1re partie :
Connectivité des réseaux de base et les communications

Modules 1 - 3

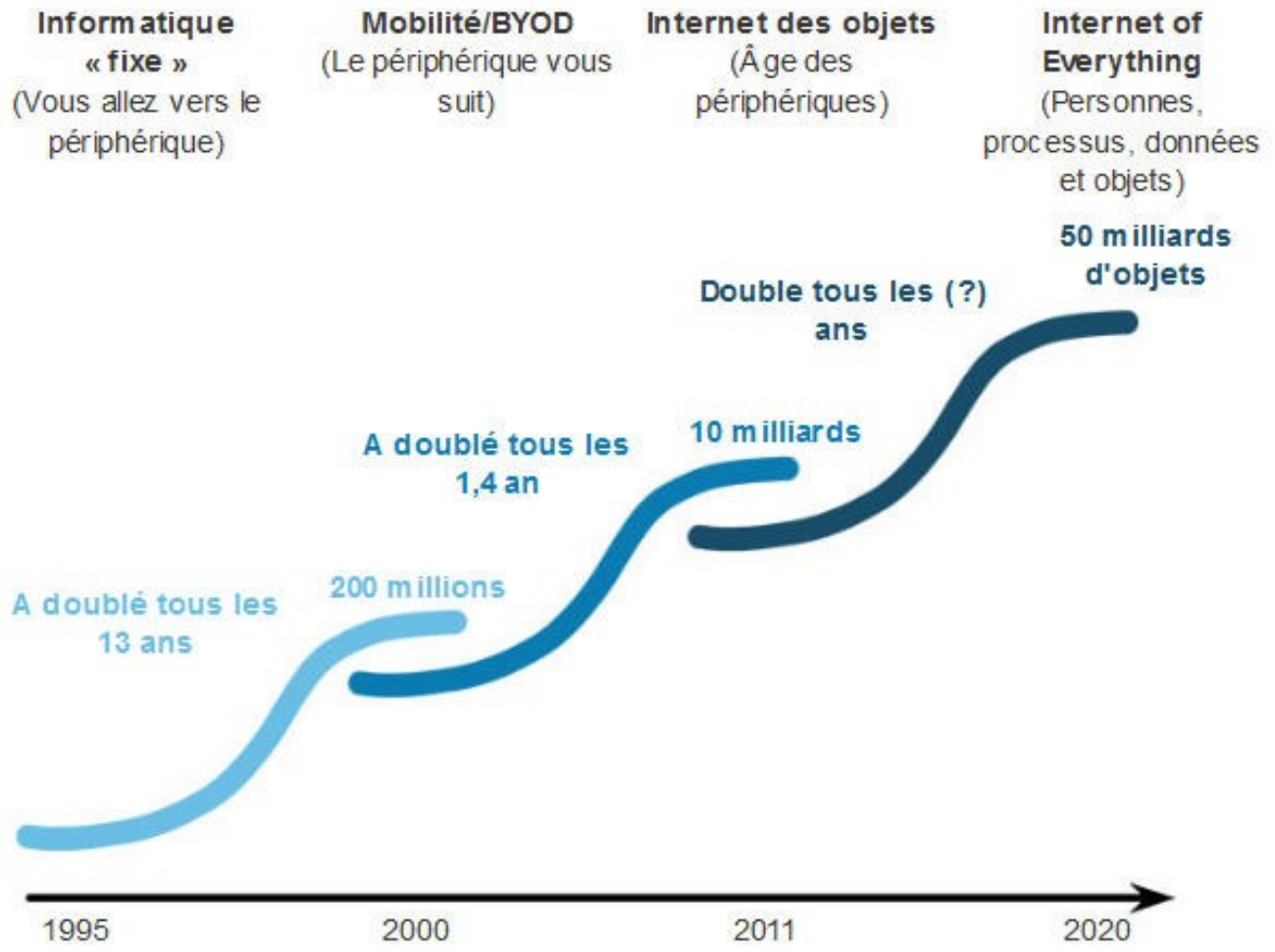
AVIGNON UNIVERSITÉ

Module 1 : Les réseaux aujourd'hui

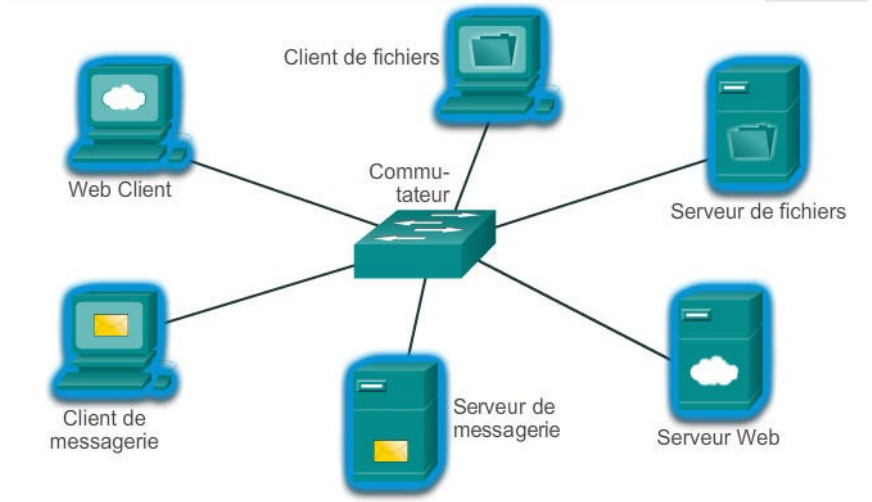
Initiation aux réseaux

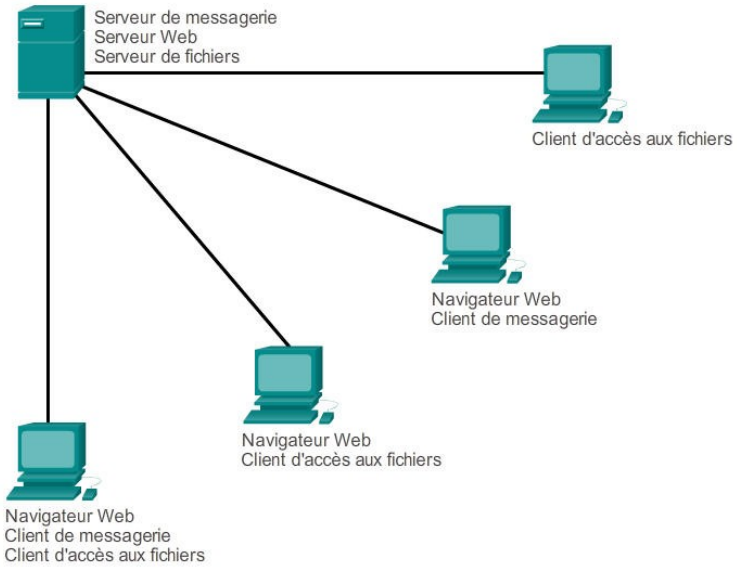
Cisco | Networking Academy®
Mind Wide Open™

Les réseaux que nous avons connus et ceux de notre vie quotidienne

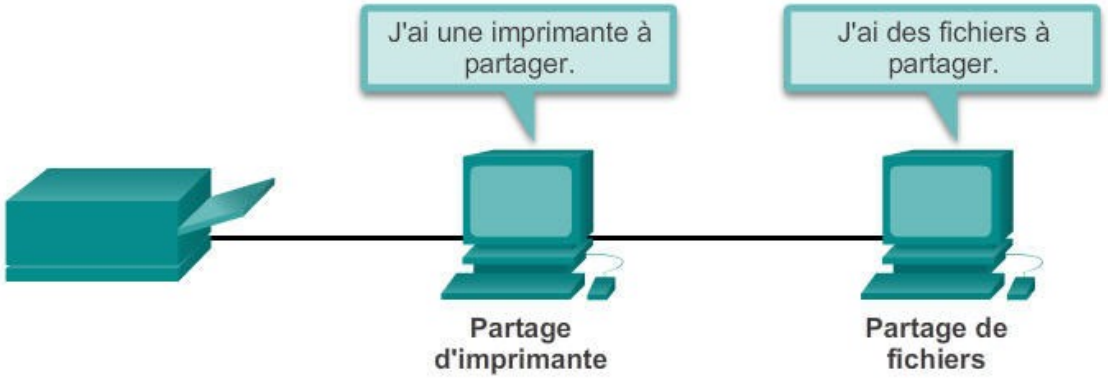


Clients et serveurs





Peer-to-Peer (P2P)



Avantages du réseau peer-to-peer :

- Facile à configurer
- Moins complexe
- Coût inférieur étant donné que les périphériques réseau et les serveurs dédiés peuvent ne pas être nécessaires
- Peut être utilisé pour des tâches simples telles que le transfert de fichiers et le partage des imprimantes

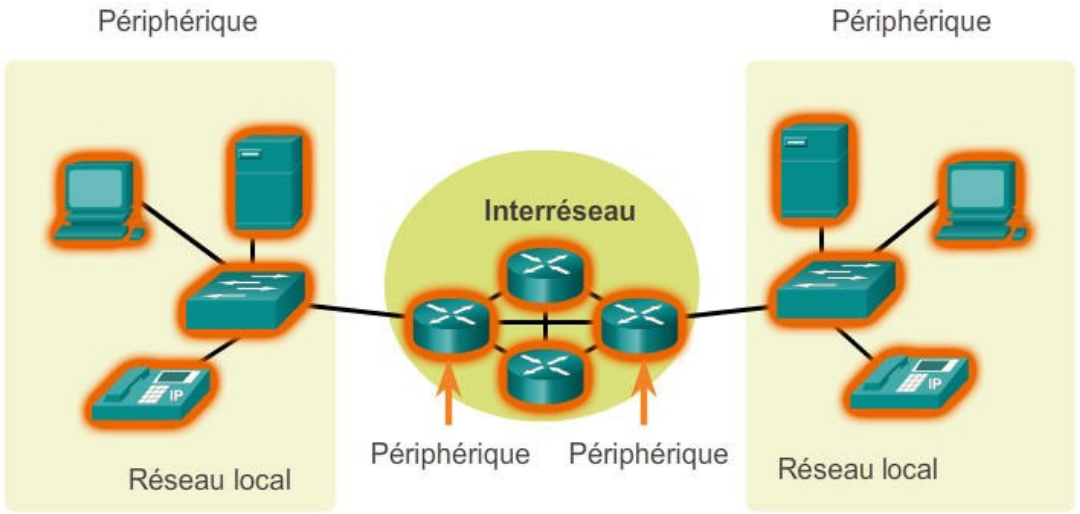
Inconvénients du réseau peer-to-peer :

- Pas d'administration centralisée
- Peu sécurisé
- Non évolutif
- Tous les périphériques peuvent servir à la fois de client et de serveur, ce qui peut ralentir les performances

Composants d'un réseau

Les composants d'un réseau se classent en trois catégories :

- Les périphériques
- Les supports de transmission
- Les services



Les périphériques finaux

Voici quelques exemples de périphériques finaux :

- Ordinateurs (stations de travail, ordinateurs portables, serveurs de fichiers, serveurs Web)
- Imprimantes réseau
- Téléphones VoIP
- Caméras de surveillance
- Appareils portatifs (smartphones, tablettes, lecteurs de carte sans fil et lecteurs de codes à barres)

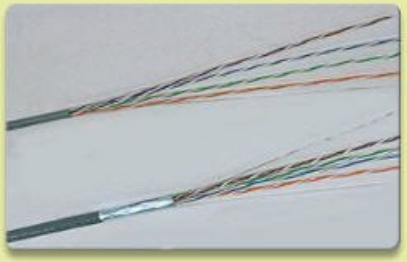
Équipements de l'infrastructure réseau

Parmi ces périphériques réseau intermédiaires, citons :

- Les périphériques d'accès réseau (commutateurs et points d'accès sans fil)
- Les périphériques interréseau (routeurs)
- Les dispositifs de sécurité (pare-feu)

Supports de transmission

Cuivre

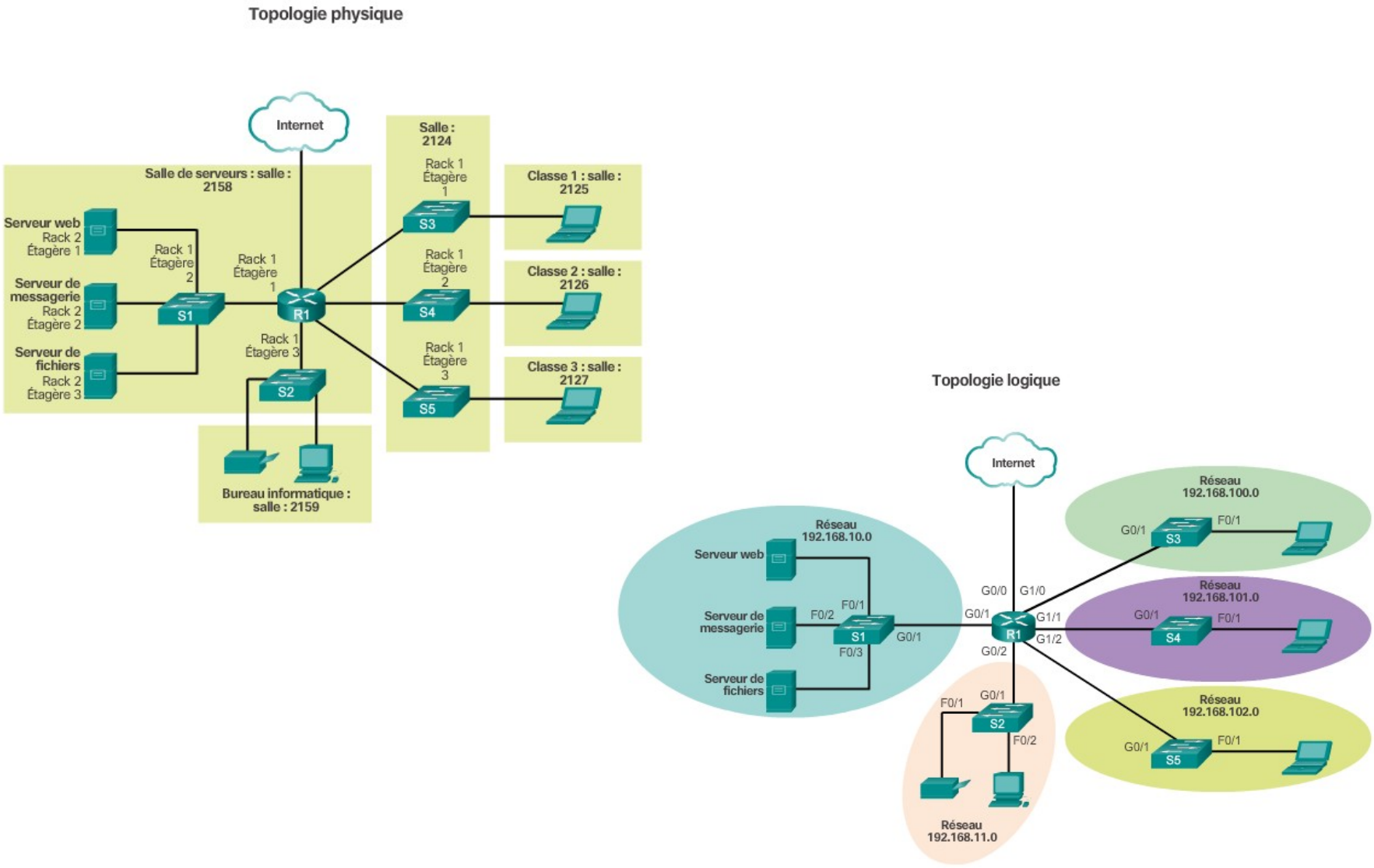


Fibre optique

Sans fil

Représentations graphiques des réseaux

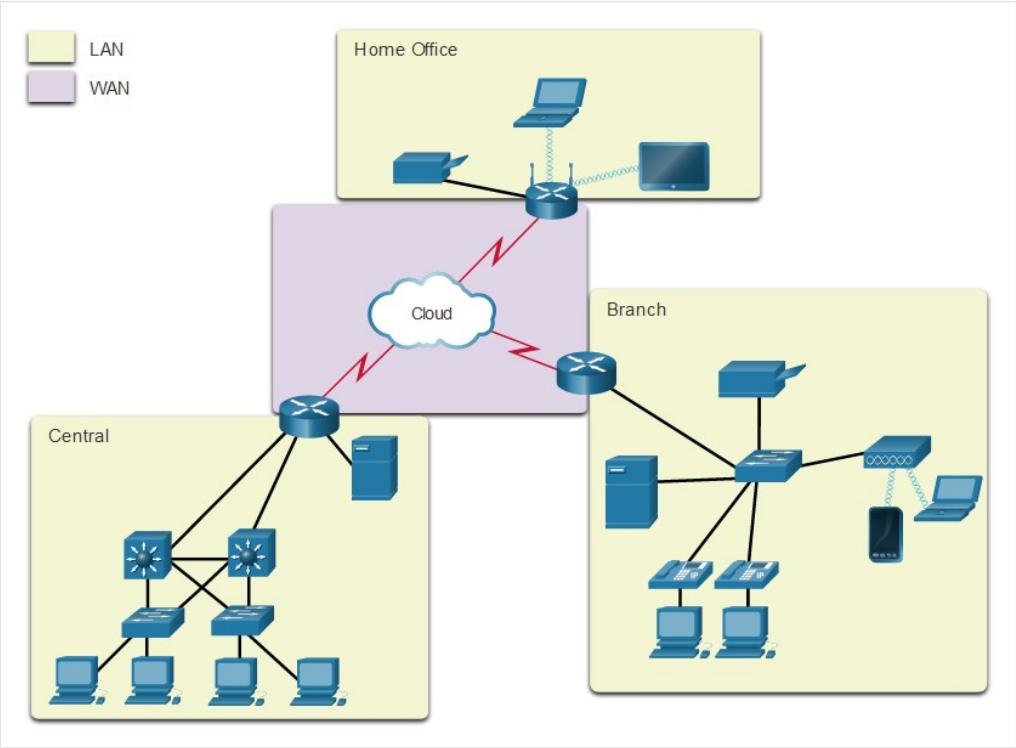
Diagrammes de topologie



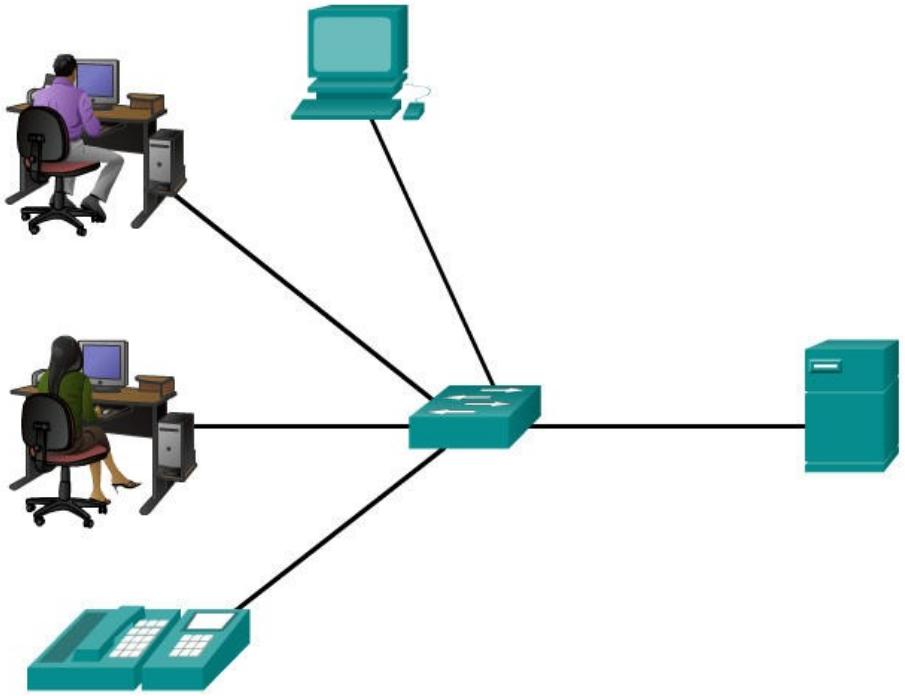
Types de réseau

Les deux types d'infrastructures réseau les plus répandus sont :

- Le réseau local (LAN)
- Le réseau étendu (WAN)

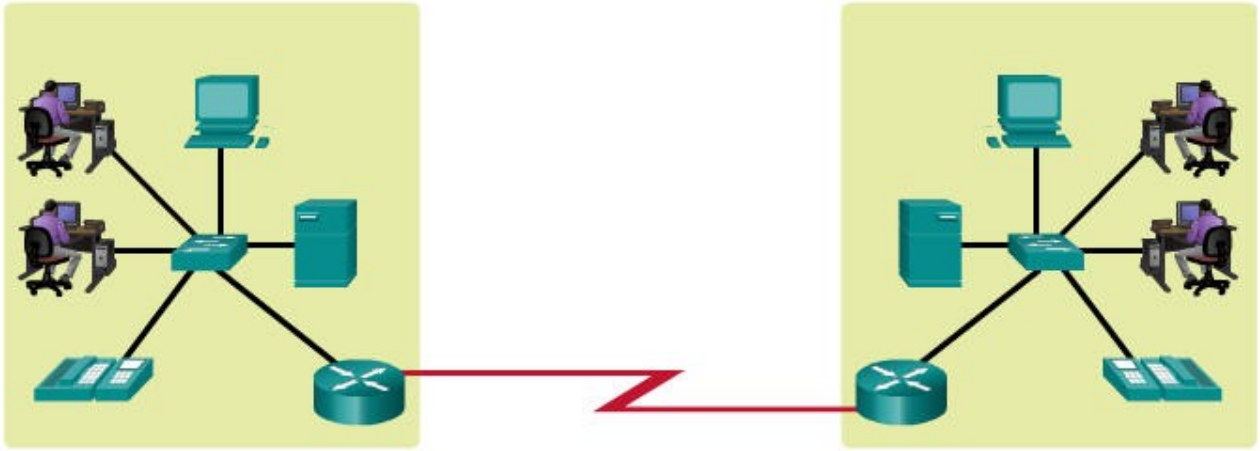


Réseaux locaux (LAN)



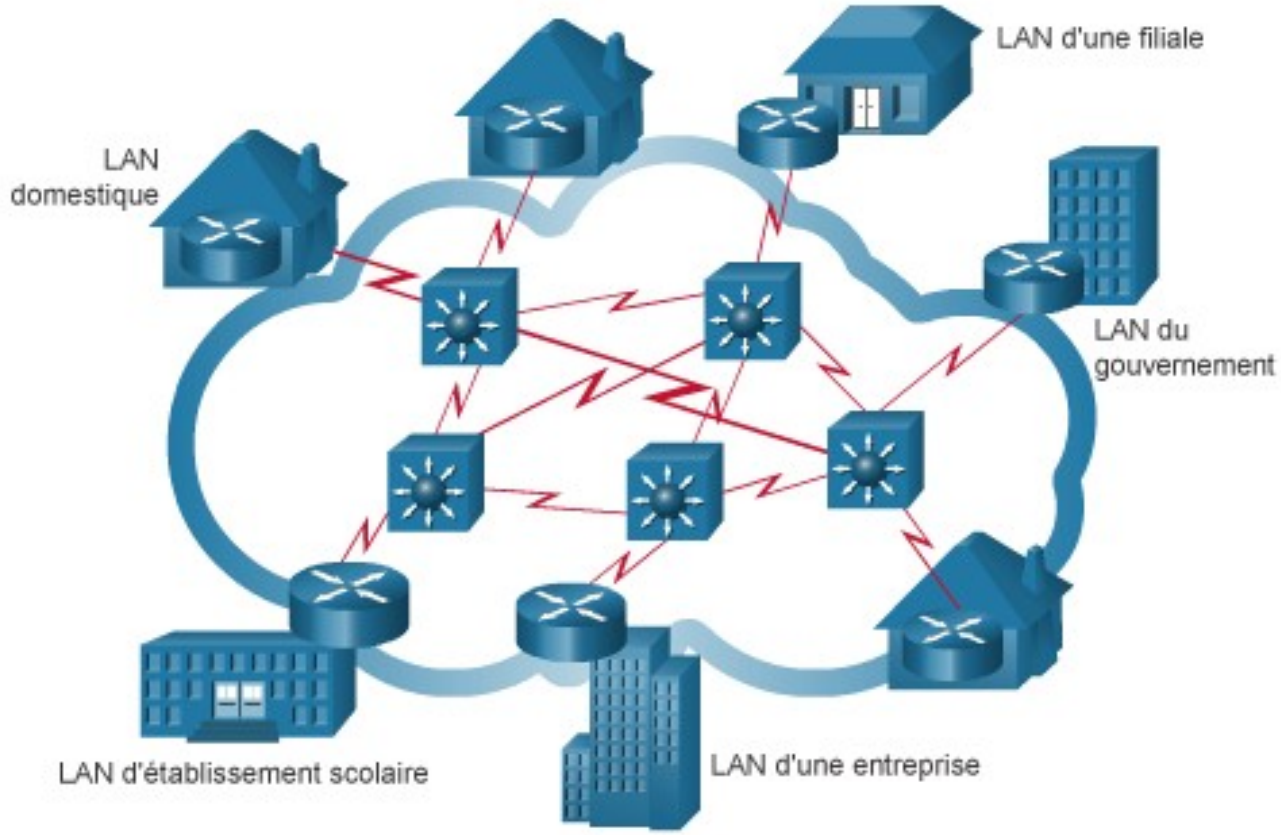
Le réseau d'une maison individuelle, d'un bâtiment ou d'un campus est appelé « réseau local ».

Réseaux étendus (WAN)

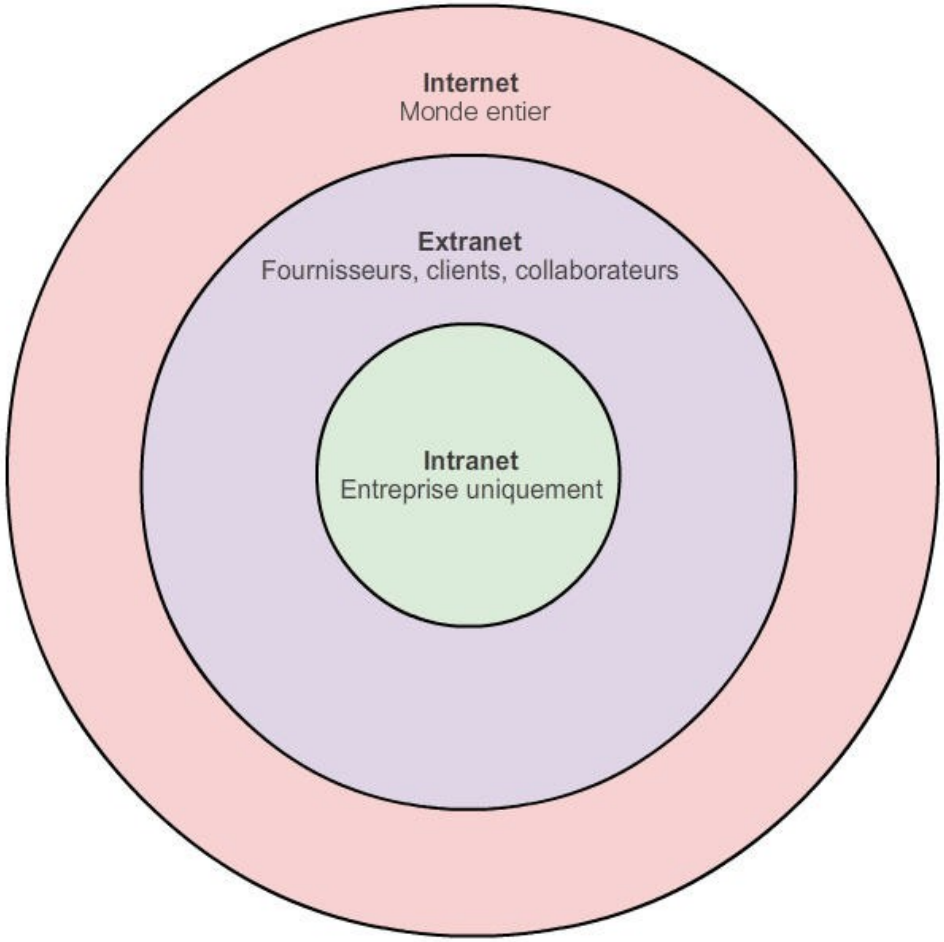


Les réseaux locaux séparés géographiquement sont reliés par le biais d'un réseau appelé « réseau étendu ».

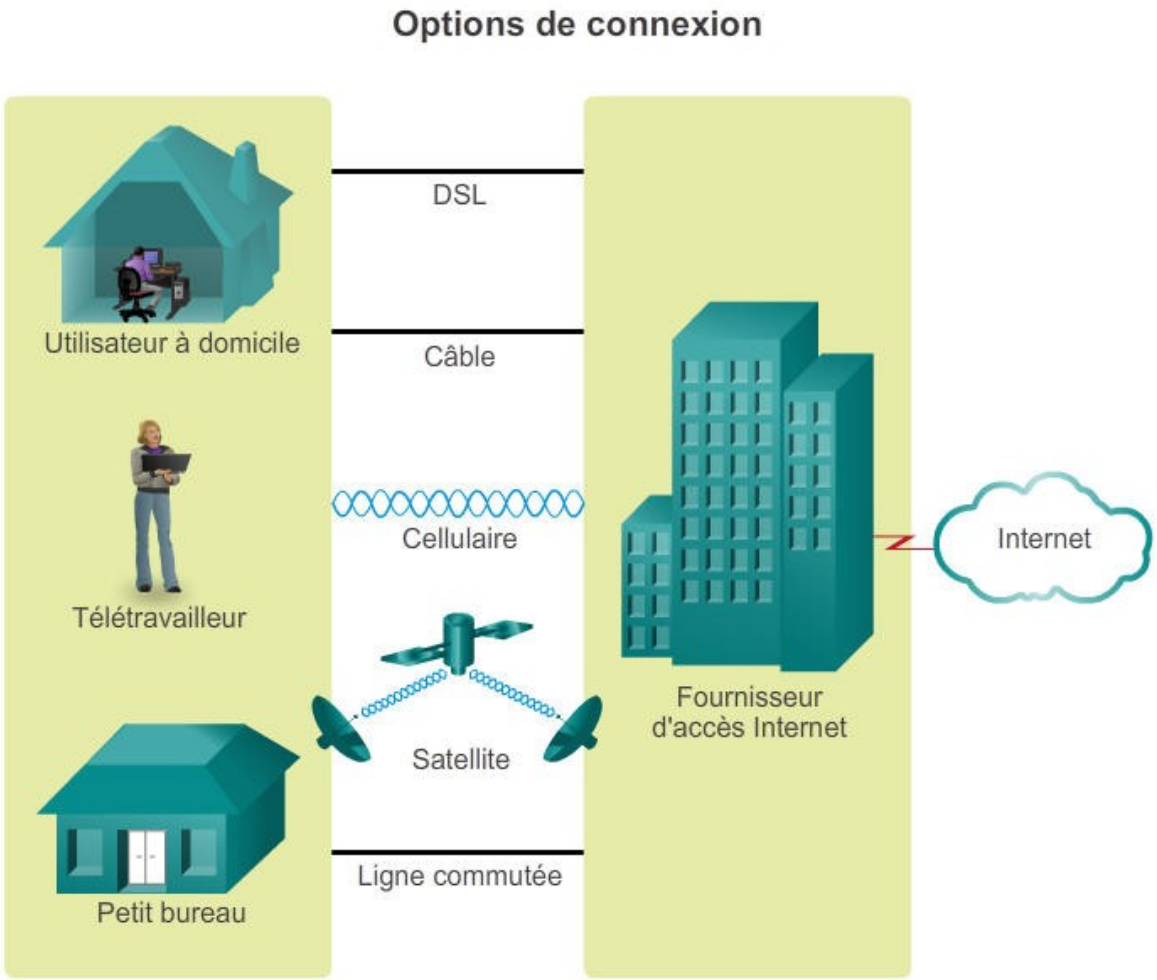
Internet


LAN d'une filiale
LAN domestique
LAN du gouvernement
LAN d'établissement scolaire
LAN d'une entreprise

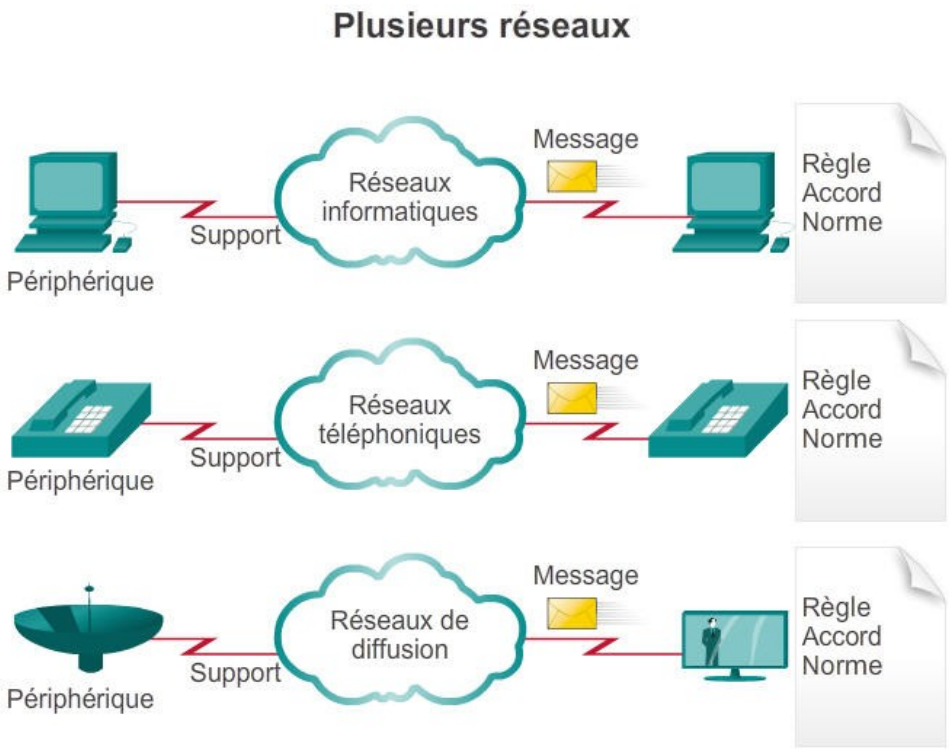
Intranet et Extranet



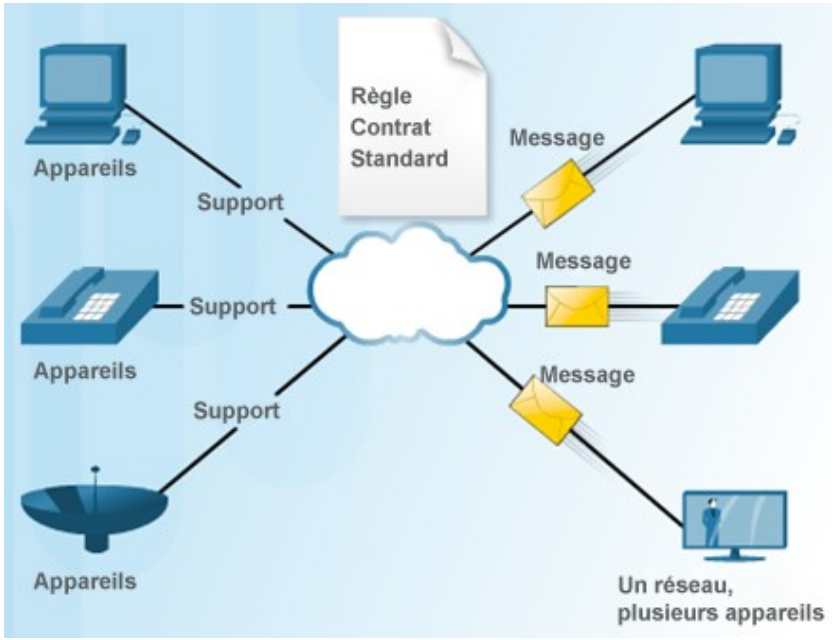
Connexion des utilisateurs distants à Internet



Réseau convergent

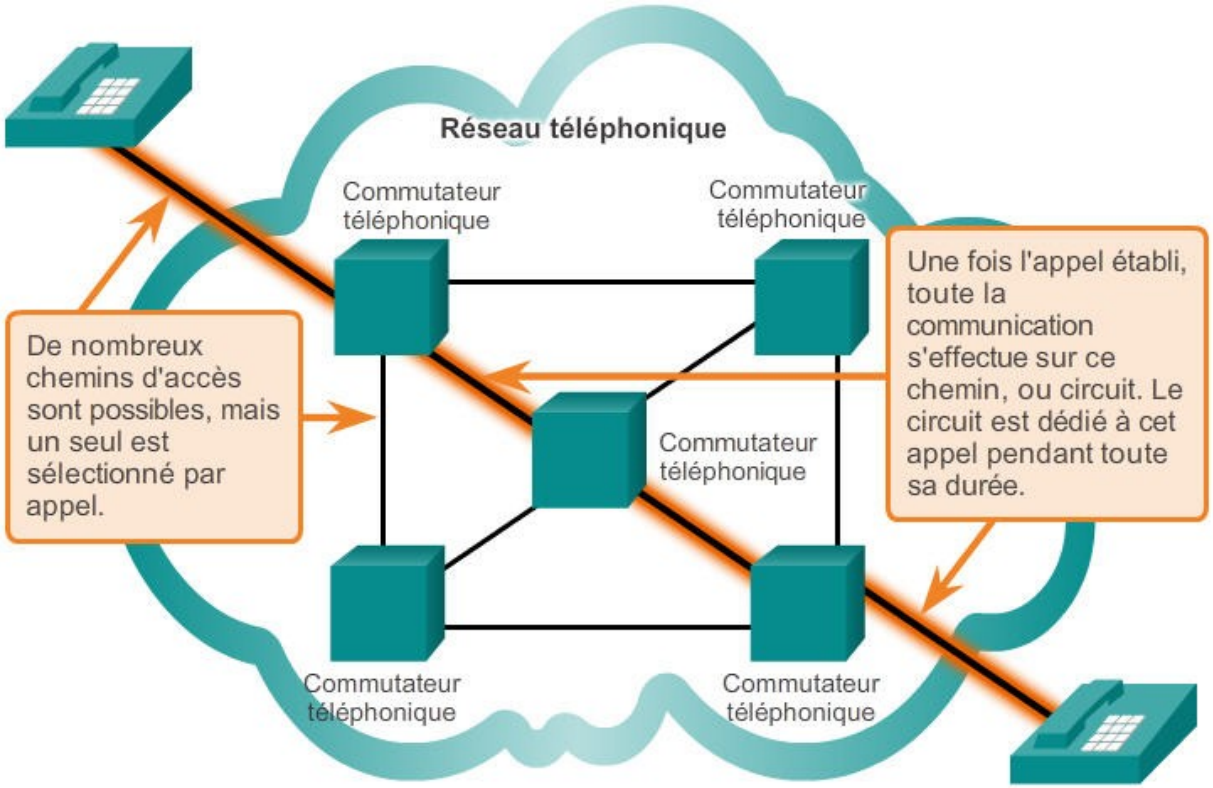


Plusieurs services s'exécutent sur plusieurs réseaux.



Réseaux à commutation de circuits

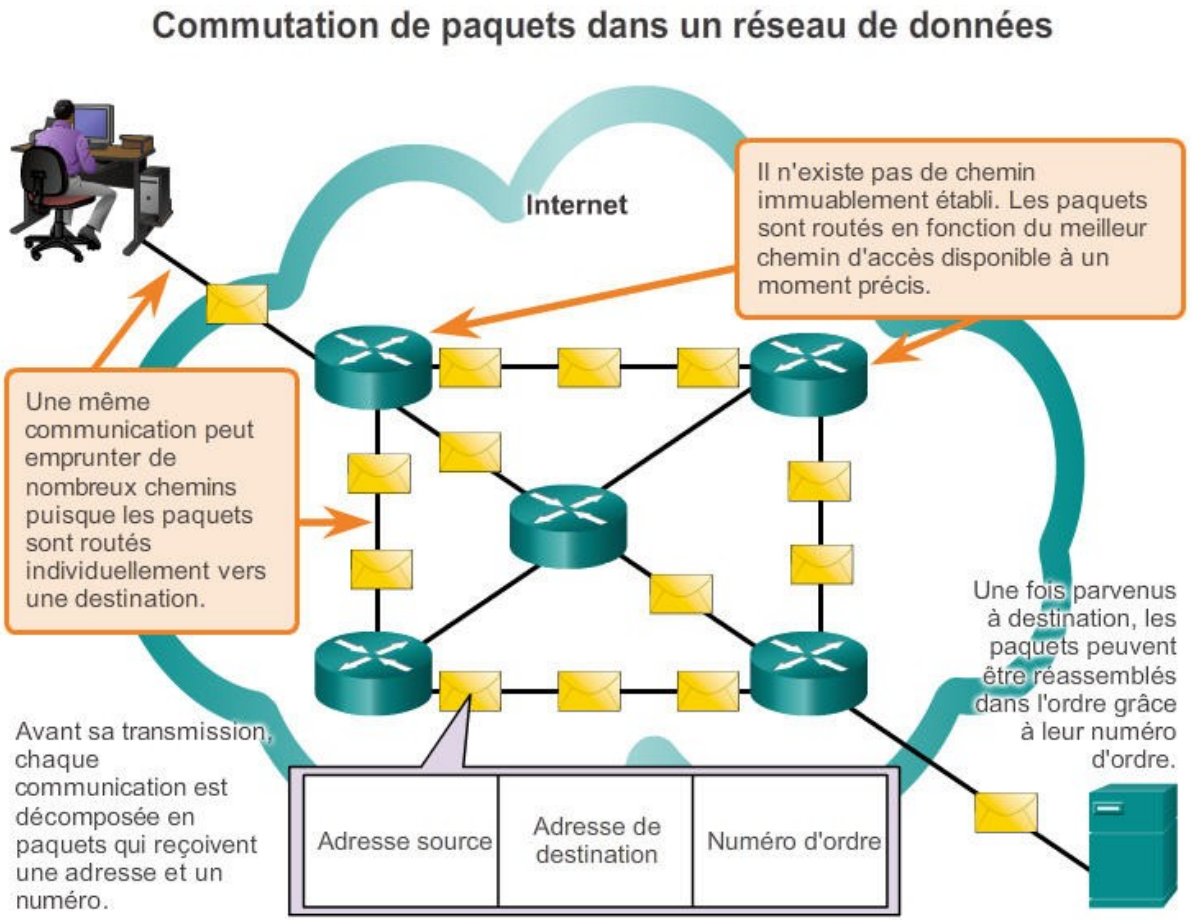
Commutation de circuits dans un réseau téléphonique



Le circuit demeure actif même si personne ne parle.

Il existe de nombreux circuits, mais leur nombre n'est cependant pas illimité. Pendant les périodes de pointe, certains appels peuvent être rejetés.

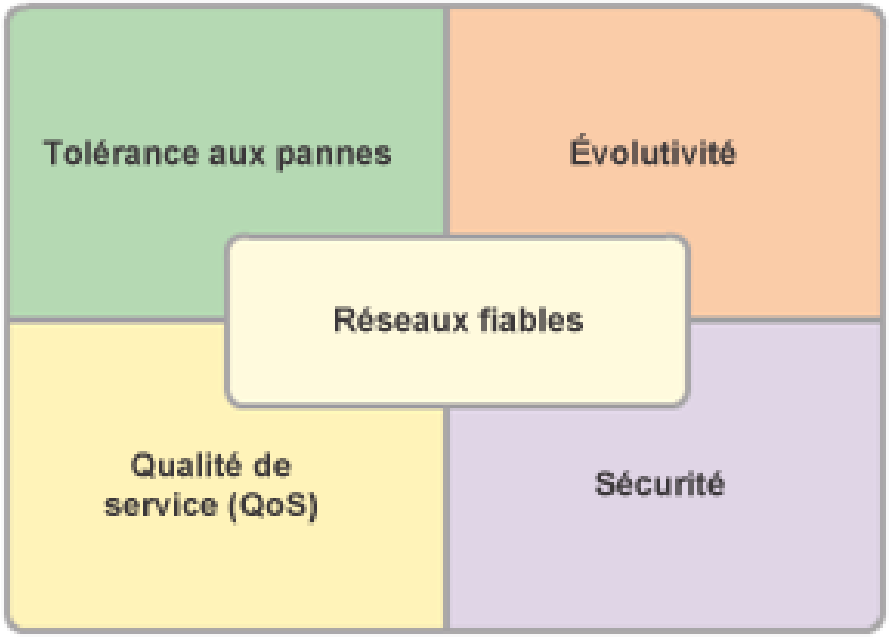
Réseaux à commutation de paquets



Pendant les périodes de pointe, une communication peut être retardée, mais pas refusée.

Caractéristiques d'une architecture réseau

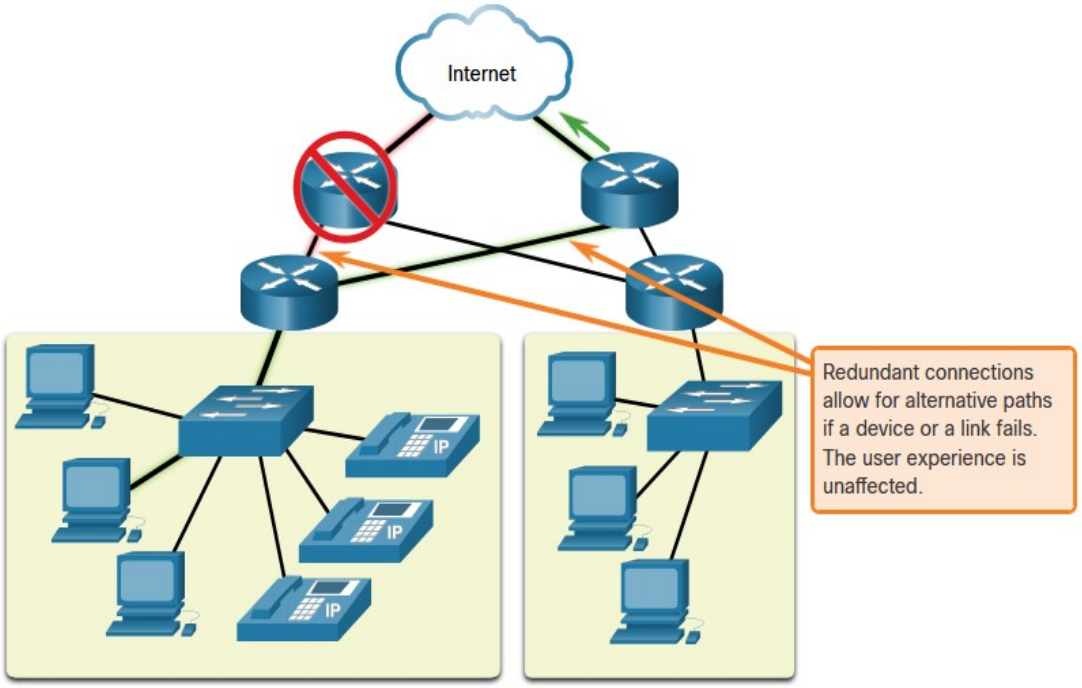
- Les quatre principales caractéristiques d'une architecture de réseau
  - Tolérance aux pannes
  - Évolutivité
  - Qualité de service (QoS)
  - Sécurité



Tolérance aux pannes

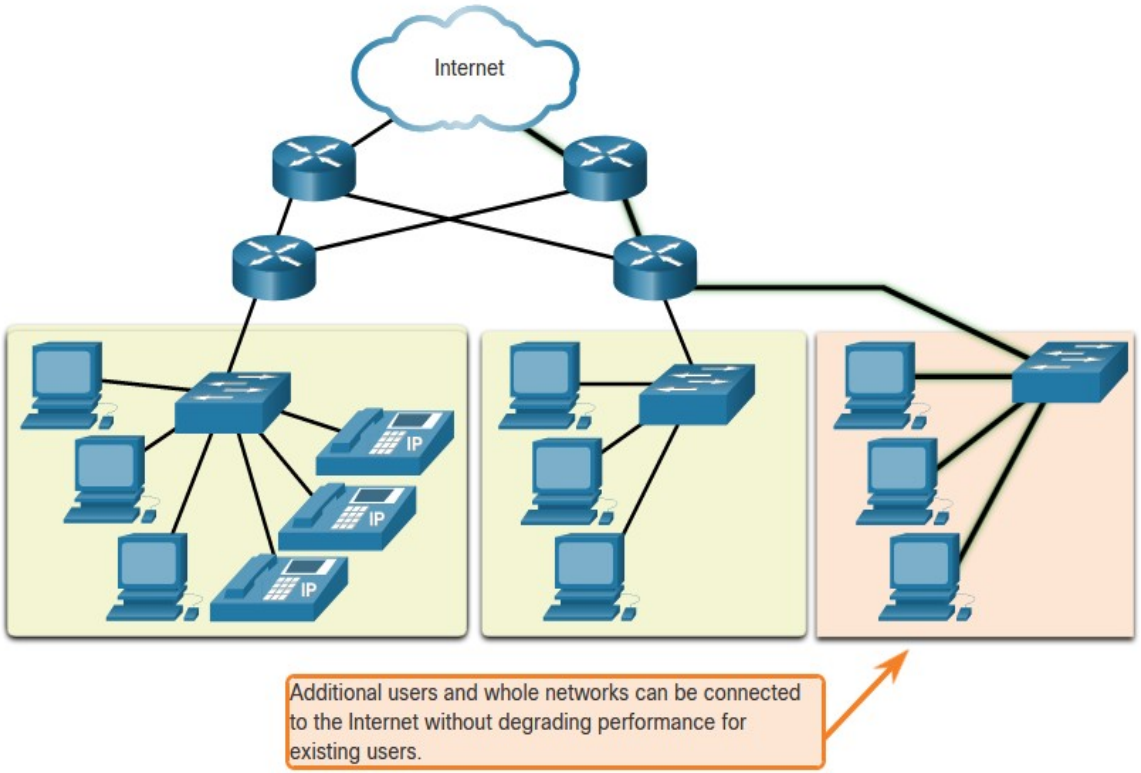
Un réseau tolérant aux pannes limite l'impact d'une défaillance d'en limitant le nombre de périphériques affectés

Plusieurs chemins d'accès sont nécessaires pour la tolérance de panne



Évolutivité

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

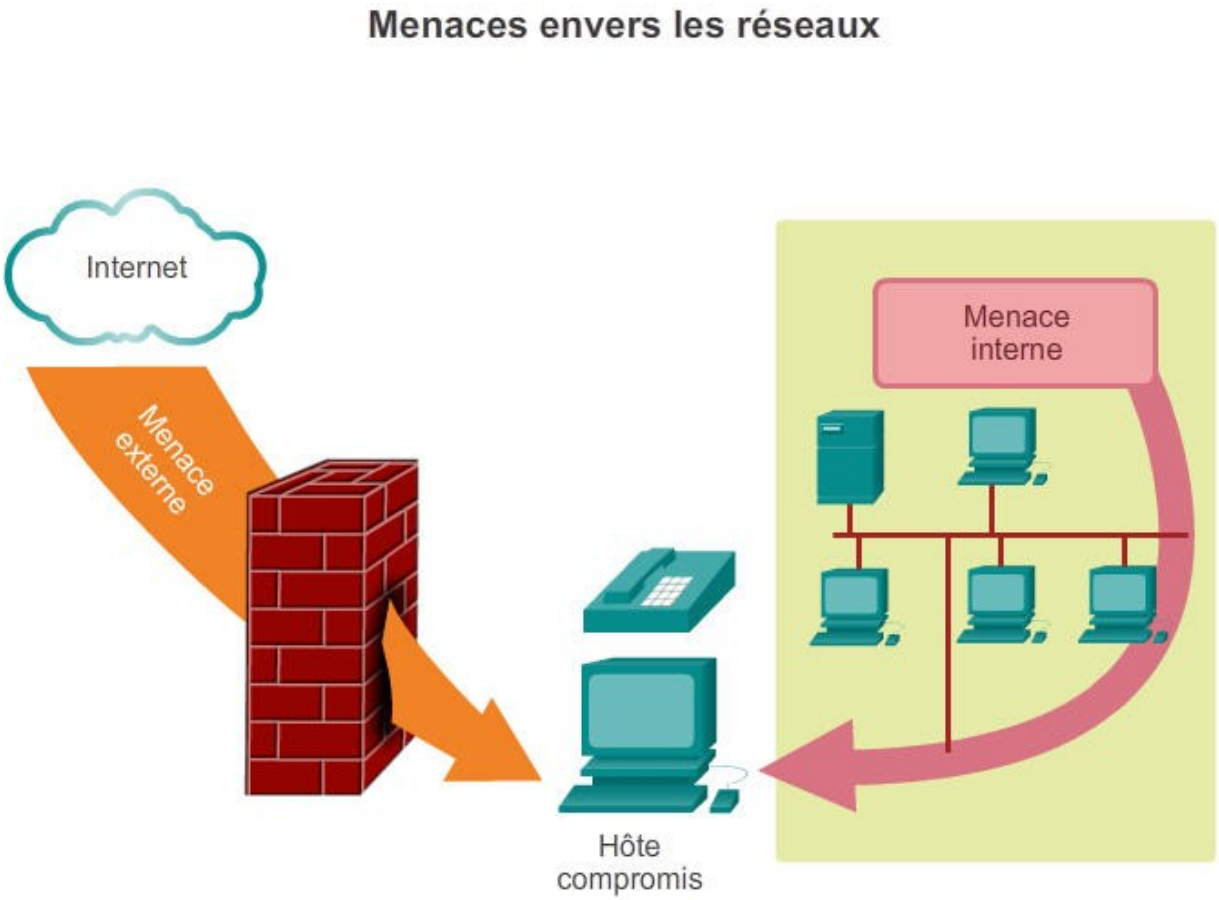


Qualité de service (QS)

Dans une entreprise, il faut établir des priorités. Par exemple :

- Les communications pour lesquelles la vitesse est importante (augmenter la priorité des services tels que la téléphonie ou la distribution vidéo)
- Les communications pour lesquelles la vitesse n'est pas importante (réduire la priorité du téléchargement des pages Web ou des e-mails)

Sécurité du réseau



Menaces pour la sécurité

Les menaces externes les plus courantes pour les réseaux sont les suivantes :

- Virus, vers et chevaux de Troie
- Logiciels espions et logiciels publicitaires
- Attaques zero-day (également appelées attaques zero-hour)
- Piratage informatique
- Attaques par déni de service
- Interception et vol de données
- Usurpation d'identité

Solutions de sécurité

La sécurité du réseau repose souvent sur les éléments suivants :

- Antivirus et logiciel anti-espion
- Filtrage au niveau du pare-feu
- Systèmes de pare-feu dédiés
- Listes de contrôle d'accès (ACL)
- Systèmes de protection contre les intrusions
- VPN

Résumé

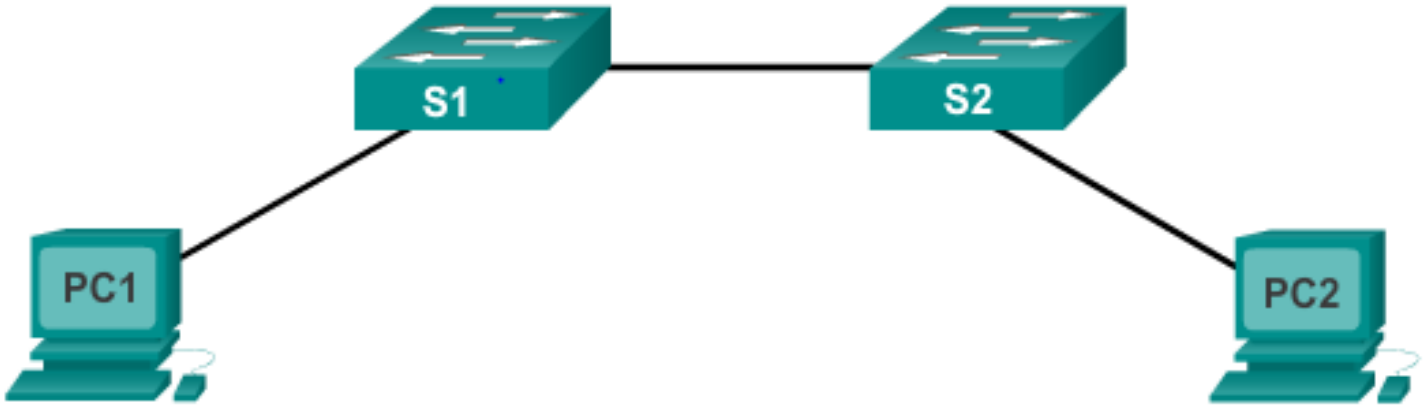
- Décrire les différents réseaux utilisés dans la vie quotidienne
- Décrire les topologies et les équipements utilisés dans un réseau de PME
- Expliquer les caractéristiques de base d'un réseau prenant en charge la communication dans une PME
- Expliquer les tendances liées au réseau qui affecteront l'utilisation des réseaux dans les PME

Module 2 : Configuration de base des commutateurs et des terminaux

Initiation aux réseaux

Cisco | Networking Academy®
Mind Wide Open™

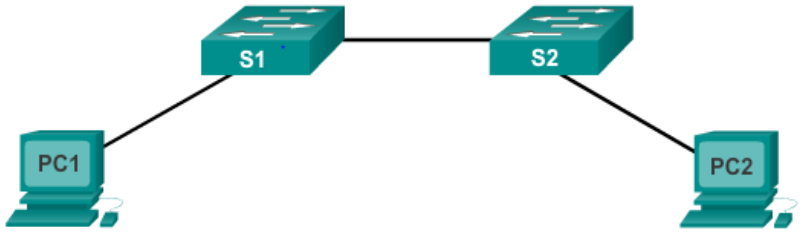
2.1 Formation à IOS



Systèmes d'exploitation

Tous les équipements réseau dépendent des systèmes d'exploitation

- Utilisateurs finaux (PC, ordinateurs portables, smartphones, tablettes)
- Commutateurs
- Routeurs
- Points d'accès sans fil
- Pare-feu



Cisco Internetwork Operating System (IOS)

- Ensemble de systèmes d'exploitation réseau utilisés sur les périphériques Cisco

Rôle du système d'exploitation

- Les systèmes d'exploitation des ordinateurs assurent les fonctions techniques qui permettent
  - D'utiliser une souris
  - D'afficher des résultats
  - De saisir du texte

- L'IOS du routeur ou du commutateur fournit des options pour
  - Configurer les interfaces
  - Activer les fonctions de routage et de commutation

- Tous les périphériques réseau sont livrés avec un IOS par défaut

- Il est possible de mettre à niveau la version de l'IOS ou l'ensemble de fonctionnalités

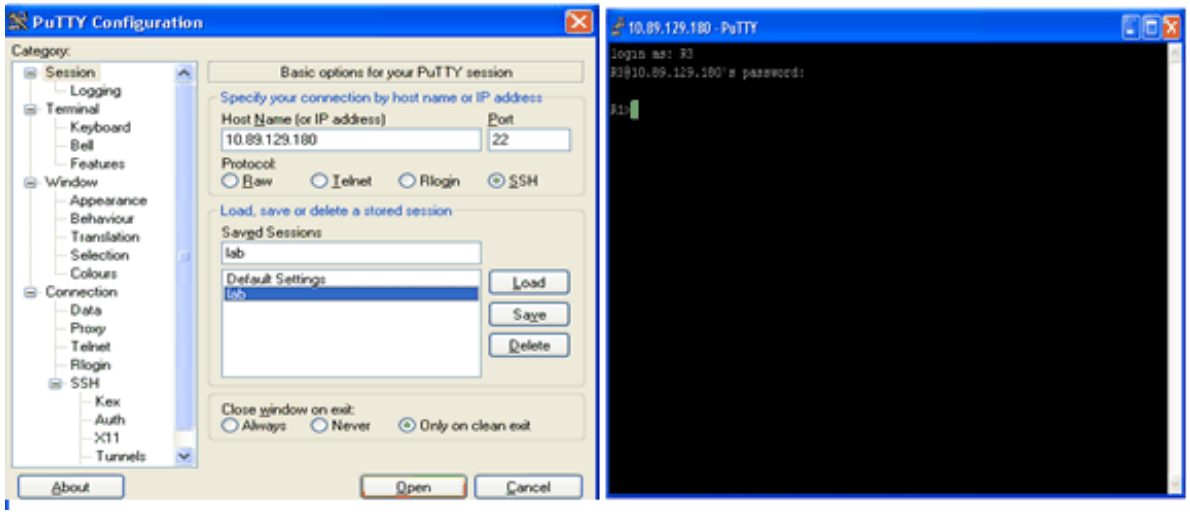
Emplacement de Cisco IOS

IOS stocké dans la **mémoire Flash**

- Stockage non volatile : préservé en cas de coupure de l'alimentation
- Peut être modifié ou remplacé si nécessaire
- Peut être utilisé pour stocker plusieurs versions d'IOS
- IOS copié de la mémoire flash vers la mémoire vive (RAM) non volatile
- La quantité de mémoire RAM et Flash détermine l'IOS qui peut être utilisé

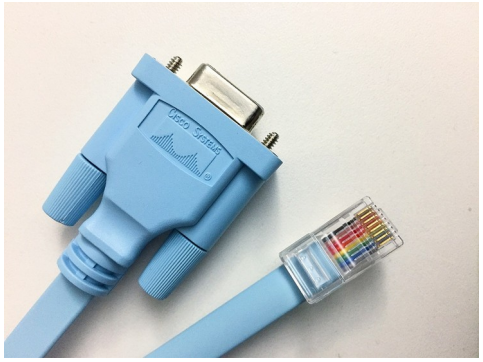
Méthodes d'accès

- **Console** – Utilise un port de gestion physique pour accéder à un périphérique afin d'assurer la maintenance, par exemple lors des configurations initiales.
- **Secure Shell (SSH)** - Établit une connexion CLI à distance sécurisée avec un périphérique, par le biais d'une interface virtuelle, sur un réseau.
- **Telnet** - Établit une connexion CLI distante non sécurisée à un périphérique sur le réseau.



Accès par une console

Port de console



- Le périphérique est accessible même si aucun service réseau n'a été configuré (hors réseau)
- Nécessite un câble de console spécial
- Permet d'entrer des commandes de configuration
- Doit être configuré avec des mots de passe pour empêcher les accès non autorisés
- Le périphérique doit se trouver dans une pièce sécurisée afin d'éviter l'utilisation non autorisée du port de console

Méthodes d'accès Telnet, SSH et AUX

Telnet

- Méthode d'accès à distance à l'interface en ligne de commande via le réseau
- Connexion sans câble console
- Les services réseau doivent être activés et une interface active doit être configurée

Secure Shell (SSH)

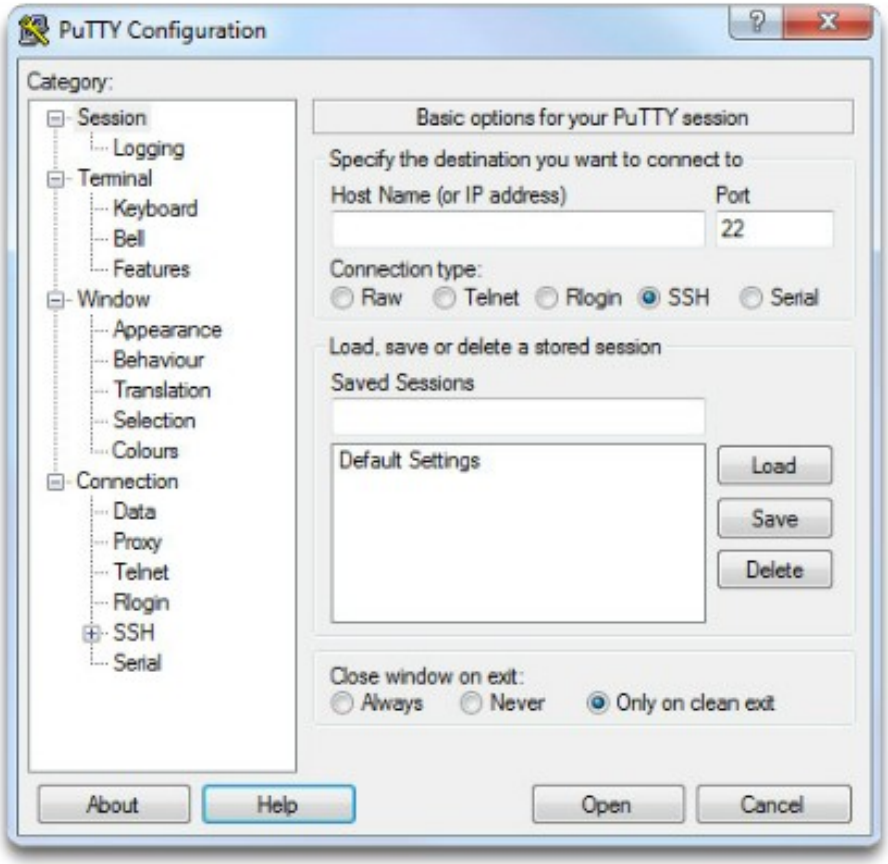
- Connexion à distance analogue à Telnet (sans câble console, configuration d'une interface active), mais mieux sécurisée
- Authentification par mot de passe plus robuste
- Utilisation du chiffrement lors du transport des données

Programmes d'émulation de terminal

Logiciels permettant de se connecter à un périphérique réseau

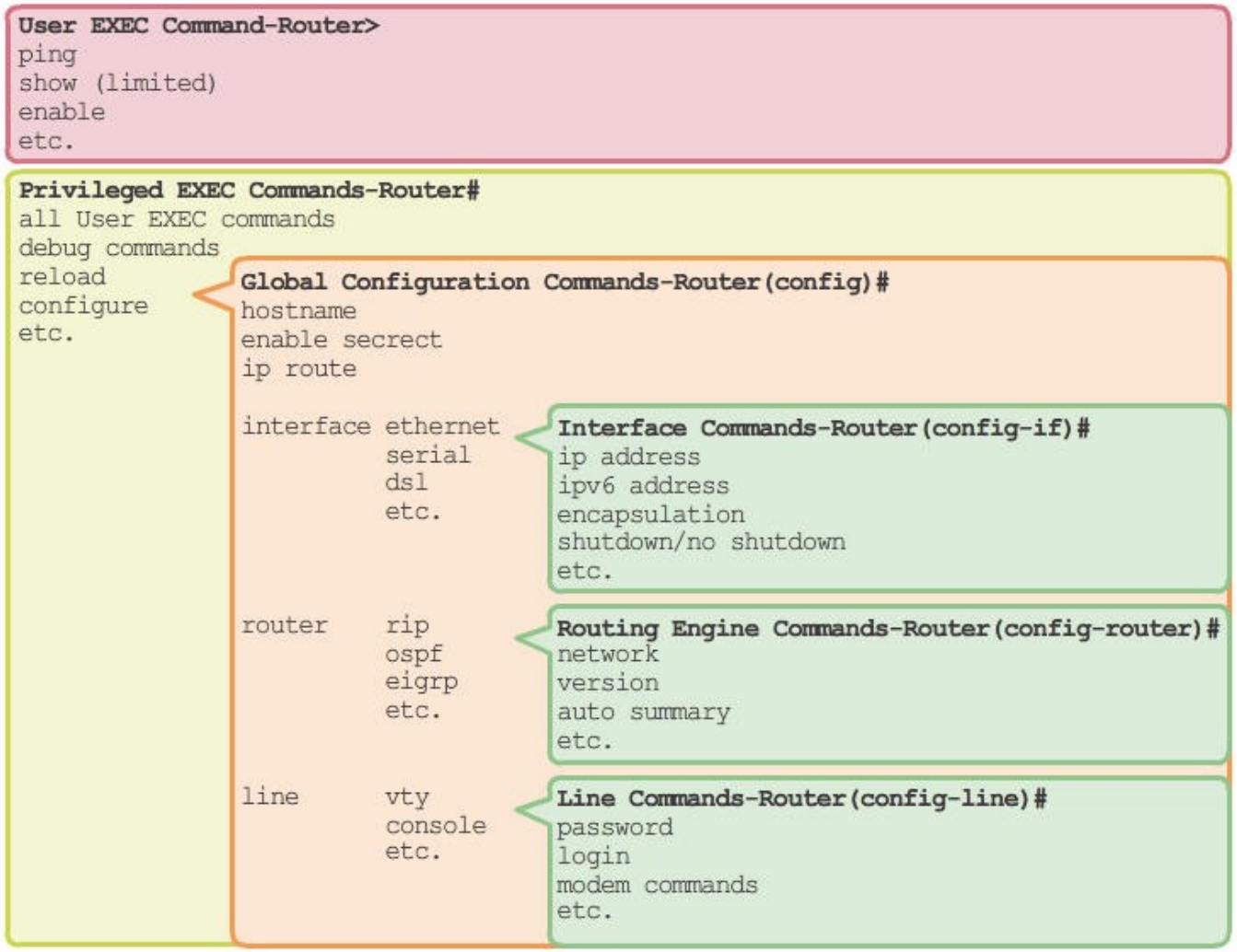
- PuTTY
- Tera Term
- SecureCRT
- HyperTerminal
- Terminal OS X

PuTTY



Modes de fonctionnement de Cisco IOS

Structure hiérarchique des modes IOS



Modes principaux

Mode d'exécution utilisateur

Examen limité du routeur. Accès à distance

```
Switch>
Router>
```

Le mode d'**exécution utilisateur** n'autorise qu'un nombre limité de commandes de surveillance de base et est souvent appelé mode « lecture seule ».

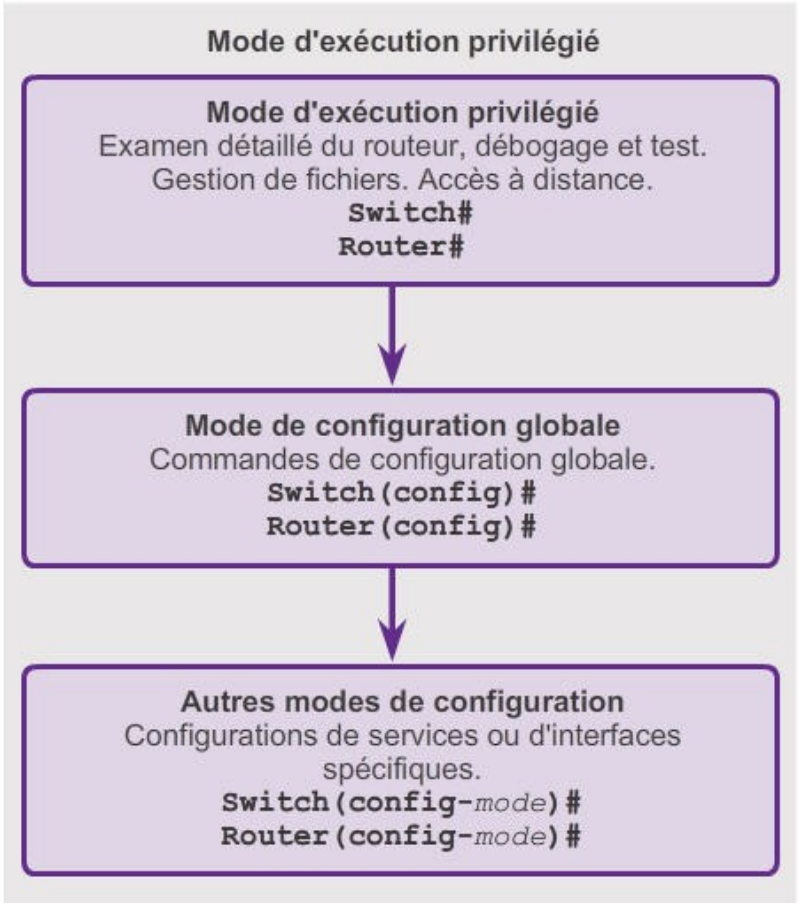
Mode d'exécution privilégié

Examen approfondi du routeur. Débogage et test. Gestion de fichiers. Accès à distance

```
Switch#
Router#
```

Le mode d'**exécution privilégié**, par défaut, autorise toutes les commandes de surveillance, ainsi que l'exécution des commandes de configuration et de gestion.

Mode de configuration globale et sous-modes



Structure d'invites IOS

```
Router>ping 192.168.10.5

Router#show running-config

Router(config)#Interface FastEthernet 0/0

Router(config-if)#ip address 192.168.10.1 255.255.255.0
```

L'invite change pour refléter le mode actuel de la CLI.

```
Switch>ping 192.168.10.9

Switch#show running-config

Switch(config)#Interface FastEthernet 0/1

Switch(config-if)#Description connection to WEST LAN4
```

Sélection des différents modes IOS

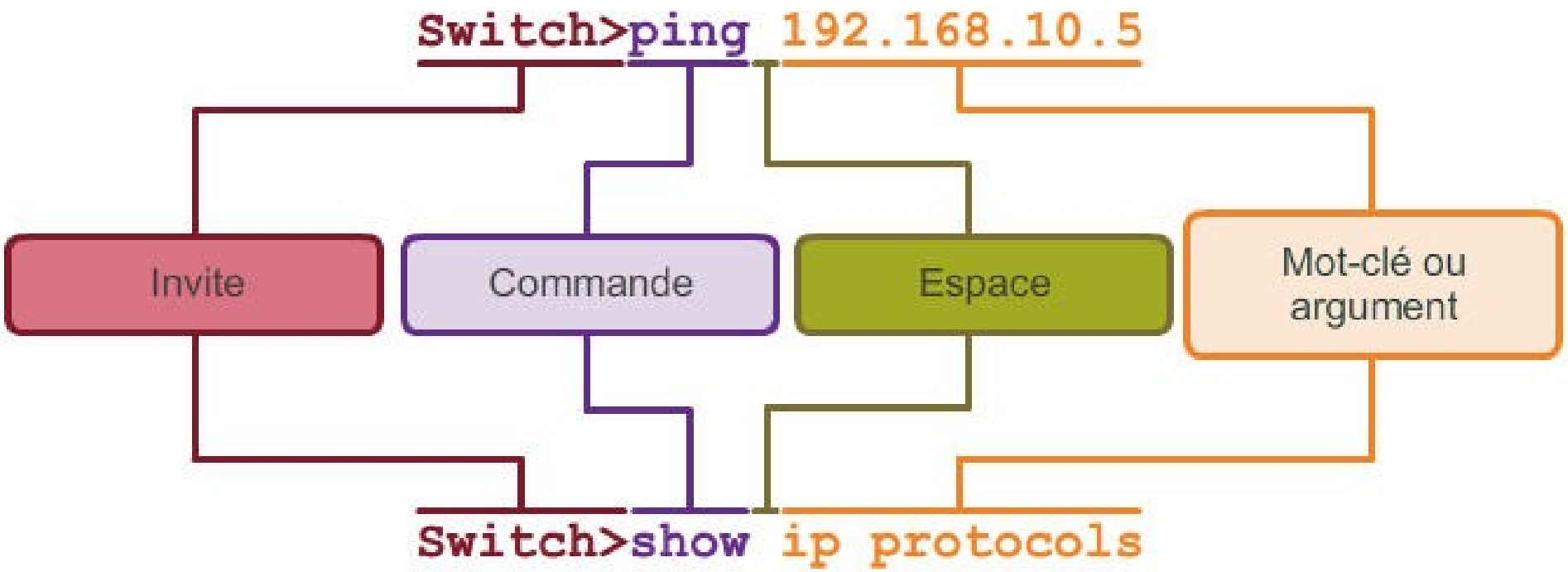
Sélection des différents modes IOS (suite)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#interface vlan 1
Switch(config-if)#exit
Switch(config)#exit
Switch#
```

```
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#vlan 1
Switch(config-vlan)#end
Switch#
```

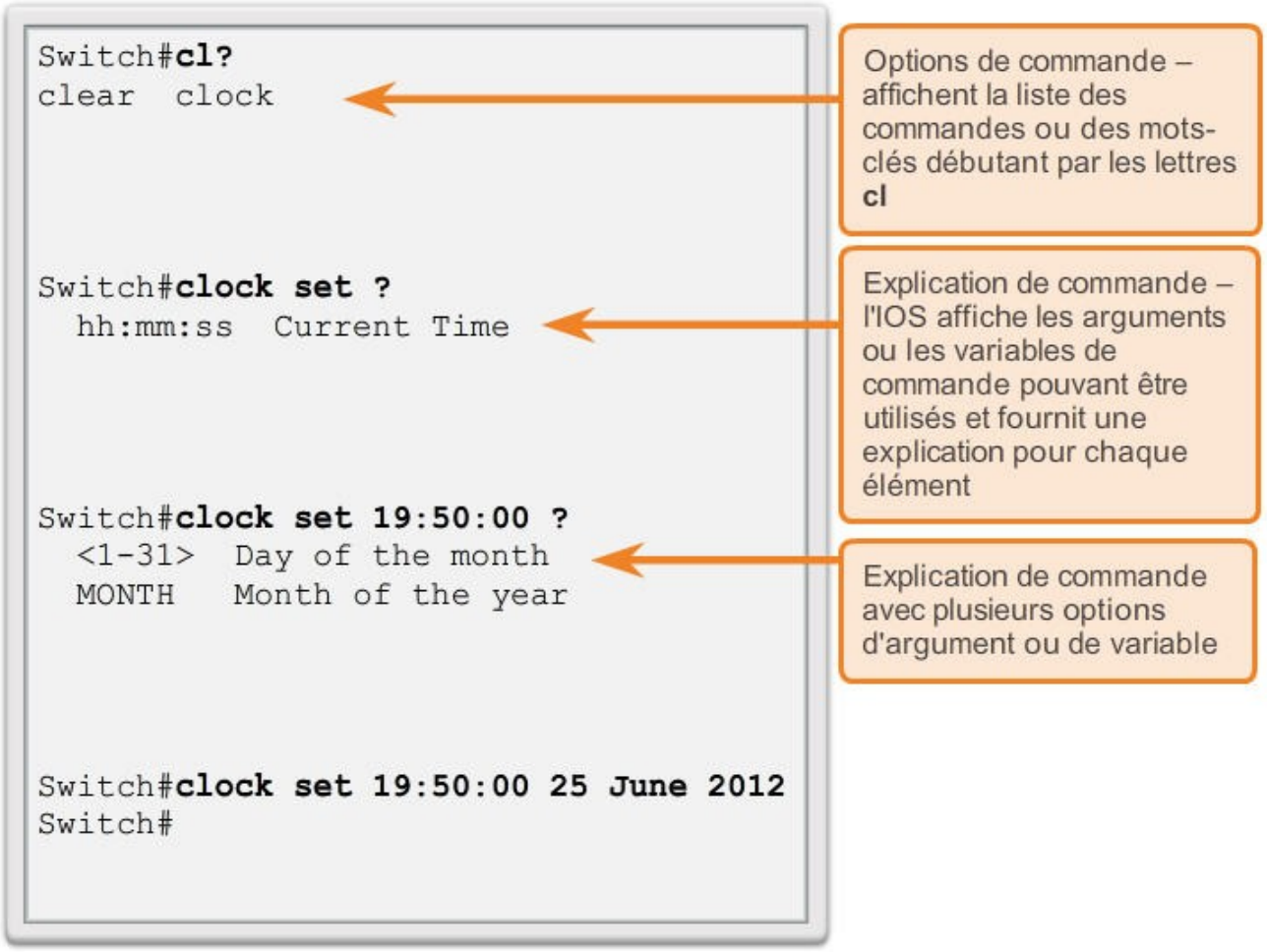
```
Switch#configure terminal
Enter configuration commands, one per line.
End with CNTL/Z.
Switch(config)#line vty 0 4
Switch(config-line)#interface fastethernet 0/1
Switch(config-if)#end
Switch#
```

Structure des commandes IOS



Aide contextuelle

Aide contextuelle



Vérification de la syntaxe d'une commande

```
Switch#>clock set
% Incomplete command.
Switch#clock set 19:50:00
% Incomplete command.
```

L'IOS renvoie un message d'aide indiquant que des mots-clés ou des arguments obligatoires manquent à la fin de la commande.

```
Switch#c
% Ambiguous command:'c'
```

L'IOS renvoie un message d'aide indiquant que vous n'avez pas entré assez de caractères pour permettre à l'interpréteur de commandes de reconnaître la commande.

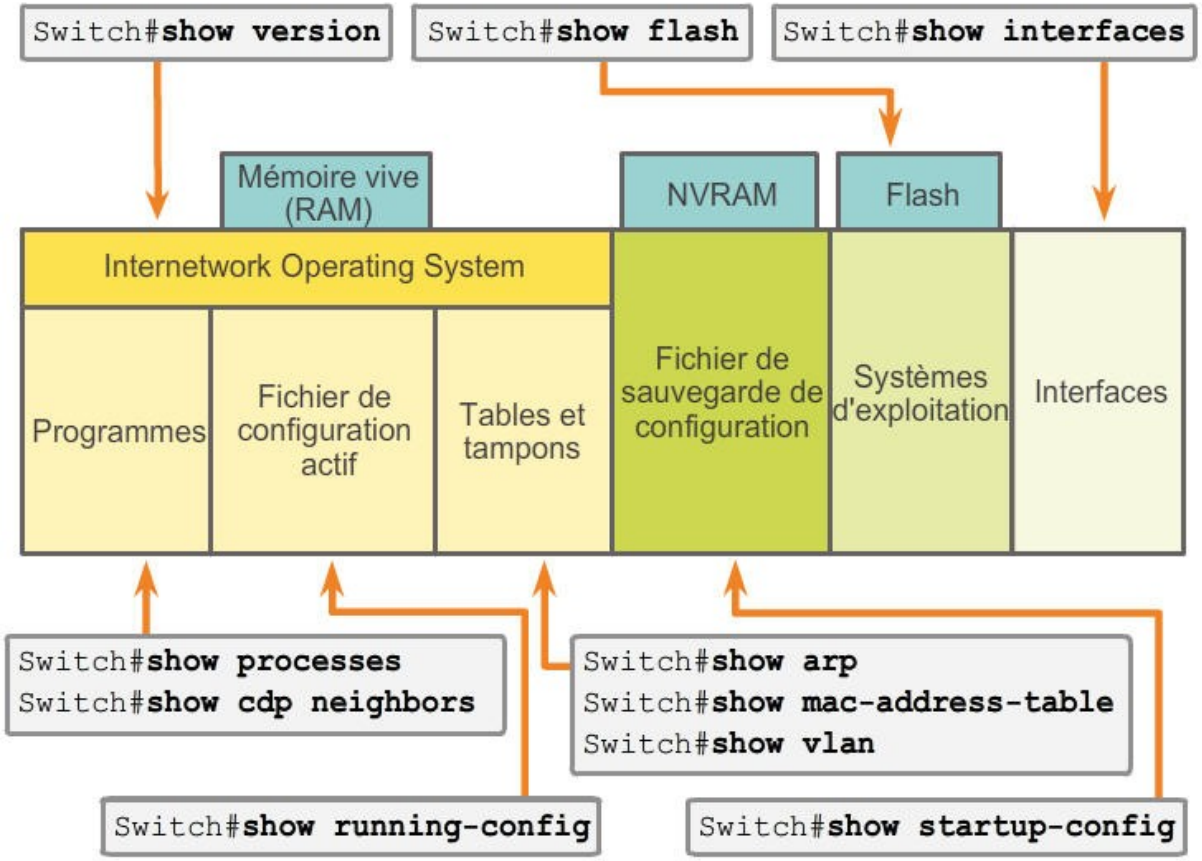
```
Switch#clock set 19:50:00 25 6
                           ^
% Invalid input detected at '^'
marker.
```

L'IOS renvoie un accent circonflexe (^) pour indiquer l'emplacement où l'interpréteur de commandes ne parvient pas à déchiffrer la commande.

Touches d'accès rapide et raccourcis

- **Tab :** complète une commande ou un mot clé partiellement saisis
- **Ctrl-R :** affiche à nouveau une ligne
- **Ctrl-A :** amène le curseur au début de la ligne
- **Ctrl-Z :** quitte le mode de configuration pour revenir au mode d'exécution utilisateur
- **Flèche Bas :** permet à l'utilisateur de faire défiler les commandes précédentes, de la plus ancienne à la plus récente
- **Flèche Haut :** permet à l'utilisateur de faire défiler les commandes précédentes, de la plus récente à la plus ancienne
- **Ctrl-Maj-6** (avec un clavier QWERTY) : permet à l'utilisateur d'interrompre un processus IOS tel que **ping** ou **traceroute.**
- **Ctrl-C :** permet d'abandonner la commande actuelle et de quitter le mode de configuration.

Commandes d'analyse d'IOS



Les commandes IOS **show** peuvent fournir des informations sur la configuration, l'utilisation et l'état des pièces d'un commutateur ou d'un routeur Cisco.

2.2 Notions de base

Configuration des noms d'hôte

Configurer un nom d'hôte

Configurez le nom d'hôte du commutateur en « Sw-Floor-1 ».

```
Switch# configure terminal
Enter configuration commands, one per line. Terminez par CNTL/Z.
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

You successfully configured the switch hostname.

Sécurisation de l'accès aux périphériques

Caractéristiques des mots de passe présentés ici :

- **Enable password :** limite l'accès au mode d'exécution privilégié.
- **Enable secret :** mot de passe chiffré – limite l'accès au mode d'exécution privilégié.
- **Mot de passe de console :** limite l'accès aux périphériques par une connexion console.
- **Mot de passe VTY :** limite l'accès aux périphériques via Telnet.

Remarque : dans la plupart des travaux pratiques de ce cours, nous utiliserons des mots de passe simples tels **que Cisco** ou **classe**.

Sécurisation de l'accès au mode d'exécution privilégié

- Utilisez la commande **enable secret**, et **non** l'ancienne commande enable password.
- **enable secret** offre davantage de sécurité, puisque le mot de passe est chiffré.

```
Sw-Floor-1>enable
Sw-Floor-1#
Sw-Floor-1#conf terminal
Sw-Floor-1(config)#enable secret class
Sw-Floor-1(config)#exit
Sw-Floor-1#
Sw-Floor-1#disable
Sw-Floor-1>enable
Password:
Sw-Floor-1#
```

Sécurisation de l'accès au mode d'exécution utilisateur

```
Sw-Floor-1(config)#line console 0
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#exit
Sw-Floor-1(config)#
Sw-Floor-1(config)#line vty 0 15
Sw-Floor-1(config-line)#password cisco
Sw-Floor-1(config-line)#login
Sw-Floor-1(config-line)#
```

- Le port de console doit être sécurisé
  - Ainsi, il y aura moins de risques que des personnes non autorisées branchent un câble sur l'appareil pour y accéder.

- Les lignes vty permettent d'accéder à un périphérique Cisco via Telnet
  - Le nombre de lignes vty prises en charge varie selon le type de périphérique et la version de l'IOS.

Chiffrement de l'affichage des mots de passe

Configuration du chiffrement des mots de passe

Entrez la commande permettant de chiffrer les mots de passe en clair.

```
Switch(config)# service password-encryption
```

Quitter le mode de configuration globale et afficher la configuration en cours.

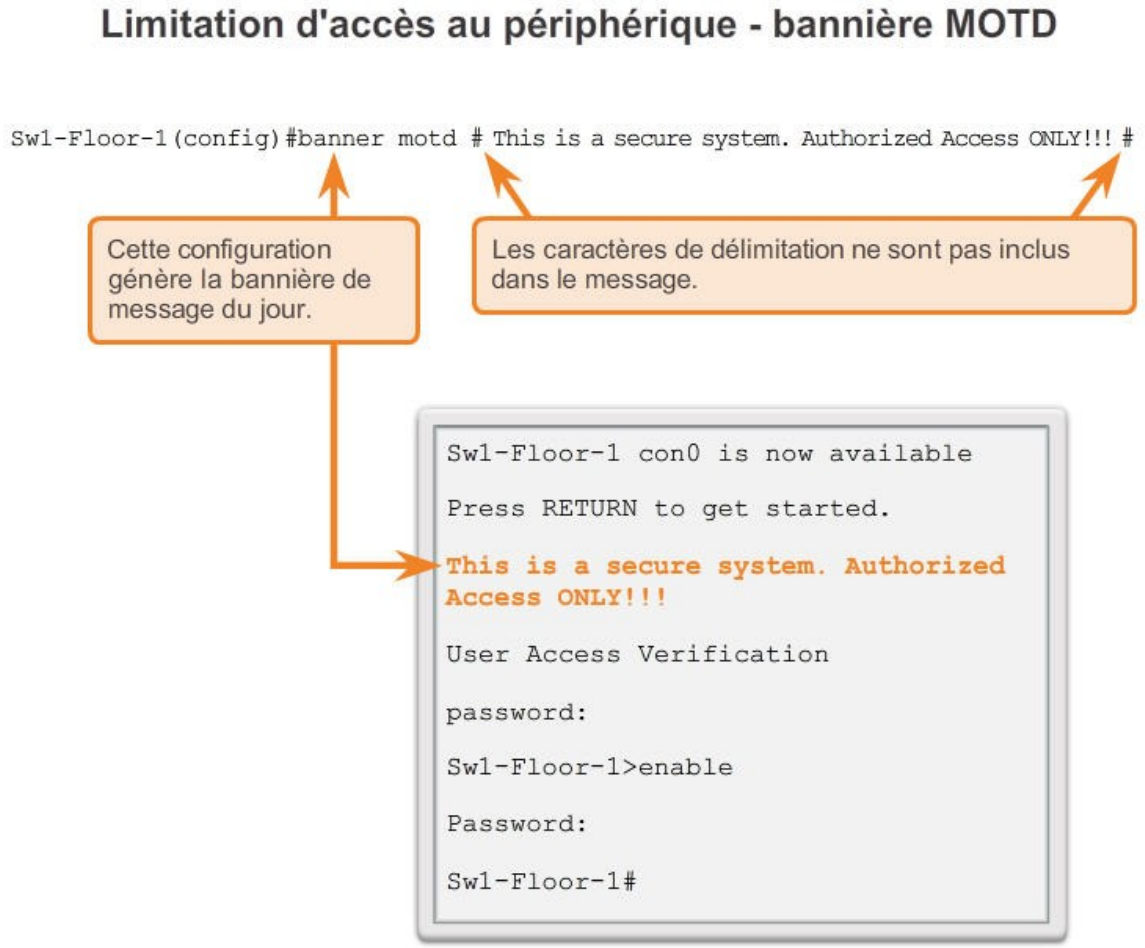
```
Switch(config)# exit

Switch# show running-config
 !
<résultat omis>
 !
line con 0
 password 7 094F471A1A0A
 login
 !
line vty 0 4
 password 7 03095A0F034F38435B49150A1819
 login
 !
 !
end
```

Le service de chiffrement des mots de passe :

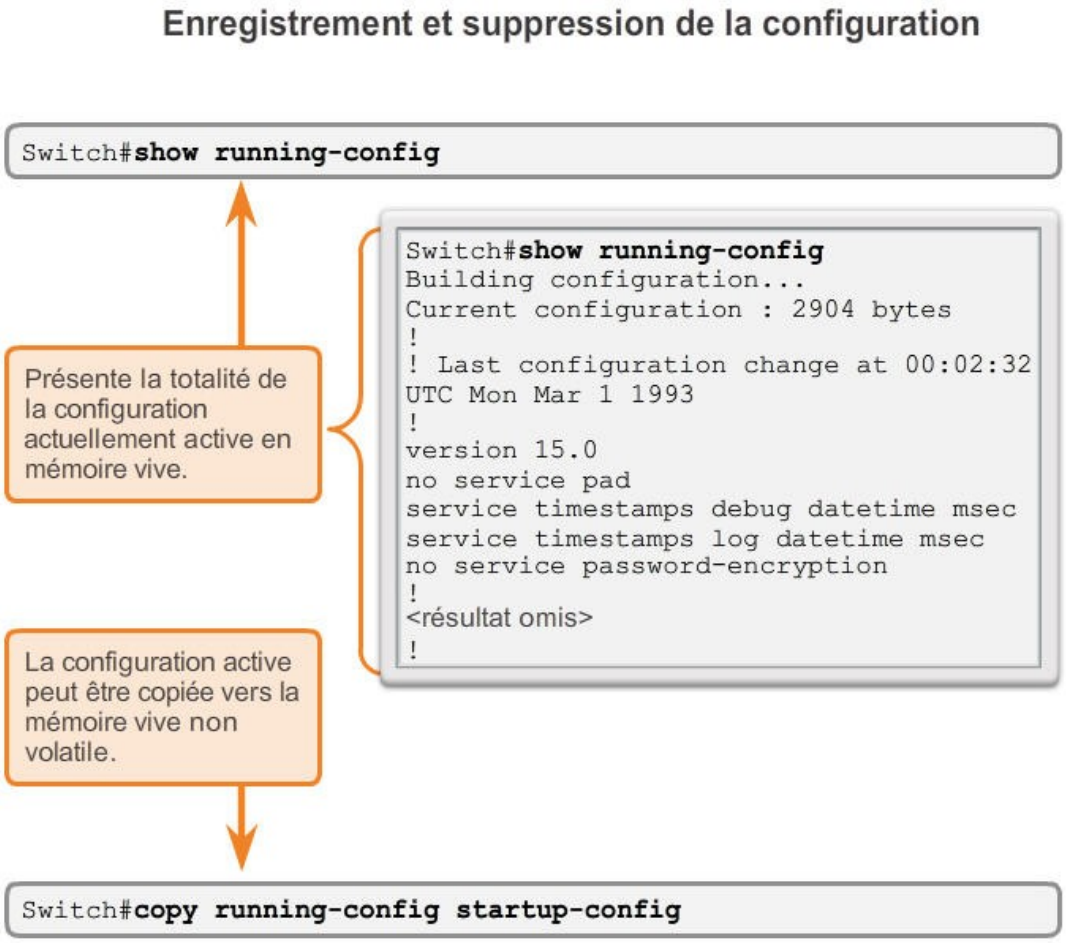
- Empêche que les mots de passe soient indiqués en clair dans les informations de configuration
- Cette commande a pour but d'empêcher les personnes non autorisées de lire les mots de passe dans le fichier de configuration.
- L'annulation du service de chiffrement ne supprime pas ce chiffrement.

Messages de bannière

- Élément important en cas de poursuite contre une personne ayant accédé sans autorisation à un périphérique
- Suggérer que l'utilisateur qui se connecte est « bienvenu » ou « invité à se connecter » est une mauvaise idée
- Ce message s'utilise souvent comme mention légale, parce qu'il apparaît sur tous les terminaux connectés



Fichiers de configuration



- Switch# **reload**

  System configuration has been modified. Save? [yes/no]: **n**

  Proceed with reload? [confirm]

- La commande **erase startup-config** permet de supprimer la configuration initiale.

  Switch# **erase startup-config**

- Sur un commutateur, vous devez également utiliser **delete vlan.dat**

  Switch# **delete vlan.dat**

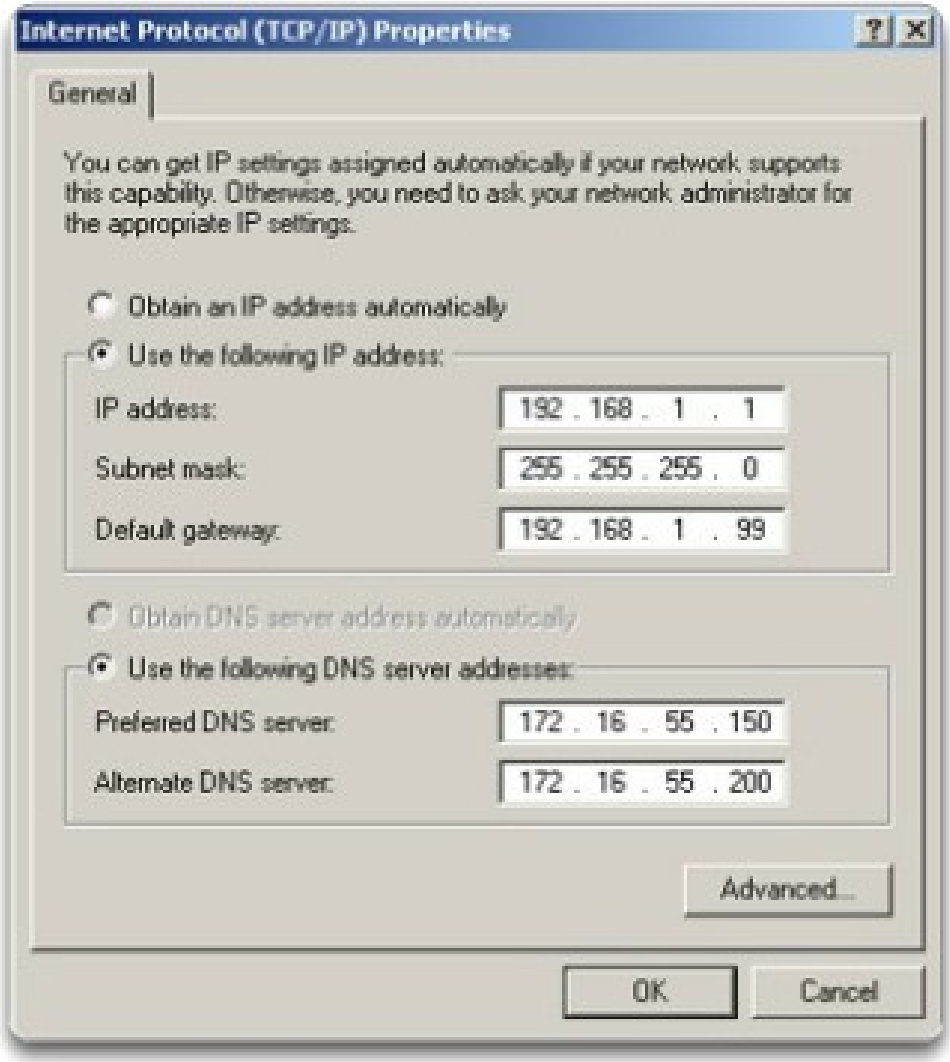
  Delete filename [vlan.dat]?

  Delete flash:vlan.dat? [confirm]

2.3 Schémas d'adressage

Généralités sur l'adressage IP

- Chaque périphérique final d'un réseau doit avoir une adresse IP.
- La structure d'une adresse IPv4 est appelée *notation décimale à point.*
- L'adresse IP est affichée en notation décimale, avec quatre nombres décimaux compris entre 0 et 255.
- Avec l'adresse IP, il faut aussi un masque de sous-réseau.
- Les adresses IP peuvent être attribuées à la fois aux ports physiques et aux interfaces virtuelles des périphériques.



Interfaces et ports

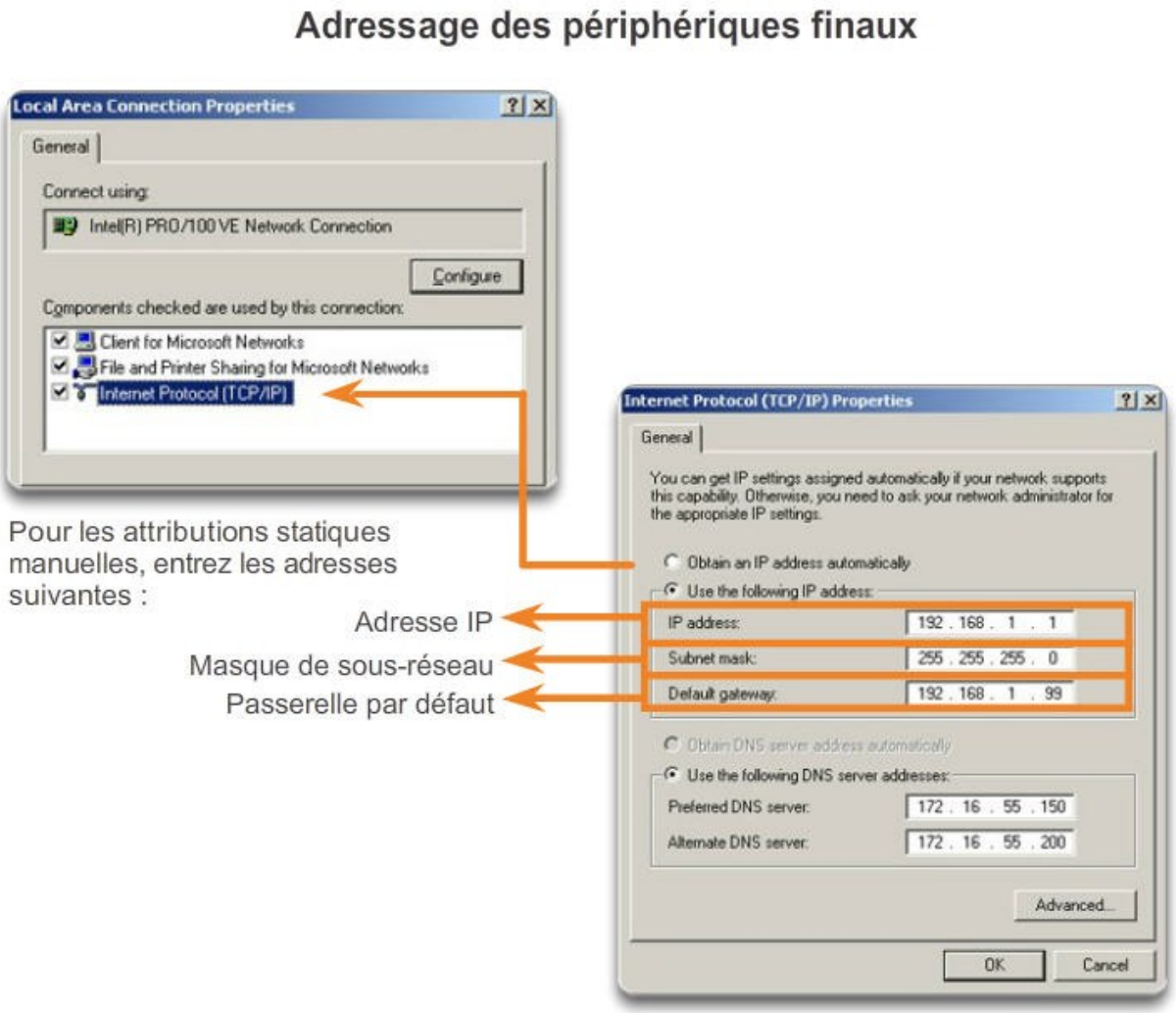
- Ethernet est la technologie de réseau local (LAN) la plus répandue aujourd'hui.
- Les ports Ethernet sont fournis sur les périphériques des utilisateurs, les commutateurs et autres périphériques réseau.
- Les commutateurs Cisco IOS sont équipés de ports physiques pour la connexion, mais intègrent également une ou plusieurs interfaces virtuelles de commutateur (SVI). Autrement dit, il n'y a aucun composant matériel, cette fonctionnalité étant gérée par logiciel.
- L'interface virtuelle de commutateur permet de gérer à distance le commutateur sur un réseau.

Configuration d'une interface virtuelle de commutateur

```
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#interface VLAN 1
Switch(config-if)#ip address 192.168.10.2 255.255.255.0
Switch(config-if)#no shutdown
```

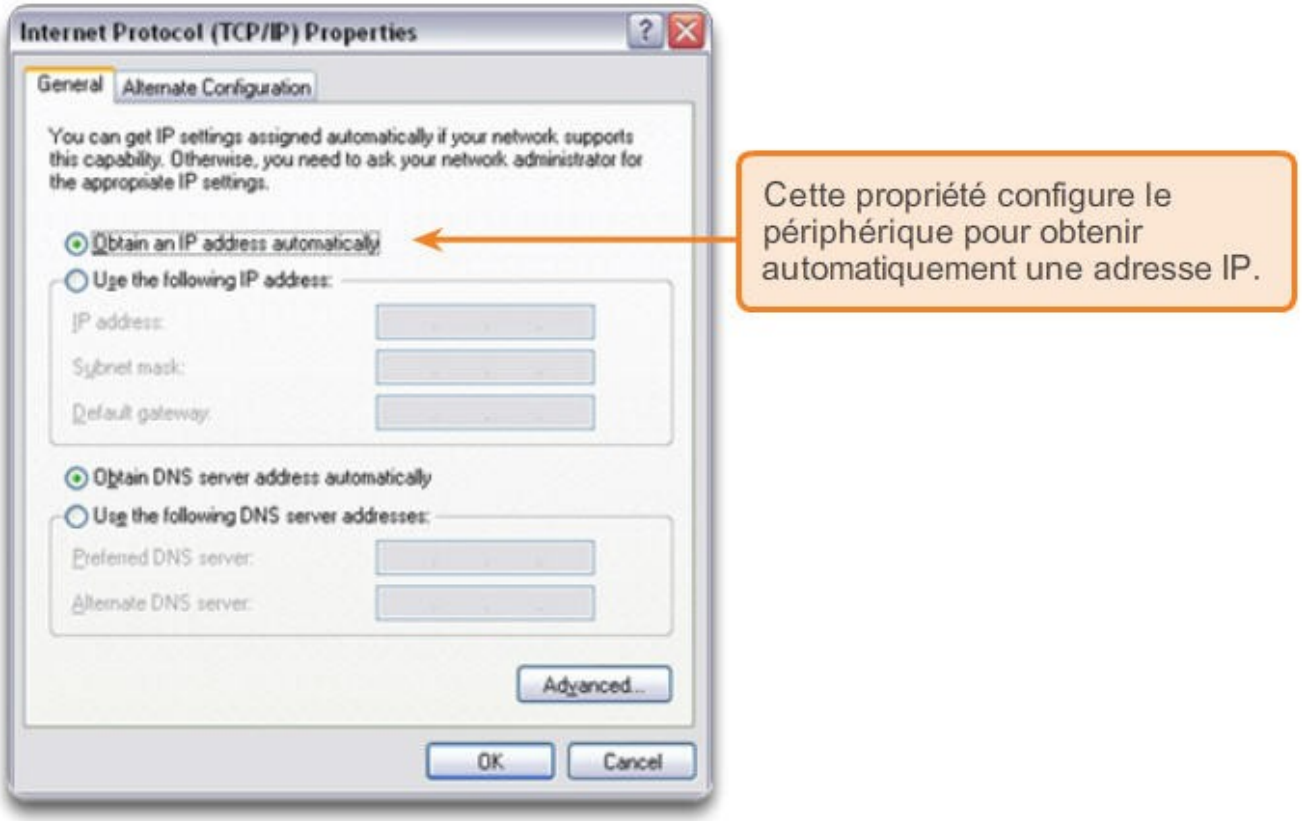
- **Adresse IP :** combinée au masque de sous-réseau, elle identifie de manière unique le périphérique final sur l'interréseau.
- **Masque de sous-réseau :** détermine quelle partie d'un réseau plus vaste est utilisée par une adresse IP.
- **interface VLAN 1 :** mode de configuration d'interface
- **ip address 192.168.10.2 255.255.255.0 :** configure l'adresse IP et le masque de sous-réseau du commutateur.
- **no shutdown :** active l'interface.
- Le commutateur doit toutefois avoir des ports physiques configurés et des lignes VTY pour que la gestion à distance soit possible.

Configuration manuelle des adresses IP des périphériques finaux



Configuration automatique des adresses IP des périphériques finaux

Affectation d'adresses dynamiques

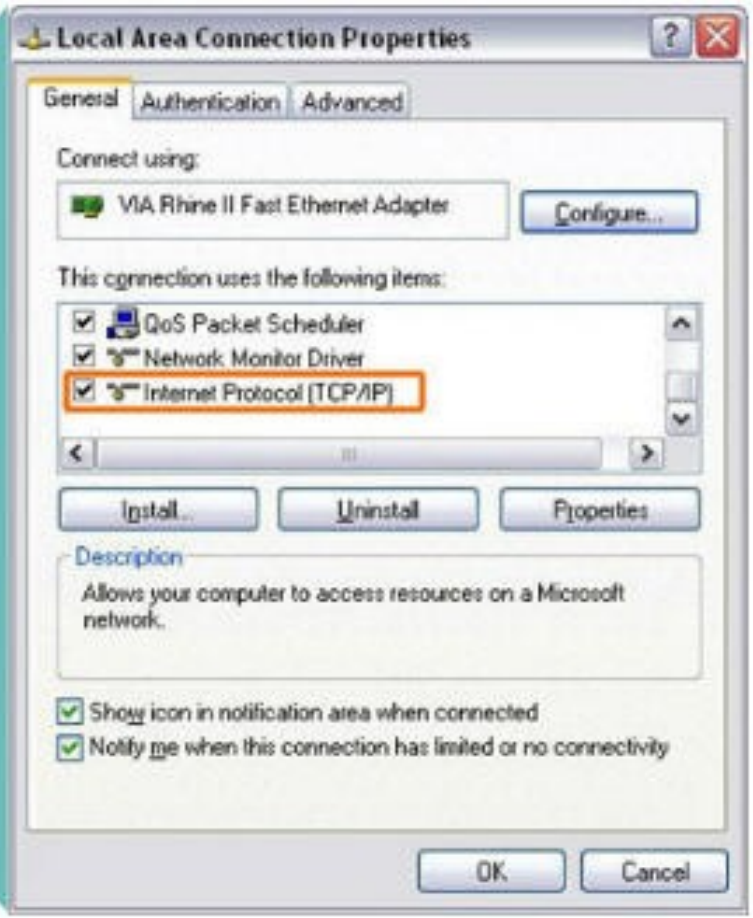


Test de l'adresse de bouclage sur un périphérique final

Test de la pile TCP/IP locale

L'envoi d'une requête ping à l'hôte local confirme que la suite de protocoles TCP/IP est installée et fonctionne sur la carte réseau locale.

Envoyer une requête ping à l'adresse 127.0.0.1 revient à ce que le périphérique s'envoie la requête ping à lui-même.



Test de l'affectation des interfaces

```
S1#show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
FastEthernet0/1        unassigned      YES manual  up        up
FastEthernet0/2        unassigned      YES manual  up        up

<output omitted>


Vlan1                  192.168.10.2    YES manual  up        up
```

```
S2#show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
FastEthernet0/1        unassigned      YES manual  up        up
FastEthernet0/2        unassigned      YES manual  up        up

<output omitted>


Vlan1                  192.168.10.3    YES manual  up        up
```

Test de la connectivité de bout en bout

```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:
Reply from 192.168.10.2: bytes=32 time=838ms TTL=35
Reply from 192.168.10.2: bytes=32 time=820ms TTL=35
Reply from 192.168.10.2: bytes=32 time=883ms TTL=36
Reply from 192.168.10.2: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=838ms TTL=35
Reply from 192.168.10.11: bytes=32 time=820ms TTL=35
Reply from 192.168.10.11: bytes=32 time=883ms TTL=36
Reply from 192.168.10.11: bytes=32 time=828ms TTL=36

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 820ms, Maximum = 883ms, Average = 842ms

C:\>
```

Résumé

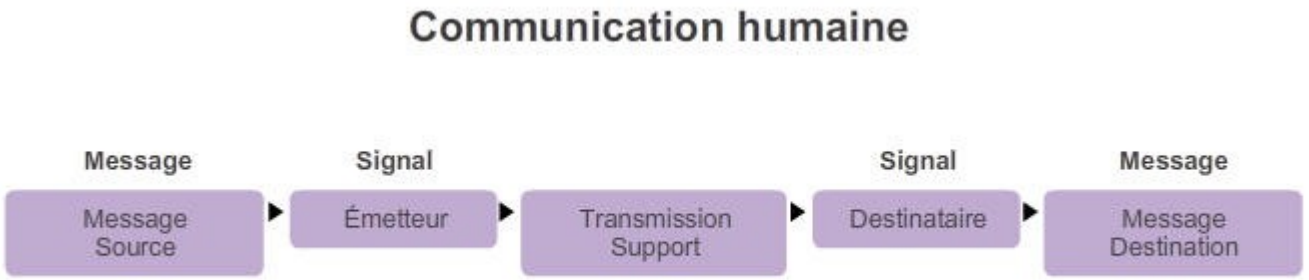
- Expliquer les caractéristiques et les fonctions du logiciel Cisco IOS
- Configurez les paramètres initiaux d'un périphérique réseau avec le logiciel Cisco IOS
- À partir d'un schéma d'adressage IP, configurer les paramètres d'adresse IP sur les périphériques pour assurer la connectivité de bout en bout d'un réseau de PME.

Module 3 :
Modèles et protocoles

Initiation aux réseaux

Cisco | Networking Academy®
Mind Wide Open™

Qu'est-ce que la communication ?



Détermination des règles

Détermination des règles

- Expéditeur et destinataire identifiés
- Accord sur le mode de communication (face-à-face, téléphone, lettre, photographie)
- Même langue et syntaxe
- Vitesse et rythme d'élocution
- Demande de confirmation ou d'accusé de réception

Mise en forme et encapsulation des messages

Exemple – Une lettre personnelle comprend les éléments suivants :

- Le nom du destinataire
- Une formule de politesse
- Le contenu du message
- Une phrase de conclusion
- Le nom de l'expéditeur

Taille des messages

En raison des restrictions imposées pour la taille des trames, l'hôte source doit décomposer les messages longs en portions répondant aux impératifs de taille minimale et maximale.

C'est ce que l'on appelle la segmentation.

Chaque portion est encapsulée dans une trame distincte avec les informations d'adresse, puis transmise sur le réseau.

Au niveau de l'hôte destinataire, les messages sont désencapsulés et recomposés pour être traités et interprétés.

Synchronisation des messages

- Méthode d'accès
- Contrôle de flux
- Délai d'attente de la réponse

Règles qui régissent les communications

Protocoles : règles qui régissent les communications

Couche contenu

Où est le café ?

Suite des protocoles de conversation
1. Utiliser une langue commune
2. Attendre son tour
3. Signaler la fin du message

Couche règles

Les suites de protocoles sont des ensembles de règles qui fonctionnent conjointement en vue de résoudre un problème.

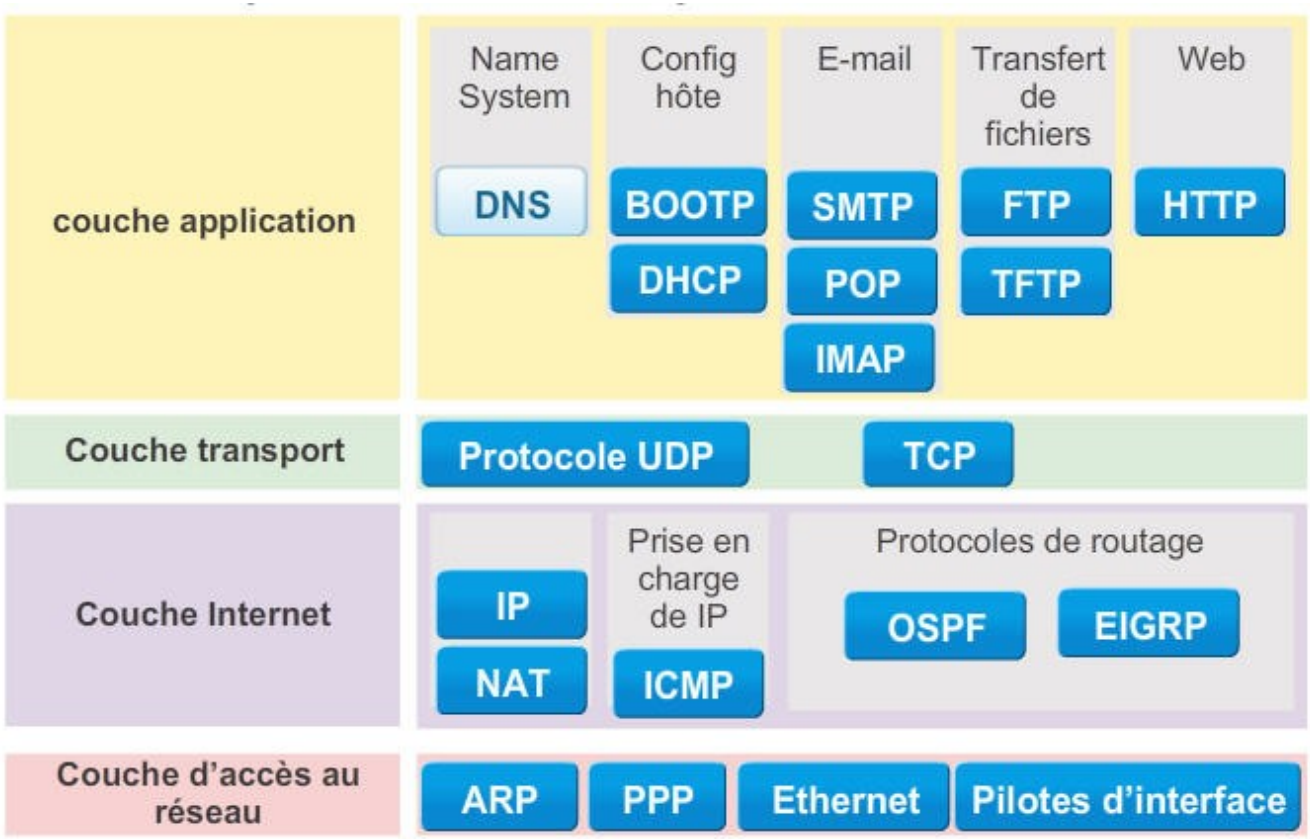
Protocoles réseau

- Format ou structure du message
- La méthode selon laquelle les périphériques réseau partagent des informations à propos des chemins avec d'autres réseaux
- Le mode et le moment de transmission de messages d'erreur et de messages systèmes entre les périphériques
- L'établissement et la fin des sessions de transfert de données

Suites de protocoles et normes de l'industrie

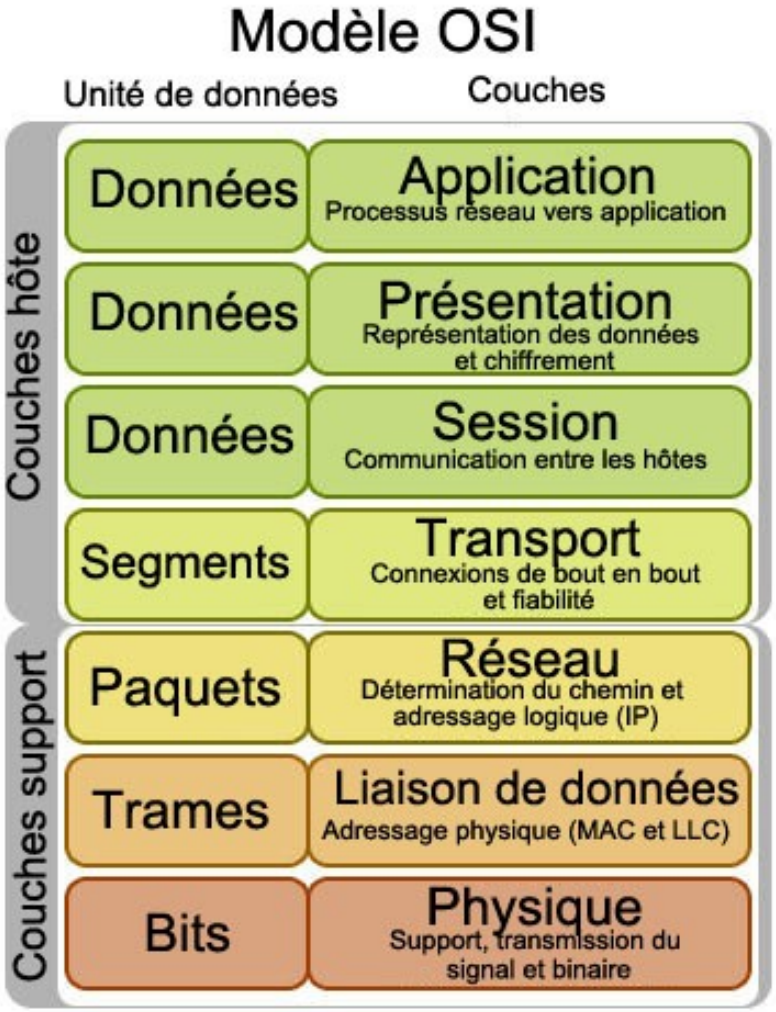
	TCP/IP	ISO	AppleTalk	Novell Netware
7 6 5	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
4	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
3	IPV4 IPV6 ICMPV4 ICMPV6	CONP/CMNS CLNP/CLNS	AFP	IPX
2 1	Ethernet PPP Frame Relay ATM WLAN			

Suite de protocoles TCP/IP et processus de communication

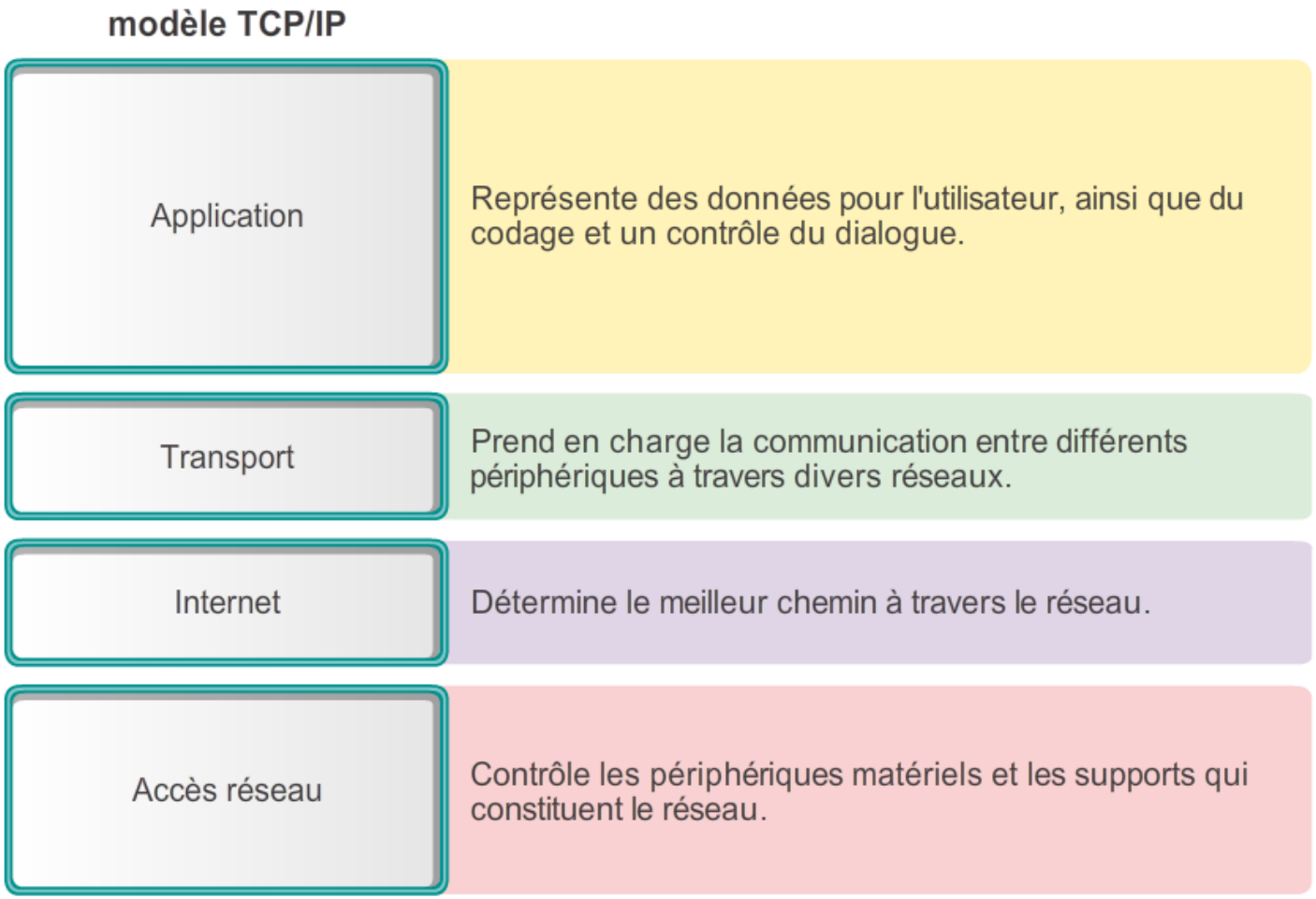


Organismes de normalisation

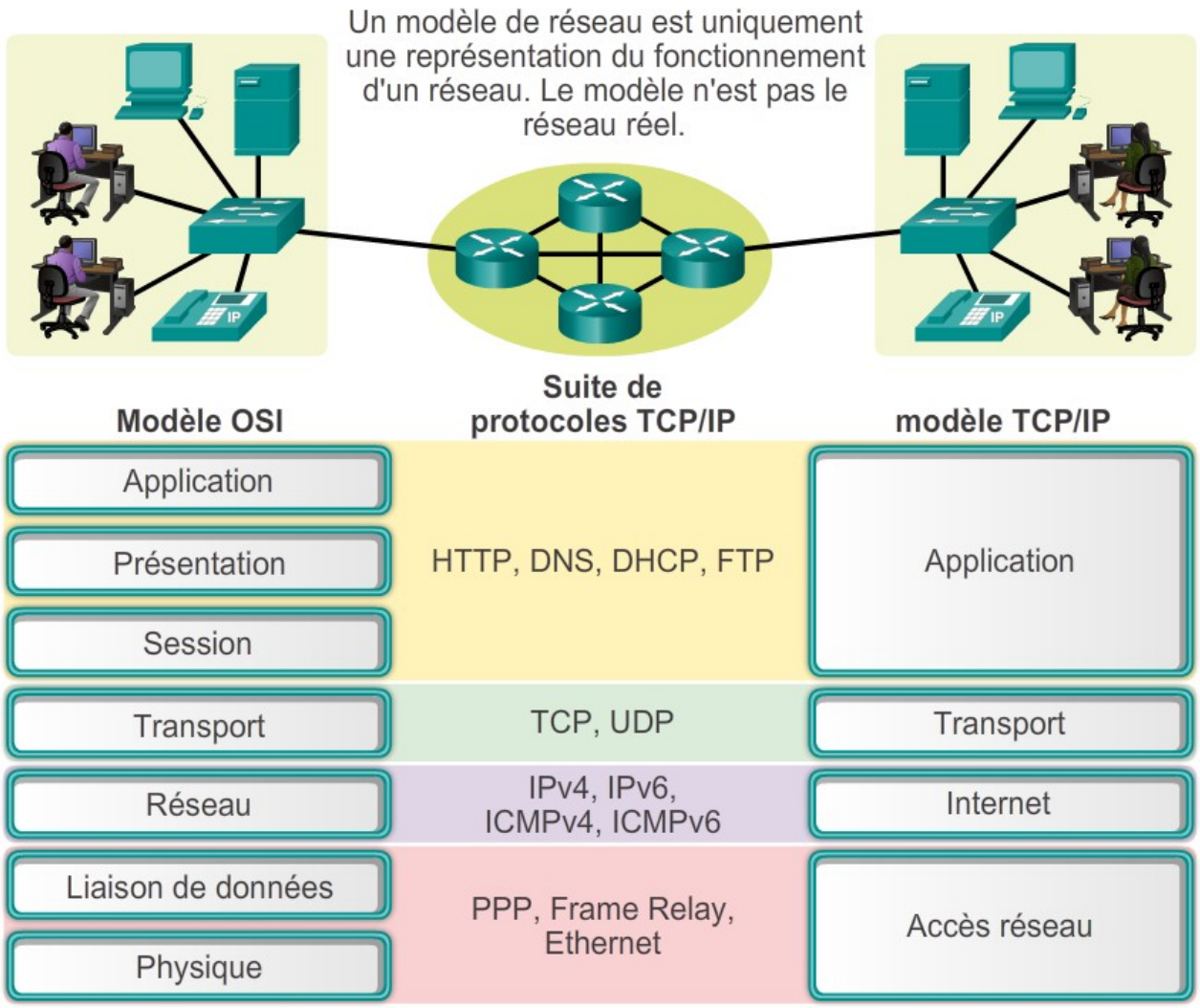
Le modèle de référence OSI



Le modèle de référence TCP/IP

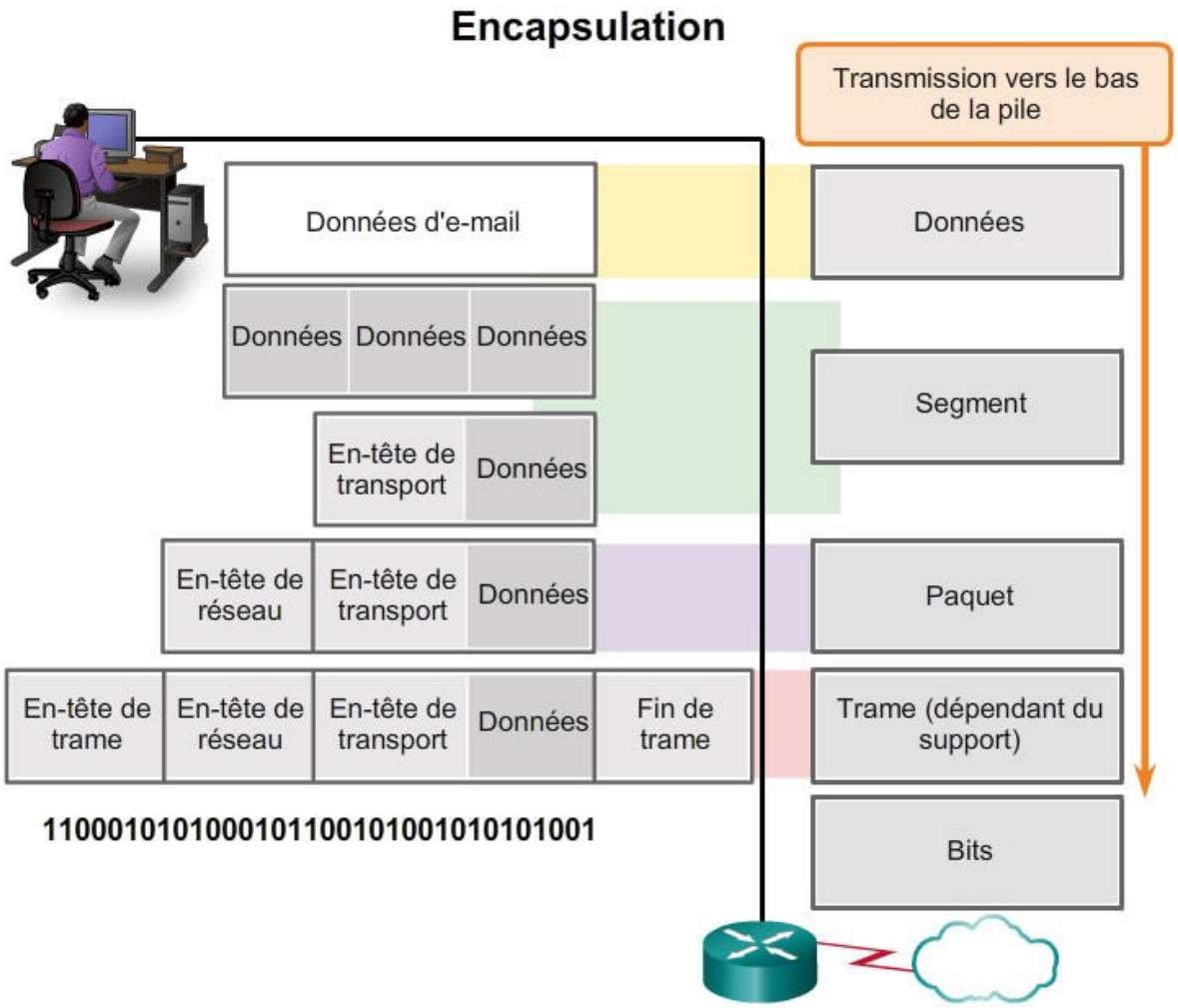


Comparaison des modèles OSI et TCP/IP

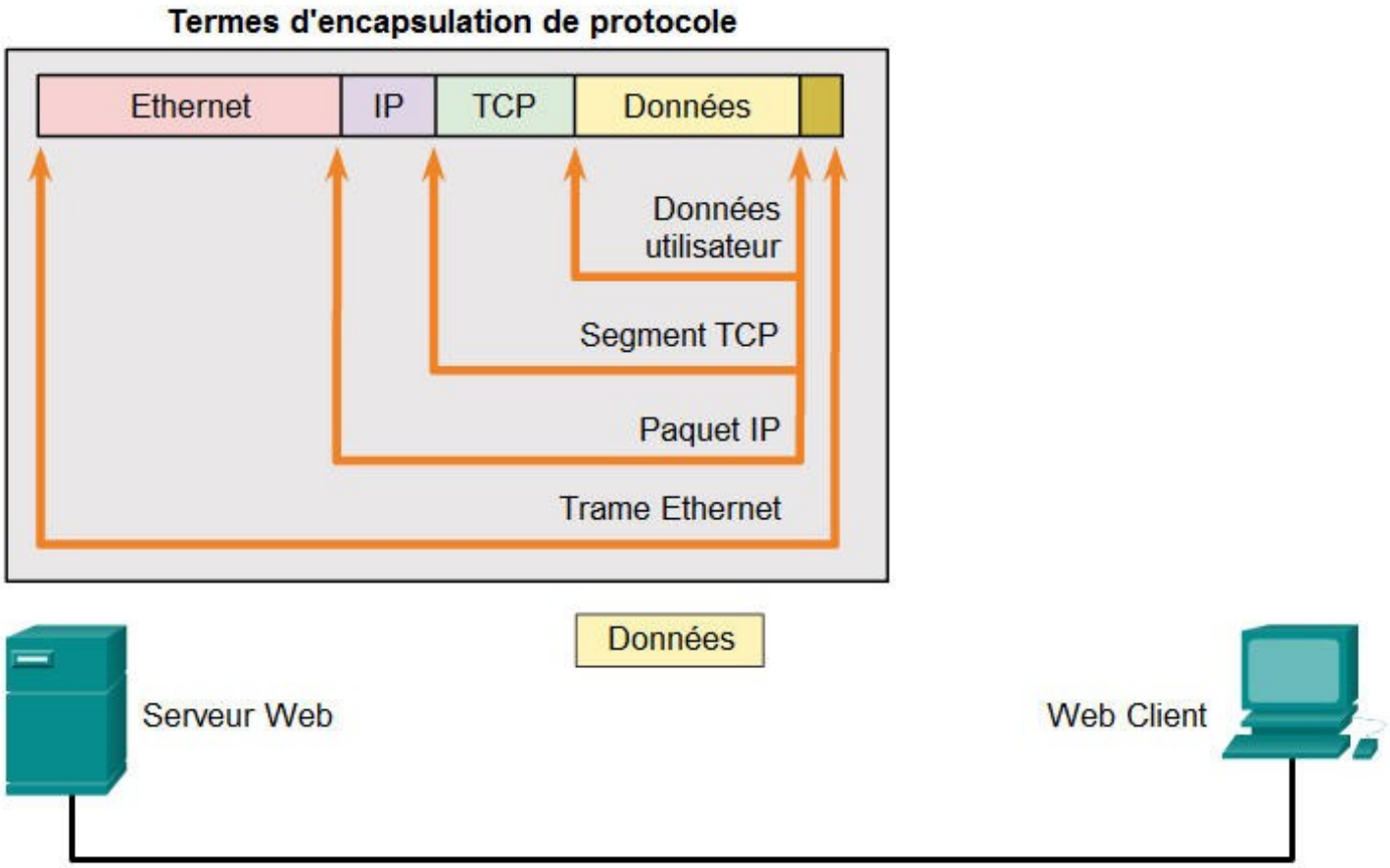


Unités de données de protocole (PDU)

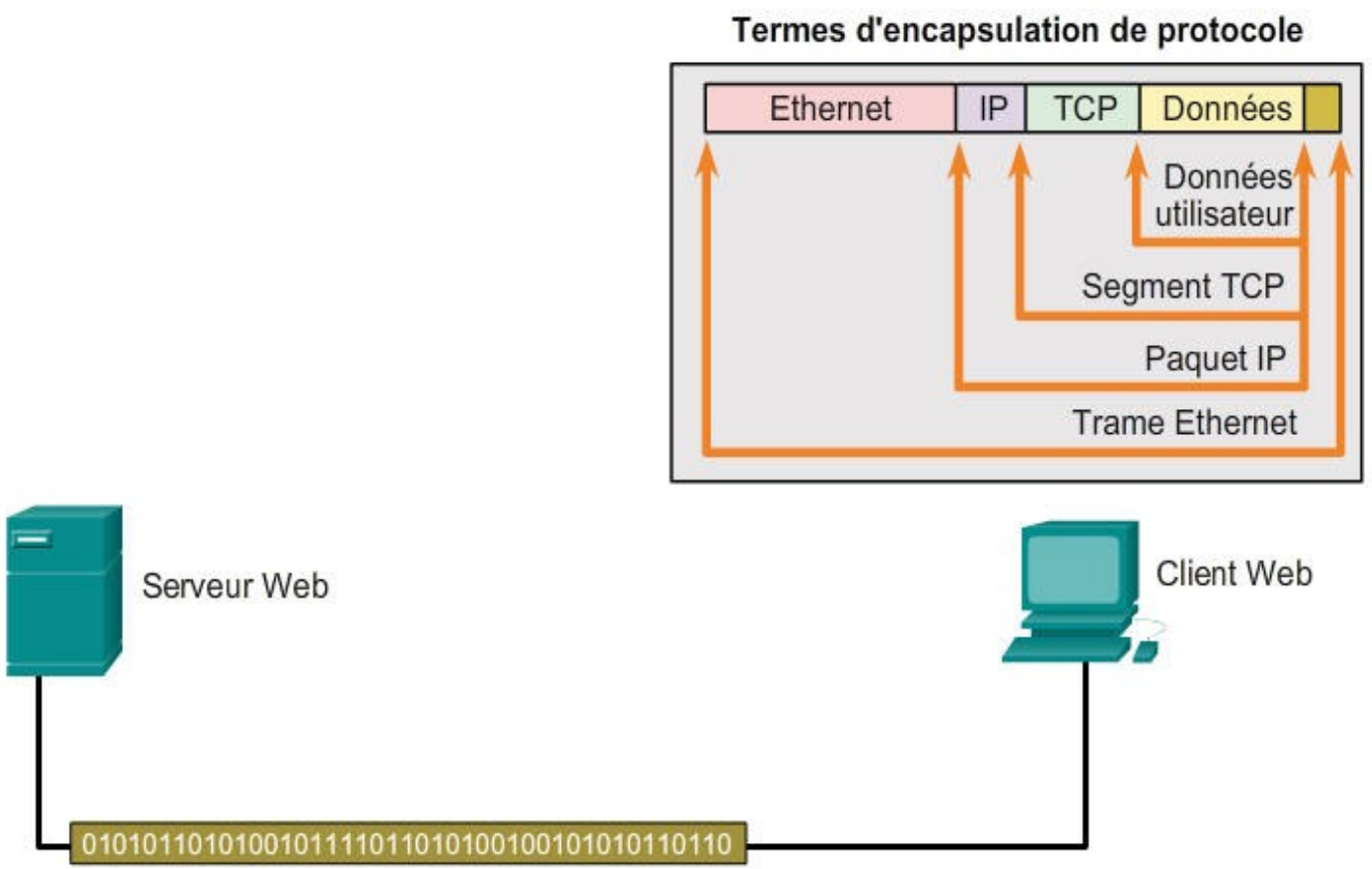
- Données
- Segment
- Paquet
- Trame
- Bits



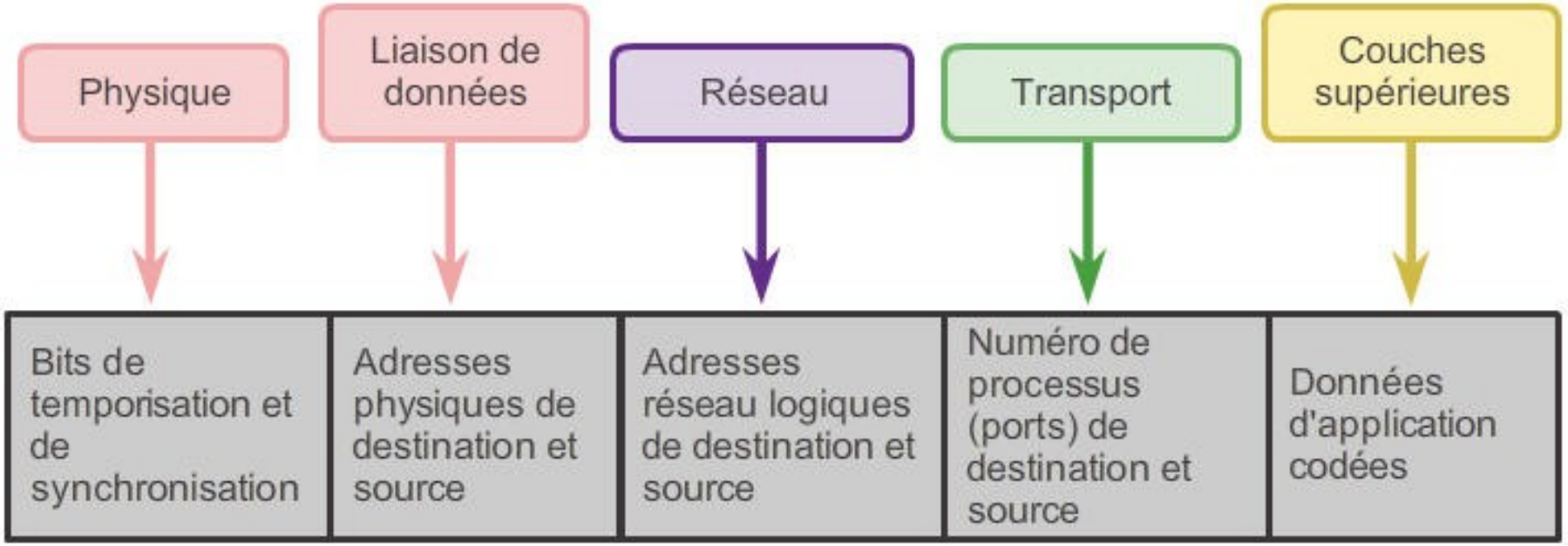
Encapsulation



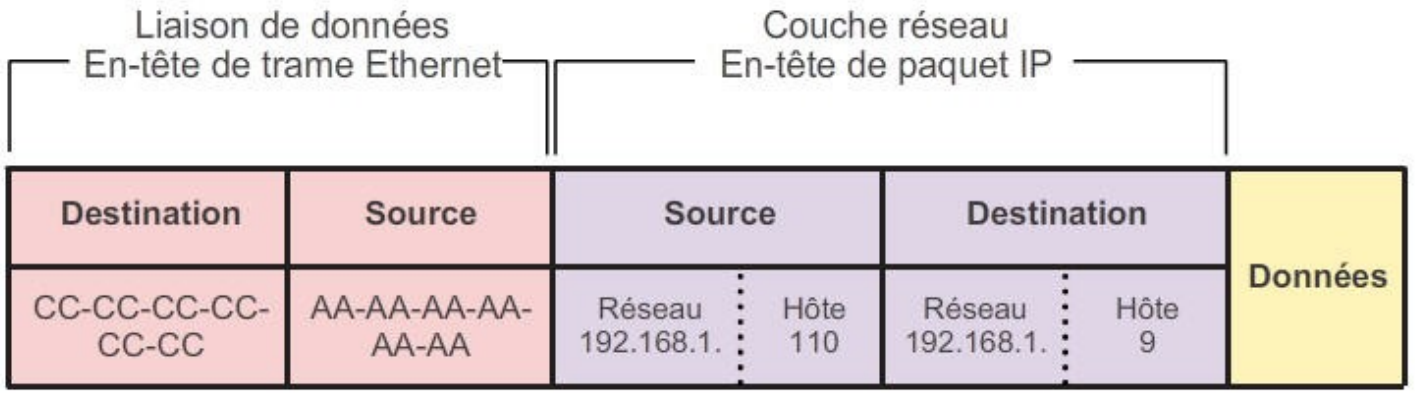
Désencapsulation



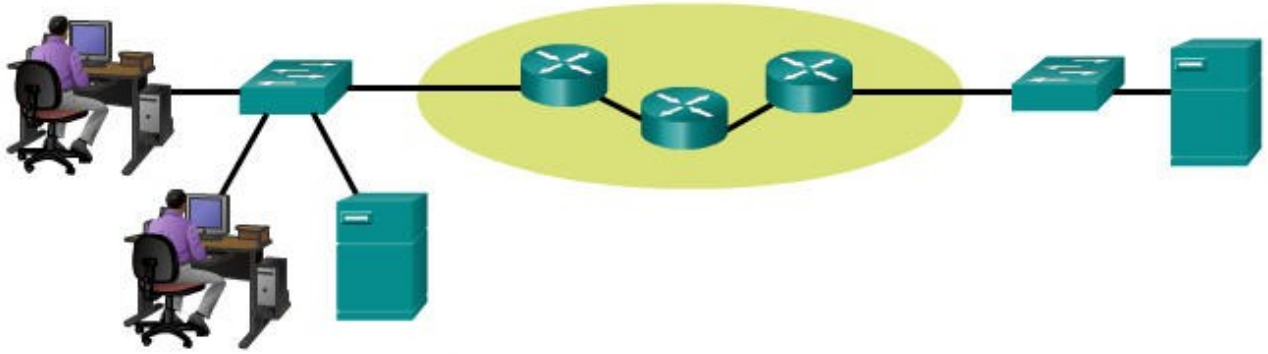
Accès aux ressources locales



Communication avec un périphérique sur le même réseau

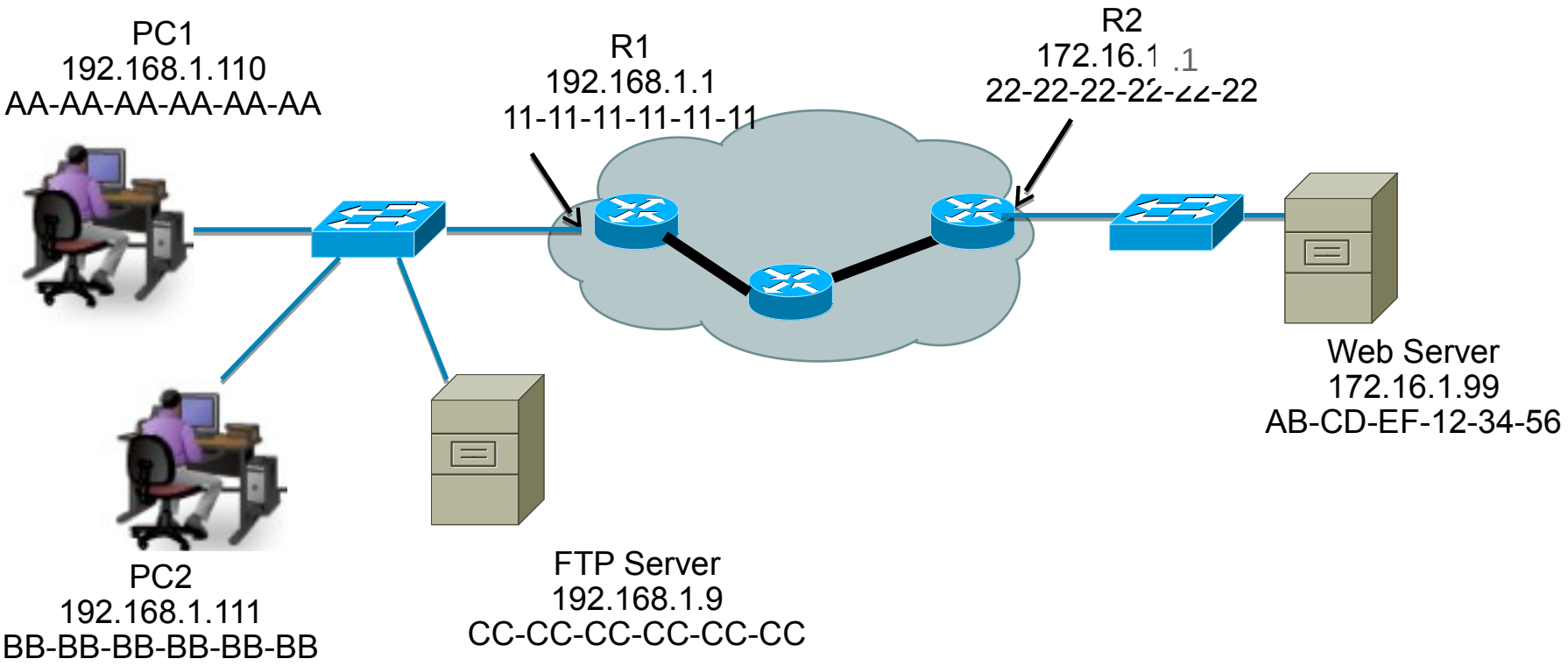


PC1
192.168.1.110
AA-AA-AA-AA-AA-AA



Serveur FTP
192.168.1.9
CC-CC-CC-CC-CC-CC

Passerelle par défaut



Communication avec un périphérique sur un réseau distant

Liaison de données
En-tête de trame Ethernet

Couche réseau
En-tête de paquet IP

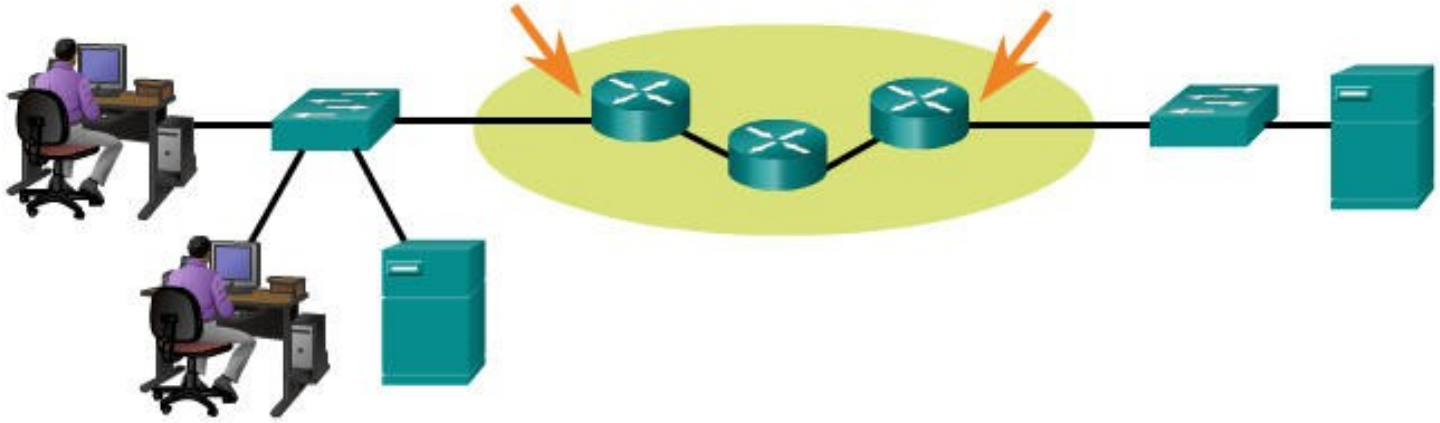
Destination	Source	Source		Destination		Données
11-11-11-11-11-11	AA-AA-AA-AA-AA-AA	Réseau 192.168.1.	Périphérique 110	Réseau 172.16.1.	Périphérique 99	

PC1
192.168.1.110
AA-AA-AA-AA-AA-AA

R1
192.168.1.1
11-11-11-11-11-11

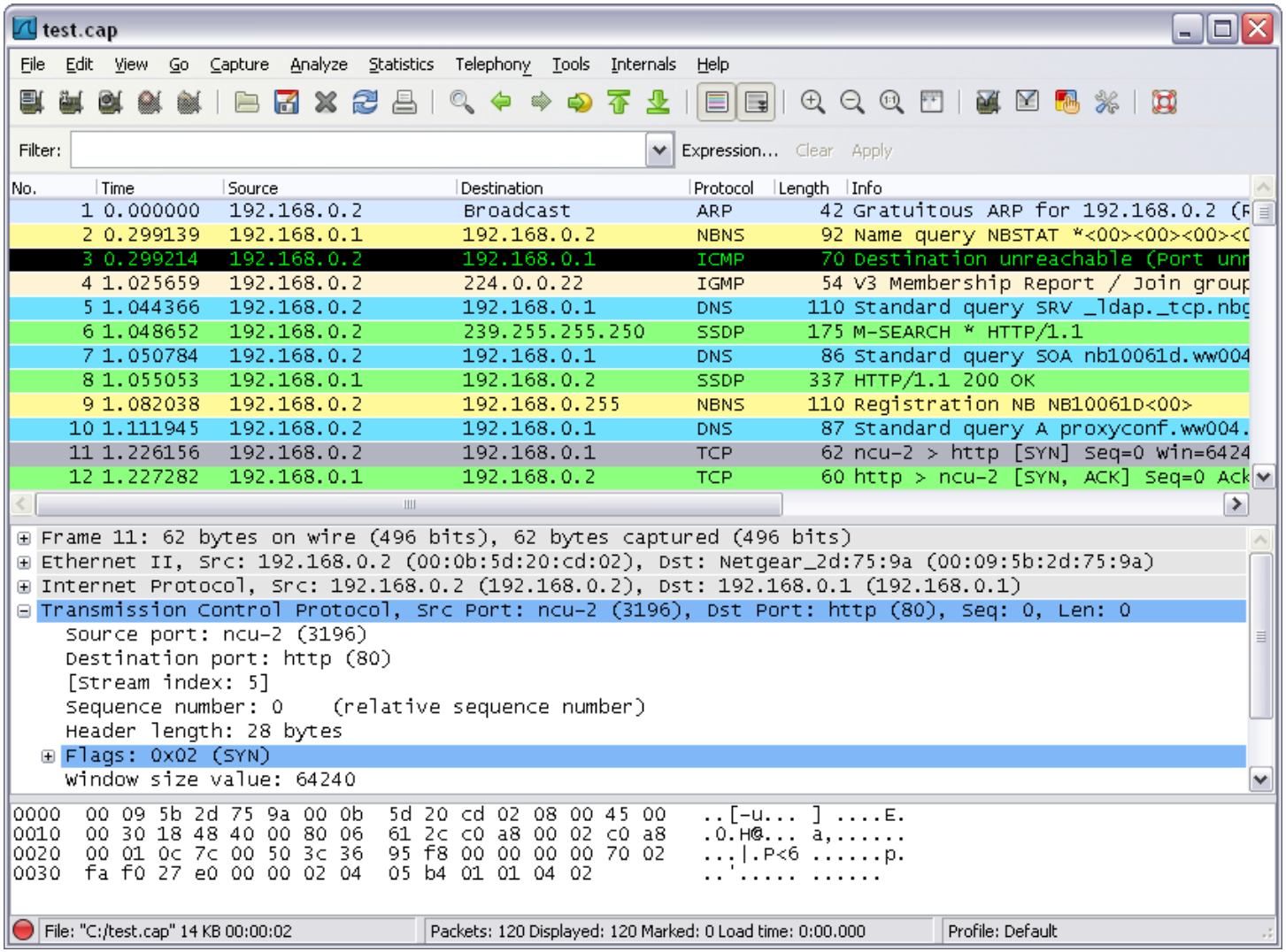
R2
172.16.1 .1
22-22-22-22-22-22

Serveur Web
172.16.1.99
AB-CD-EF-12-34-56



Accès aux ressources distantes

Utilisation de Wireshark pour voir le trafic réseau



Résumé

- Expliquer comment les règles sont utilisées pour faciliter la communication
- Expliquer le rôle des protocoles et des organismes de normalisation en tant que facilitateurs de l'interopérabilité des communications réseau
- Expliquer comment les périphériques d'un réseau local accèdent aux ressources dans un réseau de PME