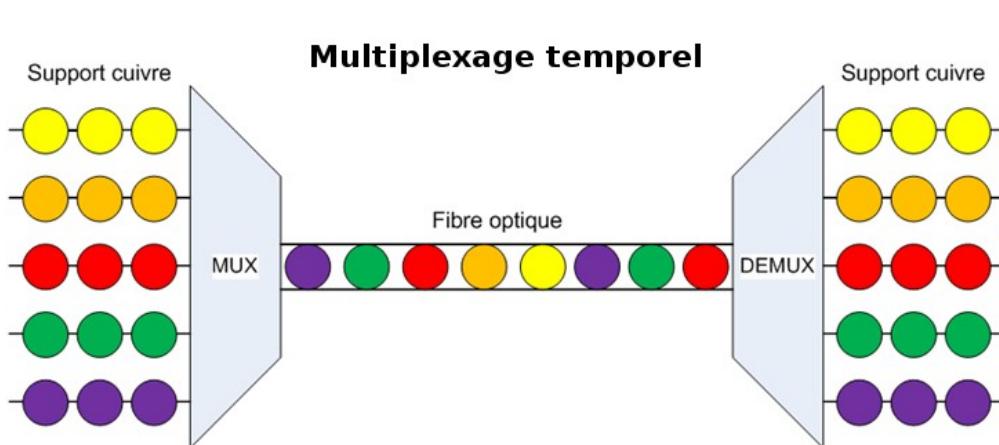
- **Message de multi-diffusion (Multicast)**

le message est envoyé d'un hôte à un groupe d'hôtes du réseau.



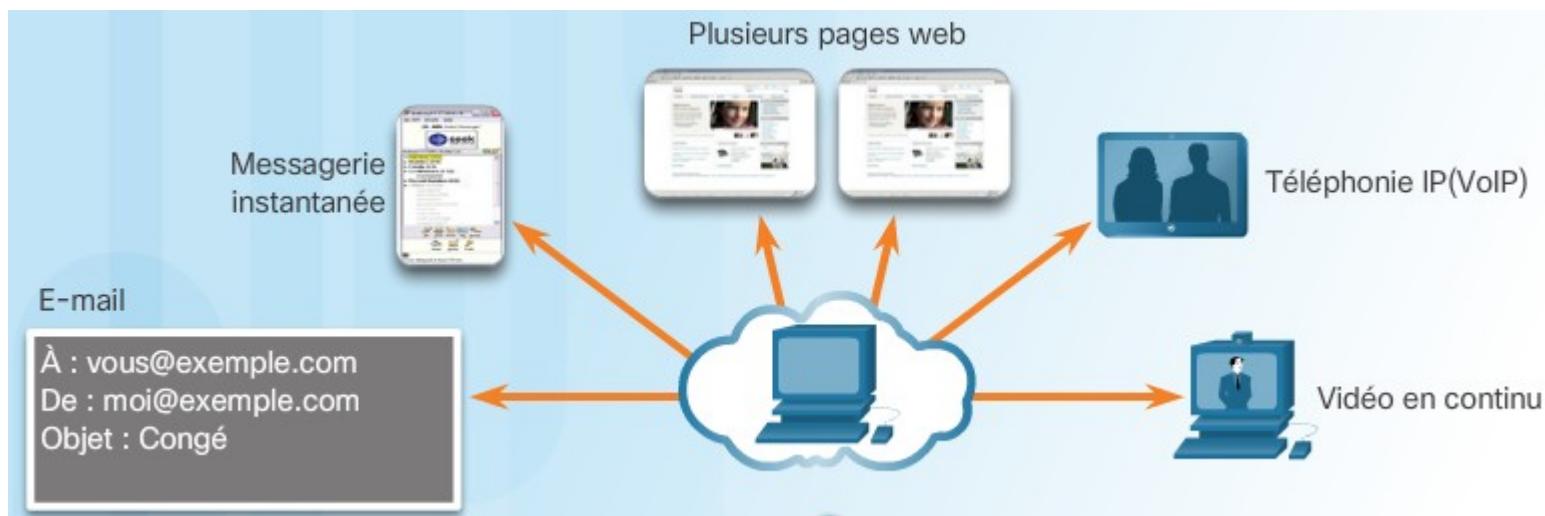
# Multiplexage

- Le multiplexage est une technique qui consiste à faire passer plusieurs informations à travers un seul support de transmission. Elle permet de partager une même ressource entre plusieurs utilisateurs. Quelques une des principales techniques de multiplexage :
  - Multiplexage Temporel** : Répartition du temps d'utilisation de la totalité de la bande passante entre les différentes communications.
  - Multiplexage Statistique** : Le multiplexage statistique est fondé sur le multiplexage temporel, on n'attribue la voie haute vitesse qu'aux voies basse vitesse qui ont effectivement quelque chose à transmettre.
  - Multiplexage Fréquentiel** : Cette technique alloue des fractions de la bande passante à chaque communication.



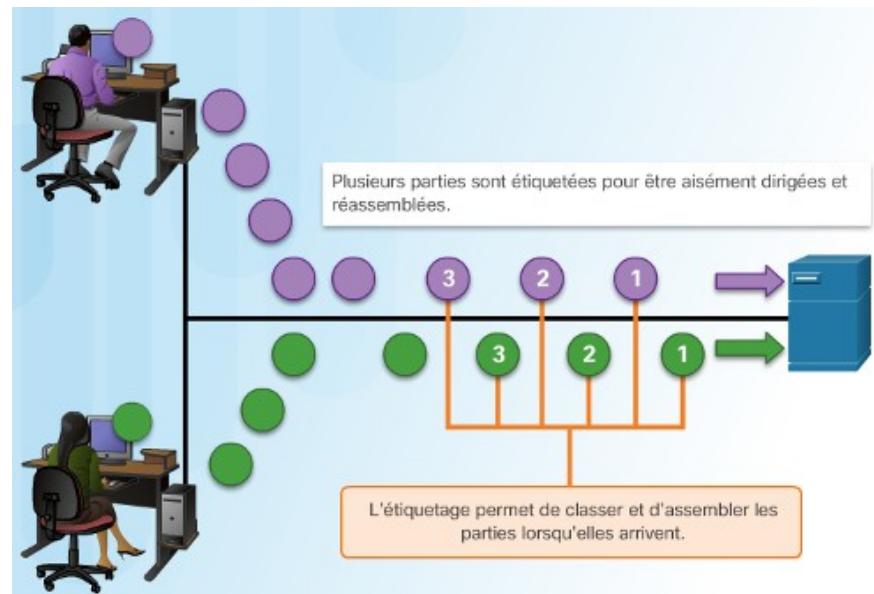
# Numéro de port

- Les numéros de port source et destination permettent d'identifier respectivement l'application source sur l'hôte local, et de destination sur l'hôte distant. Ces numéros permettent aux périphériques de gérer plusieurs communications simultanées impliquant plusieurs applications. On parle de multiplexage d'applications.
  - **Port source** : Pour le client, le numéro du port source est généré de manière dynamique par le système d'exploitation pour identifier l'application qui désire accéder à un service. Il peut ainsi envoyer simultanément plusieurs requêtes de service HTTP, par exemple, à un serveur web.
  - **Port de destination** : Le client indique un numéro de port de destination pour informer le serveur de destination du service demandé. Par exemple, lorsque le client spécifie le port 80 comme port de destination, le serveur qui reçoit le message sait que le service web est demandé. Un serveur peut offrir plusieurs services simultanés.



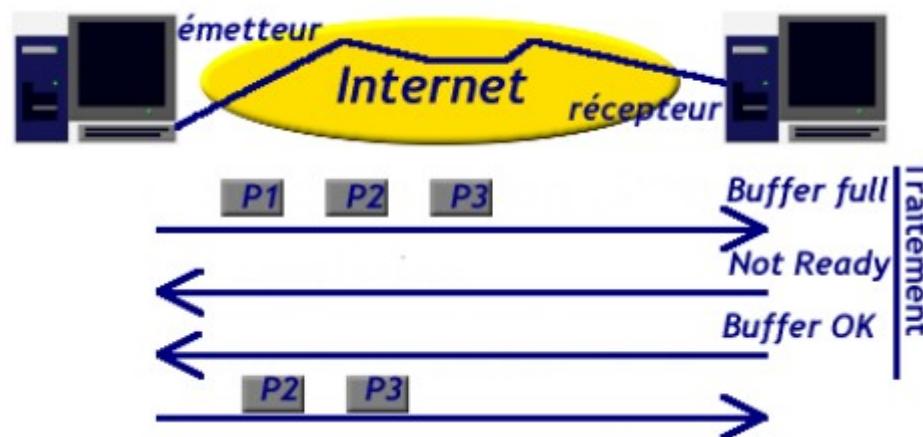
# Segmentation des messages

- La segmentation de données consiste à diviser les données en segments de taille moins importantes et plus facilement gérables avant de les envoyer sur le réseau. La segmentation des messages présente deux avantages majeurs :
  - Elle permet d'entremêler de nombreuses conversations différentes sur le même réseau (multiplexage) évitant ainsi qu'un seul périphérique n'occupe tout le canal de communication durant l'envoi d'un message volumineux.
  - Elle permet d'augmenter l'efficacité des communications réseau. Si une partie du message ne parvient pas à sa destination, en raison d'une panne réseau ou de l'encombrement du réseau, seules les parties manquantes doivent être retransmises.



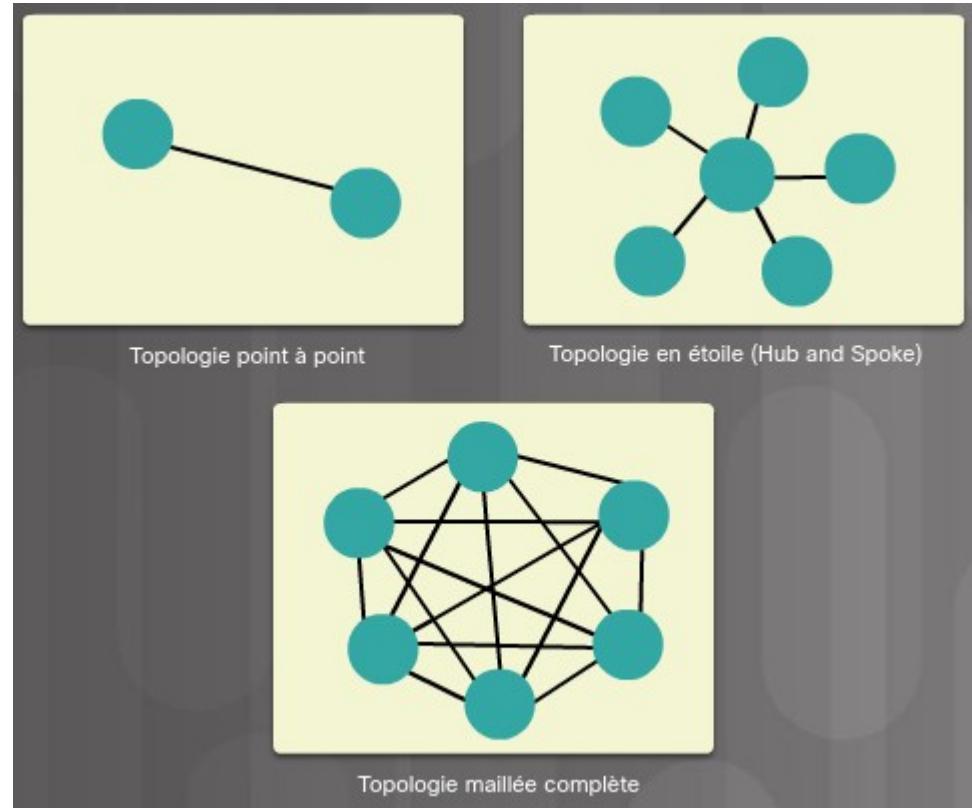
# Contrôle de flux

- Le contrôle de flux, dans un réseau informatique, représente un asservissement du débit binaire de l'émetteur vers le récepteur. Quand une machine qui a un débit montant supérieur au débit descendant de la destination, la source diminue son débit pour ne pas submerger le Buffer de réception du récepteur.



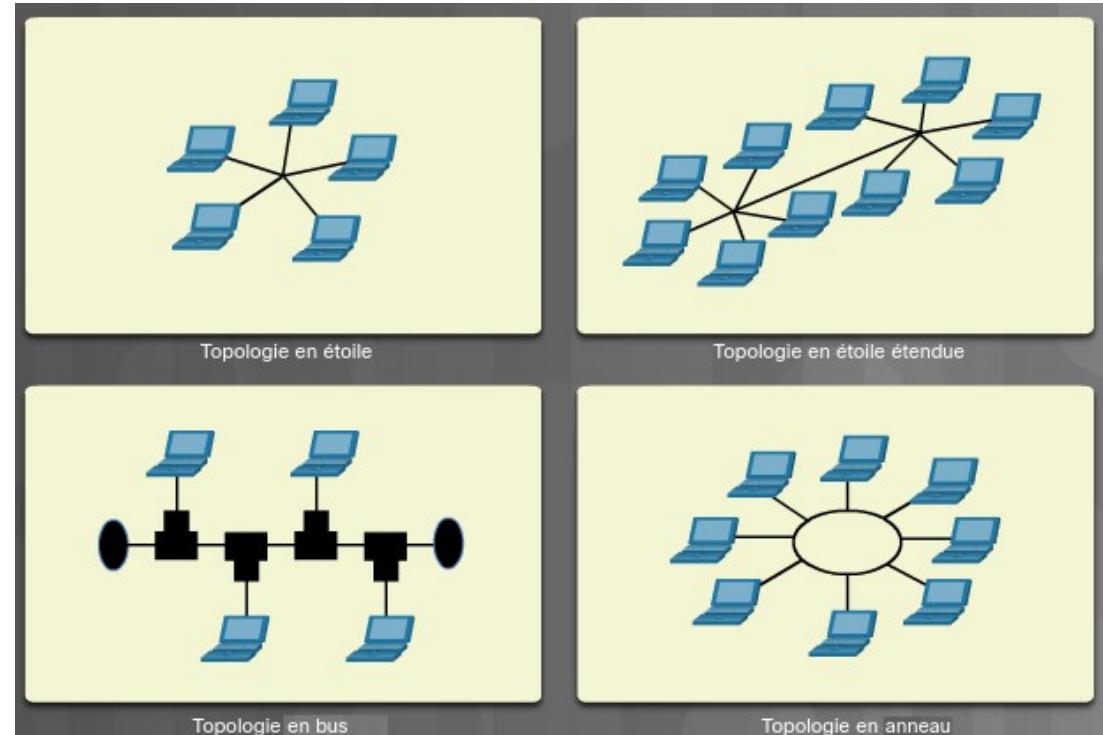
# Topologies physiques des réseaux étendus WAN

- Les réseaux étendus sont généralement interconnectés selon les topologies physiques suivantes :
  - **Point à point** : c'est la topologie la plus simple, composée d'une liaison permanente entre deux terminaux. Elle est donc très répandue.
  - **Hub and Spoke** : version WAN de la topologie en étoile, dans laquelle un site central connecte entre eux les sites des filiales à l'aide de liaisons point à point.
  - **Maillée** : cette topologie offre une haute disponibilité, mais nécessite que tous les systèmes finaux soient connectés entre eux. Les coûts, tant administratifs que physiques, peuvent donc être élevés. Chaque liaison est simplement une liaison point à point avec l'autre nœud.



# Topologies physiques des réseaux LAN

- La topologie physique définit la façon dont les systèmes finaux sont physiquement interconnectés. Sur les réseaux locaux à supports partagés, les périphériques finaux peuvent être interconnectés selon les topologies physiques suivantes :
  - Topologie en étoile
  - Topologie en étoile étendue
  - Topologie en bus
  - Topologie en anneau
- Dans certains réseaux locaux, les topologies maillées peuvent être utilisées.



# Topologies physiques des réseaux LAN

- **Topologie en étoile** : les périphériques finaux sont connectés à un périphérique intermédiaire central. Dans les premières topologies en étoile, les périphériques finaux étaient interconnectés à l'aide de concentrateurs Ethernet. De nos jours, des commutateurs Ethernet sont utilisés. La topologie en étoile est simple à installer, très évolutive (il est facile d'ajouter et de retirer des périphériques finaux) et facile à dépanner.
- **Topologie en étoile étendue** : dans une topologie en étoile étendue, les périphériques Ethernet supplémentaires sont interconnectés avec d'autres topologies en étoile. Une topologie en étoile étendue est un exemple de topologie hybride.
- **Topologie en bus** : tous les systèmes finaux sont reliés entre eux en formant une chaîne et le réseau est terminé à chaque extrémité par un bouchon de terminaison. Les périphériques d'infrastructure tels que les commutateurs ne sont pas nécessaires pour interconnecter les périphériques finaux. Les topologies en bus sur câbles coaxiaux étaient utilisées dans les anciens réseaux Ethernet en raison de leur faible coût et de leur simplicité d'installation.
- **Topologie en anneau** : les systèmes finaux sont connectés à leur voisin respectif et forment ainsi un anneau. Contrairement à la topologie en bus, l'anneau n'a pas besoin d'être terminé. Les topologies en anneau étaient utilisées dans les réseaux FDDI (Fiber Distributed Data Interface) et Token Ring.

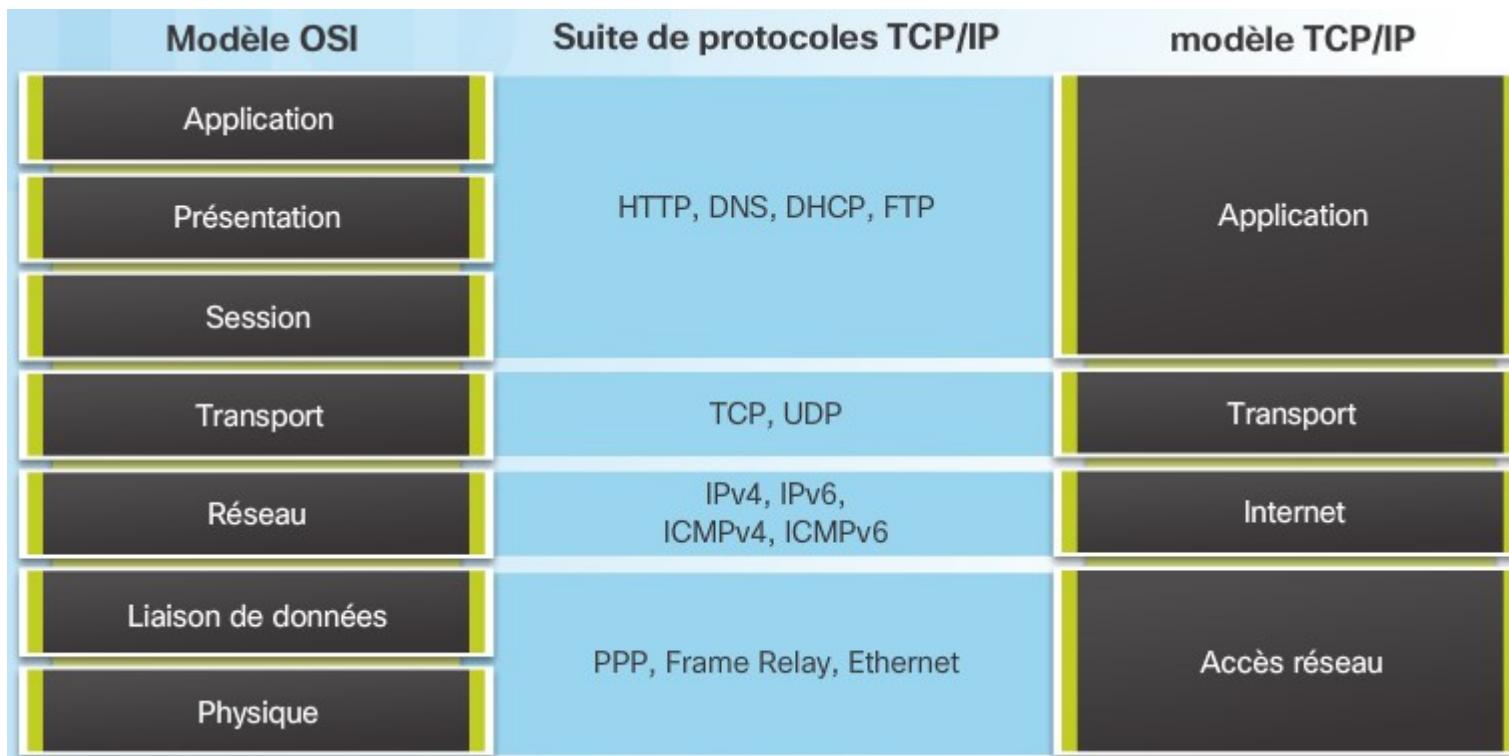
# Modèles en couches

# Avantage des modèles en couches

- L'utilisation d'un modèle en couches pour décrire des protocoles et des opérations sur un réseau présente plusieurs avantages dont on peut citer :
  - Encourager la concurrence et l'interopérabilité, afin de permettre à des produits de différents fournisseurs de fonctionner ensemble.
  - Permet d'éviter que des changements technologiques ou fonctionnels dans une couche ne se répercutent sur d'autres couches, supérieures et inférieures.
  - Les modifications apportées à une couche n'affectent pas les autres couches.
  - Il facilite l'évolutivité des réseaux en intervenant uniquement dans les couches nécessitant des changements.
  - Il divise les communications sur le réseau en éléments plus petits, ce qui permet de les comprendre plus facilement.
  - Fournit un langage commun pour décrire des fonctions et des fonctionnalités réseau.

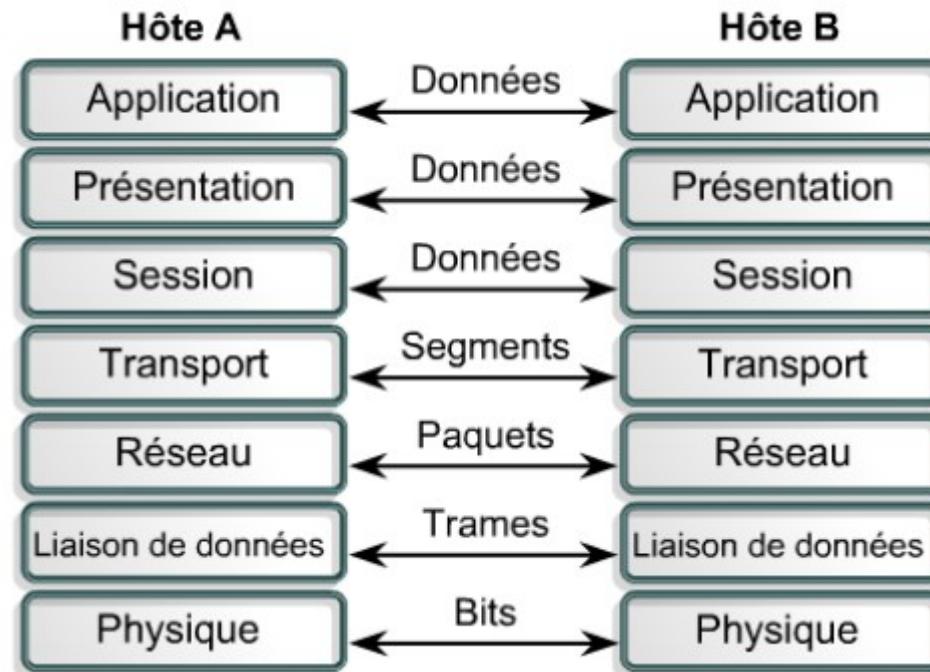
# Modèles OSI et TCP/IP

- Le modèle OSI (Open Systems Interconnection) et le modèle TCP/IP sont les principaux modèles utilisés en matière de fonctionnalités réseau. La figure ci-dessous montre l'équivalence des couches entre ces deux modèles et des exemples de protocoles correspondants à chaque couches.



# Unités de données de protocole

- La forme qu'emprunte une donnée sur n'importe quelle couche est appelée **unité de données de protocole (PDU ou « Protocole Data Unit » en anglais)**.
- Au cours de l'encapsulation, chaque couche, encapsule l'unité de données de protocole qu'elle reçoit de la couche supérieure en respectant le protocole en cours d'utilisation. À chaque étape du processus, une unité de données de protocole possède un nom différent qui reflète ses nouvelles fonctions. La figure ci-dessous montre les noms des PDU de chaque couche OSI.



# Rôles des couches OSI

- **Couche 1 - Physique**

Les protocoles de la couche physique décrivent les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.

- **Couche 2 - Liaison de données**

Les protocoles de couche liaison de données décrivent des méthodes d'échange de trames de données sans erreurs entre des périphériques sur un même segment réseau.

- **Couche 3 - Réseau**

La couche réseau fournit des services pour échanger des données sur le réseau entre des périphériques finaux n'appartenant pas forcément au même segment réseau.

- **Couche 4 - Transport**

La couche transport définit des services pour segmenter, transférer et réassembler les données de communications individuelles entre les périphériques finaux. Elle permet également de gérer le type de transfert (fiable ou non fiable), le contrôle de flux, et le multiplexage d'applications.

# Rôles des couches OSI

- **Couche 5 - Session**

La couche session fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.

- **Couche 6 - Présentation**

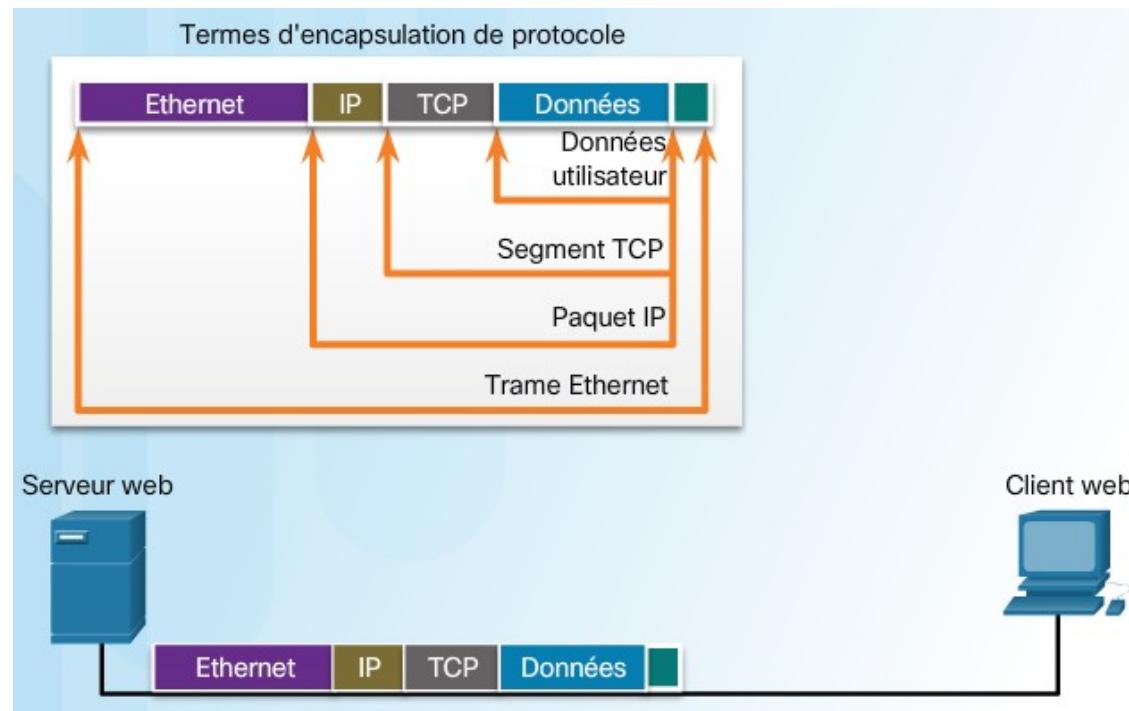
La couche présentation fournit une représentation commune des données transférées entre des services de couche application (cryptage, compression, codage de données).

- **Couche 7 - Application**

La couche application contient des protocoles utilisés pour les communications de processus à processus. C'est la couche la plus proche de l'utilisateur.

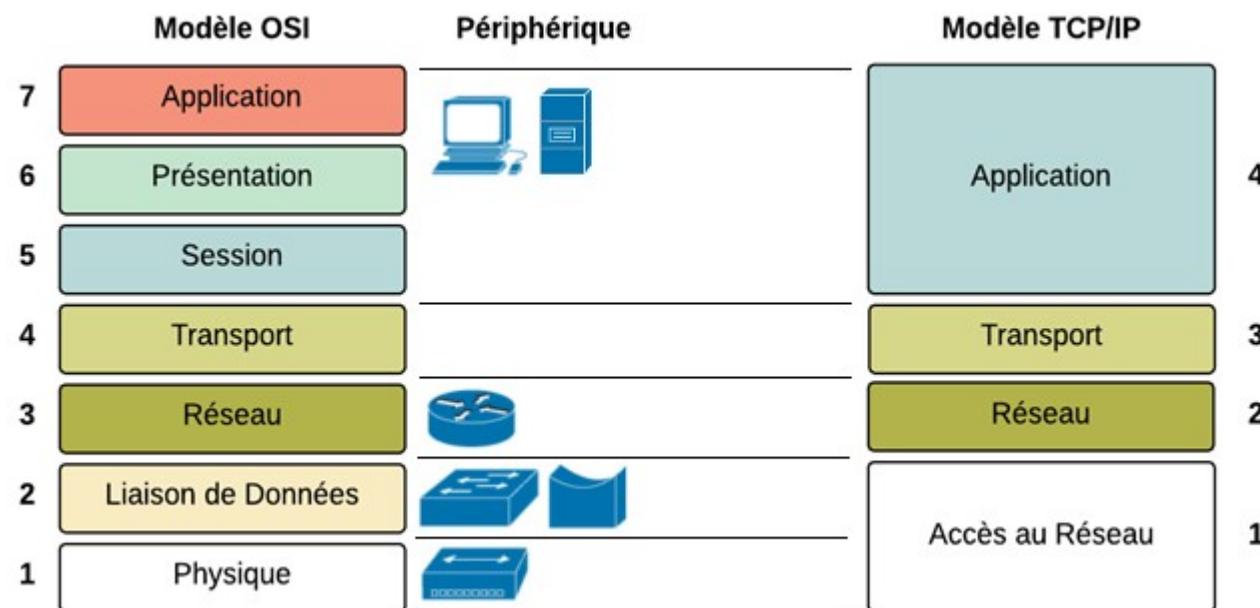
# Encapsulation / Dés-encapsulation

- L'encapsulation, en réseaux informatiques, est un procédé consistant à inclure les données d'un protocole dans un autre protocole. Le processus d'encapsulation conditionne les données en leur ajoutant des informations relatives au protocole avant de les transmettre sur le réseau. Ainsi, en descendant dans les couches du modèle OSI, les données reçoivent des en-têtes et des en-queues. Lors de la réception des données, l'opération inverse est effectuée. On peut parler de dés-encapsulation des données.



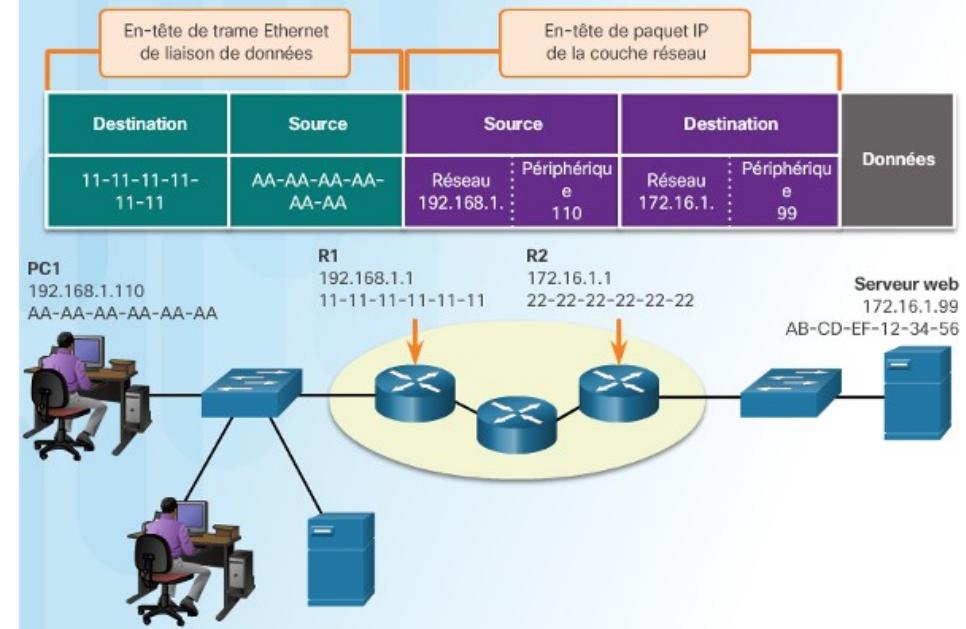
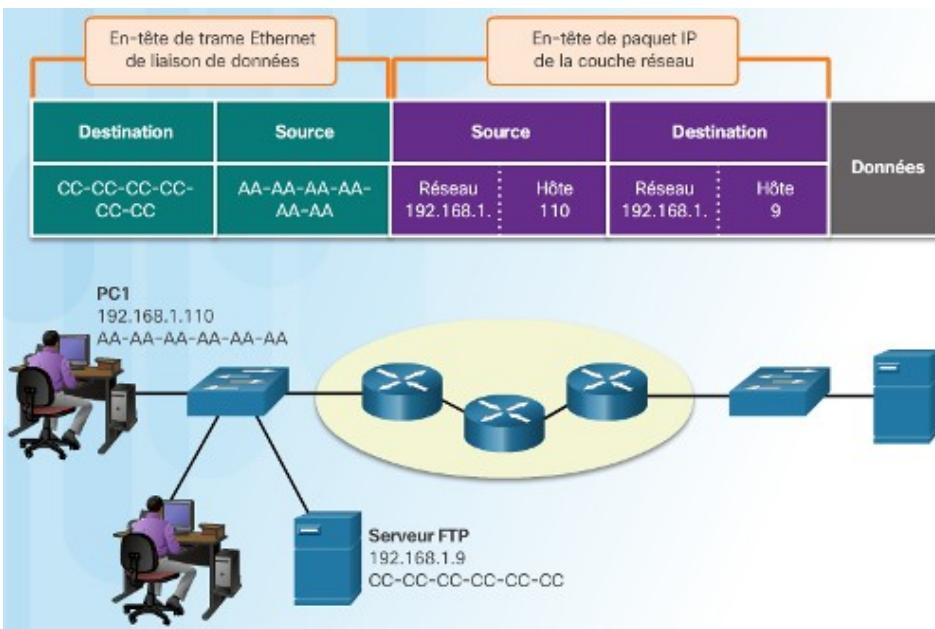
# Exemples d'équipements réseau

- Ci-dessous quelques exemples d'équipements réseaux situés selon les couches où ils opèrent :
  - **Couche 1 OSI** : Concentrateur (Hub), Répéteur, Modem, Antenne Wifi, Médias
  - **Couche 2 OSI** : Commutateur (Switch), Pont (Bridge), Point d'accès sans fil, Carte réseau
  - **Couche 3 OSI** : Routeur
  - **Couche 7 OSI** : Ordinateur, Serveur, IP Phone, Smartphone



# Adresses physique et logique

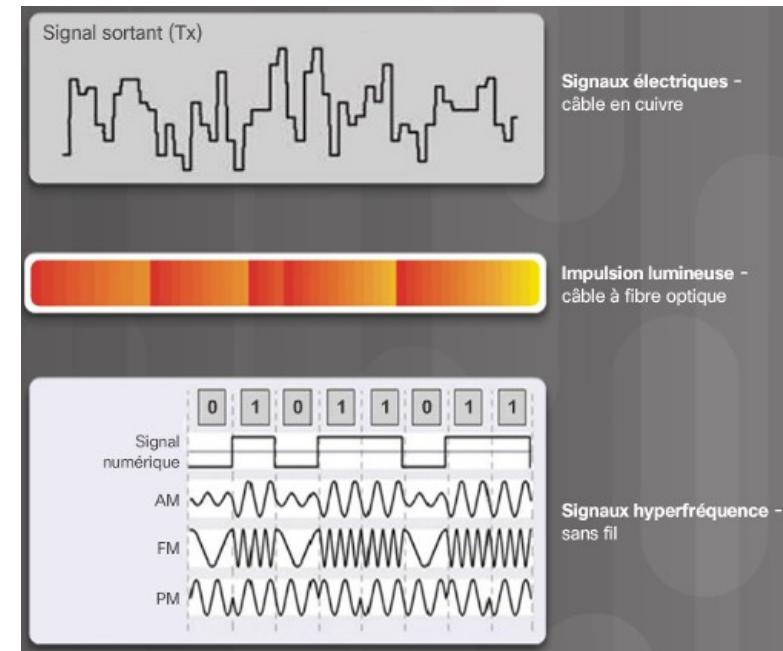
- Les couches réseau et liaison de données sont chargées de transmettre les données du périphérique source au périphérique de destination. Les protocoles de ces deux couches contiennent les adresses source et destination, mais ils ne les utilisent pas aux mêmes fins.
  - Les **adresses de couche réseau** source et destination (adresses logiques) remettent le paquet IP de l'hôte source à la destination finale, sur le même réseau ou sur un réseau distant.
  - Les **adresses de couche liaison de données** source et destination (adresses physiques) transmettent la trame liaison de données d'une carte réseau à une autre, sur un même réseau.



# Couche physique

# Les types de supports réseau

- Il existe trois formes élémentaires de support réseau. La couche physique produit la représentation et les groupements de bits pour chaque type de support comme suit :
  - Câble en cuivre** : les signaux sont des variations d'impulsions électriques.
  - Câble à fibre optique** : les signaux sont des variations lumineuses.
  - Sans fil** : les signaux sont des variations de transmission d'hyperfréquences.
- Pour permettre l'interopérabilité sur la couche physique, tous les aspects de ces fonctions sont régis par les organismes de normalisation.



# Normes de couche physique

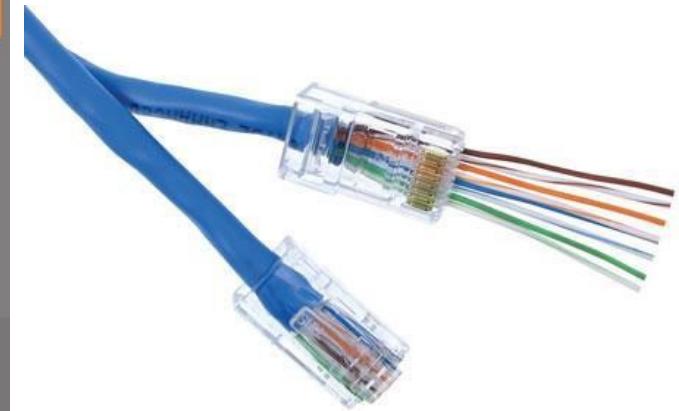
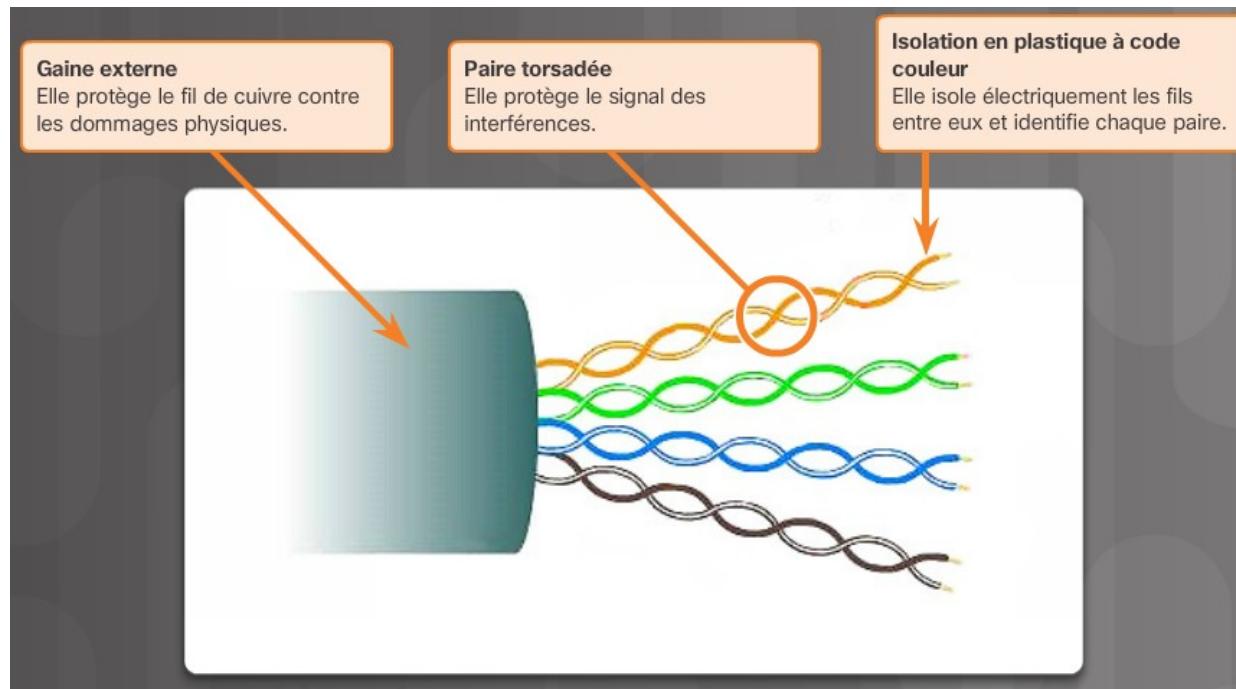
- La couche physique est constituée de circuits électroniques, de supports et de connecteurs. Il est par conséquent approprié que les normes régissant ces matériels soient définies par les organisations d'ingénierie électrique et de communications correspondantes.
- Les normes relatives au matériel, aux supports, au codage et à la signalisation de la couche physique sont définies et régies par les organismes suivants :
  - ISO (International Standards Organization)
  - TIA/EIA (Telecommunications Industry Association/Electronic Industries Association)
  - UIT (Union Internationale des Télécommunications)
  - ANSI (American National Standards Institute)
  - IEEE (Institute of Electrical and Electronics Engineers - Institut des ingénieurs en équipements électriques et électroniques)
  - ...

# Supports en cuivre

- Trois principaux types de supports en cuivre sont utilisés dans les réseaux :
  - **Paires torsadées non blindées (UTP)**
  - **Paires torsadées blindées (STP)**
  - **Coaxial**
- Ces câbles sont utilisés pour interconnecter les nœuds d'un réseau local et des périphériques d'infrastructure tels que des commutateurs, des routeurs et des points d'accès sans fil.
- Diverses normes de couche physique spécifient l'utilisation de différents connecteurs. Ces normes définissent les dimensions mécaniques des connecteurs et les propriétés électriques acceptables pour chaque type. Les supports réseau utilisent des connecteurs et des fiches modulaires qui facilitent la connexion et la déconnexion. De plus, un même type de connecteur physique peut servir à plusieurs types de connexions. Par exemple, le connecteur RJ-45 est largement employé dans les réseaux locaux avec un type de support et dans certains réseaux étendus avec un autre type de support.
- Ces types de supports peuvent être sujet à des problèmes de :
  - Diaphonie
  - Interférences électromagnétiques ou radioélectriques

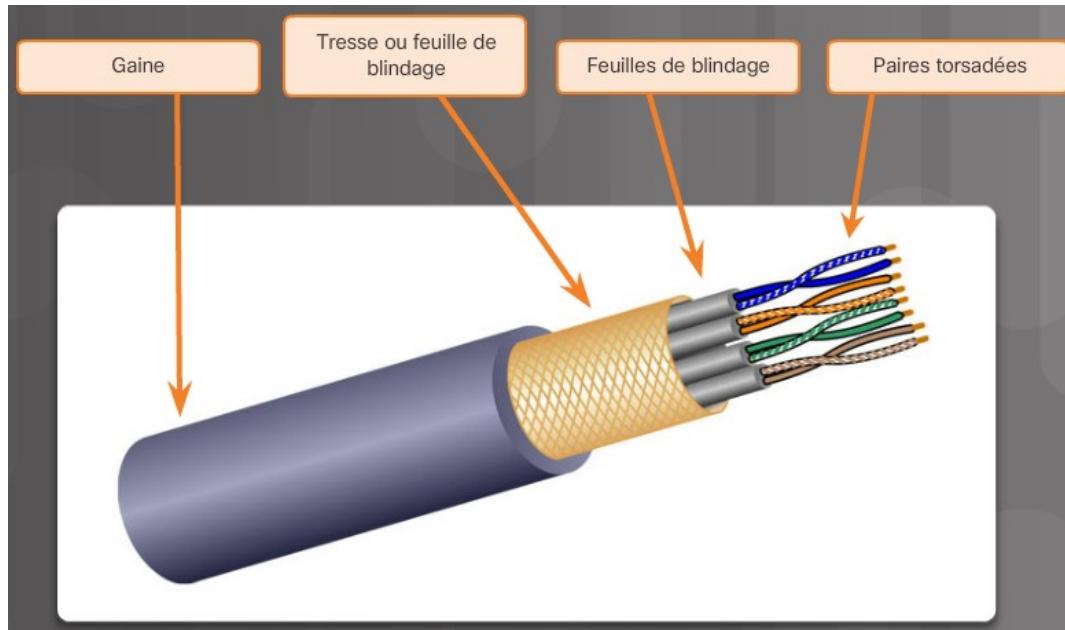
# Câble à paires torsadées non blindé

- Le câblage à paires torsadées non blindées (UTP ou Unshielded Twisted Pair) est le support réseau le plus répandu. Ces câbles terminés par des connecteurs RJ-45 sont utilisés pour relier des hôtes réseau à des périphériques réseau intermédiaires, tels que des commutateurs et des routeurs.
- Dans les réseaux locaux, chaque câble UTP se compose de quatre paires de fils à code couleur qui ont été torsadés, puis placés dans une gaine en plastique souple qui les protège des dégâts matériels mineurs. Le fait de torsader les fils permet de limiter les interférences causées par les signaux d'autres fils et réduire l'effet de diaphonie.



# Câble à paires torsadées blindé

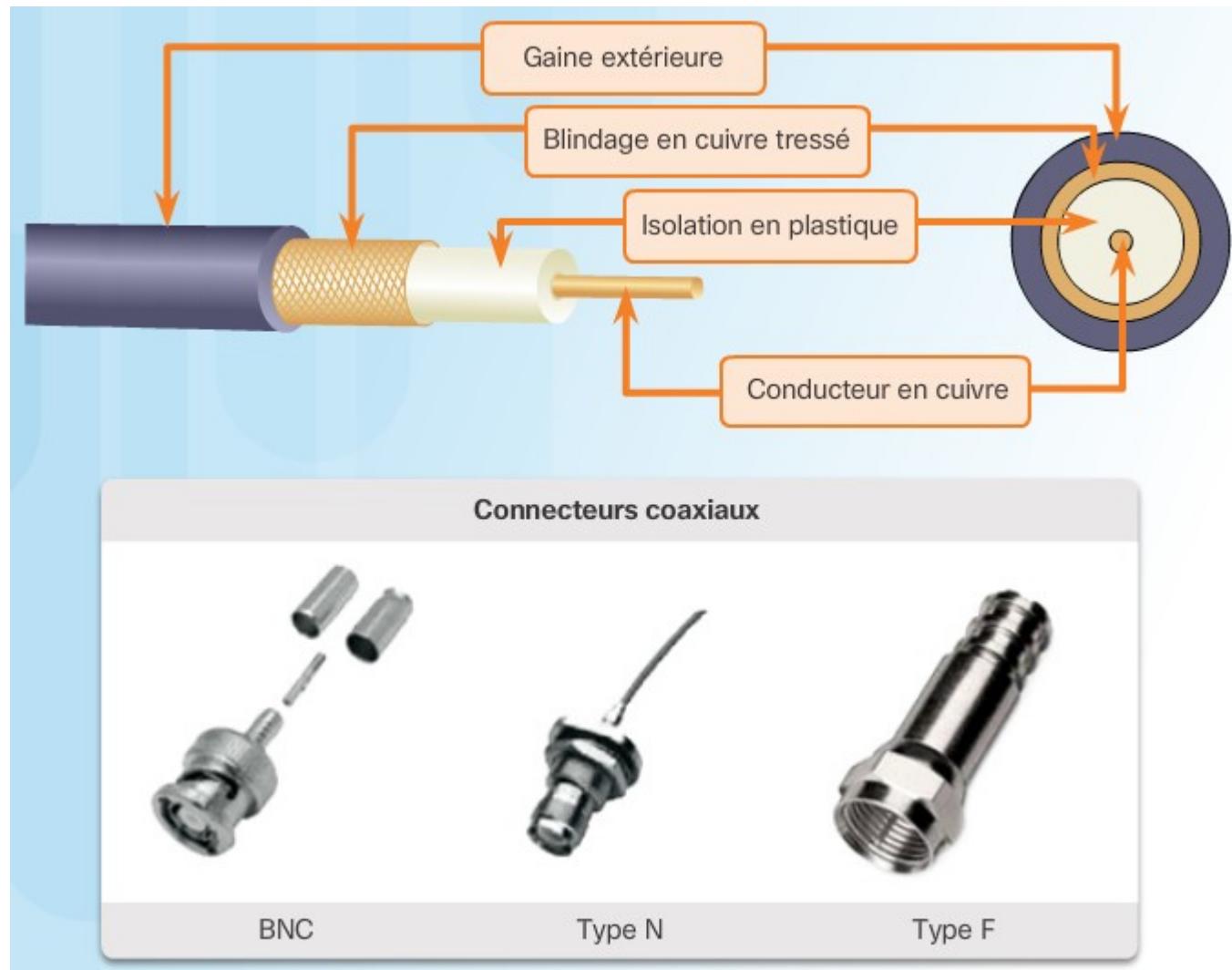
- Les câbles à paires torsadées blindées (STP - Shielded Twisted Pair) offrent une meilleure protection contre les parasites que le câblage UTP. Ils sont toutefois bien plus onéreux et plus difficiles à installer que les câbles UTP. Comme les câbles UTP, les câbles STP utilisent un connecteur RJ-45.
- Les câbles à paires torsadées blindées allient les techniques de blindage pour contrer les interférences électromagnétiques et radioélectriques, et les torsades pour éviter la diaphonie. Pour tirer entièrement parti des avantages du blindage, les câbles STP sont terminés par des connecteurs RJ45 blindés. Si le câble n'est pas correctement mis à la terre, le blindage peut agir comme une antenne et capter des signaux parasites.



# Câble coaxial

- Le câble coaxial tire son nom du fait qu'il contient deux conducteurs qui partagent le même axe. Le câble coaxial est composé des éléments suivants :
  - Un conducteur en cuivre utilisé pour transmettre les signaux électroniques.
  - Un conducteur en cuivre entouré d'une couche de matériau isolant flexible en plastique.
  - Sur ce matériau isolant, une torsade de cuivre ou une feuille métallique constitue le second fil du circuit et fait office de protection pour le conducteur intérieur. Cette seconde couche, ou blindage, réduit également les interférences électromagnétiques externes.
  - Le câble dans son entier est ensuite entouré d'une gaine afin d'empêcher tout dégât matériel mineur.
- Bien que les câbles UTP aient pratiquement remplacé les câbles coaxiaux dans les installations Ethernet modernes, la conception du câble coaxial est utilisée aux fins suivantes :
  - **Installations sans fil** : les câbles coaxiaux relient les antennes aux périphériques sans fil.
  - **Installations de câbles Internet** : les fournisseurs d'accès par câble offrent une connexion Internet à leurs clients en remplaçant des sections du câble coaxial et les composants d'amplification connexes par un câble en fibre optique. Toutefois, le câblage à l'intérieur des locaux des clients reste coaxial.

# Câble coaxial

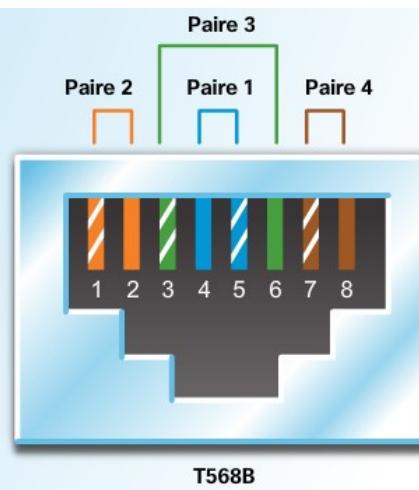
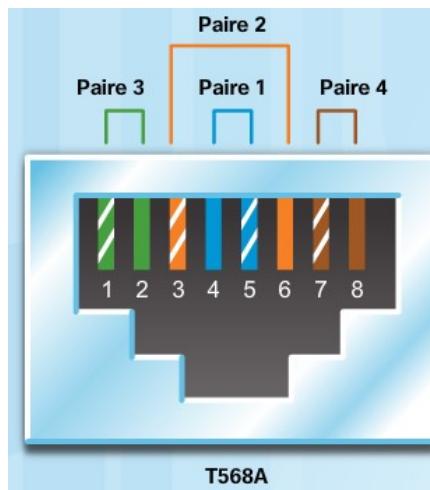


# Catégories de câbles UTP

- Les caractéristiques électriques du câblage en cuivre sont définies par l'IEEE (Institute of Electrical and Electronics Engineers). L'IEEE classe le câblage UTP suivant ses performances dans des catégories en fonction de leur capacité à prendre en charge des débits supérieurs de bande passante. Par exemple, un câble de catégorie 5e (Cat5e) est généralement utilisé dans les installations Fast Ethernet (100BASE-TX). Il constitue désormais le type de câble minimum acceptable dans un réseau local. Les câbles de catégorie 6 (Cat6) sont recommandés pour les installations de nouveaux bâtiments.
- Les principales catégories de câbles utilisées actuellement dans les réseaux LAN sont les suivantes :
  - **Catégorie 3** : Utilisée pour les communications vocales le plus souvent pour les lignes téléphoniques.
  - **Catégorie 5e** : Utilisée pour la transmission de données. Les supports de catégorie 5e sont utilisés pour des débits de 100 Mbit/s (100BASE-TX) mais peuvent prendre en charge le 1000 Mbit/s (1000BASE-T). La longueur maximale de ces câbles est de 100m.
  - **Catégorie 6** : Utilisée pour la transmission de données. Les supports de catégorie 6 sont recommandés pour des débits de 1000 Mbit/s (1000BASE-T). La longueur maximale de ces câbles est de 100m.
  - **Catégorie 6a** : Utilisée pour la transmission de données. Les supports de catégorie 6a sont recommandés pour des débits de 10 Gbit/s (10GBASE-T). La longueur maximale de ces câbles est de 100m.

# Normes de câblage TIA-568 A et B

- Les principaux types de câbles qu'on rencontre dans un réseau local sont les suivants :
  - **Câble Ethernet droit** : type de câble réseau le plus courant. Il permet de relier des périphériques de types différents. Par exemple, pour connecter un hôte à un commutateur ou un commutateur à un routeur. Il peut utiliser l'une ou l'autre des deux normes de câblage à condition qu'elle soit utilisée des deux cotés du câble.
  - **Câble Ethernet croisé** : câble peu utilisé. Il permet de relier des périphériques similaires. Par exemple, pour connecter un commutateur à un commutateur, un hôte à un autre hôte ou un routeur à un routeur. Il doit utiliser les deux normes de câblage chacune de chaque cotés du câble.
  - **Câble inversé** : câble propriétaire Cisco permettant l'accès à la ligne de commande en reliant le port console d'un routeur ou d'un commutateur au port série RS232 d'un PC.



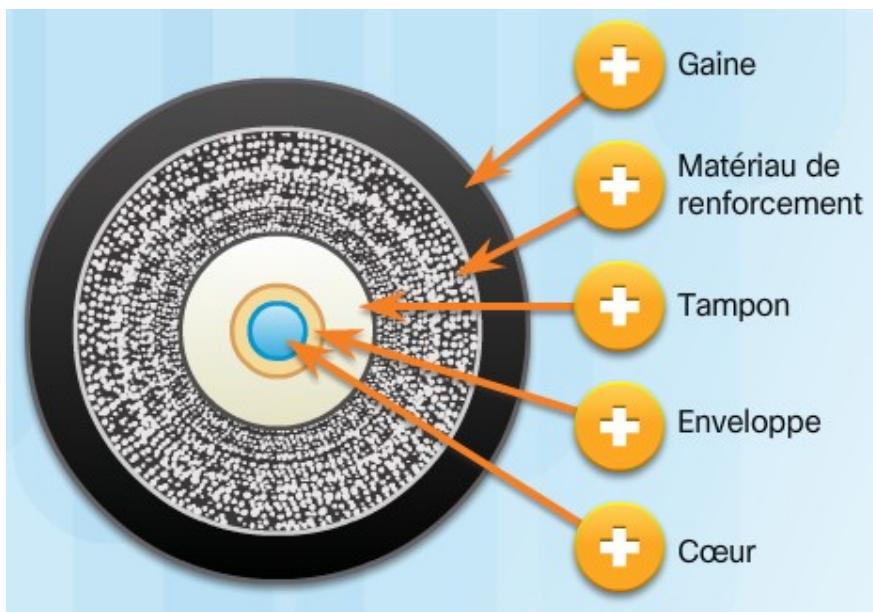
Câble inversé ou câble console

# Fibres optiques

- Les câbles à fibre optique transmettent les données sur de plus longues distances et avec une bande passante plus large que n'importe quel autre support réseau. Contrairement aux fils de cuivre, les câbles à fibre optique peuvent transmettre des signaux avec moins d'atténuation et sont entièrement protégés des perturbations électromagnétiques et radioélectriques.
- Actuellement, les câbles à fibre optique sont utilisés dans quatre domaines d'application :
  - **Les réseaux d'entreprise.** La fibre est utilisée pour les applications de câblage du réseau fédérateur et pour relier les périphériques d'infrastructure.
  - **La technologie FTTH** (fiber to the home ou fibre optique jusqu'au domicile). Cette technologie est utilisée pour fournir des services haut débit disponibles en permanence aux particuliers et aux petites entreprises.
  - **Les réseaux longue distance.** Les câbles à fibre optique sont utilisés par les prestataires de services pour relier les pays et les villes.
  - **Les réseaux sous-marins.** Des câbles spéciaux sont utilisés pour fournir des solutions haut débit et haute capacité fiables, à l'épreuve des environnements sous-marins et sur des distances à l'échelle d'un océan. Le lien suivant renvoi vers une carte indiquant l'emplacement des câbles sous-marins : <http://www.submarinecablemap.com/>

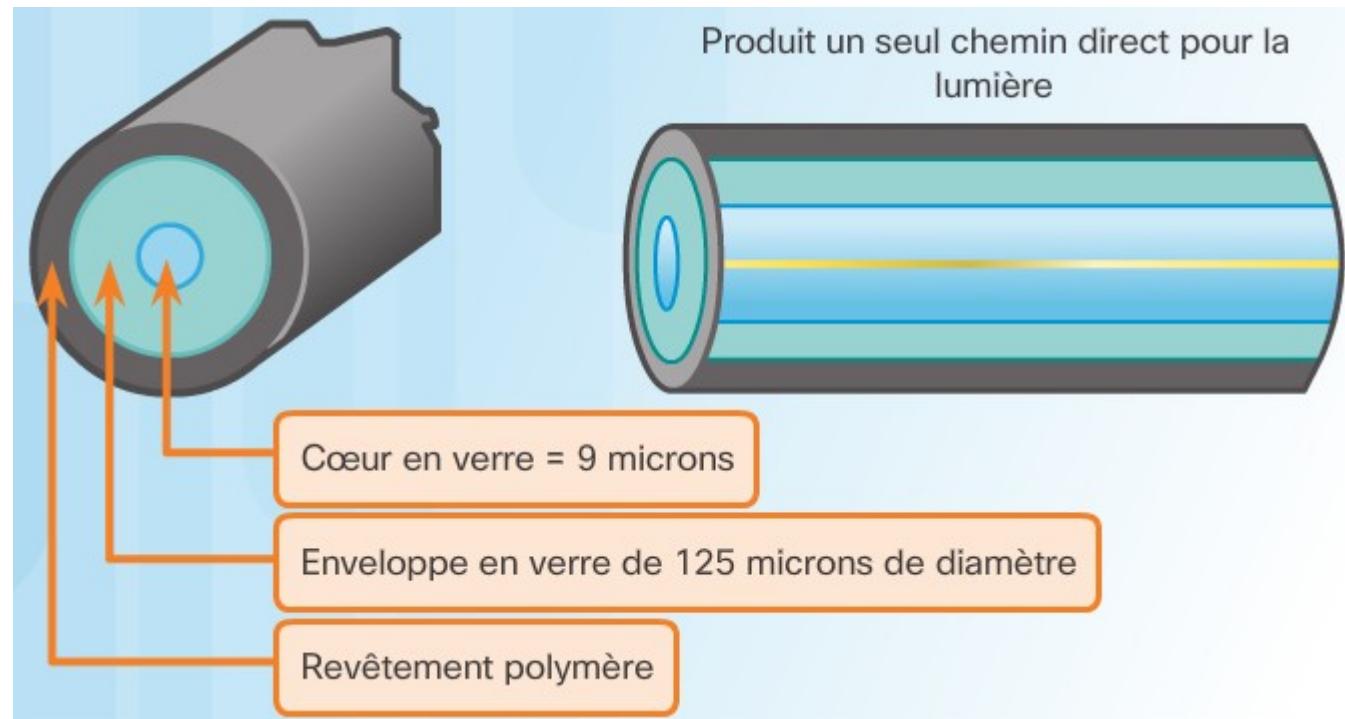
# Fibres optiques - Constitution

- **Cœur** : Le cœur est l'élément qui transmet la lumière au centre de la fibre optique. Il est généralement en silice ou en verre. Les impulsions lumineuses circulent dans le cœur de la fibre.
- **Enveloppe** : Elle agit comme un miroir en reflétant la lumière dans le cœur de la fibre.
- **Tampon** : Sert à protéger le cœur et l'enveloppe.
- **Matériau de renforcement** : Empêche le câble à fibre optique de s'étirer lorsqu'on tire dessus. Il s'agit souvent du même matériau que celui utilisé dans les gilets pare-balles.
- **Gaine** : Elle protège la fibre de l'usure, de l'humidité et d'autres contaminants.



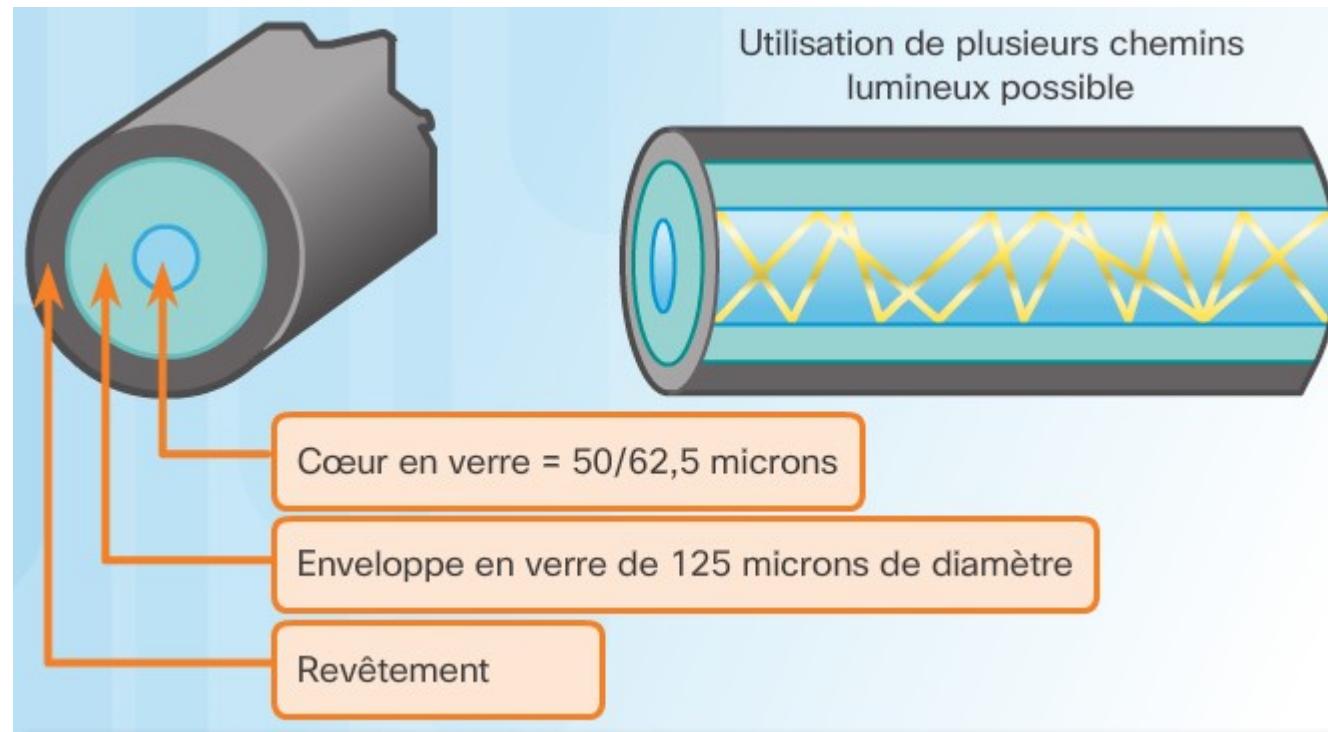
# Fibre optique Monomode (SMF)

- Son cœur présente un **très faible diamètre** (de l'ordre de 10um) et elle fait appel à la technologie coûteuse qu'est le **laser** pour envoyer un faisceau lumineux très directif. Elle est répandue dans les réseaux longue distance (plusieurs centaines de kilomètres), tels que ceux nécessaires pour les applications de téléphonie, de télévision par câble longue distance, ou les liaisons WAN.
- **Exemple :** Une fibre optique de désignation 10/125 est une fibre monomode dont le diamètre du cœur est de 10um, et celui de l'enveloppe de 125um.



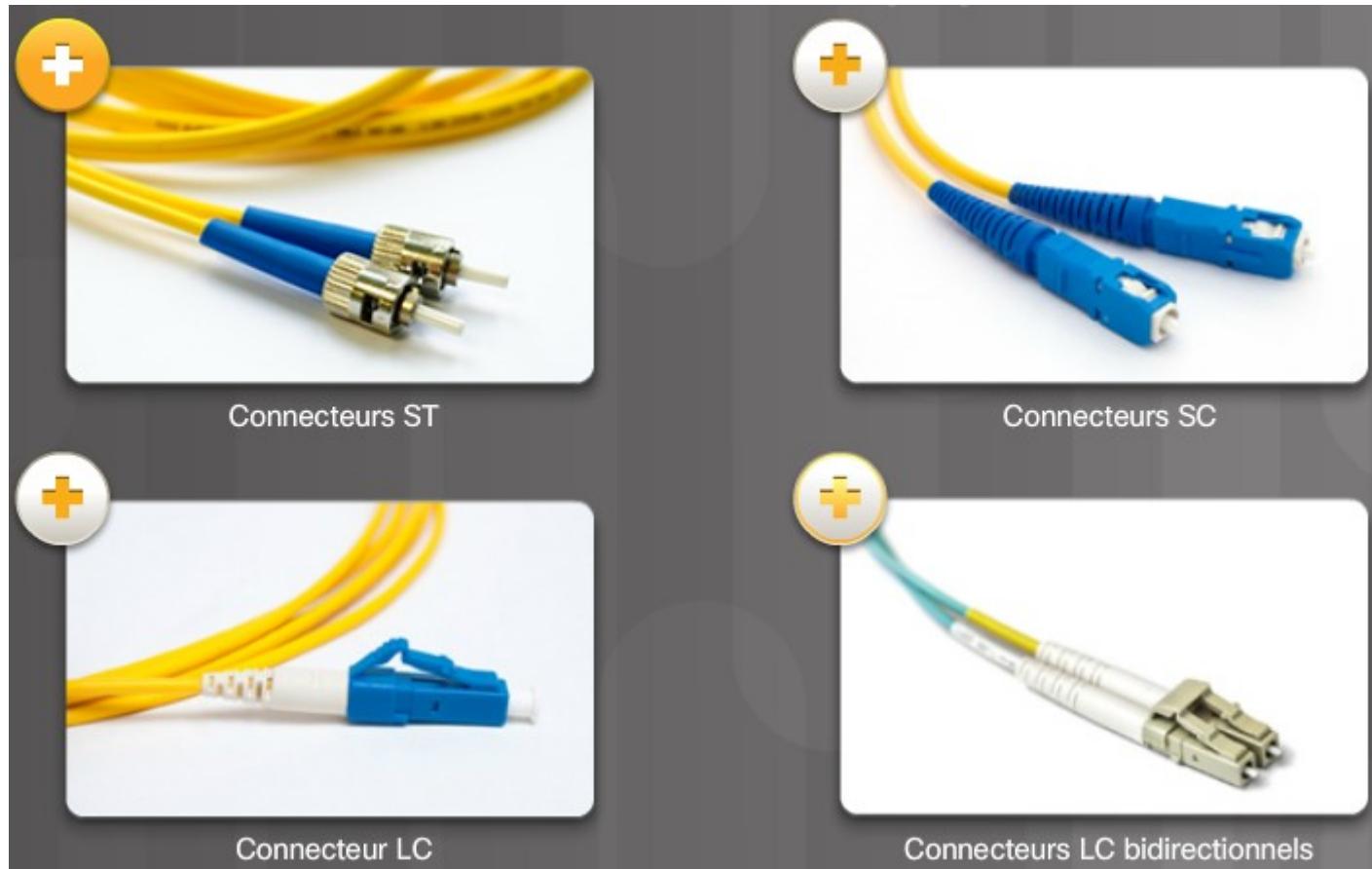
# Fibres optiques Multimodes (MMF)

- La taille de son **cœur** est supérieur à 50um et elle utilise des émetteurs **infrarouge** pour envoyer des impulsions lumineuses. La lumière entre dans la fibre multimode sous différents angles, et subit plusieurs réflexions à l'intérieur du cœur. Elle est généralement utilisée dans les réseaux locaux, car grâce à son faible coût Elle fournit une bande passante allant jusqu'à 10 Gbit/s sur des liaisons pouvant atteindre plusieurs centaines de mètres de long.
- **Exemple :** Une fibre optique de désignation 50/125 est une fibre multimode dont le diamètre du cœur est de 50um, et celui de l'enveloppe de 125um.



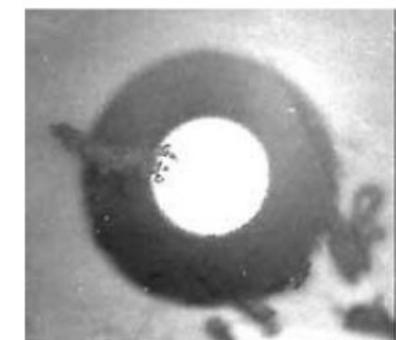
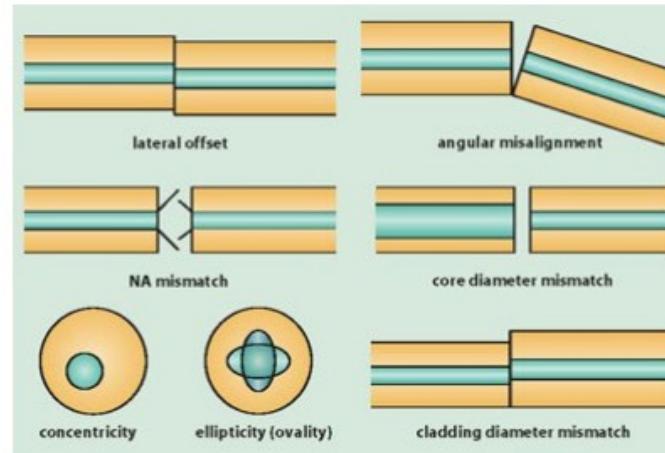
# Connecteurs fibres optiques

- Un connecteur à fibre optique termine l'extrémité d'un câble à fibre optique. Divers connecteurs de ce type sont disponibles. Les principales différences entre les types de connecteurs sont les dimensions et les méthodes de couplage. Les entreprises décident en fonction de leur équipement des types de connecteurs qu'elles utiliseront.



# Tests de fibres optiques

- Le raccordement et l'épissage de câblage en fibre optique exigent une formation et un matériel adapté. Le raccordement incorrect de supports en fibre optique diminue les distances de signalisation ou entraîne l'échec complet de la transmission.
- On peut citer trois erreurs courantes de raccordement de fibre optique et d'épissage :
  - **Mauvais alignement** : les supports en fibre optique ne sont pas alignés précisément lors de la jonction.
  - **Écart à l'extrémité** : les supports ne se touchent pas complètement à l'épissure ou à la connexion.
  - **Finition de l'extrémité** : les extrémités des supports ne sont pas bien polies ou de la poussière est présente au niveau du raccordement.



# Réseaux sans fils

- Les supports sans fil transportent à l'aide de fréquences radio et micro-ondes des signaux électromagnétiques qui représentent les chiffres binaires des communications de données. Ils ont l'avantage de permettre la mobilité des clients.
- Toutefois, cette technologie présente également quelques contraintes :
  - **La zone de couverture** : les technologies de communication de données sans fil fonctionnent bien dans les environnements ouverts. Cependant, certains matériaux de construction utilisés dans les bâtiments et structures, ainsi que le terrain local, limitent la couverture effective.
  - **Les interférences** : la transmission sans fil est sensible aux interférences et peut être perturbée par des appareils aussi courants que les téléphones fixes sans fil, certains types d'éclairages fluorescents, les fours à micro-ondes et d'autres communications sans fil.
  - **La sécurité** : la connexion à un réseau sans fil ne nécessite aucun accès physique à un support. Par conséquent, les périphériques et les utilisateurs non autorisés à accéder au réseau peuvent quand même accéder à la transmission. La sécurité du réseau constitue un composant essentiel de l'administration des réseaux sans fil.
  - **Le support partagé** : les réseaux locaux sans fil fonctionnent en mode semi-duplex, ce qui signifie qu'un seul périphérique peut envoyer ou recevoir des données à la fois. Le support sans fil est partagé entre tous les utilisateurs sans fil. Plus le nombre d'utilisateurs ayant besoin d'accéder simultanément au réseau local sans fil est grand, moins il y a de bande passante disponible pour chacun d'entre eux.
- Bien que la technologie sans fil soit de plus en plus utilisée pour la connectivité entre les ordinateurs de bureau, le cuivre et la fibre sont les supports de couche physique les plus répandus dans les déploiements réseau.

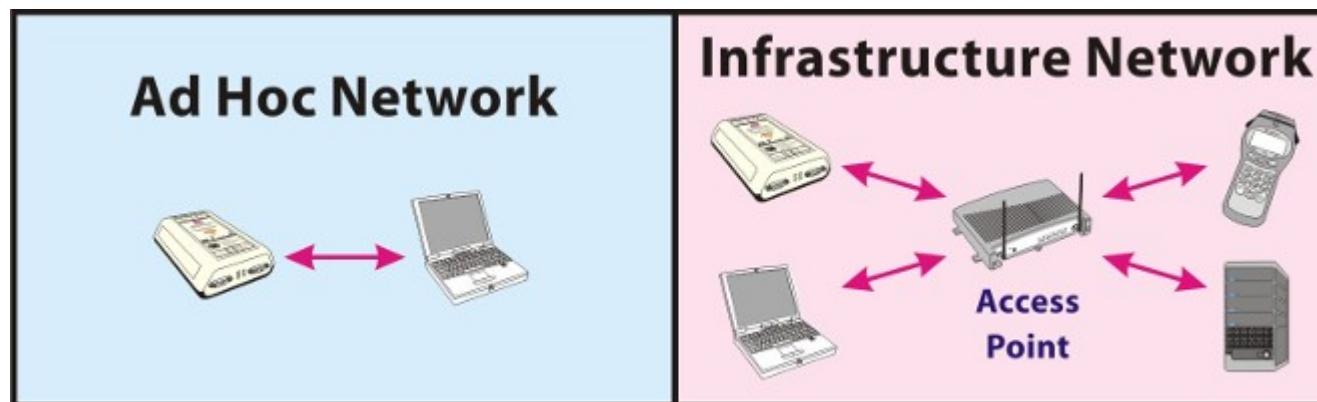
# Réseaux WIFI

- Le Wi-Fi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11. Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.
- Grâce aux normes Wi-Fi, il est possible de créer des réseaux locaux sans fil à haut débit. En pratique, le Wi-Fi permet des débits de :
  - 11 Mbit/s théoriques ou 6 Mbit/s réels en **802.11b** (porteuse à 2.4GHz),
  - 54 Mbit/s théoriques ou environ 25 Mbit/s réels en **802.11a** (porteuse à 5GHz), ou **802.11g** (porteuse à 2.4GHz),
  - 600 Mbit/s théoriques pour le **802.11n** (porteuse à 2.4GHz ou 5GHz), ,
  - 1,3 Gbit/s théoriques pour le **802.11ac** (porteuse à 5GHz), normalisé depuis décembre 2013.
- La portée peut atteindre plusieurs dizaines de mètres en intérieur (généralement entre une vingtaine et une cinquantaine de mètres) s'il n'y a aucun obstacle gênant (mur en béton par exemple) entre l'émetteur et l'utilisateur. Ainsi, des fournisseurs d'accès à Internet peuvent établir un réseau Wi-Fi connecté à Internet dans une zone à forte concentration d'utilisateurs (gare, aéroport, hôtel, train, etc.). Ces zones ou points d'accès sont appelés bornes ou points d'accès Wi-Fi ou « hot spots ».

# Modes de mise en réseau

- Il existe différents modes de mise en réseau :

- **Le mode « Infrastructure »** : mode qui permet de connecter les ordinateurs équipés d'une carte Wi-Fi entre eux via un ou plusieurs points d'accès (PA) qui agissent comme des concentrateurs. Dans ce cas, la mise en place d'un tel réseau oblige de poser à intervalles réguliers des bornes « Point d'accès » (PA) dans la zone qui doit être couverte par le réseau. Les bornes, ainsi que les machines, doivent être configurées avec le même nom de réseau (SSID = Service Set IDentifier) afin de pouvoir communiquer. L'avantage de ce mode, en entreprise, est de garantir un passage obligé par le Point d'accès: il est donc possible de vérifier qui accède au réseau.
- **Le mode « Ad hoc »** : mode qui permet de connecter directement les ordinateurs équipés d'une carte Wi-Fi, sans utiliser un matériel tiers tel qu'un point d'accès. Ce mode est idéal pour interconnecter rapidement des machines entre elles sans matériel supplémentaire (exemple : échange de fichiers entre portables dans un train, dans la rue, au café...). La mise en place d'un tel réseau consiste à configurer les machines en mode « Ad hoc », la sélection d'un canal (fréquence), d'un nom de réseau (SSID) communs à tous et si nécessaire d'une clé de chiffrement. L'avantage de ce mode est de s'affranchir de matériels tiers, c'est-à-dire de pouvoir fonctionner en l'absence de point d'accès.

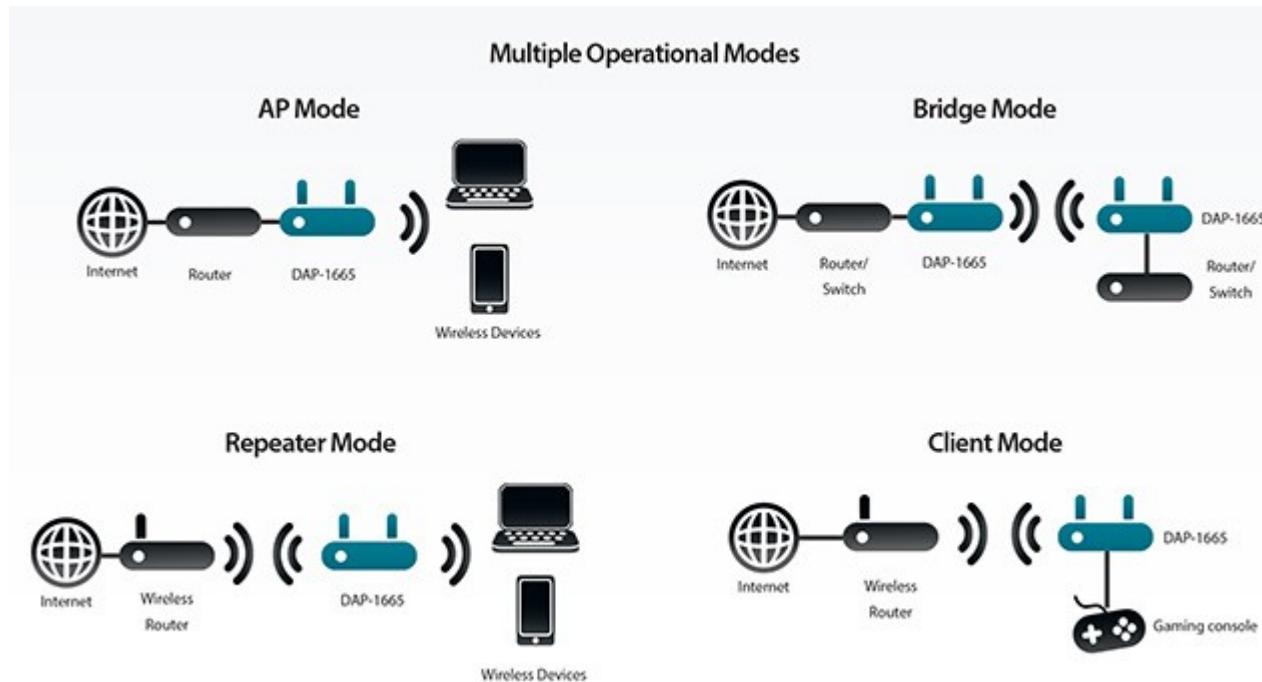


# Modes de mise en réseau

- **Le mode « Pont » :** Un point d'accès en mode « Pont » sert à connecter un ou plusieurs points d'accès entre eux pour étendre un réseau filaire, par exemple entre deux bâtiments. La connexion se fait au niveau de la couche 2 OSI. Un point d'accès doit fonctionner en mode «Racine» (« Root Bridge », généralement celui qui distribue l'accès Internet) et les autres s'y connectent en mode « Bridge » pour ensuite retransmettre la connexion sur leur interface Ethernet. Chacun de ces points d'accès peut éventuellement être configuré en mode «Pont» avec connexion de clients. Ce mode permet de faire un pont tout en accueillant des clients comme le mode « Infrastructure ».
- **Le mode « Répéteur » :** Un point d'accès en mode « Répéteur » permet de répéter un signal Wi-Fi plus loin (par exemple pour atteindre un fond de couloir en « L »). Contrairement au mode « Pont », l'interface Ethernet reste inactive. Chaque « saut » supplémentaire augmente cependant le temps de latence de la connexion. Un répéteur a également une tendance à diminuer le débit de la connexion. En effet, son antenne doit recevoir un signal et le retransmettre par la même interface ce qui en théorie divise le débit par deux.

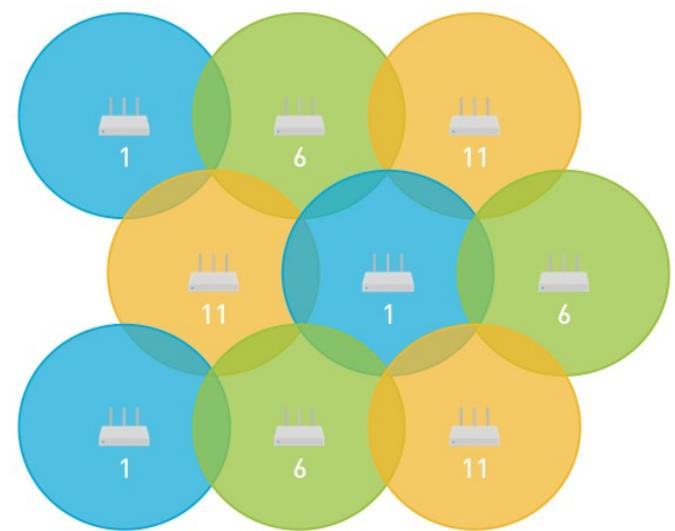
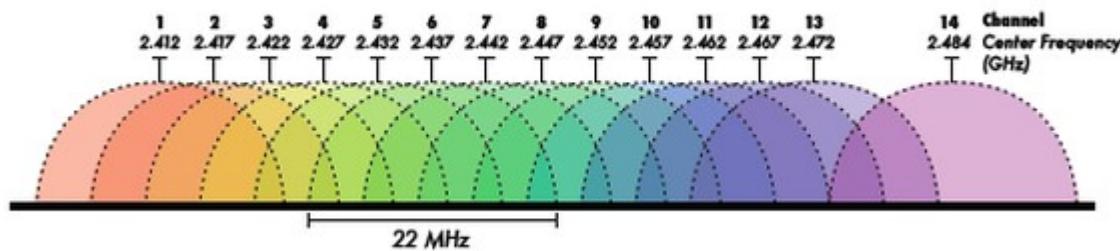
# Modes de mise en réseau

- **Le mode « Client » :** Ce mode nécessite deux points d'accès, l'un configuré en Point d'accès et l'autre en Point d'accès client. Il permet de relier un LAN filaire distant à un réseau WIFI ou inversement. Un point d'accès configuré en client ne peut être joint par une station WIFI cliente. Le point d'accès configuré en client communiquera de manière exclusive avec le point d'accès auquel il aura été rattaché (via l'adresse mac du PA). Il agira comme un client du point d'accès, c'est pourquoi les stations WIFI ne pourront pas communiquer avec directement, mais par contre pourront communiquer avec les machines du réseau filaire qui lui sont rattachées.



# Les canaux WIFI

- Les équipements Wi-Fi, utilisent une partie limitée des bandes de fréquences hertziennes, afin de limiter les interférences avec d'autres équipements; un certain nombre de canaux Wi-Fi sont donc définis par les États et les organismes de normalisation (figure gauche).
- Lors de la disposition de plusieurs points d'accès WIFI dans une entreprise (figure de droite), il faut veiller à ce que les points d'accès dont les signaux chevauchent, utilisent des canaux qui ne présentent pas d'interférences entre eux ( comme les canaux 1, 6 et 11 dans la bande de fréquence 2.4GHz).



# WIFI - Méthode d'accès au média

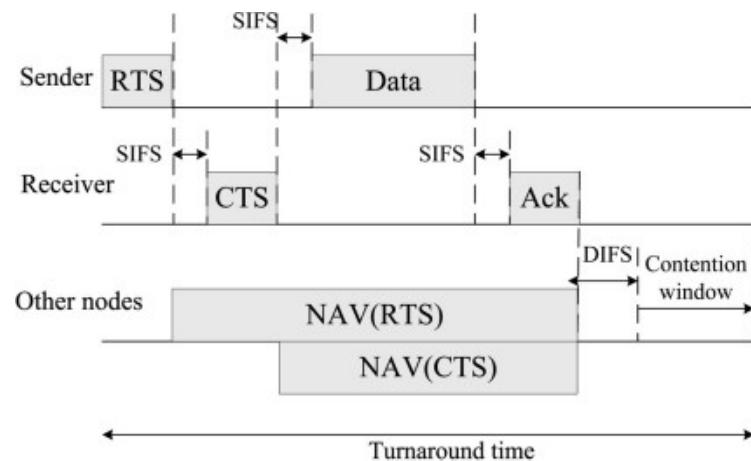
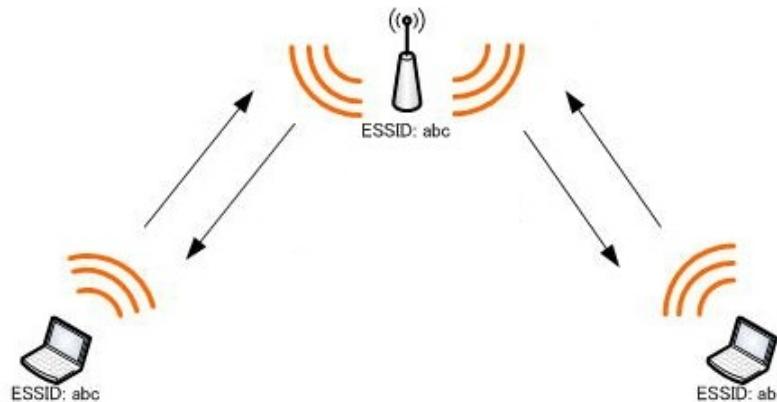
- **CSMA/CA (Carrier Sens, Multiple Access - Collision Avoidance)**

La méthode **CSMA/CA** s'utilise dans les réseaux sans-fil. En effet, contrairement aux réseaux filaires, **deux stations peuvent émettre vers une troisième sans se détecter** (la première étant hors de portée de la seconde).

Pour éviter cela, une station est considérée comme le maître des transmissions qui autorise une station à communiquer lorsque celle-ci le demande. Pour cela, la station doit émettre une courte trame **RTS (Ready To Send)** contenant quelques informations sur la communication (débit, longueur de la trame, etc.).

Si la station maître accepte cette communication, elle renvoie alors une trame **CTS (Clear To Send)** et la station peut transmettre son message. En revanche, si la station ne reçoit pas de message elle doit attendre à nouveau avant de redemander une autorisation d'émettre.

- C'est la méthode utilisée dans les réseaux **Wi-Fi (802.11)** et la station maître est généralement le point d'accès.



# Sécurité des réseaux WIFI

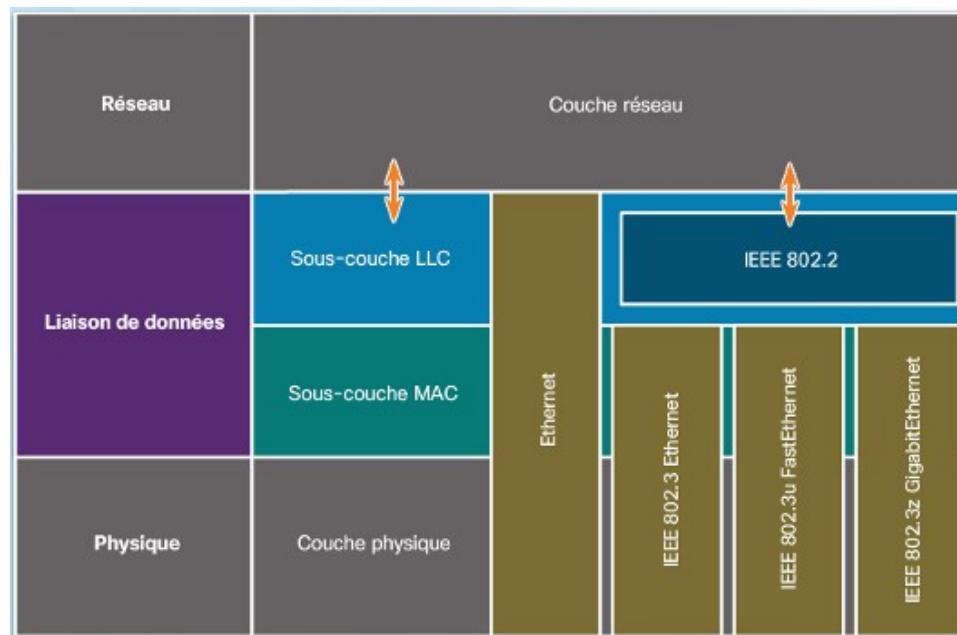
- Les réseaux Wi-Fi disposent de différentes options de sécurité pouvant être configurées afin d'améliorer la confidentialité de nos communications. Les options les plus courantes sont les suivantes :
  - Cacher le SSID du réseau WIFI
  - Effectuer un filtrage par adresses MAC
  - Utiliser un algorithme de cryptage de données (WEP (pas recommandé), WPA, WPA2)
  - Utiliser un serveur d'authentification (Solution recommandée pour l'entreprise).



# Couche Liaison de données

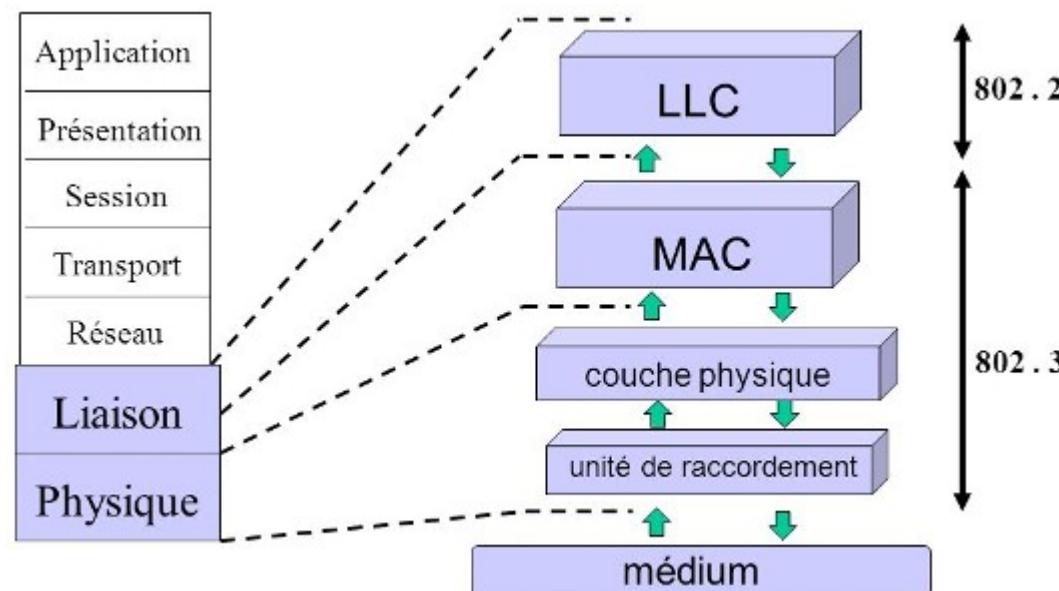
# Technologies ETHERNET

- Ethernet est la technologie LAN la plus répandue aujourd'hui, surtout dans les réseaux LAN.
- Il fonctionne au niveau de la couche liaison de données et de la couche physique. Ethernet est une famille de technologies de réseau définies par les normes **IEEE 802.2** et **IEEE 802.3**. Ethernet prend en charge des bandes passantes de données suivantes : **10 Mbit/s**, **100 Mbit/s**, **1 000 Mbit/s** (1 Gbit/s), **10 000 Mbit/s** (10 Gbit/s), **40 000 Mbit/s** (40 Gbit/s), **100 000 Mbit/s** (100 Gbit/s), **2 500 Mbit/s** (2,5 Gbit/s), **5 000 Mbit/s** (5 Gbit/s).
- Les normes Ethernet définissent à la fois les protocoles de la **couche 2** et les technologies de la **couche 1**. Pour les protocoles de couche 2, comme pour toutes les normes IEEE 802, le fonctionnement d'Ethernet dépend de deux sous-couches distinctes de la couche liaison de données : la **sous-couche de contrôle de liaison logique (LLC)** et la **sous-couche MAC**.



# Sous-couche LLC ETHERNET

- La sous-couche LLC Ethernet gère la **communication entre les couches supérieures et les couches inférieures**. Celle-ci a généralement lieu entre les logiciels et les matériels réseau du périphérique. La sous-couche LLC extrait les données des protocoles réseau, en principe un paquet IPv4, et leur ajoute des informations de contrôle pour faciliter la transmission du paquet jusqu'au nœud de destination. Elle est utilisée pour communiquer avec les couches supérieures de l'application et pour faire passer le paquet aux couches inférieures en vue de son acheminement.
- La mise en œuvre de la sous-couche LLC se fait au niveau logiciel et est indépendante du matériel. Dans un ordinateur, **la sous-couche LLC est en quelque sorte le pilote de la carte réseau**, qui n'est autre qu'un logiciel qui interagit directement avec le matériel de la carte réseau pour transmettre les données entre la sous-couche MAC et les supports physiques.



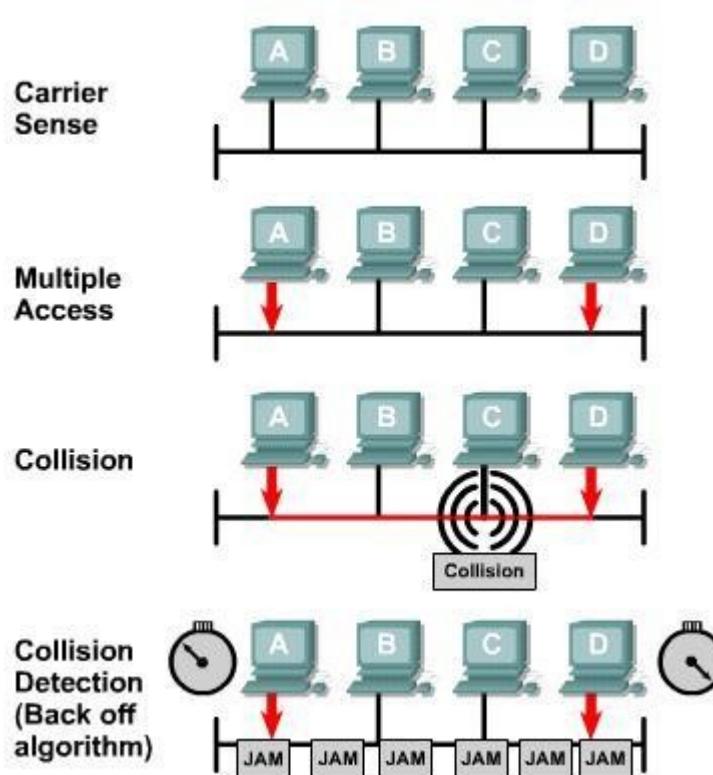
# Sous-couche MAC ETHERNET

- La sous-couche MAC est la sous-couche inférieure de la couche liaison de données. Elle est mise en œuvre au niveau matériel, généralement sur la carte réseau de l'ordinateur. Les spécifications sont décrites par les normes IEEE 802.3. La figure ci-dessous présente une liste de quelques normes Ethernet courantes de l'IEEE.
- La sous-couche MAC Ethernet a deux fonctions principales :
  - L'encapsulation de données (la délimitation des trames, l'adressage, la détection des erreurs)
  - Le contrôle de l'accès aux supports (placement des trames sur les supports et leur récupération). La méthode **CSMA/CD** (**Carrier Sense Multiple Access with Collision Detection**) est utilisée avec les réseaux locaux Ethernet en **mode semi-duplex** pour détecter et gérer les conflits d'accès au média.

Common Name	Speed	Alternative Name	Name of IEEE Standard	Cable Type, Maximum Length
Ethernet	10Mbps	10BASE-T	802.3	Copper, 100 m
Fast Ethernet	100Mbps	100BASE-TX	802.3u	Copper, 100 m
Gigabit Ethernet	1000Mbps	1000BASE-LX	802.3z	Fiber, 550 m
Gigabit Ethernet	1000Mbps	1000BASE-T	802.3ab	Copper, 100 m
10GigE (Gigabit Ethernet)	10Gbps	10GBASE-T	802.3an	Copper, 100 m

# Méthode d'accès CSMA/CD

- Les réseaux locaux Ethernet avec concentrateurs, et les anciens réseaux de bus Ethernet constituent des exemples de réseaux d'accès avec gestion des conflits CSMA/CD. Tous ces réseaux fonctionnent en mode semi-duplex. Une procédure est donc nécessaire pour déterminer à quel moment un périphérique peut envoyer des données et ce qui doit se produire lorsque plusieurs périphériques envoient des données au même moment.



# Méthode d'accès CSMA/CD

- La topologie logique d'Ethernet est un bus à accès multiple. Par conséquent, tous les nœuds (périphériques) d'un même segment réseau doivent partager le support.
- Le processus d'accès multiple avec écoute de porteuse et détection de collision (CSMA/CD) se déroule comme suit :
  - L'hôte A a une trame Ethernet à envoyer à l'hôte B.
  - La carte réseau de l'hôte A doit déterminer si le support de transmission est libre. Si elle ne détecte aucun signal (porteuse) elle considère que le réseau est disponible pour effectuer un envoi.
  - La carte réseau de l'hôte A envoie la trame Ethernet.
  - Si un autre périphérique, comme l'hôte C, veut transmettre des données mais est en train de recevoir une trame, il doit patienter jusqu'à ce que le canal soit libre.
  - Tous les périphériques reliés au concentrateur reçoivent la trame. Étant donné que la trame possède une adresse de liaison de données de destination pour l'hôte B, seul ce périphérique acceptera et copiera la trame dans son ensemble. Les cartes réseau de tous les autres périphériques ignoreront la trame.
  - Si deux périphériques transmettent en même temps (A et D par exemple), il se produit une collision. Les deux périphériques détectent la collision sur le réseau. Les données envoyées par les deux périphériques sont corrompues et doivent être envoyées de nouveau.
- Les LAN Ethernet actuels utilisent des commutateurs en mode duplex intégral, ce qui permet à plusieurs périphériques d'envoyer et de recevoir simultanément des données sans créer de conflits.

# Format d'une trame ETHERNET

- La taille minimale des trames Ethernet est de 64 octets et la taille maximale de 1518 octets. Cela comprend tous les octets du champ Adresse MAC de destination jusqu'au champ Séquence de contrôle de trame (FCS). Le champ Préambule n'est pas inclus dans la description de la taille d'une trame.
- Toute trame inférieure à 64 octets est interprétée comme un «fragment de collision» ou une «trame incomplète» et est automatiquement rejetée par les périphériques récepteurs. Les trames de plus de 1500 octets de données sont considérées comme des trames «jumbo» (géantes) ou «baby giant frames» (légèrement géantes). Elles sont également abandonnées par les périphériques récepteurs.
- Les trames abandonnées sont souvent le résultat de collisions et sont donc traités comme étant non valides.

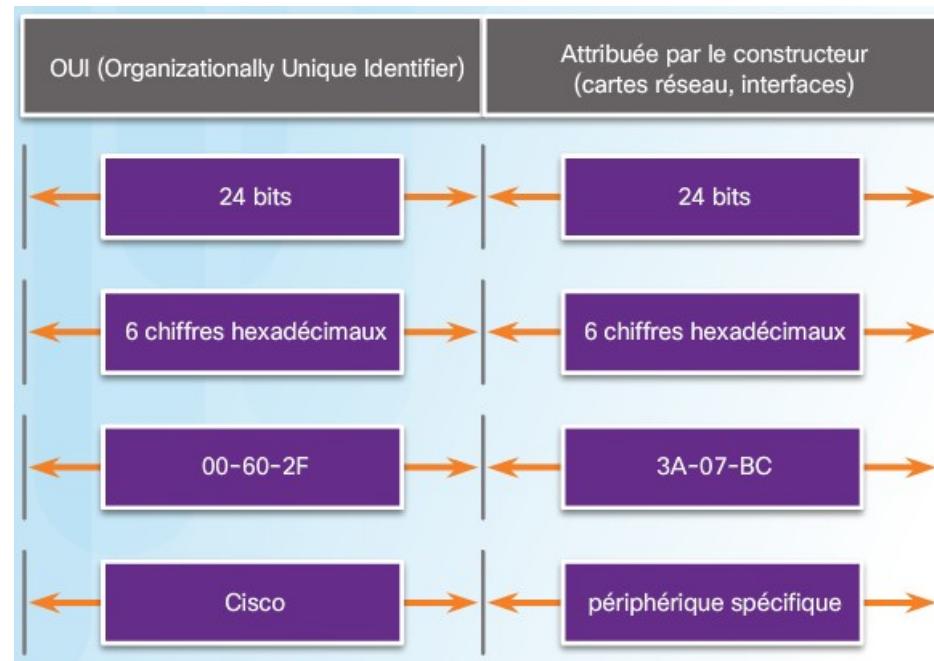


# Format d'une trame ETHERNET

- **Préambule** (7 octets) : champ Délimiteur de début de trame (SFD). Il est utilisé à des fins de synchronisation entre les périphériques d'envoi et de réception. Les huit premiers octets de la trame préparent les noeuds de réception à recevoir.
- **Adresse MAC de destination** (6 octets) : identifie la carte réseau du destinataire. Il peut s'agir d'une adresse monodiffusion (un seul hôte destinataire), de multidiffusion (un groupe d'hôte destinataire) ou de diffusion (tous les hôtes du segment réseau sont concernés par la trame).
- **Adresse MAC de source** (6 octets) : identifie la carte réseau origine de la trame. Il doit s'agir d'une adresse de monodiffusion.
- **EtherType** (2 octets) : identifie le protocole de la couche supérieure encapsulé dans la trame Ethernet. Les valeurs hexadécimales les plus fréquentes sont 0x0800 pour IPv4, 0x86DD pour IPv6 et 0x0806 pour ARP.
- **Données** (46 à 1 500 octets) : contient les données encapsulées d'une couche supérieure. La longueur minimale de la trame est fixée à 64 octets. Si un paquet de petite taille est encapsulé, d'autres bits appelés remplissage sont utilisés pour augmenter la taille de la trame et la ramener à cette taille minimale.
- **FCS** (4 octets) : permet de détecter les erreurs d'une trame. Il utilise le contrôle de redondance cyclique (CRC, Cyclic Redundancy Check). Le périphérique d'envoi inclut les résultats du CRC dans le champ FCS de la trame. Le périphérique de réception reçoit la trame et génère son propre CRC pour détecter les erreurs. Si les calculs correspondent, aucune erreur ne s'est produite. Les calculs non rapprochés indiquent que les données ont changé et que la trame est abandonnée. Si les données sont modifiées, cela provient sans doute d'une perturbation des signaux électriques qui représentent les bits.

# Structure d'une adresse MAC

- Les règles établies par l'IEEE exigent de chaque revendeur de périphérique Ethernet qu'il s'enregistre auprès de l'IEEE. Ce dernier attribue au constructeur un code de 3 octets (24 bits) appelé **OUI (Organizationally Unique Identifier)**. L'IEEE demande aux constructeurs de respecter deux règles simples représentées sur la figure :
  - Toutes les adresses MAC attribuées à une carte réseau ou à un autre périphérique Ethernet doivent utiliser, comme 3 premiers octets, l'identifiant OUI attribué au revendeur correspondant.
  - Toutes les adresses MAC ayant le même identifiant OUI doivent utiliser une valeur unique dans les 3 derniers octets.



# Représentation d'une adresse MAC

- Sur un hôte Windows, la commande **ipconfig /all** permet d'identifier l'adresse MAC d'un adaptateur Ethernet. Elle est alors affichée sous la forme XX-XX-XX-XX-XX-XX où X est un caractère hexadécimal.
- Sur les hôtes MAC ou Linux, c'est la commande **ifconfig** qui est utilisée. L'adresse MAC est affichée sous la forme XX:XX:XX:XX:XX:XX où X est un caractère hexadécimal.
- Selon le périphérique et le système d'exploitation, différentes représentations des adresses MAC s'affichent, comme le montre la figure ci-dessous. Les routeurs et les commutateurs Cisco utilisent la forme XXXX.XXXX.XXXX où X est un caractère hexadécimal.

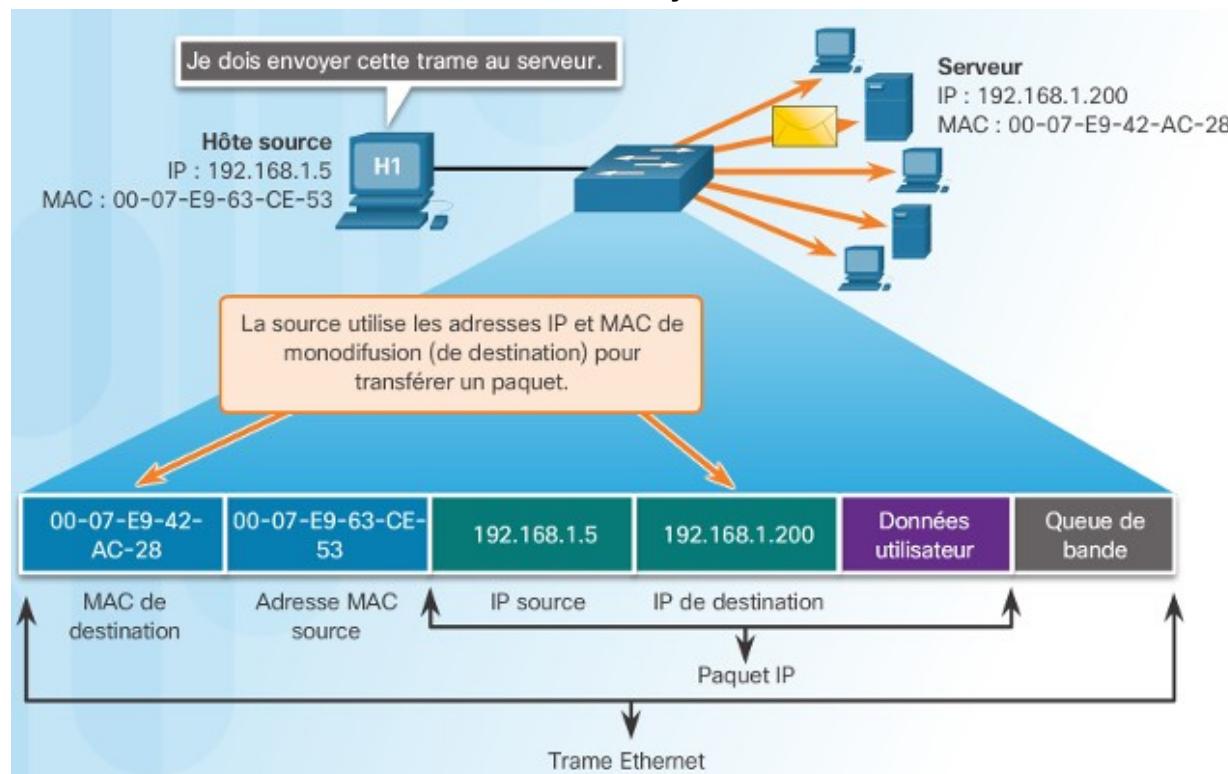
Avec des tirets 00-60-2F-3A-07-BC

Avec deux-points 00:60:2F:3A:07:BC

Avec des points 0060.2F3A.07BC

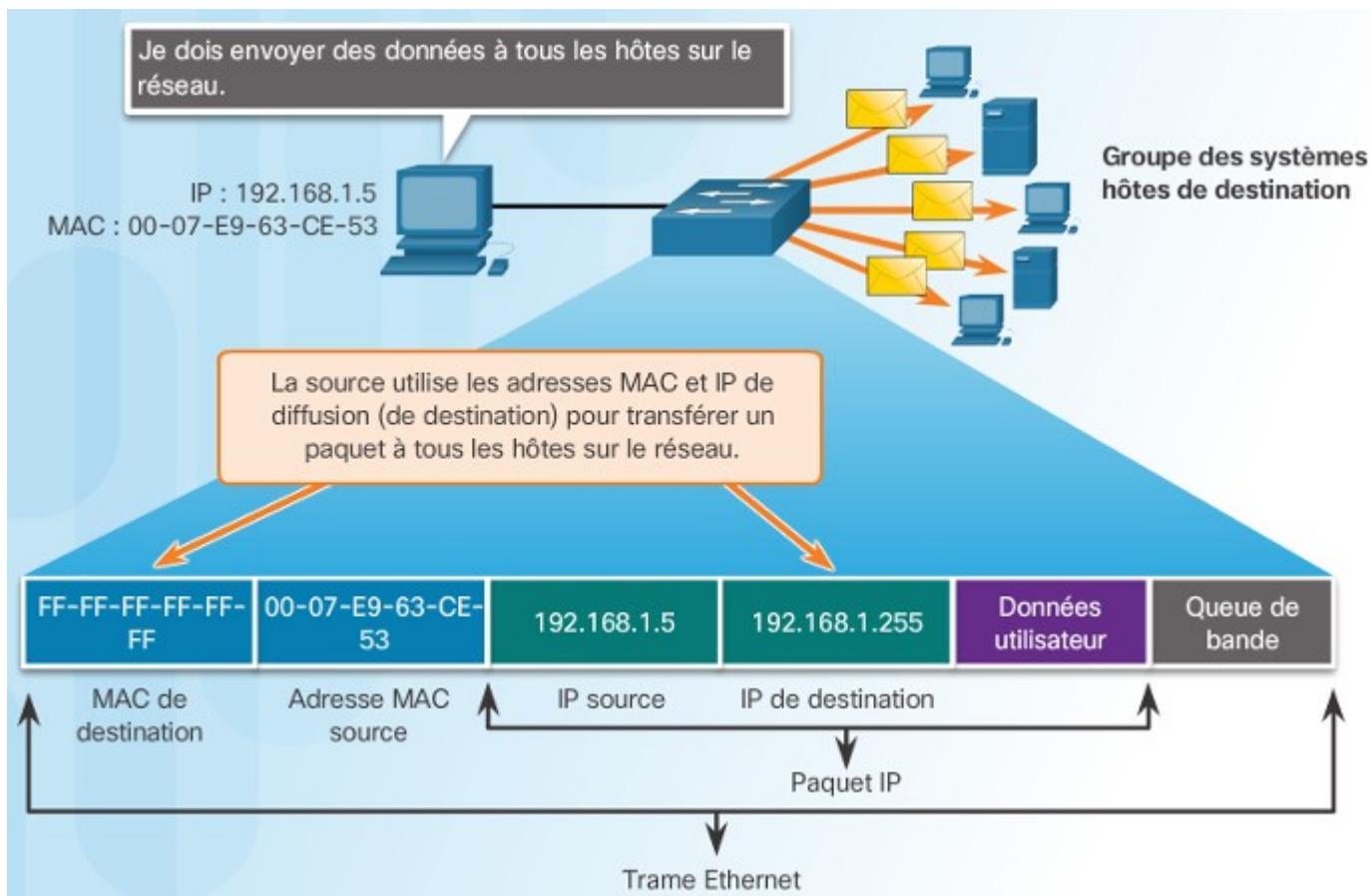
# Adresse MAC monodiffusion

- L'adresse MAC de monodiffusion est l'adresse utilisée lorsqu'une trame est envoyée à partir d'un périphérique émetteur, à un seul périphérique destinataire.
- Le processus qu'un hôte source utilise pour déterminer l'adresse MAC de destination est appelé protocole ARP (Address Resolution Protocol).
- L'adresse MAC de destination peut donc être une adresse de monodiffusion, de diffusion ou de multidiffusion, mais l'adresse MAC source doit toujours être une adresse de monodiffusion.



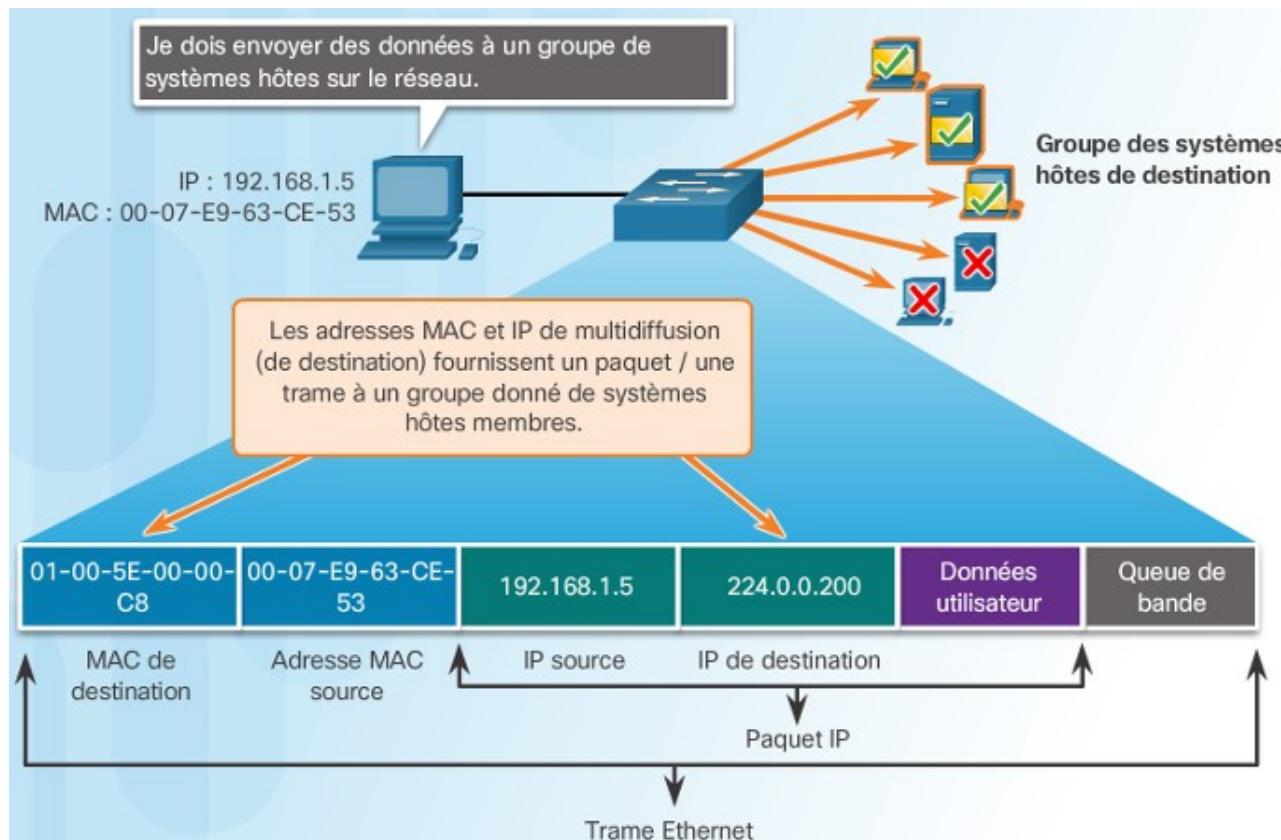
# Adresse MAC de diffusion

- Lorsqu'un paquet est destiné à tous les hôtes d'un segment réseau local, il est encapsulé dans une trame dont l'adresse MAC de destination est égale à **FF-FF-FF-FF-FF-FF**. Cette adresse est appelée **Adresse MAC de diffusion**.
- De nombreux protocoles réseau, tels que DHCP et ARP, utilisent les diffusions.



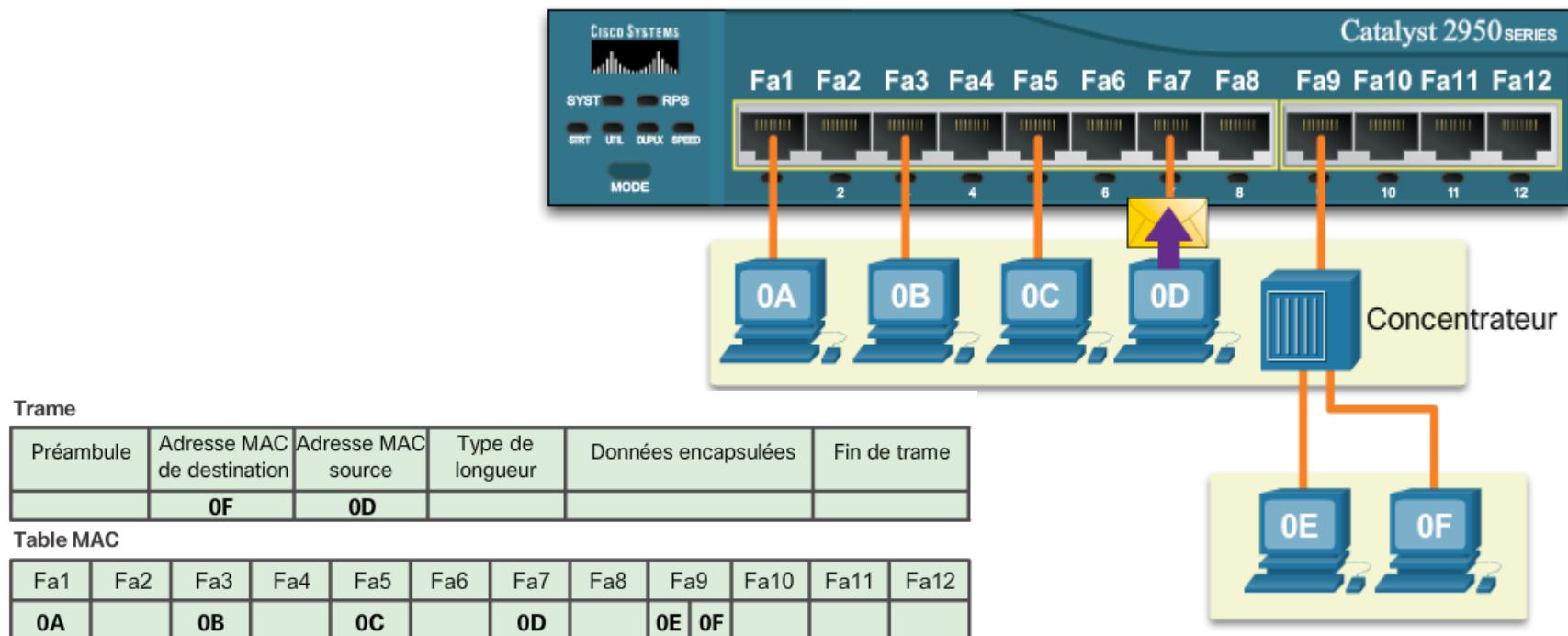
# Adresse MAC multidiffusion

- Les adresses de multidiffusion permettent à un périphérique source d'envoyer un paquet à un groupe de périphériques. L'adresse MAC de multidiffusion est associée à une adresse de multidiffusion IPv4. Elle commence par les six caractères hexadécimaux **01-00-5E**. L'autre partie de l'adresse MAC de multidiffusion provient de la conversion des 23 bits inférieurs de l'adresse IP du groupe de multidiffusion en 6 caractères hexadécimaux. Pour une adresse IPv6, l'adresse MAC de multidiffusion commence par 33-33.



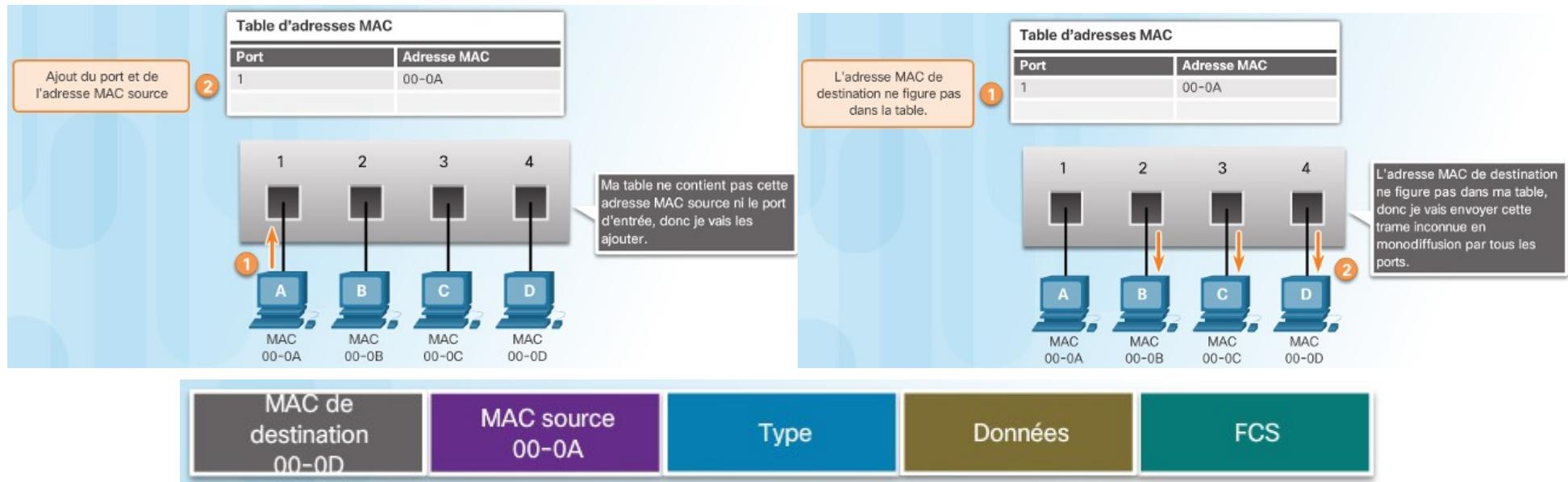
# Commutateurs ETHERNET

- Un commutateur Ethernet de couche 2 utilise des adresses MAC pour prendre des décisions de transmission. Il ignore totalement le protocole transporté dans le champ données de la trame, tel qu'un paquet IPv4.
- Contrairement à un concentrateur Ethernet qui répète les bits sur tous les ports sauf le port entrant, un commutateur Ethernet consulte une table d'adresses MAC pour décider de la transmission de chaque trame.
- Cette table d'adresses MAC est parfois appelée table de mémoire associative (CAM).



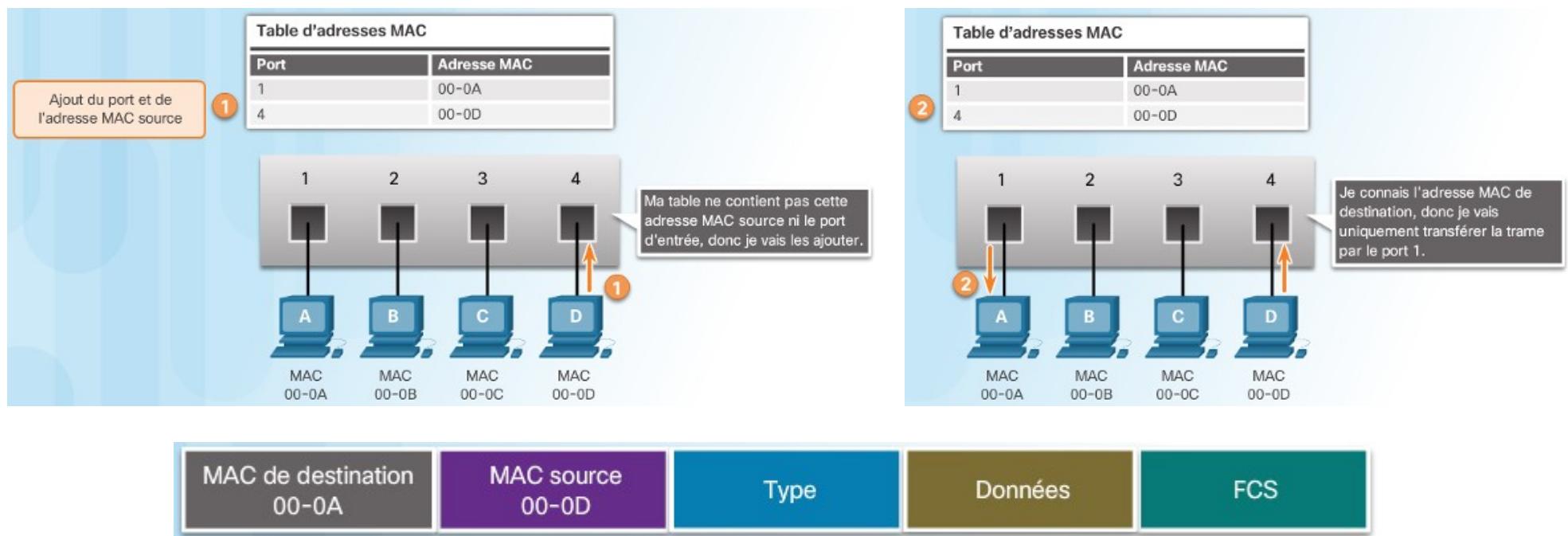
# Apprendre des adresses MAC

- A chaque fois qu'un commutateur reçoit une trame sur un port, il récupère son **adresse MAC source**, et la place dans sa table d'adresses MAC en l'associant au numéro de port où elle a été reçue. Si l'adresse MAC est déjà associée à ce port dans la table d'adresses MAC, il réinitialise le compteur d'obsolescence correspondant. Par défaut, la plupart des commutateurs Ethernet conservent les entrées dans la table pendant 5 minutes.
- Si l'adresse **MAC de destination** est **inconnue** par le commutateur (n'existe pas dans sa table d'adresses MAC), **la trame sera diffusée** vers tous les ports sauf celui par lequel elle est arrivée. Ça sera également le cas si l'adresse MAC de destination est une adresse de diffusion ou de multidiffusion.



# Déterminer le port de destination

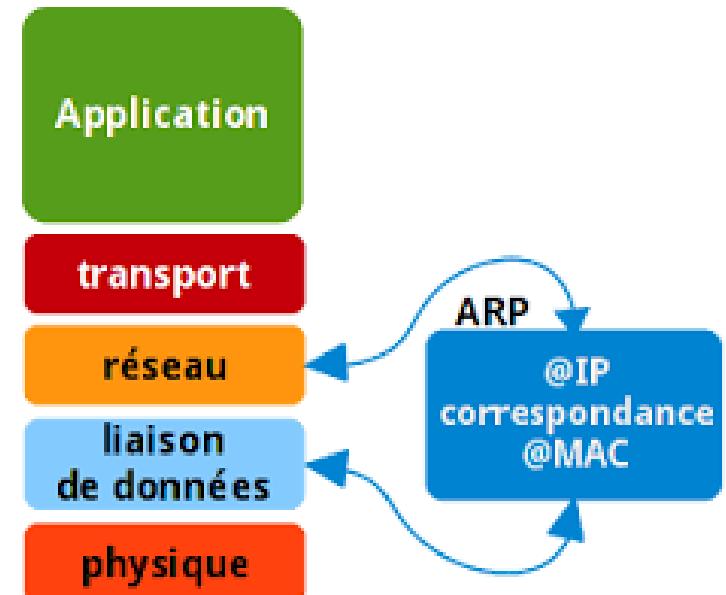
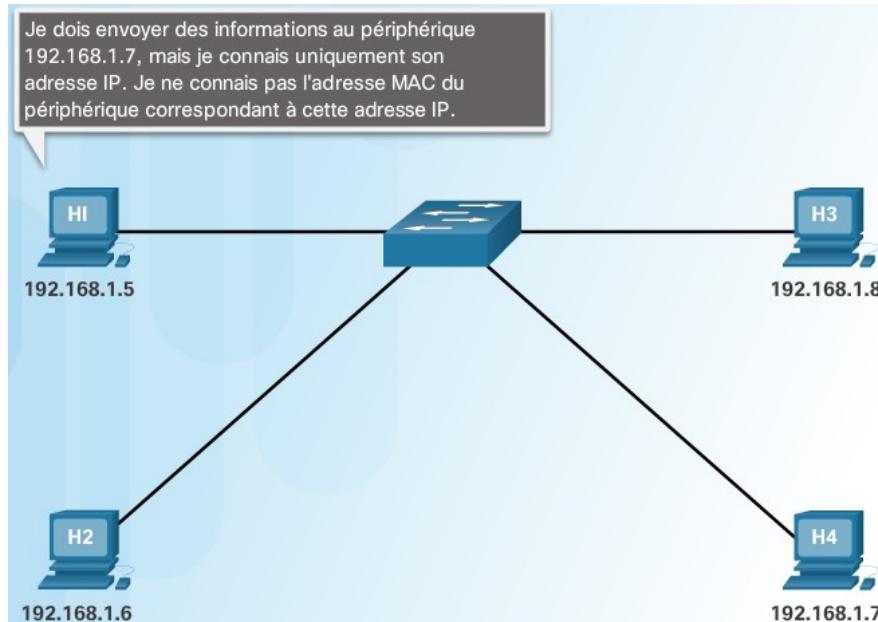
- À mesure qu'un commutateur reçoit des trames de différents périphériques, il remplit sa table d'adresses MAC en examinant l'adresse MAC source de chaque trame. Si la table d'adresses MAC du commutateur contient l'**adresse MAC de destination** de la trame, il va la transmettre sur le port correspondant.



# ARP (Address Resolution Protocol)

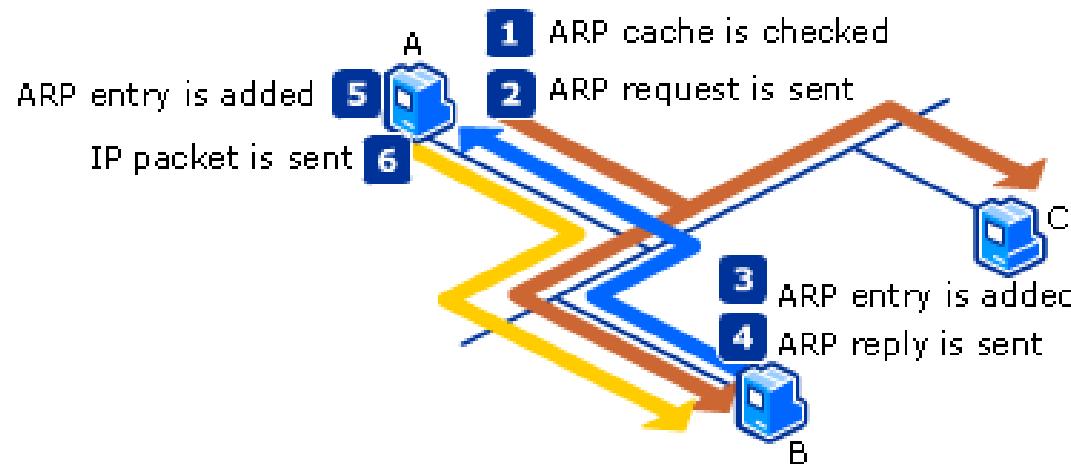
# Rôle du protocole ARP

- Tout périphérique possédant une adresse IP sur un réseau Ethernet possède également une adresse MAC Ethernet. Lorsqu'un périphérique envoie une trame Ethernet, celle-ci contient deux adresses : l'adresse MAC de destination, et l'adresse MAC source.
- Pour déterminer l'adresse MAC de destination, le périphérique utilise le protocole ARP.
- Le protocole ARP assure deux fonctions principales :
  - la résolution des adresses IPv4 de destination en adresses MAC correspondante;
  - la gestion d'une table des mappages (le cache ARP).



# Fonctionnement du protocole ARP

- Quand un paquet arrive à la couche liaison de données pour être encapsulé dans une trame Ethernet, le périphérique consulte une table stockée dans sa mémoire pour connaître l'adresse MAC qui correspond à l'adresse IPv4. Cette table est appelée table ARP ou cache ARP. Cette table ARP est stocké dans la mémoire vive (RAM) du périphérique.
- Le périphérique expéditeur recherche dans sa table ARP une adresse IPv4 de destination et l'adresse MAC correspondante.
  - Si l'adresse IPv4 de destination du paquet appartient au même réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de destination dans sa table ARP.
  - Si l'adresse IPv4 de destination du paquet appartient à un autre réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de la passerelle par défaut dans sa table ARP.



# Fonctionnement du protocole ARP

- La table ARP stocke temporairement (dans la mémoire cache) les adresses IPv4 des périphériques du réseau local et les adresses MAC correspondantes.
- Si le périphérique localise l'adresse IPv4, l'adresse MAC correspondante est utilisée comme adresse MAC de destination dans la trame. Si l'entrée n'existe pas, le périphérique envoie une requête ARP.
- La requête ARP est une trame de diffusion (envoyée à l'adresse MAC **FF-FF-FF-FF-FF-FF**), mais la réponse ARP est une trame monodiffusion (destinée uniquement à l'hôte ayant envoyé la requête).
- Pour chaque périphérique, un compteur de cache ARP supprime les entrées ARP qui n'ont pas été utilisées pendant une période donnée. Cette période varie en fonction du système d'exploitation du périphérique. Par exemple, certains systèmes d'exploitation Windows stockent les entrées de cache ARP pendant 2 minutes, comme illustré sur la figure.
- Des commandes permettent aussi de supprimer manuellement les entrées du tableau ARP totalement ou partiellement. Lorsqu'une entrée est supprimée, le processus d'envoi d'une requête ARP et de réception d'une réponse ARP doit être répété pour entrer le mappage dans le tableau ARP.

# Commandes ARP

- La commande arp permet la consultation et parfois la modification de la table ARP dans certains systèmes d'exploitation.
  - arp -a : affiche toutes les entrées dans le cache ARP.
  - arp -s @ip @MAC : ajout manuel d'une entrée statique permanente dans le cache (ce besoin se manifeste si on appelle régulièrement des hôtes, pour réduire le trafic réseau).
  - arp -d : permet de vider le cache ARP

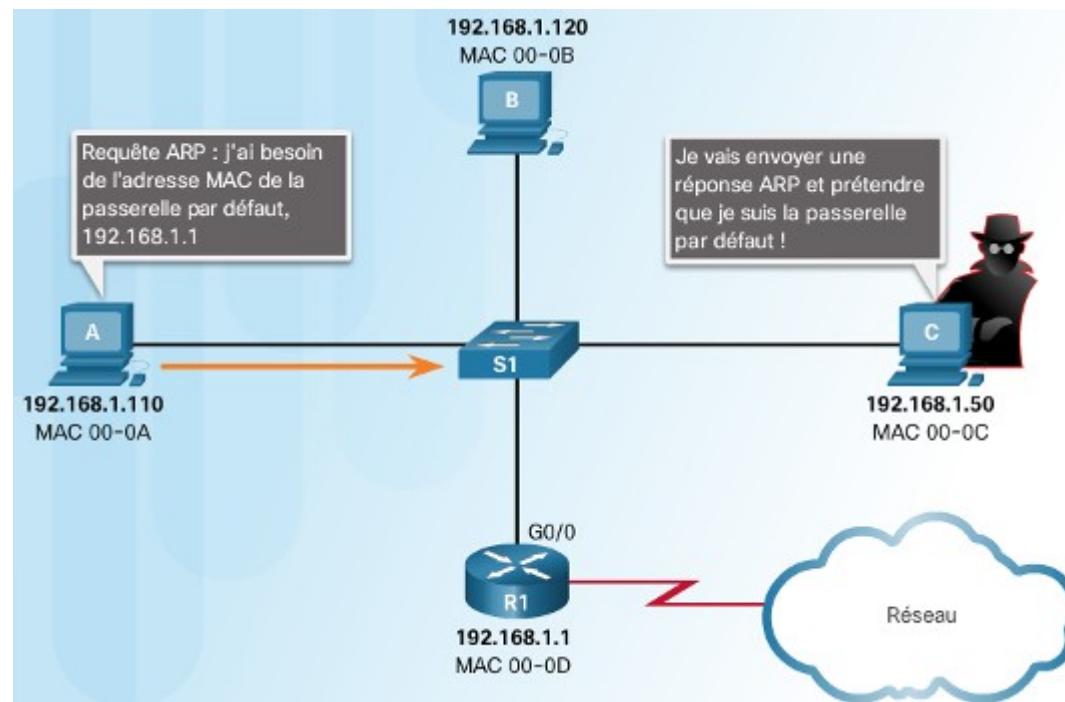
```
C:\> arp -a

Interface: 192.168.1.67 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.254        64-0f-29-0d-36-91    dynamic
  192.168.1.255        ff-ff-ff-ff-ff-ff    static
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static

Interface: 10.82.253.91 --- 0x10
  Internet Address      Physical Address      Type
  10.82.253.92          64-0f-29-0d-36-91    dynamic
  224.0.0.22            01-00-5e-00-00-16    static
  224.0.0.251           01-00-5e-00-00-fb    static
  224.0.0.252           01-00-5e-00-00-fc    static
  255.255.255.255      ff-ff-ff-ff-ff-ff    static
```

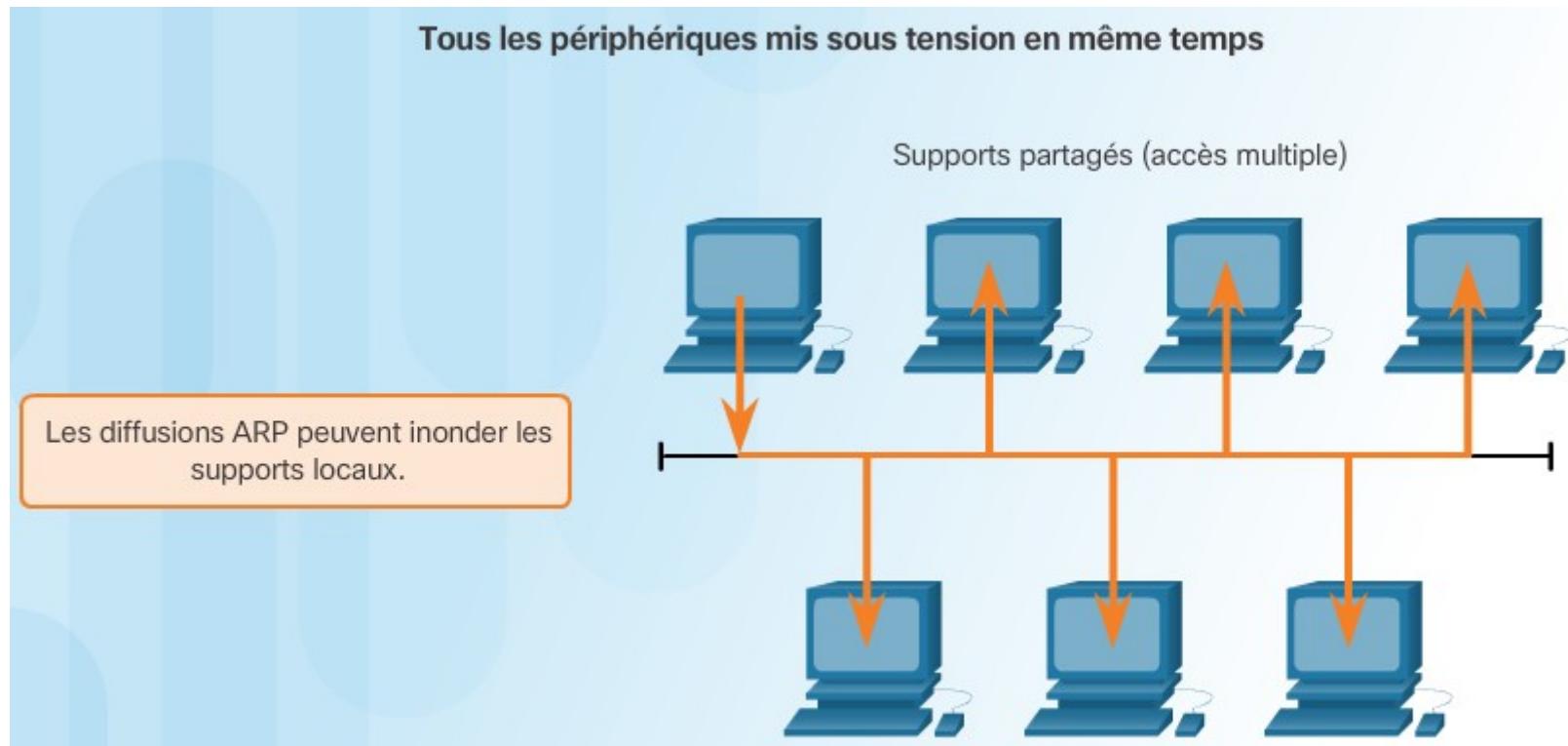
# Usurpation ARP

- L'utilisation du protocole ARP peut créer un risque de sécurité appelé usurpation ARP (**ARP Spoofing**) ou empoisonnement ARP (**ARP poisoning**). Il s'agit d'une technique utilisée par un pirate pour répondre à une requête ARP concernant l'adresse IPv4 d'un autre périphérique tel que la passerelle par défaut. Le pirate envoie une réponse ARP avec sa propre adresse MAC. Ainsi, le récepteur de la réponse ARP ajoute la mauvaise adresse MAC à sa table ARP et envoie les paquets au pirate.
- Les commutateurs destinés aux grandes entreprises offrent des méthodes de limitation de ce risque appelées **inspection ARP dynamique**.



# Diffusions ARP

- **Les requêtes ARP sont des trames de diffusion** (destinées à l'adresse MAC FFFF.FFFF.FFFF). Elles sont reçues et traitées par chaque périphérique du réseau local. Sur un réseau d'entreprise type, ces diffusions auraient probablement une incidence minime sur les performances du réseau. Toutefois, si un grand nombre de périphériques sont mis sous tension et accèdent aux services du réseau au même moment, les performances du réseau peuvent s'en trouver réduites sur un court laps de temps. Si les périphériques envoient les messages de diffusion ARP initiaux et disposent des adresses MAC nécessaires, l'impact sur le réseau sera minime.



# Couche réseau

# La couche réseau

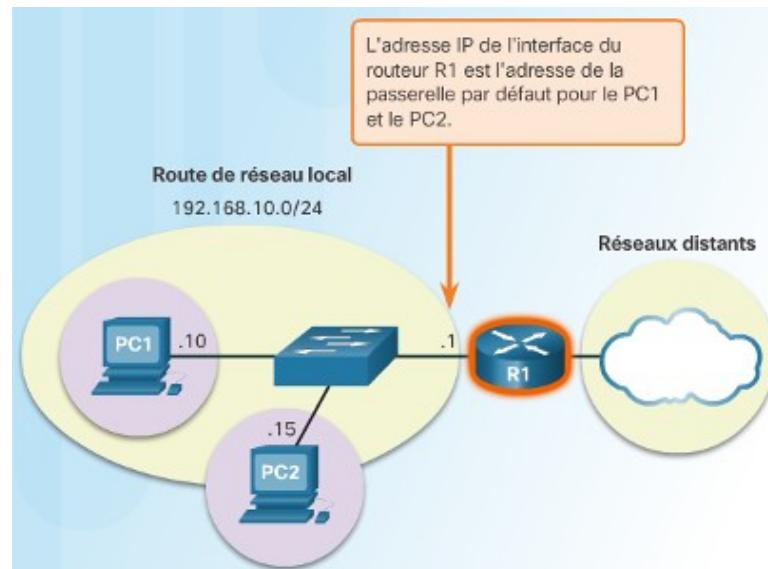
- La couche réseau, ou couche 3 du modèle OSI, fournit des services permettant aux périphériques finaux d'échanger des données sur le réseau. Pour effectuer ce transport de bout en bout, la couche réseau utilise quatre processus de base :
  - L'adressage des périphériques finaux
  - L'encapsulation
  - Le routage
  - La désencapsulation
- Il existe plusieurs protocoles de couche réseau parmi lesquels on trouve :
  - Le protocole IP version 4 (IPv4)
  - Le protocole IP version 6 (IPv6)
  - Le protocole ICMP

# Transmission de paquets entre hôtes

- La couche réseau est responsable de diriger les paquets entre les hôtes. Un hôte peut envoyer un paquet à :
  - **Lui-même** : un hôte peut s'envoyer une requête ping en envoyant un paquet à une adresse IPv4 spécifique, **127.0.0.1**, appelée **interface de bouclage**. L'envoi d'une requête ping à l'interface de bouclage permet de tester la pile de protocoles TCP/IP sur l'hôte.
  - **Un hôte local** : il s'agit d'un hôte sur le même réseau local que l'hôte émetteur. Les hôtes partagent la même adresse réseau.
  - **Un hôte distant** : il s'agit d'un hôte sur un réseau distant. Les hôtes ne partagent pas la même adresse réseau.
- Pour déterminer si le paquet est destiné à un hôte local ou à un hôte distant, **la combinaison adresse IPv4/masque** de sous-réseau du périphérique source (expéditeur) est comparée à la combinaison adresse IPv4/masque de sous-réseau du périphérique de destination.
- Les périphériques se trouvant au-delà du segment de réseau local sont appelés hôtes distants. Lorsqu'un périphérique source envoie un paquet à un périphérique de destination distant, alors l'aide des **routeurs** et le **routage** sont nécessaires. Le routage est le processus de détermination du meilleur chemin vers une destination. Le routeur connecté au segment de réseau local est appelé **la passerelle par défaut**.

# Passerelle par défaut

- La **passerelle par défaut** correspond au périphérique réseau capable d'acheminer le trafic vers d'autres réseaux. C'est le **routeur** qui peut acheminer le trafic en dehors du réseau local.
- Une passerelle par défaut :
  - Achemine le trafic vers d'autres réseaux,
  - Possède une interface LAN reliée au même réseau local que les hôtes, et ayant une adresse IP située dans la même plage d'adresses que les hôtes du réseau,
  - Possède au moins une interface (LAN ou WAN) reliée à un autre réseau,
  - Les données échangées entre les hôtes du réseau LAN et les autres réseaux transitent par la passerelle par défaut.

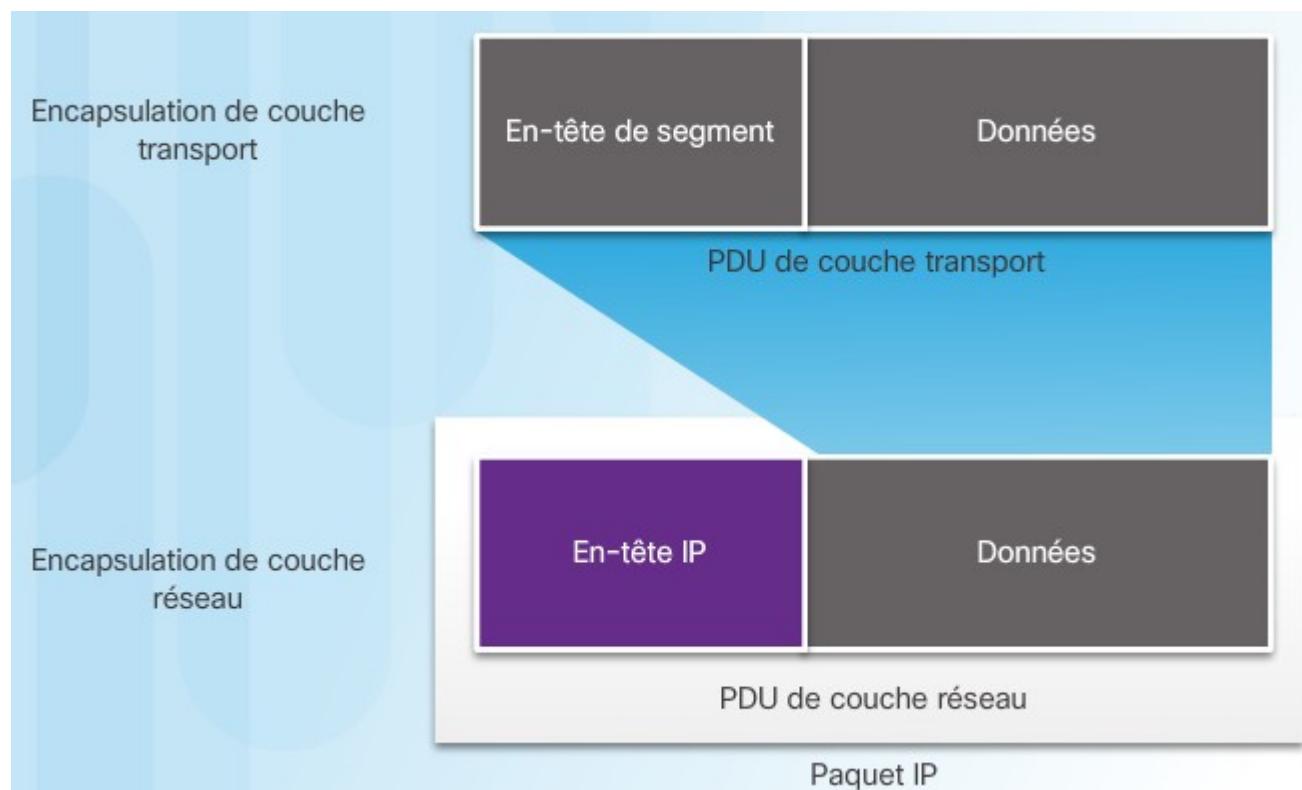


# Caractéristiques du protocole IP

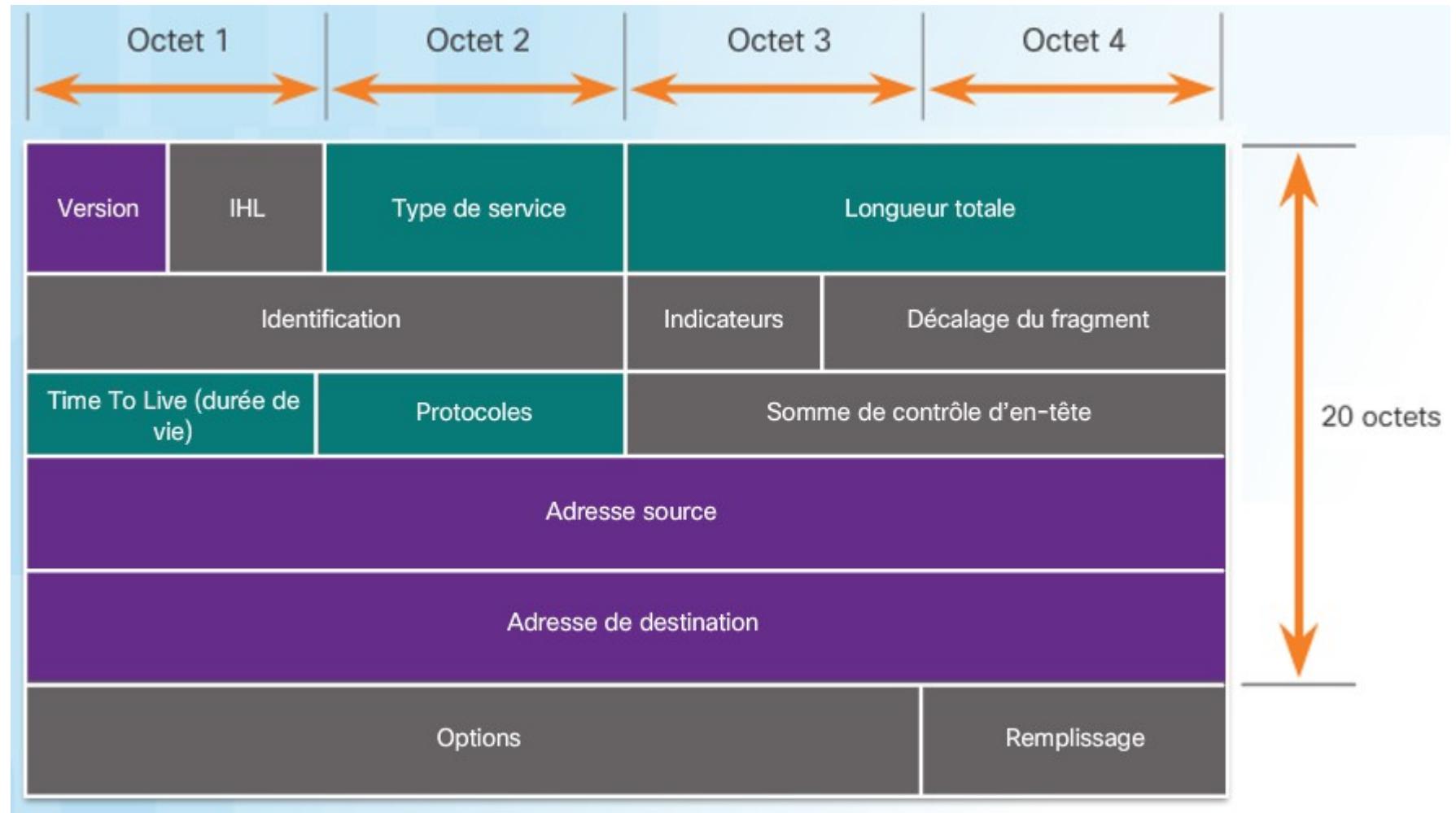
- Le protocole IP a été conçu pour ne pas surcharger les réseaux. Il fournit uniquement les fonctions requises pour transférer un paquet d'une source à une destination en passant par un système interconnecté de réseaux. Ce protocole n'est pas destiné au suivi et à la gestion du flux de paquets. Ces fonctions, si elles sont requises, sont exécutées par d'autres protocoles, sur d'autres couches, principalement TCP sur la couche 4.
- Les principales caractéristiques du protocole IP sont :
  - **Sans connexion** : Aucune connexion avec la destination n'est établie avant l'envoi des paquets de données.
  - **Acheminement au mieux (Best effort)** : IP n'est pas fiable par nature, car la livraison des paquets n'est pas garantie.
  - **Indépendant du support de transmission de données** : Le fonctionnement est indépendant du support (cuivre, fibre optique ou sans fil) qui transporte les données.

# Encapsulation IP

- Le protocole IP encapsule le segment de couche transport ou les données de certains protocoles de couche réseau comme les paquets ICMP en ajoutant un en-tête IP. Cet en-tête fournit les informations permettant d'acheminer le paquet vers l'hôte de destination.
- Les routeurs s'occupent de la fonction de routage en tenant compte uniquement du contenu de l'en-tête de paquet de couche réseau. Dans tous les cas, la partie données du paquet reste inchangée durant les traitements au niveau de la couche réseau.



# Entête de paquet IPv4



# Entête de paquet IPv4

- Les champs importants de l'en-tête IPv4 sont les suivants :
  - **Version** : ce champ contient une valeur binaire de 4 bits définie sur 0100 indiquant qu'il s'agit d'un paquet IP version 4.
  - **Services différenciés ou Type de service** : ce champ de 8 bits est utilisé pour définir la priorité de chaque paquet.
  - **Time To Live (durée de vie, TTL)** : ce champ contient une valeur binaire de 8 bits utilisée pour limiter la durée de vie d'un paquet. L'expéditeur du paquet définit la valeur TTL initiale et celle-ci diminue d'un point chaque fois que le paquet est traité par un routeur. Si la valeur du champ TTL arrive à zéro, le routeur rejette le paquet et envoie un message de dépassement du délai ICMP (Internet Control Message Protocol) à l'adresse IP source.
  - **Protocole** : utilisé pour identifier le protocole de couche supérieure. Cette valeur binaire de 8 bits indique le type de données utiles transportées par le paquet, ce qui permet à la couche réseau de transmettre les données au protocole de couche supérieure approprié. Les valeurs les plus courantes sont notamment ICMP (1), TCP (6) et UDP (17).
  - **Adresse IP source** : ce champ contient une valeur binaire de 32 bits, qui représente l'adresse IP source du paquet. L'adresse IPv4 source est toujours une adresse de monodiffusion.
  - **Adresse IP de destination** : ce champ contient une valeur binaire de 32 bits qui représente l'adresse IP de destination du paquet. L'adresse IPv4 de destination est une adresse de monodiffusion, de diffusion ou de multidiffusion.

# Entête de paquet IPv4

- Les deux champs les plus utilisés sont les **adresses IP source et de destination**. Ces champs indiquent d'où vient le paquet et où il va. Généralement, ces adresses ne changent pas lors du déplacement entre la source et la destination.
- Les champs **Longueur d'en-tête Internet (IHL)**, **Longueur totale** et **Somme de contrôle d'en-tête** permettent d'identifier et de valider le paquet.
- D'autres champs sont utilisés pour remettre dans l'ordre un paquet fragmenté. En particulier, le paquet IPv4 utilise les champs **Identification**, **Indicateurs** et **Décalage du fragment** pour garder la trace des fragments. Un routeur peut être amené à fragmenter un paquet pour le transmettre d'un support à un autre, dont la MTU est inférieure.
- Les champs **Options** et **Remplissage** sont rarement utilisés.

# Limites du protocole IPv4

- Au fil des années, l'IPv4 a été mis à jour afin de relever de nouveaux défis. Cependant, malgré ces modifications, l'IPv4 présente toujours trois problèmes majeurs :
  - **La pénurie d'adresses IP** : l'IPv4 a un nombre limité d'adresses IP publiques disponibles. Bien qu'il existe environ 4 milliards d'adresses IPv4, le nombre croissant de périphériques IP, les connexions permanentes et la croissance potentielle des pays en voie de développement entraînent une hausse du nombre d'adresses devant être disponibles.
  - **La croissance de la table de routage Internet** : une table de routage est utilisée par les routeurs pour déterminer les meilleurs chemins disponibles. Le nombre de routes de réseau augmente parallèlement au nombre de serveurs connectés à Internet. Ces routes IPv4 consomment beaucoup de mémoire et de ressources processeur sur les routeurs Internet.
  - **Le manque de connectivité de bout en bout** : la technologie de traduction d'adresses réseau (NAT) est généralement implémentée dans les réseaux IPv4. Elle permet à plusieurs périphériques de partager une adresse IPv4 publique unique. Cependant, étant donné que l'adresse IPv4 publique est partagée, l'adresse IPv4 d'un hôte interne du réseau est masquée, ce qui peut poser problème pour les technologies nécessitant une connectivité de bout en bout.

# Adresse IP / masque de sous-réseau

- Une adresse IPv4 est une chaîne de 32 bits représentée en décimal sous forme de quatre octets séparés par des points. Elle sert à **identifier de façon unique un hôte, un groupe d'hôtes ou un réseau**.
- Une adresse IPv4 est formée d'**une partie réseau**, située au **poids fort** de l'adresse IP, et d'**une partie hôte**, située au **poids faible** de l'adresse IP.
- Pour identifier les parties réseau et hôte d'une adresse IPv4, chaque bit du masque de sous-réseau est superposé au bit correspondant de l'adresse IPv4. Les "**1**" dans le **masque de sous-réseau** indiquent la **partie réseau de l'adresse IP**, et les "**0**" indiquent la **partie hôte**.



# Adresse IP / masque de sous-réseau

- Dans sa représentation en binaire, **les "1"** du masque de sous réseau sont toujours placés à gauche, et **les "0"** à droite du masque.
- Lorsqu'une adresse IPv4 est attribuée à un périphérique, **le masque de sous-réseau est utilisé pour déterminer l'adresse du réseau auquel le périphérique appartient**. Celle-ci est déterminée en effectuant une **opération ET logique bit par bit entre l'adresse IP et le masque de sous-réseau correspondant**.

Adresse de l'hôte	10	209	22	175
Masque de sous-réseau	255	255	255	252
Adresse de l'hôte en notation binaire	00001010	11010001	00010110	10101111
Masque de sous-réseau (format binaire)	11111111	11111111	11111111	11111100
Adresse réseau en notation binaire				
Adresse du réseau (format décimal)				

# Longueur de préfixe

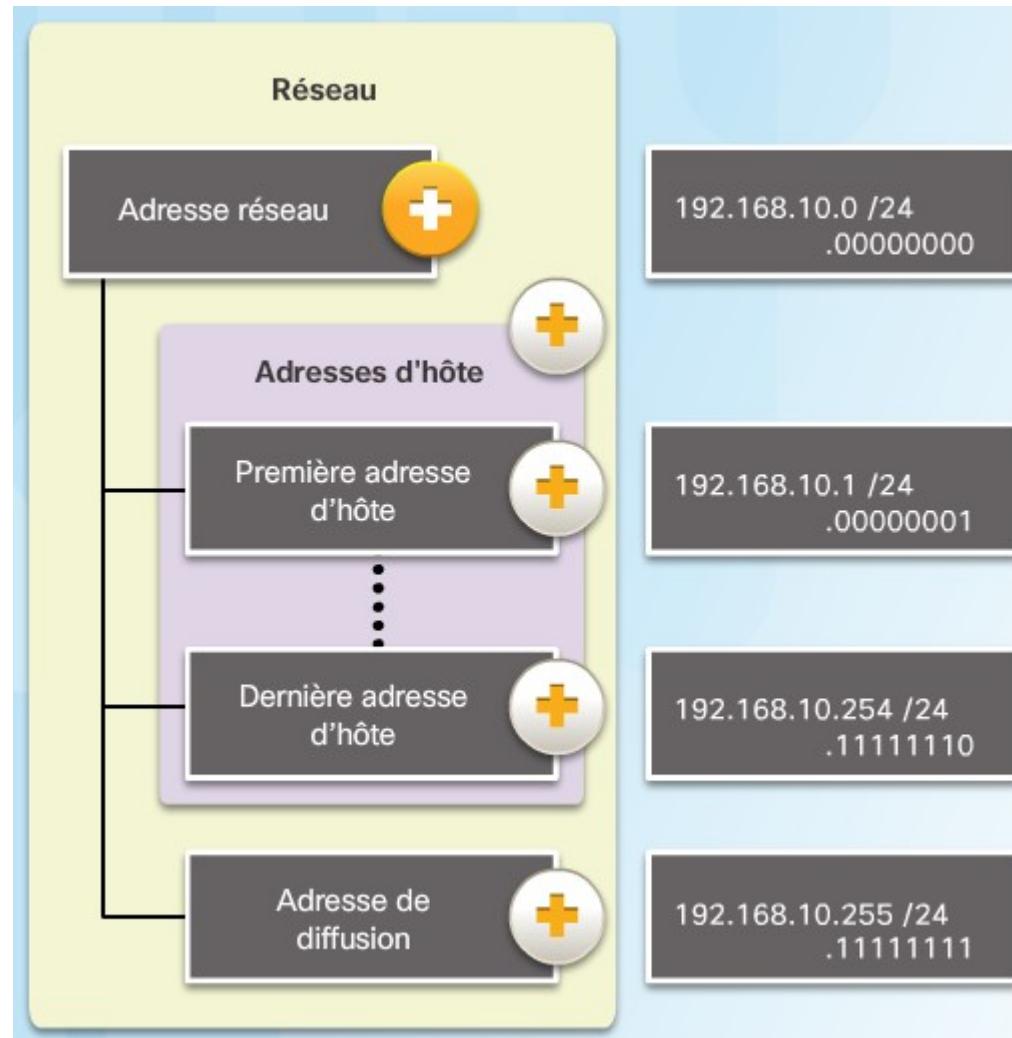
- Il peut devenir **fastidieux d'exprimer** les adresses réseau et les adresses d'hôtes avec **le masque de sous-réseau au format décimal à point**. Heureusement, il existe une méthode plus rapide d'identification du masque de sous-réseau, appelée la longueur de préfixe.
- La longueur de préfixe correspond au **nombre de bits à 1 dans le masque de sous-réseau**. Elle est notée au moyen de la « notation de barre oblique / » suivi du nombre de bits à 1 dans le masque de sous-réseau. Il suffit donc de **compter ce nombre de bits à 1 et de le faire précéder d'une barre oblique**.

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

# Adresses réseau, hôte et de diffusion

- **Adresse du réseau** : elle peut être obtenue en mettant à "0" tous les bits de sa partie hôte. L'adresse du réseau et son masque de sous-réseau définissent le réseau concerné. Tous les hôtes du réseau partagent la même adresse réseau. L'adresse réseau correspond à la plus petite adresse de la plage d'adresses du réseau correspondant.
- **Adresse de diffusion** : elle peut être obtenue en mettant à "1" tous les bits de sa partie hôte. C'est une adresse qui permet de communiquer avec tous les hôtes du réseau auquel elle appartient. L'adresse de diffusion correspond à la plus grande adresse de la plage d'adresses d'un réseau.
- **Adresse hôte** : Adresses IP uniques attribuées à des hôtes et des périphériques. La partie hôte contient toujours à la fois des 0 et des 1, mais jamais uniquement des 0 ni uniquement des 1.
  - **Première adresse IP d'hôte du réseau** : C'est l'adresse qui vient juste après l'adresse du réseau. Elle peut être obtenue en ajoutant "1" à l'adresse du réseau.
  - **Dernière adresse IP d'hôte du réseau** : C'est l'adresse qui vient juste avant l'adresse de diffusion du réseau. Elle peut être obtenue en retranchant "1" à l'adresse de diffusion.

# Adresses réseau, hôte et de diffusion



# Nombre d'hôtes d'un réseau

- Le nombre d'hôtes dans un réseau est défini par le masque de sous-réseau associé à ce réseau. En effet, ce masque permet de déterminer le nombre de bits réservés au hôtes, et donc le nombre de combinaisons possibles qu'on peut obtenir avec ces bits.
- Étant donné que la première adresse du réseau (adresse IP réseau), et la dernière adresse du réseau (adresse IP de diffusion) ne peuvent pas être affectées aux hôtes, le nombre d'hôtes possible pour un réseau donné est calculé à l'aide de la formule mathématique suivante :

**Nombre maximal d'hôtes =  $2^N - 2$**  où N est le nombre de bits hôtes

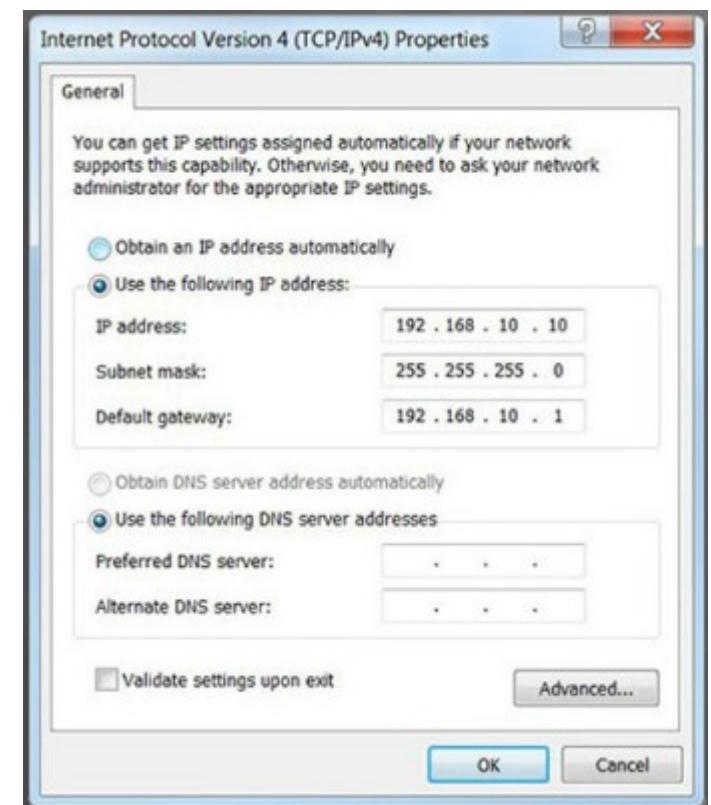
- Pour rappel, le nombre de bits hôtes n'est autre que le nombre de zéros dans le masque de sous réseau associé au réseau concerné.
- **Exemple :**

Dans le réseau **192.168.1.0 /24**, le masque de sous réseau contient **24 bits à « 1 » et 8 bits à « 0 »**. Le nombre de bits hôtes est donc égal à 8, ce qui nous permet d'en conclure que le nombre maximal d'hôtes que peut supporter ce réseau est **254 hôtes ( $2^8-2$ )**.

- L'adresse du réseau sera donc **192.168.1.0**
- L'adresse de diffusion est égale à **192.168.1.255**
- Les adresses hôtes possibles vont de **192.168.1.1** à **192.168.1.254**, soit **254 adresses IP**.

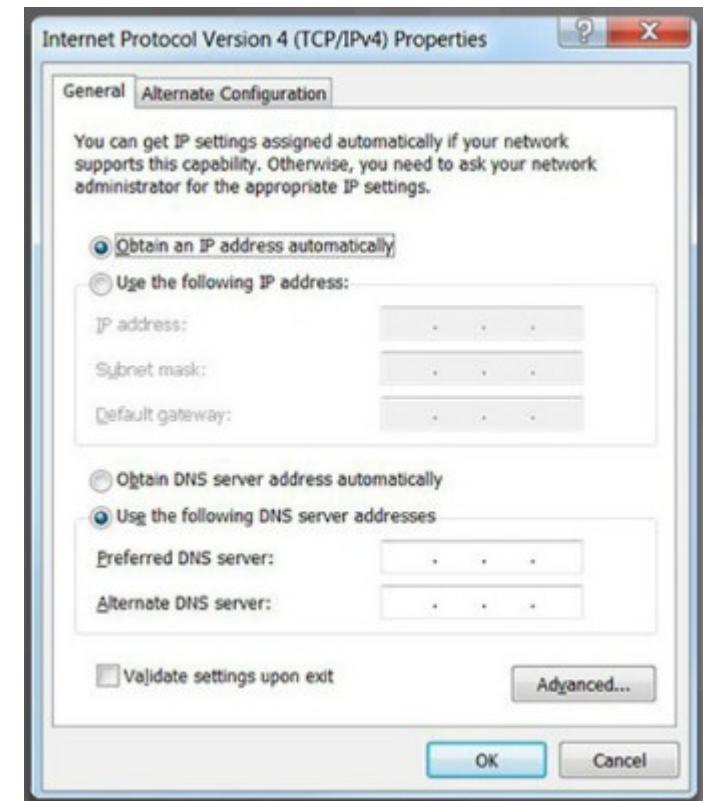
# Attribution d'une adresse IPv4 statique à un hôte

- Les **adresses IP** peuvent être **attribuées** aux périphériques de manière **statique** ou **dynamique**.
- Sur les réseaux, **certains périphériques doivent avoir une adresse IP fixe**. Par exemple, les **imprimantes, serveurs et périphériques réseau** comme les routeurs, les commutateurs et les points d'accès, **doivent conserver la même adresse IP**. De ce fait, une adresse IP statique leur est généralement attribuée.
- Il est également possible d'attribuer une adresse IPv4 statique à un hôte, comme l'illustre la figure ci-dessous. **L'attribution d'adresses IP statiques aux hôtes est une pratique acceptable dans les petits réseaux**. Toutefois, il serait fastidieux de saisir des adresses statiques sur chaque hôte d'un grand réseau. **Il est important de tenir à jour une liste exacte des adresses IP statiques attribuées à chaque périphérique**.



# Attribution d'une adresse IPv4 dynamique à un hôte

- Dans la plupart des réseaux de données, les hôtes sont principalement des ordinateurs, des tablettes, des smartphones, des imprimantes et des téléphones IP. Bien souvent, les utilisateurs et leurs périphériques changent fréquemment. Il serait donc impossible d'attribuer des adresses IPv4 statiques à chaque périphérique. C'est pourquoi on leur **attribue des adresses IPv4 de manière dynamique à l'aide du protocole DHCP** (Dynamic Host Configuration Protocol).
- Un hôte peut obtenir automatiquement des informations d'adressage IPv4. L'hôte est un **client DHCP** qui demande des informations d'adresse IPv4 à un serveur DHCP.
- Le serveur DHCP lui fournit une **adresse IPv4**, un **masque de sous-réseau**, une **passerelle par défaut**, l'adresse du **serveur DNS** et **d'autres informations de configuration**. Sur les grands réseaux, la méthode DHCP est généralement privilégiée pour l'attribution des adresses IPv4. L'autre avantage de cette méthode réside dans le fait que **les adresses ne sont pas attribuées aux hôtes de manière permanente**, elles sont uniquement « louées » pour une certaine durée. Cela est particulièrement intéressant pour les utilisateurs mobiles qui se connectent et se déconnectent d'un réseau.



# Configuration IP des hôtes

- La configuration IP d'un hôte, fournie par un serveur DHCP ou configurée statiquement doit contenir les informations suivants :
  - **Adresse IP** : cette adresse doit être unique dans le réseau où est localisé l'hôte pour éviter des conflits d'adresse.
  - **Le masque de sous-réseau** : ce masque, combiné avec l'adresse IP, permet à l'hôte de déterminer l'adresse du IP du réseau auquel il appartient.
  - **L'adresse IP de la passerelle par défaut** : C'est l'adresse IP du nœud qui permet à l'hôte d'envoyer des messages vers l'extérieur de son réseau. Ce nœud est généralement un routeur. **Si ce paramètre n'est pas configuré dans l'hôte, il pourra communiquer avec les hôtes de son propre réseau local, mais pas avec ceux situés à l'extérieur.**
  - **L'adresse IP du serveur DNS** : C'est l'adresse IP à laquelle l'hôte doit envoyer les requêtes DNS lui permettant de récupérer les adresses IP correspondantes aux noms de domaines qu'il essaye de joindre. **Si cette adresse n'est pas fournie à l'hôte, il pourra naviguer sur Internet en utilisant les adresses IP des serveurs qu'il désire joindre, mais pas en utilisant leurs noms de domaines.**

# Classes d'adresses IPv4

- En 1981, les adresses IPv4 Internet étaient attribuées à l'aide de l'adressage par classe. Le RFC 790 a divisé les plages monodiffusion en classes spécifiques, respectivement appelées :
  - **Classe A (0.0.0.0 à 127.255.255.255)** : créée pour prendre en charge les réseaux de très grande taille, comportant jusqu'à **16 777 214 d'adresses d'hôte**. Elle utilisait un **préfixe /8** par défaut. Toutes les adresses de classe A nécessitaient que le bit de poids fort du premier octet soit un zéro.
  - **Classe B (128.0.0.0 à 191.255.255.255)** : créée pour répondre aux besoins des réseaux de taille moyenne ou de grande taille comportant jusqu'à **65 534 adresses d'hôtes**. Elle utilisait un **préfixe /16** par défaut. Les deux bits de poids fort de l'octet de poids fort doivent être "10".
  - **Classe C (192.0.0.0 à 223.255.255.255)** : créée pour répondre aux besoins des réseaux de petite taille comportant **254 hôtes maximum**. Elle utilisait un **préfixe /24** par défaut. Les trois bits de poids fort de l'octet de poids fort doivent être "110".
  - **Classe D (224.0.0.0 à 239.255.255.255)** : créée pour prendre en charge le trafic multidiffusion. Les quatre bits de poids fort de l'octet de poids fort doivent être "1110".
  - **Classe E (240.0.0.0 à 255.255.255.254)** : réservée pour des utilisations expérimentales. Les quatre bits de poids fort de l'octet de poids fort doivent être "1111".

# Classes pour l'adressage des hôtes

Spécifications de la classe A	
Bloc d'adresses	0.0.0.0 à 127.255.255.255
Masque de sous-réseau par défaut	/8 (255.0.0.0)
Nombre maximal de réseaux	128
Nombre d'hôtes par réseau	16 777 214
Bit d'ordre haut	0xxxxxx.-----.

Spécifications de la classe B	
Bloc d'adresses	128.0.0.0 à 191.255.255.255
Masque de sous-réseau par défaut	/16 (255.255.0.0)
Nombre maximal de réseaux	16 384
Nombre d'hôtes par réseau	65 534
Bit d'ordre haut	10xxxxxx.-----.

Spécifications de la classe C	
Bloc d'adresses	192.0.0.0 à 223.255.255.255
Masque de sous-réseau par défaut	/24 (255.255.255.0)
Nombre maximal de réseaux	2 097 152
Nombre d'hôtes par réseau	254
Bit d'ordre haut	110xxxxx.-----.

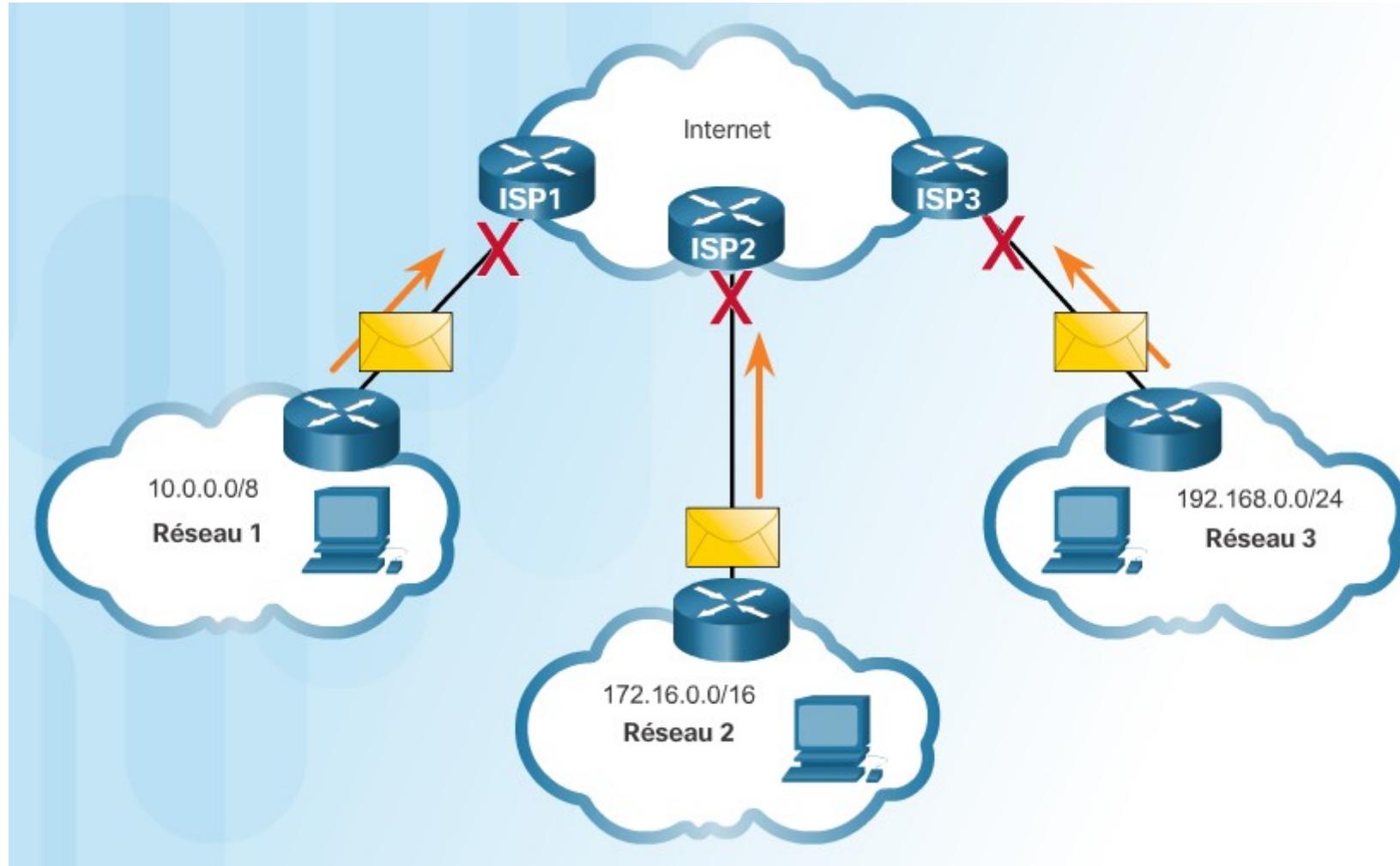
# Adresses IPv4 particulières

- Certaines adresses, telles que l'adresse réseau et l'adresse de diffusion ne peuvent pas être attribuées à des hôtes. Il existe également des adresses spéciales qui peuvent être attribuées aux hôtes, mais des restrictions s'appliquent sur les interactions de ces hôtes sur le réseau.
- **Adresses 0.0.0/8 (ou 0.0.0.0 à 0.255.255.255)** : ces adresses ne peuvent pas être affectées à des hôtes. L'adresse 0.0.0.0 peut par exemple être utilisée par un client DHCP qui cherche à acquérir une configuration IP depuis un serveur DHCP.
- **Adresses de bouclage (127.0.0.0 /8 ou 127.0.0.1 à 127.255.255.254)** : ces adresses spéciales sont **utilisées par des hôtes pour diriger le trafic vers eux-mêmes**. Par exemple, elles peuvent être utilisées sur un hôte pour vérifier si la configuration TCP/IP est opérationnelle.
- **Adresses lien-local (169.254.0.0 /16 ou 169.254.0.1 à 169.254.255.254)** : plus connues sous le nom d'adresses **APIPA** (Automatic Private Internet Protocol Addressing), elles sont utilisées par un client DHCP pour se configurer automatiquement si **aucun serveur DHCP n'est disponible**.
- **Adresses TEST-NET (192.0.2.0/24 ou 192.0.2.0 à 192.0.2.255)** : ces adresses sont réservées à des **fins pédagogiques** et utilisées dans la documentation et dans des exemples de réseau.

# Adresses IPv4 publiques et privées

- Les adresses IPv4 privées ont été créées au milieu des années 1990 en raison de la **pénurie d'espace d'adresses IPv4**.
- Contrairement aux adresses IP publiques, elles **ne sont pas routables sur Internet**. Elles **peuvent donc être réutilisées dans plusieurs réseau internes** connectés à Internet sans causer de conflits d'adresses.
- Pour permettre aux hôtes de ces réseaux d'accéder à Internet, une **traduction d'adresses IP privées en adresses IP publiques** doit être effectuée. Cette traduction est effectuée par le processus **NAT** (Network Address Translation) généralement **implémenté dans les routeurs** reliant les réseaux LAN à Internet.
- Les routeurs domestiques assurent cette fonction **NAT**. Par exemple, la plupart des routeurs domestiques attribuent des adresses IPv4 à leurs hôtes filaires et sans fil à partir de l'adresse privée 192.168.1.0 /24. L'interface WAN du routeur domestique utilise une adresse IP publique. C'est vers cette adresse que toutes les adresses privées seront traduites.
- Les blocs d'adresses privées sont les suivants :
  - **10.0.0.0 à 10.255.255.255** (10.0.0.0 /8)
  - **172.16.0.0 à 172.31.255.255** (172.16.0.0 /12)
  - **192.168.0.0 à 192.168.255.255** (192.168.0.0 /16)

# Adresses IPv4 publiques et privées



# Commandes liées à la couche réseau

- Sous Windows, les commandes suivantes peuvent être utilisées pour tester la communication au niveau de la couche réseau :

- **Ping** : prend comme argument une adresse IP ou un nom de domaine. Elle permet de tester la connectivité vers un hôte distant.

```
C:\>ping www.google.com

Pinging www.l.google.com [74.125.224.17] with 32 bytes of data:
Reply from 74.125.224.17: bytes=32 time=14ms TTL=52
Reply from 74.125.224.17: bytes=32 time=23ms TTL=52
Reply from 74.125.224.17: bytes=32 time=13ms TTL=52
Reply from 74.125.224.17: bytes=32 time=18ms TTL=52

Ping statistics for 74.125.224.17:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 23ms, Average = 17ms
```

- **Tracert** : prend comme argument une adresse IP ou un nom de domaine. Elle permet d'afficher le chemin parcouru par les paquet pour atteindre un hôte distant. Elle renvoi les adresses IP de tous les routeurs intermédiaire séparant les hôtes source et destination.

```
C:\Documents and Settings\qa>tracert www.forio.com

Tracing route to www.forio.com [98.129.39.212]
over a maximum of 30 hops:

 1      5 ms     <1 ms     <1 ms  gate.foriodev.com [192.168.3.1]
 2     14 ms     48 ms      4 ms   10.0.0.9
 3     28 ms      8 ms      3 ms   68.80.208.web-pass.com [208.80.68.193]
 4     39 ms     11 ms      4 ms  ge-11-3-4.mpr3.sfo7.us.above.net [64.125.199.37]

 5     45 ms      5 ms      7 ms  xe-1-3-0.er1.sjc2.us.above.net [64.125.26.58]
 6      5 ms      4 ms      7 ms  64.125.28.18.available.above.net [64.125.28.18]

 7     44 ms     14 ms     13 ms  xe-2-1-0.cr1.lax112.us.above.net [64.125.24.17]

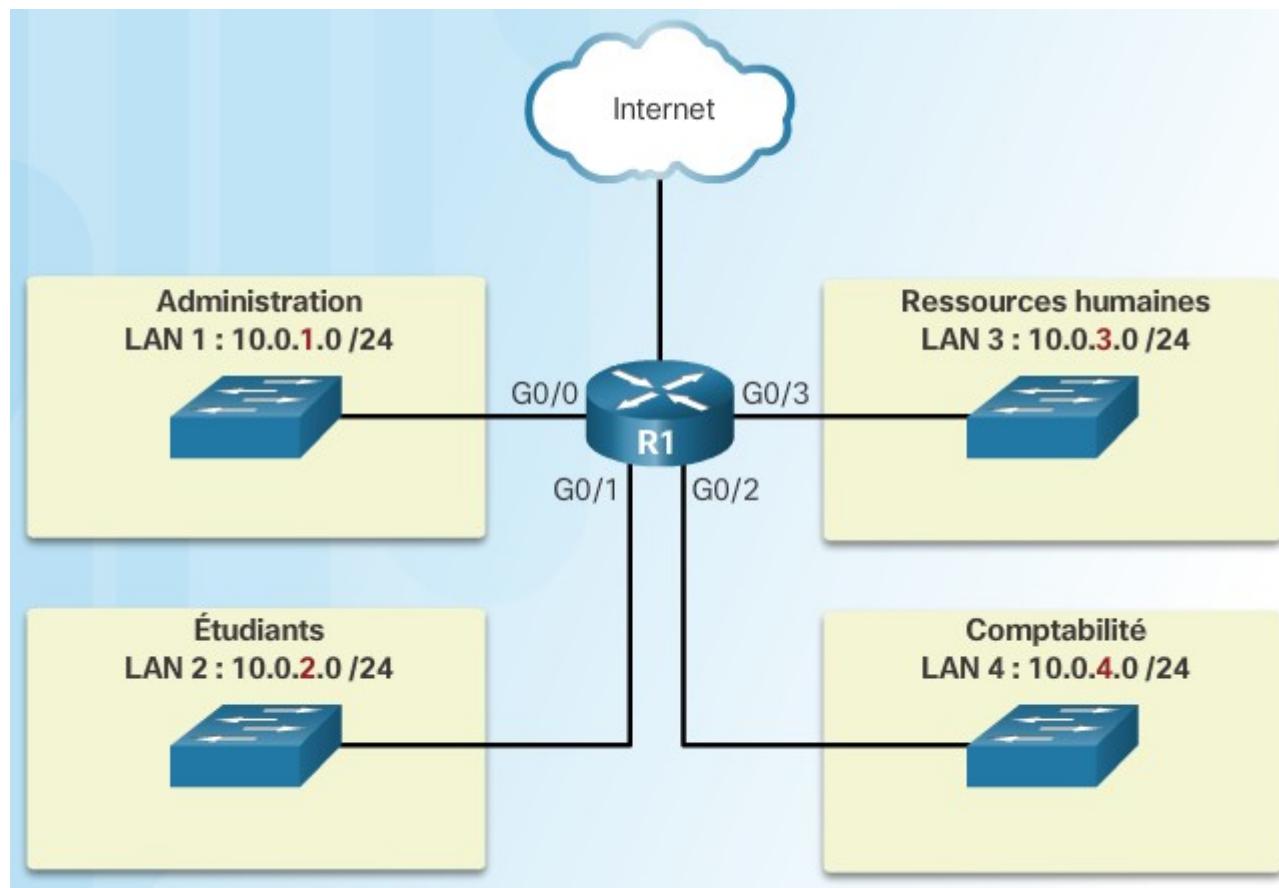
 8     53 ms     66 ms     45 ms  xe-2-0-0.cr1.iah1.us.above.net [64.125.25.46]
 9     72 ms     75 ms     70 ms  xe-2-1-0.cr1.dfw2.us.above.net [64.125.30.58]
10     51 ms     89 ms     49 ms  xe-0-1-0.er1.dfw2.us.above.net [64.125.27.74]
11     52 ms     51 ms     56 ms  main1.above.net [209.133.126.42]
12     53 ms     80 ms     51 ms  vlan905.core5.dfw1.rackspace.com [67.192.56.229]

13     55 ms     87 ms     53 ms  67.192.56.43
14     53 ms     60 ms     51 ms  98.129.39.212

Trace complete.
```

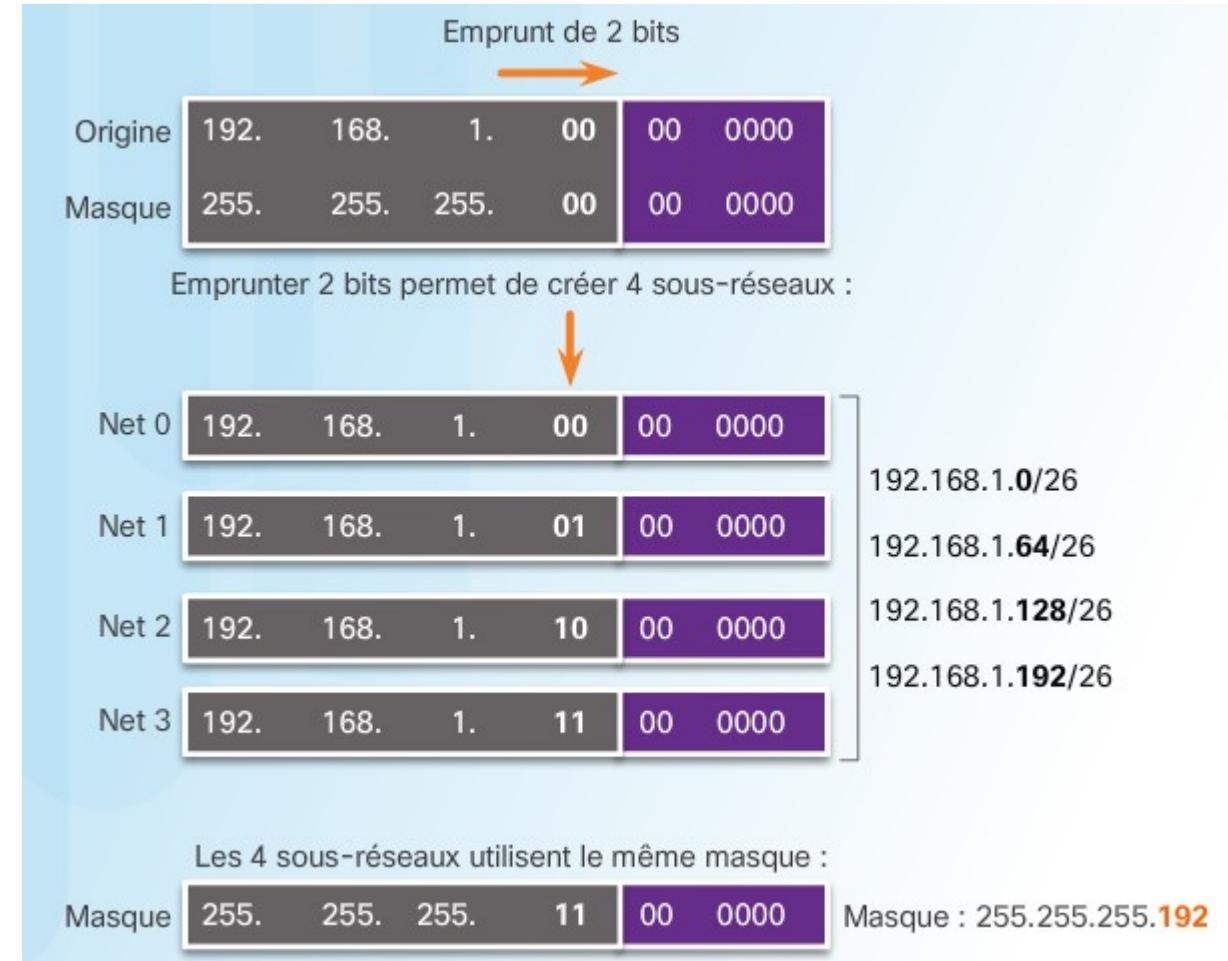
# Segmentation de réseaux

- La segmentation en sous-réseaux réduit le trafic global et améliore les performances réseau. Elle permet également aux administrateurs de mettre en œuvre des politiques de sécurité, notamment pour définir si les différents sous-réseaux sont autorisés ou non à communiquer entre eux.



# Technique de Segmentation

- Pour créer des sous-réseaux IPv4, on utilise un ou plusieurs bits d'hôte en tant que bits réseau. Pour cela, il faut étendre le masque de sous-réseau en empruntant quelques bits de la partie hôte de l'adresse et les affecter à la partie réseau. Plus les bits d'hôte empruntés sont nombreux, plus le nombre de sous-réseaux qui peuvent être définis est important.
- L'exemple ci-contre montre la technique de découpage du réseau 192.168.1.0/24 en 4 sous-réseaux. Pour cela, les deux bits les plus à gauche de la partie hôte sont empruntés. Le masque de sous-réseau des sous-réseaux obtenus devient donc /26.



# Nombre de bits à emprunter

- Pour déterminer le nombre N de bits hôtes à emprunter, il suffit d'utiliser la formule suivante :

$$\text{Nombre de sous-réseaux} = 2^N$$

- **Exemple :**
  - Pour obtenir 2 sous-réseaux, N doit être égale à 1. Un seul bit va donc être emprunté.
  - Pour obtenir 4 sous-réseaux, N doit être égale à 2. Deux bits vont donc être empruntés.
  - Pour obtenir 8 sous-réseaux, N doit être égale à 3. Trois bits vont donc être empruntés.
  - Pour obtenir 16 sous-réseaux, N doit être égale à 4. Quatre bits vont donc être empruntés.
  - Pour obtenir 32 sous-réseaux, N doit être égale à 5. Cinq bits vont donc être empruntés.
  - Pour obtenir 64 sous-réseaux, N doit être égale à 6. Six bits vont donc être empruntés.
  - ...

# Le nouveau masque de sous-réseaux

- La calcul du nouveau masque de sous-réseau obtenu après segmentation se fait en additionnant le nombre de bits empruntés, au masque du réseau ayant été découpé.
- **Exemples :**
  - Si le réseau à découper possède un masque de sous-réseau égal à **/24**, et que **3 bits** ont été empruntés pour le segmenter, alors le masque de sous-réseau des sous-réseaux obtenus sera égal à **/27** ( $27 = 24 + 3$ ).
  - Si le réseau à découper possède un masque de sous-réseau égal à **/16**, et que **5 bits** ont été empruntés pour le segmenter, alors le masque de sous-réseau des sous-réseaux obtenus sera égal à **/21** ( $21 = 16 + 5$ ).
  - Si le réseau à découper possède un masque de sous-réseau égal à **/10**, et que **1 bits** a été emprunté pour le segmenter, alors le masque de sous-réseau des sous-réseaux obtenus sera égal à **/11** ( $11 = 10 + 1$ ).

# Nombre d'hôtes par sous-réseaux

- Le nombre maximal d'hôtes par sous-réseau, obtenu après segmentation, est calculé de la même manière que pour n'importe quel réseau. Pour le calculer, il suffit de déterminer le nombre n de bits hôtes, en utilisant le nouveau masque de sous-réseau, et d'utiliser la formule déjà vue précédemment :

$$\text{Nombre maximal d'hôtes} = 2^n - 2$$

- **Exemples :**

- Si le nouveau masque de sous-réseau obtenu après segmentation est égal à /29, alors le nombre n de bits hôtes est égal à 3 ( $3 = 32 - 29$ ), ce qui donne un nombre maximal d'hôtes par sous-réseau égal à 6 ( $6 = 2^3 - 2$ ).
- Si le nouveau masque de sous-réseau obtenu après segmentation est égal à /25, alors le nombre n de bits hôtes est égal à 7 ( $7 = 32 - 25$ ), ce qui donne un nombre maximal d'hôtes par sous-réseau égal à 126 ( $126 = 2^7 - 2$ ).
- Si le nouveau masque de sous-réseau obtenu après segmentation est égal à /22, alors le nombre n de bits hôtes est égal à 10 ( $10 = 32 - 22$ ), ce qui donne un nombre maximal d'hôtes par sous-réseau égal à 1022 ( $1022 = 2^{10} - 2$ ).

# Processus de routage d'un paquet

- A partir de l'adresse IP de destination contenue dans l'entête d'un paquet IP reçu, le routeur essaye de déterminer le réseau de destination en effectuant un **ET Logique** entre cette adresse et les masques de sous réseau de chacune des adresses réseau contenues dans sa table de routage.
  - Si le résultat obtenu correspondant à l'une des adresses réseau connues par le routeur, celui ci utilise la route correspondante pour délivrer le paquet.
  - Si le résultat obtenu ne correspond à aucune adresse, le paquet est détruit, et un message d'erreur ICMP est envoyé vers la source.
- **Exemple :**

Un routeur reçoit un paquet dont l'adresse IP de destination est **212.217.1.130**. Le contenu de sa table de routage est décrit ci-dessous.

S (route statique)	212.217.1.64/26	joignable à travers 212.217.2.193
C (réseau connecté)	<b>212.217.1.128 /27</b>	est directement connecté à <b>FastEthernet0/0</b>
C (réseau connecté)	212.217.2.192/30	est directement connecté à Serial0/0

- L'interface de sortie sera donc Fastethernet0/0 parce que l'opération ET logique entre l'adresse IP 212.217.1.130 et le masque de sous réseau /27 de la 2ème ligne de la table de routage donne bien l'adresse réseau de cette même ligne.

# Routage statique

- Dans le routage statique, l'administrateur configure les routeurs un à un au sein du réseau afin d'y saisir les routes à emprunter pour aller vers les différents réseaux de la topologie.
- Le routage statique présente plusieurs avantages :
  - Économie de bande passante.
  - Sécurité.
  - Connaissance du chemin à l'avance.
- Le routage statique présente plusieurs inconvénients :
  - La configuration de réseaux de taille importante peut devenir assez longue et complexe.
  - A chaque fois que le réseau évolue, il faut que chaque routeur soit au courant de l'évolution par une mise à jour manuelle de la part de l'administrateur qui doit modifier les routes selon l'évolution.

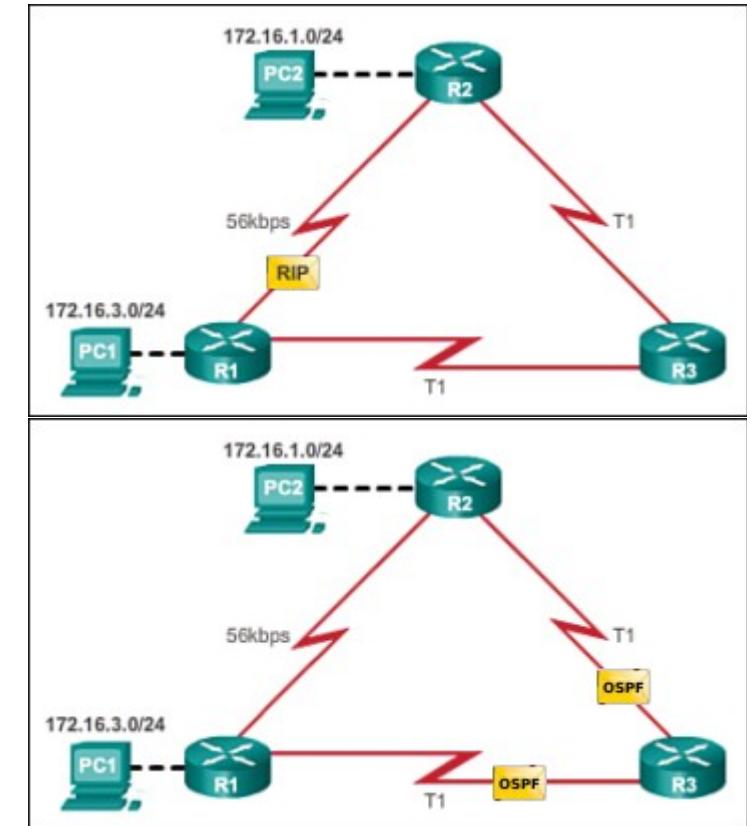
# Routage dynamique

- Les routeurs d'une même topologie peuvent utiliser un protocole de routage dynamique pour échanger entre eux des mises à jour de routage contenant des informations sur les **meilleurs chemins** menant vers les différents réseaux de la topologie. Chaque protocoles de routage utilise une **métrique** qui lui est propre pour déterminer ces meilleurs chemins. La métrique de routage est une mesure permettant le calcul du coût d'un chemin. Plus la métrique d'un chemin est faible meilleur sera ce chemin.

## Exemple:

La métrique du **protocole de routage RIP** est le **nombre de sauts** (nombre de routeurs à traverser pour atteindre la destination). Moins le chemin contiendra de routeurs, meilleurs il sera considéré. Dans l'exemple ci-dessous, le paquet envoyé de PC1 à PC2 va passer par R1 et R2.

La métrique du **protocole de routage OSPF** utilise la bande passante des liaisons pour calculer le coût des chemins. Plus élevée sera la bande passante d'un chemin, meilleurs il sera considéré. Dans l'exemple ci-dessous, le paquet envoyé de PC1 à PC2 va passer par R1, R3 puis R2.

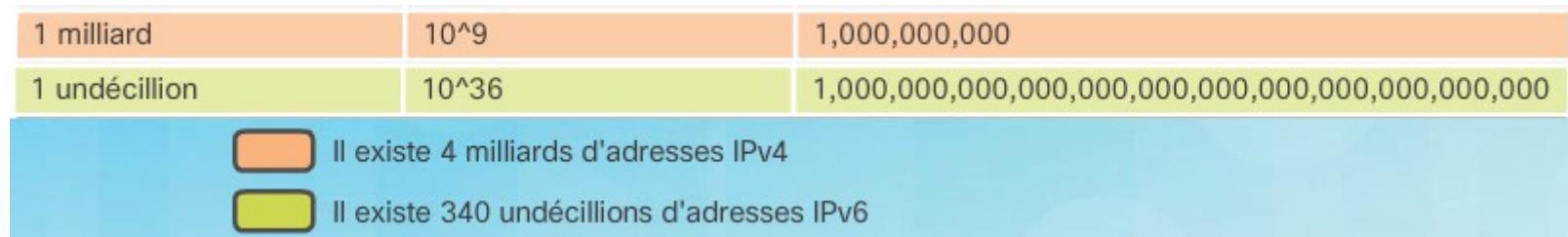


# Routage dynamique

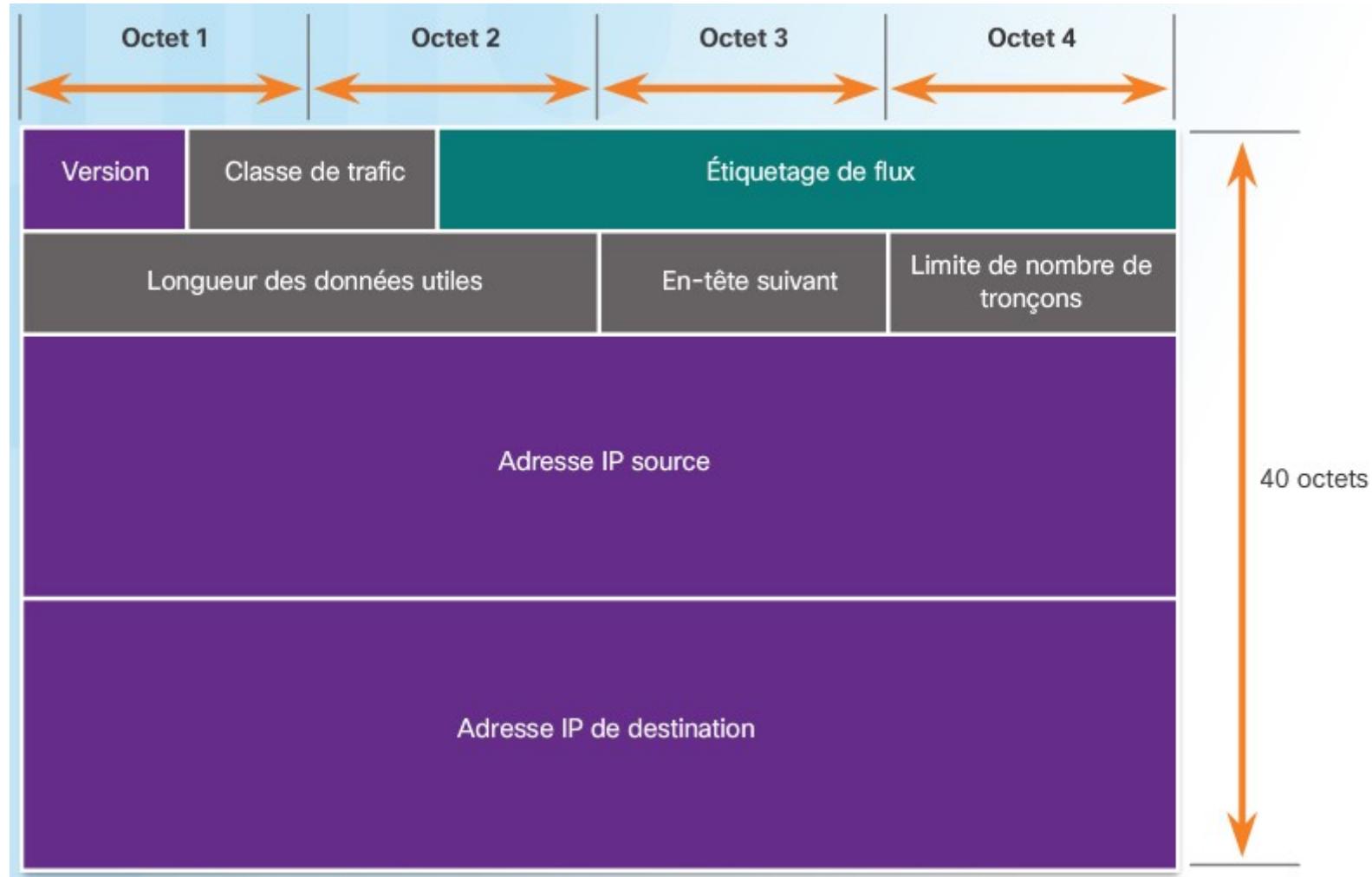
- **Avantages du routage dynamique :**
  - Facilite la tache de l'administrateur en réduisant ses interventions de configuration et de maintenance.
  - S'adapte automatiquement aux changements des topologies des réseaux.
  - Facilite l'évolutivité des réseaux.
- **Inconvénients du routage dynamique :**
  - Peut nécessiter un savoir faire pointu.
  - Il consomme de la bande passante lorsque les mises à jour de routage sont échangée entre les routeurs sur le réseau.
  - La diffusion automatique de message sur le réseau peut constituer un problème de sécurité car un attaquant peut obtenir des informations sur la topologie du réseau simplement en écoutant et en lisant ces messages d'information du protocole de routage et même en créer afin de se faire passer pour un membre du réseau.
  - Le traitement des messages réseau et le calcul des meilleures routes à emprunter représentent une consommation de CPU et de RAM supplémentaire qui peut encombrer certains éléments du réseau peu robuste.

# Protocole IPv6

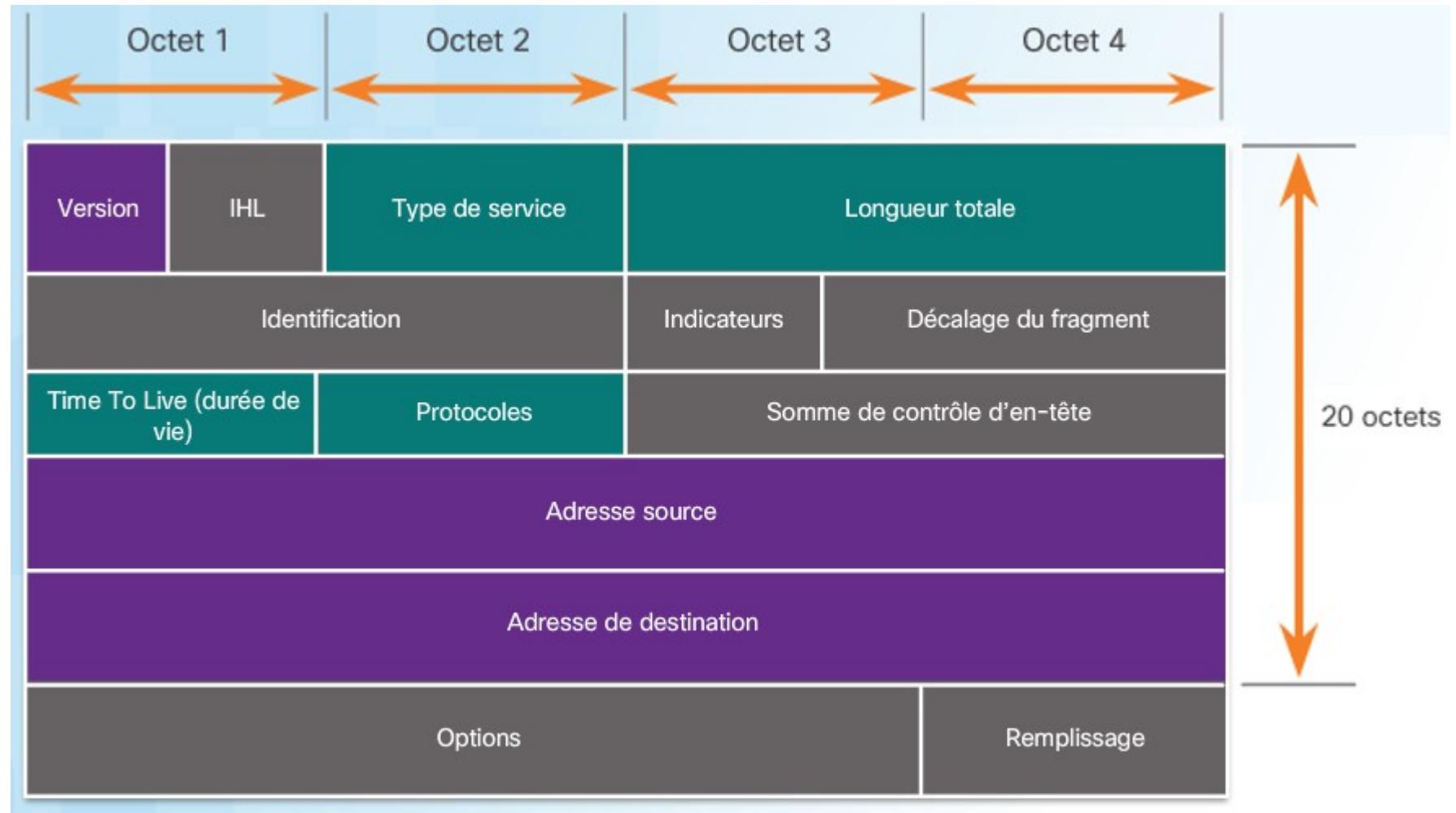
- Le protocole IPv6 supprime les limites de l'IPv4 et améliore le protocole de façon efficace, grâce à des fonctionnalités qui correspondent mieux aux exigences actuelles et futures des réseaux. Parmis ces améliorations on trouve :
- Espace d'adressage plus important : les adresses IPv6 sont représentées sur 128 bits (au lieu de 32 bits pour l'IPv4). Le nombre d'adresses IPv6 possible est plus de 340 undécillions ( $3.4 \times 10^8$ ), ce qui correspond à peu près au nombre de grains de sable sur Terre.
- Traitement plus efficace des paquets : l'en-tête IPv6 a été simplifié et comporte moins de champs.
- Traduction d'adresses réseau NAT inutile : grâce au grand nombre d'adresses publiques IPv6, la technologie NAT n'est plus nécessaire entre une adresse privée et publique. Cela évite certains des problèmes rencontrés par les applications nécessitant une connectivité de bout en bout.



# Entête de paquet IPv6



# Entête de paquet IPv4



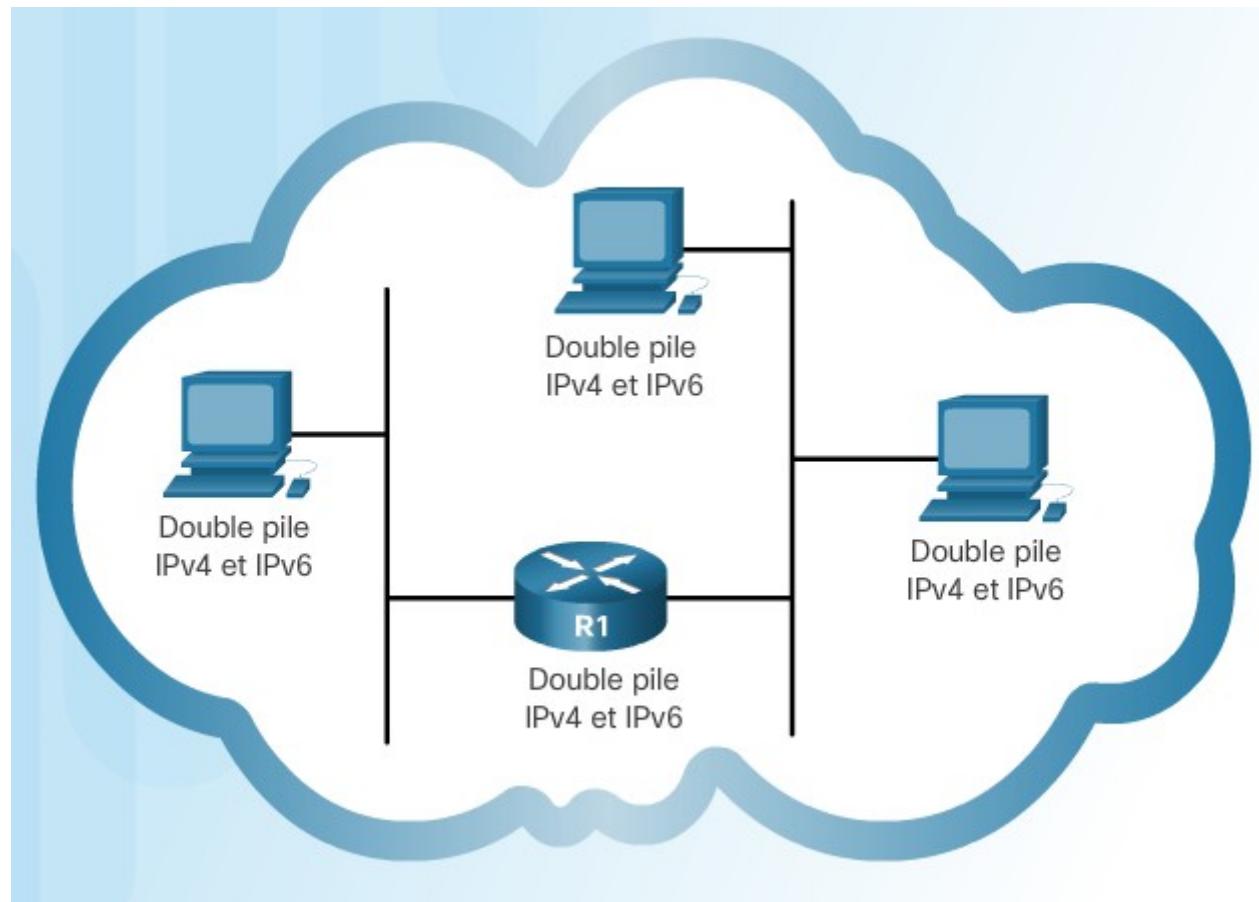
# Détails de l'en-tête de paquet IPv6

- Les champs d'en-tête de paquet IPv6 sont les suivants :
  - **Version** : ce champ contient une valeur binaire de 4 bits définie sur 0110 indiquant qu'il s'agit d'un paquet IP version 6.
  - **Classe de trafic** : ce champ de 8 bits est l'équivalent du champ de services différenciés pour l'IPv4.
  - **Étiquetage de flux** : ce champ de 20 bits indique que tous les paquets portant la même étiquette de flux doivent être traités de la même manière par les routeurs.
  - **Longueur des données utiles** : ce champ de 16 bits indique la longueur de la partie données (utiles) du paquet IPv6.
  - **En-tête suivant** : ce champ de 8 bits est l'équivalent du champ de protocole de l'IPv4. Il indique le type de données utiles transportées par le paquet, permettant ainsi à la couche réseau de transmettre les données au protocole de couche supérieure approprié.
  - **Limite du nombre de tronçons** : ce champ de 8 bits remplace le champ de durée de vie (TTL) de l'IPv4. Cette valeur est réduite d'un point chaque fois qu'un routeur transmet le paquet. Lorsque le compteur atteint 0, le paquet est rejeté et un message ICMPv6 de délai dépassé est transféré à l'hôte émetteur, indiquant que le paquet n'a pas atteint sa destination en raison du dépassement du nombre limite de tronçons.
  - **Adresse IPv6 source** : ce champ de 128 bits identifie l'adresse IPv6 de l'hôte émetteur.
  - **Adresse IPv6 de destination** : ce champ de 128 bits identifie l'adresse IPv6 de l'hôte destinataire.

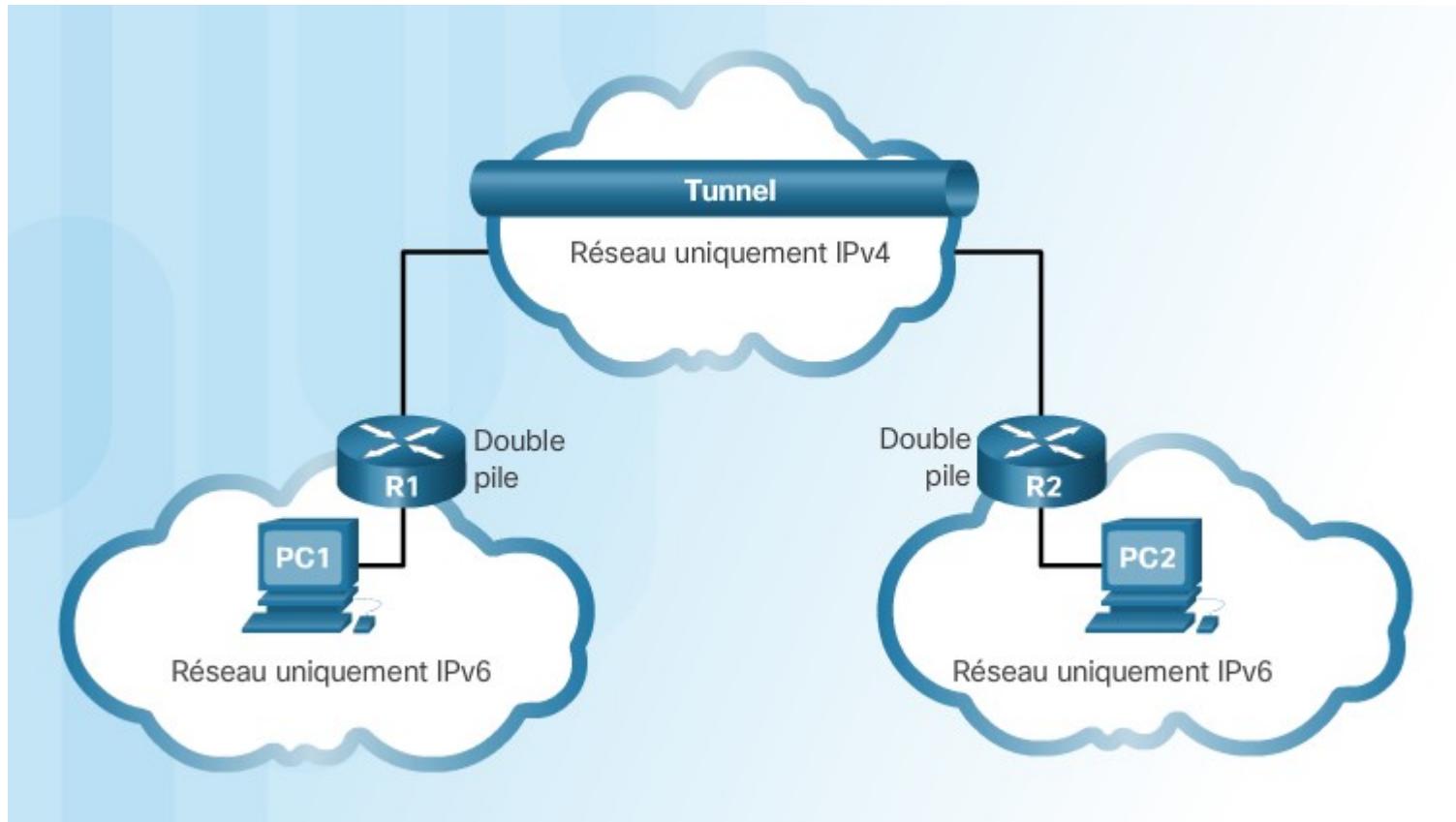
# Migration de l'IPv4 vers l'IPv6

- La transition vers l'IPv6 n'aura pas lieu à une date fixe. Dans un futur proche, l'IPv4 et l'IPv6 vont continuer à coexister. La transition vers l'IPv6 durera probablement plusieurs années. L'IETF a créé divers protocoles et outils pour aider les administrateurs réseau à migrer leurs réseaux vers l'IPv6. Les techniques de migration peuvent être classées en trois catégories :
  - **La double pile** : elle permet à l'IPv4 et à l'IPv6 de coexister sur le même segment de réseau. Les périphériques double pile exécutent les piles de protocoles IPv4 et IPv6 simultanément.
  - **Le tunneling 6to4** : c'est une méthode de transport des paquets IPv6 via un réseau IPv4. Les paquets IPv6 sont encapsulés dans des paquets IPv4, de la même manière que d'autres types de données.
  - **La traduction NAT64** : les périphériques IPv6 peuvent utiliser la traduction d'adresses réseau NAT64 pour communiquer avec les périphériques IPv4 à l'aide d'une technique de traduction similaire à la NAT pour l'IPv4. Un paquet IPv6 est traduit en un paquet IPv4, et inversement.

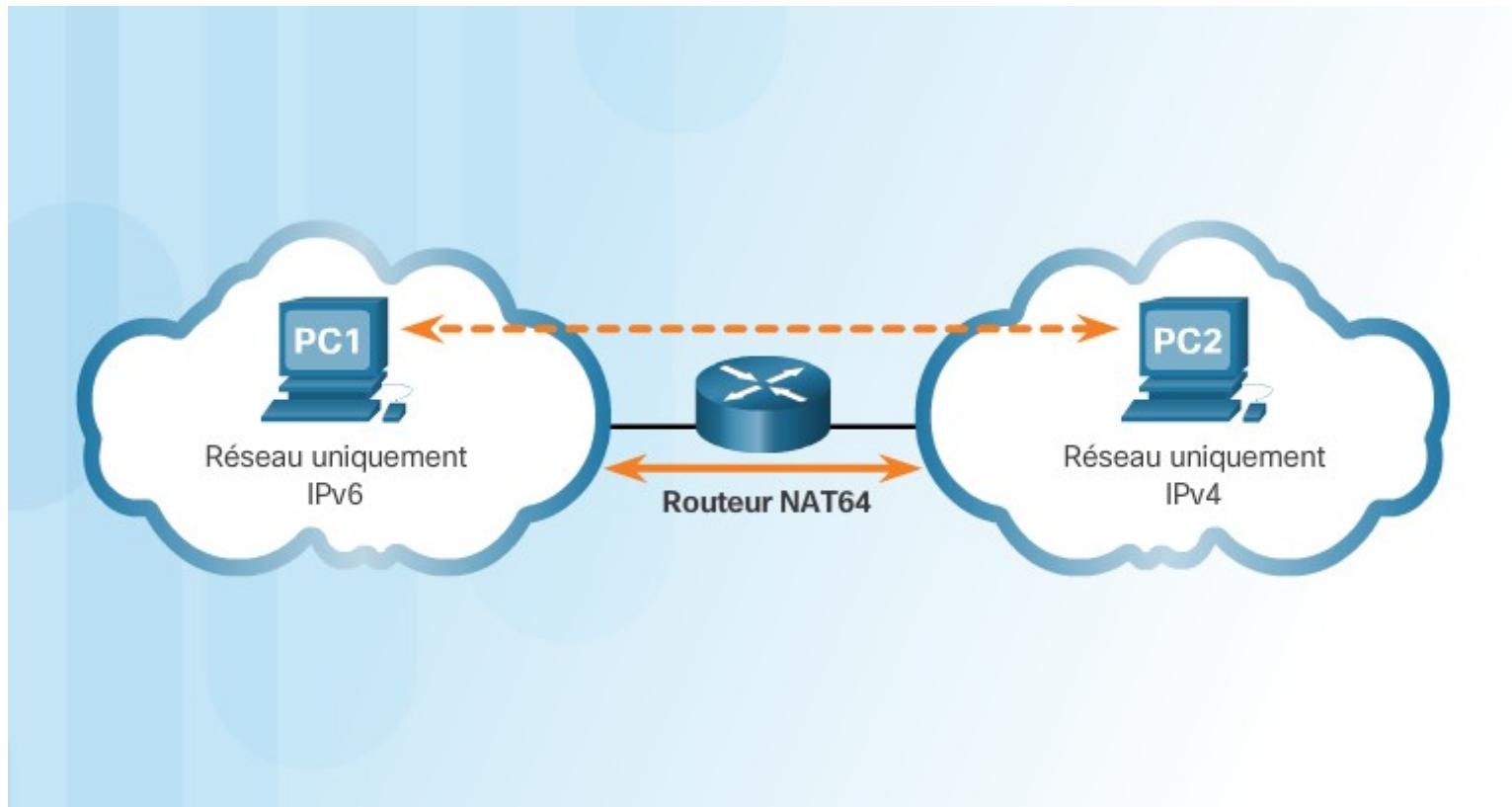
# Double pile



# Tunneling 6to4

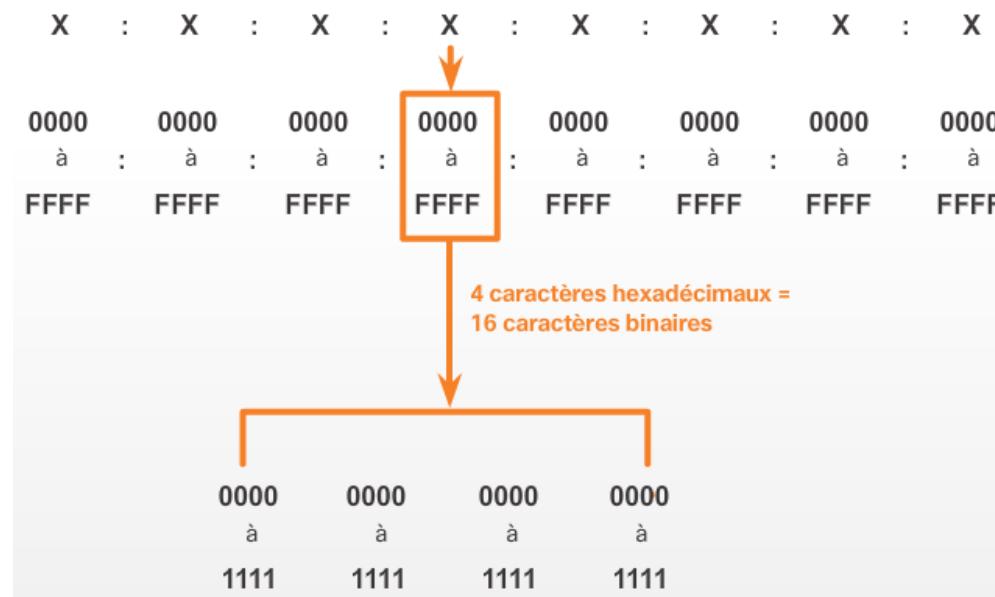


# Traduction NAT64



# Représentation d'une adresse IPv6

- Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales. Tous les groupes de 4 bits sont représentés par un caractère hexadécimal unique; pour un total de 32 valeurs hexadécimales. Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.
- Le format privilégié pour noter une adresse IPv6 est  $x:x:x:x:x:x:x:x$ , où chaque «  $x$  » est un groupe de quatre valeur hexadécimales. Le format privilégié implique que l'adresse IPv6 soit écrite à l'aide de 32 caractères hexadécimaux. Cela ne signifie pas nécessairement que c'est la solution idéale pour représenter une adresse IPv6.



# Simplification de la représentation

- **Règle n° 1 - Omettre les zéros situés à gauche de chaque groupe de quatre chiffres hexadécimaux**

La première règle pour réduire la notation des adresses IPv6 consiste à omettre les zéros (0) situés à gauche de chaque section de 16 bits (quatre chiffres hexadécimaux). Par exemple :

- 01AB est équivalent à 1AB
- 09F0 est équivalent à 9F0
- 0A00 est équivalent à A00
- 00AB est équivalent à AB

Cette règle s'applique bien entendu uniquement aux zéros à gauche de chaque segment et NON aux zéros situés à droite.

Recommandé	2 001 : 0 DB8 : 0 0 0 : 1 1 1 1 : 0 0 0 0 : 0 0 0 0 : 0 2 0 0
Sans zéros en début de segment	2 001 : DB8 : 0 : 1 1 1 1 : 0 : 0 : 0 : 2 0 0

# Simplification de la représentation

- **Règle n° 2 - Omettre les séquences composées uniquement de zéros**

La deuxième règle permettant d'abréger la notation des adresses IPv6 est qu'une suite de deux fois deux points (::) peut remplacer toute chaîne unique et contiguë d'un ou plusieurs segments de 16 bits composés uniquement de zéros.

Une suite de deux fois deux points (::) peut être utilisée une seule fois par adresse. Lorsque l'omission des zéros de début de segment est utilisée, la notation des adresses IPv6 peut être considérablement réduite. Il s'agit du « format compressé ».

Recommandé	2 0 0 1 : 0 D B 8 : 0 0 0 0 : 0 0 0 0 : A B C D : 0 0 0 0 : 0 0 0 0 : 0 1 0 0
Sans zéros en début de segment	2 0 0 1 : D B 8 : 0 : 0 : A B C D : 0 : 0 : 1 0 0
Compressé	2 0 0 1 : D B 8 :: A B C D : 0 : 0 : 1 0 0
ou	
Compressé	2 0 0 1 : D B 8 : 0 : 0 : A B C D :: 1 0 0

Diagramme illustrant la simplification de l'adresse IPv6 :

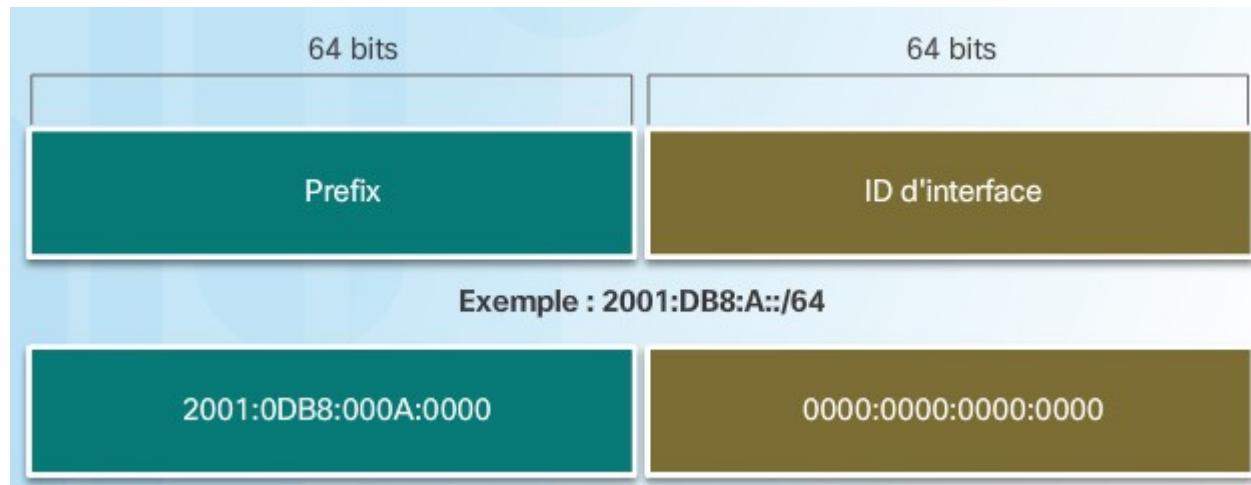
- Un trait orange pointe vers le premier double deux-points (::) dans la ligne "Compressé".
- Un autre trait orange pointe vers le deuxième double deux-points (::) dans la ligne "Compressé".
- Un callout orange indique : ":: peut être utilisé une seule fois."

# Types d'adresses IPv6

- Il existe trois types d'adresses IPv6 :
  - **Unicast ou monodiffusion** : une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique. Une adresse IPv6 source doit toujours être une adresse de monodiffusion.
  - **Multicast ou multidiffusion** : une adresse de multidiffusion IPv6 est utilisée pour envoyer un seul paquet IPv6 vers un groupe de périphériques.
  - **Anycast** : une adresse anycast IPv6 est une adresse de monodiffusion IPv6 qui peut être attribuée à plusieurs périphériques. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse. Les adresses anycast sortent du cadre de ce cours.
- Contrairement à l'IPv4, l'IPv6 n'a pas d'adresse de diffusion. Cependant, il existe une adresse de multidiffusion destinée à tous les nœuds IPv6 et qui offre globalement les mêmes résultats.

# Longueur de préfixe IPv6

- L'IPv6 utilise la longueur de préfixe pour représenter le masque de sous-réseau. Le protocole IPv6 n'utilise pas la notation décimale à point. Comme pour l'IPv4, la longueur de préfixe est utilisée dans l'IPv6 pour indiquer la partie réseau d'une adresse à l'aide de la notation adresse IPv6/longueur de préfixe.
- La longueur de préfixe peut être comprise entre 0 et 128. La longueur de préfixe IPv6 standard pour les réseaux locaux et la plupart des autres types de réseau est /64. Cela signifie que le préfixe ou la partie réseau de l'adresse a une longueur de 64 bits, ce qui laisse 64 bits pour l'ID d'interface (partie hôte) de l'adresse.



# Types d'adresses monodiffusion IPv6

- Les types d'adresses de monodiffusion IPv6 les plus courants sont les adresses de monodiffusion globale et les adresses de monodiffusion link-local.
- **Monodiffusion globale**

Une adresse de monodiffusion globale est similaire à une adresse IPv4 publique. Ces adresses sont uniques au monde et routables sur Internet. Les adresses de monodiffusion globale peuvent être configurées de manière statique ou attribuées dynamiquement. Actuellement, seules des adresses de diffusion globale dont les trois bits de poids fort sont 001 sont attribuées (les adresses qui commencent par 2000 à 3FFF).

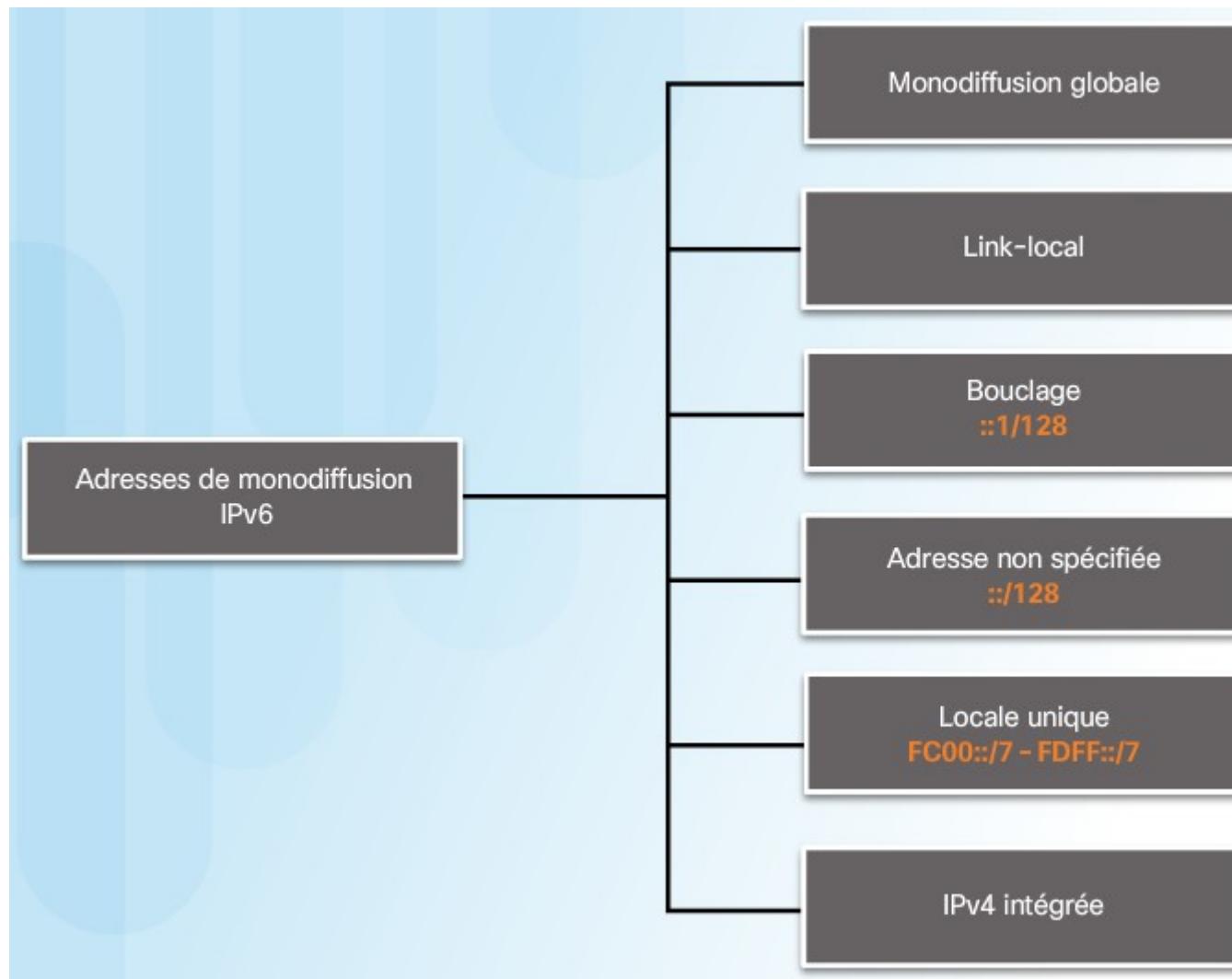
- **Link-local**

Les adresses link-local sont utilisées pour communiquer avec d'autres périphériques uniquement sur la même liaison locale (le même sous-réseau). Leur caractère unique doit être confirmé uniquement sur cette liaison, car elles ne sont pas routables au-delà de la liaison. En d'autres termes, les routeurs ne transmettent aucun paquet avec une adresse source ou de destination link-local. Les adresses link-local sont comprises entre FE80::/10 et FEBF::/10.

- **Adresse locale unique**

Les adresses IPv6 locales uniques ont certains points communs avec les adresses privées RFC 1918 utilisées dans l'IPv4, mais présentent également d'importantes différences. Des adresses locales uniques sont utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites. Ces adresses ne doivent pas être routables sur le réseau IPv6 global et ne doivent pas être traduites en adresses IPv6 globales. Les adresses locales uniques sont comprises entre FC00::/7 et FDFF::/7.

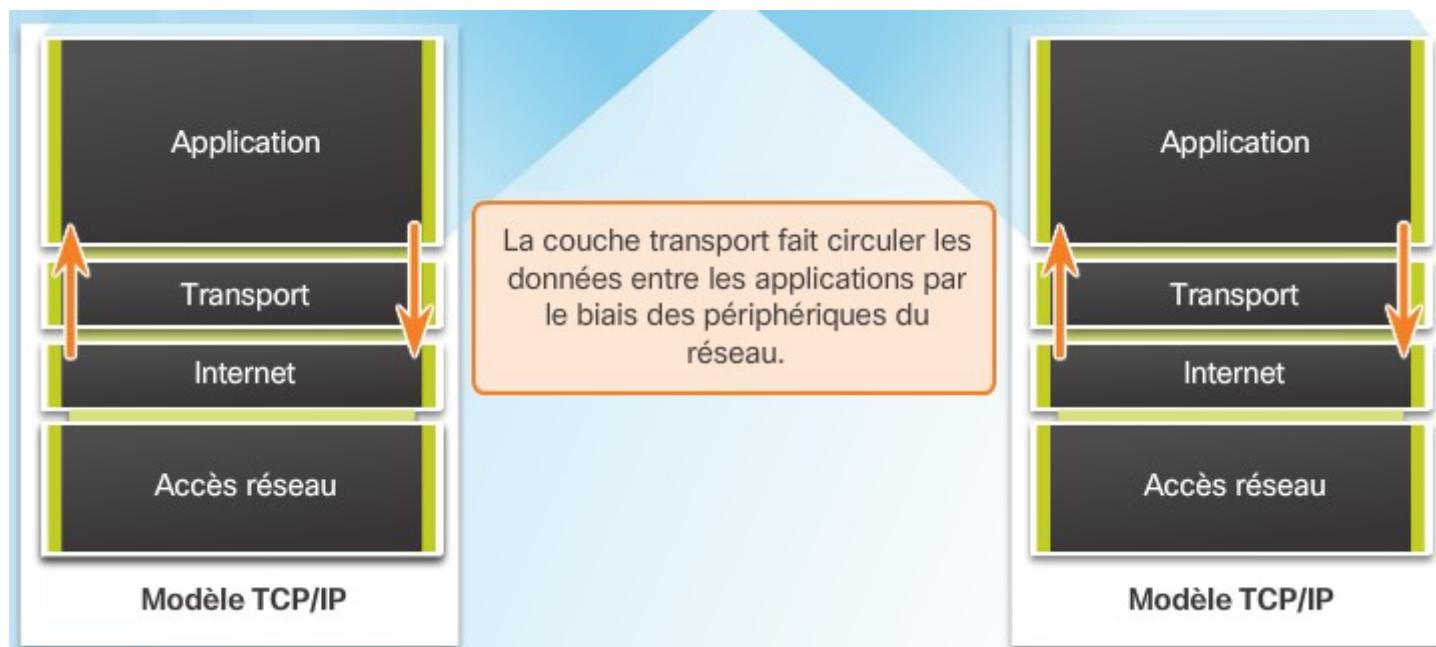
# Types d'adresses monodiffusion IPv6



# Couche Transport

# Rôle de la couche transport

- La couche transport est chargée de l'établissement d'une communication temporaire entre deux applications et de l'acheminement des données entre elles. Une application génère des données qui sont envoyées d'un hôte source à une autre application située sur un hôte de destination. Et ce, sans se soucier du type de l'hôte de destination, du type de support que les données doivent emprunter, du chemin suivi par ces données, de l'encombrement de la liaison ni de la taille du réseau.



# Couche transport - Fonctionnalités

- **Suivi des conversations individuelles**

Au niveau de la couche transport, chaque **ensemble de données transitant entre une application source et une application de destination** est appelé une **conversation**. Un hôte peut héberger plusieurs applications qui communiquent sur le réseau simultanément. Chacune de ces applications communique avec une ou plusieurs applications sur un ou plusieurs hôtes distants. La couche transport est chargée de **garantir ces multiples conversations** et d'en effectuer le suivi.

- **Segmentation des données et reconstitution des segments**

Les données doivent être préparées à être envoyées sur le support sous forme de **blocs faciles à gérer**. Les protocoles de couche transport disposent de services qui **segmentent les données d'application en blocs de taille appropriée**. Un en-tête, utilisé pour la réorganisation, est ajouté à chaque bloc de données.

Au niveau du destinataire, **la couche transport doit pouvoir reconstituer le flux de données initial**, à partir des blocs de données reçus. Les protocoles intervenant au niveau de la couche transport gèrent la façon dont les informations d'en-tête de la couche transport servent à rassembler les blocs de données.

- **Identification des applications**

Pour que les flux de données atteignent les applications auxquelles ils sont destinés, **la couche transport doit identifier l'application cible et l'application source** à l'aide d'un identificateur d'application appelé **numéro de port**. Chaque processus logiciel ayant besoin d'accéder au réseau se voit affecter un numéro de port unique sur son hôte.

# Couche transport - Fonctionnalités

- **Transfert fiable ou non fiable**

La suite de protocoles TCP/IP propose deux protocoles de couche transport :

- Le **protocole TCP (Transmission Control Protocol)** est un protocole de couche transport fiable qui garantit que toutes les données arrivent à destination. Toutefois, cela nécessite des champs supplémentaires dans l'en-tête TCP, ce qui augmente la taille du paquet et engendre des retards.
- Le **protocole UDP (User Datagram Protocol)** est un protocole de couche transport plus simple, qui ne permet pas de garantir la fiabilité du transport. Il possède un en-tête plus petit et s'avère donc plus rapide que le protocole TCP.

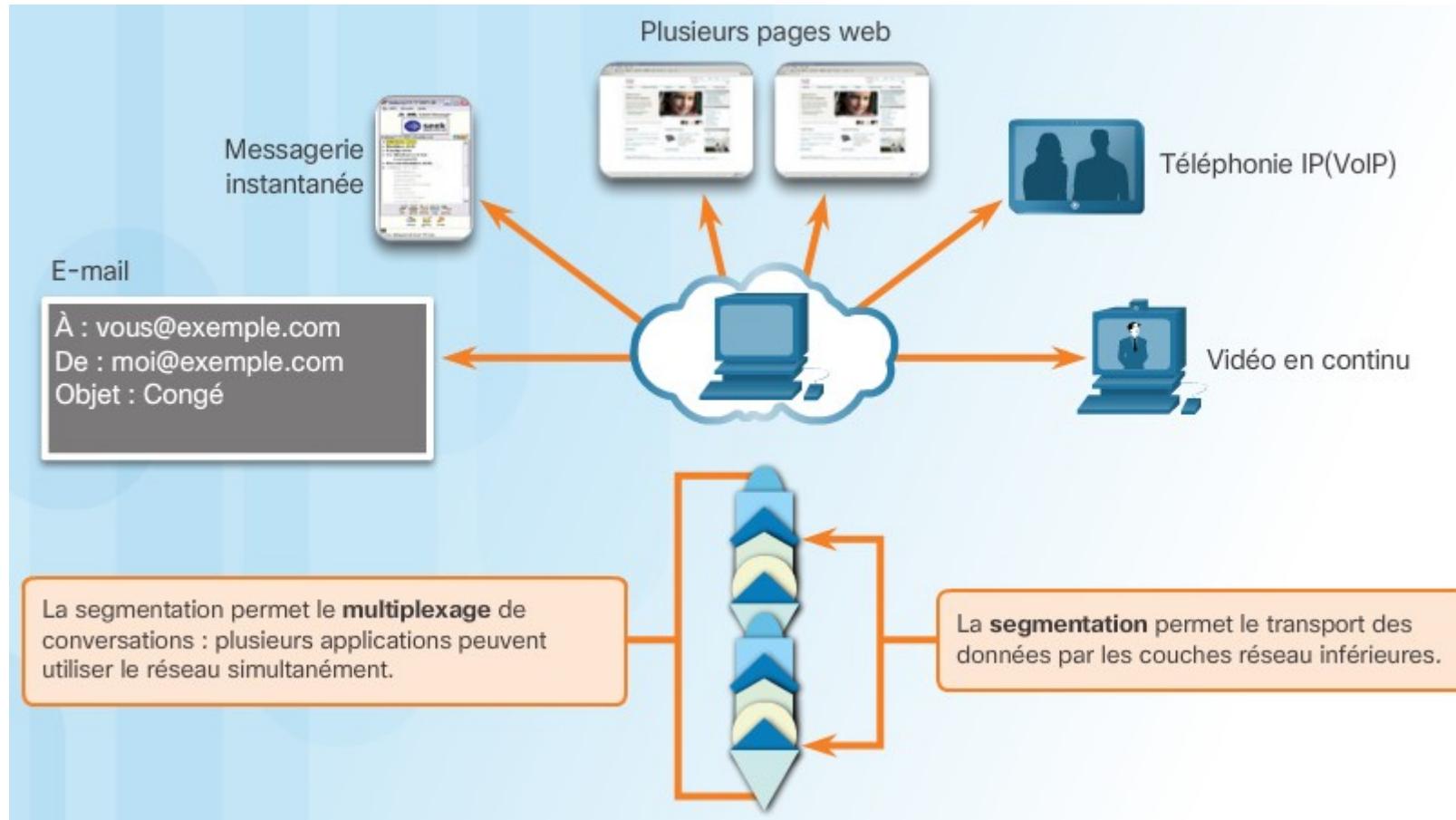
- **Contrôle de flux**

Le protocole TCP offre également des mécanismes relatifs au **contrôle de flux**, qui aide à maintenir la fiabilité des transmissions TCP **en réglant le flux de données** entre la source et la destination en fonction de la **capacité de traitement**. Pour cela, l'en-tête TCP inclut un champ de 16 bits appelé **taille de fenêtre**.

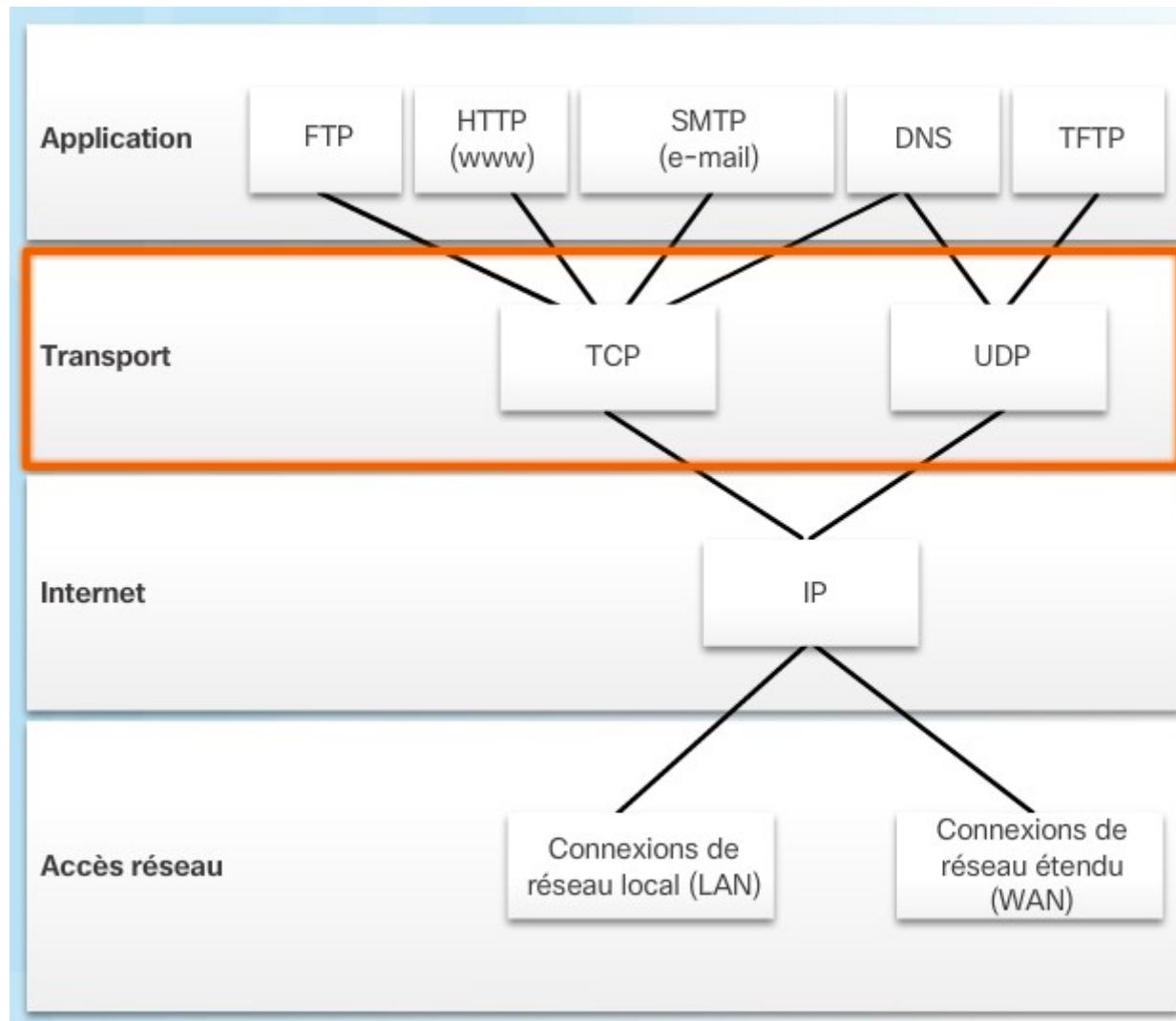
- **Multiplexage d'applications**

La segmentation des données en éléments plus petits permet à **plusieurs communications différentes**, provenant de nombreux utilisateurs, **d'être imbriquées (multiplexées) sur le même réseau**. C'est ainsi que plusieurs applications peuvent communiquer en réseau simultanément. On appelle ce processus le **multiplexage d'applications**.

# Multiplexage d'applications



# Protocoles TCP et UDP



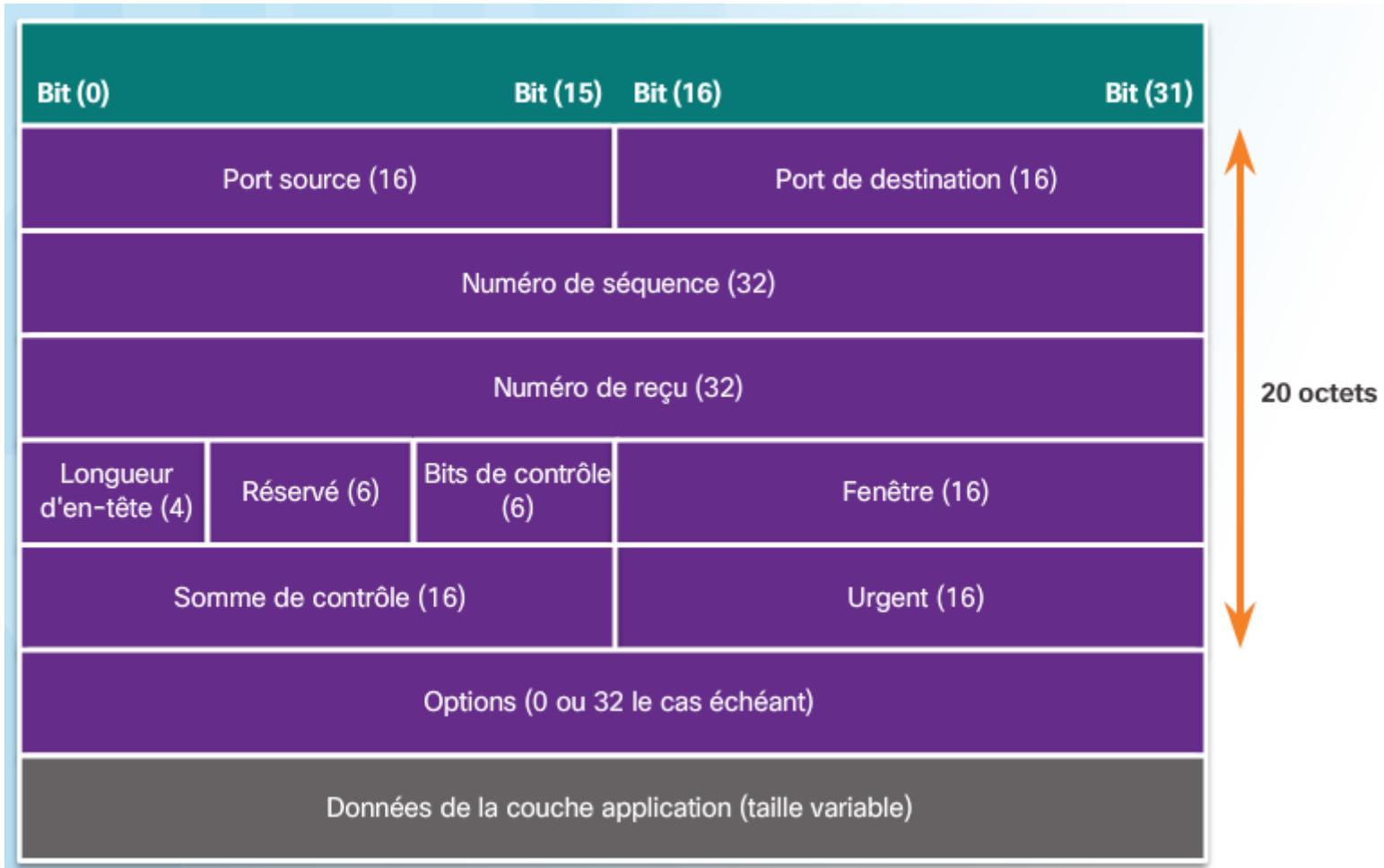
# Protocole TCP

- Fonctions du protocole TCP :
  - L'**établissement d'une connexion** permet de s'assurer que l'application est prête à recevoir les données.
  - La **livraison dans un ordre défini** permet de s'assurer que les segments sont remis dans le bon ordre.
  - L'**acheminement fiable** permet de s'assurer que les données soient reçues dans leur intégralité.
  - Le **contrôle de flux** permet de s'assurer que le récepteur est capable de traiter les données reçues.
- Avec le protocole TCP, les **trois fonctions de fiabilité** de base sont :
  - **Numérotation** et suivi des segments de données transmis à un hôte donné à partir d'une application spécifique
  - **Accusé de réception** des données reçues
  - **Retransmission des données** pour lesquelles aucun accusé de réception n'a été reçu, après un certain temps

# En-tête TCP

- L'en-tête d'un segment TCP est formé de **20 octets**. Les principaux champs qui le constituent sont :
  - **Port source** (16 bits) et **port de destination** (16 bits) : utilisés pour identifier respectivement les applications source et destination.
  - **Numéro d'ordre** (32 bits) : des fois appelé « numéro de séquence », il est utilisé pour pouvoir réorganiser les données à la réception.
  - **Numéro d'accusé de réception** (32 bits) : indique quelles données ont été reçues.
  - **Bits de contrôle** (6 bits) : des fois appelé « drapeau », il est constitué par six bits dont chacun indique une propriété du segment de données en cours.
  - **Taille de fenêtre** (16 bits) : indique le nombre d'octets de données pouvant être traitées en même temps.
  - **Somme de contrôle** (16 bits) : utilisée pour le contrôle des erreurs dans l'en-tête et les données de segment.
  - **Urgent** (16 bits) : indique si les données sont urgentes.

# Entête d'un segment TCP

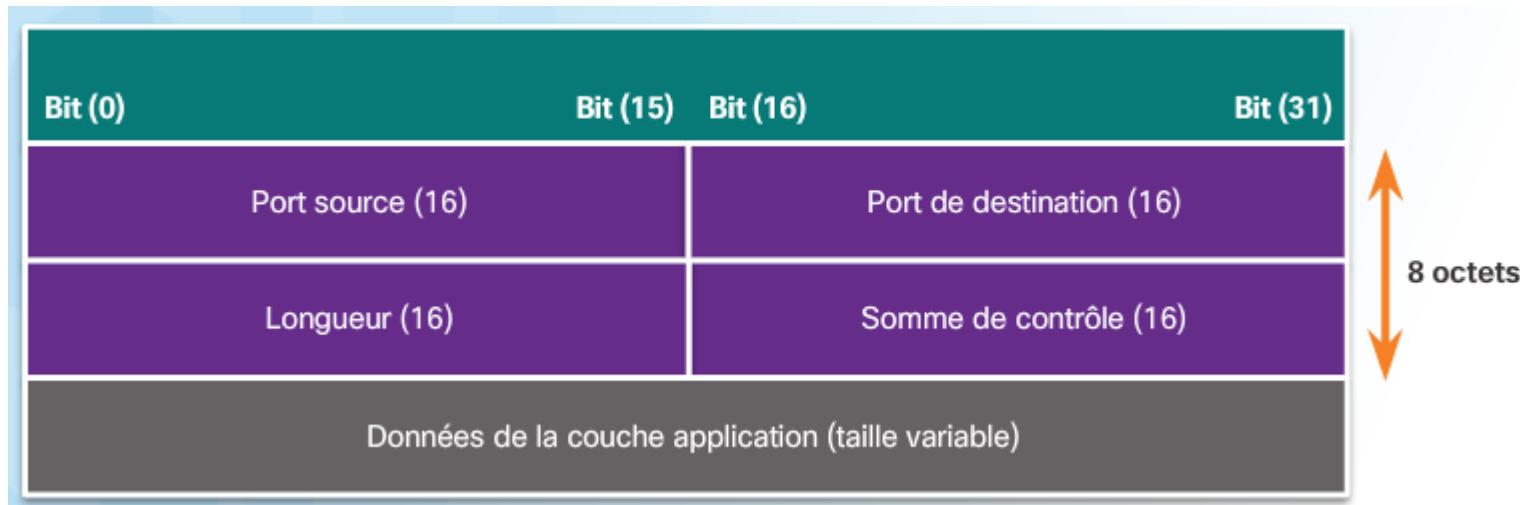


# Protocole UDP

- Le protocole UDP est considéré comme un protocole d'**acheminement au mieux**. Le protocole UDP est un **protocole de transport léger** qui offre les mêmes fonctions de **segmentation** des données que le protocole TCP, mais **sans fiabilité ni contrôle de flux**. C'est un protocole simple, qui est généralement décrit en indiquant ce qu'il ne fait pas par rapport au protocole TCP.
- Si la fiabilité est nécessaire dans le cadre de l'utilisation du protocole UDP, elle doit être prise en charge par la couche application.
- **Fonctionnalités du protocole UDP :**
  - Les données sont reconstituées selon l'ordre de réception.
  - Les segments perdus ne sont pas renvoyés.
  - Pas d'établissement de connexion.
  - L'expéditeur n'est pas informé de la disponibilité des ressources.

# En-tête UDP

- L'en-tête d'un segment UDP (appelé également **datagramme UDP**) est formé de **8 octets**. Les quatre champs qui le constituent sont :
  - Port source** (16 bits) et **port de destination** (16 bits) : utilisés pour identifier respectivement les applications source et destination.
  - Longueur** (16 bits) : indique la longueur totale (exprimée en octets) du segment UDP (en-tête et données). La longueur minimale est donc de 8 octets (taille de l'en-tête).
  - Somme de contrôle** (16 bits) : utilisée pour le contrôle des erreurs dans l'en-tête et les données de segment



# TCP ou UDP

## UDP



Téléphonie IP



Vidéo en continu  
en direct

## TCP



SMTP/POP  
(E-mail)



HTTP

### Propriétés de protocole requises :

- Rapide
- Faible surcharge
- Pas d'accusé de réception requis
- Pas de renvoi des données perdues
- Envoi des données à mesure de leur arrivée

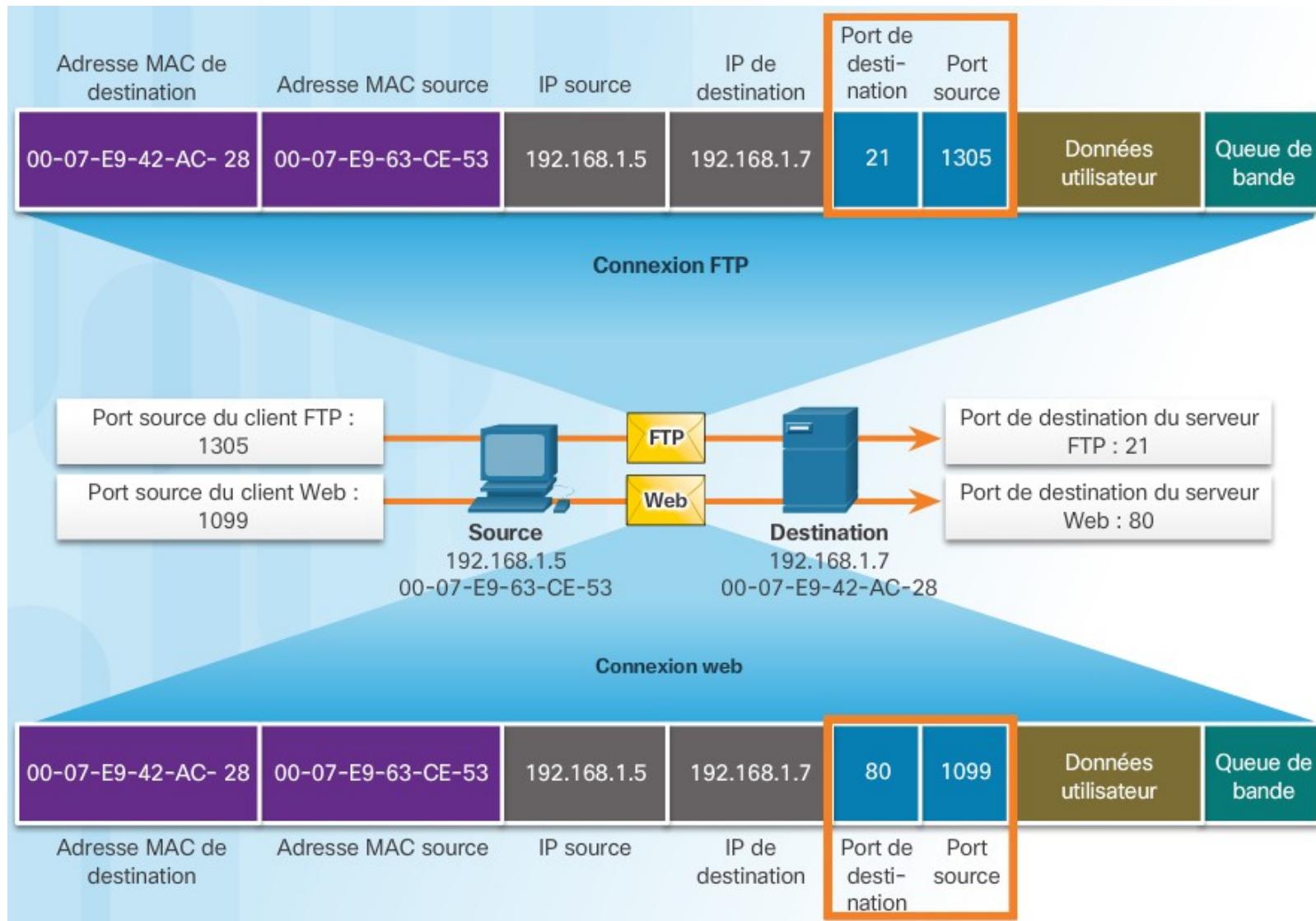
### Propriétés de protocole requises :

- Fiable
- Accusé de réception des données
- Renvoi des données perdues
- Envoi des données en ordre séquentiel

# Numéros de ports

- Le numéro du **port source** est associé à l'**application d'origine sur l'hôte local**. Le numéro du **port de destination** est associé à l'**application de destination sur l'hôte distant**.
- Il existe trois types de numéros de port :
  - **Ports réservés** (numéros 0 à 1023) : ces numéros sont réservés à des services et des applications connues, comme les services HTTP (80), FTP (20 et 21), DHCP (67 et 68), DNS (53) ... etc.
  - **Ports enregistrés** (numéros 1024 à 49151) : ces numéros de port sont affectés à une entité demandeuse pour une utilisation avec des processus ou des applications spécifiques. Ces processus sont essentiellement des applications particulières qu'un utilisateur a choisi d'installer plutôt que des applications courantes qui recevraient un port réservé. Par exemple, Cisco a enregistré le port 1985 pour son processus HSRP (Hot Standby Routing Protocol).
  - **Ports privés ou dynamiques** (numéros 49152 à 65535) : également appelés ports éphémères, ces ports sont généralement affectés de façon dynamique par le système d'exploitation aux clients lorsqu'une connexion à un service donné. Le port dynamique est utilisé pour identifier l'application cliente durant la communication.

# Numéros de ports

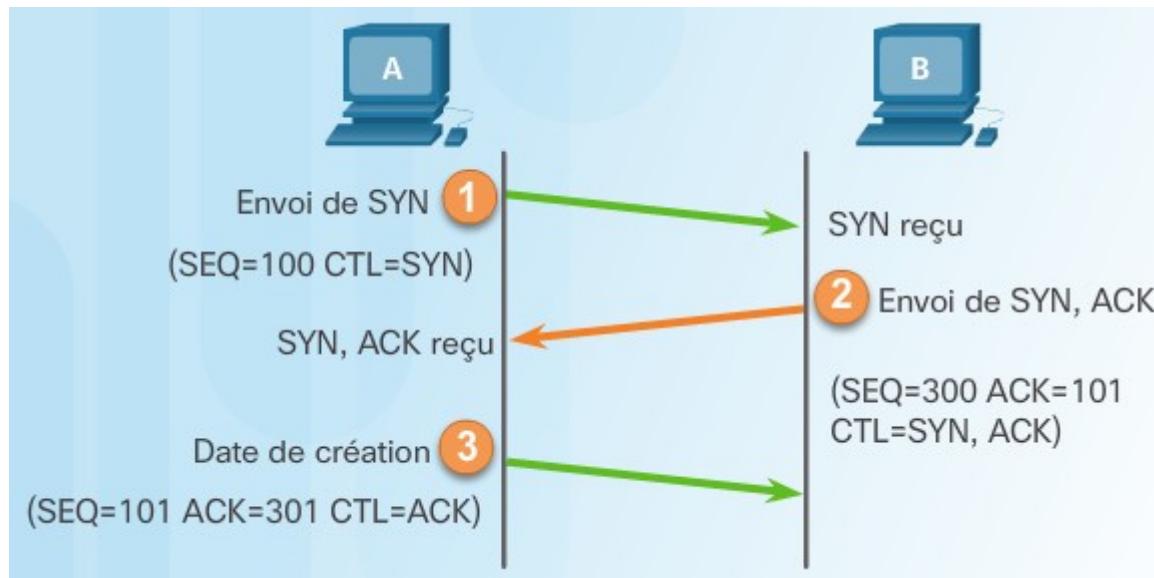


# Exemples de ports réservés

Numéro de port	Protocole	Application	Acronyme
20	TCP	Protocole FTP (File Transfer Protocol) (données)	FTP
21	TCP	Protocole FTP (File Transfer Protocol) (contrôle)	FTP
22	TCP	Secure Shell	SSH
23	TCP	Telnet	—
25	TCP	Protocole SMTP (Simple Mail Transfer Protocol)	SMTP
53	UDP, TCP	Domain Name Service (service de noms de domaines)	DNS
67	UDP	Protocole DHCP (Dynamic Host Configuration Protocol) (serveur)	DHCP
68	UDP	Protocole DHCP (Dynamic Host Configuration Protocol) (client)	DHCP
69	UDP	Protocole TFTP (Trivial File Transfer Protocol)	TFTP
80	TCP	Protocole HTTP (Hypertext Transfer Protocol)	HTTP
110	TCP	Protocole POP (Post Office Protocol) version 3	POP3
143	TCP	Protocole IMAP (Internet Message Access Protocol)	IMAP
161	UDP	Protocole SNMP (Simple Network Management Protocol)	SNMP
443	TCP	Protocole HTTPS (Hypertext Transfer Protocol Secure)	HTTPS

# Établissement de connexion TCP

- Lorsque le protocole TCP est utilisé, le client établit toujours la connexion avec le serveur avant tout échange de données.
- Une connexion TCP s'établit en trois étapes :
  - 1. Le client A demande l'établissement d'une session de communication avec le serveur B.
  - 2. Le serveur B accueille réception de la session de communication et demande au client A l'établissement d'une session de communication à son tour.
  - 3. Le client A accueille réception de la session de communication demandée par le serveur B.



# Commande liée à la couche transport

- La commande **netstat** peut être utilisée pour afficher les processus en cours de communication dans un hôte. Elle indique le type de protocole de couche transport concerné, les numéros de ports utilisés, ainsi que les adresses IP source et destination des messages échangés.

```
Mark Administrator: D:\windows\system32\cmd.exe
D:\Users\greg>netstat -an

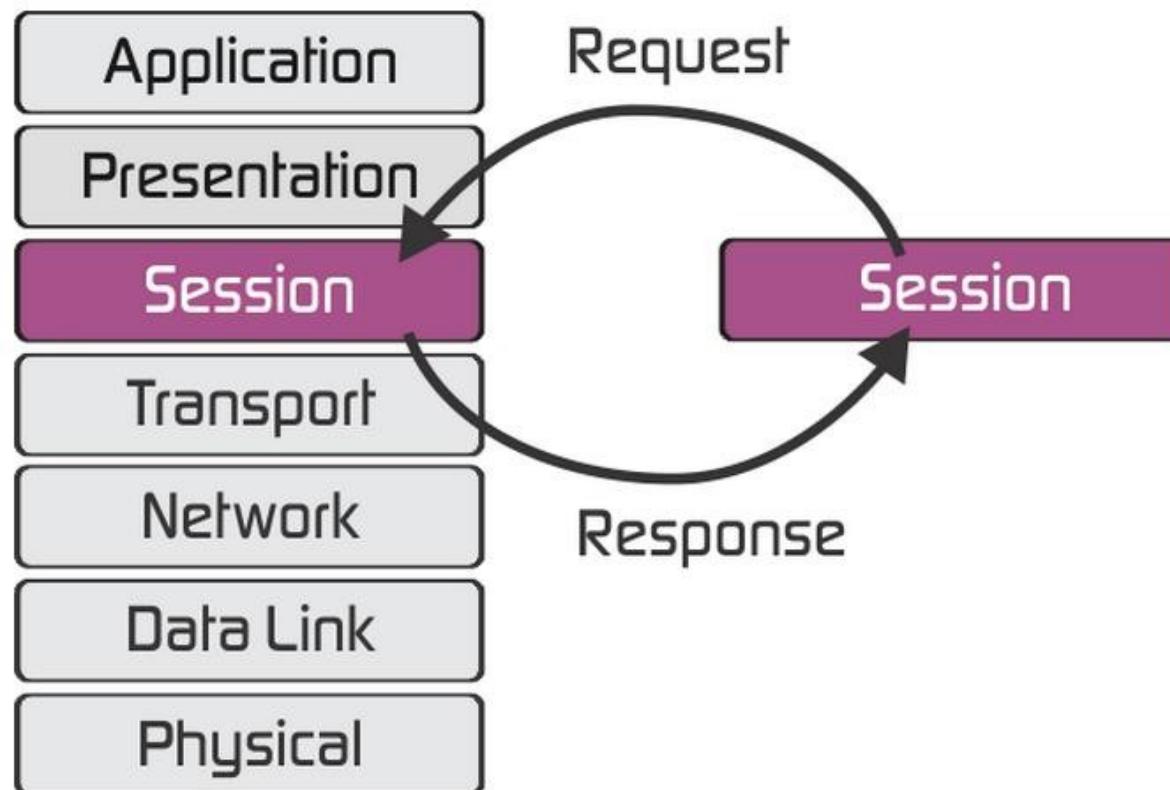
Active Connections

Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:80              0.0.0.0:0            LISTENING
TCP    0.0.0.0:135             0.0.0.0:0            LISTENING
TCP    0.0.0.0:445             0.0.0.0:0            LISTENING
TCP    0.0.0.0:3389            0.0.0.0:0            LISTENING
TCP    0.0.0.0:16001            0.0.0.0:0            LISTENING
TCP    0.0.0.0:49152            0.0.0.0:0            LISTENING
TCP    0.0.0.0:49153            0.0.0.0:0            LISTENING
TCP    0.0.0.0:49154            0.0.0.0:0            LISTENING
TCP    0.0.0.0:49155            0.0.0.0:0            LISTENING
TCP    0.0.0.0:49156            0.0.0.0:0            LISTENING
TCP    10.114.242.92:80         24.200.167.248:60734  ESTABLISHED
TCP    10.114.242.92:80         65.107.86.243:7884   ESTABLISHED
TCP    10.114.242.92:80         65.107.86.243:56679  ESTABLISHED
TCP    10.114.242.92:80         71.134.235.236:55974  ESTABLISHED
TCP    10.114.242.92:80         71.134.235.236:55975  ESTABLISHED
TCP    10.114.242.92:80         71.134.235.236:55982  ESTABLISHED
TCP    10.114.242.92:80         71.206.126.119:55530  ESTABLISHED
TCP    10.114.242.92:80         71.206.126.119:55534  ESTABLISHED
TCP    10.114.242.92:80         72.184.198.160:50191  ESTABLISHED
TCP    10.114.242.92:80         90.217.238.177:50776  ESTABLISHED
TCP    10.114.242.92:80         99.14.95.45:52713   ESTABLISHED
TCP    10.114.242.92:80         99.14.95.45:52720   ESTABLISHED
TCP    10.114.242.92:80         108.204.14.117:57065  ESTABLISHED
TCP    10.114.242.92:80         108.204.14.117:57068  ESTABLISHED
TCP    10.114.242.92:80         122.3.252.98:33972  TIME_WAIT
TCP    10.114.242.92:80         122.3.252.98:46852  TIME_WAIT
TCP    10.114.242.92:80         122.3.252.98:47730  TIME_WAIT
TCP    10.114.242.92:80         122.3.252.98:54537  TIME_WAIT
TCP    10.114.242.92:80         122.3.252.98:57597  TIME_WAIT
TCP    10.114.242.92:80         174.127.9.2:64502  ESTABLISHED
TCP    10.114.242.92:80         184.78.65.34:50619  ESTABLISHED
TCP    10.114.242.92:80         188.60.198.170:36075  ESTABLISHED
TCP    10.114.242.92:80         193.105.210.133:3619  TIME_WAIT
TCP    10.114.242.92:80         208.48.4.102:36805  ESTABLISHED
TCP    10.114.242.92:80         208.105.122.202:5969  ESTABLISHED
TCP    10.114.242.92:80         222.127.28.138:37888 ESTABLISHED
```

# **Couches Session, Présentation et Application**

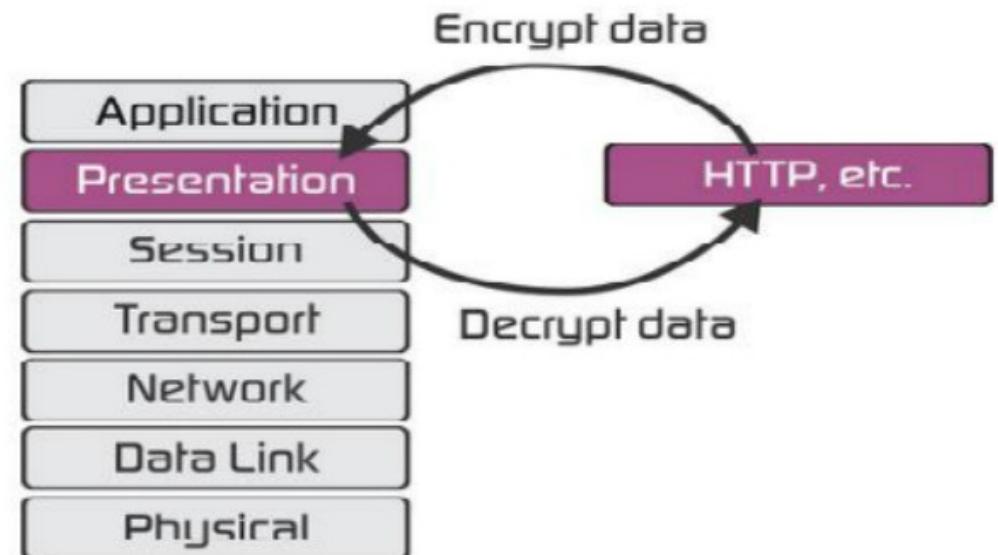
# Couche session

- La couche session crée et gère les dialogues entre les applications source et de destination. Elle traite l'échange des informations pour établir et maintenir un dialogue et pour redémarrer les sessions interrompues ou inactives pendant une longue période.



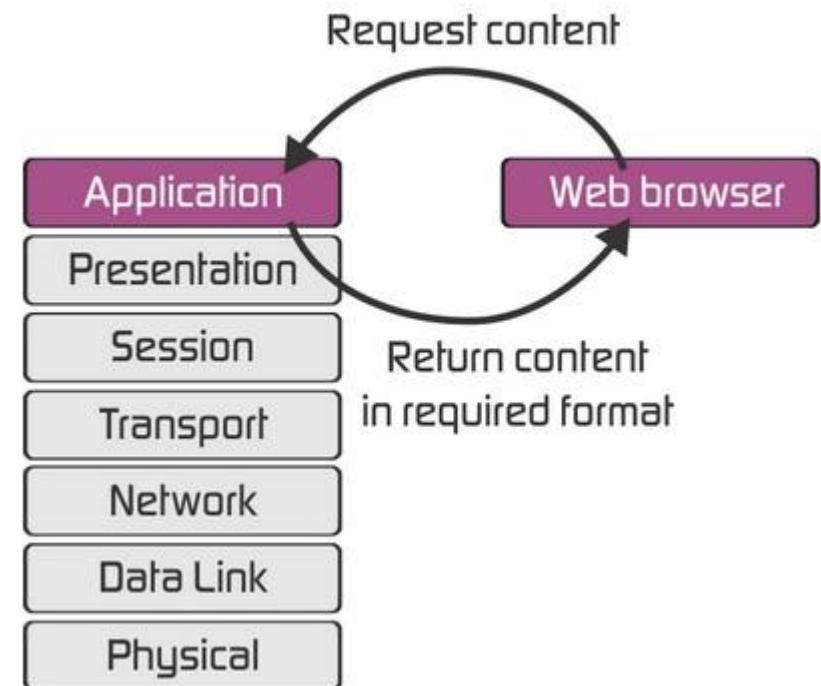
# Couche présentation

- La couche présentation remplit trois fonctions principales :
  - Mettre en forme ou présenter les données provenant du périphérique source dans un format compatible pour la réception par le périphérique de destination
  - Compresser les données de sorte que celles-ci puissent être décompressées par le périphérique de destination
  - Chiffrage des données pour la transmission et déchiffrage des données à la réception
- La couche présentation met en forme les données pour la couche application et définit les normes des formats de fichiers.



# Couche application

- La couche application est la plus proche de l'utilisateur final. C'est elle qui sert d'interface entre les applications que nous utilisons pour communiquer et le réseau via lequel les messages sont transmis. Les protocoles de couche application sont utilisés pour échanger des données entre les programmes s'exécutant sur les hôtes source et de destination.
- Il existe de nombreux protocoles de couche application et de nouveaux protocoles sont constamment développés. Parmi les protocoles de couche application les plus connus on trouve les protocoles HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), TFTP (Trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), IMAP (Internet Message Access Protocol), DHCP (Dynamic Host Configuration Protocol) et DNS (Domain Name System).



# Protocole HTTP

- Lorsqu'une adresse web (ou URL) est tapée dans un navigateur web, ce dernier établit une connexion au service web s'exécutant sur le serveur à l'aide du protocole HTTP. L'URL (Uniform Resource Locator) et l'URI (Uniform Resource Identifier) sont les noms que la plupart des utilisateurs associent aux adresses web.
- Le protocole HTTP est extrêmement flexible, mais il n'est pas sécurisé. Pour une communication sécurisée via Internet, le protocole HTTPS (HTTP Secure) est utilisé. HTTPS utilise l'authentification et le chiffrement pour sécuriser les données pendant leur transfert entre le client et le serveur. Il utilise pour cela le protocole SSL (Secure Socket Layer).
- Les services HTTP et HTTPS utilisent respectivement les ports 80 et 443.



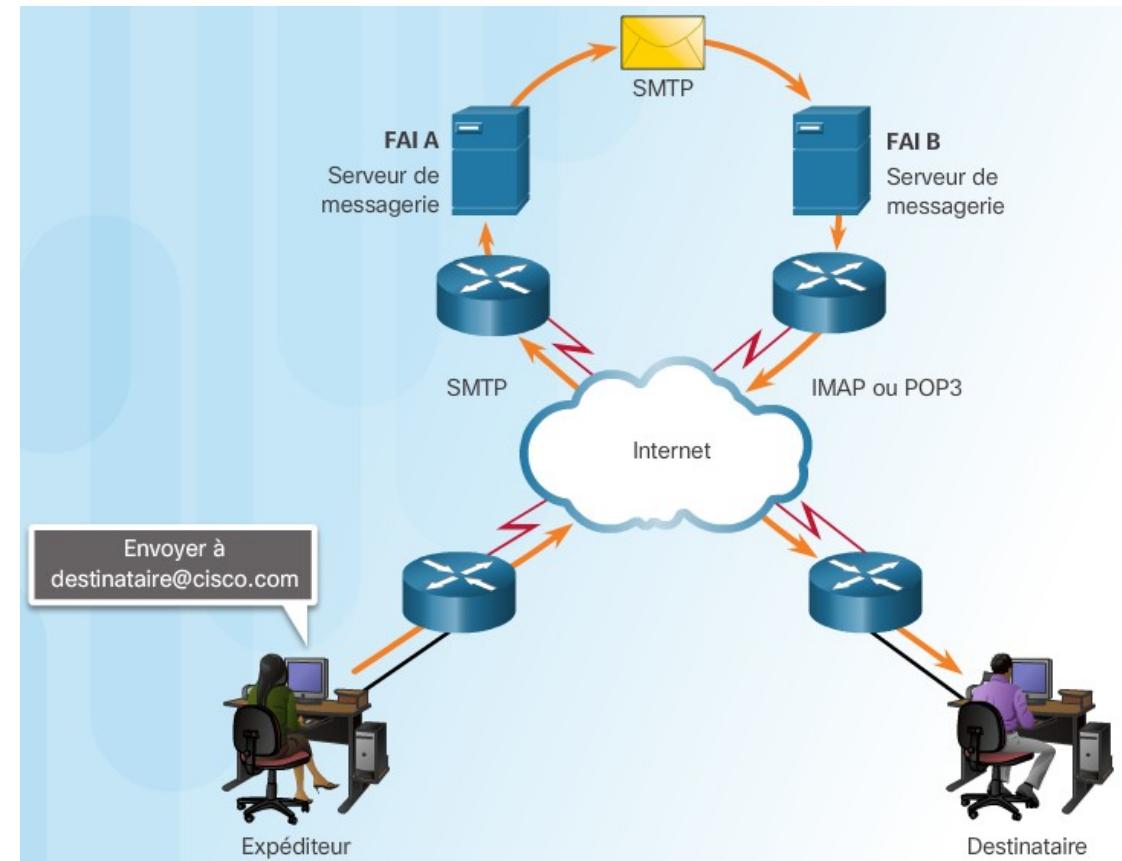
# Protocoles SMTP, POP et IMAP

- L'un des principaux services offerts par un FAI est l'hébergement de la messagerie. Le courriel permet d'envoyer, de stocker et de récupérer des messages électroniques à travers un réseau. Les messages électroniques sont stockés dans des bases de données sur des serveurs de messagerie.

Les e-mails font appel à trois protocoles distincts : SMTP (Simple Mail Transfer Protocol), POP (Post Office Protocol) et IMAP (Internet Message Access Protocol). Le processus de couche application qui envoie les e-mails utilise le protocole SMTP. Pour les récupérer, le client fait appel à l'un des deux protocoles de couche application suivants : POP ou IMAP.

Les ports utilisés par ces services sont :

- 25 : Protocole SMTP
- 110 : Protocole POP
- 143 : Protocole IMAP



# Protocole FTP

- Le protocole FTP (File Transfer Protocol) permet le transfert de données entre un client et un serveur. Un client FTP est une application s'exécutant sur un ordinateur client. Il sert à envoyer et à extraire des données d'un serveur FTP.
- Pour transférer avec succès les données, le protocole FTP nécessite deux connexions entre le client et le serveur, l'une pour les commandes et les réponses, l'autre pour le transfert de fichiers en lui-même :
  - Le client établit la première connexion au serveur pour le trafic de contrôle sur le port TCP 21. Cette première connexion se compose de commandes de clients et de réponses du serveur.
  - Le client établit la seconde connexion au serveur pour le transfert de données proprement dit sur le port TCP 20. Cette connexion est créée chaque fois que des données doivent être transférées.
- Le transfert de fichiers peut s'effectuer dans les deux sens. Le client peut télécharger (extraire) des données à partir du serveur ou le client peut télécharger (stocker) des données vers le serveur.

# Protocole DNS

- Le protocole DNS définit un service automatisé qui associe les noms des ressources aux adresses IP associées.
- Dans les réseaux de données, les périphériques sont identifiés par des adresses IP pour l'envoi et la réception de données. Des noms de domaine ont été créés pour convertir ces adresses IP en noms simples à utiliser.
- Sur Internet, ces noms de domaine (par exemple, [www.cisco.com](http://www.cisco.com)) sont beaucoup plus faciles à mémoriser que leurs équivalents numériques (par exemple, 198.133.219.25, l'adresse numérique du serveur de Cisco). Si Cisco décide de changer l'adresse numérique de [www.cisco.com](http://www.cisco.com), l'utilisateur n'en a pas conscience, car le nom de domaine reste le même. La nouvelle adresse est simplement reliée au nom de domaine existant et la connexion est ainsi assurée.



# Commandes DNS

- Il est possible de questionner le serveur DNS dont l'adresse est indiquée dans la configuration IP d'un client en exécutant la commande **nslookup**.

Cette commande permettra par exemple de récupérer la ou les adresses IP correspondantes à un nom de domaine.

```
C:\Users\VincentPC>nslookup
Serveur par défaut : livebox.home
Address: 192.168.1.1

> piratebay.me
Serveur : livebox.home
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : piratebay.me
Address: 185.53.178.6

> server 8.8.8.8
Serveur par défaut : google-public-dns-a.google.com
Address: 8.8.8.8

> piratebay.me
Serveur : google-public-dns-a.google.com
Address: 8.8.8.8

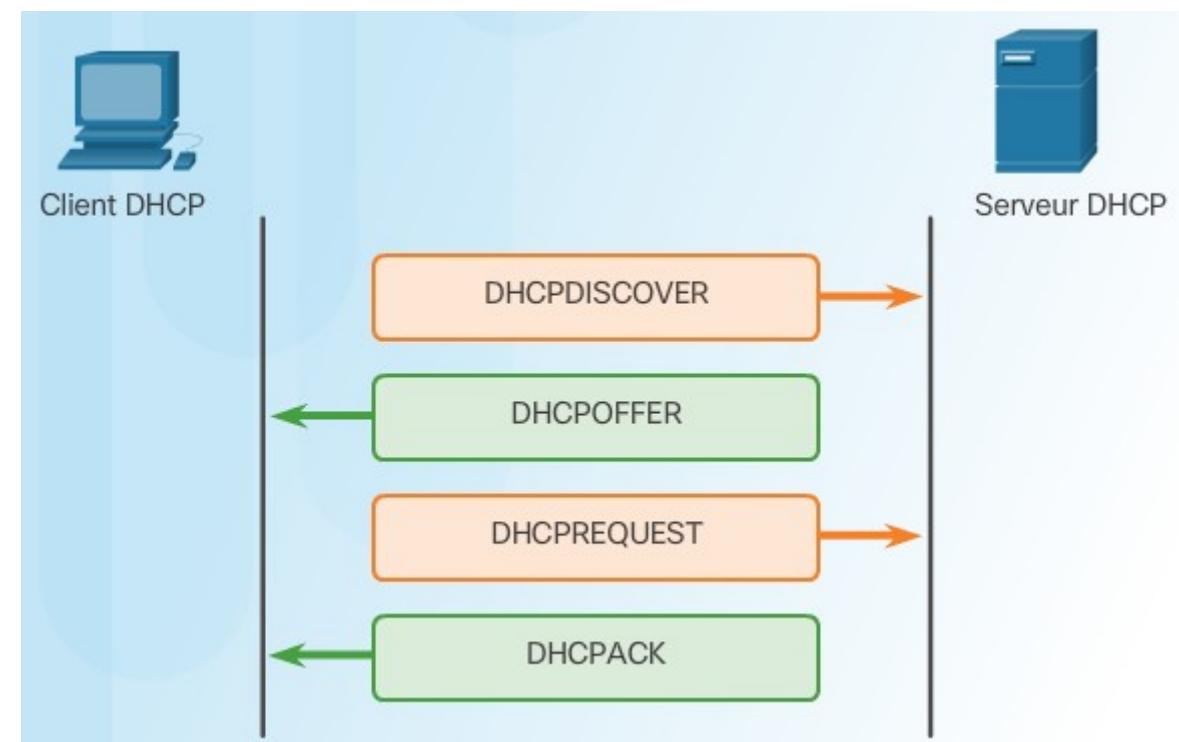
Réponse ne faisant pas autorité :
Nom : piratebay.me
Address: 185.53.178.6
```

# Protocole DHCP

- Lorsqu'un périphérique configuré en client DHCP démarre ou se connecte au réseau, il diffuse un message de détection DHCP (DHCPDISCOVER) pour identifier les serveurs DHCP disponibles sur le réseau. Si un serveur DHCP est présent, il répond par un message d'offre DHCP (DHCPOFFER), qui offre une configuration IP au client. Ce message contient l'adresse IPv4 et le masque de sous-réseau à attribuer, l'adresse IP du serveur DNS, l'adresse IP de la passerelle par défaut, et la durée du bail (durée pendant laquelle le client a le droit d'utiliser cette configuration IP).

Si le client reçoit plusieurs messages DHCP OFFER (cas où le réseau comporte plusieurs serveurs DHCP), il effectue un choix en envoyant une requête DHCP (DHCPREQUEST) qui identifie le serveur et la configuration IP qu'il accepte. Un client peut choisir de demander une adresse que le serveur lui a déjà attribuée précédemment.

Si l'adresse IP est disponible, le serveur renvoie un message d'accusé de réception DHCP (DHCPACK) confirmant au client que le bail est conclu.



# Commandes DHCP

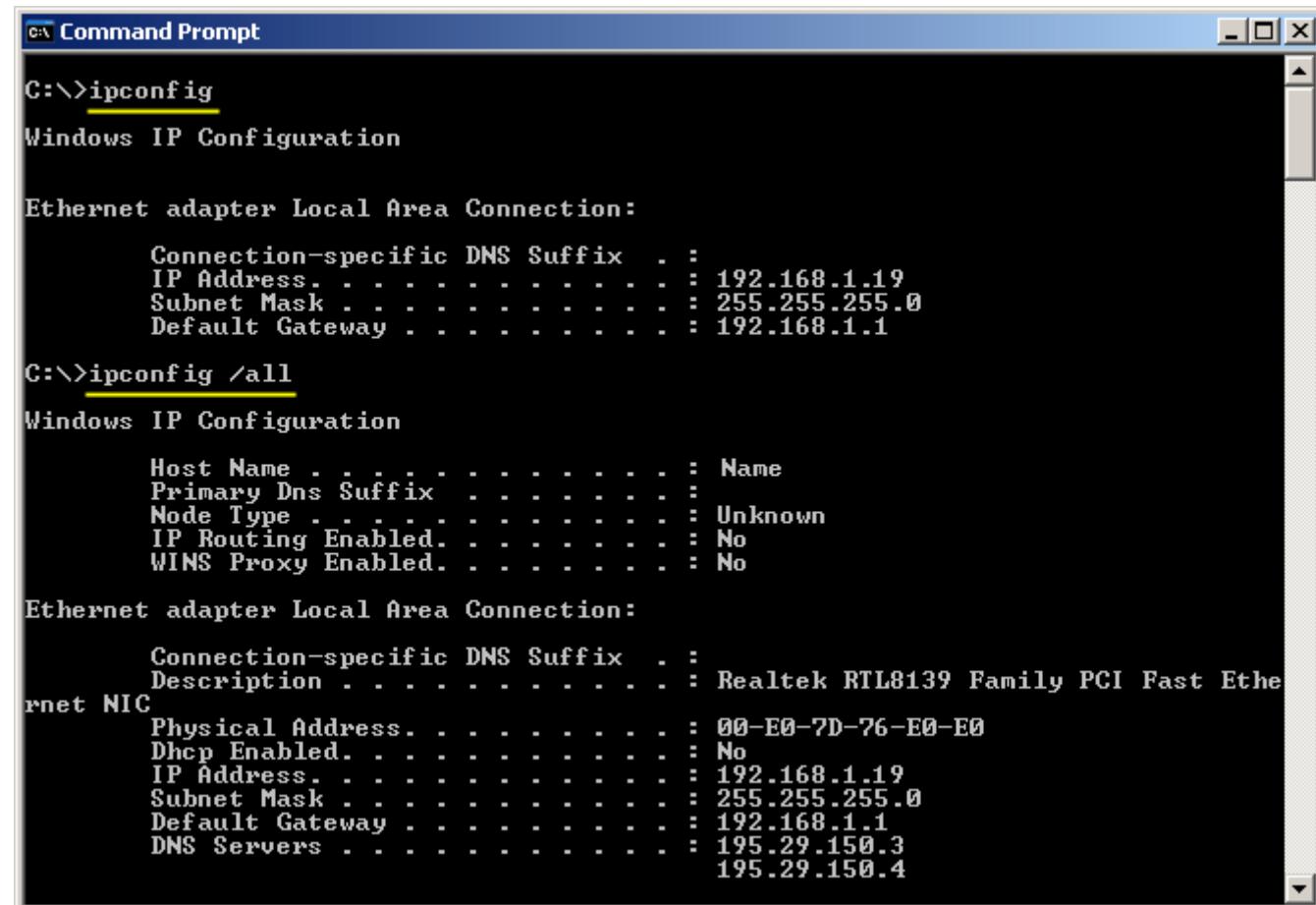
- Sous le système d'exploitation Windows, les commandes suivantes peuvent être exécutée du coté client :

**ipconfig** : Affiche la configuration IP résumée reçue depuis un serveur DHCP.

**ipconfig /all** : Affiche la configuration IP détaillée reçue depuis un serveur DHCP.

**ipconfig /release** : libère la configuration IP reçue depuis un serveur DHCP.

**ipconfig /renew** : renouvelle la configuration IP reçue depuis un serveur DHCP.



The screenshot shows a Windows Command Prompt window titled "Command Prompt". It displays two sets of IP configuration outputs for an "Ethernet adapter Local Area Connection".

**First Set (Output of ipconfig):**

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . . . . . : 192.168.1.19
  IP Address . . . . . : 192.168.1.19
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
```

**Second Set (Output of ipconfig /all):**

```
C:\>ipconfig /all
Windows IP Configuration

Host Name . . . . . : Name
Primary Dns Suffix . . . . . :
Node Type . . . . . : Unknown
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:
  Connection-specific DNS Suffix . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
  Description . . . . . : Realtek RTL8139 Family PCI Fast Ethe
rnet NIC
  Physical Address. . . . . : 00-E0-7D-76-E0-E0
  Dhcp Enabled. . . . . : No
  IP Address. . . . . : 192.168.1.19
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.1
  DNS Servers . . . . . : 195.29.150.3
                                         195.29.150.4
```

# Commandes DHCP

```
C:\WINDOWS\System32\cmd.exe
C:\Documents and Settings\Grégoire>ipconfig /release
Configuration IP de Windows

Carte Ethernet Connexion au réseau local:
    Suffrage DNS propre à la connexion :
    Adresse IP. . . . . : 0.0.0.0
    Masque de sous-réseau : . . . . . : 0.0.0.0
    Passerelle par défaut : . . . . . :

C:\Documents and Settings\Grégoire>ipconfig /renew
Configuration IP de Windows

Carte Ethernet Connexion au réseau local:
    Suffrage DNS propre à la connexion : 128.127.100.51
    Adresse IP. . . . . : 128.127.100.51
    Masque de sous-réseau : . . . . . : 255.255.0.0
    Passerelle par défaut : . . . . . : 128.127.100.100

C:\Documents and Settings\Grégoire>ipconfig /all
Configuration IP de Windows

    Nom de l'hôte . . . . . : srv
    Suffrage DNS principal . . . . . :
    Type de nœud . . . . . : Mixte
    Routage IP activé . . . . . : Non
    Proxy WINS activé . . . . . : Non

Carte Ethernet Connexion au réseau local:
    Suffrage DNS propre à la connexion : Sis 900 PCI Fast Ethernet Adapter
    Description . . . . . : Sis 900 PCI Fast Ethernet Adapter
    Adresse physique . . . . . : 00-0A-E4-46-2D-2A
    DHCP activé . . . . . : Oui
    Configuration automatique activée . . . . . : Oui
    Adresse IP. . . . . : 128.127.100.51
    Masque de sous-réseau : . . . . . : 255.255.0.0
    Passerelle par défaut . . . . . : 128.127.100.100
    Serveur DHCP. . . . . : 128.127.100.50
    Serveurs DNS . . . . . : 10.10.1.247
    Bail obtenu . . . . . : lundi 1 mars 2004 18:21:58
    Bail expirant . . . . . : lundi 8 mars 2004 18:21:58
```