

Ethernet

| Structure des adresses MAC (Media Access Control) | | | | | | |
|---|--|--|---------------|--------------------|---------------------|---|
| ID unique du constructeur 24 bits | | | | | | ID unique du périphérique 24 bits |
| Mono / Multi diffusion 1 bit | Local / Global 1 bit | N° identification d'organisation 22 bits | | | | |
| Structure de la trame Ethernet 802.3 | | | | | | |
| 7 octets | 1 octet | 6 octets | 6 octets | 2 octets | 46 à 1500 octets | 4 octets |
| Préambule | Délimiteur début de trame (SFD) | MAC Destination | MAC Source | Longueur / Type | Données | Séquence de contrôle de trame (FCS) |

Champ FCS (Frame Check Sequence) : ce champ représente la séquence de contrôle de trame, utilisée dans le cadre du service de contrôle d'erreurs fourni par la couche liaison de données du modèle OSI, afin de valider la conformité de la trame Ethernet reçue par le destinataire. L'émetteur calcule le CRC (Contrôle de Redondance Cyclique) de la trame avant sa transmission sur le réseau. A réception de celle-ci, en vue de détecter d'éventuelles erreurs engendrées durant la transmission, le destinataire effectue le même calcul puis compare les deux résultats qui doivent être identiques. Le cas échéant, la retransmission de la trame sera demandée par le destinataire. Ces erreurs sont généralement dues à des interférences électromagnétiques ou à l'affaiblissement du signal sur les câbles Ethernet à paires torsadées.

Domaine de diffusion : zone du réseau dans laquelle une trame de diffusion envoyée par une interface réseau est reçue par toutes les autres interfaces du domaine. Le routeur et le commutateur de niveau 3 créent respectivement un domaine de diffusion par interface et un domaine de diffusion par VLAN.

Domaine de collision : zone du réseau dans laquelle une trame envoyée par une interface réseau pourrait entrer en collision avec une trame envoyée par une autre interface du domaine. Tous les ports d'un concentrateur (hub) constitue un seul et unique domaine de collision, tandis que le commutateur crée un domaine de collision par port.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection) :

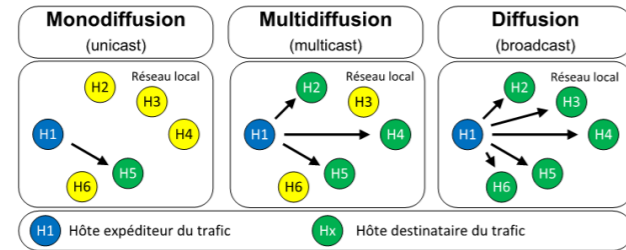
Le périphérique détermine si le support comporte un signal de porteuse. Si aucun signal n'est détecté, cela signifie que le support est libre et que le périphérique peut transmettre ses données. Si un signal est détecté, indiquant qu'un autre périphérique était au même moment en train de transmettre, tous les périphériques stoppent leur transmission et réémettent ultérieurement dans un délai aléatoire. Ethernet filaire (IEEE 802.3) utilise cette méthode.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) :

Le périphérique détermine si le support comporte un signal de porteuse. Si aucun signal n'est détecté, le périphérique envoie une notification sur le support pour indiquer son intention d'émettre. Dès qu'il reçoit une autorisation de transmission, le périphérique émet des données. Ethernet sans fil (IEEE 802.11) utilise cette méthode.

Adressage IPv4

3 méthodes de transmission sont disponibles en IPv4 :



- Monodiffusion :** transmission de données entre deux hôtes identifiés chacun par une adresse IP unique. La communication est établie d'un seul expéditeur vers un seul destinataire.
Exemple : téléchargement de fichiers via le protocole FTP.
- Multidiffusion :** transmission de données d'un expéditeur vers un groupe de destinataires préalablement et dynamiquement inscrits vers un groupe de multidiffusion. La communication est établie d'un seul expéditeur à un groupe de destinataires.
Exemple : échange de paquets OSPF entre routeurs OSPF.
- Diffusion :** transmission de données d'un expéditeur unique vers l'ensemble des destinataires du réseau local. La communication est établie d'un seul expéditeur vers tous les destinataires joignables.
Exemple : résolution d'une adresse IPv4 en adresse MAC via le protocole ARP (Address Resolution Protocol).

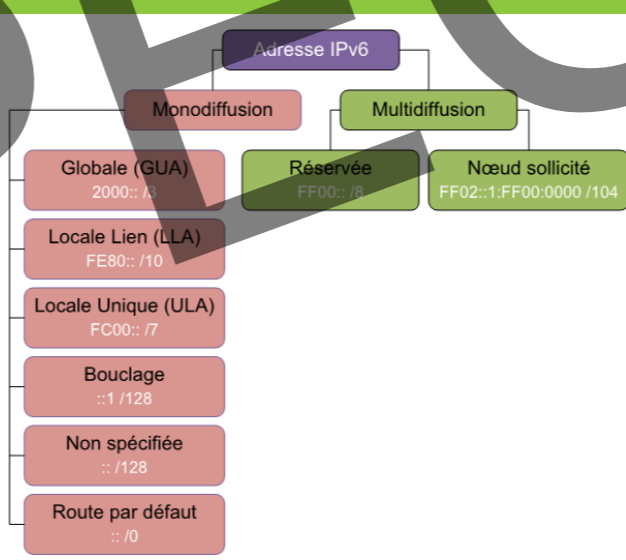
| Classe d'adresses IPv4 | | | | | | |
|-------------------------------|--------|--|--|---------------------------|-----------------------|---------------------------------|
| Type | Classe | Plage du 1 ^{er} octet (décimal) | Plage du 1 ^{er} octet (binaire) | ID réseau (R) ID hôte (H) | Masque de sous-réseau | Nombre d'adresses hôtes valides |
| Monodiffusion (unicast) | A | 0 -> 127 | de 00000000 à 01111111 | R.H.H.H | 255.0.0.0 ou /8 | 2 ²⁴ -2=16777214 |
| | B | 128 -> 191 | de 10000000 à 10111111 | R.R.H.H | 255.255.0.0 ou /16 | 2 ¹⁶ -2=65534 |
| | C | 192 -> 223 | de 11000000 à 11011111 | R.R.R.H | 255.255.255.0 ou /24 | 2 ⁸ -2=254 |
| Multidiffusion (multicast) | D | 224 -> 239 | de 11100000 à 11101111 | | | |
| Expérimentale (réservée IANA) | E | 240 -> 255 | de 11110000 à 11111111 | | | |

| Espace d'adressage IP privé (RFC 1918) | | | |
|--|-------------|--------|-------------------------------|
| Classe | Préfixe | Masque | Plage d'adresses valides |
| A | 10.0.0.0 | /8 | 10.0.0.1 à 10.255.255.254 |
| B | 172.16.0.0 | /12 | 172.16.0.1 à 172.31.255.254 |
| C | 192.168.0.0 | /16 | 192.168.0.1 à 192.168.255.254 |

| Espaces d'adressage réservés | | | |
|------------------------------|--------|-------------------------------|----------------------|
| Préfixe | Masque | Plage d'adresses | Description |
| 127.0.0.0 | /8 | 127.0.0.1 à 127.255.255.254 | Adresses de bouclage |
| 169.254.0.0 | /16 | 169.254.0.1 à 169.254.255.254 | Adresses APIPA |
| 192.0.2.0 | /24 | 192.0.2.0 à 192.0.2.255 | Adresses TEST-NET |

| Adresse IPv4 (4 octets ou 32 bits) Exemple : 192.168.54.147 /27 | | | | | |
|--|---------------|----------|----------|--------------------|-------------|
| | < ID Réseau > | | | < ID Sous-réseau > | < ID Hôte > |
| Adresse IP | 192 | 168 | 54 | 147 | |
| Masque de sous-réseau | 11111111 | 11111111 | 11111111 | 111 | 00000 |
| Adresse du réseau | 192 | 168 | 54 | 128 | |
| 1 ^{ère} adresse d'hôte valide | 192 | 168 | 54 | 100 | 00001 |
| Dernière adresse valide | 192 | 168 | 54 | 158 | 11110 |
| Adresse de diffusion | 192 | 168 | 54 | 159 | 11111 |

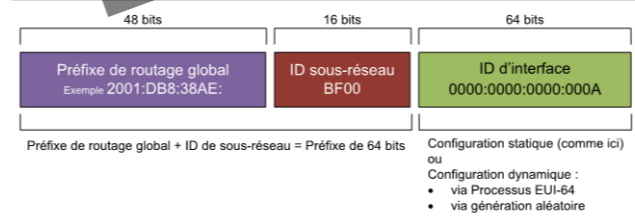
Adressage IPv6



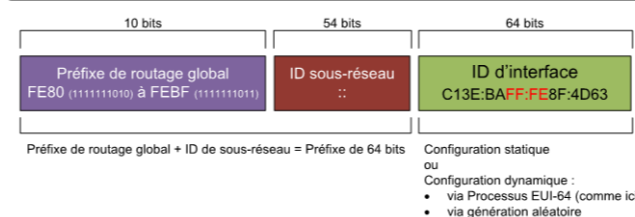
| Types d'adresses IPv6 | | |
|-----------------------------------|-----------|---|
| Adresse | Préfixe | Équivalence IPv4 |
| Monodiffusion globale (GUA) | 2000::/3 | Adresse publique |
| Monodiffusion locale lien (LLA) | FE80::/10 | Adresse APIPA (169.254.x.y/16) |
| Monodiffusion locale unique (ULA) | FC00::/7 | Adresse privée (RFC1918) |
| Multidiffusion | FF00::/8 | Adresse multidiffusion (224 à 239) |
| Réservée | ::/8 | Adresse non spécifiée (::/128) Adresse de bouclage (::1/128) |

| Adresses de multidiffusion IPv6 réservées | |
|---|---|
| Adresse de multidiffusion | Description |
| FF02::1 | Tous les nœuds du réseau local. |
| FF02::2 | Tous les routeurs du réseau local. |
| FF02::5 | Tous les routeurs OSPF du réseau local. |
| FF02::6 | Tous les routeurs DR OSPF du réseau local. |
| FF02::1:FF00:0000/104 | Nœud sollicité NDP (découverte du voisin). |
| FF02::1:2 | Tous les agents et serveurs DHCP du réseau local. |
| FF05::1:3 | Tous les serveurs DHCP du réseau local. |

Format d'adresse IPv6 de monodiffusion globale (GUA)



Format d'adresse IPv6 de monodiffusion locale lien (LLA)



Deux règles permettent la simplification de l'écriture des adresses IPv6 :

Règle n°1 : suppression des zéros en début d'hexet uniquement

!/\ Uniquement les zéros en début d'hexet

Ainsi :
2001:0AF7:002C:85D7:0080:95EC:FF2A:0050
équivaut à :
2001:AF7:2C:85D7:80:95EC:FF2A:50.

Règle n°2 : concaténation des hexets composés uniquement de zéros

!/\ Possible une seule fois par adresse

Ainsi :
2001:0AF7:0000:0000:0000:95EC:0000:0050
équivaut à :
2001:AF7::95EC:0:50.

| Caractéristiques méthodes RA (Router Advertisement) du routeur IPv6 | | |
|--|--------------------------------------|--|
| Annonces envoyées toutes les 200 sec à destination de FF02::01 (All Nodes Address) | | |
| Sans état | Méthode 1 (par défaut) : SLAAC | Informations fournies par le routeur IPv6 à l'hôte demandeur |
| | | - Préfixe de réseau - Longueur de préfixe - Passerelle par défaut |
| | Méthode 2 : SLAAC + DHCPv6 sans état | - ID d'interface (aléatoire ou via EUI-64) - Options DHCPv6 (serveur DNS, nom de domaine) |
| Avec état | Méthode 3 : DHCPv6 avec état | - Passerelle par défaut - Serveur DHCPv6 pour l'obtention de la configuration IP complète |
| | | - ID d'interface (aléatoire ou via EUI-64) - Options DHCPv6 (serveur DNS, nom de domaine) |

| Systèmes de numération | | | TCP/UDP | N° de Port | Service |
|------------------------|------------------|-------------------|------------|------------|-------------|
| Hexadécimal (base 16) | Binaire (base 2) | Décimal (base 10) | | | |
| 01 | 0000 0001 | 1 | TCP | 20 | FTP Data |
| 03 | 0000 0011 | 3 | TCP | 21 | FTP Control |
| 05 | 0000 0101 | 5 | TCP | 22 | SSH |
| 06 | 0000 0110 | 6 | TCP | 23 | Telnet |
| 07 | 0000 0111 | 7 | TCP | 25 | SMTP |
| 0A | 0000 1010 | 10 | TCP et UDP | 53 | DNS |
| 0F | 0000 1111 | 15 | UDP | 67 | DHCP Server |
| 10 | 0001 0000 | 16 | UDP | 68 | DHCP Client |
| 40 | 0100 0000 | 64 | TCP | 80 | HTTP |
| CA | 1100 1010 | 202 | TCP | 110 | POP |
| FD | 1111 0000 | 240 | UDP | 161 | SNMP |
| FF | 1111 1111 | 255 | UDP | 162 | SNMP TRAP |
| | | | TCP | 443 | HTTPS |

Sébastien ARTU

CISCO

Introduction aux réseaux
v7.0

Préparation à la certification
CCNA 200-301



ISBN : 978-2-409-02931-8

Prix : 7 €

www.editions-eni.fr



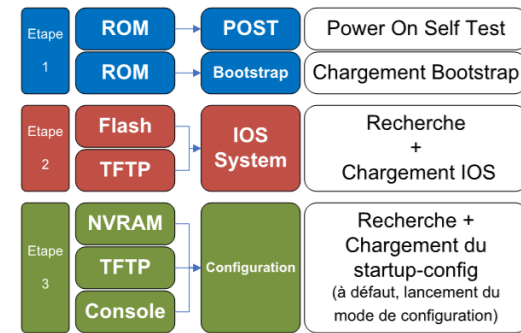
© Editions ENI - www.editions-eni.fr

© Editions ENI - www.editions-eni.fr

© Editions ENI - www.editions-eni.fr

© Editions ENI - www.editions-eni.fr

Séquence de démarrage des périphériques



Modes de configuration IOS

```
Router>
Prompt du mode utilisateur.

Router>enable
Bascule du mode utilisateur vers le mode privilégié.

Router#
Prompt du mode privilégié.

Router#disable
Bascule du mode privilégié vers le mode utilisateur.

Router#configure terminal
Bascule du mode privilégié vers le mode de configuration globale.

Router(config)#
Prompt du mode de configuration globale.

Router(config)#end (ou Ctrl Z)
Permet de revenir au mode privilégié depuis n'importe quel contexte.
```

Configuration de base des périphériques

```
(config)#hostname name
Attribue un nom d'hôte au périphérique.

(config)#no hostname
Restaure le nom d'hôte par défaut du périphérique.

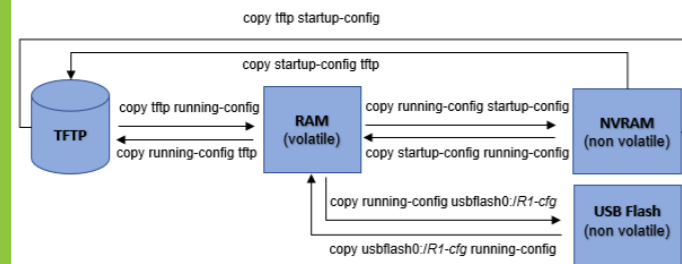
(config)#banner motd # Message #
Définit et active une bannière d'information type MOTD (Message Of The Day) visible lors d'un accès au périphérique avant la phase d'authentification.

(config)#no ip domain-lookup
Désactive la tentative de résolution de noms via le service DNS lors de la saisie erronée d'une commande.

(config-line)#logging synchronous
Synchronise l'affichage des messages Syslog avec la saisie clavier.
```

Gestion des fichiers de configuration

| Mémoire | Fichier(s) stocké(s) | Type |
|---------|---|--------------|
| Flash | Système d'exploitation IOS et autres fichiers système | Non volatile |
| NVRAM | Fichier startup-config | Non volatile |
| RAM | Fichier running-config Tables ARP et de routage IP Mémoire tampon de paquets IP | Volatile |
| ROM | Programme Bootstrap, ROMmon (version IOS limitée) | Non volatile |



```
#show version
Affiche les capacités matérielles et logicielles du système.

#show file systems
Affiche la liste des systèmes de fichiers disponibles.

#show {startup-config | running-config}
Affiche le contenu du fichier de configuration spécifié.

#erase {nvram: | startup-config}
Supprime le fichier de configuration initiale.

(config)#boot system flash:IOS-filename
Spécifie l'image IOS à charger au prochain démarrage.

(config)#boot system rom
Charge le mode ROMmon au prochain démarrage.

#reload
Redémarre le périphérique.
```

Configuration du commutateur

```
(config-if)#duplex {full | half | auto}
Définit le mode duplex du port sélectionné.

(config-if)#speed {10 | 100 | 1000 | auto}
Définit la vitesse (en Mbits/s) du port sélectionné.

(config-if)#mdix auto
Active la détection automatique du type de câble connecté sur le port sélectionné.

#show controllers ethernet-controller intf-type intf-number phy
Affiche les paramètres physiques du port spécifié.
```

| Type de commutation | Description |
|--------------------------|---|
| Store and Forward | Le commutateur reçoit les trames complètes, les stocke et vérifie le champ FCS (Frame Check Sequence) avant de les retransmettre. |
| Cut through (par défaut) | Le commutateur retransmet les trames sans contrôler le champ FCS. Cela réduit la latence, mais accroît le risque d'erreurs. |
| Fragment Free | Le commutateur retransmet les trames après avoir stocké uniquement les 64 premiers octets de celles-ci et contrôler le champ FCS. |

Adressage IPv4/v6 des périphériques

```
#show interfaces [intf-type intf-number]
Affiche l'état et la configuration des interfaces ou de l'interface spécifiée.

#show running-config interface [intf-type intf-number]
Affiche la configuration actuelle complète (IPv4/v6, description, ACL etc.) de l'interface spécifiée.

(config)#interface intf-type intf-number
Bascule vers le mode de configuration de l'interface spécifiée.

(config)#interface loopback number
Crée l'interface de bouclage spécifiée et/ou bascule dans son contexte.

(config)#ip default-gateway router-ip-address
Définit une passerelle par défaut sur le commutateur.

(config)#interface vlan vlan-id
Crée l'interface virtuelle SVI liée au VLAN de gestion spécifié.

(config-if)#ip address ip-address subnet-mask
Définit une configuration IPv4 sur l'interface sélectionnée.

(config)#ipv6 unicast-routing
Active le routage IPv6 et l'envoi de messages RA (Router Advertisement) à destination de FF02::1 (IPv6-All-nodes).

(config-if)#ipv6 address ipv6-address/prefix-length [link-local | eui-64]
Définit soit une adresse IPv6 de monodiffusion globale (GUA) complète ou utilisant le processus EUI-64, soit une adresse IPv6 de monodiffusion lien local (LLA) spécifique.

(config)#sdm prefer dual-ipv4-and-ipv6 default
#reload
Active la pile IPv6 afin de configurer une SVI en IPv6 pour l'administration distante du commutateur.

(config-if)#ipv6 enable
Génère une adresse de monodiffusion lien local (LLA) IPv6 (en l'absence de GUA configurée) et active l'envoi de messages RS (Router Solicitation) sur l'interface sélectionnée.

(config-if)#ipv6 address dhcp
Configure l'interface sélectionnée en tant que client DHCPv6 avec état.

(config-if)#ipv6 address autoconfig
Active la configuration automatique de la GUA via SLAAC sur l'interface sélectionnée.
```

```
(config-if)#no {ip | ipv6} address {address/mask}
Supprime la configuration IPv4/v6 de l'interface sélectionnée.

(config-if)#description text
Définit une description sur l'interface sélectionnée.

(config-if)#no shutdown
Active l'interface sélectionnée.

(config-if)#shutdown
Désactive l'interface sélectionnée.

#show {ip | ipv6} interface [brief | intf-type intf-number]
Affiche des statistiques IP résumées ou détaillées relatives à toutes les interfaces ou à l'interface spécifiée.

#show ipv6 neighbors
Affiche les entrées Neighbor Discovery mises en cache.

#clear ipv6 neighbors
Efface les entrées Neighbor Discovery statiques mises en cache.

#show ipv6 routers
Affiche les informations RA (Router Advertisement) reçues sur le lien local.
```

Sécurisation des périphériques

```
(config)#line {console 0 | vty 0 15}
Bascule dans le mode de configuration de ligne (port console ou terminaux virtuels VTY).

(config-line)#password password
Définit un mot de passe pour protéger l'accès au port console ou aux terminaux virtuels VTY.

(config-line)#login
Active la demande d'authentification par mot de passe pour l'accès au port console ou aux terminaux virtuels VTY.

(config-line)#no login
Désactive la demande d'authentification par mot de passe pour l'accès au port console ou aux terminaux virtuels VTY.

(config)#enable secret password
Active l'authentification et définit le mot de passe (haché en MD5) pour accéder au mode d'exécution privilégié.

(config)#service password-encryption
Active le chiffrement de tous les mots de passe stockés en clair dans les fichiers de configuration.

(config)#security passwords min-length number
Définit et impose une longueur minimale des mots de passe.

(config)#login block-for seconds attempts tries within seconds
Bloque les tentatives de connexion au périphérique pendant la période définie si le nombre spécifié d'échecs survient pendant la période définie.

(config-line)#exec-timeout minutes [seconds]
Déconnecte automatiquement tout utilisateur en ligne en cas d'inactivité pendant le délai spécifié.

(config)#no cdp run
Désactive globalement le protocole CDP sur le périphérique.
```

```
(config-if)#no cdp enable
Désactive le protocole CDP sur l'interface sélectionnée.

#auto secure [management | forwarding]
Renforce la sécurité du plan de gestion et/ou de données du routeur en activant la fonctionnalité AutoSecure.

#show ip ports all [sur IOS-XE]
ou
#show control-plane host open-ports [sur IOS]
Affiche la liste des ports TCP/IP ouverts sur le système.
```

Administration via SSH

```
(config)#ip domain-name domain-name
Définit un nom de domaine pour le protocole SSH.

(config)#crypto key generate rsa [general-keys] [modulus modulus-size]
Génère les clés de chiffrement RSA pour les connexions SSH.

(config)#crypto key zeroize rsa
Supprime les clés de chiffrement RSA, désactive SSH.

(config)#ip ssh version {1 | 2}
Définit la version utilisée du protocole SSH (v2 recommandée).

(config)#username name secret password
Créer un compte d'utilisateur et le mot de passe associé (haché en MD5) dans la base de données locale du périphérique.

(config)#line vty 0 15
Bascule en mode de configuration de lignes VTY.

(config-line)#login local
Active l'authentification locale lors de la connexion Telnet/SSH.

(config-line)#transport input ssh
Impose le protocole SSH, désactive le protocole Telnet.

#show ip ssh
Affiche la configuration du service SSH du périphérique.

#show ssh
Affiche les connexions en cours au service SSH.
```

Diagnostic et Dépannage

```
#debug ip icmp
Active une instance de débogage sur le périphérique, ici ICMP.

#no debug ip icmp (ou #undebug ip icmp)
Désactive une instance de débogage spécifique, ici ICMP.

#undebug all
Désactive toutes les instances de débogage actives.

#terminal monitor
Affiche les messages de débogage lors de connexions Telnet/SSH (par défaut, uniquement affichés sur la console).

#terminal no monitor
Désactive l'affiche des messages lors de connexions Telnet/SSH.
```

```
#show ip arp
Affiche la table ARP du périphérique.

#ping [ip | ipv6] {ip-address | hostname}
Teste la connectivité IPv4 ou v6 à l'hôte spécifié.

#ping
Exécute la commande ping en mode étendu.

#traceroute [ip | ipv6] {ip-address | hostname}
Détermine le chemin emprunté par un paquet IPv4 ou v6.

#traceroute
Exécute la commande traceroute en mode étendu.

#show cdp neighbors [details]
Collecte via CDP des informations détaillées sur les périphériques Cisco voisins.
```

Modèle OSI et Modèle TCP/IP

| Modèle TCP/IP | Modèle OSI | Protocole Data Unit | Protocole / Norme |
|---------------|--------------------|-------------------------------|--|
| Application | Application | Donnée | HTTP, DNS, DHCP, FTP, SIP, NTP, SNMP, NFS, SSH, RDP, SMTP, POP, IMAP, LDAP, CIFS |
| | Présentation | | ASCII, Unicode, HTML, XML |
| | Session | | RPC, Netbios |
| Transport | Transport | Segment TCP Datagramme UDP | TCP, UDP |
| Internet | Réseau | Paquet IP | IP, RIP, OSPF, ARP, ICMP |
| Accès réseau | Liaison de données | Trame | HDLCL, PPP, Ethernet, Bluetooth, STP, Wi-Fi, Token Ring |
| | Physique | Bit | CSMA/CD, xDSL, 1000BASE-TX |

| Caractéristiques | Concentrateur (Hub) | Commutateur (Switch) | Routeur |
|---|---------------------|----------------------|---------|
| Couche 1 du modèle OSI | Oui | Oui | Oui |
| Couche 2 du modèle OSI | Non | Oui | Oui |
| Couche 3 du modèle OSI | Non | Non ¹ | Oui |
| Accroît la distance de câblage autorisée | Oui | Oui | Oui |
| Sépare le réseau en domaines de collision | Non | Oui | Oui |
| Accroît la bande passante du réseau | Non | Oui | Oui |
| Sépare le réseau en domaines de diffusion | Non | Non ² | Oui |

¹sauf s'il s'agit d'un commutateur de couche 3.
²sauf si des VLAN sont mis en œuvre (1 VLAN = 1 domaine de diffusion)