



## IT Essentials 5.0

### Chapitre 6: Réseaux



**Speaker**

Cisco | Networking Academy®  
Mind Wide Open™



# Objectifs

- 6.1 Expliquer les principes des réseaux
- 6.2 Identifier les types de réseaux
- 6.3 Décrire technologies et concepts de base des réseaux
- 6.4 Décrire les composants matériels d'un réseau
- 6.5 Décrire les topologies des réseaux
- 6.6 Décrire Les normes ethernet
- 6.7 Explique les modèles de données (OSI et TCP/IP)
- 6.8 Décrire comment configurer et connecter un PC à un réseau
- 6.9 Choisir d'un type de connexion à un FAI
- 6.10 Techniques courantes de maintenance préventive pour les réseaux
- 6.11 Procédure de dépannage de base des réseaux



# Principes des réseaux

- Les réseaux sont des systèmes composés de liens
- Tout le monde utilise les réseaux suivants dans la vie quotidienne :

- ✓ Réseau postal
- ✓ Réseau téléphonique
- ✓ Réseau de transports publics
- ✓ Réseau informatique d'entreprise
- ✓ Internet



- Les ordinateurs peuvent être interconnectés via un réseau dans le but de partager les ressources matérielles ou des données.
- Un réseau peut être une simple connexion entre 2 PCs ou un peu plus complexe en interconnectant plus d'une centaines de PCs aux moyen de périphériques spécifiques en charge du contrôle du flux.d'information



# Réseaux Informatiques

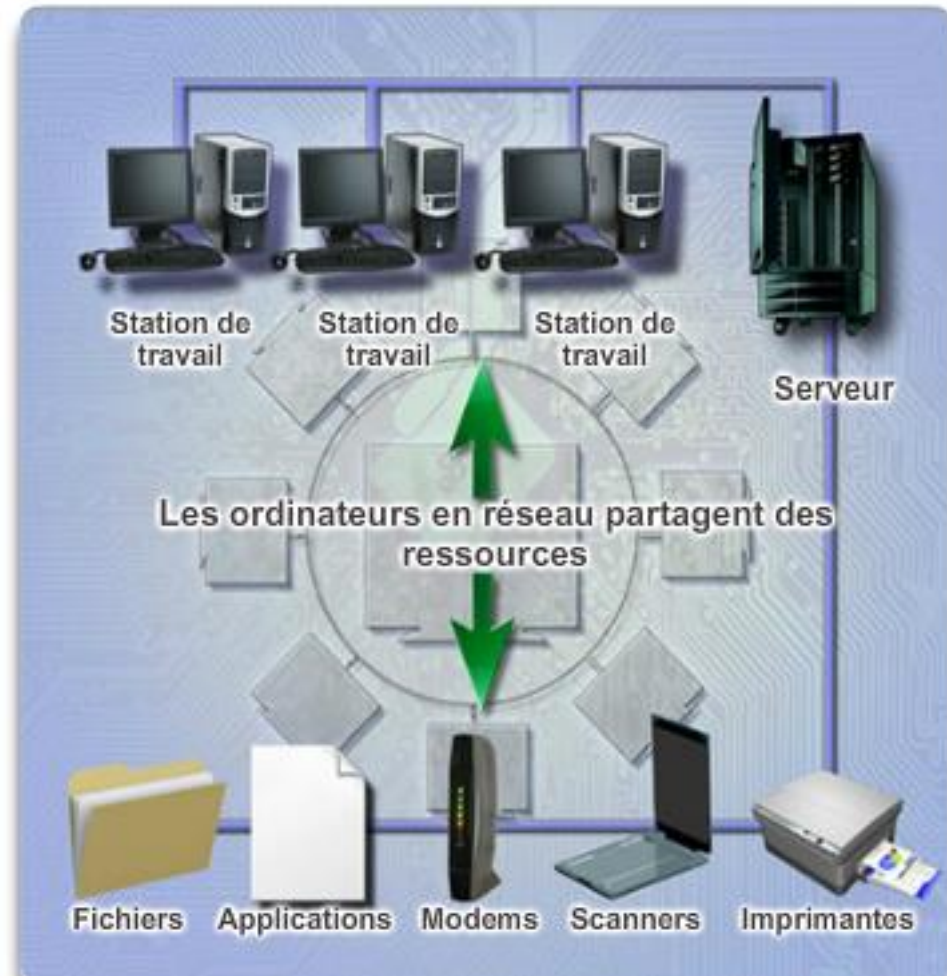
- Un réseau informatique représente un ensemble d'hôtes interconnectés via les périphériques réseaux tels que: ordinateurs, imprimante, scanners, smartphones, serveur d'impression et de fichier, électroménagers, etc.
- Les ressources partagées sur un réseau peuvent être de plusieurs types: Services, Supports de stockage, applications, documents,.
- Les périphériques réseau sont reliés entre eux via différentes connexions :
  - **Câblage en cuivre**
  - **Câblage en fibre optique**
  - **Connexion sans fil**
- Les avantages de la mise en réseau d'ordinateurs et d'autres périphériques incluent :
  - Moins de périphériques nécessaire
  - Éviter la duplication des données et mieux protéger les fichiers
  - Coût de licence moins élevé
  - Administration centralisée
  - Ressources préservées



# Réseaux Informatiques

## Partage des ressources

### ■ Exercice – 6.1.1.3





# Types de réseaux

Les réseaux de données évoluent en permanence en matière de complexité, d'utilisation et de conception. Un réseau informatique est ainsi identifié par les caractéristiques suivantes :

- **La zone qu'il dessert**
- **La façon dont les données sont stockées**
- **La manière dont les ressources sont gérées**
- **La manière dont le réseau est organisé**
- **Le type de périphériques réseau utilisés**
- **Le moyen utilisé pour connecter les périphériques**



# Types de réseaux

- **LAN (Local Area Network):** Un groupe d'ordinateurs interconnectés sous le contrôle d'un administrateur qui définit les règles d'accès et de la politique de sécurité appliquée sur le réseau.
- **WLAN (Wireless Local Area Network):** un groupe de périphériques sans fil se connectant à un point d'accès dans un espace bien défini. L'AP est généralement connecté au réseau via un câble à paire torsadée.
- **PAN (Personal Area Network):** Un réseau personnel relie des périphériques tels que des souris, des claviers, des imprimantes, des smartphones et des tablettes sur une portée très limitée, pour une seule personne. Les PAN utilisent généralement une connexion **Bluetooth (norme IEEE 802.15.1 | -10 mètres)**.





# Types de réseaux

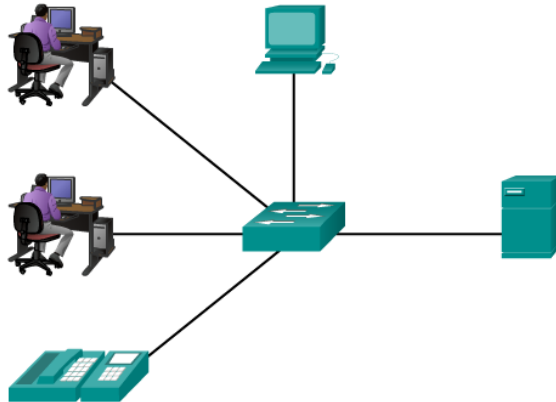
- **MAN (Metropolitan Area Network):** Un réseau métropolitain est un réseau qui couvre une vaste zone, comme un grand complexe ou une ville. Il comprend plusieurs bâtiments interconnectés en réseaux fédérateurs sans fil ou à fibres optiques.
- **WAN (Wide Area Network):** Un réseau étendu relie entre eux plusieurs réseaux plus petits (par exemple des réseaux locaux) situés sur des sites éloignés les uns des autres. L'exemple le plus courant de réseau étendu est Internet..



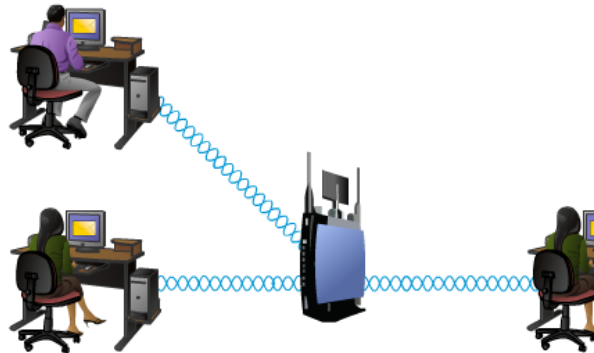


# Types de réseaux

Réseau local



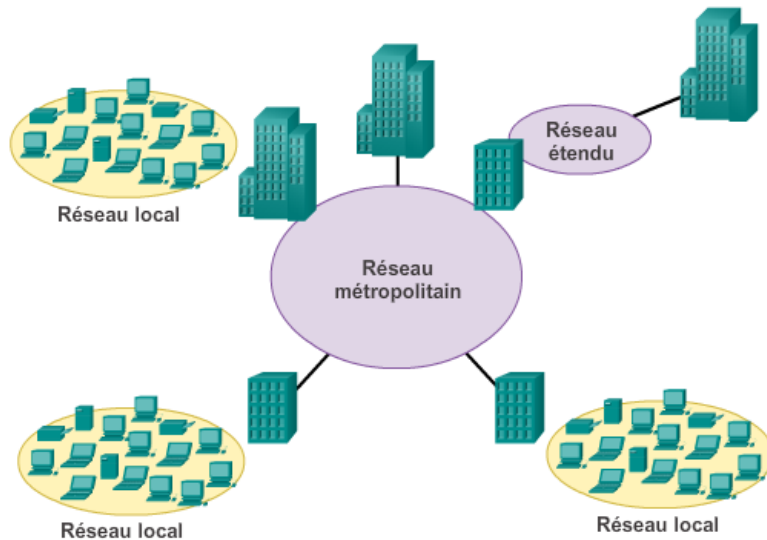
Réseau local sans fil



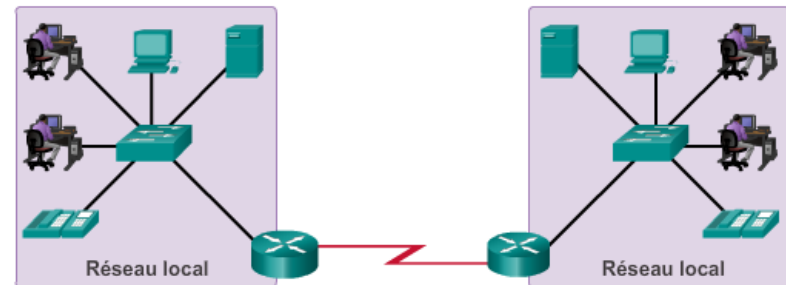
Réseau personnel



Réseau métropolitain



Réseau étendu

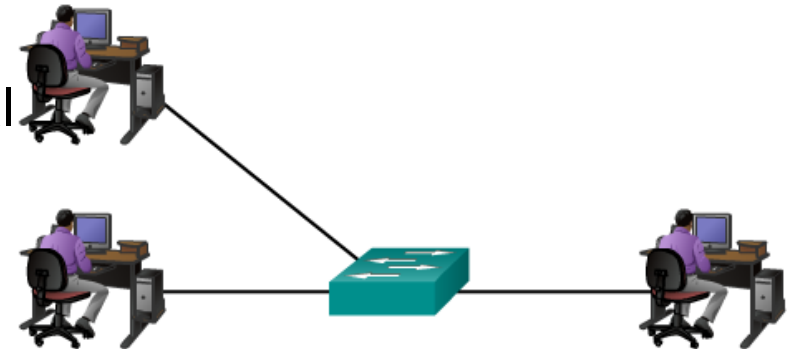




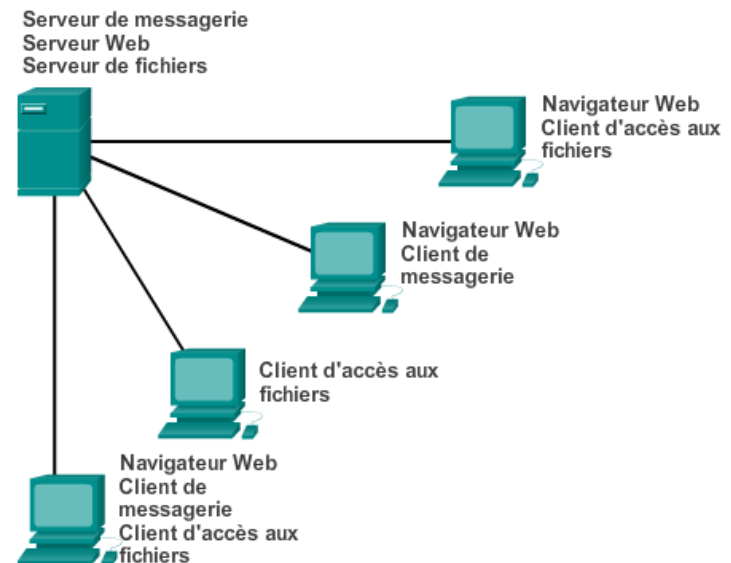
# Types de réseaux

- **Réseaux Peer-to-peer (P2P) :** Les périphériques sont connectés entre eux sans nul besoin d'un point central et chacun est maître de ses ressources qu'il décide de partager ou non.
- **Réseaux Client/serveur :** Dans ce modèle, nous avons 2 entités (Client demandeur de service et un serveur offreur de services). D'où l'existence d'un point central pour les échanges et l'implémentation de la politique de sécurité.
- **6.2.1.8 Exercice – Identification des types de réseau**

Réseau P2P



Réseau client/serveur





# Bande passante et Latence (Flux Données)

- **La bande passante** détermine le nombre de paquets pouvant être transmis sur une période donnée.
- La bande passante se mesure en bits par seconde ; sa valeur est généralement suivie par l'une des mesures suivantes :
  - bps - bits per second
  - Kbps - kilobits per second
  - Mbps - megabits per second
  - Gbps - gigabits per second
- **La latence** est le temps nécessaire aux données pour parcourir la distance séparant une source d'une destination. les données sont retardées par: **les périphériques réseau** et la **longueur des câbles**.
- Les données transmises sur le réseau circulent selon l'un des trois modes suivants :
  - **Mode unidirectionnel** Le mode unidirectionnel est une transmission simple, dans un seul sens ( *Le signal envoyé par une station de télévision à votre téléviseur*).
  - **Mode bidirectionnel non simultané:** En mode bidirectionnel non simultané, les données circulent dans un seul sens à la fois (*talkie-walkie*).
  - **Mode bidirectionnel simultané:** les données circulent dans les deux sens à la fois. La bande passante est mesurée uniquement dans un sens. (*Téléphone, et autres technologies Large bande*)



# Notion d'adressage

- Toute correspondance dans le monde commence par une identification atomique des entités désirantes échanger des informations. (Poste, numéro de téléphone, etc...)
- Dans l'univers des réseaux Informatiques, chaque hôte intervenant dans le réseau a besoin de 2 paramètres important.
  - ✓ **L'adresse MAC** (Medium Access Control) / Physique, Matérielle / Ethernet.
    - *L'adresse physique ne change pas, quel que soit l'emplacement de l'hôte sur le réseau;*
    - Les adresses MAC sont constituées de 48bits soit 6 groupes de 2 valeurs hexadécimales, séparés par un tiret (-) ou un double point (:), *Exple:* 00-26-6C-FC-D5-AF
    - Les valeurs hexadécimales sont composées de chiffres 0 et 9 ou de lettres de A à F;



# Adresse IP - IPV4

- Le protocole TCP/IP définit les règles que doivent suivre les ordinateurs pour communiquer entre eux sur Internet.
- Une adresse IP est un numéro utilisé pour identifier un périphérique situé sur un réseau. IPV4 est constituée de 32 bits regroupés en 4 octets séparés par des points. :
  - Example: 10111110.01100100.00000101.00110110
- Une adresse IPV4 peut aussi être représenté sous forme de **notation décimale pointé.**
  - Example: 190.100.5.54
- L'administrateur renseigne les paramètres IP sur un hôte sous la forme de notation décimal pointée. **Chaque adresse IP sur un réseau doit être unique.** L'adresse IP est **hiérarchique (Partie hôte et partie Réseau)**
- IP Classes
  - Class A: Large networks, implemented by large companies and some countries
  - Class B: Medium-sized networks, implemented by universities
  - Class C: Small networks, implemented by ISP for customer subscriptions
  - Class D: Special use for multicasting
  - Class E: Used for experimental testing



# Adresse IP - IPV4

## IPv4

Classe A	Réseau	Hôte		
Octet	1	2	3	4
Masque de sous-réseau par défaut	255	0	0	0
Plage d'adresses IP :	de 1.0.0.0 à 126 255 255 255			
Hôtes par réseau	$2^{24}-2=16\ 777\ 214$			

Classe B	Réseau		Hôte	
Octet	1	2	3	4
Masque de sous-réseau par défaut	255	255	0	0
Plage d'adresses IP :	de 128.0.0.0 à 191.255.255.255			
Hôtes par réseau	$2^{16}-2=65\ 534$			

Classe C	Réseau			Hôte
Octet	1	2	3	4
Masque de sous-réseau par défaut	255	255	255	0
Plage d'adresses IP :	de 192.0.0.0 à 223 255 255 255			
Hôtes par réseau	$2^8-2=254$			

Les adresses de Classe D sont utilisées pour les groupes de multidiffusion, comme des émissions Web ou de la vidéo diffusée en continu vers un groupe spécifique. Les adresses de Classe E sont uniquement utilisées à des fins expérimentales.



# IP Addressing – IPV4

- L'IETF a réservé certains espaces d'adressage Internet pour les réseaux privés.
- Les réseaux privés ne sont pas reliés aux réseaux publics.
- Les adresses réseau privées ne sont pas acheminées sur Internet.
- **Classe A** - 10.0.0.0 à 10.255.255.255
- **Classe B** - 172.16.0.0 à 172.31.255.255
- **Classe C** - 192.168.0.0 à 192.168.255.255





# Notion de Masque de sous-réseau

- Le masque de sous-réseau est utilisé pour indiquer la partie de réseau correspondant à une adresse IPv4.
- Tous les hôtes d'un réseau local utilisent généralement le même masque de sous-réseau
- les masques de sous-réseau par défaut correspondant aux adresses IPv4 sont:
  - **255.0.0.0** - Classe A, qui indique que le premier octet de l'adresse IPv4 correspond à la partie réseau.
  - **255.255.0.0** - Classe B, qui indique que les deux premiers octets de l'adresse IPv4 correspondent à la partie réseau.
  - **255.255.255.0** - Classe C, qui indique que les trois premiers octets de l'adresse IPv4 correspondent à la partie réseau.



# Adresse IP – IPV6

- Adresse IPv6 - 128 bits ou 32 valeurs hexadecimal.

Les 32 valeurs hexadécimales sont ensuite divisées en huit groupes de quatre valeurs hexadécimales, séparés par le symbole : (deux-points). Chaque groupe de 4 = **Bloc**

- Les adresses IPv6 ont une hiérarchie à 3 niveaux:
  - **Le préfixe global**, également appelé préfixe de site, correspond aux trois premiers blocs de l'adresse..
  - **L'ID de sous-réseau**, correspond au quatrième bloc de l'adresse.
  - **L'ID d'interface**, est quant à lui composé des quatre derniers blocs de l'adresse..L'administrateur réseau contrôle à la fois *l'ID de sous-réseau* et *l'ID d'interface*.

Address Hierarchy	Global Prefix	Subnet ID	Interface ID
IPv6 Address	3ffe:6a88:85a3:	08d3:	1319:8a2e:0370:7344



# Abréviation d'une Adresse IPV6

- Une adresse IPv6 peut être abrégée en appliquant les règles suivantes :
  - ✓ **Les zéros au début d'un groupe de 16 bits peuvent être omis.**
  - ✓ **Un groupe uniquement constitué de zéros peut être remplacé par deux doubles points.**

Abréviation des adresses IPv6

Règles d'abréviation des adresses IPv6									
Adresse	2001	:	0db8	:	0000	:	0000	:	0000 : 0000 : 1428 : 57ab
Après application de la première règle	2001	:	db8	:	0	:	0	:	0 : 0 : 1428 : 57ab
Après application de la deuxième règle	2001	:	db8	:		:		:	1428 : 57ab
Les adresses sont représentées ci-dessous :									
Adresse	2001:0db8:0000:0000:0000:0000:1428:57ab								
Après application de la première règle	2001:db8:0:0:0:0:1428:57a								
Après application de la deuxième règle	2001:db8::1428:57ab								



# Exercices d'application sur IPV6

- 1- Quels sont les différentes parties d'une adresse IPV6?
- 2- Identifier les 3 parties de l'adresse IPV6 suivante:  
3ffe:6a88:85a3:08d3:1319:8a2e:0370:7344
- 3- Utiliser les techniques d'abréviations pour réduire l'adresse IPV6 suivante  
2001:0db8:0000:0000:0000:0000:1408:0100





# Attribution des paramètres IP aux hôtes

## Configuration d'une adresse IP statique



- **Adressage IP statique.**
- **Adressage IP Dynamique via le protocole DHCP.**
- Le Serveur DHCP peut assignés les paramètres IP suivants à un hôte:
  - Adresse IP
  - Masque de sous-réseau
  - Passerelle par défaut
  - Valeurs facultatives (Adresse des serveurs DNS).

**Question: Que se passe t-il si le serveur DHPC ne répond pas alors que l'hôte est configuré pour un adressage dynamique?**



# Internet Control Message Protocol (ICMP)

- Le protocole ICMP (**Internet Control Message Protocol**) est utilisé par les périphériques d'un réseau pour envoyer des messages d'erreur et de contrôle aux ordinateurs et aux serveurs.
- **PING (Packet Internet Groper)**; Cette cmde est couramment utilisée pour tester les connexions entre les ordinateurs.
  - Très utile, pour déterminer si une adresse IP spécifique est accessible
  - Peut être utiliser avec soit l'adresse IP ou le nom de la machine.
  - Fonctionne en envoyant demande de renvoie(Echo) à l'ordinateur de destination; le périphérique de destination répond en envoyant des paquets de réponses.
- La commande **ipconfig** est un autre utilitaire en ligne de commande très utile, qui permet de vérifier qu'une carte réseau a une adresse IP valide.
- Quatre demandes « echo » ICMP (ping) sont envoyées à l'ordinateur de destination. S'il est joignable, cet ordinateur envoie en retour quatre réponses « echo » ICMP.
- **Le pourcentage de réponses reçues** peut vous aider à déterminer la fiabilité et l'accessibilité de l'ordinateur de destination.



# Travaux pratiques

- TP a Faire: 6.3.2.7, 6.3.2.8, 6.3.2.9, 6.3.2.10)
- Planifier un TP sur l'utilisation de Packet Tracer avec les apprenants en s'inspirant du fichier d'utilisation sur la plate forme de lecture de cours en local. Chapitre 3 – CCNA Discovery





# Ports et Protocoles courants

- **Un protocole** est un ensemble de règles. Les protocoles Internet sont des ensembles de règles qui régissent les communications au sein des ordinateurs d'un réseau et entre eux.
- Les spécifications de protocole définissent le format des messages échangés. Une lettre envoyée par voie postale utilise également des protocoles.
- Les périphériques et ordinateurs connectés à Internet utilisent une **suite de protocoles appelée TCP/IP** pour communiquer entre eux.
- Voici les principales fonctions des protocoles :
  - **Détection et traitement des erreurs**
  - **Compression des données**
  - **Sélection de la méthode de division des données et de création de packages de données**
  - **Adressage des paquets de données**
  - **Sélection de la méthode de communication de l'envoi et de la réception des paquets de données**



# Comparaison entre TCP et UDP

- Les informations sont transmises le plus souvent en suivant deux protocoles : TCP et UDP.

TCP	Protocole UDP
<p>Avantages :</p> <p>Détection des erreurs : TCP retransmet les paquets perdus, met de côté les doublons et garantit la transmission des données dans l'ordre approprié.</p> <p>Reliable Transport Protocol (Protocole de transport fiable) : TCP surveille les données pour garantir leur transmission.</p>	<p>Avantages :</p> <p>Moins de surcharge : utilise moins de bande passante que TCP.</p> <p>Sans négociation préalable : le destinataire des données ne doit pas forcément être disponible et prêt à recevoir les données. Il n'a pas non plus à accuser réception des données.</p>
<p>Applications :</p> <p>Messagerie</p> <p>Navigateur Web</p>	<p>Applications :</p> <p>Simple File Transfer : envoi des données sans dispositif de sécurité et ne requiert pas d'accusé de réception.</p> <p>Network File System : système pour accéder aux fichiers sur un réseau, similaire à un accès local aux données.</p>

## Exercice: 6.3.3.2 – TCP et UDP



# Ports et protocoles TCP et UDP

- **Un port** est un identifiant numérique utilisé pour garder une trace de conversations spécifiques. Chaque message envoyé par un hôte contient un **port source** et un **port de destination**..

Protocoles réseau les plus courants et ports associés		
Protocole	Port	Description
TCP/IP	N/D	Suite de protocoles utilisée pour transporter des données sur Internet
NetBEUI/NetBIOS	137, 139, 150	Petit protocole rapide conçu pour un réseau de type groupe de travail qui ne requiert aucune connexion à Internet
HTTP	80	Protocole de communication qui établit une connexion de type question/réponse sur Internet
HTTPS	443	Utilise l'authentification et le chiffrement pour sécuriser les données pendant leur transfert entre le client et le serveur Web
FTP	20/21	Fournit des services de transfert et de traitement de fichiers
SSH	22	Se connecte à un périphérique réseau à distance de façon sécurisée
Telnet	23	Se connecte à un périphérique réseau à distance
POP3	110	Télécharge des e-mails à partir d'un serveur de messagerie
IMAP	143	Télécharge des e-mails à partir d'un serveur de messagerie



# Rafraîchissement Mémoire

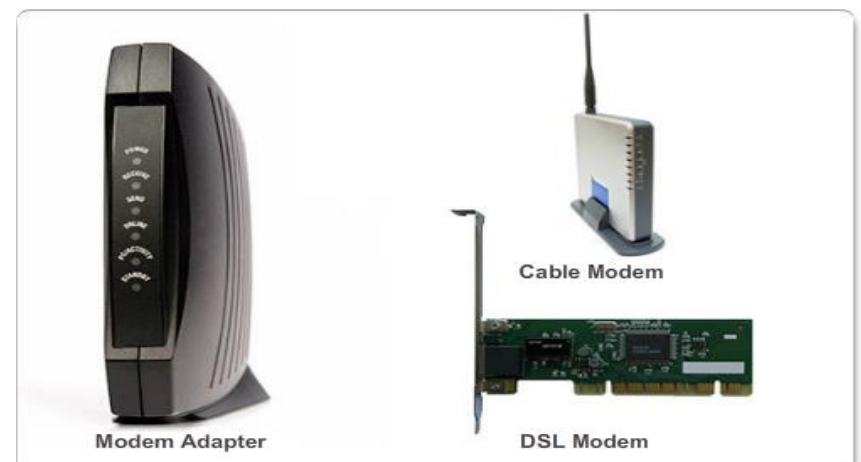


# **PARTIE 2: Composants matériels d'un réseau, Topologies et Normes**



# Périphériques réseaux

- Un **modem** est un dispositif électronique qui se connecte à Internet en passant par un FAI. DUN (Dial-Up Networking)
- Le modem convertit des données numériques en signaux analogiques afin de les transmettre sur le réseau téléphonique. **Un modem interne** s'installe dans un slot d'extension de la carte mère.
  - Les modems externes se connectent à l'ordinateur via les ports série et USB.





# Périphériques réseaux

## ■ Network devices:

- Ordinateurs
- Concentrateurs
- Commutateurs
- Routeurs
- Access Point

## ■ Média Réseau:

- La paire torsadée
- Fibre Optique
- Ondes Radio







# Périphériques réseaux

## ■ Hub / Concentrateur

- Les concentrateurs permettent d'étendre la portée du réseau en recevant des données sur un port, puis en les régénérant et en les envoyant à tous les autres ports.
- Les concentrateurs sont moins courants aujourd'hui car génèrent facilement des collisions.

## ■ Ponts et commutateurs

- Un **Pont** filtre le trafic réseau sur différents segments du réseau local.
- Lorsque le pont reçoit une trame, il examine l'adresse de destination afin de déterminer si la trame doit être envoyée à un autre segment ou abandonnée.
- Un commutateur (pont multiports) possède plusieurs ports et se sert d'une table d'adresse Mac pour déterminer l'hôte de destination d'une trame.

## • Power over Ethernet (PoE)

- Un commutateur PoE transfère de petites quantités de courant continu via le câble Ethernet, parallèlement aux données, pour alimenter les périphériques PoE (*points d'accès Wi-Fi, les périphériques de vidéosurveillance et les cartes réseau*).



# Périphériques réseaux

## ▪ Routeurs / ISR

- Les routeurs relient les réseaux les uns aux autres. Les routeurs utilisent les adresses IP pour transférer des paquets vers d'autres réseaux.
- Un routeur peut être un ordinateur équipé d'un logiciel réseau spécifique ou un périphérique conçu par des fabricants d'équipement réseau.
- Les routeurs gèrent les tables de routage avec les algorithmes pour calculer et stocker les meilleures routes vers les différentes destinations.

## ▪ Wireless Access Points (WAP)

- procurent l'accès réseau à des périphériques sans fil tels que des ordinateurs portables, smartphones et des tablettes.
- utilise les ondes radio pour communiquer avec les cartes réseau sans fil des périphériques et les autres points d'accès sans fil.
- Un point d'accès a une portée (couverture) limitée.



# Périphériques réseaux

## ■ Périphériques Multifonctions (ISR)

- Joue plusieurs rôles à la fois;
- Il est en effet plus pratique d'acheter et de configurer un seul périphérique qui répondra à tous vos besoins plutôt qu'un équipement pour chaque fonction.
- Le routeur sans fil sert de passerelle domestique, de point d'accès sans fil et de commutateur.
- Le routeur Linksys E2500 / WRT150N sont des exemples de périphériques multifonctions.



# Périphériques réseaux

## Network-attached storage (NAS)

- Composé d'un ou de plusieurs disques durs, d'une connexion Ethernet et d'un système d'exploitation intégré
- Il se connecte au réseau, ce qui permet aux utilisateurs d'accéder aux fichiers et de les partager, de diffuser du contenu et de sauvegarder des données à un emplacement centralisé.





# Périphériques réseaux

- **téléphones VoIP** - permet de faire transiter les appels téléphoniques sur des réseaux de données et sur Internet..
- **Hardware firewalls** - protègent les données et l'équipement d'un réseau contre les accès non autorisés. Un pare-feu matériel est un dispositif autonome qui se place entre les réseaux.
- **Appareils Internet**— certains modèles de télévisions, consoles de jeux, lecteurs Blu-ray et lecteurs multimédias.
- **Achat des périphériques réseaux authentiques** - Suivez ces conseils au moment de passer une commande ou lorsque vous demandez des devis pour être sûr que vous obtiendrez des produits authentiques.



# Produits authentiques

- Achetez toujours votre équipement directement chez des distributeurs autorisés.
- Vérifiez que l'équipement est un produit neuf
- Soyez méfiant lorsque les prix sont anormalement bas.
- Le produit est proposé avec une remise beaucoup plus importante que les produits authentiques.

Authentique



Contrefaçon



Les différences visuelles entre un produit authentique et un produit contrefait peuvent être extrêmement subtiles, voire indétectables.



# Connecteurs et câbles

- Une grande variété de câbles de mise en réseau est disponible sur le marché
- Les câbles coaxiaux et à paires torsadées utilisent du cuivre pour transmettre les données
- Les câbles en fibre optique utilisent du verre ou du plastique
- Ces câbles diffèrent en termes de **bande passante**, de **taille** et de **coût**.
- Un réseau filaire est généralement plus sûr qu'un réseau sans fil.
- De nombreuses entreprises choisissent d'installer dès le départ des câbles de très grande qualité
- Une solution sans fil peut être nécessaire si l'installation de câbles est impossible

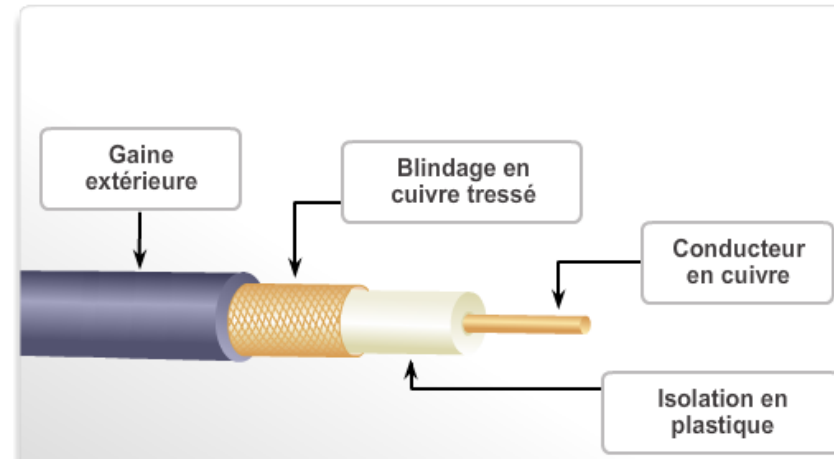




# Cable Coaxial

- Les câbles coaxiaux sont entourés d'une gaine
- Il existe plusieurs types de câbles coaxiaux :
  - **Ethernet épais ou 10BASE5** : câble coaxial utilisé sur les réseaux et fonctionnant à 10 Mbit/s, sur une longueur maximum de 500 mètres.
  - **Ethernet fin ou 10BASE2** : câble coaxial utilisé sur les réseaux et fonctionnant à 10 Mbit/s, sur une longueur maximum de 185 mètres.
  - **RG-59** : câble principalement utilisé pour la télévision câblée aux États-Unis
  - **RG-6** : câble de meilleure qualité que le RG-59, avec une bande passante supérieure et moins de sensibilité aux interférences

Éléments d'un câble coaxial



Connecteurs coaxiaux

Connecteurs coaxiaux



Une prise BNC

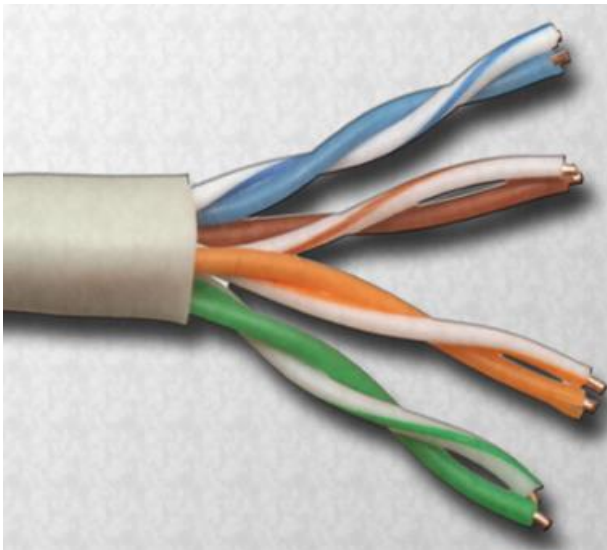


Type F



# Cable à paire torsadée

- Ils se composent de paires de fils qui forment un circuit capable de transmettre les données. .
- Chaque paire est torsadée afin d'offrir une protection contre les interférences.
- Les paires de fils en cuivre sont recouvertes d'un plastique isolant coloré (code couleur) et sont elles-mêmes torsadées.



- Une gaine extérieure protège le faisceau de paires torsadées.
- Il existe deux principaux types de câble à paires torsadées :
  - **Câbles à paires torsadées non blindées (UTP)** (Cat 3, Cat 5, 5e, Cat 6 and Cat 7)
  - **Câbles à paires torsadées blindées (STP)**



# Cable à fibre Optique

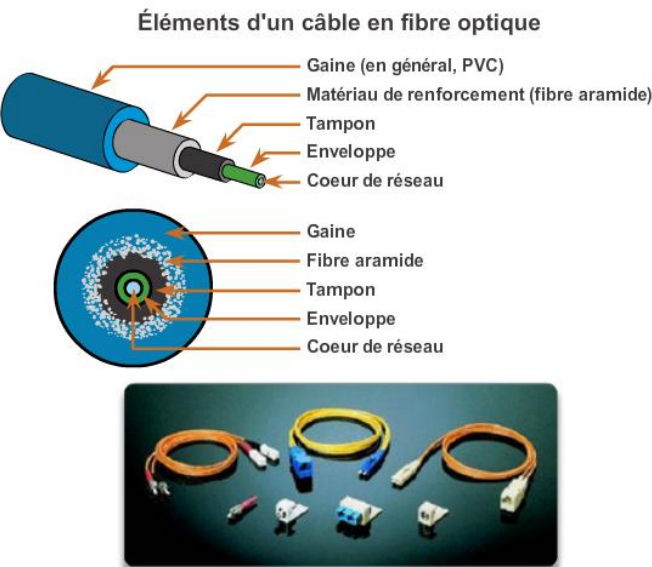
- Une fibre optique est un support en verre ou en plastique qui transmet les informations par le biais de la lumière.

Ne sont pas affectés par les perturbations électromagnétiques ou radioélectriques.

les câbles à fibres optiques peuvent transmettre des signaux plus clairs, plus loin et avec une meilleure bande passante que les câbles en cuivre ou en autre métal.

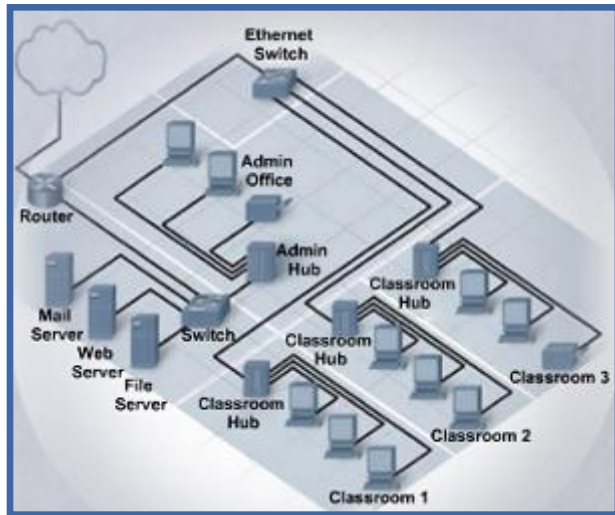
Des **lasers** ou des **diodes électroluminescentes** (LED ou DEL)

- Ces dispositifs sont généralement plus coûteux que les câbles en cuivre, les connecteurs également ; ceux-ci sont également plus difficiles à assembler..
- Il existe deux types de câble à fibres optiques :

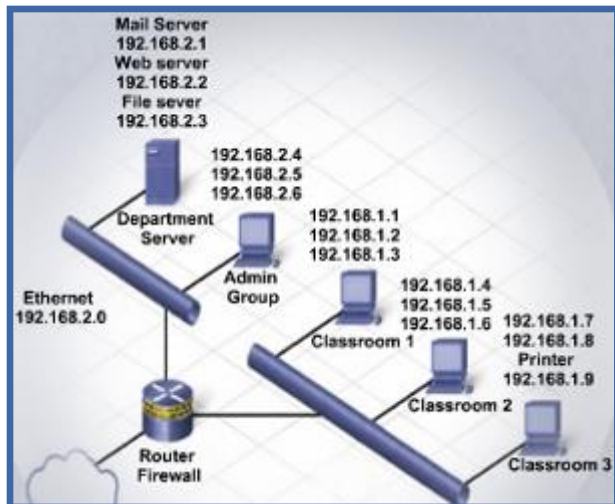




# Topologies des réseaux



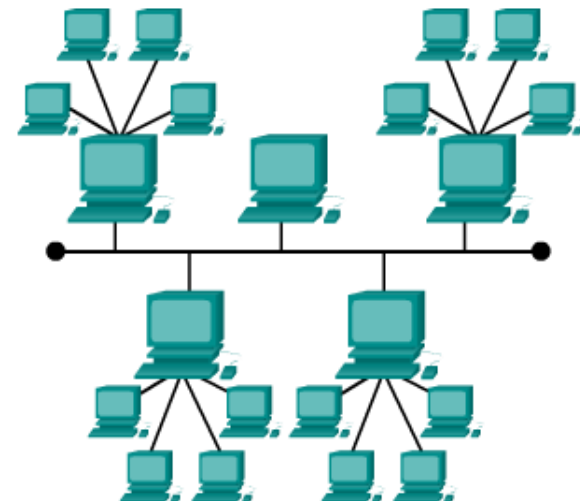
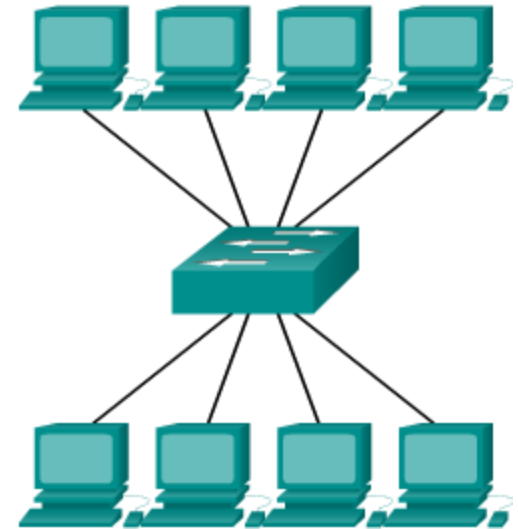
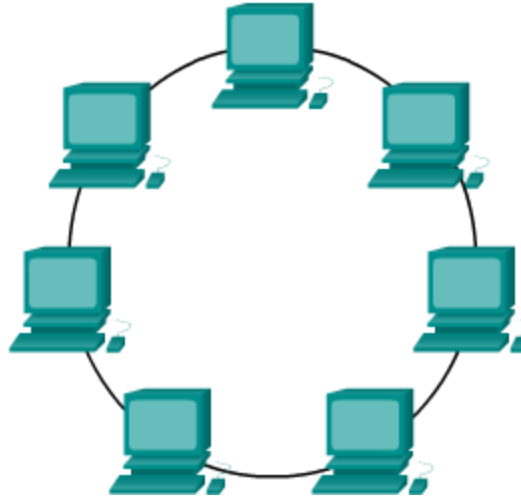
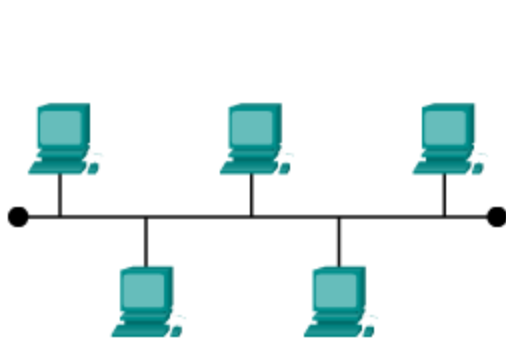
**Topologie physique** définit la manière dont les ordinateurs, les imprimantes et les autres périphériques sont connectés au réseau.



**Topologie logique** La topologie logique décrit comment les hôtes accèdent au support et communiquent sur le réseau..



# Topologie physique





# Logical Topologies

- Les deux types de topologies logiques les plus courants sont la **diffusion** et le **passage de jeton**.
  - **Topologie à diffusion** un hôte diffuse un message à tous les hôtes du même segment réseau. Les hôtes n'ont pas à suivre un ordre particulier pour transmettre des données. Les messages sont envoyés selon la méthode du premier entré, premier sorti.
  - **Passage de jeton** chaque hôte reçoit tour à tour un jeton électronique, ce qui permet de contrôler l'accès au réseau. L'hôte de destination récupère les données dans la trame. Si un hôte n'a pas de données à envoyer, le jeton passe à un autre hôte ainsi de suite.





# Bonne pratiques dans le câblage réseau

- Les facteurs importants suivants doivent être évoqués avec le client concernant le choix du réseau :
  - ✓ Normes de câblage et de réseaux sans fil
  - ✓ Évolutivité
  - ✓ Nombre d'utilisateurs et situation géographique
- Une évaluation de site consiste en une inspection matérielle du bâtiment permettant de choisir une topologie physique de base.
  - ✓ Emplacement des ordinateurs du client
  - ✓ Emplacement des équipements réseau, tels que les commutateurs et les routeurs
  - ✓ Emplacement des serveurs
- Un plan d'étage ou un schéma d'ensemble est très utile pour déterminer la disposition physique des équipements et du câblage.
- Si aucun plan d'étage ou schéma d'ensemble n'est disponible, réalisez vous-même un dessin indiquant l'emplacement des futurs périphériques réseau



# LES NORMES

	Name	Type	Standards	Established
ITU-T	ITU Telecommunication Standardization Sector (formerly CCITT)	one of the three Sectors of the International Telecommunication Union	Standards covering all fields of telecommunications	Became ITU-T in 1992
IEEE	Institute of Electrical and Electronics Engineers	A but non lcrative en charge de l'élaboration des norme info et electro	A but non lcrative en charge de l'élaboration des norme info et electro	1884
ISO	International Organization for Standardization	Elaboe les normes informatiques, standards institutes of 157 countries	Promote the development of international standards agreements	1947
IAB	Internet Architecture Board	Comité chargé de superviser le développement technique et structurel d'Internet	Oversees the technical and engineering development of the Internet	1979; first named ICCB
IEC	International Electrotechnical Commission	Global organization	Standards for all electrical, electronic, and related technologies	1906
ANSI	American National Standards Institute	Private, non-profit organization	Seeks to establish consensus among groups	1918
TIA/EIA	Telecommunications Industry Association / Electronic Industries Alliance	Trade associations	Standards for voice and data wiring for LANs	After the deregulation of the U.S. telephone industry in 1984





# Ethernet Standards

- Les normes permettent de garantir **la compatibilité entre périphériques de différents fabricants**, grâce à l'utilisation de technologies communes.
- Les protocoles Ethernet décrivent les règles qui régissent les communications sur un réseau Ethernet.
- L'architecture Ethernet est basée sur la norme **IEEE 802.3**. Celle-ci spécifie qu'un réseau doit utiliser la méthode de contrôle d'accès **CSMA/CD** (accès multiple avec écoute de porteuse et détection des collisions).
- Avec cette méthode, toutes les stations d'extrémité « **écoutent** » le câble réseau pour savoir quand elles sont autorisées à envoyer des données. Lorsque la station d'extrémité détecte qu'aucun autre hôte n'est en cours de transmission, elle tente à son tour d'envoyer ses données
- La première station qui détecte la **collision** (ou le doublement de tension qui en résulte) envoie un **signal de bourrage** qui indique à toutes les stations d'arrêter de transmettre et d'exécuter un **algorithme de réémission temporisée**.



# La norme Ethernet

## ■ 10BASE-T

- est une technologie Ethernet qui utilise la topologie en étoile.
- « **10** » représente un débit de 10 Mbit/s.
- Le terme **BASE** indique une transmission en bande de base. Avec ce type de transmission, la totalité de la bande passante d'un câble est utilisée pour un seul type de signal.
- Le **T** indique un câblage en cuivre à paires torsadées

Normes Ethernet		
Normes Ethernet	Supports	Débits de transfert
10BASE-T	Catégorie 3	Transfert de données à un débit de 10 Mbit/s
100BASE-TX	Catégorie 5	Débit de 100 Mbit/s soit dix fois plus élevé que pour les câbles 10BASE-T
1000BASE-T	Catégories 5 et 6	Prend en charge des débits de transfert de données de 1 Gbit/s
10GBASE-T	Catégories 6a et 7	Prend en charge des débits de transfert de données de 10 Gbit/s



# Normes Ethernet sans fil

- **IEEE 802.11** définit la connectivité des réseaux sans fil..
- **Wi-Fi** (wireless fidelity), fait référence à un ensemble de normes sans fil:
  - **802.11** (the original specification)
  - **802.11a**
  - **802.11b**
  - **802.11g**
  - **802.11n**
- Ces protocoles spécifient les fréquences, les vitesses et autres fonctionnalités des différentes normes Wi-Fi.



# Normes Ethernet sans fil

	Bandwidth	Frequency	Range	Interoperability
<b>802.11a</b>	Up to 54 Mbps	5 GHz band	152 feet (45 meters)	Not interoperable with 802.11b, 802.11g, or 802.11n
<b>802.11b</b>	Up to 11 Mbps	2.4 GHz band	303 feet (91 meters)	Interoperable with 802.11g
<b>802.11g</b>	Up to 54 Mbps	2.4 GHz band	303 feet (91 meters)	Interoperable with 802.11b
<b>802.11n</b>	Up to 540 Mbps	2.4 GHz band	820 feet (250 meters)	Interoperable with 802.11b and 802.11g
<b>802.15.1 Bluetooth</b>	Up to 2 Mbps	2.4 GHz band or 5 GHz band	30 feet (10 meters)	Not interoperable with any other 802.11



# Modèles de données / Architectural

- Un **modèle architectural** est un cadre de référence commun servant à expliquer les communications Internet et à développer des protocoles de communication.
- Il **sépare les fonctions des protocoles** en **couches distinctes** pouvant être gérées individuellement.
- Chaque **couche a une fonction spécifique** dans la communication réseau.
- On distingue deux modèles de données:
  - ✓ **Le modèle OSI**
  - ✓ **Le modèle TCP/IP**
- ✓ Le modèle TCP/IP a été créé par des chercheurs du Ministère de la Défense des États-Unis.



# Le modèle de référence TCP/IP

- **La suite de protocoles TCP/IP** est la norme principale pour le transfert de données sur les réseaux et Internet.
- Il se compose **quatre (04) de différentes couches**, qui exécutent les fonctions nécessaires pour préparer les données à une transmission sur le réseau.

	Description	Protocoles
Application	Fournissent des services réseau aux applications des utilisateurs	HTTP, HTML, Telnet, FTP, SMTP, DNS
Transport	Précise l'application qui demande ou reçoit des données par le biais des ports spécifiques.	TCP, UDP
Internet	Utilisés pour assurer la connectivité entre les hôtes d'un réseau. L'adressage IP et le routage ont lieu ici	IP, ICMP, RIP, ARP
Accès réseau	Contient l'adressage MAC et les composants physique du réseau	Ethernet



# Le modèle OSI

- Le modèle OSI sépare les communications réseau en sept couches distinctes..
- Destiné à normaliser la manière dont les périphériques communiquent sur un réseau.
- Bien qu'il existe d'autres modèles, la plupart des fournisseurs de solutions réseau actuels conçoivent leurs produits sur la base de ce cadre.
- Une « **pile de protocoles** » est un système qui met en œuvre une gestion des protocoles en les implémentant dans la série des couches.
  - Les piles de protocoles peuvent être implémentées au niveau logiciel ou matériel, ou les deux.
  - Généralement, seules les couches basses du modèle sont implémentées au niveau matériel, tandis que les couches supérieures sont implémentées au niveau logiciel.
  - Le processus **d'encapsulation** démarre à la couche Application



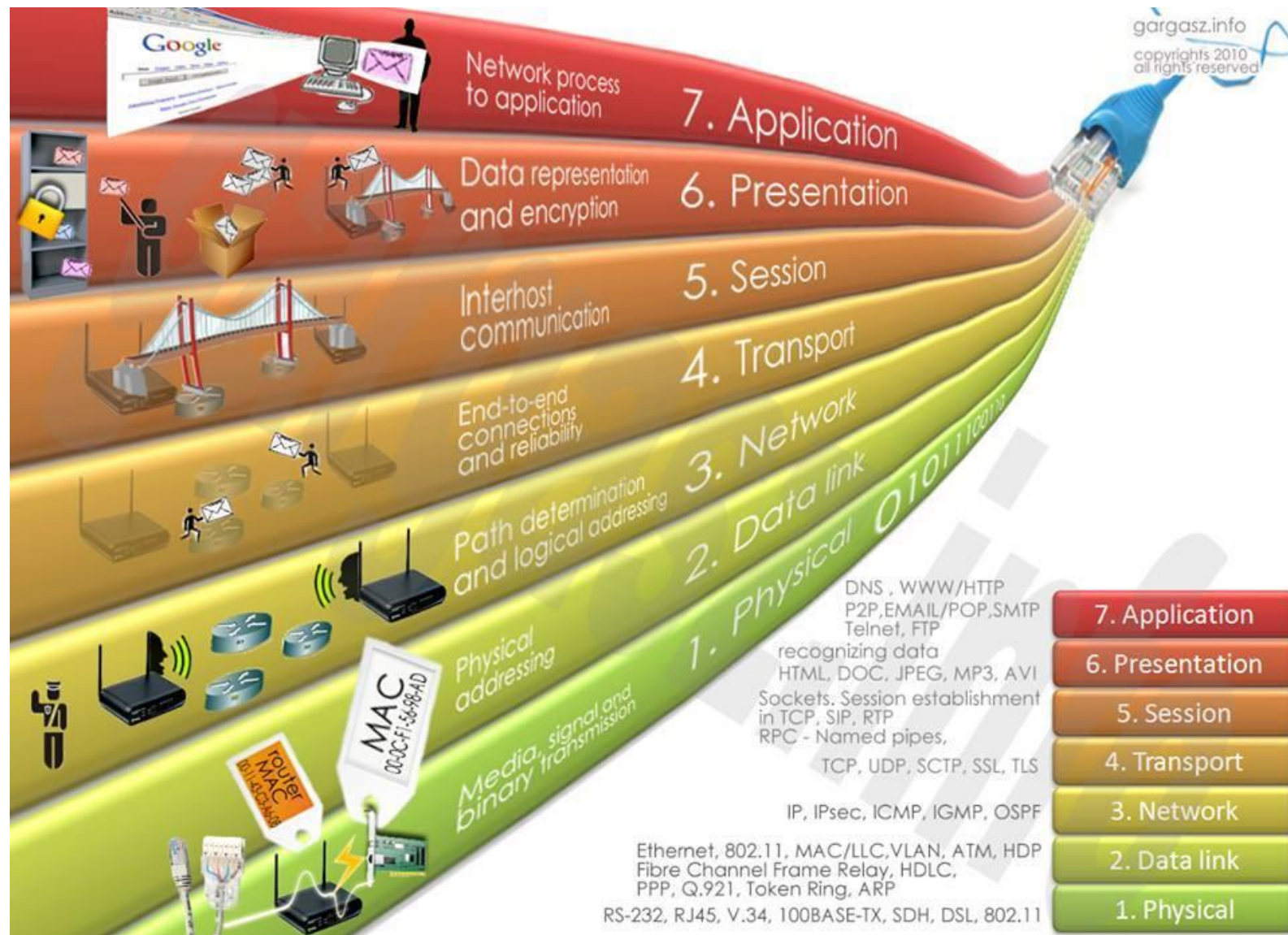
# Le modèle OSI

Modèle OSI		
Modèle OSI	Couche	Description
Application	7	Responsable des services réseau pour les applications
Présentation	6	Transforme les formats de données pour fournir une interface standard à la couche Application
Session	5	Établit, gère et interrompt les connexions entre l'application locale et distante
Transport	4	Propose un transport fiable et un contrôle de flux sur tout un réseau
Réseau	3	Responsable de l'adressage logique et du domaine de routage
Liaison de données	2	Propose des procédures d'adressage physique et d'accès au support
Physique	1	Définit toutes les spécifications électriques et physiques des équipements

moyens mnémotechniques pour vous aider à mémoriser les sept couches

" **A**près **P**lusieurs **S**emaines **T**out **R**espirait **L**a **P**aix "

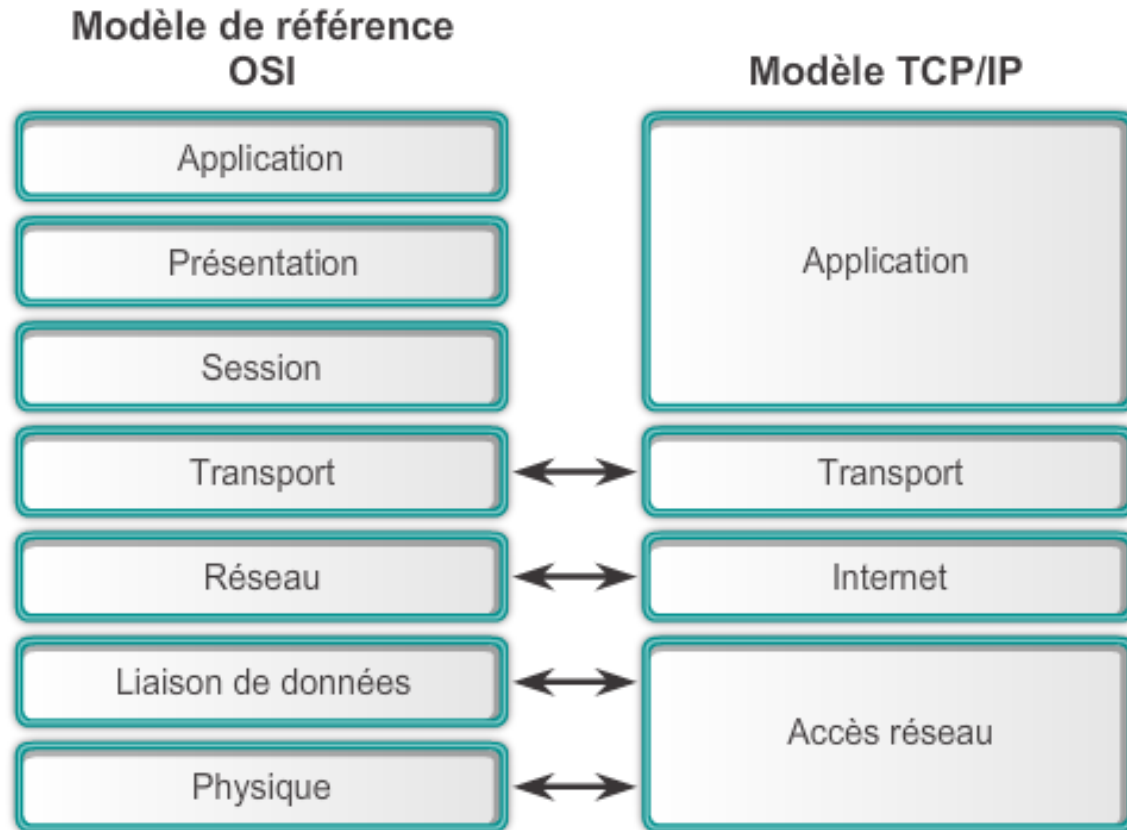






# Comparaison des modèles OSI et TCP/IP

## Comparaison des modèles OSI et TCP/IP



## Exercice 6.7.1.4 – Correspondances entre le OSI et TCP/IP



# Rafraîchissement Mémoire



## PARTIE 3:

# Mise en réseau, choix d'un FAI et procédures de maintenance



# Etape d'installation d'un réseau

- **Étape 1.** Assurez-vous que tous les emplacements des prises Ethernet murales sont signalés et qu'ils correspondent aux attentes du client.  
« la norme TIA/EIA 606-A »
- **Étape 2.** Une fois les câbles terminés à chaque extrémité, utilisez un testeur de câble pour vous assurer qu'il n'y a pas d'interférences ni de courts-circuits.
- **Étape 3.** Servez-vous du plan d'étage pour trouver l'emplacement idéal des points d'accès, de façon à avoir une couverture optimale.
- **Étape 4.** Connectez le point d'accès au réseau existant.
- **Étape 5.** Assurez-vous que les interfaces réseau sont correctement installées au niveau des terminaux du réseau.
- **Étape 6.** Faites en sorte de placer les commutateurs et les routeurs dans un endroit central et protégé.
- **Étape 7.** Installez un câble de raccordement Ethernet entre la prise murale et chaque périphérique réseau.
- **Étape 8.** Lorsque tous les périphériques sont connectés et les voyants allumés, testez la connectivité du réseau.

# Choix de la carte réseau

- La plupart des interfaces réseau pour ordinateur de bureau sont intégrées à la carte mère ou c'est une carte d'extension qui se place dans un slot d'extension.
- La plupart des interfaces réseau pour ordinateur portable sont intégrées à la carte mère ou c'est une **carte PC** ou **ExpressBus** qui se place dans un slot d'extension.
- Les **cartes réseau USB** peuvent se brancher sur un port USB et s'utilisent à la fois sur les ordinateurs portables et de bureau.

Choix de la carte réseau





# Installation et Mise à niveau d'une NIC

- Pour installer une carte réseau sans fil sur un ordinateur de bureau, vous devez retirer le capot du boîtier
- Parfois, le fabricant publie un nouveau pilote logiciel pour une carte réseau.
  - améliorer les fonctionnalités de la carte
  - assurer la compatibilité avec le système d'exploitation.
- Lors de l'installation d'un nouveau pilote, désactivez le logiciel de protection antivirus afin que le pilote s'installe correctement.
- **Démarrer > Panneau de configuration > Gestionnaire de périphériques**
- Si le nouveau pilote de la carte réseau ne fonctionne pas correctement après installation, vous pouvez le désinstaller ou réutiliser la version précédente

**TP 6.8.2.4 et 6.8.2.6– Installation d'une carte réseau sans fil sous Windows7 et XP**





# Configuration d'un Carte réseau

- Chaque carte réseau doit être configurée avec les informations suivantes :
  - **Protocoles**
  - **Adresse IP**
  - **Adresse MAC**
- Le paramétrage d'une **configuration IP alternative** sous Windows simplifie le passage d'un réseau nécessitant l'utilisation d'un serveur DHCP à un réseau utilisant des paramètres IP statiques.
- **l'adresse APIPA** est attribuée à un hôte lorsque le serveur DHCP est indisponible.





# Paramètres avancés de la carte réseau

## Mode bidirectionnel et débit

- Les paramètres du mode bidirectionnel et du débit d'une carte réseau peuvent ralentir le transfert des données sur un ordinateur s'ils ne sont pas adaptés au périphérique connecté.

## Wake on LAN

- Les paramètres WOL (Wake on LAN) sont utilisés pour redémarrer un ordinateur du réseau se trouvant en mode de faible consommation. **La fonction WOL est configurable depuis le BIOS de la carte mère ou dans le firmware de la carte réseau**

## Quality of Service

- La QoS (qualité de service), également appelée 802.1q QoS, est un ensemble de techniques de contrôle du flux de trafic réseau qui améliore le débit de transmission et le trafic des communications en temps réel. [**Activité PT: 6.8.2.9**]

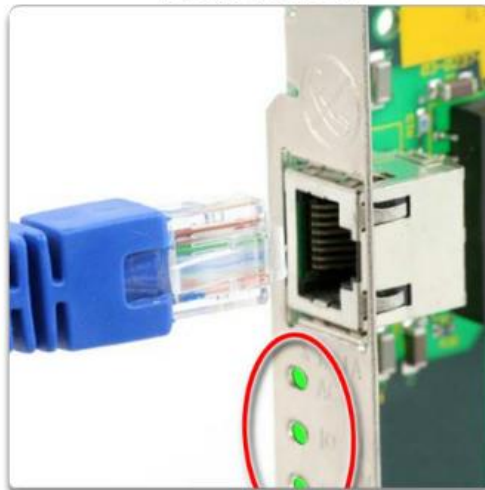


# Connexion au routeur

- Une fois le câble réseau branché, examinez les **LED (ou voyants de liaison)** situées à côté du port Ethernet de la carte réseau pour détecter tout signe d'activité.
- un profil d'emplacement réseau doit être sélectionné..
- Se connecter au routeur

à l'adress 192.168.1.1 via un navigateur

Voyants de liaison





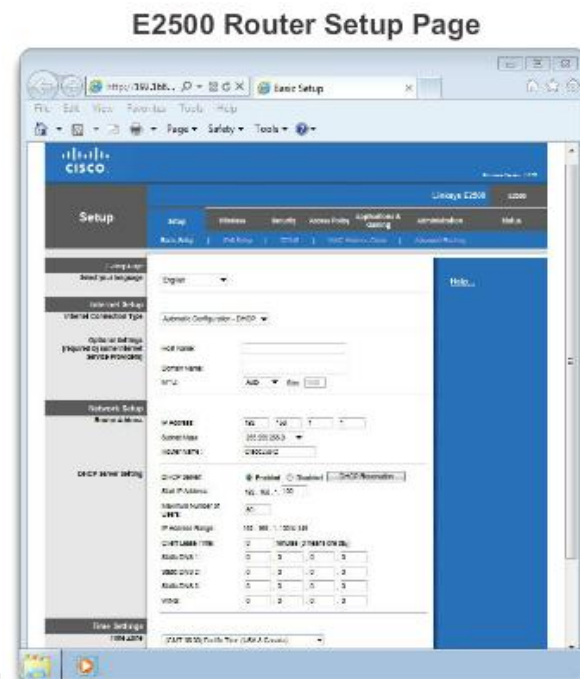
# Configuration basique du routeur

- Il est conseillé de modifier les paramètres par défaut suivants :

- Router Name
- Network Device Access Permissions (login/password)
- Basic QoS

- Le processus utilisé pour convertir les **adresses privées** en adresses Publiques routables sur Internet est appelé la **translation d'adresses réseau (NAT)**.

**TP: 6.8.3.5 et PT: 6.8.3.6**





# Paramètre de base d'un point d'accès

- La mise en service d'un routeur ISR exige la configuration d'un ensemble de paramètres
  - **Network mode** - Un environnement réseau sans fil en mode mixte peut inclure les normes 802.11b, 802.11g et 802.11n.
  - **Service Set Identifier (SSID)** - est le nom du réseau sans fil.
  - **Channel** - Les canaux 1 et 11 ne se superposent pas avec le canal 6 (utilisé par défaut). Il est donc recommandé d'utiliser l'un de ces 3 canaux .
  - **Wireless security modes**
    - **Wired Equivalent Privacy (WEP)**
    - **Temporal Key Integrity Protocol (TKIP)**
    - **Advanced Encryption Standard (AES)**
    - **Wi-Fi Protected Access (WPA)**
    - **Wi-Fi Protected Access 2 (WPA2)**

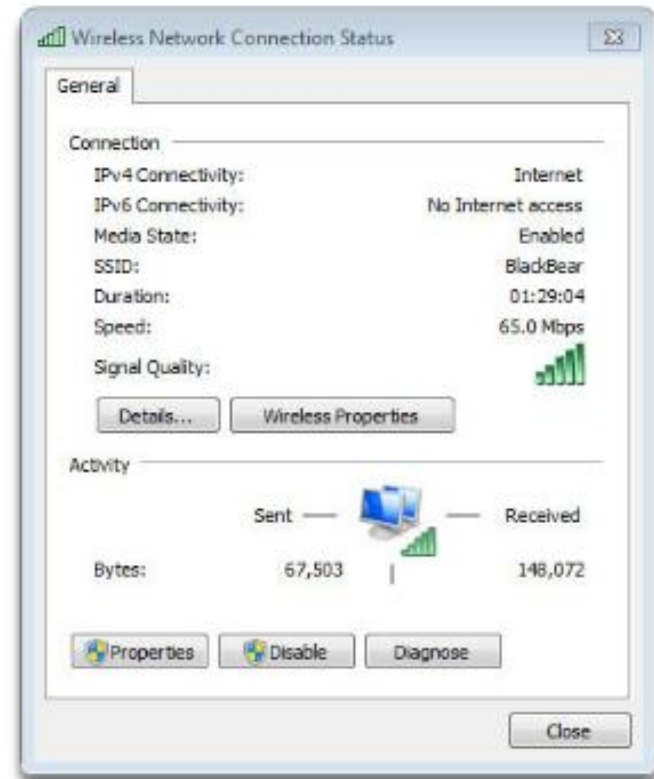
**TP: 6.8.3.7, 6.8.3.8, 6.8.3.10 et PT: 6.8.3.11**



# Test de la connectivité

- Lorsque tous les périphériques sont connectés et les voyants allumés, **testez la connectivité** du réseau.
- **Le test peut se faire via l'interface graphique (GUI)**
- La méthode la plus simple pour tester une connexion Internet est **d'ouvrir le navigateur Web** et d'essayer d'accéder à une page Web.

Fenêtre État de Connexion réseau sans fil





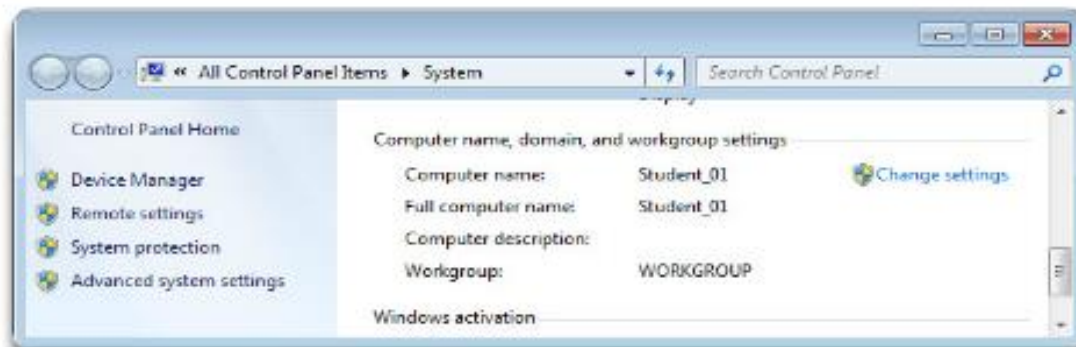
# Test de la connectivité

- Test via l'Interface Ligne de Commande
  - **Ipconfig** – affiche les informations de configuration de base de toutes les cartes réseau.
  - **Ping** – permet de tester la connectivité entre des périphériques.
  - **Net commands** – pour gérer les ordinateurs du réseau, les serveurs et certaines ressources réseau comme les lecteurs et les imprimantes.
  - **Tracert** – permet de suivre le trajet emprunté par les paquets pour aller de votre ordinateur jusqu'à l'hôte de destination.
  - **Nslookup** – permet de tester et de dépanner les serveurs DNS.

**TP: 6.8.3.13, 6.8.3.14, 6.8.3.16 et PT: 6.8.3.17**

# Domain et groupe de travail

- **Domaine** - Un domaine est un groupe d'ordinateurs et de périphériques électroniques dotés d'un ensemble de règles et de procédures commun, géré en tant qu'unité.
- **Groupe de travail** - Un groupe de travail est un groupe de stations de travail et de serveurs situé sur un réseau local et conçu pour permettre la communication et l'échange de données entre les unités du groupe.
- Avant que les ordinateurs puissent **partager des ressources**, ils doivent partager le **même nom de domaine** ou le **même nom de groupe de travail**







# Groupe résidentiel sous Windows 7

- Tous les ordinateurs Windows 7 appartenant à un même groupe de travail peuvent également faire partie d'un groupe résidentiel.
- il ne peut exister qu'un **groupe résidentiel** par groupe de travail.
- Les ordinateurs ne peuvent faire partie que d'un groupe résidentiel à la fois.
- Vous pouvez partager des **images**, de la **musique**, des **vidéos**, des **documents** et des **imprimantes** avec d'autres personnes de votre groupe résidentiel.
- Les groupes résidentiels ne sont pas disponibles sous Windows Vista ou Windows XP.





# Sharing Resources in Windows Vista

- **La fonction Partage et découverte**, située dans le Centre Réseau et partage, permet de gérer les paramètres d'un réseau domestique.
  - ✓ Recherche de réseau
  - ✓ Partage de fichiers
  - ✓ Partage de dossiers publics
  - ✓ Partage d'imprimante
  - ✓ Partage protégé par mot de passe
  - ✓ Partage des fichiers multimédias
- Pour accéder à la fonction Partage et découverte, sélectionnez :

**Démarrer > Panneau de configuration > Centre Réseau et partage**



# Partage de ressources dans Windows XP

- L'Assistant Configuration du réseau de Windows XP (voir ci-contre) permet de configurer les éléments suivants :
- La connexion à Internet de l'ordinateur par le biais d'une connexion haut débit ou bas débit, ou via un autre ordinateur du réseau domestique.
- Le partage de connexion Internet entre un ordinateur exécutant Windows XP et les autres ordinateurs du réseau domestique.
- Le nom de l'ordinateur, la description de l'ordinateur et le nom du groupe de travail
- Le partage de fichiers et d'imprimantes.
- Pour accéder à l'Assistant Configuration du réseau, sélectionnez :
- **Démarrer > Panneau de configuration > Assistant Configuration du réseau**



# Partage de ressources et mappage de lecteurs

- **Le mappage d'un lecteur local** est une méthode utile pour accéder à un fichier particulier, à des dossiers spécifiques ou à un lecteur depuis des ordinateurs en réseau exécutant des systèmes d'exploitation différents.
- Le mappage d'un lecteur, effectué en attribuant une lettre (de A à Z) à la ressource à partager sur un lecteur distant, vous permet d'accéder à ce dernier comme si vous utilisiez un lecteur local.
- Les autorisations définissent les droits dont disposent les utilisateurs pour accéder à un fichier ou un dossier spécifique
  - **Lecture** – afficher les données contenues dans les fichiers et exécuter les fichiers programmes
  - **Modification** – en plus des autorisations de lecture, l'utilisateur peut ajouter des fichiers et des sous-dossiers, modifier les données au sein des fichiers et supprimer des sous-dossiers et des fichiers
  - **Contrôle total** - en plus des autorisations de modification, l'utilisateur peut modifier les autorisations d'accès aux fichiers et dossiers sur une partition NTFS et s'appropriier les fichiers et dossiers.

**TP: 6.8.4.6, 6.8.4.7, 6.8.4.9**



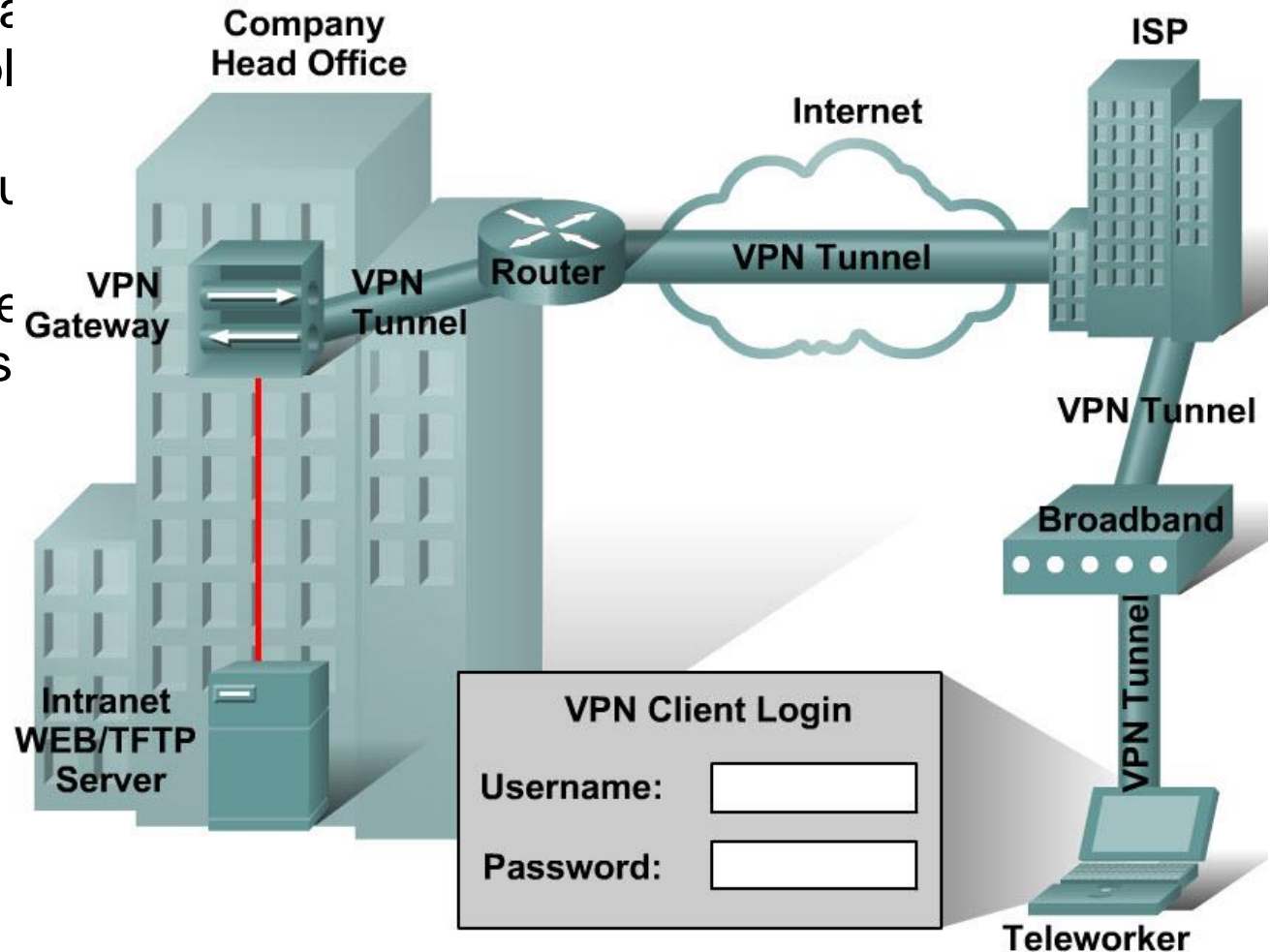
# Réseau Privé Virtuel (VPN)

- **Virtual Private Network (VPN)** - est un réseau privé qui utilise un réseau public, par exemple Internet pour connecter entre eux, de manière sécurisée, des sites ou des utilisateurs distants.
- Une fois les utilisateurs connectés au réseau privé de l'entreprise, ils sont intégrés à celui-ci et peuvent accéder à tous les services et ressources dont ils bénéficieraient s'ils étaient physiquement connectés au réseau local de l'entreprise.
- Les utilisateurs distants doivent installer le client VPN sur leur ordinateur afin d'établir une connexion sécurisée avec le réseau privé de l'entreprise.
- Les passerelles VPN établissent, gèrent et contrôlent les connexions du réseau privé virtuel, également appelées « tunnels » du réseau privé virtuel.



# Virtual Private Network (VPN)

- est un réseau privé qui utilise un réseau public, par exemple Internet pour connecter entre eux de manière sécurisée, des sites ou des utilisateurs distants





# Rafraîchissement Mémoire



# Technologies de connexion à Internet

- Dans les années quatre-vingt-dix, le réseau Internet était généralement utilisé pour les transferts de données.
- Aujourd'hui, il existe de nombreuses méthodes pour se connecter à Internet offrant des liaisons **large bande** pour les entreprises et les particuliers:
  - ✓ Les opérateurs téléphoniques (CAMTEL),
  - ✓ câblo-opérateurs,
  - ✓ opérateurs satellites (Saconets)
  - ✓ compagnies de télécommunications privées (MTN, Orange, Ringo, etc.)
- Les technologies à large bande utilisent une large plage de fréquences pouvant ensuite être divisée en canaux.
- Les clients (particuliers et entreprises) sont connectés via:
  - **Téléphonie analogique**
  - **Réseau numérique à intégration de services (RNIS)**
  - **Large bande** (câble, DSL, RNIS et satellite).



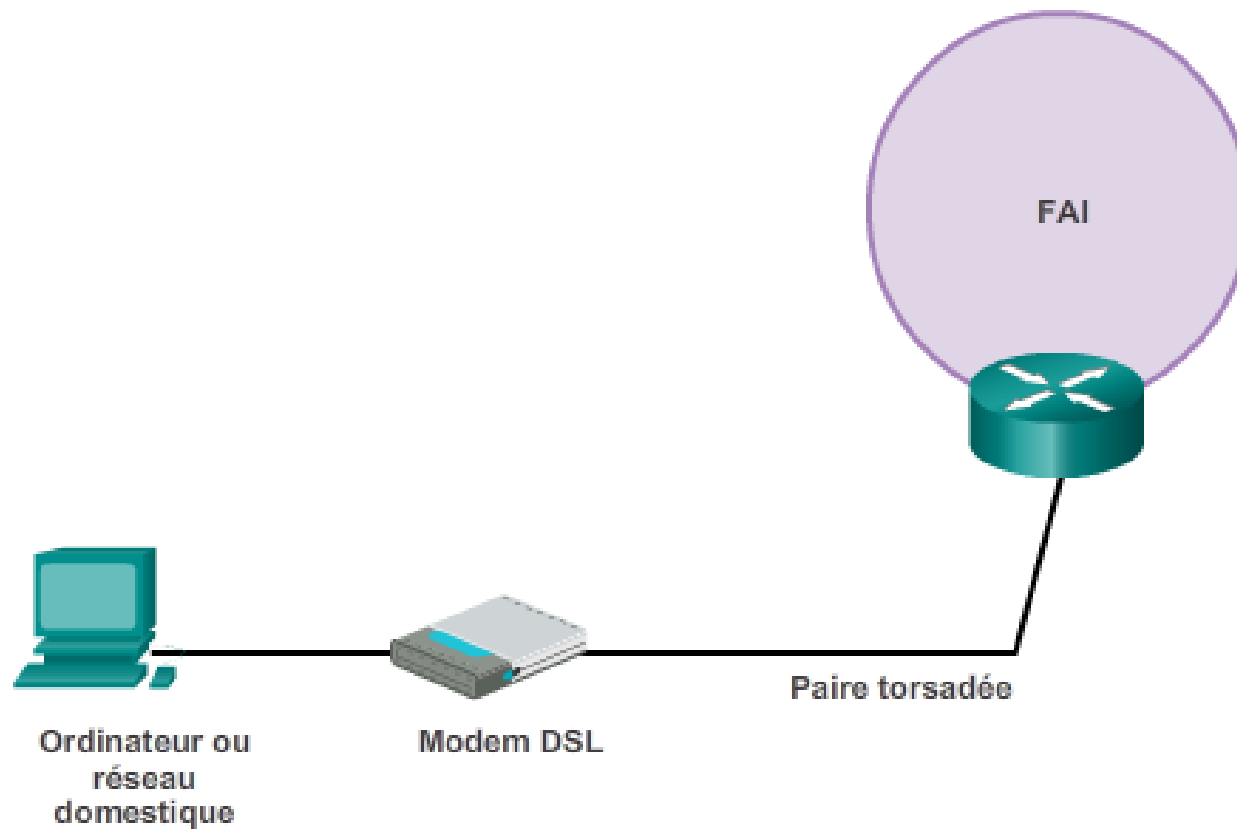
# Digital Subscriber Line (DSL)

- Le procédé DSL consiste en un **service disponible en permanence** : cela signifie qu'il n'est pas nécessaire d'établir une connexion à chaque session Internet.
- La technologie DSL utilise les **lignes téléphoniques** existantes en cuivre pour fournir une communication de données haute vitesse entre les utilisateurs finaux et les compagnies téléphoniques.
- Un filtre est utilisé pour empêcher les signaux DSL d'interférer avec les signaux téléphoniques
- Asymmetric DSL (ADSL) est actuellement la technologie DSL la plus utilisée.
  - Permet de bénéficier d'un débit de téléchargement élevé 1.5 Mbps.
  - Les débits de chargement en ADSL sont faibles.
  - L'ADSL n'est pas très performant lorsque le serveur Web ou le serveur FTP est hébergé.





## Connexion DSL



### 6.9.1.6 Fiche de travail – Questionnaire sur les technologies à large bande



# DSL Types

Type	Description
<b>ADSL</b>	Asymmetric DSL is most common. Downstream speed from 384 Kbps to 6 Mbps. Upstream speeds lower than downstream speeds.
<b>HDSL</b>	High Data Rate DSL provides equal bandwidth in both directions.
<b>SDSL</b>	Symmetric DSL provides the same speed, up to 3 Mbps, for uploads and downloads.
<b>VDSL</b>	Very High Data Rate DSL is capable of bandwidths between 13 and 52 Mbps downstream, and 16 Mbps upstream.
<b>IDSL</b>	ISDN DSL is DSL over ISDN lines. Uses ordinary phone lines. Requires ISDN adapters.

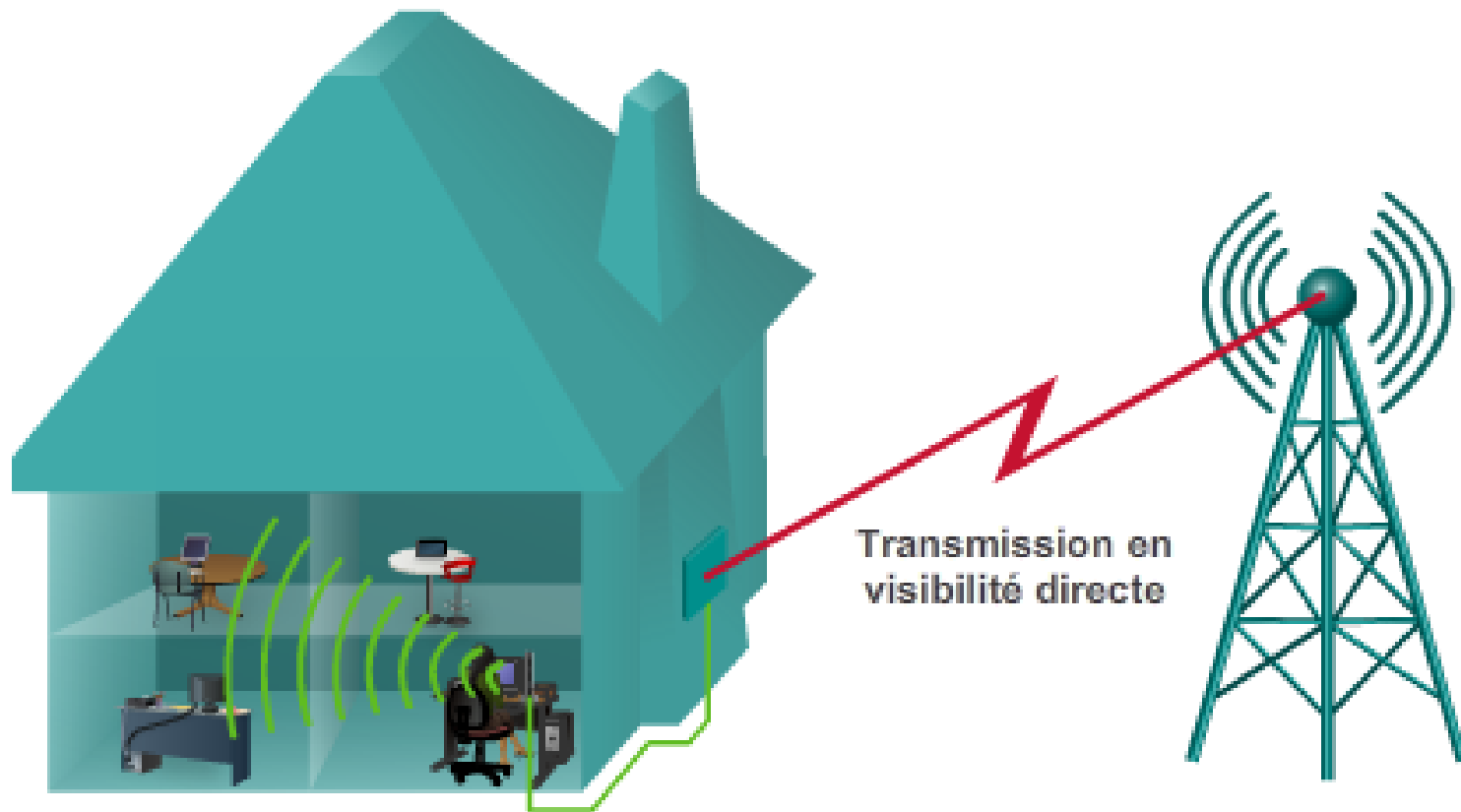


# Service Internet sans fil en visibilité directe

- **Une connexion Internet sans fil en visibilité directe** est une connexion disponible en permanence qui utilise des **signaux radio** pour diffuser la couverture Internet.
- Les signaux radio sont envoyés par une station à un récepteur que le client connecte à un ordinateur ou à un périphérique réseau.
- Cependant, une visibilité directe entre la station d'émission et le client est requise. La station doit être connectée à d'autres stations ou directement à un réseau fédérateur Internet.
- La distance que les signaux radio peuvent parcourir pour fournir une connexion fiable dépend de la fréquence des signaux. Des **signaux basse fréquence de 900 MHz peuvent parcourir jusqu'à 65 km**, alors que des **signaux haute fréquence de 5,7 GHz peuvent seulement parcourir 3 km**
- Les **conditions météorologiques extrêmes**, les **arbres** et les **bâtiments** peuvent également affecter la puissance et la fiabilité des signaux.



## Service Internet sans fil en visibilité directe



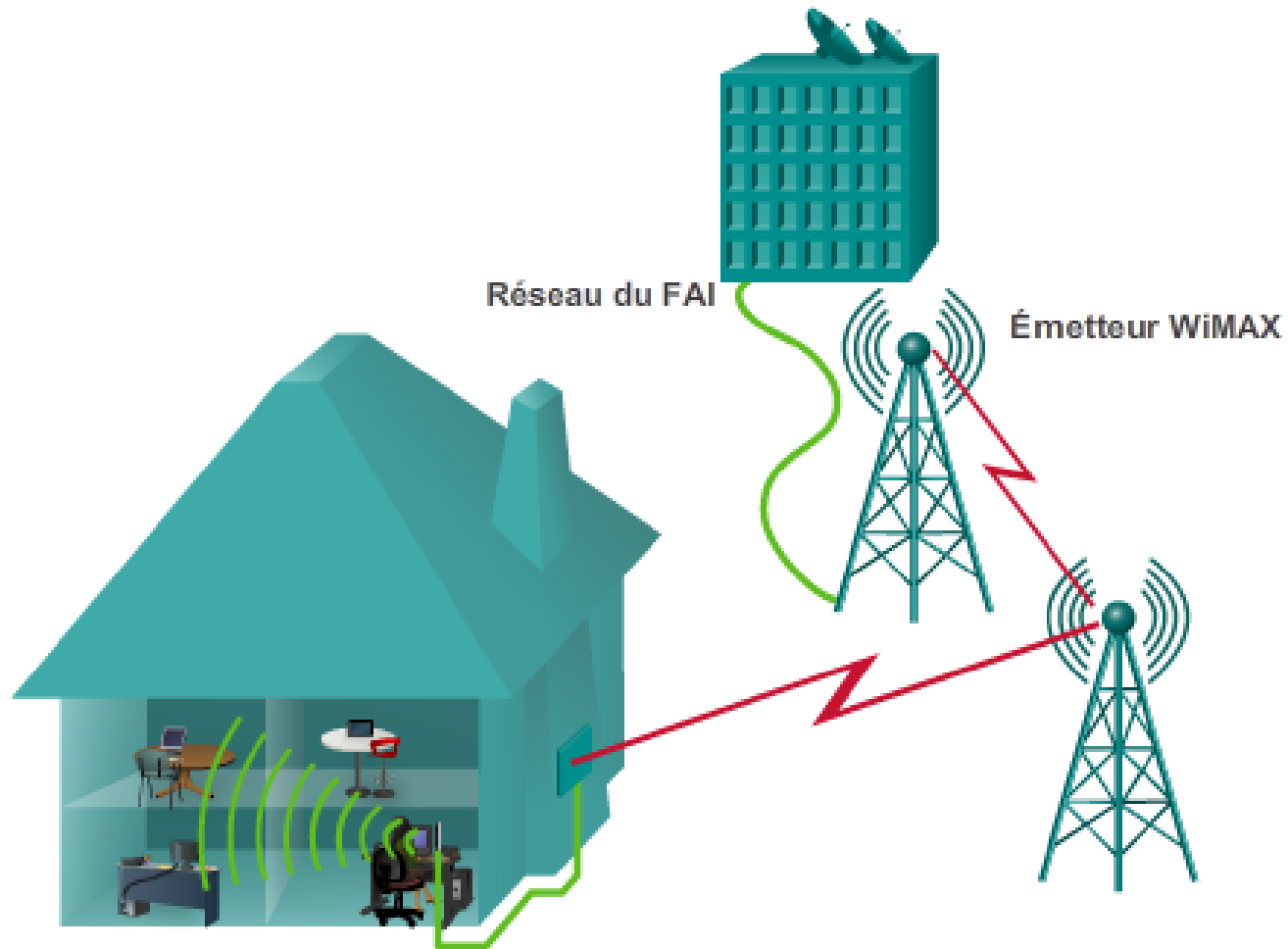


# WiMAX

- **Worldwide Interoperability for Microwave Access (WiMAX)**
  - est une technologie sans fil haut débit 4G sur IP qui offre un accès Internet mobile haut débit aux appareils mobiles.
- Le WiMAX est une norme appelée **IEEE 802.16e**
- Cette technologie est utilisable sur les réseaux de type métropolitain et permet de bénéficier d'un débit de téléchargement de **70 Mbit/s** à des **distances** pouvant atteindre **50 km**.
- Le WiMAX utilise des transmissions haute fréquence, généralement entre 2 GHz et 11 GHz. Ces fréquences rendent les signaux plus fiables.
- **WiMAX Fixe** - Service point à point ou point à multipoint offrant un débit allant jusqu'à 72 Mbit/s et une portée de 50 km.
- **WiMAX Mobile** - Service mobile, comme le Wi-Fi, mais offrant un débit supérieur et une portée plus importante..



## Transmission WiMAX



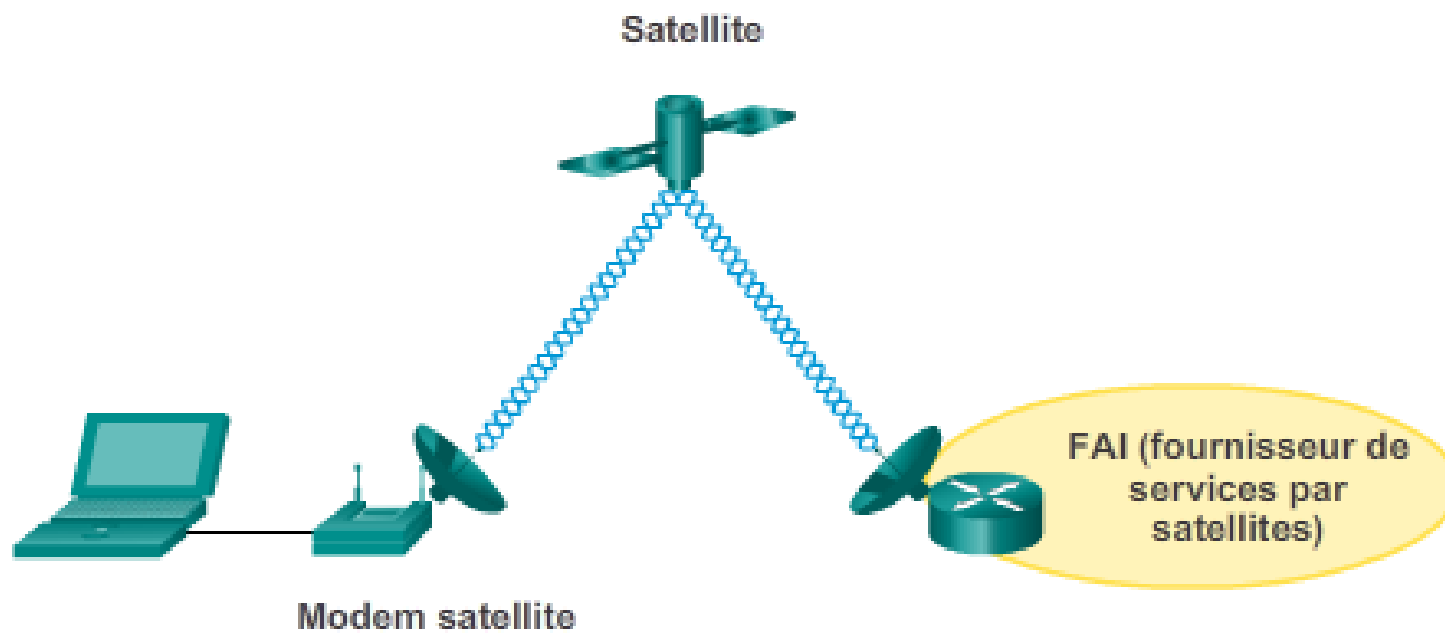


# Autres technologies à large bande

- **Cellulaire** – La technologie cellulaire permet le transfert de la voix, de vidéo et de données.
  - **1G** : uniquement pour les signaux vocaux analogiques
  - **2G** : signaux vocaux numériques, téléconférences: 9,6 kbit/s (GSM)
  - **2.5G** : débit compris entre 30 kbit/s et 90 kbit/s, navigation Web, clips audio et vidéo de courte durée, jeux vidéo (**GPRS**)
  - **3G** - Débit compris entre 144 kbit/s et 2 Mbit/s(UMTS, CDMA)
  - **4G** - débit compris entre 5,8 Mbit/s et 672 Mbit/s en mode mobile, jusqu'à 1 Gbit/s en mode fixe, voix sur IP, services de jeu vidéo, diffusion multimédia haute qualité et IPv6
- **Cable** - Il s'agit de lignes en câble coaxial, initialement prévues pour la transmission de la télévision câblée. Un modem câble relie un ordinateur à un câblo-opérateur.
- **Satellite** - Une parabole transmet et reçoit des signaux satellites.
- **Fibre optique large bande** - offre des connexions plus rapides et des bandes passantes plus larges que les modems câble ou les technologies DSL et RNIS.



## Connexion satellite







# Choix d'un FAI pour un client

- Quatre éléments majeurs sont à prendre en compte pour choisir une connexion Internet :

- ✓ **Coût**
- ✓ **Vitesse**
- ✓ **Fiabilité**
- ✓ **Disponibilité**

Exercice: 6.9.1.8 Fiche de travail – Types de connexion FAI

Type	Avantages	Inconvénients	Vitesse
POTS	Très répandu	Débits très lents Impossible de recevoir des appels téléphoniques durant la connexion	MAX 56 kbit/s
RNIS	Débits plus élevés que POTS	Toujours beaucoup plus lent que les autres technologies à large bande	BRI : jusqu'à 128 kbit/s PRI : jusqu'à 2 048 Mbit/s
DSL	Coût peu élevé	Débit différent en fonction de la distance du central	24 kbit/s - 100 Mbit/s
Câble	Très haut débit	Vitesses de chargement (upload) lentes	27 kbit/s - 160 Mbit/s
Satellite	Disponible en l'absence de la DSL et du câble	Plus cher que d'autres technologies à large bande, et sensible aux conditions météo	9 kbit/s - 24 Mbit/s



# Procédures de maintenance préventive

- Vous devez vérifier l'état des câbles, des périphériques réseau, des serveurs et des ordinateurs, pour vous assurer qu'ils sont toujours propres et en bon état de fonctionnement.
  - Les salles informatiques doivent être propres et les filtres à air changés régulièrement.
  - Mettre au point un planning régulier de maintenance et de nettoyage.
  - Inspectez tous les câbles. Assurez-vous également que les câbles sont correctement étiquetés et que les étiquettes sont bien fixées; Suivez toujours les directives de l'entreprise relatives à l'étiquetage des câbles
  - Vérifiez que les supports de câble sont correctement installés et qu'aucun point de fixation ne se défait
  - Les câbles sont souvent déplacés ou heurtés lorsqu'ils se trouvent sous des bureaux.
  - Vous devez également éduquer les utilisateurs du réseau
  - Le Système d'Alimentation sans Coupure (UPS) doit être mise en place question de s'assurer de la continuité du service même en cas de panne d'électricité.



# Application de la procédure de dépannage pour les réseaux

**Step 1** Identification du problème

**Step 2** Élaboration d'une théorie sur les causes probables

**Step 3** Test de la théorie en vue de déterminer la cause

**Step 4** Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution

**Step 5** Vérification du fonctionnement de l'ensemble du système et implémentation des mesures préventives

**Step 6** Documentation des résultats des recherches et des actions entreprises



# Step 1- Identification du problème

- Les problèmes de réseau peuvent résulter d'une combinaison de problèmes matériels, logiciels et de connectivité de différente envergure.
- Les techniciens informatiques doivent être capables d'analyser le problème et d'en déterminer la cause afin de résoudre le problème du réseaux: C'est le **Dépannage**
- Si le problème concerne un seul ordinateur, commencez la procédure de dépannage sur celui-ci. S'il concerne l'ensemble des ordinateurs du réseau, commencez le dépannage dans la salle réseau contenant toutes les connexions.

## Étape 1. Identification du problème

### Questions ouvertes

- Quels problèmes rencontrez-vous avec votre ordinateur ou votre périphérique réseau ?
- Quel logiciel a été installé sur votre ordinateur récemment ?
- Que faisiez-vous lorsque le problème a été détecté ?
- Quels messages d'erreur avez-vous reçus ?
- Quel type de connexion réseau l'ordinateur utilise-t-il ?

### Questions fermées

- Une tierce personne a-t-elle utilisé votre ordinateur récemment ?
- Pouvez-vous voir des imprimantes ou des fichiers partagés ?
- Avez-vous modifié votre mot de passe récemment ?
- Pouvez-vous accéder à Internet ?
- Êtes-vous connecté au réseau actuellement ?



## Step 2 - Elaboration d'une théorie sur les causes probables

- Après avoir parlé au client, vous pouvez élaborer une théorie sur les causes probables
  - Câbles mal branchés
  - Carte réseau mal installée
  - Problème avec le FAI
  - Faible intensité du signal sans fil
  - Paramètres d'adressage IP invalides

### Étape 2. Élaboration d'une théorie sur les causes probables

Causes courantes des problèmes de réseau

- Câbles mal branchés
- Carte réseau mal installée
- Problème avec le FAI
- Faible intensité du signal sans fil
- Adresse IP non valide



## Step 3 - Test de la théorie en vue de déterminer la cause

- Après avoir élaboré une théorie sur l'origine du problème, passez à la pratique afin de déterminer la cause exacte.
- Lorsqu'une procédure rapide permet de résoudre le problème, vous pouvez passer à l'étape de vérification du fonctionnement de l'ensemble du système

### Étape 3. Test de la théorie en vue de déterminer la cause

Étapes classiques pour déterminer la cause

- Vérifier que tous les câbles sont connectés aux bons endroits
- Déconnecter et reconnecter les câbles et les connecteurs
- Redémarrer l'ordinateur ou le périphérique réseau
- Ouvrir une session avec un nom d'utilisateur différent
- Réparer ou réactiver la connexion réseau
- Contacter l'administrateur réseau
- Envoyer une requête ping à la passerelle par défaut
- Accéder à une page Web distante telle que <http://www.cisco.com>

- Si la cause exacte du problème n'est pas déterminée à l'issue de cette étape, il pourrait s'avérer utile d'établir une nouvelle théorie sur les causes possibles.



# Step 4 - Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution

- La division de la panne en petite panne par le principe de l'isolation pourrait permettre une analyse individuelle des différents segment du réseau.

## Étape 4. Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution

Si aucune solution n'a été trouvée à l'étape précédente, des recherches complémentaires sont nécessaires pour implémenter la solution.

- Journaux des réparations du centre d'assistance
- Autres techniciens
- FAQ des sites Web des fabricants
- Sites Web techniques
- Forums de discussion
- Guides d'utilisation des ordinateurs
- Guides d'utilisation des périphériques
- Forums en ligne
- Recherche sur Internet



## Step 5 - Vérification du fonctionnement de l'ensemble du système et implémentation des mesures préventives

- Après avoir résolu le problème, vous devez vérifier le fonctionnement de l'ensemble du système et s'il y a lieu, implémenter des mesures préventives.
  - **Ipconfig /all** is used to display IP Address information.
  - **Ping** is used to check network connectivity.
  - **Nslookup** is used to query Internet domain name server.
  - **Tracert** is used to determine the route taken by packets when they travel across the network.
  - **Net View** is used to display a list of computers in a workgroup.
- Le client doit vérifier s'assurer de la résolution de la panne en vérifiant à son tour le bon fonctionnement de son système.





# Step 6 - Documentation des résultats des recherches et des actions entreprises

- Discuter de la solution avec le client.
- Permettre au client de vérifier et de confirmer la résolution du problème.
- Documenter les résultats de vos recherches ainsi que les actions entreprises
  - Description du problème
  - Description de la solution
  - Présentation des outils utilisés
  - Indiquez le temps moyen passé pour résoudre le problème

## Étape 6. Documentation des résultats des recherches et des actions entreprises

Documenter les résultats des recherches et les actions entreprises

- Discuter de la solution mise en œuvre avec le client
- Faire vérifier par le client que le problème a été résolu
- Fournir tous les documents au client
- Dans le bon de travail et dans le journal du technicien, décrire les étapes suivies pour résoudre le problème
- Décrire tous les composants utilisés pour la réparation
- Indiquer le temps passé pour résoudre le problème



# Identification des problèmes courants et des solutions

- Vous pouvez identifier les problèmes courant des réseaux à la section: 6.11.2.1

Problèmes courants et solutions		
Identification du problème	Causes probables	Solutions possibles
Les voyants (LED) de la carte réseau ne s'allument pas.	Le câble réseau est débranché, défectueux ou endommagé.	Reconnecter ou remplacer le câble réseau connecté à l'ordinateur.
L'utilisateur ne peut pas établir de connexion Telnet avec un périphérique distant.	<ul style="list-style-type: none"> <li>Le périphérique distant n'est pas configuré pour l'accès Telnet.</li> <li>L'accès Telnet n'est pas autorisé à partir de l'utilisateur ou d'un réseau particulier.</li> </ul>	<ul style="list-style-type: none"> <li>Configurer le périphérique distant pour l'accès Telnet.</li> <li>Autoriser l'accès Telnet à partir de l'utilisateur ou du réseau.</li> </ul>
Un ancien ordinateur portable ne peut pas détecter le routeur sans fil.	<ul style="list-style-type: none"> <li>Le routeur sans fil / point d'accès est configuré avec un protocole 802.11 différent.</li> <li>Le SSID n'est pas diffusé.</li> <li>La carte réseau sans fil de l'ordinateur</li> </ul>	<ul style="list-style-type: none"> <li>Configurer le routeur sans fil à l'aide d'un protocole compatible avec l'ordinateur portable.</li> <li>Configurer le routeur sans fil de telle sorte qu'il active la diffusion SSID.</li> </ul>



## Chapter 6 Summary

- A computer network is composed of two or more computers that share data and resources.
- A Local Area Network (LAN) refers to a group of interconnected computers that are under the same administrative control.
- A Wide Area Network (WAN) is a network that connects LANs in geographically separated locations.
- In a peer-to-peer network, devices are connected directly to each other. A peer-to-peer network is easy to install, and no additional equipment or dedicated administrator is required. Users control their own resources, and a network works best with a small number of computers. A client/server network uses a dedicated system that functions as the server. The server responds to requests made by users or clients connected to the network.



## Chapter 6 Summary (Continued)

- A LAN uses a direct connection from one computer to another. It is suitable for a small area, such as in a home, building, or school. A WAN uses point-to-point or point-to-multipoint, serial communications lines to communicate over greater distances. A WLAN uses wireless technology to connect devices together.
- The network topology defines the way in which computers, printers, and other devices are connected. Logical topology describes how the hosts access the medium and communicate on the network. Physical topology describes the layout of the wire and devices, as well as the paths used by data transmissions.. Topologies include bus, star, ring, and mesh.
- Networking devices are used to connect computers and peripheral devices so that they can communicate. These include hubs, bridges, switches, routers, and multipurpose devices. The type of device implemented depends on the type of network.



## Chapter 6 Summary (Continued)

- Networking media can be defined as the means by which signals, or data, are sent from one computer to another. Signals can be transmitted either by cable or wireless means. The media types discussed were coaxial, twisted-pair, fiber-optic cabling, and radio frequencies.
- Ethernet is now the most popular type of LAN technology. The Ethernet architecture is based on the IEEE 802.3 standard. The IEEE 802.3 standard specifies that a network implement the CSMA/CD access control method.
- The OSI reference model is an industry standard framework that is used to divide the functions of networking into seven distinct layers. These layers include Application, Presentation, Session, Transport, Network, Data Link, and Physical. It is important to understand the purpose of each layer.



## Chapter 6 Summary (Continued)

- The TCP/IP suite of protocols has become the dominant standard for the Internet. TCP/IP represents a set of public standards that specify how packets of information are exchanged between computers over one or more networks.
- A NIC is a device that plugs into a motherboard and provides ports for the network cable connections. It is the computer interface with the LAN.
- A modem is an electronic device that is used for computer communications through telephone lines. It allows data transfer between one computer and another. The modem converts byte-oriented data to serial bit streams.



## Chapter 6 Summary (Continued)

- The three transmission methods to sending signals over data channels are simplex, half-duplex, and full-duplex. Full-duplex networking technology increases performance because data can be sent and received at the same time. DSL, two-way cable modem, and other broadband technologies operate in full-duplex mode.
- Network devices and media, such as computer components, must be maintained. It is important to clean equipment regularly and use a proactive approach to prevent problems. Repair or replace broken equipment to prevent downtime.
- When troubleshooting network problems, listen to what your customer tells you so that you can formulate open-ended and closed-ended questions that will help you determine where to begin fixing the problem. Verify obvious issues and try quick solutions before escalating the troubleshooting process.

# Cisco | Networking Academy<sup>®</sup>

Mind Wide Open<sup>™</sup>