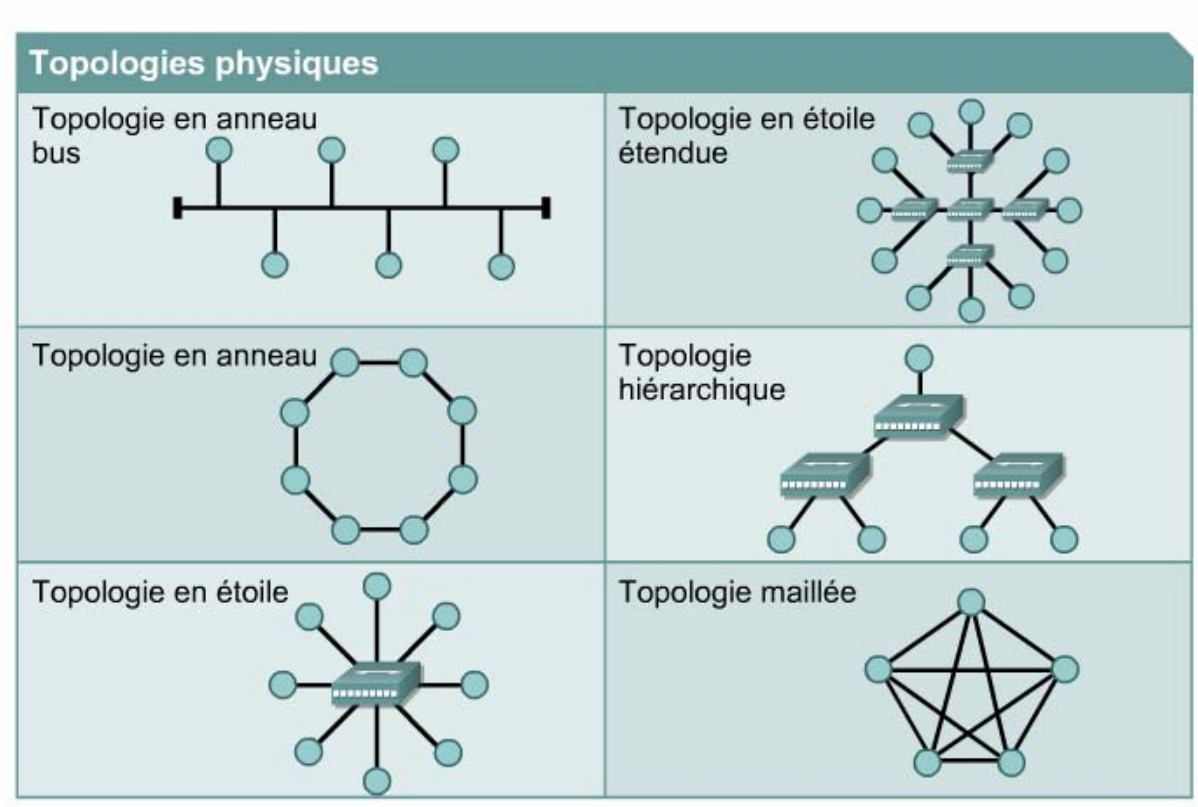
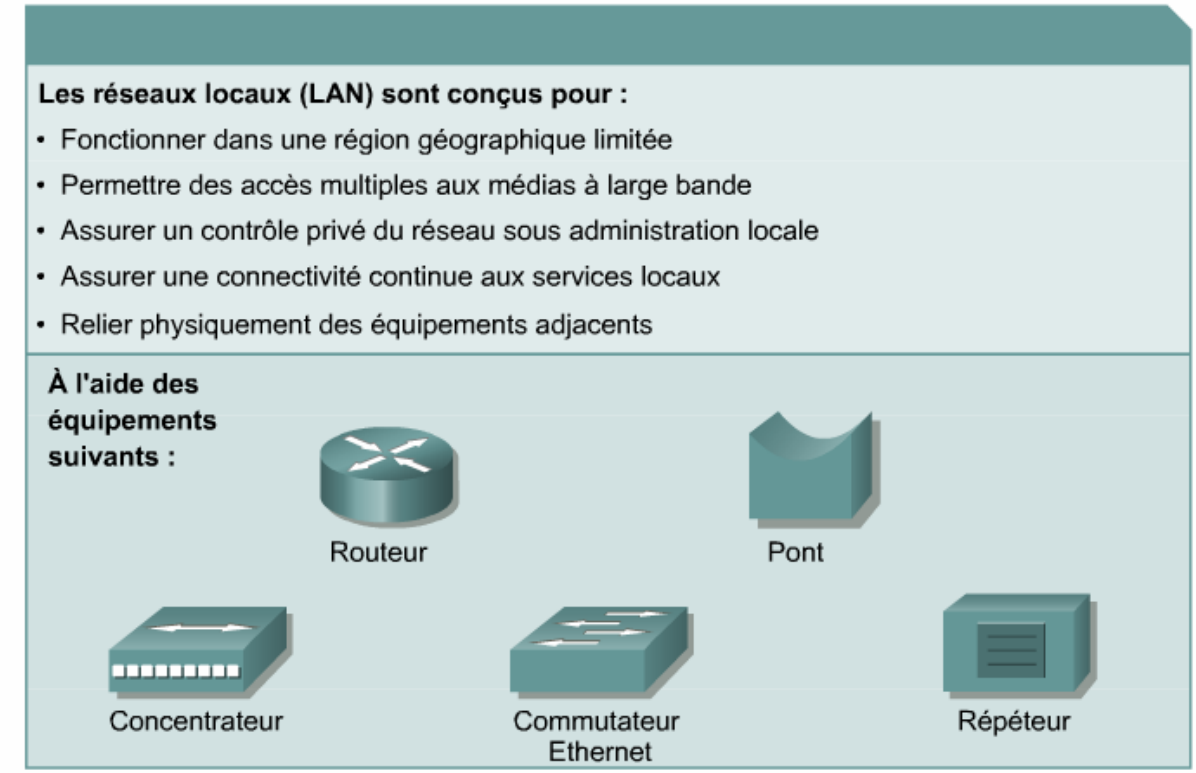
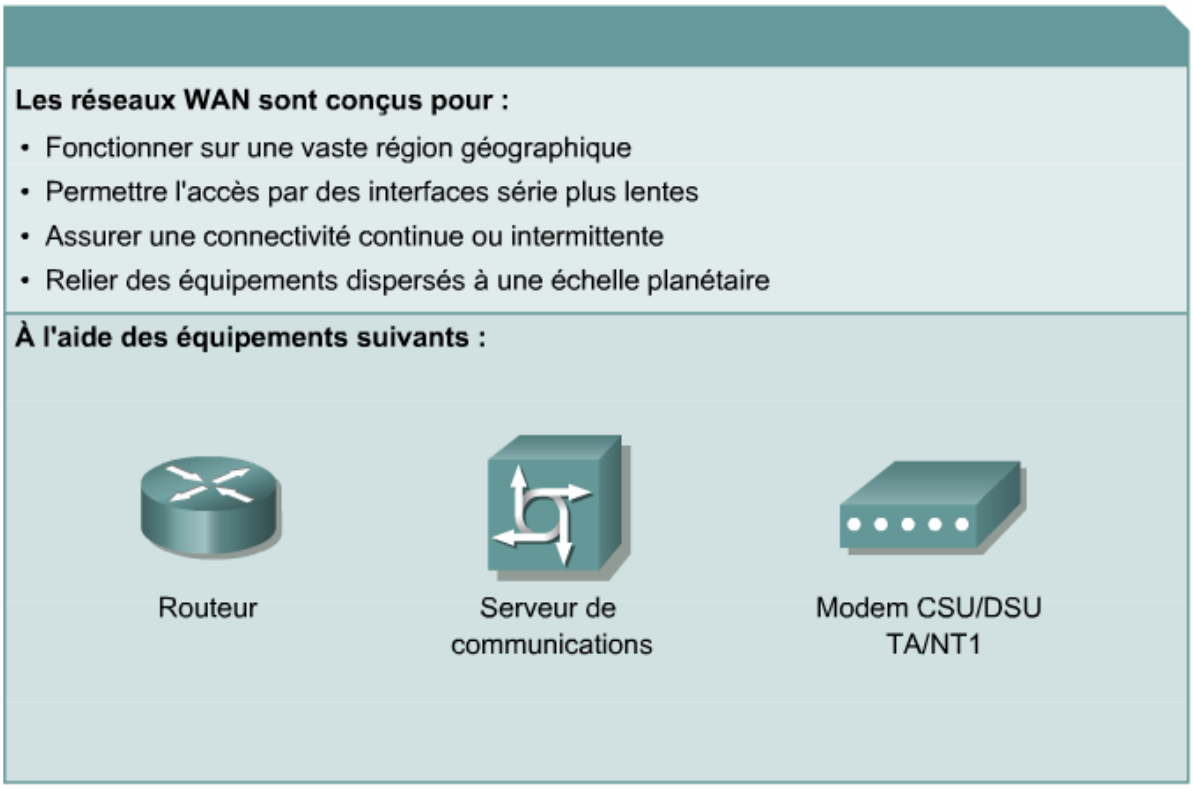
La commande **ping** utilise des paquets de données IP (*Internet Protocol*) spéciaux, nommés datagrammes ICMP (*Internet Control Message Protocol*), pour envoyer des messages de demande d'écho à une destination donnée. Chaque paquet envoyé équivaut à une demande de réponse. La réponse renvoyée indique le taux de réussite et le temps de parcours aller-retour entre les équipements source et de destination. Ces informations déterminent la connectivité avec l'équipement de destination. La commande **ping** sert à tester les fonctions de transmission et de réception de la carte réseau, la configuration TCP/IP et la connectivité réseau. Les différentes utilisations possibles de la commande ping sont les suivantes :

- **ping** *127.0.0.1* – Utilisée pour tester la boucle locale interne, cette commande permet de vérifier la configuration réseau TCP/IP.
- **ping** *Adresse IP d'un ordinateur hôte* – Envoyée à un hôte du réseau, cette commande vérifie la configuration de l'adresse TCP/IP pour l'hôte et la connectivité avec ce dernier.
- **ping** *Adresse IP de la passerelle par défaut* – L'exécution de la commande ping vers la passerelle par défaut sert à vérifier si le routeur qui relie le réseau local à d'autres réseaux est accessible.
- **ping** *Adresse IP d'un hôte distant* – Permet de tester la connectivité avec un hôte distant.

L'activité de TP porte sur l'utilisation des commandes **ping** et **tracert**.







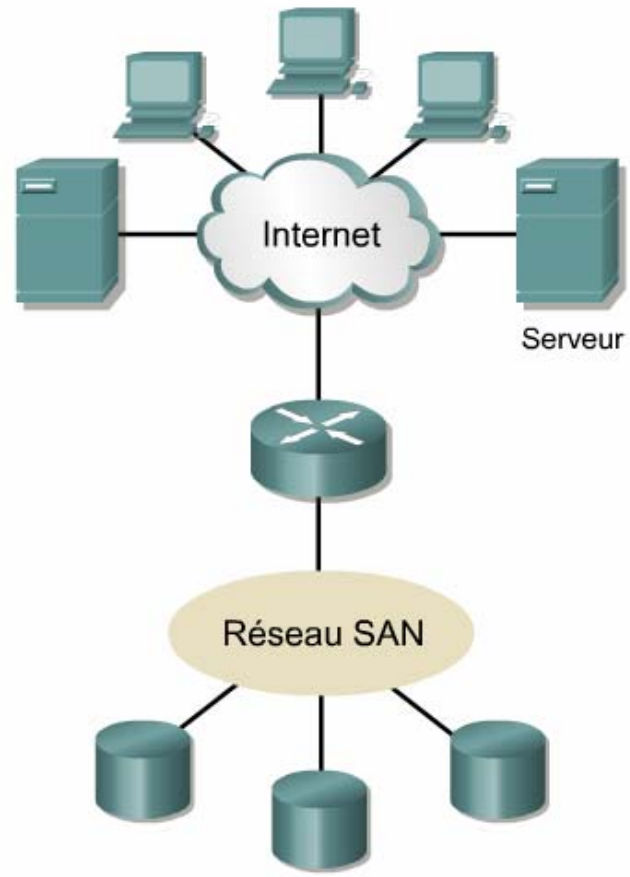
Cette page décrit les caractéristiques des réseaux SAN.

Un réseau de stockage (SAN) est un réseau à haute performance dédié qui permet de transférer des données entre des serveurs et des ressources de stockage. Du fait qu'il s'agit d'un réseau dédié distinct, il évite tout conflit de trafic entre les clients et les serveurs.

La technologie SAN permet de bénéficier d'une connectivité haut débit pour différentes configurations : serveur/stockage, stockage/stockage ou serveur/serveur. Cette méthode recourt à une infrastructure de réseau séparée qui résout tout problème associé à la connectivité réseau existante.

Les réseaux SAN offrent les caractéristiques suivantes:

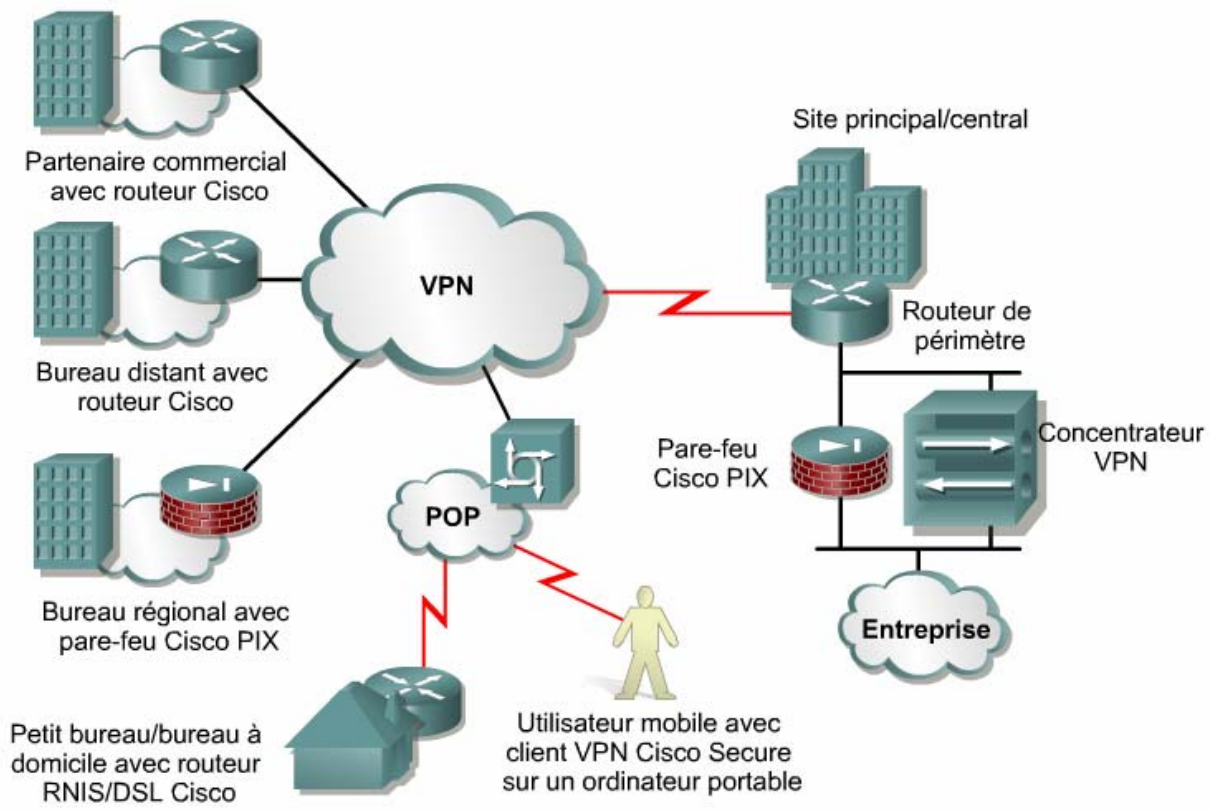
- **Performance** – les réseaux SAN permettent un accès simultané à haut débit, par deux serveurs ou plus, aux matrices de disques et de bandes. Cela améliore les performances du système.
- **Disponibilité** – Les réseaux SAN intègrent la tolérance aux sinistres. Les données peuvent être dupliquées sur un réseau SAN situé jusqu'à 10 km de distance.
- **Évolutivité** – Un réseau SAN peut utiliser les technologies les plus variées. Cela facilite le déplacement des données de sauvegarde, des opérations, la migration des fichiers et la réplication des données entre les systèmes.



Un réseau privé virtuel est un service qui offre une connectivité sécurisée et fiable sur une infrastructure de réseau public partagée telle qu'Internet. Les VPN maintiennent les mêmes politiques de sécurité et de gestion qu'un réseau privé. L'utilisation d'un réseau privé virtuel est la façon la plus rentable d'établir une connexion point-à-point entre des utilisateurs distants et un réseau d'entreprise.

Voici une liste des trois principaux types de VPN :

- Les VPN d'accès fournissent aux utilisateurs mobiles et de petits bureaux/bureaux à domicile (SOHO) l'accès distant à un intranet ou à un extranet sur une infrastructure partagée. Les VPN d'accès utilisent des technologies analogiques, d'accès par ligne téléphonique, RNIS, DSL, IP mobile et câble afin de connecter en toute sécurité les utilisateurs mobiles, les télétravailleurs et les agences.
- Les VPN d'intranet font appel à des connexions dédiées pour raccorder des bureaux régionaux et des bureaux distants à un réseau interne sur une infrastructure partagée. Les VPN d'intranet diffèrent des VPN d'extranet en ce qu'ils n'autorisent l'accès qu'aux employés de l'entreprise.
- Les VPN d'extranet utilisent des connexions dédiées pour relier des partenaires commerciaux à un réseau interne sur une infrastructure partagée. Les VPN d'extranet diffèrent des VPN d'intranet en ce qu'ils permettent l'accès aux utilisateurs en dehors de l'entreprise.



Types de médias	Bande passante théorique maximale	Distance théorique maximale
(Ethernet 10Base2 ; Ethernet à câble fin)		
Câble coaxial de 50 ohms (Ethernet 10Base5 ; câble Ethernet épais)	10 Mbits/s	500 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 10BaseT)	10 Mbits/s	100 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 100BaseTX)	100 Mbits/s	100 m
Paire torsadée non blindée (UTP) de catégorie 5 (UTP) (Ethernet 1000BaseTX)	1000 Mbits/s	100 m
Fibre optique multimode (62,5/125 m) (Ethernet 100BaseFX)	100 Mbits/s	220 m
Fibre optique multimode (62,5/125 m) (Ethernet 100BaseFX)	1000 Mbits/s	220 m
Fibre optique multimode (50/125 m) (Ethernet 1000BaseSX)	1000 Mbits/s	550 m
Fibre optique monomode (9/125 m) (Ethernet 1000BaseLX)	1000 Mbits/s	5000 m

Service WAN	Utilisateur type	Bande passante
	fiables	(U.S.) ou 34 368 Mbits/s (Europe) = 0,056 Mbits/s à 44 736 Mbits/s (U.S.) ou 34 368 Mbits/s (Europe)
T1	Grandes organisations	1.544 Mbits/s
E1	Grandes organisations	2.048 Mbits/s
T3	Grandes organisations	44.736 Mbits/s
E3	Grandes organisations	34.368 Mbits/s
STM-0 (OC-1)	Compagnies de téléphone ; backbones des opérateurs Télécom	51.840 Mbits/s
STM-1	Compagnies de téléphone ; backbones des opérateurs Télécom	155.52 Mbits/s
STM-1 (OC-3)	Compagnies de téléphone ; backbones des opérateurs Télécom	155.251 Mbits/s
STM-3	Compagnies de téléphone ; backbones des opérateurs Télécom	466.56 Mbits/s
STM-16 (OC-48)	Compagnies de téléphone ; backbones des opérateurs Télécom	2.488320 Gbits/s

Meilleur téléchargement

$$D = \frac{T}{BP}$$

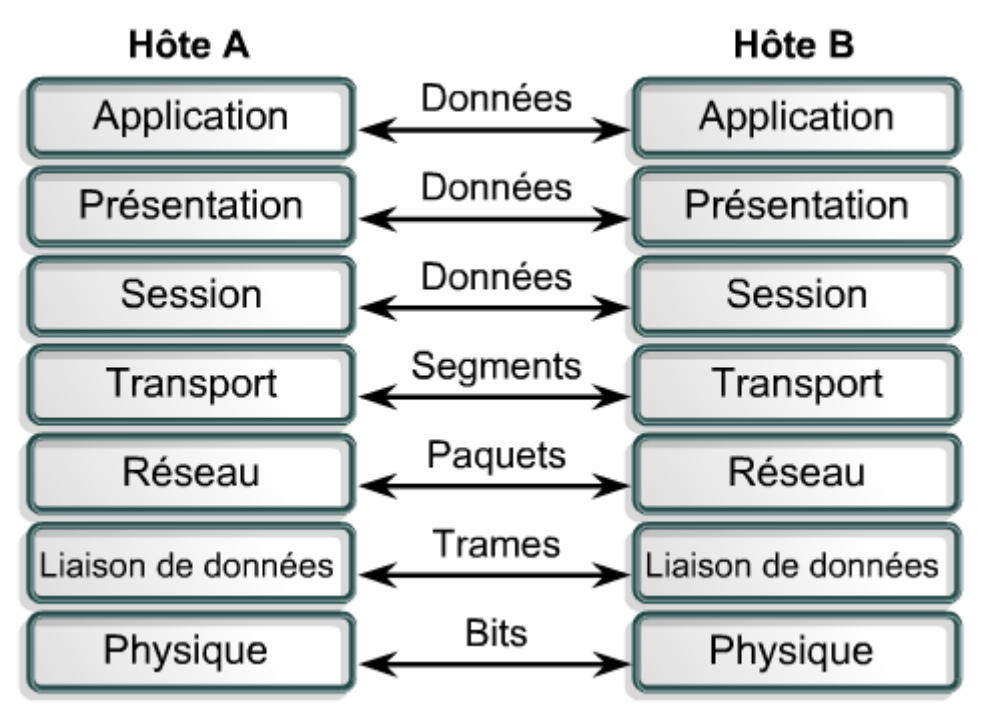
Téléchargement type

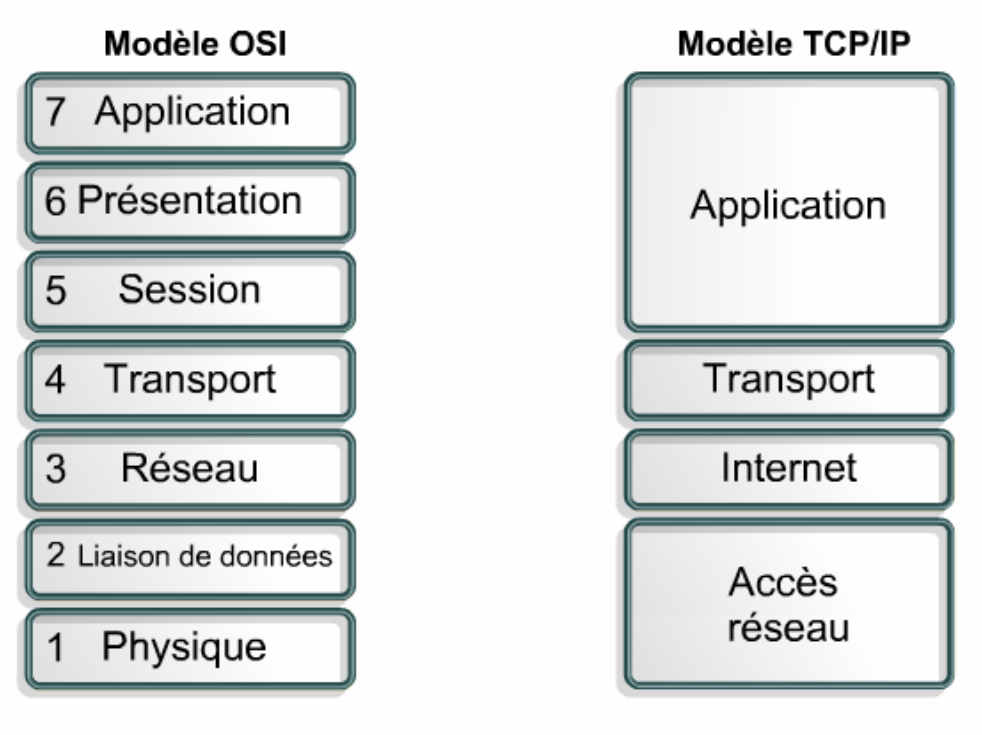
$$D = \frac{T}{P}$$

BP	Bande passante théorique maximale de la liaison " la plus lente " entre l'hôte source et l'hôte de destination (mesurée en bits par seconde)
P	Débit effectif au moment du transfert (mesuré en bits par seconde)
D	Durée du transfert des fichiers (mesuré en secondes)
T	Taille de fichier en bits

Avantages du modèle OSI :

- Il réduit la complexité.
- Il uniformise les interfaces.
- Il facilite la conception modulaire.
- Il assure l'interopérabilité de la technologie.
- Il accélère l'évolution.
- Il simplifie l'enseignement et l'acquisition des connaissances.


Hôte A
Hôte B
Application
Données
Application
Présentation
Données
Présentation
Session
Données
Session
Transport
Segments
Transport
Réseau
Paquets
Réseau
Liaison de données
Trames
Liaison de données
Physique
Bits
Physique


Modèle OSI
7 Application
6 Présentation
5 Session
4 Transport
3 Réseau
2 Liaison de données
1 Physique
Modèle TCP/IP
Application
Transport
Internet
Accès réseau

3)

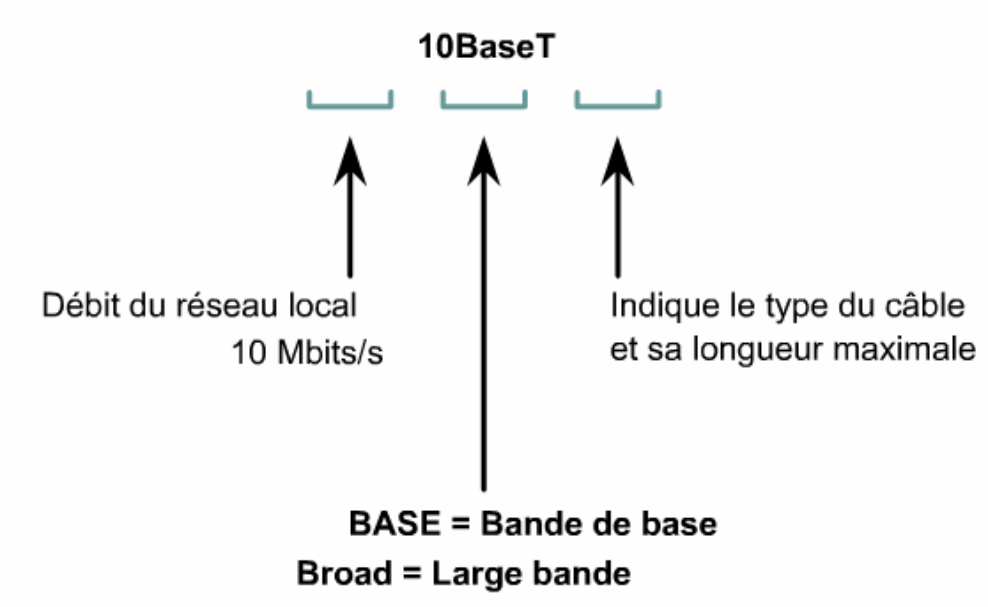
Les spécifications Ethernet suivantes se rapportent au type de câble:

- 10BaseT
- 10Base5
- 10Base2

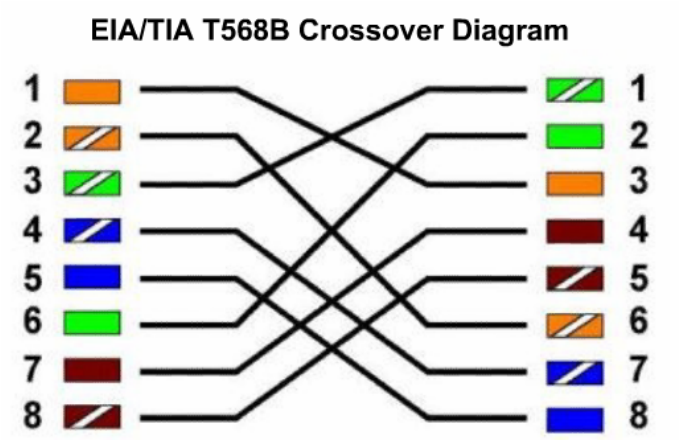
10BaseT indique une vitesse de transmission de 10 Mbits/s. La transmission est du type à bande de base ou interprétée numériquement. La lettre T indique une paire torsadée.

10Base5 indique une vitesse de transmission de 10 Mbits/s. La transmission est du type à bande de base ou interprétée numériquement. Le chiffre 5 indique qu'un signal peut parcourir environ 500 mètres avant que l'atténuation ne puisse empêcher le récepteur d'interpréter le signal. La spécification 10Base5 est souvent appelée ThickNet. Ethernet à câble épais (Thicknet) est un type de réseau alors que 10BASE5 est la norme Ethernet utilisée dans ce réseau.

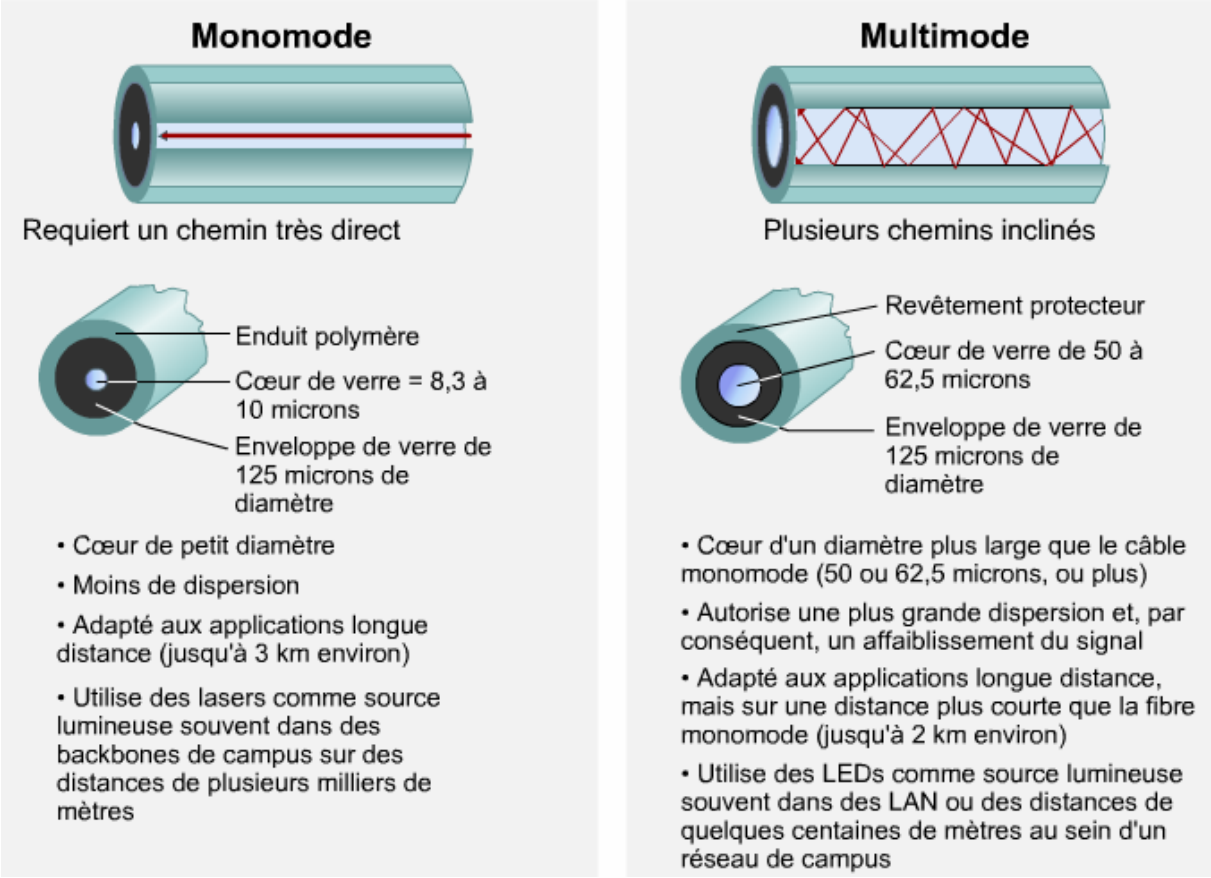
10Base2 indique une vitesse de transmission de 10 Mbits/s. La transmission est du type à bande de base ou interprétée numériquement. Le chiffre 2 indique qu'une longueur de segment maximale de 200 mètres peut être parcourue avant que l'atténuation ne puisse empêcher le récepteur d'interpréter correctement le signal reçu. La longueur de segment maximale est en fait de 185 mètres. La spécification 10Base2 est souvent appelée ThinNet. Ethernet à câble fin (Thinnet) est un type de réseau alors que 10BASE2 est la norme Ethernet utilisée dans ce réseau.



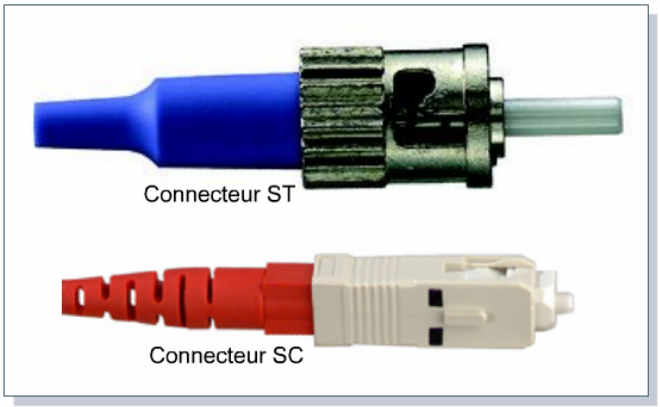
Cable croisé



Cable console <-> PC : cable droit



Les connecteurs les plus fréquemment utilisés sont les connecteurs SC (*Subscriber Connector*) pour la fibre multimode, et les connecteurs ST *(Straight Tip)* pour la fibre monomode.



À l'instar des réseaux câblés, l'IEEE est le premier éditeur de normes en matière de réseaux sans fil. Ces normes ont été élaborées dans le cadre des réglementations instaurées par la FCC *(Federal Communications Commission)*.

Le DSSS *(Direct Sequence Spread Spectrum* ou *étalement du spectre en séquence directe)* est une technologie clé contenue dans la norme 802.11 qui s'applique aux équipements sans fil fonctionnant dans la gamme des 1 à 2 Mbits/s. Un système DSSS pouvant fonctionner jusqu'à un débit de 11 Mbits/s n'est pas considéré comme étant conforme au-dessus des 2 Mbits/s. La norme 802.11b a été ensuite approuvée pour accroître les fonctions de transmission à 11 Mbits/s. Même si les LAN sans fil DSSS pouvaient interopérer avec les LAN sans fil FHSS *(Frequency Hopping Spread Spectrum* ou *étalement du spectre à sauts de fréquence)*, certains problèmes ont conduit les constructeurs à modifier leur conception. Dans ce contexte, l'IEEE a créé une norme qui correspondait à la solution proposée par les constructeurs.

La norme 802.11b est aussi appelée norme Wi-Fi™ ou norme sans fil haut débit pour les systèmes DSSS qui opèrent à 1, 2, 5,5 et 11 Mbits/s. Tous les systèmes 802.11b sont compatibles en amont dans la mesure où ils prennent également en charge la norme 802.11 à 1 et 2 Mbits/s s'appliquant au DSSS uniquement. Cette compatibilité amont est extrêmement importante car elle permet de mettre à niveau le réseau sans fil sans remplacer les cartes réseau ou les points d'accès.

Les équipements 802.11b prennent en charge un débit de données plus élevé en recourant à une technique de codage différente de celle des équipements 802.11, qui les autorise à transmettre une plus grande quantité de données dans le même délai. La plupart des équipements 802.11b ne parviennent toujours pas à atteindre une largeur de bande de 11 Mbits/s et fonctionnent généralement à un débit compris entre 2 et 4 Mbits/s.

La norme 802.11a s'applique aux équipements de réseau LAN sans fil opérant dans la bande de transmission de 5 GHz. La plage de 5 GHz ne permet pas l'interopérabilité des équipements 802.11b lorsqu'ils opèrent à 2,4 GHz. Les équipements 802.11a réalisent un débit de données de 54 Mbits/s et peuvent atteindre 108 Mbits/s grâce à la technologie propriétaire qui permet de doubler le débit. Dans les réseaux de production, la norme se situe plutôt entre 20 et 26 Mbits/s.

Les équipements 802.11g fournissent la même bande passante que les équipements 802.11a, mais avec une compatibilité en amont pour les équipements 802.11b utilisant la technologie de modulation OFDM (*Orthogonal Frequency Division Multiplexing* ou *multiplexage par*

répartition orthogonale de la fréquence) et fonctionnent dans la bande de transmission de 2,4 GHz. Cisco a développé un point d'accès qui autorise les équipements 802.11b et 802.11a à coexister sur le même LAN sans fil. Ce point d'accès fournit des services de passerelle permettant à ces équipements normalement incompatibles de communiquer entre eux.

Types d'authentification et d'association

- Non authentifié et non associé
  - Le nœud est déconnecté du réseau et non associé à un point d'accès.
- Authentifié et non associé
  - Le nœud a été authentifié sur le réseau mais n'est pas encore associé au point d'accès.
- Authentifié et associé
  - Le nœud est connecté au réseau et peut transmettre et recevoir des données via le point d'accès.

Méthodes d'authentification
La norme IEEE 802.11 spécifie deux types de processus d'authentification.

Le premier est le système ouvert (open). Il s'agit d'une norme de connectivité standard dans laquelle seul le SSID doit correspondre. Cette norme peut être utilisée dans un environnement sécurisé ou non, bien qu'il soit fort probable que des sniffeurs de réseau de niveau inférieur découvrent le SSID du réseau LAN sans fil.

Le second processus est la clé partagée (shared key). Ce processus requiert l'utilisation du cryptage WEP (*Wired Equivalent Privacy*), un algorithme simple utilisant des clés de 64 et 128 bits. Le point d'accès est configuré avec une clé cryptée, et les nœuds tentant d'accéder au réseau via le point d'accès doivent disposer d'une clé correspondante. Les clés WEP attribuées de façon statique fournissent un niveau de sécurité supérieur à celui du système ouvert, mais elles ne sont pas inviolables.

4)

Le décibel (dB) est une unité de mesure utilisée pour décrire des signaux réseau. Son calcul fait appel aux exposants et aux logarithmes décrits précédemment. Deux formules servent à calculer les décibels:

$dB = 10 \log_{10}(P_{final} / P_{réf})$

$dB = 20 \log_{10} (V_{final} / V_{réf})$

- Diaphonie locale (NEXT)
- Diaphonie distante (FEXT)
- Diaphonie locale totale (PSNEXT)

La diaphonie locale (NEXT) est calculée selon le rapport d’amplitude entre le signal test et le signal de diaphonie mesurés à la même extrémité de la liaison. [1] Cette différence est exprimée par une valeur négative en décibels (dB). Des valeurs négatives faibles indiquent une plus grande présence de bruit, tout comme des températures négatives faibles indiquent plus de chaleur. En règle générale, les testeurs de câbles n’affichent pas le signe moins indiquant une valeur de diaphonie locale négative. Une valeur de diaphonie locale affichée de

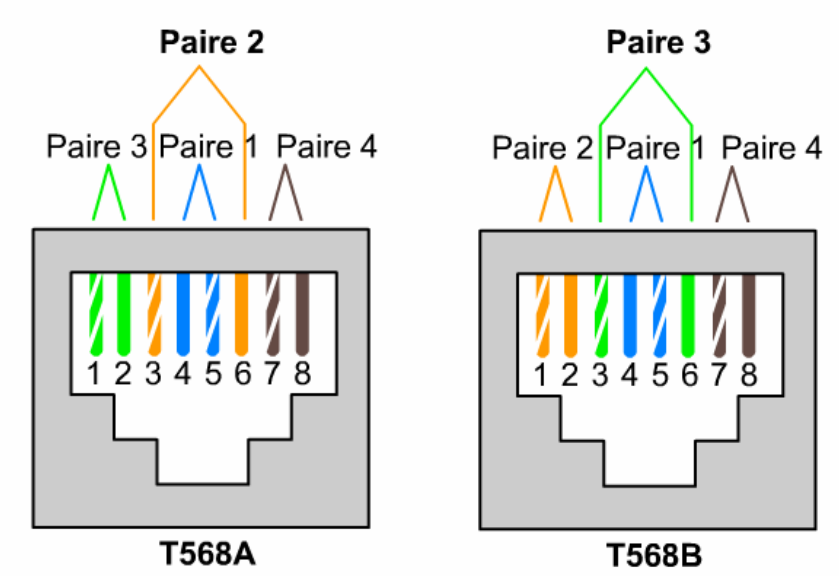
30 dB (qui signifie en fait –30 dB) indique un bruit de diaphonie locale moindre et un signal plus net qu'une valeur affichée de 10 dB.

La diaphonie locale doit être mesurée entre chaque paire et chacune des autres paires dans une liaison UTP, ainsi qu'à chacune de ses extrémités. Afin de réduire la durée des tests, certains appareils de test des câbles permettent à l'utilisateur de tester la performance de la diaphonie locale d'une liaison en utilisant des intervalles de fréquences plus grands que ceux spécifiés par la norme TIA/EIA. Néanmoins, les mesures obtenues se sont pas nécessairement conformes aux normes TIA/IEA-568-B et peuvent ne pas permettre de détecter toutes les défaillances d'une liaison. Afin de vérifier que la performance de la liaison est correcte, la diaphonie locale doit être mesurée à chaque extrémité de la liaison à l'aide d'un appareil de test de qualité. Il s'agit d'une condition nécessaire pour une conformité totale avec les normes pour câbles à haut débit.

En raison de l'atténuation, une diaphonie intervenant à un point éloigné de l'émetteur crée moins de bruit sur un câble qu'une diaphonie locale. C'est une diaphonie distante, ou FEXT. [2] Le bruit occasionné par une diaphonie distante (FEXT) retourne lui aussi vers la source mais est atténué. Par conséquent, la diaphonie distante n'est pas aussi problématique que la diaphonie locale.

La diaphonie locale totale (PSNEXT) mesure l'effet cumulé d'une diaphonie locale provenant de toutes les paires d'un câble. [3] Pour chaque paire, la diaphonie locale totale se calcule selon les effets de diaphonie locale des trois autres paires. L'effet combiné de la diaphonie provenant de sources de transmission simultanées multiples peut être très nuisible pour le signal. La certification TIA/EIA-568-B exige désormais ce test de diaphonie locale totale.

Certains standards Ethernet comme 10BaseT et 100BaseTX reçoivent des données à partir d'une seule paire de fils par direction. Cependant, pour des technologies plus récentes telles que 1000BaseT, qui reçoivent des données simultanément à partir de paires multiples dans la même direction, les tests de diaphonie totale sont très importants.

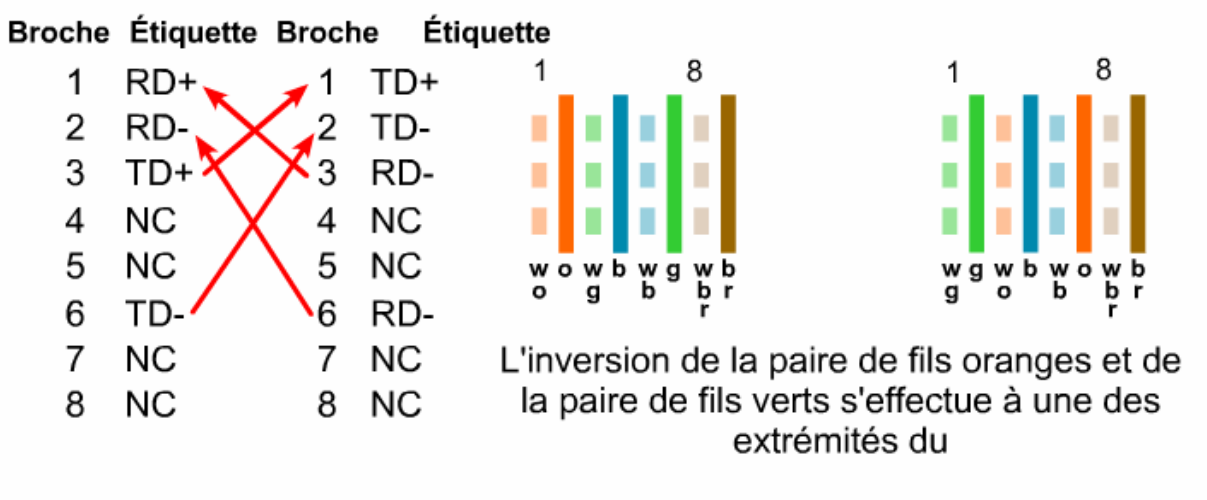


5)1

	10BASE2	10BASE5	10BASE-T	100BASE-TX	100BASE-FX
Médias	Câble coaxial de 50 ohms (Ethernet à câble fin)	Câble coaxial de 50 ohms (Ethernet épais)	Câble EIA/TIA Catégorie 3, 4, 5 UTP, deux paires	Câble EIA/TIA Catégorie 5 UTP, deux paires	Fibre multimode de 62,5/125
Longueur maximale du segment	185 m	500 m	100 m	100 m	400 m
Topologie	En bus	En bus	En étoile	En étoile	En étoile
Connecteur	BNC	AUI (Attachment Unit Interface)	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur d'interface média duplex Connecteur ST ou SC

1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX
STP	Câble EIA/TIA catégorie 5 UTP, quatre paires	Fibre multimode de 62,5/50 microns.	Fibre multimode de 62,5/50 microns ; fibre monomode de 9 microns.
25 m	100 m	275 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns	440 m pour la fibre de 62,5 microns ; 550 m pour la fibre de 50 microns ; de 3 à 10 km pour la fibre monomode.
En étoile	En étoile	En étoile	En étoile
ISO 8877 (RJ-45)	ISO 8877 (RJ-45)	Connecteur SC	Connecteur SC

Cable croisé :



5.1.5

La norme EIA/TIA spécifie un connecteur RJ-45 pour câble UTP. L'acronyme RJ correspond à Registered Jack et le numéro 45 désigne un ordre de connexion des fils spécifique. Le connecteur RJ-45 à extrémités transparentes comporte huit fils de couleur. Quatre de ces fils (T1 à T4), appelés «tips», acheminent la tension. Les quatre autres fils (R1 à R4), ou «rings», sont mis à la terre. Les termes « tip » et « ring » remontent à l'apparition du téléphone. Ils désignent aujourd'hui le fil positif et le fil négatif d'une paire. Les fils de la première paire d'un câble ou d'un connecteur sont appelés T1 et R1. La deuxième paire correspond à T2 et R2, la troisième à T3 et R3, et la quatrième à T4 et R4.

Le connecteur RJ-45 représente le composant mâle, serti à l'extrémité du câble. Vus de face, les emplacements des broches d'un connecteur mâle sont numérotés de 8 à 1 de la gauche vers la droite, comme l'illustre la figure.

La prise constitue le composant femelle d'un équipement réseau, d'une prise murale ou d'un panneau de brassage, comme l'illustre la figure. La figure montre les connexions à l'arrière de la prise à laquelle se raccorde le câble UTP Ethernet.

Pour que l'électricité circule entre le connecteur et la prise, l'ordre des fils doit respecter le code de couleurs T568A ou T568B de la norme EIA/TIA-568-B.1, comme le montre la figure . Pour déterminer la catégorie de câble EIA/TIA à utiliser pour raccorder un équipement, consultez la documentation de l'équipement concerné ou recherchez, sur celui-ci, une étiquette proche de la prise. En l'absence d'étiquette et de documentation, utilisez la catégorie 5e ou une catégorie supérieure, les catégories supérieures étant susceptibles de remplacer celles qui leur sont inférieures. Puis, déterminez si vous allez utiliser un câble droit ou un câble croisé.

Si vous maintenez les deux connecteurs RJ-45 d'un câble côte à côte et dans le même sens, vous voyez les fils de couleur dont ils se composent. Si les fils de couleur se présentent dans le même ordre à chaque extrémité, il s'agit d'un câble droit, tel que celui qui est représenté dans la figure .

Dans le cas d'un câble croisé, certains fils placés aux deux extrémités des connecteurs RJ-45 se raccordent à des broches différentes à chaque extrémité du câble. La figure montre que les broches 1 et 2 d'un connecteur se raccordent aux broches 3 et 6 de l'autre.

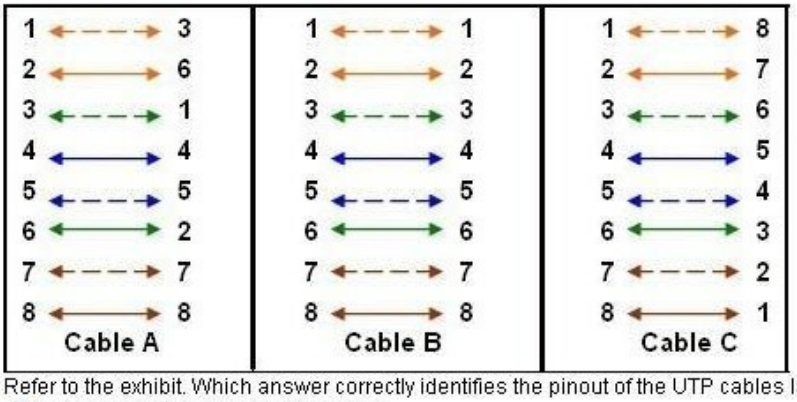
La figure illustre les directives qui permettent de déterminer le type de câble à utiliser pour relier les équipements Cisco.

Utilisez des câbles droits pour les liaisons suivantes:

- Commutateur vers routeur
- Commutateur vers PC ou serveur
- Concentrateur vers PC ou serveur

Utilisez des câbles croisés pour les liaisons suivantes:

- Commutateur vers commutateur
- Commutateur vers concentrateur
- Concentrateur vers concentrateur
- Routeur vers routeur
- PC vers PC
- Routeur vers PC

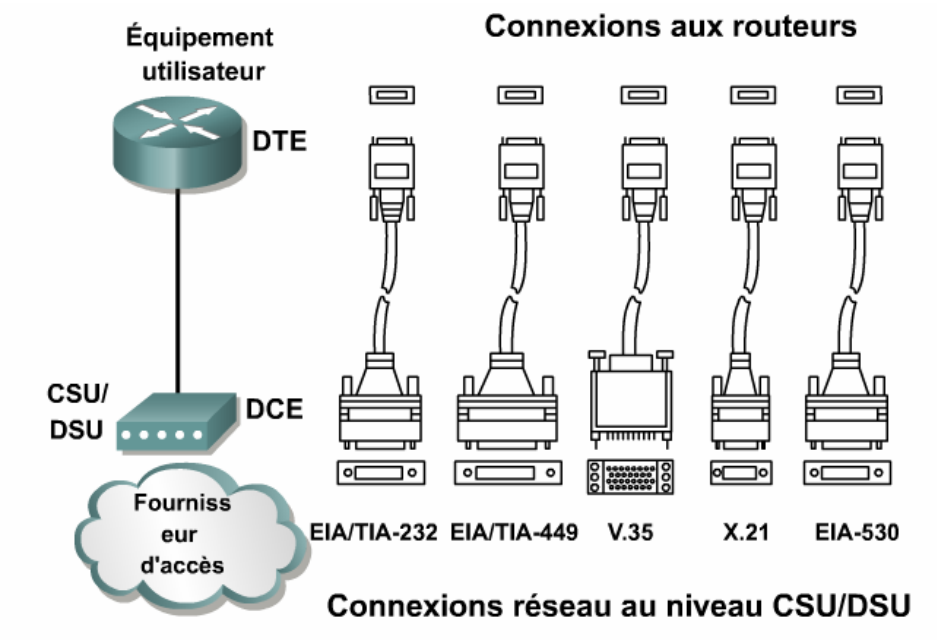


Refer to the exhibit. Which answer correctly identifies the pinout of the UTP cables labeled Cable A, Cable B, and Cable C?

- A=straight, B=rollover, C=crossover
- A=rollover, B=crossover, C=straight
- A=crossover, B=straight, C=straight
- A=crossover, B=straight, C=rollover
- A=straight, B=crossover, C=rollover
- A=rollover, B=straight, C=crossover

Concentrateurs :
Les concentrateurs (Hub) sont, en fait, des répéteurs multiports. La différence entre un concentrateur et un répéteur réside dans le nombre de ports respectifs de ces équipements. Un répéteur classique possède généralement deux ports et un concentrateur entre 4 et 24 ports

Connection WAN :

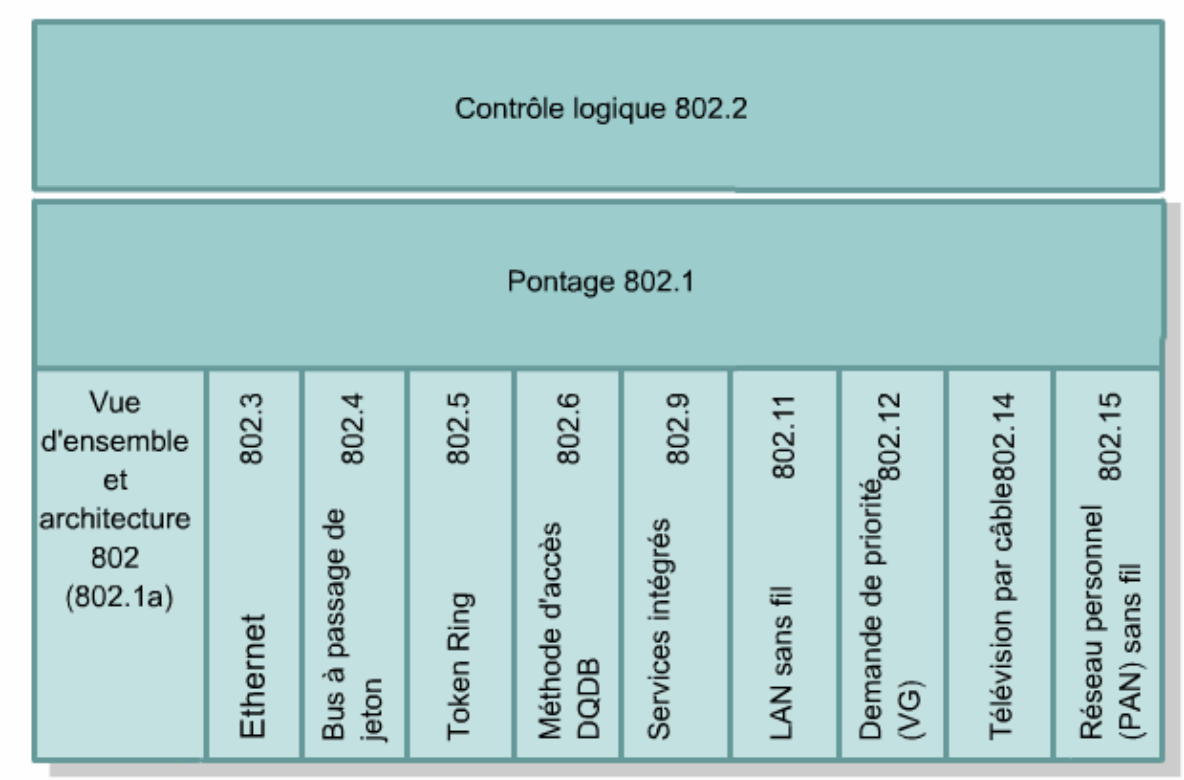


6)
Technologie Ethernet

Vitesse	Méthode de signalisation	Média
10	BASE	2
100	LARGE	5
1000		-T
10G		-TX
		-SX
		-LX

- Un chiffre qui indique le nombre de Mbits/s transmis
- Des lettres pour indiquer que la signalisation de la bande de base est utilisée
- Une ou plusieurs lettres de l'alphabet indiquant le type de média utilisé. Par exemple, F = câble à fibre optique et T = paire de cuivre torsadée non blindée

Norme IEEE 802.x



Adresse MAC : (*Media Access Control*)

Un système d'adressage est nécessaire pour identifier de façon unique les ordinateurs et les interfaces qui permettent une distribution locale des trames sur Ethernet. Ethernet utilise des adresses MAC qui comportent 48 bits et qui sont exprimées à l'aide de douze chiffres hexadécimaux. Les six premiers chiffres hexadécimaux, qui sont administrés par l'IEEE, identifient le fabricant ou le fournisseur. Cette partie de l'adresse MAC est appelée identifiant unique d'organisation (OUI). Les six autres chiffres hexadécimaux forment le numéro de série d'interface ou une autre valeur administrée par le fabricant. On dit parfois des adresses MAC qu'elles sont rémanentes (BIA - *burned-in adresses*) parce qu'elles demeurent en mémoire morte (ROM) et sont copiées en mémoire vive (RAM) lors de l'initialisation de la carte réseau.

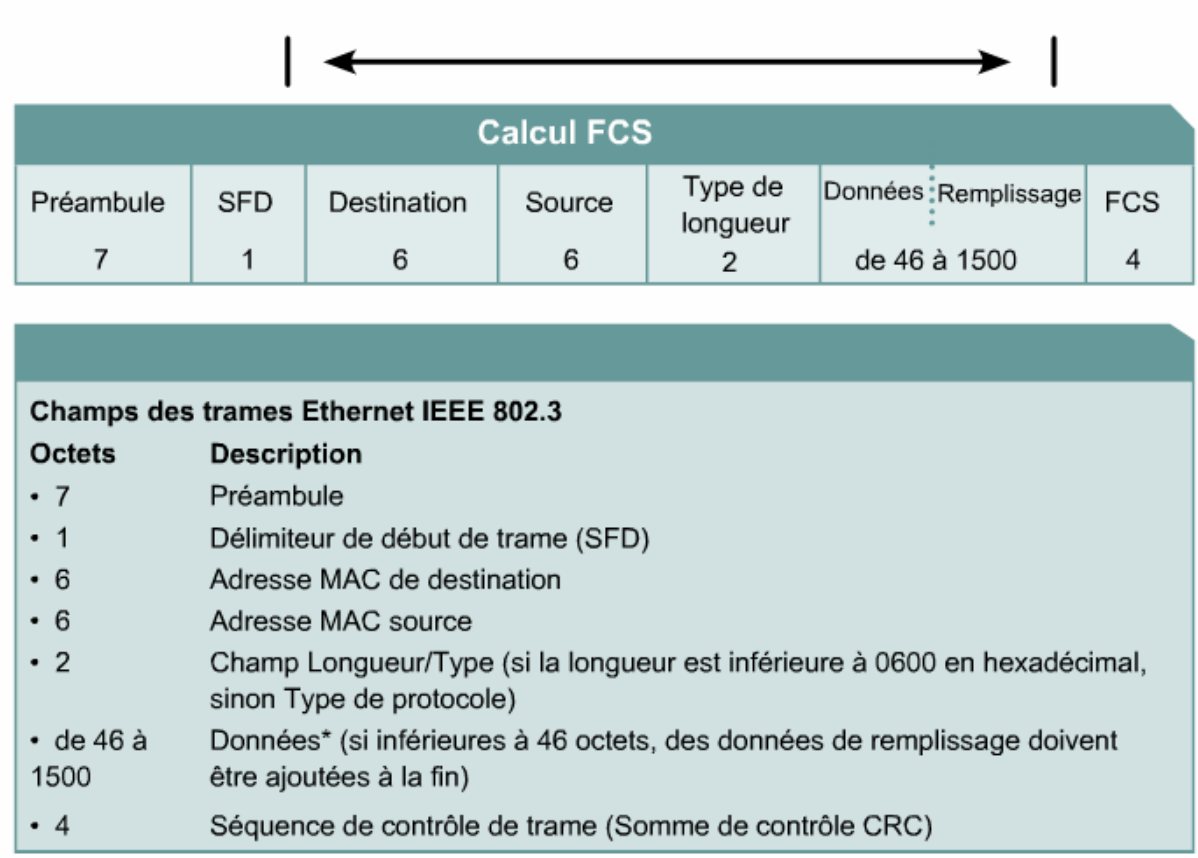
Au niveau de la couche liaison de données, des en-têtes et des en-queues MAC sont ajoutés aux données de la couche supérieure. Ces en-têtes et en-queues contiennent des informations de contrôle destinées à la couche liaison de données du système de destination. Les données des couches supérieures sont encapsulées dans la trame liaison de données, entre l'en-tête et l'en-queue, puis envoyées sur le réseau.

La carte réseau utilise l'adresse MAC afin de déterminer si un message doit être transmis aux couches supérieures du modèle OSI. Elle n'utilise pas de temps processeur pour effectuer cette évaluation, ce qui améliore les temps de communication sur le réseau Ethernet.

Sur un réseau Ethernet, lorsqu'un équipement envoie des données, il peut ouvrir une voie de communication en utilisant l'adresse MAC de l'autre équipement. L'équipement source attache un en-tête avec l'adresse MAC de l'équipement de destination prévu, et envoie des données sur le réseau. Tandis que les données se déplacent sur le média réseau, la carte réseau

de chaque équipement du réseau vérifie si son adresse MAC correspond à l'adresse physique de destination transportée par la trame de données. En l'absence de correspondance, la carte réseau ignore la trame de données. Lorsque les données atteignent le nœud de destination, la carte réseau fait une copie et transmet la trame aux couches OSI. Sur un réseau Ethernet, tous les nœuds doivent examiner l'en-tête MAC.

Ethernet IEEE 802.3



Champs des trames Ethernet IEEE 802.3

Octets	Description
• 7	Préambule
• 1	Délimiteur de début de trame (SFD)
• 6	Adresse MAC de destination
• 6	Adresse MAC source
• 2	Champ Longueur/Type (si la longueur est inférieure à 0600 en hexadécimal, sinon Type de protocole)
• de 46 à 1500	Données* (si inférieures à 46 octets, des données de remplissage doivent être ajoutées à la fin)
• 4	Séquence de contrôle de trame (Somme de contrôle CRC)

Espace intertrame :

Vitesse	Espacement intertrame	Temps nécessaire
10 Mbps	96 temps de bit	9.6 µs
100 Mbps	96 temps de bit	0.96 µs
1 Gbps	96 temps de bit	0.096 µs
10 Gbps	96 temps de bit	0.0096 µs

Paramètre de tranches de temps :

Vitesse	Tranche de temps	Intervalles de temps
10 Mbps	512 temps de bit	51.2 µs
100 Mbps	512 temps de bit	5.12 µs
1 Gbps	4096 temps de bit	4.096 µs
10 Gbps	non applicable	non applicable

L’espacement minimum entre deux trames n’entrant pas en collision est appelé espacement intertrame. Cet espacement a pour limites le dernier bit du champ de la FCS de la première trame et le premier bit du préambule de la deuxième trame.

Lorsqu'une trame est envoyée, toutes les stations d'un réseau Ethernet 10 Mbits/s doivent attendre au minimum une durée de 96 bits, soit 9,6 microsecondes, avant qu’une autre station ait le droit de transmettre la trame suivante. Sur les versions plus rapides d’Ethernet, l’espacement reste le même, à savoir 96 temps de bit, mais le temps nécessaire pour cet intervalle se réduit de façon proportionnelle. On appelle cet intervalle écart d’espacement. Cet écart est prévu pour donner le temps aux stations lentes de traiter la trame précédente et de se préparer pour la suivante.

Un répéteur doit régénérer les 64 bits d’informations de synchronisation, correspondant au préambule et à la SFD, au début de chaque trame. Cela doit se faire malgré la perte potentielle de certains bits de début de préambule en raison de la lenteur de la synchronisation. À cause de cette réintroduction forcée de bits de synchronisation, une certaine réduction minime de l’écart intertrame est non seulement possible mais attendue. Certains jeux de circuits Ethernet sont sensibles à un raccourcissement de l’espacement intertrame, et risquent de ne plus pouvoir détecter les trames en cas de réduction de l’écart. En raison de l’augmentation de leur puissance de traitement, les ordinateurs personnels pourraient très facilement saturer un segment Ethernet de trafic et commencer à retransmettre avant l’observation du délai d’espacement intertrame.

Lorsque la collision s’est produite et que toutes les stations rendent le câble inactif (en attente de l’espacement intertrame complet), alors les stations à l’origine de la collision doivent observer un délai supplémentaire et potentiellement de plus en plus long avant de tenter de retransmettre la trame entrée en collision. Le délai d’attente est conçu intentionnellement pour être aléatoire afin que les deux stations n’observent pas le même délai avant de retransmettre, ce qui entraînerait d’autres collisions. Pour cela, on étend l’intervalle qui sert de base à la sélection du temps de retransmission lors de chaque tentative de retransmission. La période d’attente est mesurée par incréments de tranche de temps.

Si la couche MAC est incapable d’envoyer la trame après seize tentatives, elle abandonne et génère une erreur sur la couche réseau. Une telle situation est assez rare et ne peut se produire qu’en cas de surcharge extrême du réseau, ou lorsqu’il existe un problème physique.

Orde de priorité de transmission :

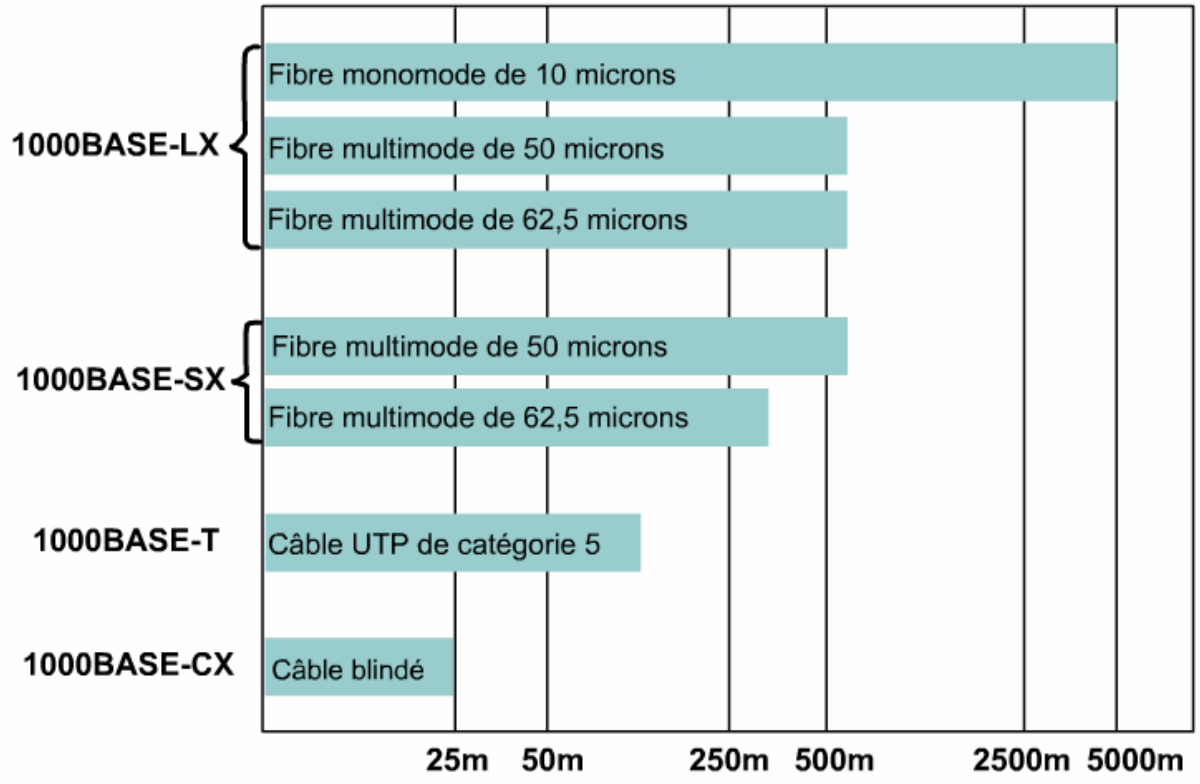
Il y a deux modes duplex, le mode half duplex et le mode full duplex. Le mode half duplex est obligatoire pour les médias partagés. Toutes les implémentations coaxiales sont en half duplex par nature et ne peuvent pas fonctionner en full duplex. Les implémentations UTP et en fibre optique peuvent fonctionner en half duplex. Les implémentations en 10 Gbits/s sont spécifiées pour le full duplex uniquement.

En half duplex, une seule station peut transmettre à la fois. Pour les implémentations coaxiales, la transmission d'une deuxième station entraîne le chevauchement et l'altération des signaux. Puisque le câble UTP et la fibre optique transmettent généralement sur des paires séparées, les signaux ne peuvent se chevaucher ou s'altérer. Ethernet a établi des règles d'arbitrage pour résoudre les conflits engendrés par des situations où plusieurs stations tentent de transmettre en même temps. Les deux stations d'une liaison point-à-point en mode full duplex sont autorisées à transmettre à n'importe quel moment, que l'autre station soit en transmission ou non.

7) Technologie Ethernet

Config des broches à prise modulaire en 10BASE-T et 100BASE-TX

Nombre de broches	Signal
1	TD+ (Envoi de données, signal différentiel positif)
2	TD- (Envoi de données, signal différentiel négatif)
3	RD+ (Réception de données, signal différentiel positif)
4	Inutilisé
5	Inutilisé
6	RD- (Réception de données, signal différentiel négatif)
7	Inutilisé
8	Inutilisé



In a departure from both 10BASE-T and 100BASE-TX, 1000BASE-T **uses all four cable pairs for simultaneous transmission in both directions** through the use of echo cancellation and a 5-level pulse amplitude modulation (PAM-5) technique

La version 10 Base 5 (10Mbps en bande de base sur câble coaxial d'une longueur maximale par segment de 500 mètres) est la version d'origine d'Ethernet,

10Gbits :

- **10GBASE-SR:** conçue pour les courtes distances sur des fibres optiques multimodes déjà installées, supporte une distance de 26 à 82 m.

- **10GBASE-LX4:** utilise le multiplexage de longueurs d'onde, supporte une distance de 240 à 300 m sur des fibres optiques multimodes déjà installées et 10 km sur des fibres optiques monomodes.
- **10GBASE-LR et 10GBASE-ER:** supportent une distance de 10 km et 40 km respectivement sur des fibres optiques monomodes.
- **10GBASE-SW, 10GBASE-LW et 10GBASE-EW:** généralement appelées « 10GBase-W », conçues pour fonctionner avec un équipement de réseaux WAN SONET et SDH, avec module de transport synchrone OC-192.

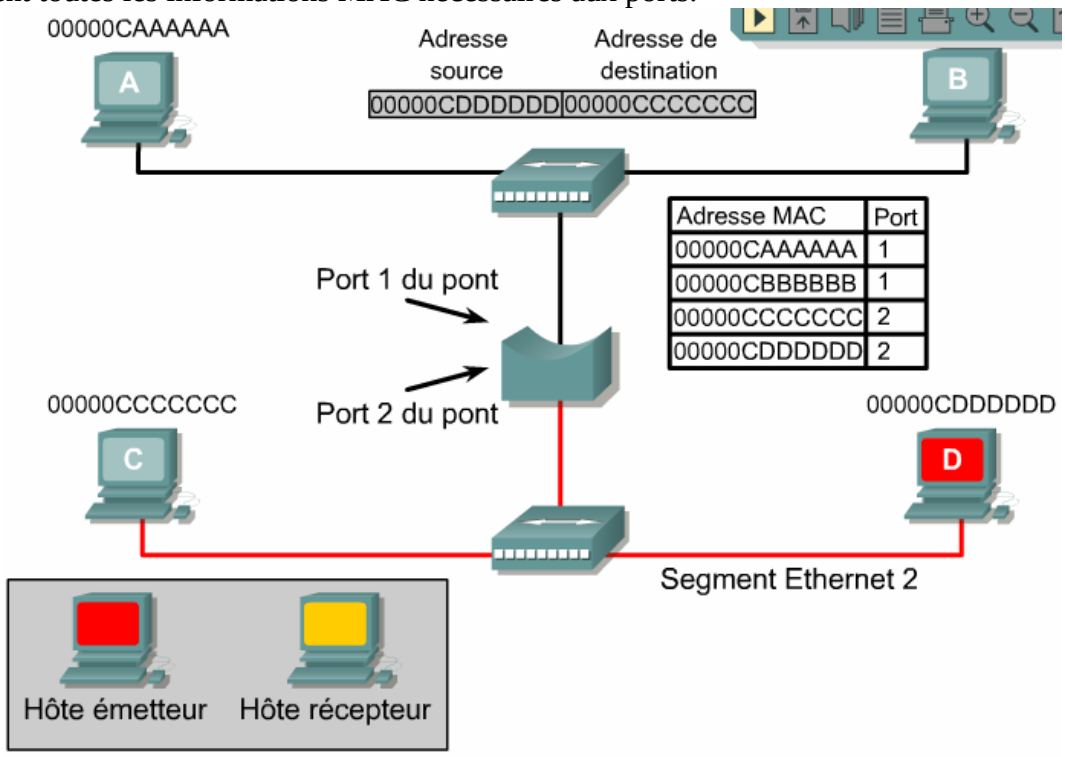
Mise en œuvre	Longueur d'	Média	Bande passante modale minimale	Longueur d'exploita
10GBASE-LX4	1310 nm	62.5µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	50µm MMF	400 MHz/km	2 - 240 m
10GBASE-LX4	1310 nm	50µm MMF	500 MHz/km	2 - 300 m
10GBASE-LX4	1310 nm	10µm MMF	N/A	2 - 10 km
10GBASE-S	850 nm	62.5µm MMF	160 MHz/km	2 - 26 m
10GBASE-S	850 nm	62.5µm MMF	200 MHz/km	2 - 33 m
10GBASE-S	850 nm	50µm MMF	400 MHz/km	2 - 66 m
10GBASE-S	850 nm	50µm MMF	500 MHz/km	2 - 82 m
10GBASE-S	850 nm	50µm MMF	2000 MHz/km	2 - 300 m
10GBASE-L	1310 nm	10µm SMF	N/A	2 - 10 km
10GBASE-E	1550 nm	10µm SMF	N/A	2 - 30 km

8) Commutation :

Bridge : pont : commutation niveau 2

Un pont comprend deux ports et subdivise un domaine de collision en deux segments. Les décisions prises par un pont dépendent uniquement des adresses MAC (ou adresses de couche 2) et n'affectent pas les adresses de couche 3 (ou adresses logiques). Un pont subdivise un domaine de collision, mais il n'a aucun effet sur le domaine logique ou de broadcast. Si un réseau ne dispose d'aucun équipement relié aux adresses de couche 3, tel qu'un routeur, le réseau tout entier partage le même espace d'adresse de broadcast logique. Un pont crée davantage de domaines de collision, mais n'ajoute pas de domaine de broadcast.

Un commutateur est en fait un pont multiport très rapide qui peut contenir des douzaines de ports. Chaque port crée son propre domaine de collision. Lorsqu'un réseau comporte 20 nœuds, 20 domaines de collision doivent exister si chaque nœud est connecté à son propre port de commutation. Dans le cas où un port uplink est installé, un commutateur crée 21 domaines de collision (nœuds uniques). Un commutateur crée et gère de façon dynamique une table de mémoire associative (CAM, *Content Addressable Memory*), qui contient toutes les informations MAC nécessaires aux ports.



La commutation d'une trame vers un port de destination est fonction du niveau de latence et de fiabilité. Un commutateur peut commencer à transférer la trame dès que l'adresse MAC est reçue. Ce mode de commutation des paquets est appelé «Cut-through»: il se caractérise par un temps de latence très faible. Cependant, la vérification des erreurs n'est pas effectuée. Un commutateur peut également attendre de recevoir la trame entière avant de la transférer vers le port de destination. Cela permet au logiciel de commutation de vérifier la séquence de contrôle de trame (FCS, *Frame Check Sequence*). Si la trame n'est pas correcte, elle est rejetée au niveau du commutateur. Étant donné que la trame entière est stockée avant d'être transmise, ce mode de commutation des paquets est appelé «Store-and-Forward». Une solution intermédiaire de commutation des paquets est le mode «Fragment-Free». Ce mode lit les 64 premiers octets, incluant l'en-tête de la trame, puis il commence à transmettre le paquet

avant même d'avoir terminé la lecture du champ de données et de la somme de contrôle. Ce mode vérifie la fiabilité des adresses et des informations relatives au protocole LLC afin de garantir que les données sont correctement traitées et qu'elles sont acheminées vers la destination appropriée.

Avec le mode de commutation «Cut-through», les débits des ports source et de destination doivent être identiques pour ne pas endommager la trame. On parle alors de commutation symétrique. Lorsque les débits sont différents, la trame utilise un certain débit pour la réception et un autre pour l'émission. C'est ce qu'on appelle une commutation asymétrique. Le mode «Store-and-Forward» doit être utilisé dans le cadre d'une commutation asymétrique.

Cette dernière fournit des connexions commutées entre les ports ayant une bande passante différente. La commutation asymétrique est particulièrement adaptée aux flux de trafic client-serveur où plusieurs clients communiquent avec un serveur simultanément. Une bande passante plus large doit être allouée au port du serveur afin d'éviter qu'un goulot d'étranglement ne se produise au niveau de ce port.

Le protocole STP :

C’est un protocole normalisé qui permet d'éviter les boucles de commutation. Chaque commutateur d'un réseau LAN qui utilise le protocole STP envoie un message appelé BDPU (*Bridge Protocol Data Unit*) par le biais de tous ses ports afin que les autres commutateurs soient informés de son existence. Les informations contenues dans ce message sont alors utilisées pour désigner le pont racine du réseau. Les commutateurs utilisent l'algorithme «spanning-tree» pour résoudre les chemins redondants.

Chaque port d'un commutateur utilisant le protocole STP a pour état l'un des cinq suivants:

- Blocage
- Écoute
- Apprentissage
- Acheminement
- Désactivation

Un port change d'état comme suit:

- De l'initialisation au blocage.
- Du blocage à l'écoute ou à la désactivation.
- De l'écoute à l'apprentissage ou à la désactivation.
- De l'apprentissage à l'acheminement ou à la désactivation.
- De l'acheminement à la désactivation.

Le protocole STP permet de créer une arborescence hiérarchique logique sans boucle. Cependant, des chemins de remplacement sont toujours disponibles, si nécessaire.

Les domaines de collision :

La règle des quatre répéteurs Ethernet stipule qu'un maximum de quatre répéteurs ou concentrateurs est autorisé entre deux ordinateurs de réseau

La règle dite de «5-4-3-2-1» requiert que les conditions suivantes soient respectées:

- Cinq segments de média réseau.
- Quatre répéteurs ou concentrateurs.
- Trois segments hôte de réseau;
- Deux sections de liaison sans hôte.
- Un grand domaine de collision.

La règle «5-4-3-2-1» fournit également des consignes pour que le délai maximal entre deux hôtes soit compris dans des limites acceptables.

(délais du répéteur + délais du câble + délais de la carte réseau) x 2 < délai maximal entre deux hôtes
Délais de répéteur 10BASE-T Par répéteur < 2 microsecondes Délais du câble ~ 0,55 microseconde tous les 100 mètres Délais carte réseau ~ 1 microseconde par carte
Le délai maximal entre deux hôtes (durée d'un bit 10BASE-T de 0,1 microseconde x taille minimale d'une trame de 512 bits) est de 51,2 microsecondes.

Pour un câble à paires torsadées non blindées d'une longueur de 500 mètres connecté par 4 répéteurs (ou concentrateurs) et 2 cartes réseau, le délai total serait largement inférieur au délai maximal entre deux hôtes.

Par exemple, la commande **telnet mumble.com** traduit un nom en une adresse IP lorsque vous utilisez le système DNS. Une requête ARP est diffusée pour localiser l'adresse MAC. En général, les stations de travail IP peuvent conserver de 10 à 100 adresses dans le cache ARP pendant environ 2 heures. Dans une station de travail standard, le débit du protocole ARP est d'environ 50 adresses toutes les 2 heures (soit 0,007 adresse par seconde). Par conséquent, 2 000 stations d'extrémité IP fourniront environ 14 adresses par seconde.

Flux de données :

Les données sont encapsulées à l'aide des adresses IP source et de destination au niveau de la couche réseau et des adresses MAC source et de destination au niveau de la couche liaison de données.

Voici la règle expliquant la différence: un équipement de couche 1 transmettra toujours une trame, alors qu’un équipement de couche 2 essayera toujours de la transmettre. En d’autres mots, l'équipement de couche 2 transmet toujours les trames à moins qu'un événement ne l'en empêche. Un équipement de couche 3 ne transmet pas de trame à moins d'y être obligé. L’utilisation de cette règle permet d’identifier comment les données sont acheminées sur un réseau.

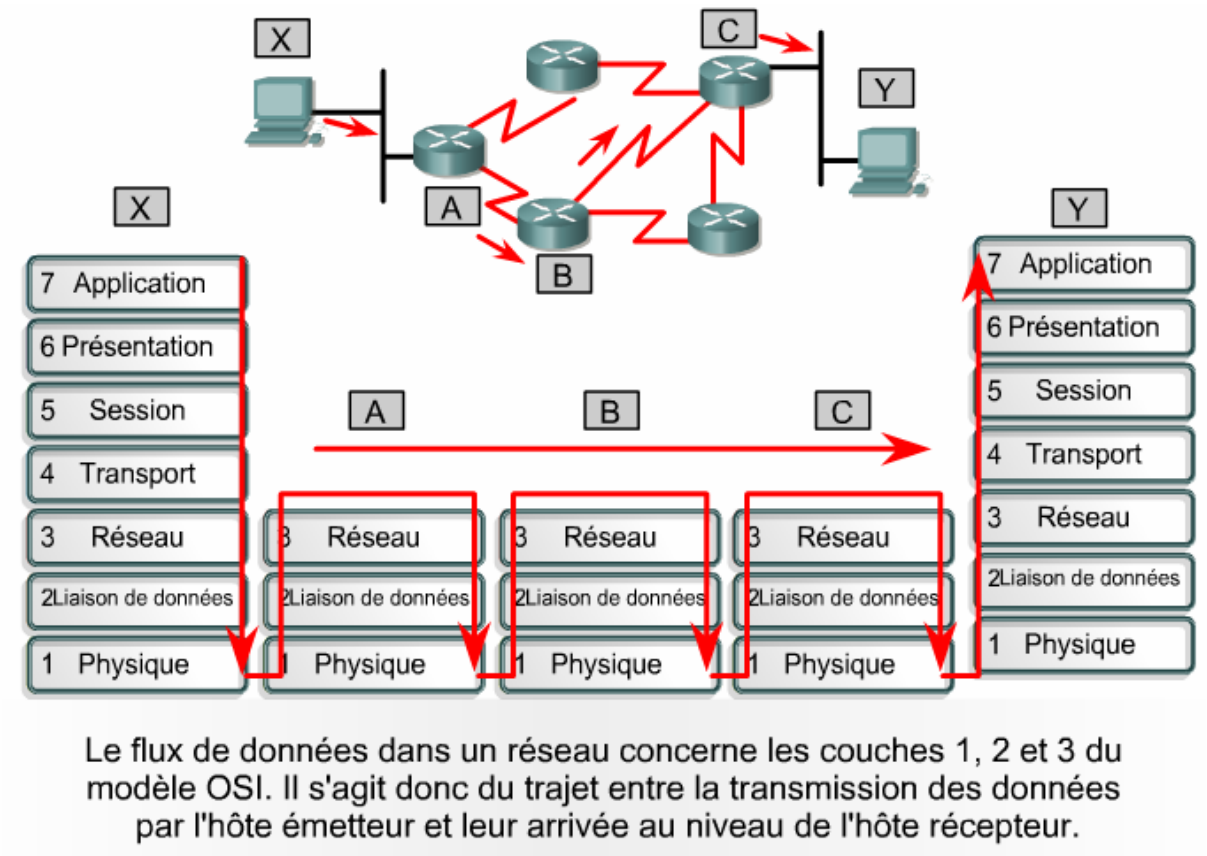
Les équipements de couche 1 n'effectuent pas de filtrage. Par conséquent, la totalité des données reçues est transmise au segment suivant. La trame est simplement régénérée et

resynchronisée afin de retrouver sa qualité de transmission initiale. Tous les segments reliés par des équipements de couche 1 appartiennent au même domaine (collision et broadcast).

Les équipements de couche 2 filtrent les trames de données en fonction des adresses MAC de destination. Une trame est transmise s'il s'agit d'une adresse inconnue qui se trouve en dehors du domaine de collision. La trame est également transmise s'il s'agit d'une adresse de broadcast, de multicast ou d'unicast devant être acheminée en dehors du domaine de collision local. La non-transmission d'une trame se produit uniquement dans le cas où un équipement de couche 2 détecte que l'hôte émetteur et l'hôte récepteur se trouvent dans le même domaine de collision. Un équipement de couche 2, tel qu'un pont, crée plusieurs domaines de collision, mais ne gère qu'un seul domaine de broadcast.

Les équipements de couche 3 filtrent les paquets de données en fonction des adresses IP de destination. Un paquet sera transmis uniquement si son adresse IP de destination est en dehors du domaine de broadcast et que le routeur a identifié l'adresse à laquelle envoyer le paquet. Un équipement de couche 3 crée plusieurs domaines de collision et de broadcast.

Le flux des données transitant sur un réseau de routage IP implique le passage des données par des équipements de gestion du trafic au niveau des couches 1, 2 et 3 du modèle OSI. La couche 1 sert à la transmission des données sur le média physique, la couche 2 à la gestion du domaine de collision et la couche 3 à la gestion du domaine de broadcast.



Le flux de données dans un réseau concerne les couches 1, 2 et 3 du modèle OSI. Il s'agit donc du trajet entre la transmission des données par l'hôte émetteur et leur arrivée au niveau de l'hôte récepteur.

9) Pile de protocole TCP/ IP et adressage IP

Modèle TCP/IP

Couche Application :

- **Le protocole FTP *(File Transfer Protocol)*:** ce protocole est un service fiable orienté connexion qui utilise le protocole TCP pour transférer des fichiers entre des systèmes qui le prennent en charge. Il gère les transferts bidirectionnels des fichiers binaires et ASCII.
- **Le protocole TFTP *(Trivial File Transfer Protocol)*:** ce protocole est un service non orienté connexion qui utilise le protocole de datagramme utilisateur UDP (*User Datagram Protocol*). Il est utilisé sur le routeur pour transférer des fichiers de configuration et des images de la plate-forme logicielle IOS Cisco, ainsi que pour transférer des fichiers entre des systèmes qui le prennent en charge. Il est utile dans certains LAN, car il s'exécute plus rapidement que le protocole FTP dans un environnement stable.
- **Le protocole NFS *(Network File System)*:** ce protocole est un ensemble de protocoles pour systèmes de fichiers distribués, développé par Sun Microsystems, permettant un accès aux fichiers d'un équipement de stockage distant, tel qu'un disque dur, dans un réseau.
- **Le protocole SMTP *(Simple Mail Transfer Protocol)*:** ce protocole régit la transmission du courrier électronique sur les réseaux informatiques. Il ne permet pas de transmettre des données autres que du texte en clair.
- **Telnet:** ce protocole permet d'accéder à distance à un autre ordinateur. Cela permet à un utilisateur d'ouvrir une session sur un hôte Internet et d'exécuter diverses commandes. Un client Telnet est qualifié d'hôte local. Un serveur Telnet est qualifié d'hôte distant.
- **Le protocole SNMP *(Simple Network Management Protocol)*:** ce protocole permet de surveiller et de contrôler les équipements du réseau, ainsi que de gérer les configurations, les statistiques, les performances et la sécurité.
- **Le protocole DNS *(Domain Name System)*:** ce protocole est utilisé par Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement.

Couche Transport :

Le rôle des protocoles TCP et UDP est le suivant:

- Segmenter les données d'application de couche supérieure.

- Envoyer des segments d'un équipement à un autre.

Le rôle du protocole TCP est le suivant:

- Etablir une connexion de bout en bout.
- Assurer le contrôle de flux à l'aide des fenêtres glissantes.
- Assurer la fiabilité du réseau à l'aide des numéros de séquençage et des accusés de réception.

Couche Internet :

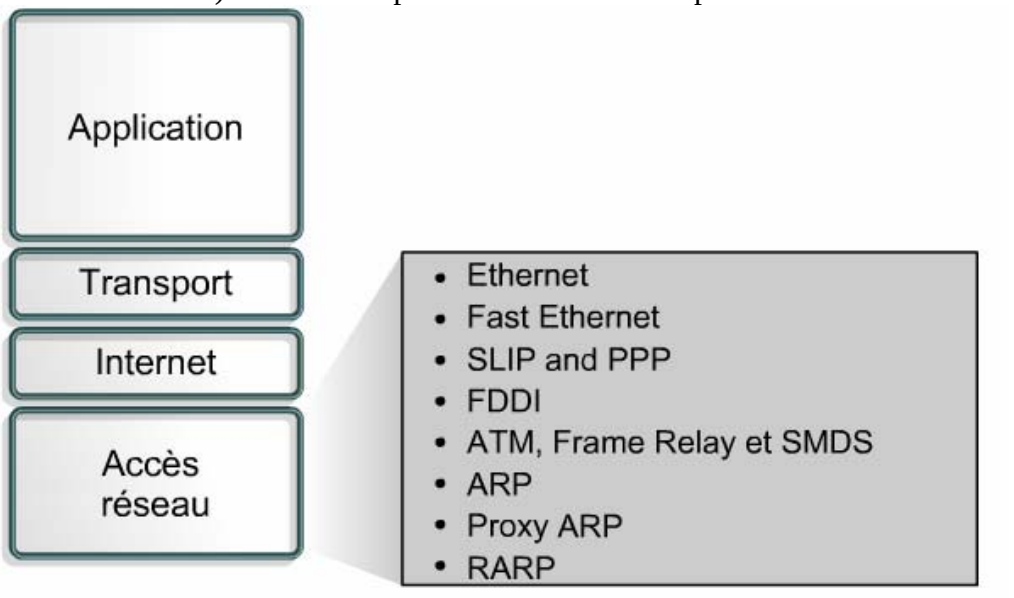
- Le protocole IP assure l'acheminement au mieux (best-effort delivery) des paquets, non orienté connexion. Il ne se préoccupe pas du contenu des paquets, mais il recherche un chemin pour les acheminer à destination.
- Le protocole ICMP (*Internet Control Message Protocol*) offre des fonctions de messagerie et de contrôle.
- Le protocole ARP (*Address Resolution Protocol*) détermine les adresses de la couche liaison de données ou les adresses MAC pour les adresses IP connues.
- Le protocole RARP (*Reverse Address Resolution Protocol*) détermine l'adresse IP pour une adresse MAC connue.

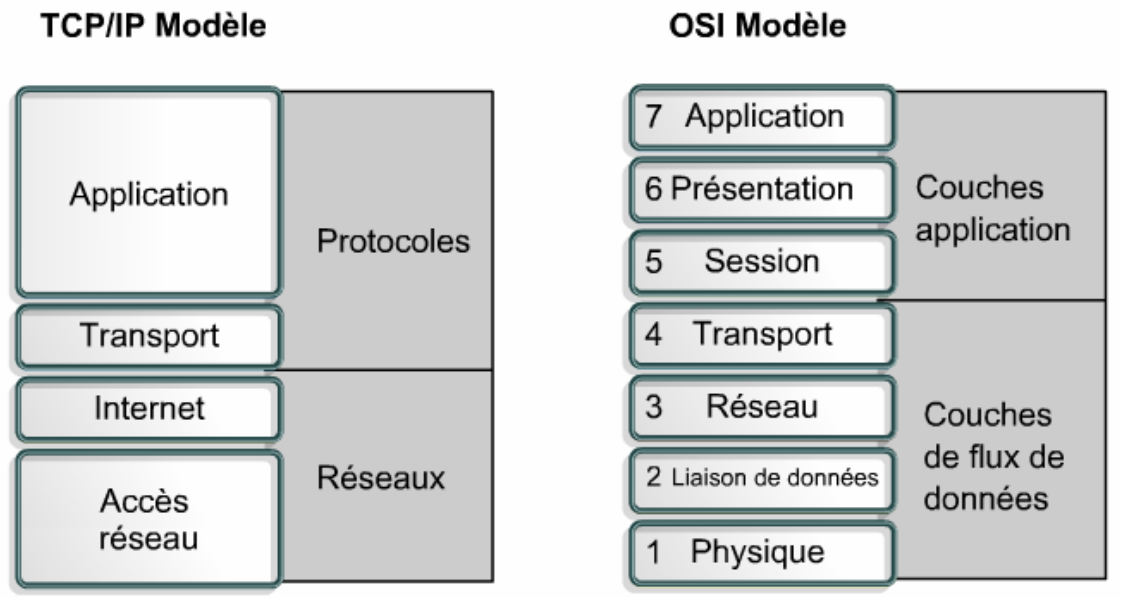
Le protocole IP effectue les opérations suivantes:

- Il définit un paquet et un système d'adressage.
- Il transfère des données entre la couche Internet et la couche d'accès au réseau.
- Il achemine des paquets à des hôtes distants.

Couche Accès Réseau :

Les protocoles de modem, à savoir les protocoles SLIP (*Serial Line Internet Protocol*) et PPP (*Point-to-Point Protocol*) sont utilisés pour accéder au réseau par modem.





2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Classe d'adresses IP :

Classe de l'adresse	Nombre de réseaux	Nombre d'hôtes par réseau
A	126 *	16,777,216
B	16,384	65,535
C	2,097,152	254
D (multicast)	S.O.	S.O.

Classe d'adresses IP	Bits de valeur supérieure	Plage d'adresses du premier octet	Nombre de bits de l'adresse réseau
Classe A	0	0 - 127 *	8
Classe B	10	128 - 191	16
Classe C	110	192 - 223	24
Classe D	1110	224 - 239	28

Classe d'adresses IP	Plage d'adresses IP (premier octet)
Classe A	1-126 (00000001-01111110) *
Classe B :	128-191 (10000000-10111111)
Classe C	192-223 (11000000-11011111)
Classe D	224-239 (11100000-11101111)
Classe E	240-255 (11110000-11111111)

IPv4 : 4 octets
IPv6 : 16 octets

Le protocole RARP :

Le protocole RARP associe des adresses MAC connues à des adresses IP. Cette association permet à certains équipements d'encapsuler les données avant de les envoyer sur le réseau. Un équipement réseau, tel qu'une station de travail sans disque dur local, peut connaître son adresse MAC mais ignorer son adresse IP. Le protocole RARP permet à l'équipement de lancer une requête afin de connaître son adresse IP. Les équipements utilisant le protocole de résolution inverse d'adresses requièrent un serveur RARP pour répondre aux requêtes de ce protocole.

Le protocole BOOTP :

Le protocole BOOTP fonctionne dans un environnement client-serveur et ne requiert qu'un seul échange de paquet pour obtenir des informations sur le protocole IP. Contrairement au protocole RARP, les paquets BOOTP peuvent contenir l'adresse IP, l'adresse du routeur, l'adresse du serveur ainsi que des informations spécifiques du fournisseur.

Le protocole DHCP :

Le protocole DHCP a été proposé pour succéder au protocole BOOTP. Contrairement au protocole BOOTP, le protocole DHCP permet à un hôte d'obtenir une adresse IP de manière dynamique sans que l'administrateur réseau ait à définir un profil pour chaque équipement. Avec le protocole DHCP, il suffit qu'une plage d'adresses IP soit définie sur un serveur DHCP. Lorsque les ordinateurs se connectent, ils communiquent avec le serveur DHCP et demandent une adresse. Le serveur DHCP choisit une adresse et l'affecte à l'ordinateur hôte. Grâce au protocole DHCP, la configuration réseau tout entière d'un ordinateur peut être obtenue dans un seul message. Cela comprend les données fournies par le message BOOTP, plus une adresse IP allouée et un masque de sous-réseau.

Les adresses IP sont attribuées aux hôtes comme suit:

- **De façon statique** (manuellement) – par l'administrateur réseau.
- **De façon dynamique** (automatiquement) – à l'aide des protocoles RARP, BOOTP ou DHCP.

10) Notions de base sur le routage et les sous-réseaux :

Un protocole décrit les éléments suivants:

- Le format de message requis.
- La manière dont les ordinateurs doivent échanger les messages d'activités spécifiques.

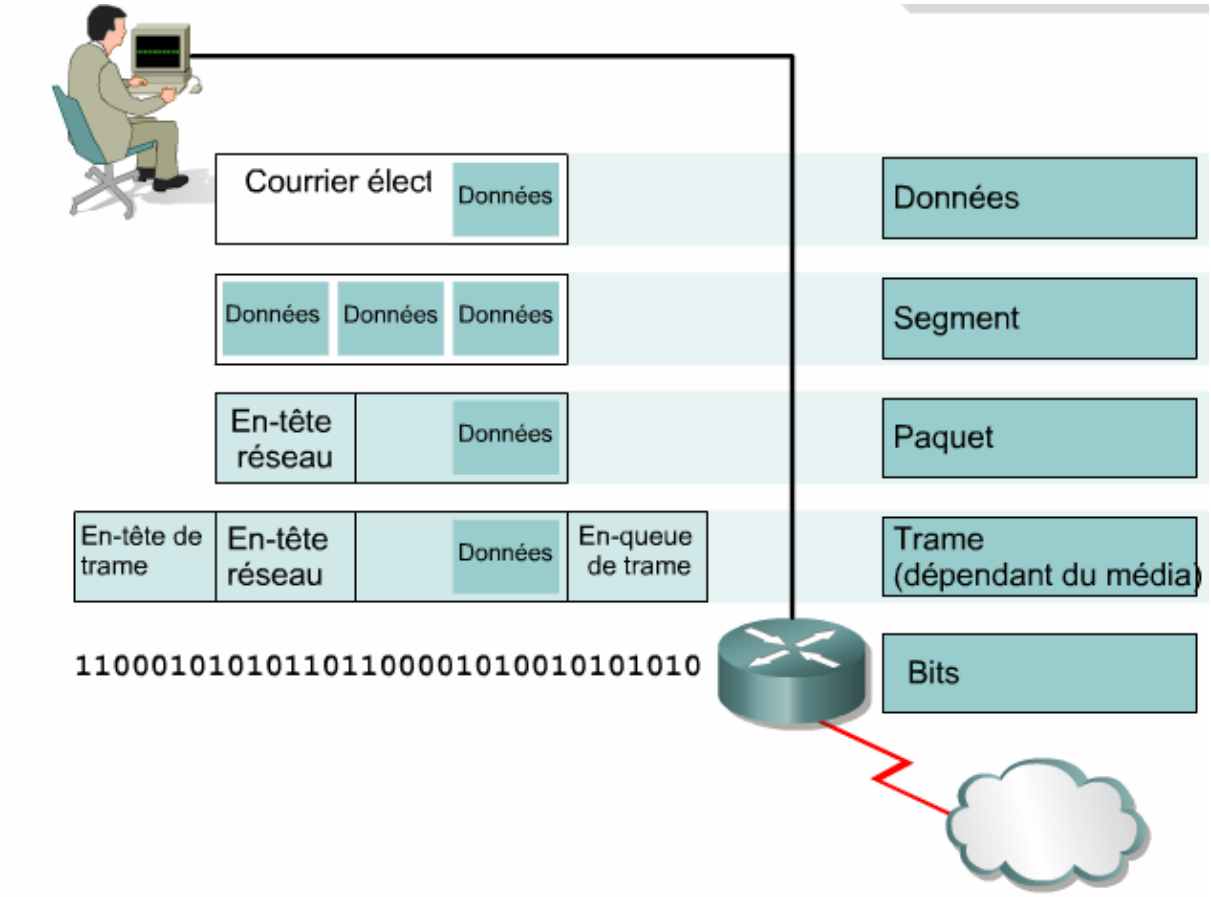
Certains protocoles, à l'instar du protocole IPX, ne requièrent que le numéro de réseau. Ils utilisent alors l'adresse MAC de l'hôte à la place de son numéro. D'autres protocoles, comme IP, nécessitent que l'adresse comporte une partie réseau et une partie hôte. Dans ce cas, un masque de réseau est nécessaire pour différencier ces deux numéros. L'adresse réseau est

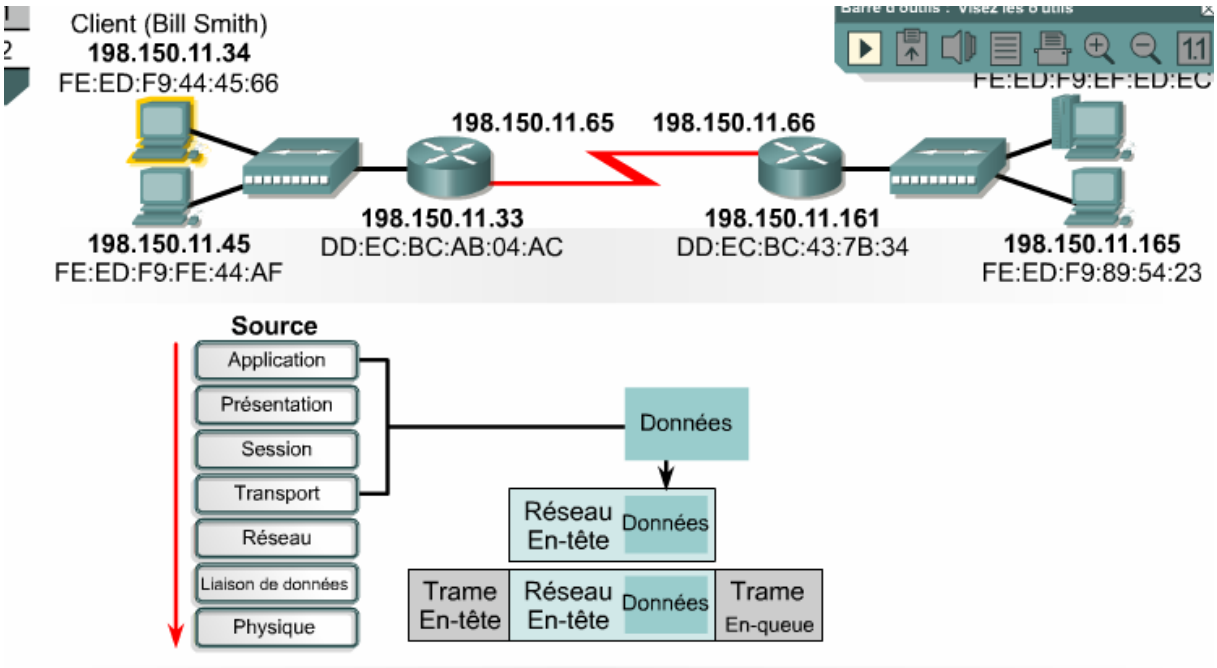
ensuite obtenue en effectuant une opération AND logique sur l'adresse et le masque de réseau.

IP est le système d'adressage hiérarchique des réseaux le plus largement utilisé. C'est un protocole non orienté connexion, peu fiable et axé sur l'acheminement au mieux (best-effort delivery).

Le protocole IP détermine le meilleur chemin pour les données en fonction du protocole de routage. Les termes «peu fiable» et «au mieux» ne signifient pas que le système n'est pas fiable et qu'il fonctionne mal, mais plutôt que le protocole IP ne s'assure pas de la bonne livraison des données envoyées sur le réseau. Si cette vérification est nécessaire, elle est effectuée par les protocoles de couche supérieure. «non orienté connexion» : aucune connexion à un circuit dédié n'est établie avant la transmission.

Les données sont traitées au niveau de chaque couche du modèle OSI au fur et à mesure qu'elles circulent vers le bas du modèle. Au niveau de la couche réseau, les données sont encapsulées dans des paquets. Ces paquets sont appelés des datagrammes. IP détermine le contenu de l'en-tête du paquet IP, qui contient les informations d'adressage. Il ne se préoccupe toutefois pas des données proprement dites. Il se contente de les accepter lorsqu'il les reçoit des couches supérieures.





La couche transport segmente, séquence et ajoute le contrôle d'erreur au message électronique. Les adresses source et de destination de la couche réseau sont ajoutées au datagramme. Le cache ARP fournit l'adresse MAC correspondant à l'adresse IP de destination. Ainsi, la trame Ethernet est ajoutée et comprend les adresses source et de destination.

10.1.3

Propagation d'un paquet et commutation au sein d'un routeur : **Tres interessant !!!**

La plupart des services réseau utilisent un système de livraison non orienté connexion. Les paquets peuvent emprunter différentes routes pour circuler sur le réseau. Ils sont ensuite rassemblés à leur arrivée.

- Système non orienté connexion, la destination n'est pas contactée avant l'envoi d'un paquet. Le système postal constitue une bonne analogie, puisque le destinataire du courrier n'est pas contacté pour savoir s'il acceptera la lettre avant son envoi. De même, l'expéditeur ne sait pas si sa lettre est arrivée à bon port.
- Systèmes orientés connexion, une connexion est établie entre l'émetteur et le récepteur avant le transfert des données. Le système téléphonique est un exemple de système orienté connexion. L'appelant initie l'appel, une connexion s'établit, puis la communication a lieu.

Les processus réseau **sans connexion** : processus à **commutation de paquets**. Au cours de leur acheminement, les paquets peuvent emprunter différents chemins et arriver de manière désordonnée. Chaque paquet contient des informations, telles que l'adresse de destination ainsi que la position dans le message, ce qui permet de coordonner l'arrivée avec les autres paquets associés. Lorsque la destination est atteinte, les paquets sont ainsi réassemblés selon la bonne séquence. Le chemin emprunté par chaque paquet est déterminé par divers critères.

Les processus réseau **orientés connexion** : processus à **commutation de circuits**. Une connexion avec le destinataire est établie avant que le transfert des données ne commence. Tous les paquets circulent de manière séquentielle sur le même circuit virtuel ou physique.

Internet est un réseau sans connexion gigantesque, dans lequel la majorité des transmissions de paquets sont traitées par le protocole IP. Le protocole TCP ajoute les services orientés connexion et fiables de la couche 4 au protocole IP.

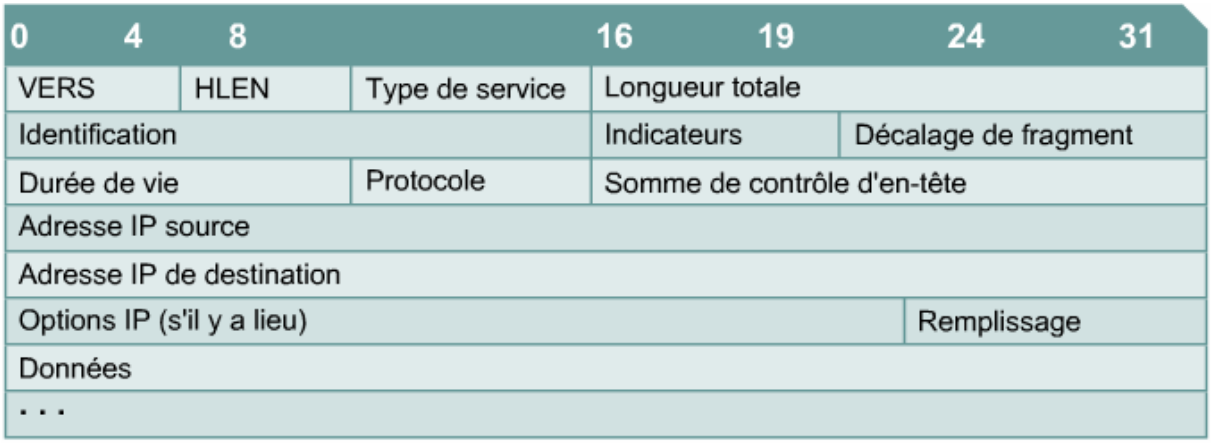
10.1.5
Anatomie d'un paquet IP

Les paquets IP comprennent les données des couches supérieures et un en-tête IP :

- **Version:** indique le format de l'en-tête du paquet IP. Le champ Version (4 bits) contient le numéro 4 s'il s'agit d'un paquet IPv4 ou le numéro 6 s'il s'agit d'un paquet IPv6. Ce champ n'est toutefois pas utilisé pour faire la distinction entre des paquets IPv4 et IPv6. C'est le rôle du champ relatif au type de protocole présent dans l'enveloppe de couche 2.
- **Longueur d'en-tête IP (HLEN):** indique la longueur de l'en-tête du datagramme en mots de 32 bits. Ce champ représente la longueur totale des informations d'en-tête et inclut les deux champs d'en-tête de longueur variable.
- **Type de service (ToS):** ce champ codé sur 8 bits indique le niveau d'importance attribué par un protocole de couche supérieure particulier.
- **Longueur totale (16 bits):** ce champ spécifie la taille totale du paquet en octets, données et en-tête inclus. Pour obtenir la taille des données proprement dites, soustrayez la longueur de l'en-tête IP de cette longueur totale.
- **Identification (16 bits):** identifie le datagramme actuel. Ce champ comporte le numéro de séquence.
- **Drapeaux (3 bits):** (indicateurs) champ dans lequel les deux bits de poids faible contrôlent la fragmentation. Un bit indique si le paquet peut être fragmenté ou non, et l'autre si le paquet est le dernier fragment d'une série de paquets fragmentés.
- **Décalage de fragment (13 bits):** champ permettant de rassembler les fragments du datagramme. Il permet au champ précédent de se terminer sur une frontière de 16 bits.
- **Durée de vie (TTL):** champ indiquant le nombre de sauts par lesquels un paquet peut passer. Ce nombre est décrémenté à chaque passage du paquet dans un routeur. Lorsque le compteur atteint zéro, le paquet est éliminé. Cela empêche les paquets de circuler indéfiniment en boucle.
- **Protocole (8 bits):** indique quel protocole de couche supérieure, tel que TCP ou UDP, reçoit les paquets entrants une fois les processus IP terminés.
- **Somme de contrôle de l'en-tête (16 bits):** champ qui aide à garantir l'intégrité de l'en-tête IP.
- **Adresse source (32 bits):** : champ indiquant l'adresse IP du nœud à partir duquel a été envoyé le paquet.
- **Adresse de destination (32 bits):** champ indiquant l'adresse IP du nœud vers lequel sont envoyées les données.
- **Options:** permet au protocole IP de prendre en charge diverses options, telles que la sécurité. La longueur de ce champ peut varier.
- **Remplissage:** des zéros sont ajoutés à ce champ pour s'assurer que l'en-tête IP est toujours un multiple de 32 bits.
- **Données:** ce champ contient les informations de couche supérieure. Sa longueur est variable.

Si les adresses IP source et de destination sont des champs capitaux, les autres champs de l'en-tête font du protocole IP un protocole très souple. Les champs de l'en-tête répertorient les informations d'adressage source et de destination du paquet et indiquent souvent la longueur

des données du message. Les informations de routage sont également contenues dans les en-têtes IP, qui, de ce fait, peuvent devenir longs et complexes.



Le routage est une fonction de la couche 3 du modèle OSI. C'est un système d'organisation hiérarchique qui permet de regrouper des adresses individuelles. Ces dernières sont traitées comme un tout jusqu'à ce que l'adresse de destination soit requise pour la livraison finale des données. Le routage cherche le chemin le plus efficace d'une unité à une autre. Le matériel au centre du processus de routage est le routeur.

Il possède les deux fonctions principales suivantes:

- Le routeur gère les tables de routage et s'assure que les autres routeurs ont connaissance des modifications apportées à la topologie du réseau. Il se sert des protocoles de routage pour échanger les informations de réseau.
- Le routeur détermine la destination des paquets à l'aide de la table de routage lorsque ceux-ci arrivent à l'une de ses interfaces. Il les transfère vers la bonne interface, ajoute les informations de trame de cette interface, puis transmet la trame.

Un routeur est une unité de couche réseau qui utilise une ou plusieurs métriques pour déterminer le chemin optimal par lequel acheminer le trafic réseau. Les métriques de routage sont les valeurs qui permettent de définir le meilleur chemin. Les protocoles de routage utilisent diverses combinaisons de ces métriques pour établir la meilleure route possible des données.

Les routeurs permettent d'interconnecter les segments d'un réseau ou des réseaux entiers. Leur rôle consiste à acheminer les trames de données entre les réseaux, en fonction des informations de la couche 3. Ils prennent des décisions logiques quant au meilleur acheminement possible des données, puis redirigent les paquets vers le port de sortie approprié afin qu'ils soient encapsulés pour la transmission. Les phases d'encapsulation et de désencapsulation se produisent à chaque passage d'un paquet dans un routeur. Le routeur doit en effet désencapsuler la trame de données de la couche 2 pour accéder à l'adresse de couche 3 et l'examiner.

L'encapsulation consiste à fractionner le flux de données en segments et à ajouter les en-têtes et les en-queues appropriés avant de transmettre les données. Le processus de désencapsulation, quant à lui, consiste à retirer les en-têtes et les en-queues, puis à recombiner les données en un flux continu.

Routage et comunication :

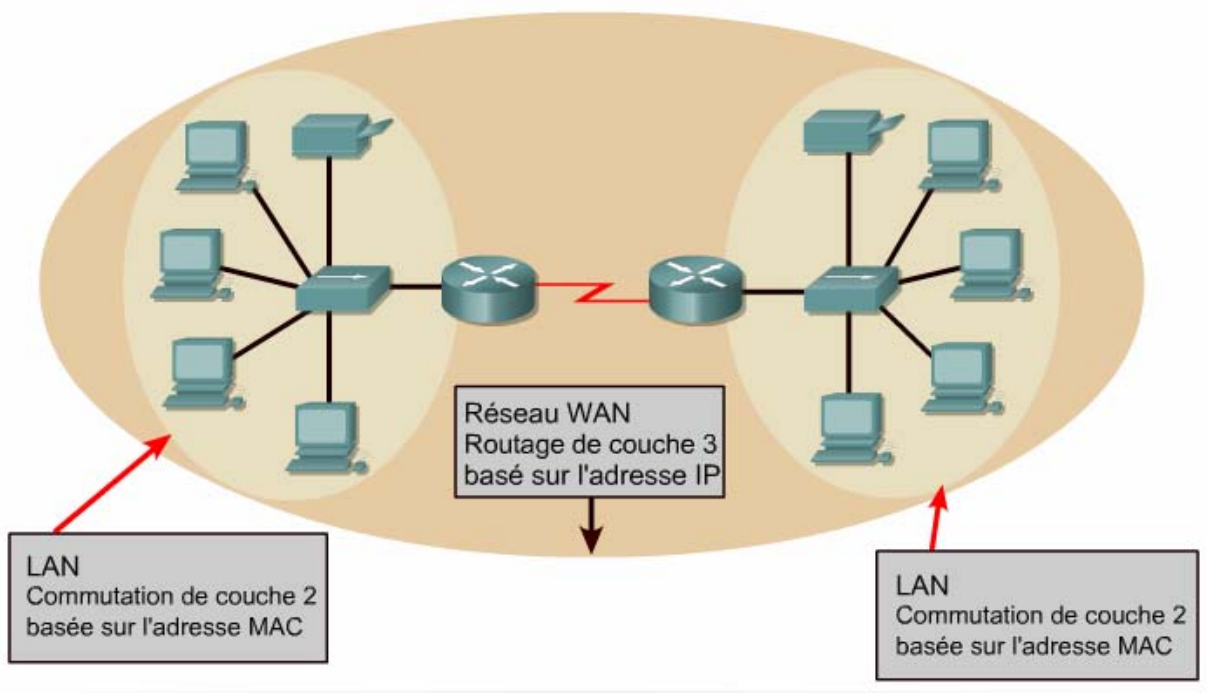
Le routeur joue un rôle similaire à celui du commutateur de niveau supérieur. La figure montre les tables ARP des adresses MAC de la couche 2 et les tables de routage des adresses IP de la couche 3. Chaque ordinateur et chaque interface de routeur gèrent une table ARP pour la communication de couche 2. La table ARP n'est utile que pour le domaine de broadcast auquel elle est connectée. Le routeur est également doté d'une table de routage qui lui permet d'acheminer les données hors du domaine de broadcast. Chaque entrée de table ARP contient une paire d'adresses IP-MAC.

Le commutateur de couche 2 établit sa table de transmission à l'aide d'adresses MAC. Lorsqu'un hôte possède des données pour une adresse IP non locale, il envoie la trame au routeur le plus proche. Ce routeur est également appelé « passerelle par défaut ». L'hôte se sert de l'adresse MAC du routeur comme adresse MAC de destination.

Un commutateur interconnecte des segments appartenant au même réseau ou sous-réseau logique. Dans le cas d'hôtes non locaux, le commutateur transfère la trame au routeur en fonction de l'adresse MAC de destination. Le routeur analyse alors l'adresse de destination de couche 3 du paquet afin de déterminer l'acheminement de la trame. L'hôte X connaît l'adresse IP du routeur parce que sa configuration IP contient l'adresse IP de la passerelle par défaut.

À l'instar du commutateur qui gère une table d'adresses MAC connues, le routeur possède une table d'adresses IP connue sous le nom de table de routage. Les adresses MAC ne sont pas organisées de manière logique, tandis que l'organisation des adresses IP est, elle, hiérarchique. Un commutateur se contentant de rechercher les adresses appartenant à son segment dans sa table, il ne traite qu'un nombre limité d'adresses MAC non organisées. Les routeurs, quant à eux, ont besoin d'un système d'adressage hiérarchique qui va permettre de regrouper les adresses similaires et de les traiter en tant qu'une seule et même unité réseau, et ce jusqu'à ce que les données atteignent le segment de destination.

Une autre différence entre les réseaux routés et commutés réside dans le fait que ces derniers ne bloquent pas les broadcasts. Les commutateurs peuvent par conséquent voir leur fonctionnement perturbé par des tempêtes de broadcasts. Les routeurs bloquant les broadcasts LAN, les tempêtes n'affectent que le domaine de broadcast dont elles sont issues. Du fait de ce blocage, les routeurs offrent une meilleure sécurité et un meilleur contrôle de la bande passante que les commutateurs.



La commutation de couche 2 s'effectue au sein du réseau LAN. Le routage de couche 3 achemine le trafic entre les domaines de broadcast. Cela nécessite le format d'adressage hiérarchique d'un système d'adressage de couche 3, tel que IP.

Fonctions	Routeur	Commutateur
Vitesse	Lente	Rapide
Couches OSI	Couche 3	Couche 2
Adressage utilisé	IP	MAC
Broadcasts	Bloqués	Transmis
Sécurité	Élevée	Faible

Les protocoles routés et les protocoles de routage :

Les protocoles routés transportent les données sur un réseau. Les protocoles de routage permettent aux routeurs de choisir le meilleur chemin possible pour acheminer les données de la source vers leur destination.

Le protocole routé englobe notamment les fonctions suivantes:

- Il inclut n'importe quelle suite de protocoles réseau capable de fournir assez d'informations dans l'adresse de couche réseau pour permettre au routeur d'effectuer le transfert vers l'unité suivante, jusqu'à la destination finale.
- Il définit le format et l'usage des champs dans un paquet.

Le protocole IP (*Internet Protocol*) et le protocole IPX (*Internetwork Packet Exchange*) de Novell, mais aussi DECnet, AppleTalk, Banyan VINES et Xerox Network Systems (XNS), sont des exemples de protocoles routés.

Les routeurs utilisent des protocoles de routage pour échanger des tables de routage et partager d'autres informations d'acheminement. En d'autres termes, les protocoles de routage permettent aux routeurs d'acheminer les protocoles routés.

Les fonctions du protocole de routage sont en partie les suivantes:

- Il fournit les processus utilisés pour partager les informations d'acheminement.
- Il permet aux routeurs de communiquer entre eux afin de mettre à jour et de gérer les tables de routage.

Les protocoles de routage prenant en charge le protocole routé IP sont par exemple les protocoles RIP, IGRP, OSPF, BGP et EIGRP.

Détermination du routage :

La détermination du chemin se produit au niveau de la couche réseau. Ce processus permet au routeur de comparer l'adresse de destination aux routes disponibles dans sa table de routage et de choisir le meilleur chemin possible. Les chemins configurés manuellement par l'administrateur réseau sont appelés «routes statiques». Ceux que le routeur a acquis d'autres routeurs à l'aide d'un protocole de routage sont dits «routes dynamiques».

La détermination du chemin permet au routeur de choisir le port à partir duquel envoyer un paquet pour que celui-ci arrive à destination. On appelle ce processus le routage d'un paquet. Chaque routeur rencontré sur le chemin du paquet est appelé un saut. Le nombre de sauts constitue la distance parcourue.

Les routeurs vont prendre leurs décisions en fonction de la charge, de la bande passante, du délai, du coût et de la fiabilité d'une liaison de réseau.

Les processus impliqués dans la sélection du chemin pour chaque paquet sont les suivants:

- Le routeur compare l'adresse IP du paquet reçu avec ses tables IP.
- Il extrait l'adresse de destination du paquet.
- Le masque de la première entrée dans la table de routage est appliqué à l'adresse de destination.
- La destination masquée est comparée avec l'entrée de la table de routage.
- Si une correspondance est établie, le paquet est transmis au port associé à cette entrée de table.
- Si aucune correspondance n'est établie, l'entrée suivante de la table est examinée.
- Si le paquet ne correspond à aucune des entrées de la table, le routeur recherche l'existence d'une route par défaut.
- Si une route par défaut a été définie, le paquet est transmis au port qui lui est associé. La route par défaut est le chemin qui doit être utilisé lorsque aucune correspondance n'a pu être établie avec la table de routage. Elle est configurée par l'administrateur réseau.
- Si aucun chemin par défaut n'existe, le paquet est éliminé. Un message est alors souvent envoyé à l'unité émettrice des données pour signaler que la destination n'a pu être atteinte.

Les routeurs conservent les informations suivantes dans leurs tables de routage:

- **Type de protocole:** cette information identifie le type de protocole de routage qui a créé chaque entrée.
- **Associations du saut suivant:** indique au routeur que la destination lui est directement connectée, ou qu'elle peut être atteinte par le biais d'un autre routeur appelé le «saut suivant» vers la destination finale. Dès réception d'un paquet, le routeur vérifie l'adresse de destination et tente de trouver une correspondance dans sa table de routage.
- **Métrique de routage:** les métriques utilisées varient selon les protocoles de routage et permettent de déterminer les avantages d'une route sur une autre. Par exemple, le protocole RIP se sert d'une seule métrique de routage : le nombre de sauts. Le protocole IGRP crée une valeur de métrique composite à partir des métriques de fiabilité, de délai, de charge et de bande passante.
- **Interfaces de sortie:** cette information désigne l'interface à partir de laquelle les données doivent être envoyées pour atteindre leur destination finale.

Les routeurs s'envoient des messages afin de mettre à jour leurs tables de routage. Certains protocoles de routage transmettent ces messages de manière périodique, ou lorsque des changements sont intervenus dans la topologie du réseau. Certains transmettent l'intégralité de la table dans leurs messages de mise à jour alors que d'autres se contentent d'envoyer les modifications. L'analyse des mises à jour de routage provenant de routeurs directement connectés permet aux routeurs de créer et de gérer leur table de routage.

10.2.6
Algorithmes et métriques de routage

Protocole	Métrique	Nombre maximum de routeurs	Origines
Protocole RIP	Nombre de sauts	15	Xerox
Protocole IGRP	• Bande passante • Charge • Délai • Fiabilité	255	Cisco

Les protocoles de routage sont conçus pour répondre à un ou plusieurs des objectifs suivants:

- **Optimisation:** capacité d'un algorithme de routage à sélectionner le meilleur chemin. Ce dernier sera choisi en fonction des métriques et de la pondération utilisées dans le calcul. Par exemple, un algorithme peut utiliser à la fois le nombre de sauts et le délai comme métriques, mais considérer que le délai doit prévaloir dans le calcul.
- **Simplicité et réduction du temps-système:** plus l'algorithme est simple et plus il sera traité efficacement par le processeur et la mémoire du routeur. Ce paramètre est important si le réseau veut pouvoir évoluer vers des proportions plus conséquentes, comme Internet.
- **Efficacité et stabilité:** un algorithme de routage doit pouvoir fonctionner correctement dans des circonstances inhabituelles ou imprévues, comme les défaillances de matériels, les surcharges et les erreurs de mise en œuvre.
- **Flexibilité:** un algorithme de routage doit pouvoir s'adapter rapidement à toutes sortes de modifications du réseau, touchant par exemple la disponibilité et la mémoire du routeur, la bande passante ou le délai réseau.
- **Rapidité de convergence:** la convergence est le processus par lequel tous les routeurs s'entendent sur les routes disponibles. Lorsqu'un événement sur le réseau entraîne des modifications au niveau de la disponibilité d'un routeur, des mises à jour sont

nécessaires afin de rétablir la connectivité du réseau. Une convergence lente des algorithmes de routage peut empêcher la livraison des données.

Les algorithmes de routage utilisent différentes métriques pour déterminer la meilleure route. Chacun d'eux interprète à sa façon ce qui est le mieux. L'algorithme génère un nombre, appelé valeur métrique, pour chaque chemin traversant le réseau. Les algorithmes de routage perfectionnés effectuent la sélection du chemin en fonction de plusieurs métriques combinées en une valeur composite.

Les métriques les plus communément utilisées par les protocoles de routage :

- **Bande passante:** la bande passante représente la capacité de débit d'une liaison. Une liaison Ethernet de 10 Mbits/s est généralement préférable à une ligne louée de 64 Kbits/s.
- **Délai:** le délai est le temps nécessaire à l'acheminement d'un paquet, pour chaque liaison, de la source à la destination. Il dépend de la bande passante des liaisons intermédiaires, de la quantité de données pouvant être temporairement stockées sur chaque routeur, de la congestion du réseau et de la distance physique.
- **Charge:** la charge est la quantité de trafic sur une ressource réseau telle qu'un routeur ou une liaison.
- **Fiabilité:** la fiabilité se rapporte habituellement au taux d'erreurs de chaque liaison du réseau.
- **Nombre de sauts:** le nombre de sauts est le nombre de routeurs par lesquels un paquet doit passer avant d'arriver à destination. Chaque routeur équivaut à un saut. Un nombre de sauts égal à 4 signifie que les données doivent passer par quatre routeurs pour atteindre leur destination. Lorsque plusieurs chemins sont possibles, c'est le chemin comportant le moins de sauts qui est privilégié.
- **Tops:** délai d'une liaison de données utilisant les tops d'horloge d'un PC IBM, un top d'horloge correspondant environ à 1/18 seconde.
- **Coût:** le coût est une valeur arbitraire, généralement basée sur la bande passante, une dépense monétaire ou une autre mesure, attribuée par un administrateur réseau.

Il existe deux familles de protocoles de routage : les protocoles IGP (*Interior Gateway Protocol*) et les protocoles EGP (*Exterior Gateway Protocol*).

Les protocoles IGP acheminent les données au sein d'un système autonome. Les protocoles EGP acheminent les données entre les systèmes autonomes.

Les protocoles de routage peuvent être classés en protocoles IGP ou EGP. Le type utilisé va dépendre de l'administration du groupe de routeurs, notamment s'ils sont placés sous une seule et même administration ou pas. Les protocoles IGP peuvent être subdivisés en protocoles à vecteur de distance et en protocoles à état de liens.

Protocoles à vecteur de distance:

- **Routing Information Protocol (RIP):** le protocole RIP est le protocole IGP le plus utilisé sur Internet. Son unique métrique de routage est basée sur le nombre de sauts.
- **Interior Gateway Routing Protocol (IGRP):** ce protocole IGP a été développé par Cisco afin de résoudre les problèmes associés au routage dans des réseaux hétérogènes étendus.

- **Enhanced IGRP (EIGRP):** ce protocole IGP, propriété de Cisco, inclut un grand nombre des caractéristiques d'un protocole de routage à état de liens. Il est, de ce fait, également appelé «protocole hybride symétrique».

Les protocoles à état de liens ont été conçus pour pallier les limitations des protocoles de routage à vecteur de distance. Ils ont pour avantage de répondre rapidement aux moindres changements sur le réseau en envoyant des mises à jour déclenchées uniquement après qu'une modification soit survenue. Ces protocoles envoient par ailleurs des mises à jour périodiques, connues sous le nom d'actualisations à état de liens, à des intervalles moins fréquents, par exemple toutes les 30 minutes.

Différents protocoles de routages :

Le protocole RIP est un protocole de routage à vecteur de distance qui utilise le nombre de sauts comme métrique pour déterminer la direction et la distance vers n'importe quelle liaison de l'interréseau. Le protocole RIP sélectionne le chemin qui comporte le moins de sauts. Toutefois, le nombre de sauts étant la seule métrique de routage utilisée par ce protocole, il ne sélectionne pas toujours le chemin le plus rapide. En outre, le protocole RIP ne peut acheminer un paquet au-delà de 15 sauts. La version 1 du protocole RIP (RIPv1) n'incluant pas les informations de masque de sous-réseau dans les mises à jour de routage, tous les équipements du réseau doivent nécessairement utiliser le même masque de sous-réseau. On parle dans ce cas de routage par classes.

La version 2 (RIPv2) fournit un routage par préfixe et envoie les informations de masque de sous-réseau dans ses mises à jour de routage. On parle ici de routage sans classe. Avec les protocoles de routage sans classe, les sous-réseaux d'un même réseau peuvent comporter des masques différents. Cette technique fait référence à l'utilisation de masques de sous-réseau de longueur variable (VLSM).

Le protocole IGRP est un protocole de routage à vecteur de distance mis au point par Cisco. Il a été spécifiquement développé pour résoudre les problèmes associés au routage dans de grands réseaux qui dépassaient la portée des protocoles tels que RIP. IGRP peut sélectionner le chemin disponible le plus rapide en fonction du délai, de la bande passante, de la charge et de la fiabilité. Le nombre de sauts maximal autorisé est par ailleurs considérablement plus élevé que celui défini dans le protocole RIP. Le protocole IGRP utilise uniquement le routage par classes.

Le protocole OSPF est un protocole de routage à état de liens mis au point par l'IETF (*Internet Engineering Task Force*) en 1988. Il a été écrit pour permettre la gestion de vastes interréseaux évolutifs hors de portée du protocole RIP.

Le protocole IS-IS (*Intermediate System-to-Intermediate System*) est un protocole de routage à état de liens utilisé pour les protocoles routés autres qu'IP. Il existe une extension du protocole IS-IS, Integrated IS-IS, qui, elle, prend en charge plusieurs protocoles routés dont IP.

Le protocole BGP (*Border Gateway Protocol*) est un exemple de protocole EGP (*External Gateway Protocol*). Il permet l'échange d'informations de routage entre systèmes autonomes tout en garantissant une sélection de chemins exempts de boucle. Le protocole BGP est le protocole de mises à jour de routage le plus utilisé par les grandes sociétés et les FAI sur Internet. BGP4 est la première version de BGP à prendre en charge le routage interdomaine sans classes (CIDR) et le regroupement de routes. À la différence des protocoles IGP

courants, comme RIP, OSPF et EIGRP, le protocole BGP ne se sert pas de métriques tels que le nombre de sauts, la bande passante ou le délai. Il prend à la place ses décisions de routage selon des stratégies de réseau (ou règles utilisant divers attributs de chemin BGP).

Attention IMPORTANT --->

Format /#	/25	/26	/27	/28	/29	/30	N/A	N/A
Masque	128	192	224	240	248	252	254	255
Bits empruntés	1	2	3	4	5	6	7	8
Valeur	128	64	32	16	8	4	2	1
Nombre total de sous-réseaux		4	8	16	32	64		
Sous-réseaux utilisables		2	6	14	30	62		
Nombre total d'hôtes		64	32	16	8	4		
Hôtes utilisables		62	30	14	6	2		

Numéro du sous-réseau	ID du sous-réseau	Plage d'hôtes	ID de broadcast
0	192.168.10.0	.1--.30	192.168.10.31
1	192.168.10.32	.33--.62	192.168.10.63
2	192.168.10.64	.65--.94	192.168.10.95
3	192.168.10.96	.97--.126	192.168.10.127
4	192.168.10.128	.129--.158	192.168.10.159
5	192.168.10.160	.161--.190	192.168.10.191
6	192.168.10.192	.193--.222	192.168.10.223
7	192.168.10.224	.225--.254	192.168.10.255

The *private internet* addresses are:

Name	IP address range	number of IPs	*classful* description	largest CIDR block
24-bit block	10.0.0.0 – 10.255.255.255	16,777,215	single class A	10.0.0.0/8
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	16 contiguous class Bs	172.16.0.0/12
16-bit block	192.168.0.0 – 192.168.255.255	65,535	256 contiguous class Cs	192.168.0.0/16

10.3.5
Découpage de réseaux de classe A et B en sous-réseaux

Intéressant

Nombre total de sous-réseaux =2$^{\text{nombre de bits empruntés}}$

Nombre total d'hôtes=2$^{\text{nombre de bits restants}}$

Sous-réseaux utilisables =2$^{\text{nombre de bits empruntés}}$ **moins 2**

Hôtes utilisables =2$^{\text{nombre de bits restants}}$**moins 2**

-- Résumé module 10 :

Le protocole IP est dit protocole non orienté connexion parce qu'aucune connexion à un circuit dédié n'est établie entre la source et la destination avant la transmission. Il est considéré comme non fiable car il ne vérifie pas la bonne livraison des données. S'il est nécessaire de vérifier la bonne livraison des données, il faut combiner le protocole IP à un protocole de transport orienté connexion, tel que TCP. S'il n'est pas nécessaire de vérifier l'intégrité des données à la livraison, IP peut être utilisé avec un protocole sans connexion, tel que UDP. Les processus réseau sans connexion sont souvent appelés processus à commutation de paquets, tandis que les processus réseau orientés connexion sont dits processus à commutation de circuits.

Des informations sont ajoutées au début et à la fin des données : encapsulation des données. La couche 3 ajoute des informations d'adresse réseau ou logique aux données et la couche 2 des informations d'adresse locale ou physique.

Le routage de la couche 3 et la commutation de la couche 2 permettent d'acheminer et de livrer les données sur le réseau. Au départ, le routeur reçoit une trame de couche 2 avec un paquet de couche 3 encapsulé en son sein. Il doit retirer la trame de couche 2 et examiner le paquet de couche 3. Si ce dernier est destiné à une adresse locale, le routeur doit l'encapsuler dans une nouvelle trame dotée de la bonne adresse MAC locale de destination. Si les données doivent être transmises vers un autre domaine de broadcast, le routeur encapsule le paquet de couche 3 dans une nouvelle trame de couche 2 contenant l'adresse MAC de l'unité d'interconnexion de réseaux suivante. La trame est ainsi transférée sur le réseau de domaine de broadcast en domaine de broadcast jusqu'à sa livraison finale à l'hôte approprié.

Les protocoles routés, comme IP, transportent les données sur un réseau. Les protocoles de routage, quant à eux, permettent aux routeurs de choisir le meilleur chemin pour acheminer les données de la source à leur destination. Ce chemin peut être une route statique, entrée manuellement, ou une route dynamique, connue par le biais des protocoles de routage. Dans le cas du routage dynamique, les routeurs s'échangent des mises à jour de routage afin de gérer leur table. Les algorithmes de routage mettent en œuvre des métriques pour traiter les mises à jour de routage et informer les tables de routage des meilleurs chemins possibles. La convergence décrit la vitesse à laquelle tous les routeurs acquièrent une même vue du réseau après qu'il ait subi une modification.

Les protocoles IGP (*Interior Gateway Protocol*) sont des protocoles de routage qui acheminent les données au sein de systèmes autonomes, tandis que les protocoles EGP (*Exterior Gateway Protocol*) acheminent les données entre les différents systèmes autonomes.

Les protocoles IGP peuvent être subdivisés en protocoles à vecteur de distance et en protocoles à état de liens. Les routeurs faisant appel aux protocoles à vecteur de distance envoient périodiquement des mises à jour de routage constituées de l'intégralité ou d'une partie de leur table de routage. Les routeurs utilisant les protocoles à état de liens, pour leur part, se servent des mises à jour de routage à état de liens (LSA) pour envoyer des mises à jour uniquement lorsque des modifications surviennent dans la topologie du réseau. Ils peuvent en outre, mais moins fréquemment, envoyer les tables de routage complètes.

Lors de la transmission des paquets sur le réseau, il est nécessaire que les unités puissent distinguer la partie réseau de la partie hôte de l'adresse IP. Un masque d'adresse de 32 bits, appelé masque de sous-réseau, permet d'indiquer les bits d'une adresse IP utilisés pour l'adresse réseau. Le masque de sous-réseau par défaut pour une adresse de classe A est 255.0.0.0. Pour une adresse de classe B, le masque de sous-réseau commence toujours par 255.255.0.0 et celui d'une adresse de classe C par 255.255.255.0. Le masque de sous-réseau peut être utilisé pour diviser un réseau existant en plusieurs « sous-réseaux ».

Le découpage d'un réseau en sous-réseaux permet de réduire la taille des domaines de broadcast, permet aux segments LAN situés dans plusieurs zones géographiques différentes de communiquer par le biais de routeurs et améliore la sécurité en isolant les segments LAN les uns des autres.

Les masques de sous-réseau personnalisés utilisent plus de bits que les masques par défaut en les empruntant à la partie hôte de l'adresse IP. Une adresse en trois parties est ainsi créée:

- L'adresse réseau d'origine;
- L'adresse de sous-réseau composée des bits empruntés;
- L'adresse hôte composée des bits restants après l'emprunt des bits servant à créer les sous-réseaux.

Les routeurs utilisent les masques de sous-réseau pour déterminer la partie sous-réseau d'une adresse d'un paquet entrant. On parle alors d'opération AND logique.

11) Couche transport TCP / IP

Les deux principaux rôles de la couche transport sont donc le contrôle de flux et la fiabilité. Elle définit une connectivité de bout en bout entre les applications hôtes. Voici quelques services de transport de base:

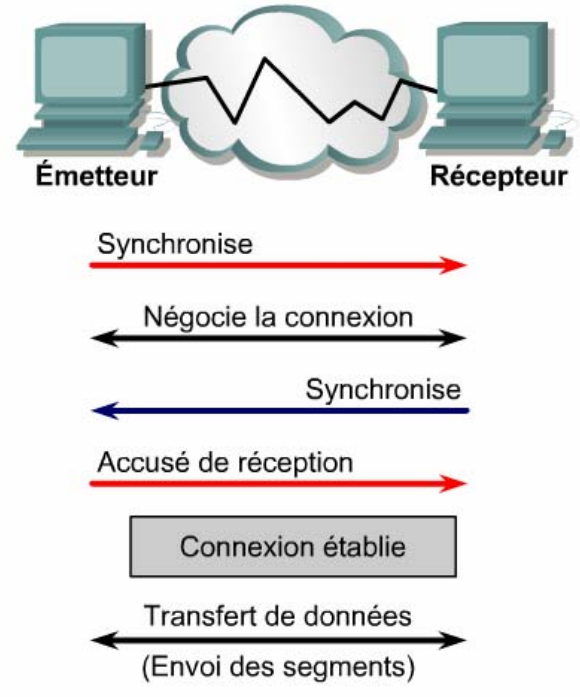
- Segmentation des données d'application de couche supérieure.
- Établissement d'une connexion de bout en bout.
- Transport des segments d'un hôte d'extrémité à un autre.
- Contrôle du flux assuré par les fenêtres glissantes.
- Fiabilité assurée par les numéros de séquence et les accusés de réception.

TCP/IP est une combinaison de deux protocoles distincts : IP et TCP. IP opère au niveau de la couche 3 du modèle OSI et est un protocole non orienté connexion offrant un acheminement au mieux (best-effort delivery) sur le réseau. TCP opère au niveau de la couche transport. C'est un service orienté connexion qui assure le contrôle du flux et la fiabilité. Combinés, ces deux protocoles offrent une gamme de services plus vaste. Ils constituent la base de la pile de protocoles TCP/IP, et c'est sur cette pile de protocoles que repose Internet.

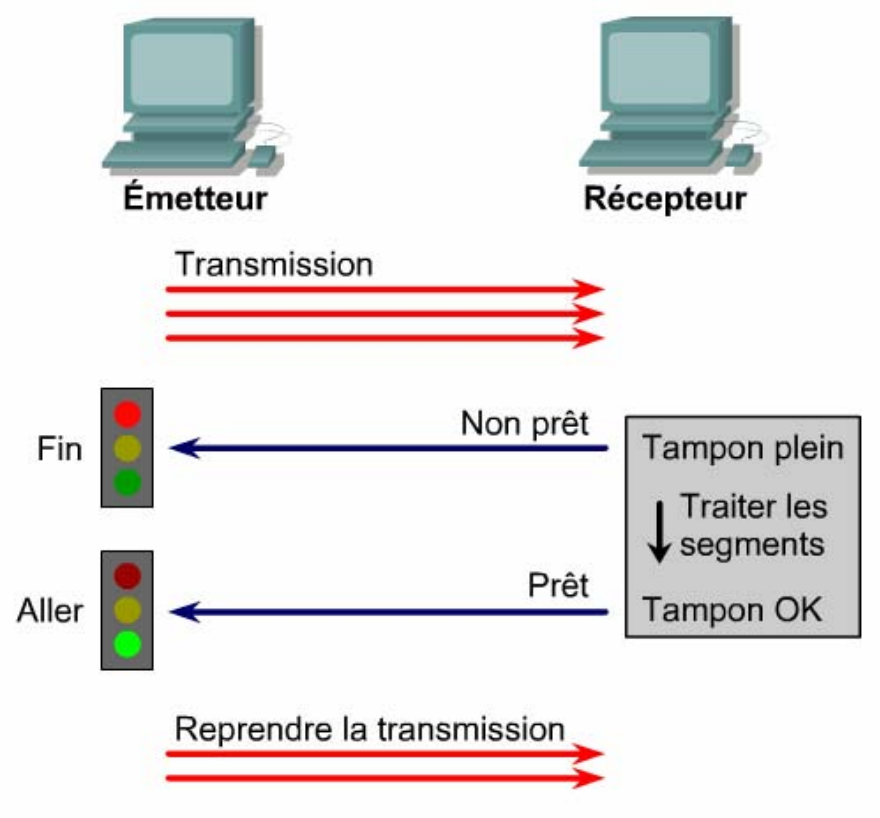
Les applications envoient des segments de données suivant la méthode du premier arrivé, premier servi. Plusieurs conversations simultanées de couche supérieure peuvent être multiplexées sur une seule connexion.

Un des rôles de la couche transport est d'établir une session orientée connexion entre des unités identiques de la couche application. Les modules logiciels de protocole des deux systèmes d'exploitation communiquent en envoyant des messages sur le réseau pour vérifier si le transfert est autorisé et si les deux ordinateurs sont prêts.

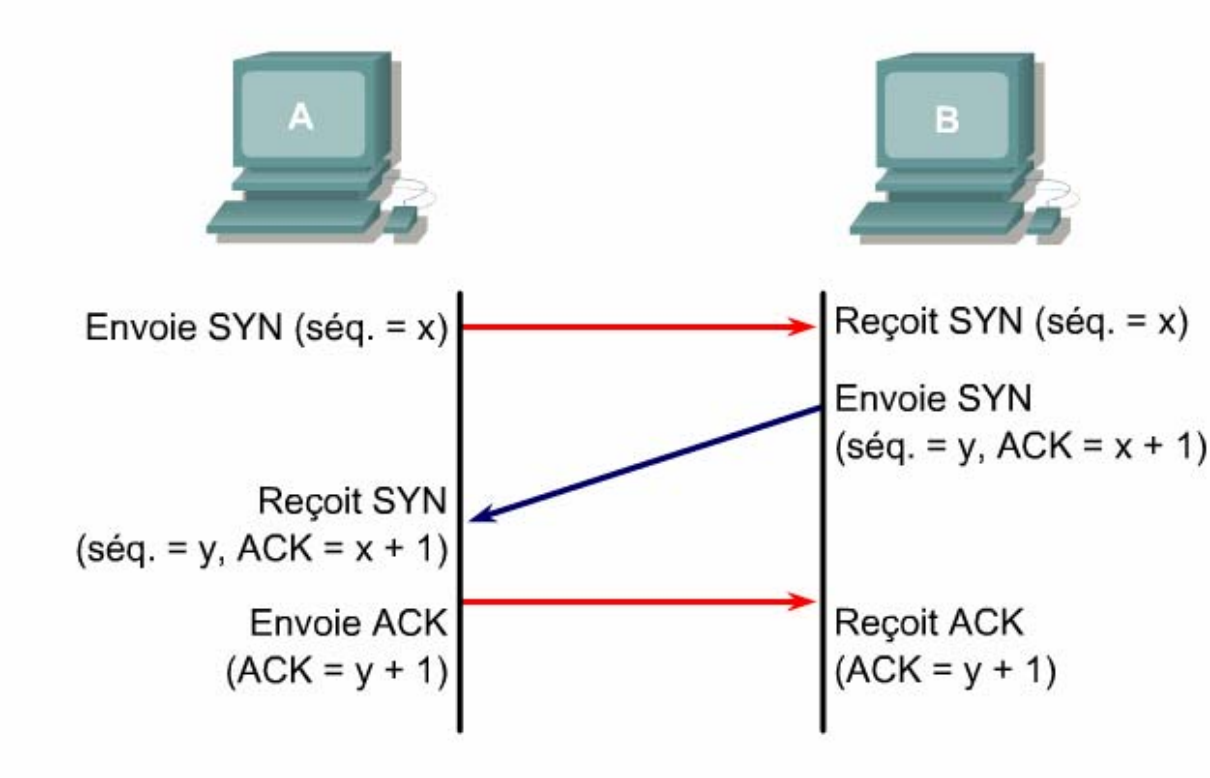
La connexion est établie et le transfert des données peut commencer après synchronisation. Pendant le transfert, les deux ordinateurs continuent de communiquer au moyen de leur logiciel de protocole pour vérifier si les données sont bien reçues.



Pour éviter la perte des données, le processus TCP de l'hôte récepteur envoie un indicateur «non prêt» à l'émetteur, afin que ce dernier arrête de transmettre lorsque des datagrammes arrivent trop rapidement et la mémoire stockant les datagrammes est saturée. Lorsque le récepteur peut accepter de nouvelles données, il envoie l'indicateur de transport «prêt» à l'émetteur qui reprend alors la transmission des segments.



La synchronisation nécessite que chaque hôte envoie son propre numéro de séquence initial (ISN) et reçoive une confirmation de cet échange par un accusé de réception (ACK) envoyé par l'autre hôte. Chaque hôte doit donc recevoir le ISN envoyé par l'autre hôte et répondre en envoyant un message ACK



Taille de fenêtre ou fenêtre : Nombre de paquets de données pouvant être transmis avant réception d'un accusé de réception (ACK).

Si la taille de fenêtre est de trois, l'hôte source peut envoyer trois octets à l'unité de destination avant d'attendre l'accusé de réception. Lorsque l'hôte de destination reçoit les trois octets, il envoie un accusé de réception à la source qui peut alors envoyer trois autres octets. Si l'unité de destination ne reçoit pas ces trois octets, parce que ses mémoires tampons sont saturées, elle n'envoie pas d'accusé de réception. L'hôte source sait alors qu'il doit retransmettre les octets à un débit de transmission inférieur.

TCP :

TCP est un protocole orienté connexion de la couche transport, qui assure une transmission fiable des données en full duplex. TCP fait partie de la pile de protocoles TCP/IP. Dans un environnement orienté connexion, une connexion est établie entre les deux extrémités avant que le transfert des informations ne commence. TCP découpe les messages en segments, les rassemble à l'arrivée et renvoie toute donnée non reçue. Il assure un circuit virtuel entre les applications utilisateur.

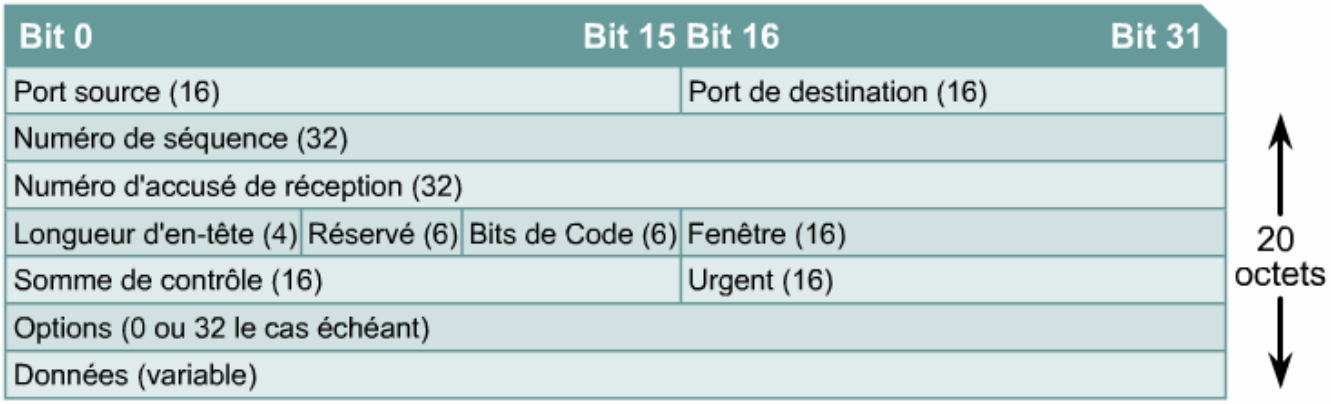
Les protocoles utilisant TCP sont les suivants:

- FTP
- HTTP
- SMTP
- Telnet

Voici la description des champs contenus dans le segment TCP:

- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.

- **Numéro de séquence:** numéro utilisé pour garantir une livraison des données dans l'ordre approprié.
- **Numéro d'accusé de réception:** octet TCP suivant attendu.
- **HLEN:** nombre de mots de 32 bits contenus dans l'en-tête.
- **Réservé:** champ réglé sur zéro.
- **Bits de code:** fonctions de contrôle, telles que l'ouverture et la fermeture d'une session.
- **Fenêtre:** nombre d'octets que l'émetteur acceptera.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Pointeur d'urgence:** indique la fin des données urgentes.
- **Option:** une des options actuellement disponibles est la taille maximale d'un segment TCP (MSS – Maximum Segment Size).
- **Données:** données de protocole de couche supérieure.



UDP :

C'est un protocole simple qui échange des datagrammes sans garantir leur bonne livraison. Il repose entièrement sur les protocoles de couche supérieure pour le contrôle des erreurs et la retransmission des données.

UDP n'utilise ni fenêtres ni accusés de réception. La fiabilité est assurée par les protocoles de la couche application. Le protocole UDP est conçu pour les applications qui ne doivent pas assembler de séquences de segments.

Les protocoles utilisant UDP sont les suivants:

- TFTP
- SNMP
- DHCP
- DNS

Voici la description des champs contenus dans le segment UDP:

- **Port source:** numéro du port qui envoie les données.
- **Port de destination:** numéro du port qui reçoit les données.
- **Longueur:** nombre d'octets de l'en-tête et des données.
- **Somme de contrôle:** somme de contrôle des champs de données et d'en-tête.
- **Données:** données de protocole de couche supérieure.

Bit 0	Bit 15 Bit 16	Bit 31
Port source (16)	Port de destination (16)	
Longueur (16)	Somme de contrôle (16)	
Données (le cas échéant)		

8 octets

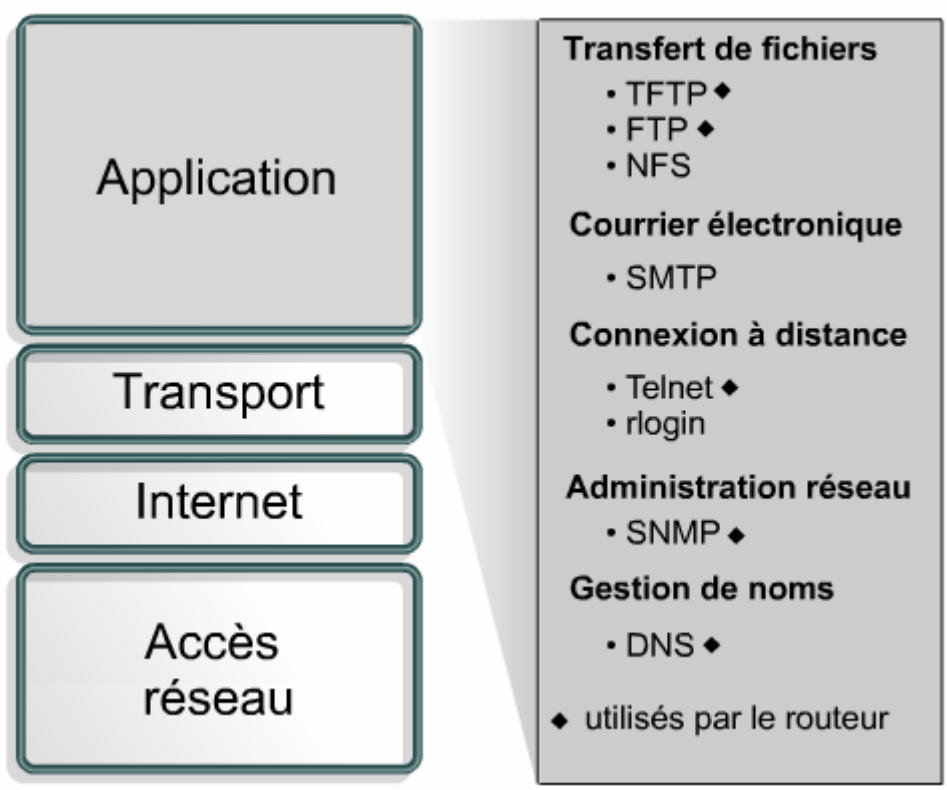
Numéros de Ports : FTP fait appel aux numéros de port standard 20 et 21. Le port 20 est utilisé pour la partie donnée et le port 21 pour le contrôle.

Decimal	Keyword	Description
0		Réservé
1-4		Non attribué
5	RJE	Protocole RJE (Soumission de travaux à distance)
7	ECHO	Écho
9	DISCARD	Élimination
11	USERS	Utilisateurs actifs
13	DAYTIME	Heure du jour
15	NETSTAT	Qui est actif ou NETSTAT
17	QUOTE	Citation du jour
19	CHARGEN	Générateur de caractères
20	FTP-DATA	Protocole FTP (données)
21	FTP	Protocole FTP
23	TELNET	Connexion en mode terminal
25	SMTP	Protocole SMTP (Simple Mail Transfer Protocol)
37	TIME	Heure du jour
39	RLP	Protocole RLP (Resource Location Protocol)
42	NAMESERVER	Serveur de noms d'hôte

43	NICNAME	Protocole Who Is
53	DOMAIN	Serveur de noms de domaine
67	BOOTPS	Serveur de protocole Bootstrap
68	BOOTPC	Client de protocole Bootstrap
69	TFTP	Protocole TFTP (Trivial File Transfer Protocol)
75		Tout service de sortie privé
77		Tout service RJE privé
79	FINGER	Finger
80	HTTP	Protocole HTTP (HyperText Transfer Protocol)
95	SUPDUP	Protocole SUPDUP
101	HOSTNAME	Serveur de noms d'hôte NIC
102	ISO-TSAP	ISO-TSAP
113	AUTH	Service d'authentification
117	UUCP-PATH	Service de chemin UUCP
123	NTP	Protocole NTP (Network Time Protocol)
137	NetBIOS	Service de noms
139	NetBIOS	Service de datagramme

143	IMAP	Protocole IMAP (Interim Mail Access Protocol)
150	NetBIOS	Service de session
156	SQL	Serveur SQL
161	SNMP	Protocole SNMP (Simple Network Management Protocol)
179	BGP	Protocole BGP (Border Gateway Protocol)
190	GACP	Protocole GACP (Gateway Access Control Protocol)
194	IRC	IRC (Internet Relay Chat)
197	DLS	Directory Location Service
224-241		Non attribué
242-255		Non attribué

Couche application du TCP / IP :



Afin de pouvoir créer un lien entre le contenu d'un site et son adresse (IP), un système de noms de domaine a été établi. Le système de noms de domaine (DNS) est utilisé sur Internet pour convertir en adresses IP les noms de domaine et leurs nœuds de réseau annoncés publiquement. Un domaine est un groupe d'ordinateurs associés en fonction de leur proximité géographique ou du type d'informations qu'ils contiennent. Il existe plus de 200 domaines de niveau supérieur sur Internet, notamment:

.us – États-Unis
.fr – France

Noms génériques, notamment: **.edu** – sites éducatifs / **.com** – sites commerciaux / **.gov** – sites gouvernementaux / **.org** – sites d'organisations à but non lucratif / **.net** – service de réseau

Protocole http :

Le protocole HTTP (*Hypertext Transfer Protocol*) est le support du Web. Un navigateur Web est une application de type client-serveur. Les pages Web sont créées avec un langage de formatage appelé HTML (*HyperText Markup Language*). Le code HTML indique au navigateur comment présenter une page Web pour obtenir un aspect particulier.

Dans l'URL http://www.cisco.com/edu/, la partie «http://» indique au navigateur le protocole à utiliser. La seconde partie, «www», indique le nom de l'hôte ou le nom d'un ordinateur précis doté d'une adresse IP spécifique. Enfin, le suffixe « /edu/ » précise l'emplacement exact du dossier sur le serveur qui contient la page Web.

SMTP :

Les serveurs de messagerie communiquent entre eux à l'aide du protocole SMTP (*Simple Mail Transfer Protocol*) pour envoyer et recevoir des messages électroniques. Ce protocole transporte les messages au format ASCII à l'aide de TCP. Serveur de messagerie les plus répandus sont POP3 et IMAP4,

Lorsque vous vérifiez la configuration d'un client de messagerie, assurez-vous que les paramètres SMTP et POP, ou IMAP, sont correctement configurés. Pour tester l'accès à un serveur de messagerie, établissez une connexion Telnet au port SMTP (25) ou au port POP3 (110). Le format de commande suivant est utilisé sur la ligne de commande Windows pour tester l'accès au service SMTP du serveur de messagerie à l'adresse IP 192.168.10.5:
C:\>telnet 192.168.10.5 25

SNMP :

- **Le système d'administration de réseaux *(NMS, Network Management System)*:** le composant NMS exécute les applications qui contrôlent et surveillent les unités gérées. Il fournit la quantité de ressources mémoire et de traitement requises pour la gestion du réseau. Tout réseau géré doit comprendre au moins un composant NMS.
- **Les unités gérées:** ces unités sont des nœuds du réseau contenant un agent SNMP et résidant sur un réseau géré. Elles collectent et stockent des informations de gestion qu'elles mettent à la disposition des composants NMS via SNMP. Ces unités gérées, parfois appelées éléments du réseau, peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des concentrateurs, des ordinateurs hôtes ou des imprimantes.
- **Les agents:** les agents sont des modules logiciels de gestion du réseau résidant sur les unités gérées. Ils contiennent les données locales des informations de gestion et les convertissent en un format compatible avec SNMP.

Telnet :

Le logiciel client Telnet permet de se connecter à un hôte Internet distant sur lequel est exécutée une application serveur Telnet, puis d'exécuter des commandes à partir de la ligne de commande. Un client Telnet est qualifié d'hôte local. Le serveur Telnet, qui utilise un logiciel spécial appelé «démon», est considéré comme l'hôte distant.

Telnet fonctionne au niveau de la couche application du modèle TCP/IP. Il opère donc au niveau des trois couches supérieures du modèle OSI. La couche application traite les commandes. La couche présentation gère le formatage, généralement ASCII. La couche session effectue la transmission. Dans le modèle TCP/IP, toutes ces fonctions sont regroupées dans la couche application.

Résumé :

- **Système DNS *(Domain Name System)*:** système utilisé dans les réseaux IP pour traduire le nom des nœuds du réseau en adresses IP.
- **Protocole FTP *(File Transfer Protocol)*:** protocole utilisé pour le transfert des fichiers entre les réseaux.
- **Protocole HTTP *(Hypertext Transfer Protocol)*:** protocole utilisé pour fournir des documents en langage HTML (*HyperText Markup Language*) à une application cliente, telle qu'un navigateur Web.
- **Protocole SMTP *(Simple Mail Transfer Protocol)*:** protocole permettant l'utilisation de services de messagerie électronique.
- **Protocole SNMP *(Simple Network Management Protocol)*:** protocole utilisé pour surveiller et contrôler les équipements du réseau, ainsi que pour gérer les configurations, la collecte de statistiques, les performances et la sécurité.
- **Telnet:** utilisé pour se connecter à un hôte distant sur lequel est exécutée une application serveur Telnet, puis pour exécuter des commandes depuis la ligne de commande.