



Cours Réseaux IP 2 :

Commutation & Routage

- Partie I -

Plan

- Couche transport (protocoles TCP et UDP)
- Couche Application
- Configuration de base d'un routeur
- Réseaux commutés
- Concepts de routage (statique, dynamiques)
- Protocoles de Routage dynamique (RIP, OSPF, ..)

La couche transport: TCP & UDP



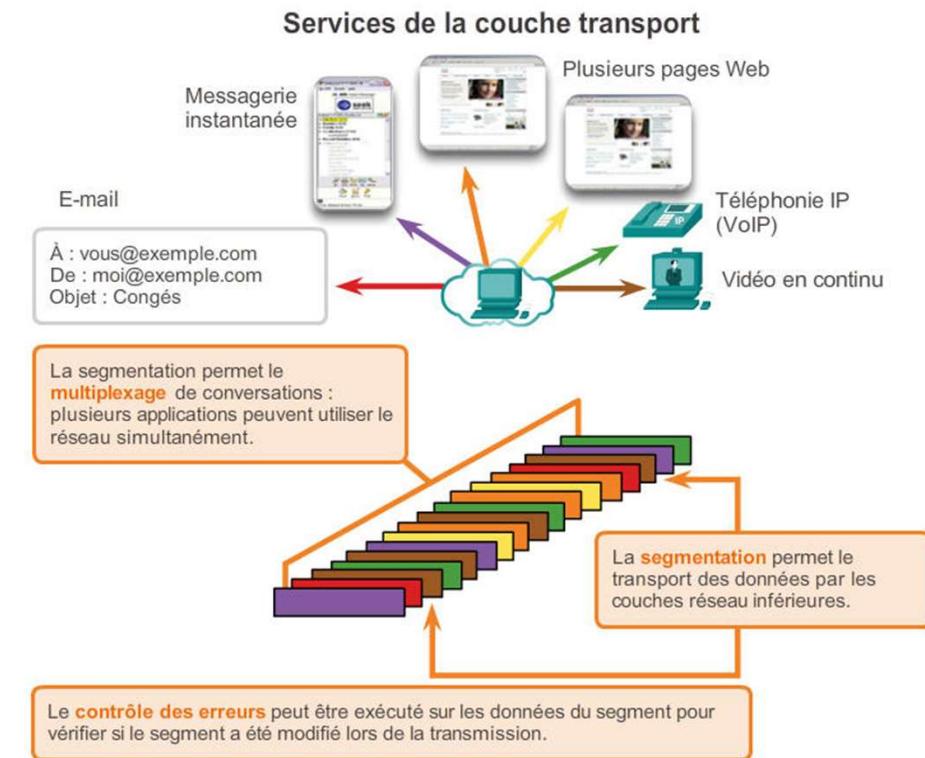
Rôle de la couche transport

- ✓ Le rôle de la **couche transport** est d'établir une session de communication temporaire entre deux applications pour acheminer les données entre elles.
- ✓ TCP/IP utilise deux protocoles pour cela :
 - TCP (Transmission Control Protocol)
 - UDP (User Datagram Protocol)
- ✓ Fonctions principales des protocoles de la couche transport :
 - Suivre les communications individuelles entre les applications résidant sur les hôtes source et de destination
 - Segmenter les données pour faciliter la gestion et réassembler les données segmentées en flux de données d'application vers la destination
 - Identifier l'application appropriée pour chaque flux de communication

Fonctions de la couche transport

La segmentation des données

- Permet de **multiplexer** sur le même réseau différentes communications provenant de nombreux utilisateurs.
- Permet d'envoyer et de recevoir des données tout en exécutant plusieurs applications.
- Un en-tête est ajouté à chaque segment **pour l'identifier**.
- La segmentation facilite la reprise sur erreur et la retransmission des données endommagées.



Fiabilité de la couche transport

- ✓ La couche transport est également responsable de la gestion des exigences de fiabilité d'une conversation
- ✓ Toutes les applications n'ont pas besoin du même degré de fiabilité.
- ✓ TCP/IP fournit deux protocoles de la couche transport, **TCP et UDP** utilisés selon le besoin de l'application.

Transmission Control Protocol (TCP)

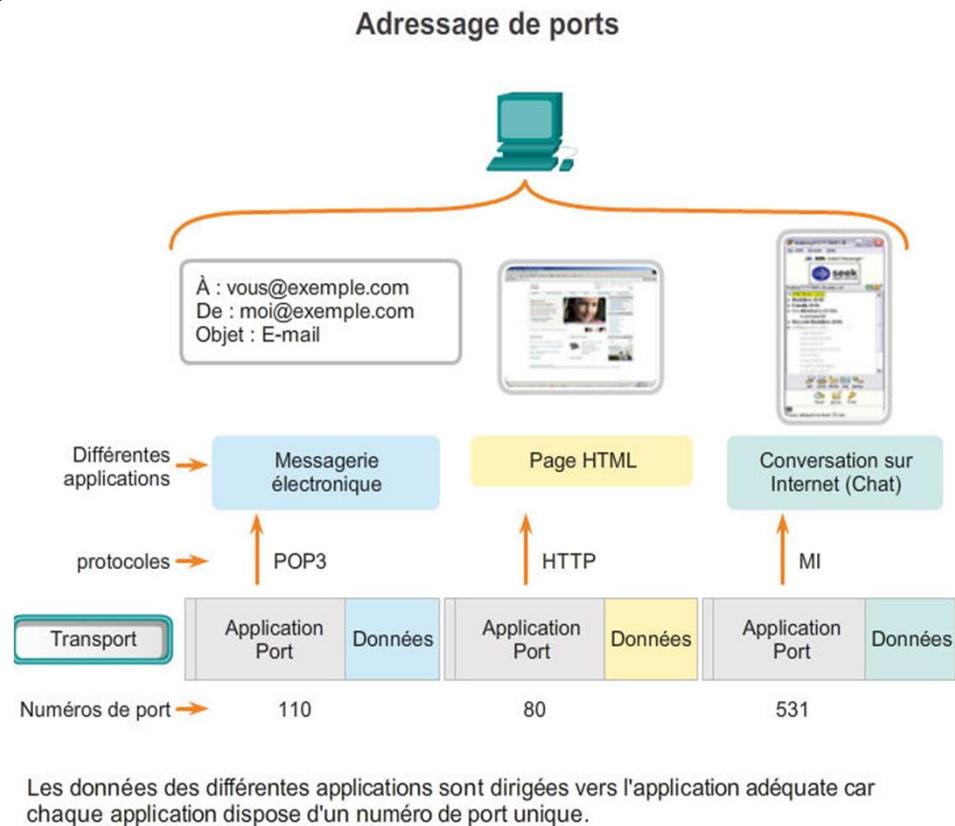
- Assure un acheminement fiable – Toutes les données arrivent à destination
- Surcharge le réseau avec les contrôles

User Datagram Protocol (UDP)

- Fournit juste les fonctions de base pour la transmission, sans aucune garantie (Moins de surcharge)

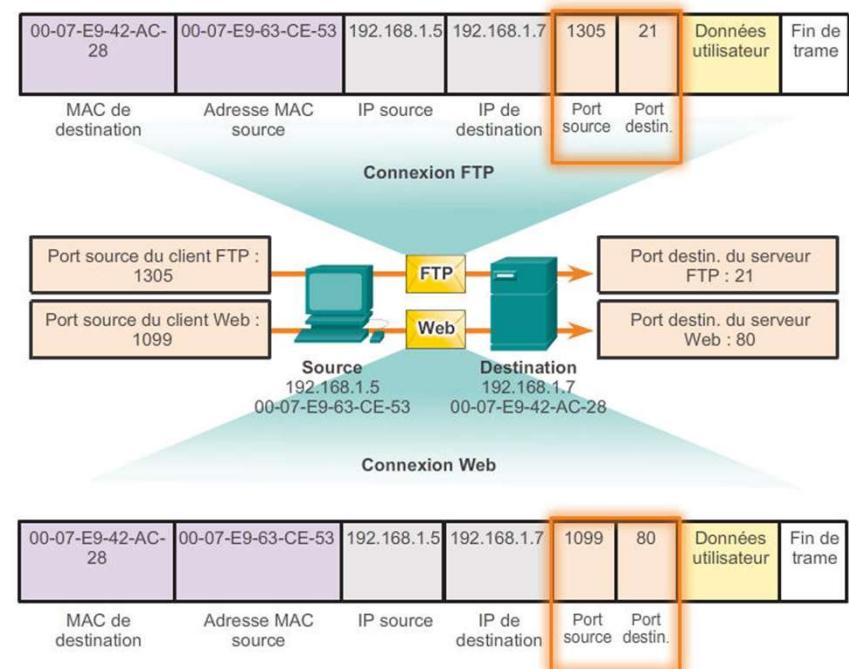
Séparation des communications multiples

- Les adresses IP désignent les machines entre lesquelles les communications sont établies.
- Sur une machine, existe plusieurs Applications.
- On a besoin d'identifier les processus applicatifs communicants
- L'adressage de ce processus (service applicatif) est effectué selon un concept abstrait: les numéros de **ports**
- Les numéros de port sont utilisés par les protocoles TCP et UDP pour différencier les applications.



Adressage de ports TCP et UDP

- Processus source et processus destination sont identifiés chacun par un numéro de port
- la combinaison du numéro de port et de l'adresse IP de l'hôte identifie de manière unique un processus d'application (socket)
- Une paire de sockets, composée des adresses IP et numéros de port source et de destination identifie d'une manière unique la conversation spécifique entre deux hôtes.



Adressage de ports TCP et UDP

Numéros de port

Plage de numéros de port	Groupe de ports
0 à 1023	Ports réservés
De 1024 à 49151	Ports inscrits
49152 à 65535	Ports dynamiques et/ou privés

- Ports réservés: numéros réservés à des services et applications connus

Ports TCP réservés :

21 FTP
23 Telnet
25 SMTP
80 HTTP
143 IMAP
194 Internet Relay Chat (IRC)
443 Secure HTTP (HTTPS)

Ports UDP réservés :

69 TFTP
520 RIP

Ports TCP/UDP réservés courants :

53 DNS
161 SNMP
531 AOL Instant Messenger, IRC

Adressage de ports TCP et UDP

- ✓ Ports Inscrits: numéros affectés à des processus ou applications particulières d'utilisateurs. Aussi utilisés par les processus client (si non affecté à un service)

Ports TCP inscrits :
1863 MSN Messenger
2000 Cisco SCCP (VoIP)
8008 Alternate HTTP
8080 Alternate HTTP

Ports UDP inscrits :
1812 RADIUS Authentication Protocol
5004 RTP (Voice and Video Transport Protocol)
5040 SIP (VoIP)

- ✓ Ports privés ou dynamiques: généralement affectés de façon dynamique à des applications clientes lorsqu'une connexion à un service est initiée par un client.

Adressage de ports TCP et UDP

Netstat Permet d'examiner les connexions TCP qui sont ouvertes et actives sur un hôte connecté au réseau

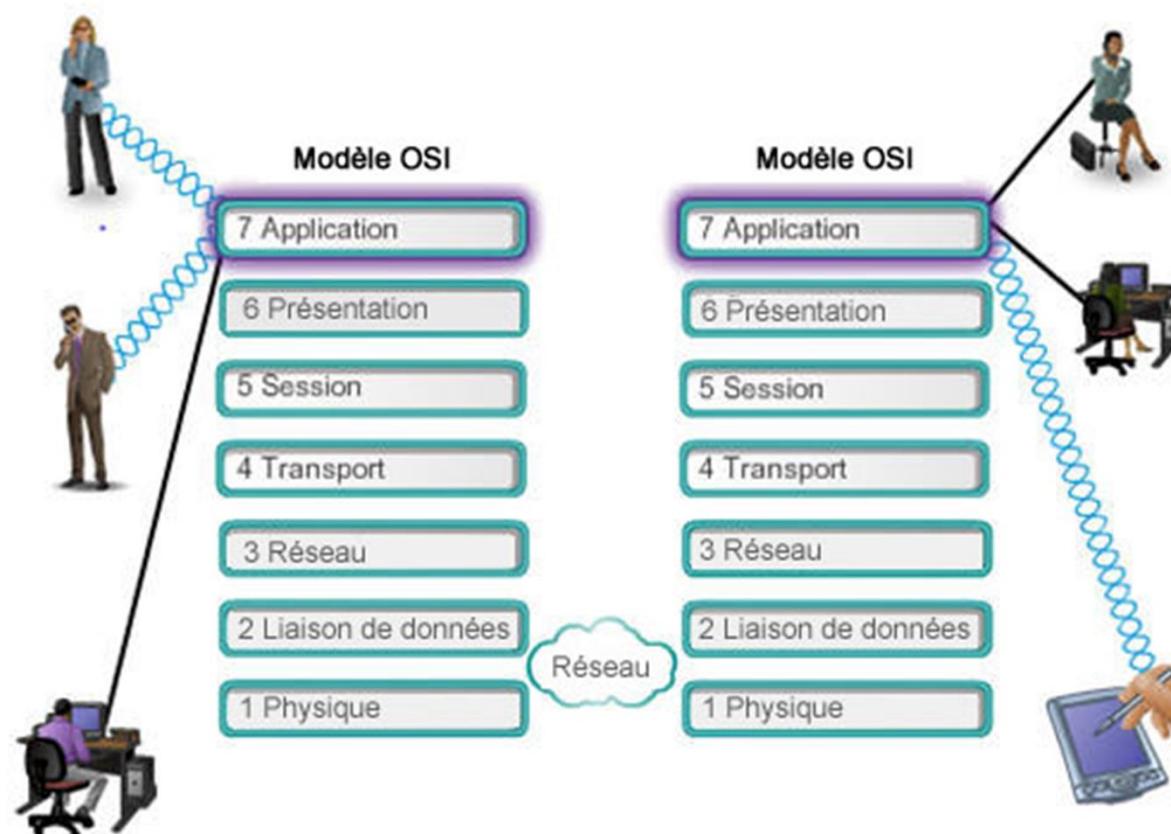
```
C:\>netstat  
  
Active Connections  
  
Proto Local Address Foreign Address State  
TCP kenpc:3126 192.168.0.2:netbios-ssn ESTABLISHED  
TCP kenpc:3158 207.138.126.152:http ESTABLISHED  
TCP kenpc:3159 207.138.126.169:http ESTABLISHED  
TCP kenpc:3160 207.138.126.169:http ESTABLISHED  
TCP kenpc:3161 sc.msn.com:http ESTABLISHED  
TCP kenpc:3166 www.cisco.com:http ESTABLISHED  
  
C:\>
```

La couche Application

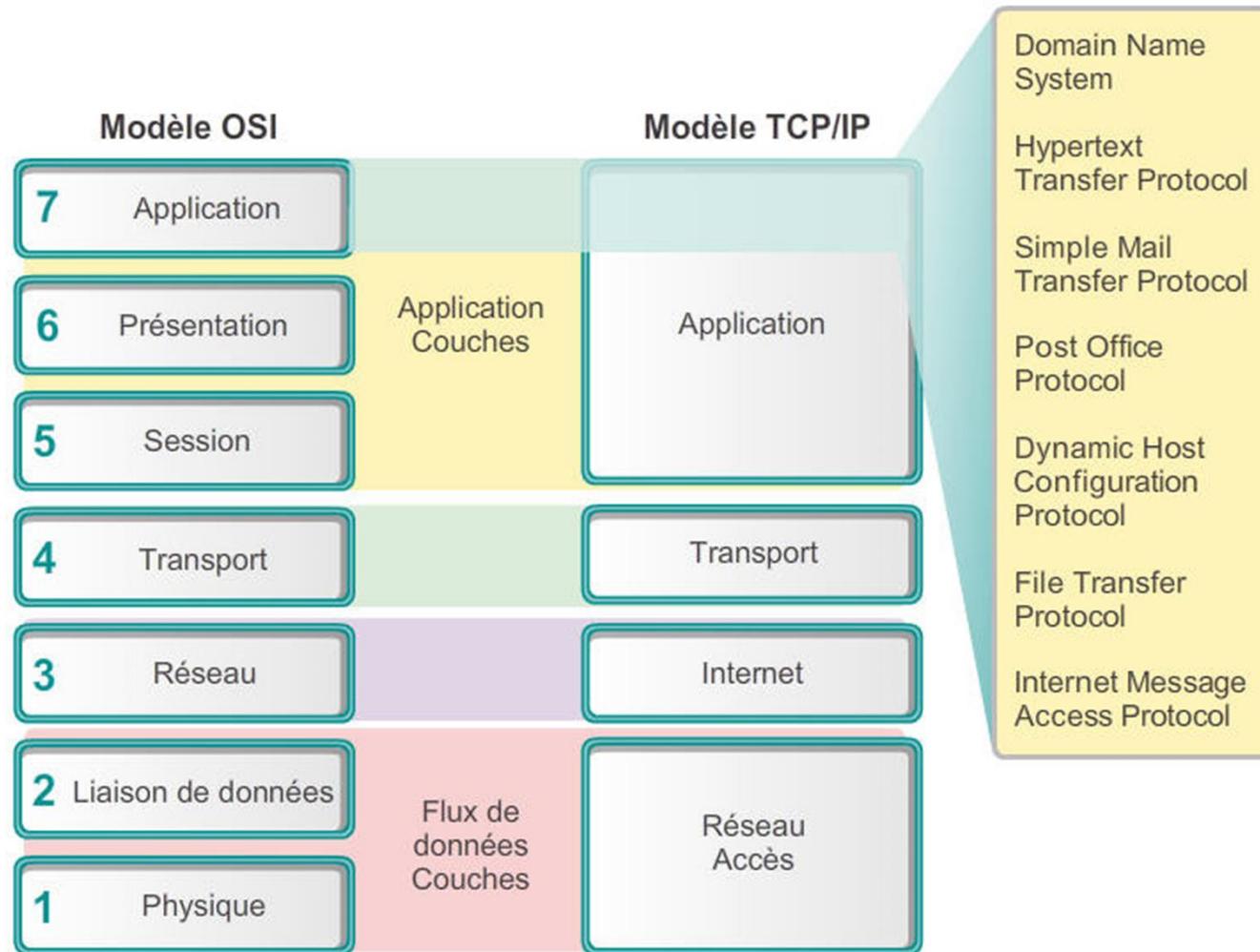


Les protocoles de couche application

La couche application fournit l'interface avec le réseau.



La couche application



Protocoles de couche application TCP/IP

DNS (Domain Name Service) : utilisé pour traduire les adresses Internet en adresses IP

Telnet : protocole d'émulation de terminal utilisé pour fournir l'accès distant aux serveurs et aux périphériques réseau

BOOTP (Bootstrap) : précurseur du protocole DHCP utilisé pour obtenir des informations d'adresse IP pendant le démarrage

DHCP (Dynamic Host control protocol) : utilisé pour attribuer une adresse IP, un masque de sous-réseau, une passerelle par défaut et un serveur DNS à un hôte

HTTP (Hypertext Transfer Protocol) : utilisé pour transférer les fichiers qui constituent les pages du Web

Protocoles de couche application TCP/IP

FTP (File Transfer Protocol) : utilisé pour le transfert interactif de fichiers entre les systèmes

TFTP (Trivial File Transfer Protocol) : utilisé pour le transfert de fichiers simple et sans connexion

SMTP (Simple Mail Transfer Protocol) : utilisé pour transférer les e-mails et les pièces jointes

POP (Post Office Protocol) : utilisé par les clients de messagerie pour récupérer des e-mails sur un serveur de messagerie

IMAP (Internet Message Access Protocol) : un autre protocole pour la récupération des e-mails

Services d'adressage IP

- ✓ Besoin:
 - ✓ Tout ordinateur a besoin de connaître son adresse IP, l'adresse du routeur, le masque de sous réseau, l'adresse d'un serveur de noms
 - ✓ Configuration statique
 - ✓ Configuration dynamique
 - ✓ Un utilisateur nomade a besoin d'une adresse IP et d'autres paramètres de configuration
- ✓ Plusieurs protocoles de configuration dynamique: RARP, BootP, DHCP.
- ✓ RARP a des lacunes
 - ✓ Il ne retourne que l'adresse IP
 - ✓ Il utilise la diffusion sur la couche liaison de données (les requêtes RARP ne sont pas propagées plus loin par les routeurs)

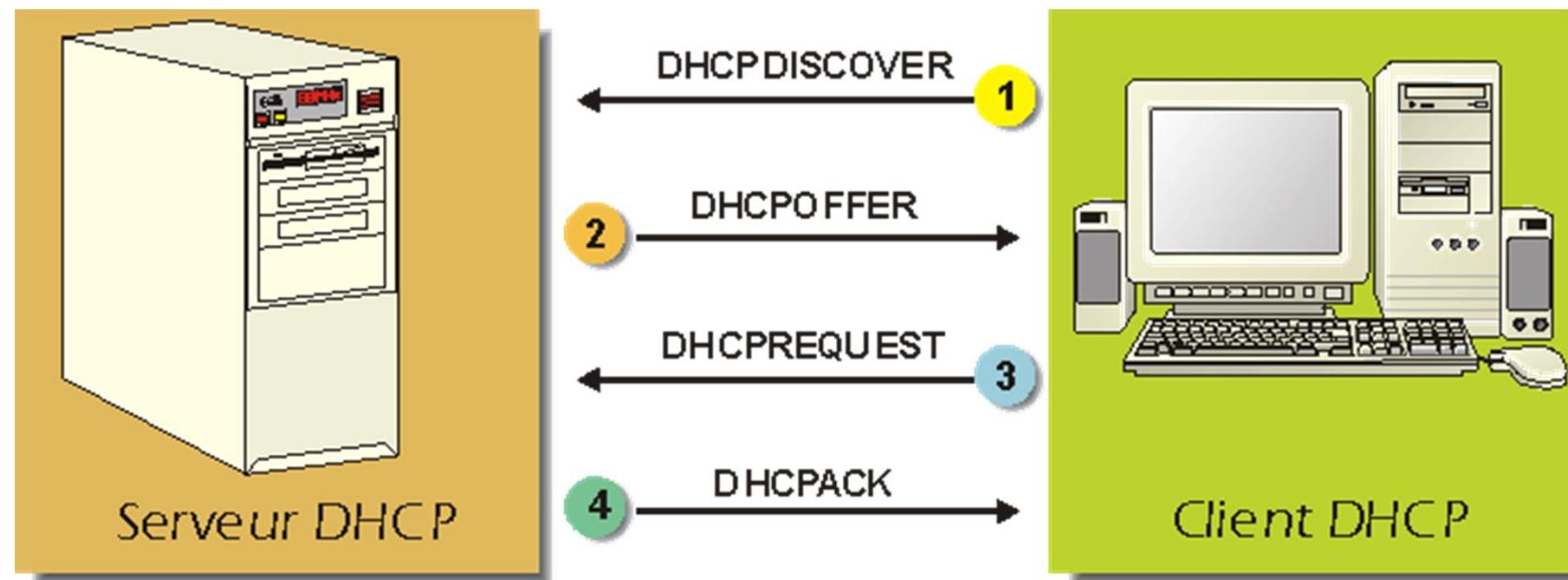
BootP

- ✓ Requiert un nombre suffisant d'adresses IP afin d'allouer à chaque ordinateur une adresse IP exclusive
- ✓ Un serveur BootP dispose d'un fichier de configuration renfermant la liste des adresses IP des clients (du même réseau)
- ✓ Un client BootP envoie son adresse physique vers un serveur BootP dans un datagramme UDP (s'il ne connaît pas l'adresse du serveur, il utilise l'adresse de diffusion 255.255.255.255)
- ✓ Le serveur bootP reçoit le datagramme et retourne au client son adresse IP et un nom de fichier boot, l'adresse du serveur et d'autres informations
- ✓ Le client utilise le TFTP pour démarrer le transfert du fichier de « boot » depuis le serveur

DHCP

- ✓ DHCP apporte des extensions par rapport au BootP
 - ✓ Permet de passer dans un message UDP plus d'informations
 - ✓ Permet à un ordinateur d'obtenir une adresse IP de manière dynamique
 - ✓ Permet à un utilisateur nomade de louer une adresse IP temporaire pour la durée de connexion
- ✓ Trois types d'allocation d'adresses IP
 - ✓ **Configuration manuelle** : identique à BootP; utilise une table de correspondance entre adresse MAC et adresse IP
 - ✓ **Configuration automatique** : le serveur DHCP alloue une adresse IP permanente lorsqu'un ordinateur se raccorde au réseau pour la première fois
 - ✓ **Configuration dynamique** : le serveur DHCP alloue une adresse IP à un ordinateur pour un temps limité
- ✓ BootP et DHCP utilisent UDP
 - ✓ Port 67 pour le serveur BootP/DHCP
 - ✓ Port 68 pour le client BootP/DHCP

DHCP : le dialogue

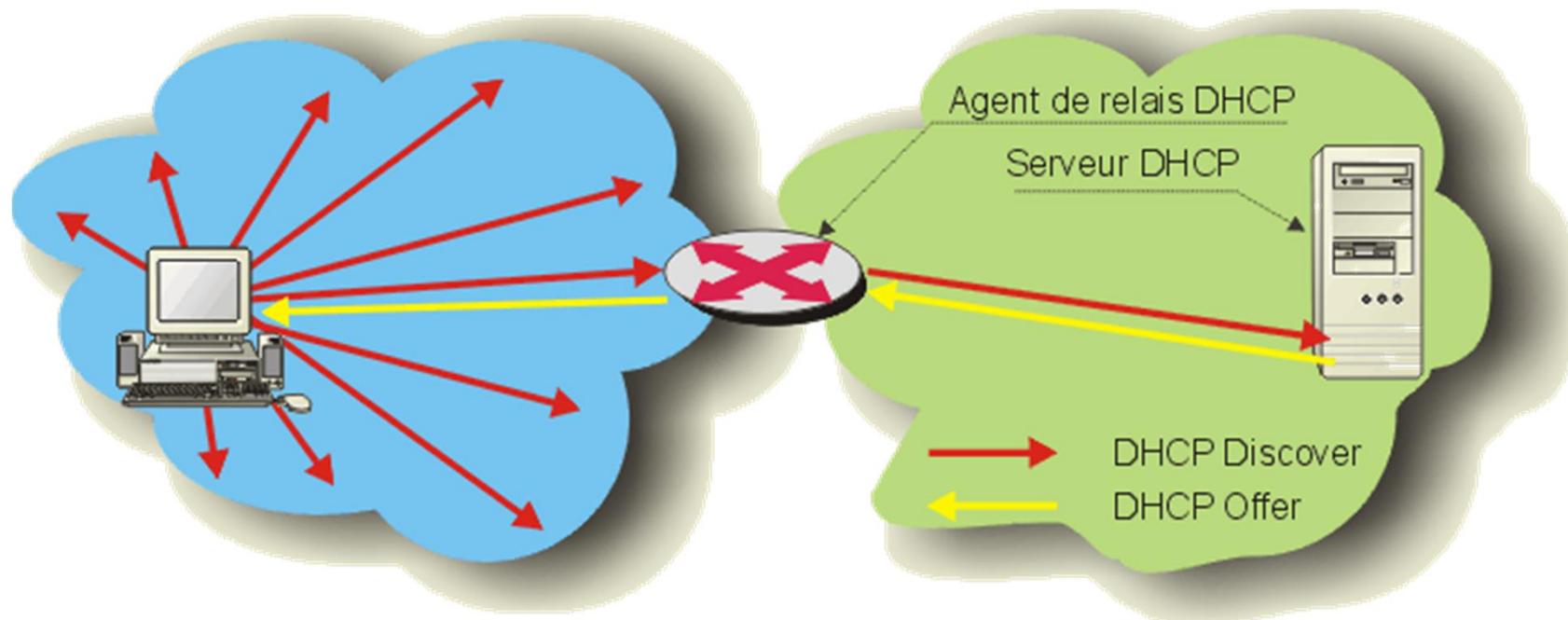


- 1- envoie en diffusion d'une trame renfermant l'adresse 0.0.0.0 et son adresse MAC
- 2- réponse des serveurs DHCP avec des propositions de « bails »
- 3-demande du client indiquant quelle offre il a accepté
- 4- accusé de réception de bail IP par le serveur DHCP concerné

DHCP : Détails sur le bail

- ✓ Adresse IP pour le client, durée de validité
- ✓ Adresse d'un ou de plusieurs DNS
- ✓ Adresse de la passerelle par défaut
- ✓ Adresse du serveur DHCP
- ✓ ...
- ✓ Renouvellement automatique de bail quand sa durée atteint la moitié
 - ✓ DHCPREQUEST
 - ✓ DHCPACK

DHCP : Agent relais



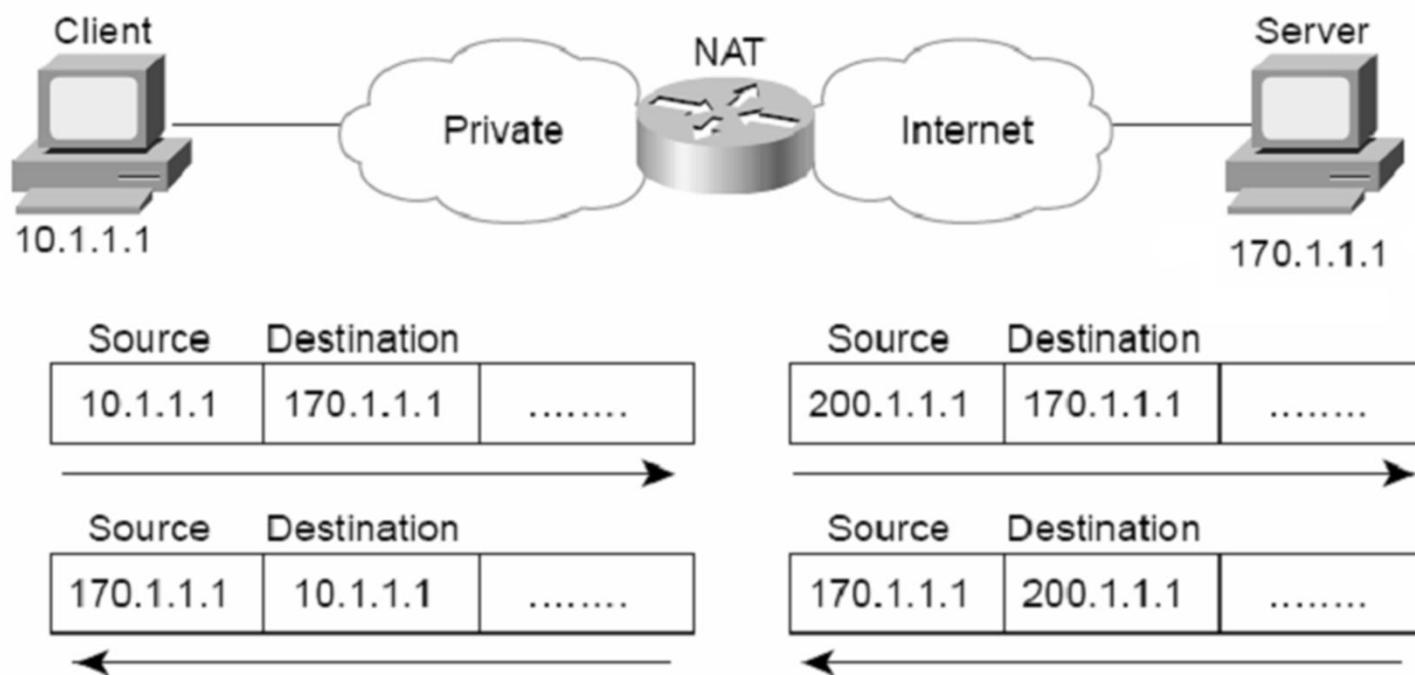
un agent de relais intercepte les requêtes en broadcast et les transmet à un serveur DHCP connu de cet agent.

Conseils pratiques

- ✓ Choisir dans la configuration TCP/IP : obtenir une adresse IP automatiquement
- ✓ ipconfig/all : affiche les détails de la configuration des interfaces réseau
- ✓ Renouvellement manuel d'un bail
 - ✓ ipconfig /renew : de renouveler le bail
- ✓ ipconfig /release : permet de résilier le bail
- ✓ Déterminer le nombre de serveurs DHCP nécessaires
- ✓ Utilisez plusieurs serveurs DHCP sur un même sous-réseau
 - ✓ Vérifier que les étendues ne se chevauchent pas
- ✓ Réserver des adresses IP pour des clients sur tous les serveurs DHCP
- ✓ Intégrer DHCP aux autres services (WINS, DNS)
- ✓ Mettre les routeurs à niveau pour relayer les messages DHCP ou créer des agents relais DHCP

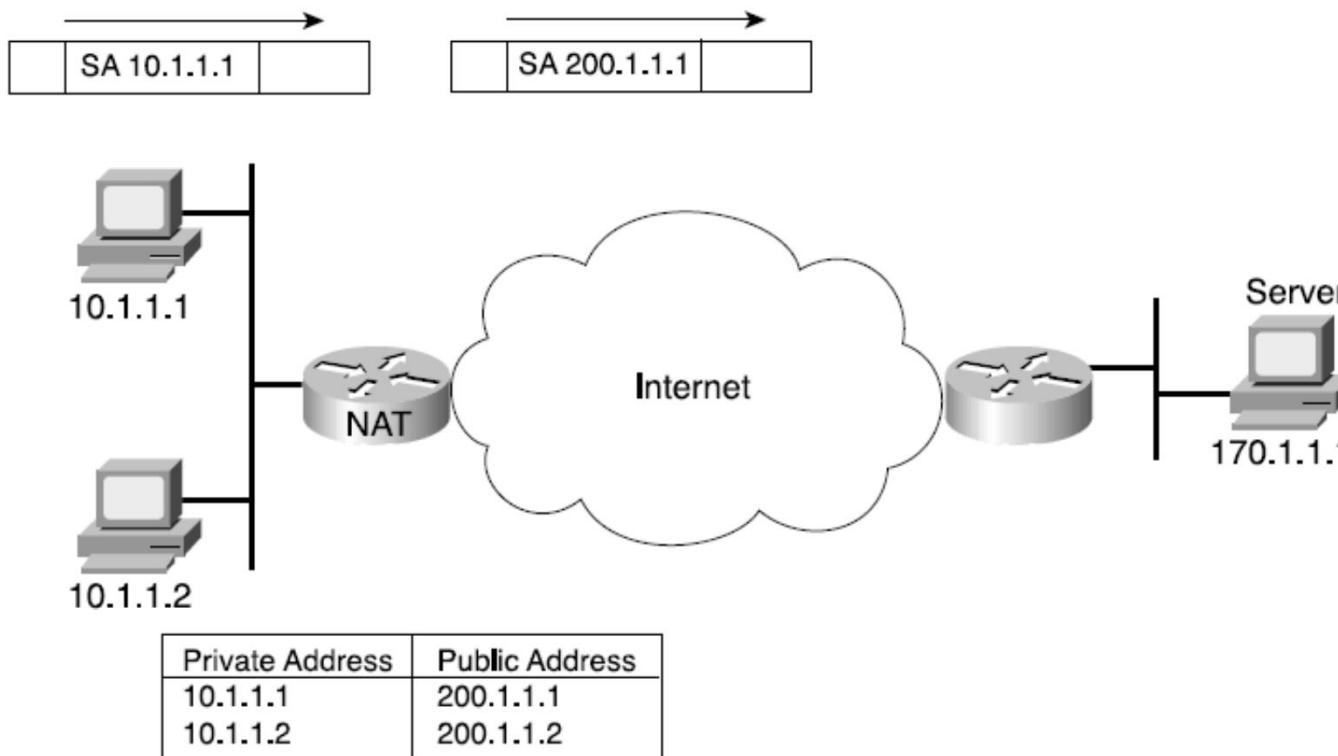
Network Address Translation (NAT)

- ✓ Solution pour la pénurie des adresses IP
- ✓ Permet à une machine ayant une adresse IP privée de communiquer avec d'autres machines sur Internet.
- ✓ Principe : changer l'adresse IP privée par une adresse publique (routable) dans chaque paquet IP



NAT statique

- ✓ A chaque adresse IP privée, une adresse IP publique est allouée d'une manière statique
- ✓ Nombre d'adresses IP publiques = nombre de machines
→ Ne résout pas le problème de pénurie d'adresse IP

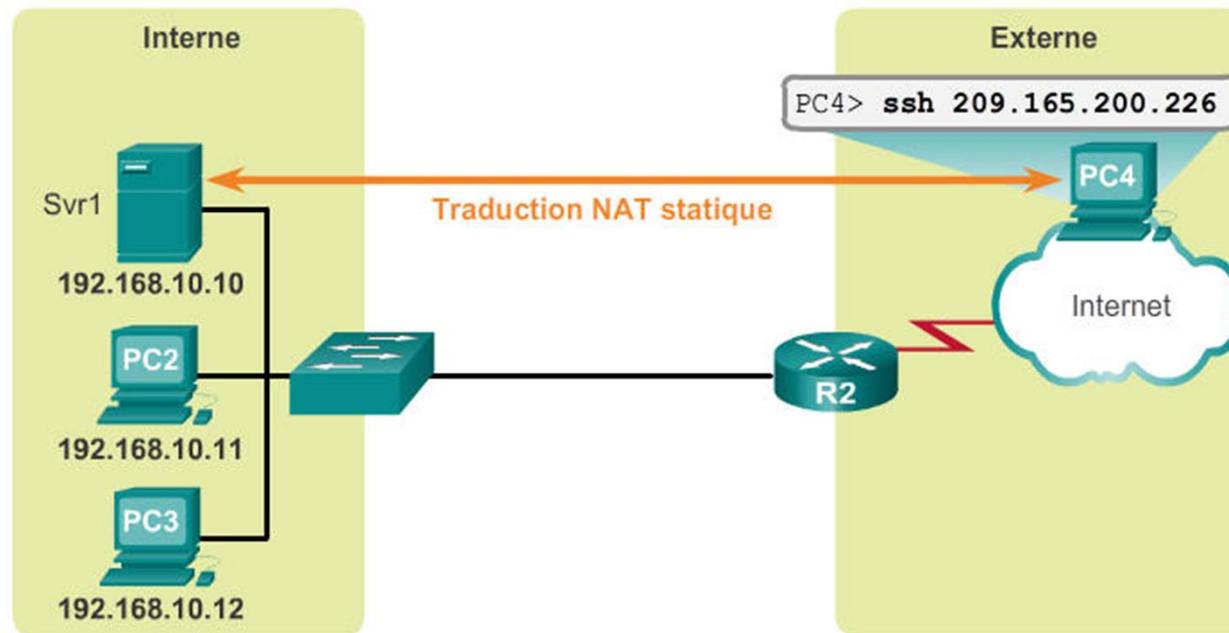


NAT statique

NAT statique

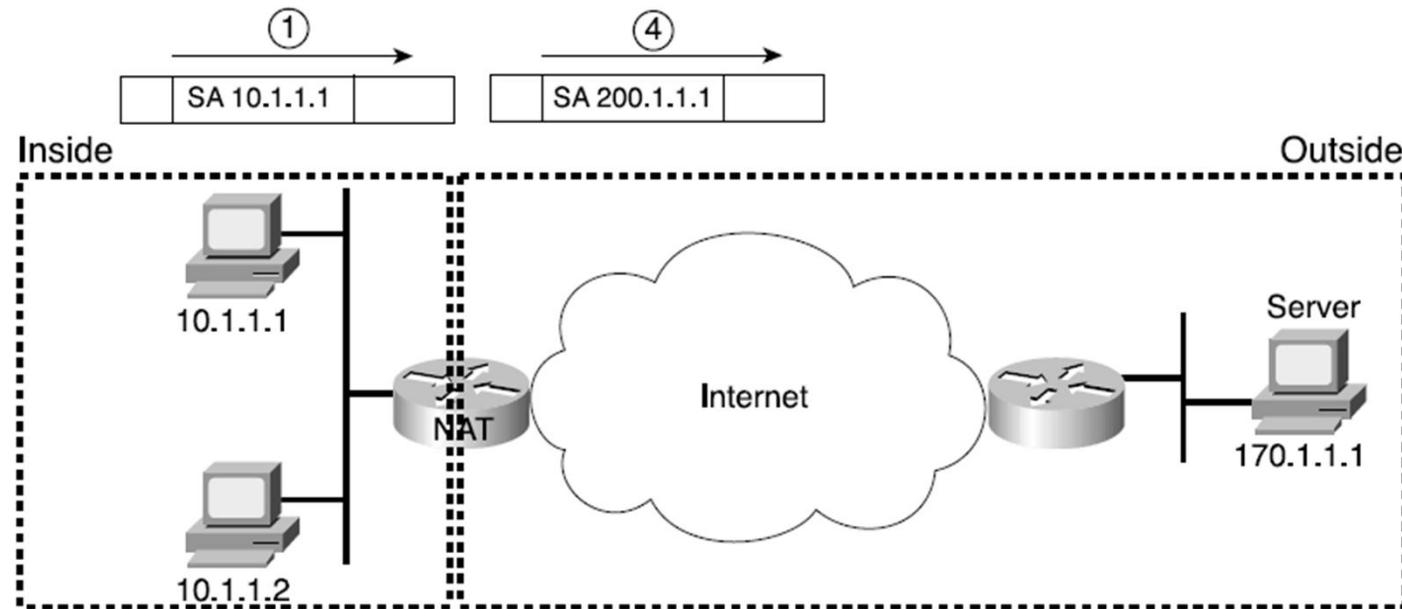
Table NAT statique

Adresse locale interne	Adresse globale interne - adresses accessibles via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228



NAT Dynamique

- ✓ La correspondance adresse publique / adresse privée est dynamique
- ✓ Nombre d'adresses IP publiques = nombre de machines connectées
→ meilleur que le NAT statique

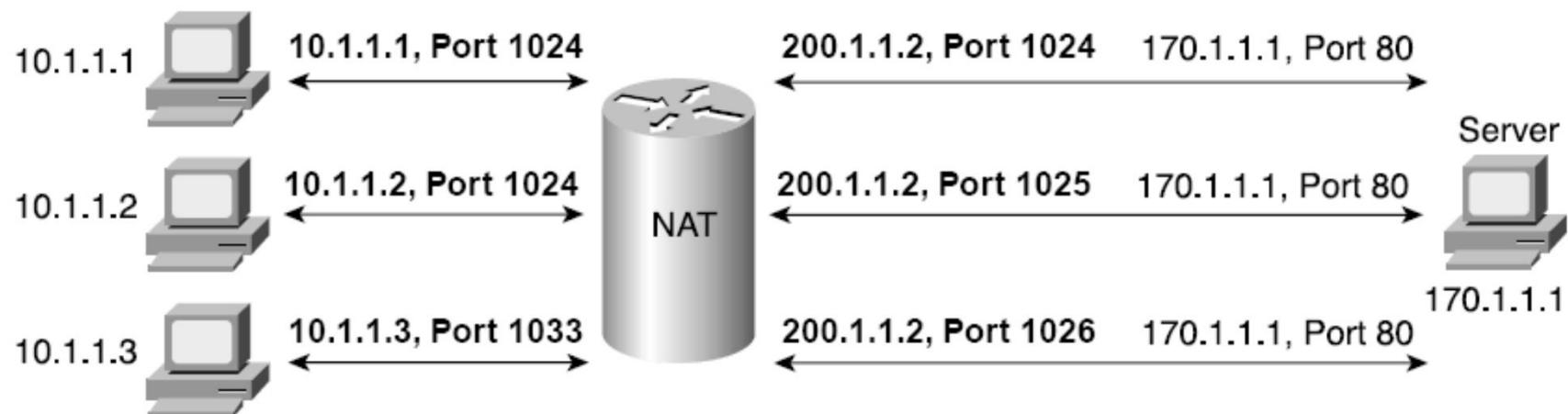


Criteria for Hosts to NAT:		NAT Table Before First Packet		NAT Pool:	
10.1.1.0 - 10.1.1.255		Inside Local	Inside Global	200.1.1.1 200.1.1.2 200.1.1.3 200.1.1.4 200.1.1.5	
(2)					
		10.1.1.1	200.1.1.1		

Port address translation (PAT)

- ✓ L'utilisation du NAT nécessite un nombre d'adresses publiques égale au nombre de machines qui se connectent à Internet simultanément
- ✓ Ceci n'est pas toujours possible → besoin d'une solution plus efficace
- ✓ Une adresse IP publique doit être utilisée par plusieurs machines simultanément

→ Solution : Port address translation (PAT)



Dynamic NAT Table, With Overloading

Inside Local	Inside Global
10.1.1.1:1024	200.1.1.2:1024
10.1.1.2:1024	200.1.1.2:1025
10.1.1.3:1033	200.1.1.2:1026

IOS Cisco

Configuration de base de routeurs



Routeur Cisco

Cisco IOS



Internetwork Operating System for Cisco networking devices



Configuration de base de routeur cisco



a) Différents mode du routeur

- Mode utilisateur :
 - Mode lecture d'informations.
 - Que des commandes d'affichage d'état.
- Mode privilégié :
 - Mode lecture avec pouvoir.
 - 2 fois plus de commandes d'état.
 - Commandes d'import/export/sauvegarde.

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

- Mode de configuration globale :
 - Que les commandes de configuration, et qui ont une portée globale.
 - Exemple : Nom du routeur, mot de passe du mode privilégié, route statique, bannière.
- Modes de configurations spécifiques :
 - Que les commandes de configuration qui ont une portée locale.
 - Exemple : Adresse IP, mot de passe d'une ligne.

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

- Mode SETUP :
 - Dialogue interactif de configuration minimaliste.
- Mode RXBoot :
 - Mode de maintenance.
 - Disponible au démarrage du routeur.
 - Sert principalement à la procédure de récupération des mots de passe.

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

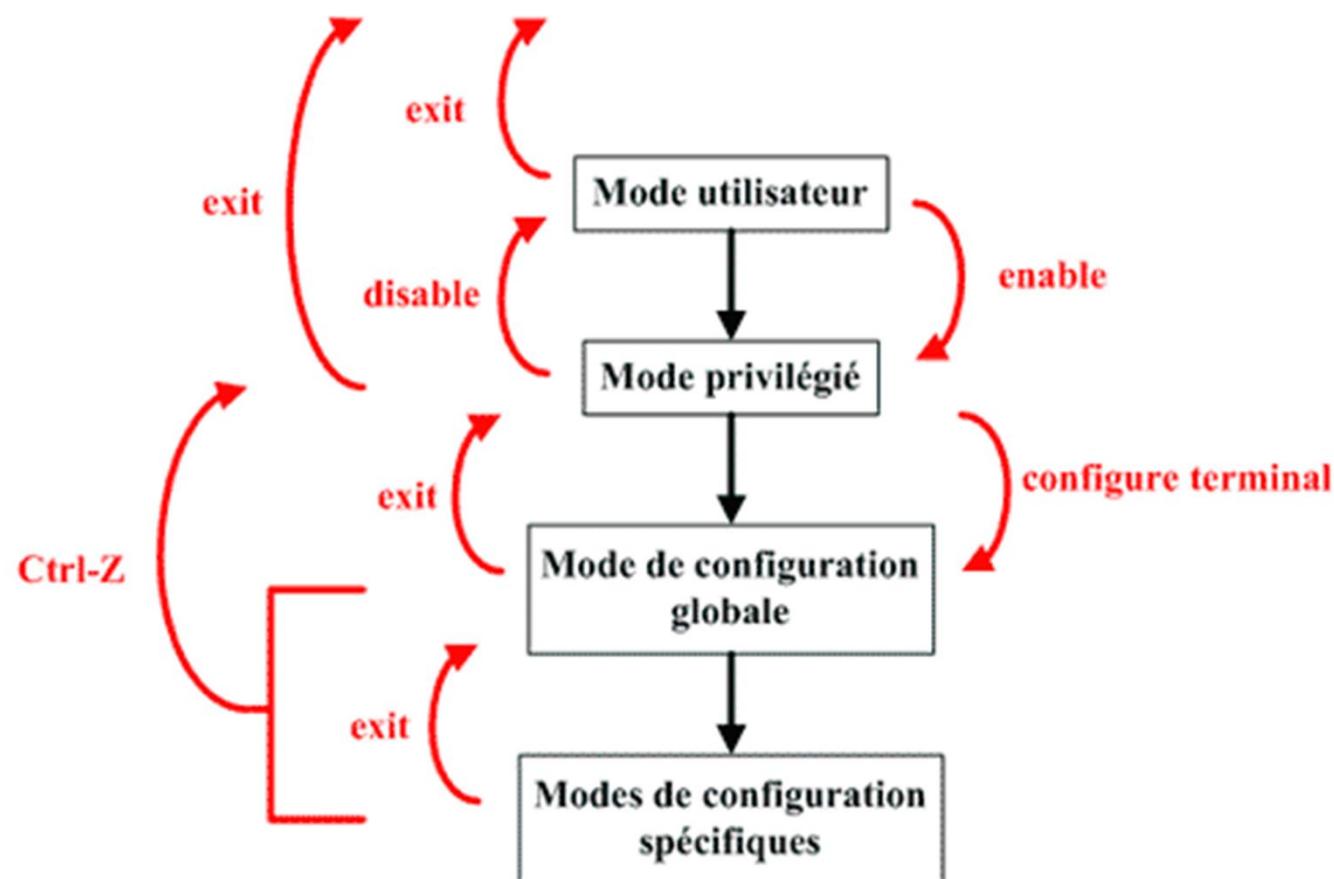
Invites de commandes associées

Mode	Invite de commande
Utilisateur	Router >
Privilégié	Router #
Configuration globale	Router (config) #
Interface	Router (config-if) #
Ligne	Router (config-line) #
Routeur	Router (config-router) #

Configuration de base de routeur cisco



Navigation dans les modes



Configuration de base de routeur cisco



b) Mode SETUP

- Objectif principal : Créer rapidement une configuration minimale :
 - Nom d'hôte du routeur
 - Mots de passe du mode privilégié
 - Mot de passe des lignes VTY

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

Caractéristiques principales

- Lancé automatiquement (voir chapitre sur IOS) ou manuellement (commande **setup**).
- Configuration sous forme de question.
- Existence de réponses par défaut (précisées entre crochets).
- Peut être arrêté avec la combinaison Ctrl-C.

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

- A la fin du processus de configuration :
 - Le fichier de configuration créé est affiché sur la console.
 - Question pour utiliser/sauvegarder la configuration créée, ou pour l'ignorer.

Configuration de base de routeur cisco



c) Fonctions d'aide du routeur

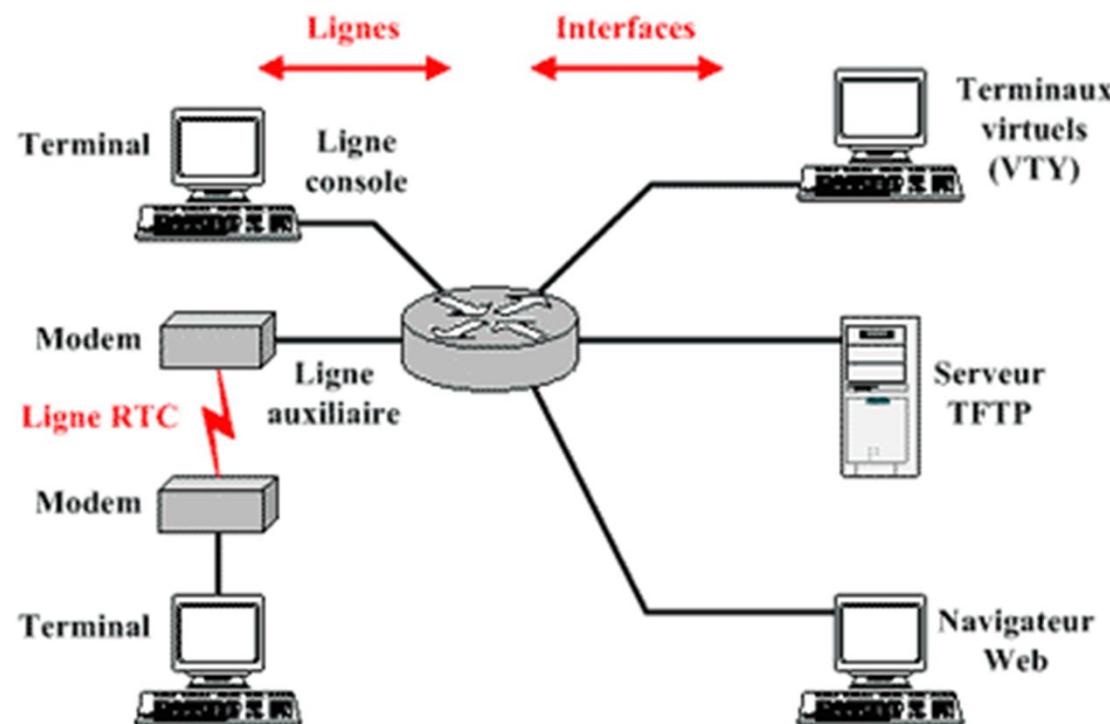
- Caractère ? : Affichages des différentes possibilités disponibles ainsi que les descriptions pour chaque entrée.
- Caractère ^ : Indicateur d'erreur.
- Touche tabulation : Complétion.

Configuration de base de routeur cisco



a) Sources de configuration externes

- Un routeur peut être configuré à partir des sources externes suivantes :



Configuration de base de routeur cisco



- Ligne console :

- Accès direct au routeur via un câble console.
 - C'est l'accès de base pour la configuration d'un routeur.

- Ligne Auxiliaire :

- Idem que ligne console.
 - Accès via ligne RTC et modems interposés.

- Lignes VTY :

- Terminaux virtuels utilisés lors des sessions Telnet vers le routeur.
 - Passent au travers d'une interface fonctionnelle.
 - 5 lignes VTY disponibles maximum.
 - Permettent un accès aux routeurs distants.

Connexion SSH : accès sécurisé et chiffré

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

- Serveur TFTP :

- Import/export de fichiers de configuration.
 - Import/export d'images IOS.

- Navigateur Web :

- Configuration d'un routeur via le service Web interne à ce dernier.
 - Pages affichant le listing des commandes disponibles.
 - Liens URL pour passer aux sous-commandes, paramètres.
 - Activation du serveur HTTP sur le routeur avec la commande ip http server (mode de configuration globale).

Configuration de base de routeur cisco



Différences entre port, ligne et interface

- Ports :

- Partie physique (RJ45, AUI, Serial).

- Lignes :

- Uniquement pour avoir accès au routeur pour administration (Lignes console, auxiliaire, VTY).

- Interfaces :

- Interviennent dans le processus d'acheminement de l'information (Trames, paquets) (Ethernet, Serial).
 - Elles seules possèdent des adresses de couche 2 & 3.

Configuration de base de routeur cisco



b) Composants internes et commandes d'état

■ RAM :

- Mémoire de travail principale du routeur.
- Equivaut à la RAM d'un PC.

■ NVRAM :

- Mémoire de sauvegarde de configuration. Relativement lente.
- Equivaut aux fichiers *.INI de Windows.

Configuration de base de routeur cisco



■ FLASH :

- Mémoire de stockage principal de type EEPROM.
- Equivaut au disque dur d'un PC.

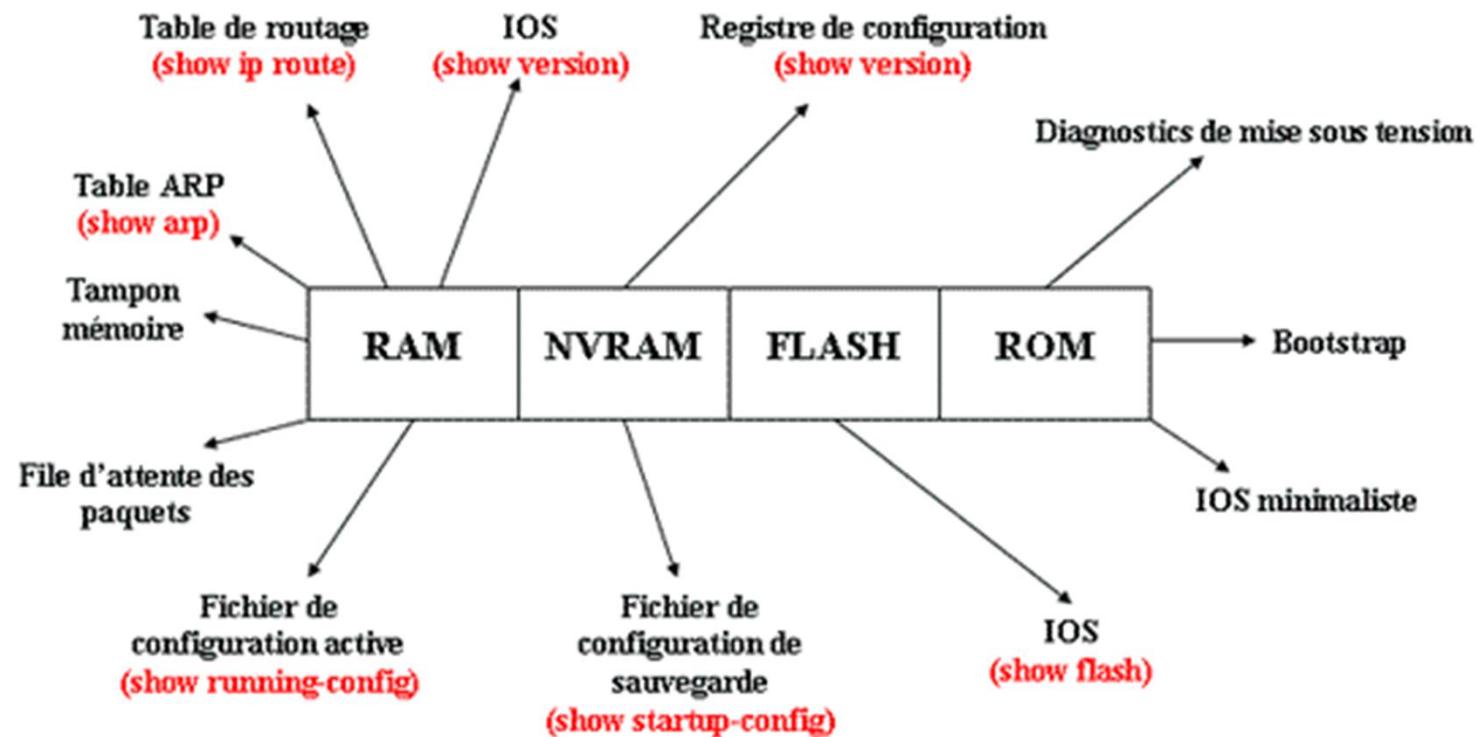
■ ROM :

- Sert principalement au moment du démarrage.
- Equivaut au BIOS d'un PC.

Configuration de base de routeur cisco



Contenu de chaque composant



Configuration de base de routeur cisco

Configuration d'un routeur

Configuration de base de routeur cisco



a) Fichiers de configuration

- Informations contenues dans un fichier de configuration :
 - Version d'IOS avec laquelle le fichier est prévu pour fonctionner.
 - Nom d'hôte et mot(s) de passe du mode privilégié.
 - Entrées statiques de résolution de nom ↔ IP.
 - Chaque interface avec sa configuration.
 - Routage (statique et dynamique).
 - Chaque ligne avec sa configuration.

Configuration de base de routeur cisco



Version d'IOS

```
Version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

Nom d'hôte
Mot(s) de passe du mode privilégié

```
!
hostname Lab_A
enable password class
```

Chaque interface avec sa configuration

```
!
ip subnet-zero
!
interface Serial0
ip address 201.100.11.1 255.255.255.0
no ip directed-broadcast
```

Routage (statique et/ou dynamique)

```
!
interface Serial1
no ip address
no ip directed-broadcast
shutdown
!
interface Ethernet0
ip address 192.5.5.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet1
ip address 205.7.5.1 255.255.255.0
no ip directed-broadcast
!
```

Chaque ligne avec sa configuration

```
router rip
network 201.100.11.0
network 192.5.5.0
network 205.7.5.0
!
ip classless
no ip http server
!
line con 0
transport input none
line aux 0
line vty 0 4
password cisco
!
End
```

Configuration de base de routeur cisco

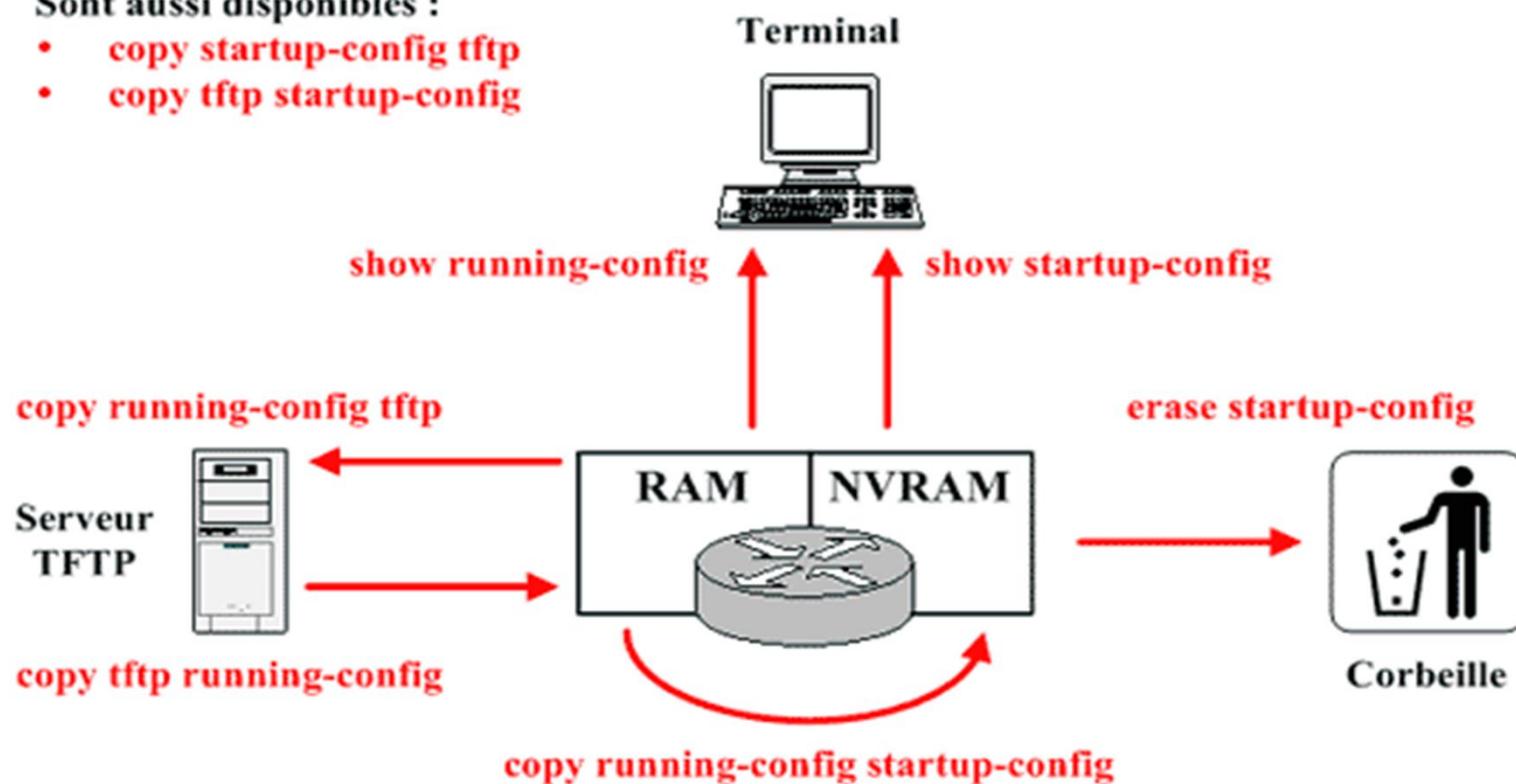


Laboratoire
Supinfo des Technologies
Cisco

Commandes associées

Sont aussi disponibles :

- `copy startup-config tftp`
- `copy tftp startup-config`



Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

b) Configuration des mots de passe

- Protection :
 - De chaque ligne.
 - De l'accès au mode privilégié.
 - De l'affichage des mots de passe en clair dans les fichiers de configuration.

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

Protection des lignes

- Depuis le mode de configuration globale :
 - **line {console | aux | vty} {numéro}** : Permet de passer dans le mode de configuration spécifique à la ligne indiquée.
 - **password {mot de passe}** : Affecte le mot de passe voulu. Mot de passe écrit en clair dans le fichier de configuration.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with END.
Router(config)#line console 0
Router(config-line)#password cisco
```

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

Limitation d'accès au mode privilégié

■ **enable password {mot de passe}** :

- Configure un mot de passe pour le mode privilégié.
- Mot de passe écrit en clair dans le fichier de configuration.

■ **enable secret {mot de passe}** :

- Idem mais est crypté dans le fichier de configuration grâce à un algorithme propriétaire Cisco.

```
Router(config)#
Router(config)#enable password cisco
Router(config)#enable secret class
Router(config)#

```

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

Informations supplémentaires

- **enable secret** et **enable password** peuvent être configurés tous les deux sur un même routeur.
- Mot de passe **enable secret** prioritaire sur mot de passe **enable password** :

```
Router(config)#
Router(config)#enable password class
Router(config)#enable secret cisco ← Prioritaire
Router(config)#exit
00:01:00: %SYS-5-CONFIG_I: Configured from console by console
Router#disable
Router>enable
Password: ← cisco
Router#
```

Configuration de base de routeur cisco



c) Configuration du nom du routeur et des descriptions

- On va étudier :
 - Le nom d'hôte du routeur.
 - La bannière de connexion.
 - La description pour chaque interface.

Configuration de base de routeur cisco



Nom d'hôte du routeur

- Commande **hostname {nom d'hôte}**.
- C'est le nom affiché par l'invite du système.
- Le nom par défaut est **Router**.

```
Router(config)#  
Router(config)#hostname Lab_A  
Lab_A(config)#[
```

Configuration de base de routeur cisco

Adressage IP et interfaces

Configuration de base de routeur cisco



Laboratoire
Supinfo des Technologies
Cisco

a) Adresse IP d'une interface

- Passer dans le mode de configuration de l'interface voulue :
 - Commande **interface {type} {numéro}** depuis le mode de configuration globale.
- Configuration de l'adresse IP :
 - Commande **ip address {IP} {masque de sous-réseau}**

Configuration de base de routeur cisco



Masque de sous-réseau

- Trois façons de l'écrire :
 - Décimale pointée (option par défaut)
(Exemple : 255.255.255.0).
 - Nombre de bits (Exemple : /24).
 - Notation hexadécimale (Exemple : 0xFFFFF00).

Configuration de base de routeur cisco



Activation/désactivation

- Une interface est par défaut désactivée (**shutdown**).
- Elle est activée :
 - Par la commande **no shutdown**.
 - Dans certains cas automatiquement après la configuration de l'interface (**no shutdown** implicite).
- Permet de désactiver une interface, donc une liaison, sans pour autant détériorer la configuration de cette dernière.

Configuration de base de routeur cisco



Exemples

```
Router(config)#
Router(config)#interface ethernet 0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#{
```

Configuration de base de routeur cisco



d) Spécificités des interfaces WAN

- Interfaces WAN plus complexes à configurer :
 - Obligé de spécifier quelle est la vitesse de synchronisation de la liaison (Exemple : 64 ou 128 Kbps).
 - Sur une liaison LAN, c'est implicite (10 ou 100 Mbps).
- Commande **clock rate {valeur}** :
 - Mode de configuration de l'interface.
 - Uniquement sur la partie ETCD de la liaison (Repérée par la dénomination V.35 DCE du câble V.35).

Configuration de base de routeur cisco



Exemple

```
Router(config)#
Router(config)#interface serial 0
Router(config-if)#ip address 172.16.40.1 255.255.0.0
Router(config-if)#clock rate 56000
Router(config-if)#no shutdown
Router(config-if)#

```

Présentation des réseaux commutés



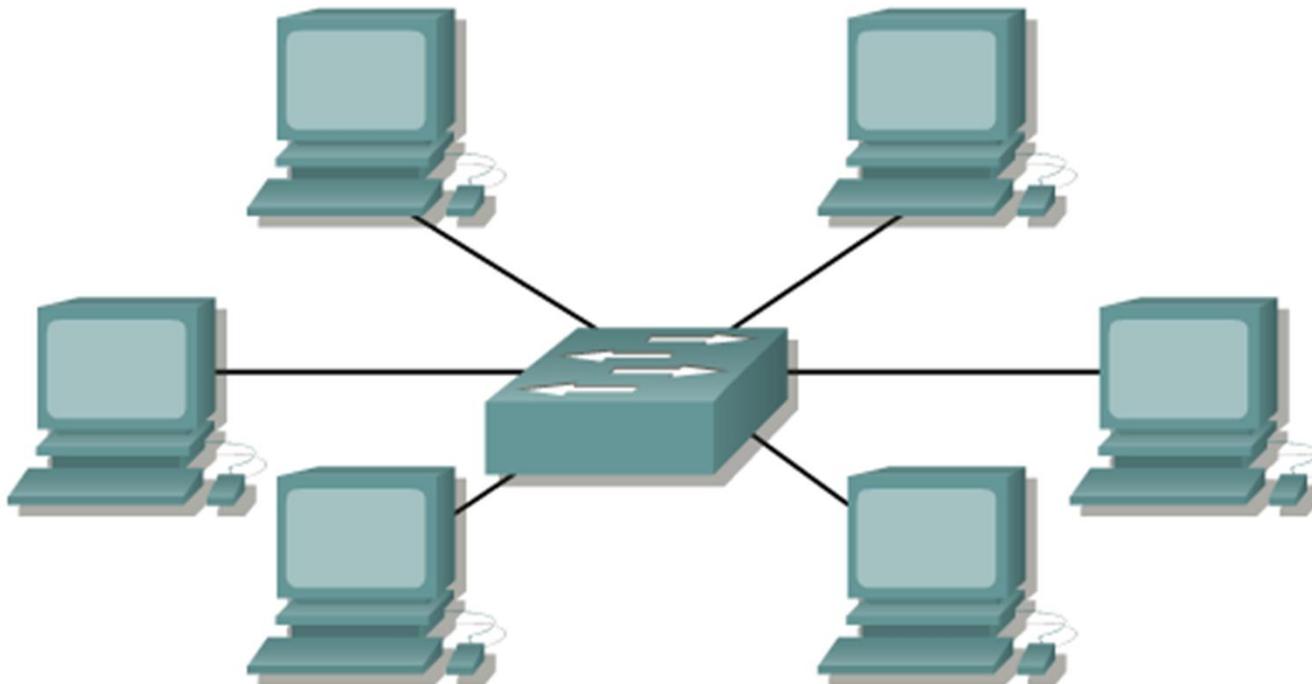
Rôle des réseaux commutés

- Le rôle des réseaux commutés a évolué
- Un réseau local (LAN) commuté accroît la flexibilité et permet la gestion du trafic
- Il prend également en charge des fonctionnalités telles que la qualité de service, la sécurité renforcée, la prise en charge de la technologie sans fil et de la téléphonie IP, et les services de mobilité

La commutation comme concept général

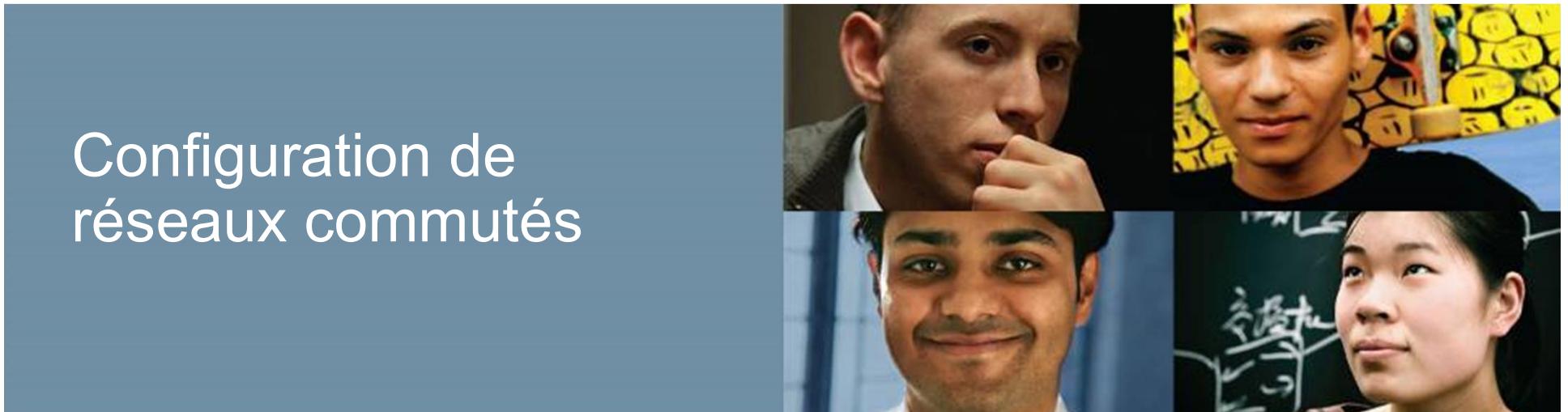
- Un commutateur est un équipement de couche 2
- Un commutateur connecte les périphériques finaux à un équipement intermédiaire central sur la plupart des réseaux Ethernet
- Un commutateur prend une décision en fonction du port d'entrée et de destination
- Un commutateur LAN gère une table qu'il utilise pour déterminer comment acheminer le trafic
- Les commutateurs LAN transmettent des trames Ethernet basées sur l'adresse MAC de destination des trames.
- Segmente le réseau (un domaine de collision par port)

Microsegmentation LAN avec commutateurs



- Élimination de l'effet des collisions grâce à la microsegmentation
- Latence faible et hauts débits d'acheminement des trames au niveau de chaque port d'interface
- Compatible avec le câblage et les cartes réseau conformes à la norme 802.3 (CSMA/CD)

Configuration de réseaux commutés



Préparation à la gestion de commutateur de base

Commandes IOS de commutateur Cisco

Passer en mode de configuration globale.	S1# configure terminal
Passez en mode de configuration d'interface pour SVI.	S1(config)# interface vlan 99
Configurer l'adresse IP de l'interface de gestion.	S1(config-if)# ip address 172.17.99.11 255.255.0.0
Activer l'interface de gestion.	S1(config-if)# no shutdown
Repassiez en mode d'exécution privilégié.	S1(config-if)# end
Enregistrez la configuration en cours dans la configuration de démarrage.	S1# copy running-config startup-config

Commandes IOS de commutateur Cisco

Passer en mode de configuration globale.	S1# configure terminal
Configurez la passerelle par défaut pour le commutateur.	S1(config)# ip default-gateway 172.17.99.1
Repassiez en mode d'exécution privilégié.	S1(config-if)# end
Enregistrez la configuration en cours dans la configuration de démarrage.	S1# copy running-config startup-config

Vérification de la config du port de commutateur

Commandes de vérification

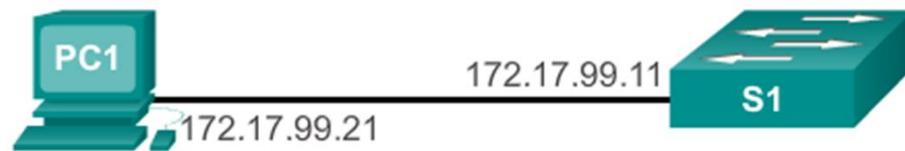
Commandes IOS de commutateur Cisco

Afficher l'état et la configuration des interfaces.	S1# show interfaces [interface-id]
Afficher la configuration initiale actuelle.	S1# show startup-config
Afficher la configuration en cours.	S1# show running-config
Afficher les informations sur le système de fichiers Flash.	S1# show flash
Afficher l'état matériel et logiciel du système.	S1# show version
Afficher l'historique des commandes exécutées.	S1# show history
Afficher les informations IP d'une interface.	S1# show ip [interface-id]
Afficher la table d'adresses MAC.	S1# show mac-address-table OU S1# show mac address-table

Fonctionnement de SSH

- Secure Shell (SSH) est un protocole qui permet de se connecter de manière sécurisée (connexion chiffrée) à un périphérique distant via une ligne de commande.
- SSH est généralement utilisé dans les systèmes basés sur UNIX.
- Cisco IOS prend également en charge SSH.
- Il faut disposer d'une version du logiciel IOS comprenant des fonctions et des fonctionnalités chiffrées pour pouvoir utiliser SSH sur les commutateurs Catalyst 2960.
- En raison de la fiabilité de ses fonctions de chiffrement, SSH devrait remplacer Telnet pour les connexions servant à la gestion.
- SSH utilise le port TCP 22 par défaut et Telnet utilise le port TCP 23.

Fonctionnement de SSH

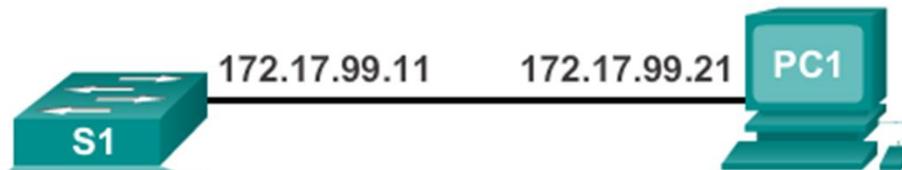


172.17.99.11 - PuTTY

```
Login as: admin
Using keyboard-interactive
authentication.
Password:

S1>enable
Password:
S1#
```

Configuration de SSH



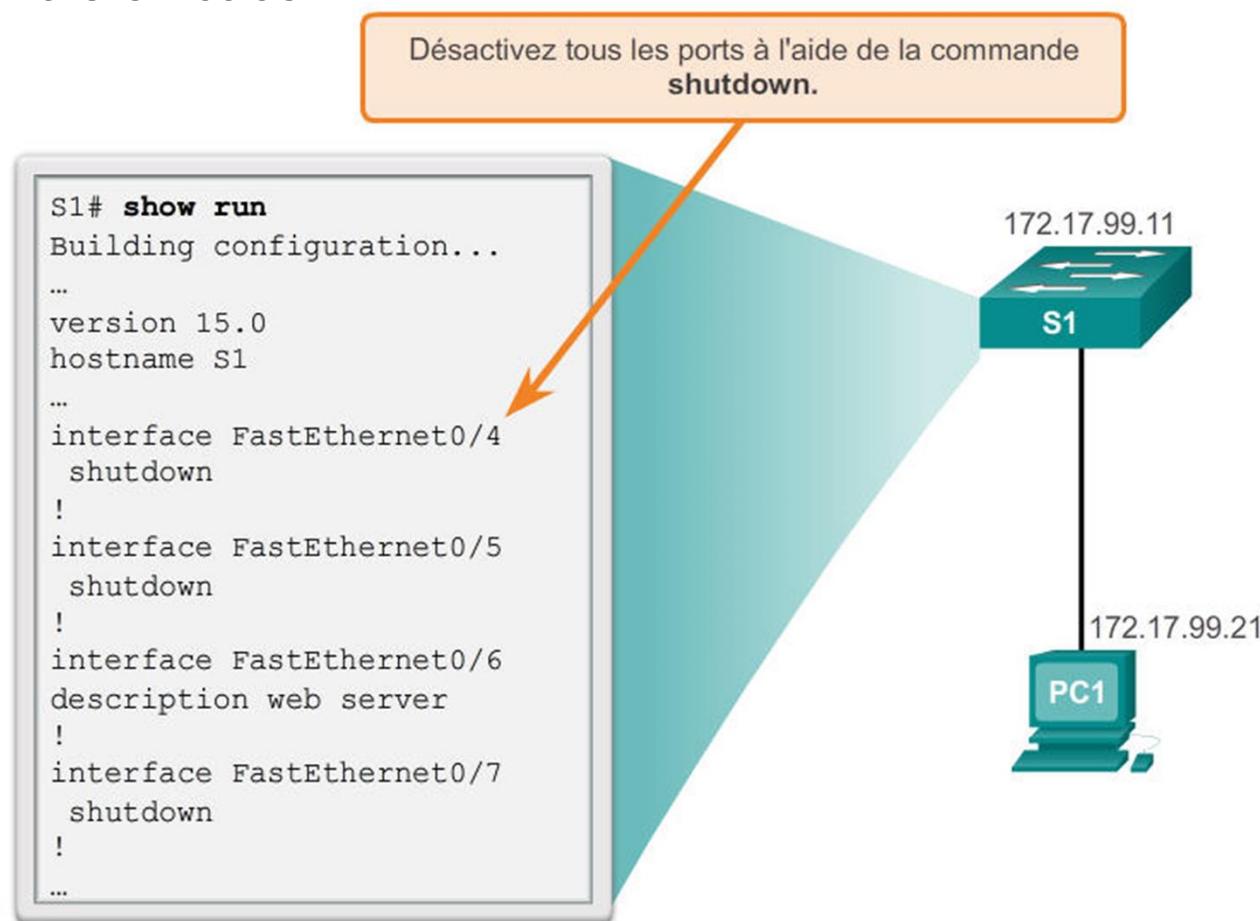
```
S1 # configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin password ccna
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config)# end
```

Utilisation du protocole CDP

- CDP est un protocole propriétaire de couche 2 développé par Cisco. Il sert à détecter les autres périphériques Cisco qui sont connectés directement.
- Il est conçu pour permettre aux équipements de configurer automatiquement leurs connexions.
- Si un pirate écoute les messages CDP, il peut apprendre des informations importantes telles que le modèle de périphérique et la version du logiciel exécuté.
- Cisco recommande de désactiver le protocole CDP quand il n'est pas utilisé.

Sécurisation des ports inutilisés

- La désactivation des ports non utilisés est une mesure de sécurité simple mais efficace.



Sécurité des ports : fonctionnement

- La sécurité des ports restreint le nombre d'adresses MAC valides autorisées sur un port.
- Les adresses MAC des périphériques légitimes peuvent y accéder, mais les autres sont refusées.
- Toute tentative supplémentaire pour se connecter avec des adresses MAC inconnues constitue une violation des règles de sécurité.

La sécurité des ports : fonctionnement

- Les adresses MAC fiables peuvent être configurées de différentes manières :
 - Adresses MAC statiques sécurisées : configurées et ajoutées manuellement à la configuration en cours : **switchport port-security mac-address** *mac-address*
 - Adresses MAC dynamiques sécurisées : supprimées au redémarrage du commutateur
 - Adresses MAC sécurisées rémanentes : ajoutées à la configuration en cours et apprises dynamiquement : commande du mode de configuration d'interface : **switchport port-security mac-address sticky**

La sécurité des ports : modes de violation

- L'IOS détecte une violation des règles de sécurité si :
 - Le nombre maximal d'adresses MAC sécurisées a été ajouté dans la table CAM et un appareil dont l'adresse MAC ne figure pas dans cette table tente d'accéder à l'interface.
- Trois actions peuvent être entreprises en cas de violation :
 - Protéger : aucune notification reçue
 - Limiter : notification relative à une violation de sécurité reçue
 - Arrêter
 - Commande du mode de configuration d'interface

```
switchport port-security
violation {protect | restrict | shutdown}
```

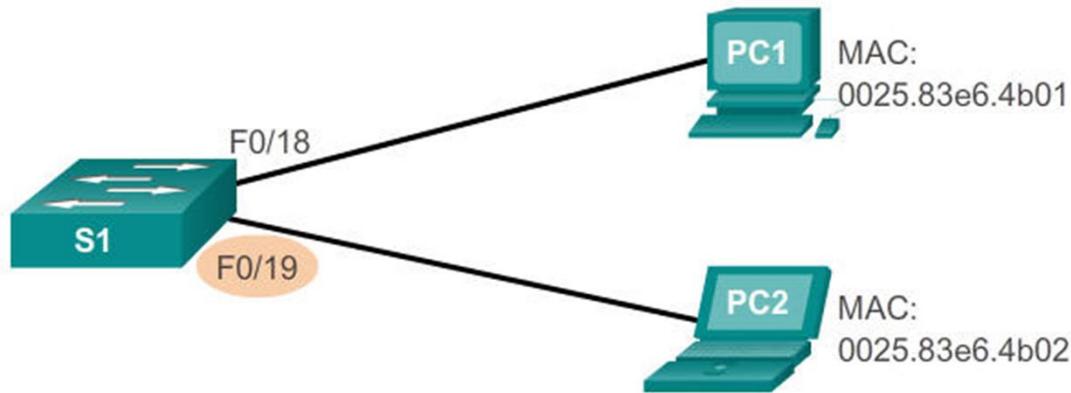
Sécurité des ports : configuration

- Failles dans la sécurité dynamique des ports

Caractéristique	Paramètre par défaut
Sécurité des ports	Désactivée sur un port
Nombre maximal d'adresses MAC sécurisées	1
Mode de violation	Shutdown. Le port est désactivé en cas de dépassement du nombre maximal d'adresses MAC sécurisées.
Apprentissage des adresses rémanentes	Désactivé

Sécurité des ports : configuration

- Configuration de la sécurité des ports rémanents



Commandes de l'interface en ligne de commande de CiscolOS	
Spécifiez l'interface à configurer pour la sécurité des ports.	S1 (config) # interface fastethernet 0/19
Définissez le mode d'interface sur le mode d'accès.	S1 (config-if) # switchport mode access
Activez la sécurité des ports sur l'interface.	S1 (config-if) # switchport port-security
Définissez le nombre maximal d'adresses sécurisées autorisées sur le port.	S1 (config-if) # switchport port-security maximum 50
Activez l'apprentissage rémanent.	S1 (config-if) # switchport port-security mac-address sticky

Sécurité des ports : vérification

- Vérification des adresses MAC sécurisées dans la sécurité des ports



```
S1# show port-security address
Secure Mac Address Table
-----
Vlan      Mac Address          Type           Ports      Remaining Age
                                         (mins)
-----
1        0025.83e6.4b01    SecureDynamic   Fa0/18      -
1        0025.83e6.4b02    SecureSticky   Fa0/19      -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port)
```

Switch>enable

Switch#Configure terminal

Switch(config)#interface FastEthernet 0/20

Switch(config-if)#switchport mode access

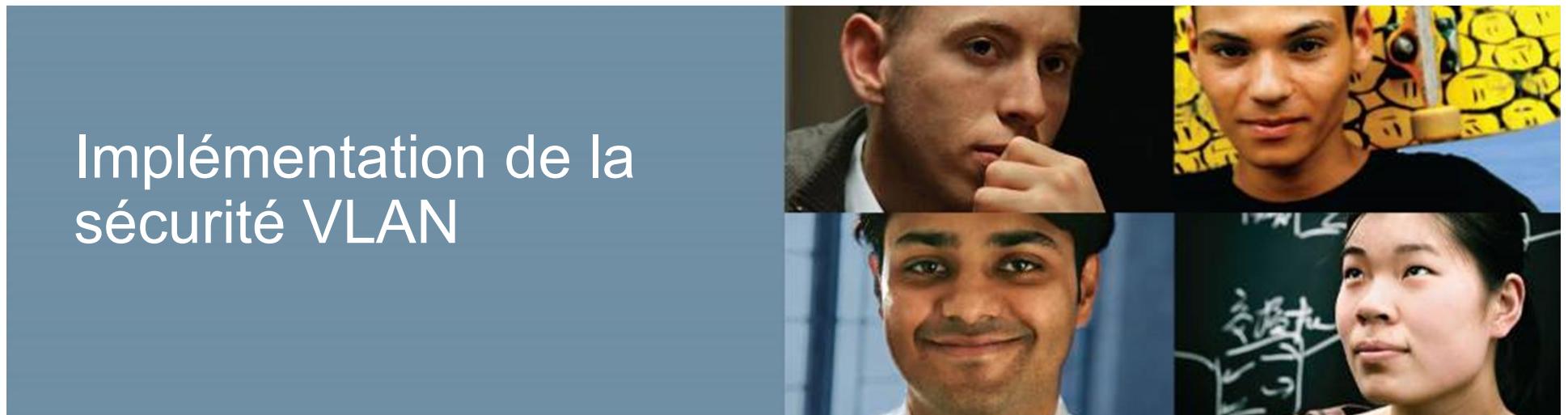
Switch(config-if)#switchport port-security

Switch(config-if)# switchport port-security maximum 1

Switch(config-if)#switchport port-security mac-address sticky

Switch(config-if)#switchport port-security violation shutdown

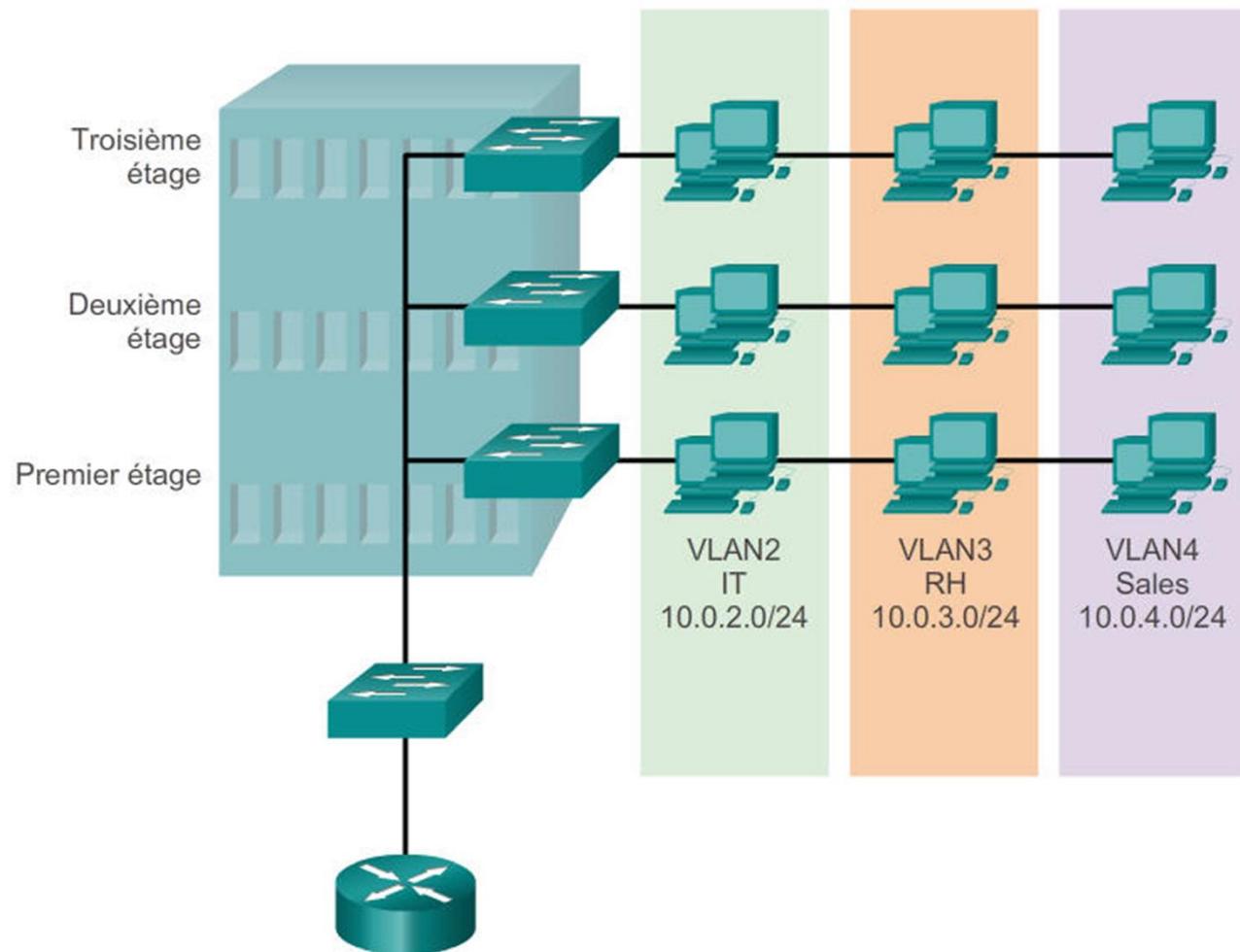
Implémentation de la sécurité VLAN



Définitions des VLAN

- Un VLAN (réseau local virtuel) est une partition logique d'un réseau de couche 2.
- Plusieurs partitions peuvent être créées, de sorte qu'il est possible de faire coexister plusieurs VLAN.
- Chaque VLAN constitue un domaine de diffusion, généralement avec son propre réseau IP.
- Les VLAN sont isolés les uns des autres et les paquets ne peuvent circuler entre eux qu'en passant par un routeur.
- La segmentation du réseau de couche 2 a lieu à l'intérieur d'un périphérique de couche 2, généralement un commutateur.
- Les hôtes regroupés dans un VLAN ignorent l'existence de celui-ci.

Définitions des VLAN



Avantages des VLAN

- Sécurité
- Réduction des coûts
- Meilleures performances
- Diminution des domaines de diffusion
- Simplification de la gestion des projets et des applications

Types de VLAN

- VLAN de données
- VLAN par défaut
- VLAN natif
- VLAN de gestion

Types de VLAN

VLAN 1

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

- Tous les ports affectés au VLAN 1 pour acheminer les données par défaut.
- Le VLAN natif est le VLAN 1 par défaut.
- Le VLAN de gestion est le VLAN 1 par défaut.
- Le VLAN 1 ne peut pas être renommé ni supprimé.

Trunks de VLAN

- Un trunk de VLAN achemine le trafic de plusieurs VLAN.
- Il est généralement établi entre des commutateurs pour permettre aux périphériques du même VLAN de communiquer même s'ils sont physiquement connectés à des commutateurs différents.
- Un trunk de VLAN n'est associé à aucun VLAN. Aucun port trunk n'est utilisé pour établir la liaison trunk.
- Cisco IOS prend en charge la norme IEEE802.1q, un protocole de trunk de VLAN très répandu.

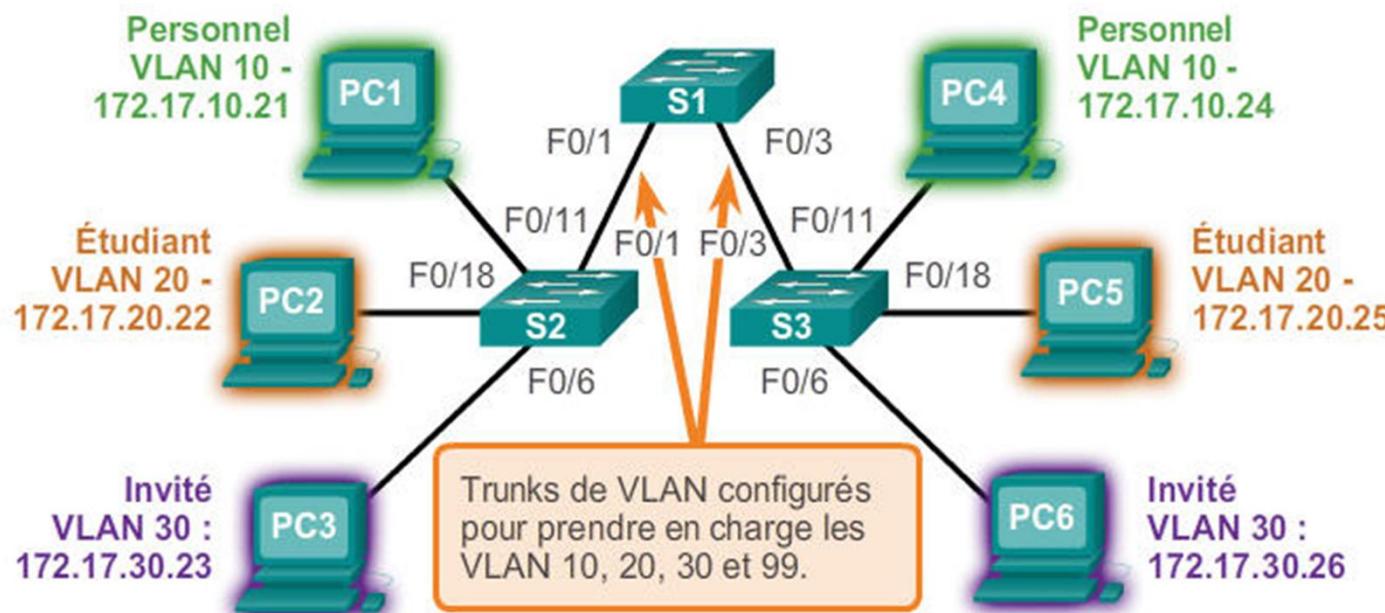
Contrôle des domaines de diffusion à l'aide des VLAN

- Les VLAN peuvent être utilisés pour limiter la portée des trames de diffusion.
- Un VLAN est un domaine de diffusion à part entière.
- Par conséquent, une trame de diffusion envoyée par un périphérique d'un VLAN donné est transmise au sein de ce VLAN uniquement.
- Cela permet de contrôler la portée des trames de diffusion et leur impact sur le réseau.
- Les trames de monodiffusion et de multidiffusion sont également transmises dans le VLAN d'où elles ont été émises.

VLAN à commutateurs multiples: Trunks de VLAN

VLAN 10 Personnel - 172.17.10.0/24
VLAN 20 Étudiants - 172.17.20.0/24
VLAN 30 Invité - 172.17.30.0/24
VLAN 99 Gestion et natif - 172.17.99.0/24

F0/1-5 sont des interfaces de trunk 802.1Q avec le VLAN 99 comme VLAN natif.
F0/11-17 se trouvent dans le VLAN 10 .
F0/18-24 se trouvent dans le VLAN 20.
F0/6-10 se trouvent dans le VLAN 30.



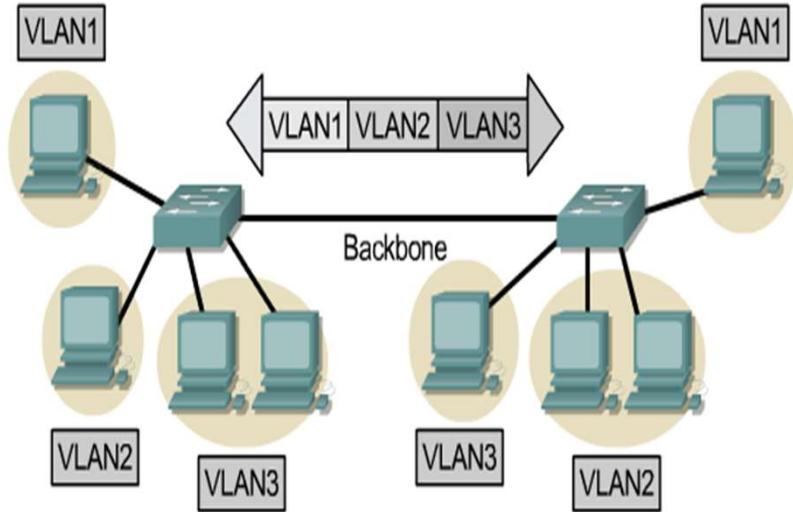
Étiquetage des trames Ethernet pour l'identification des VLAN

- L'étiquetage des trames est utilisé pour transmettre correctement plusieurs trames VLAN via une liaison trunk.
- Les commutateurs étiquettent les trames pour identifier le VLAN auquel elles appartiennent. Il existe différents protocoles d'étiquetage, IEEE 802.1q étant le plus répandu.
- Le protocole définit la structure de l'en-tête d'étiquetage ajouté à la trame.
- Les commutateurs ajouteront des étiquettes VLAN aux trames avant de les placer dans les liaisons trunk. Ils les enlèveront avant de transmettre les trames via les autres ports (non trunk).
- Une fois qu'elles sont correctement étiquetées, les trames peuvent traverser n'importe quel nombre de commutateurs via les liaisons trunk. Elles resteront dans le VLAN approprié pour atteindre leur destination.

Agrégation 802.1 Q

Trame Ethernet modifiée

adresse MAC dst.	adresse MAC src.	Tag (inséré)	Len/Etype	Data	FCS (modifié)
------------------	------------------	--------------	-----------	------	---------------



- Le commutateur reçoit une trame sur un port configuré en mode accès
- Il décompose la trame et insère une étiquette VLAN
- Il recalcule la séquence de contrôle de trame, puis envoie la trame étiquetée via un port d'agrégation.
- À la réception de la trame étiquetée, le commutateur repaire les machines concernées par la trame, élimine l'étiquette et leur envoie la trame.

Création d'un VLAN

Commandes IOS de commutateur Cisco

Passez en mode de configuration globale.

```
S1#configure terminal
```

Créez un VLAN avec un numéro d'identité valide.

```
S1(config)# vlan vlan-id
```

Indiquez un nom unique pour identifier le VLAN.

```
S1(config-vlan)# name vlan-name
```

Repassez en mode d'exécution privilégié.

```
S1(config-vlan)# end
```

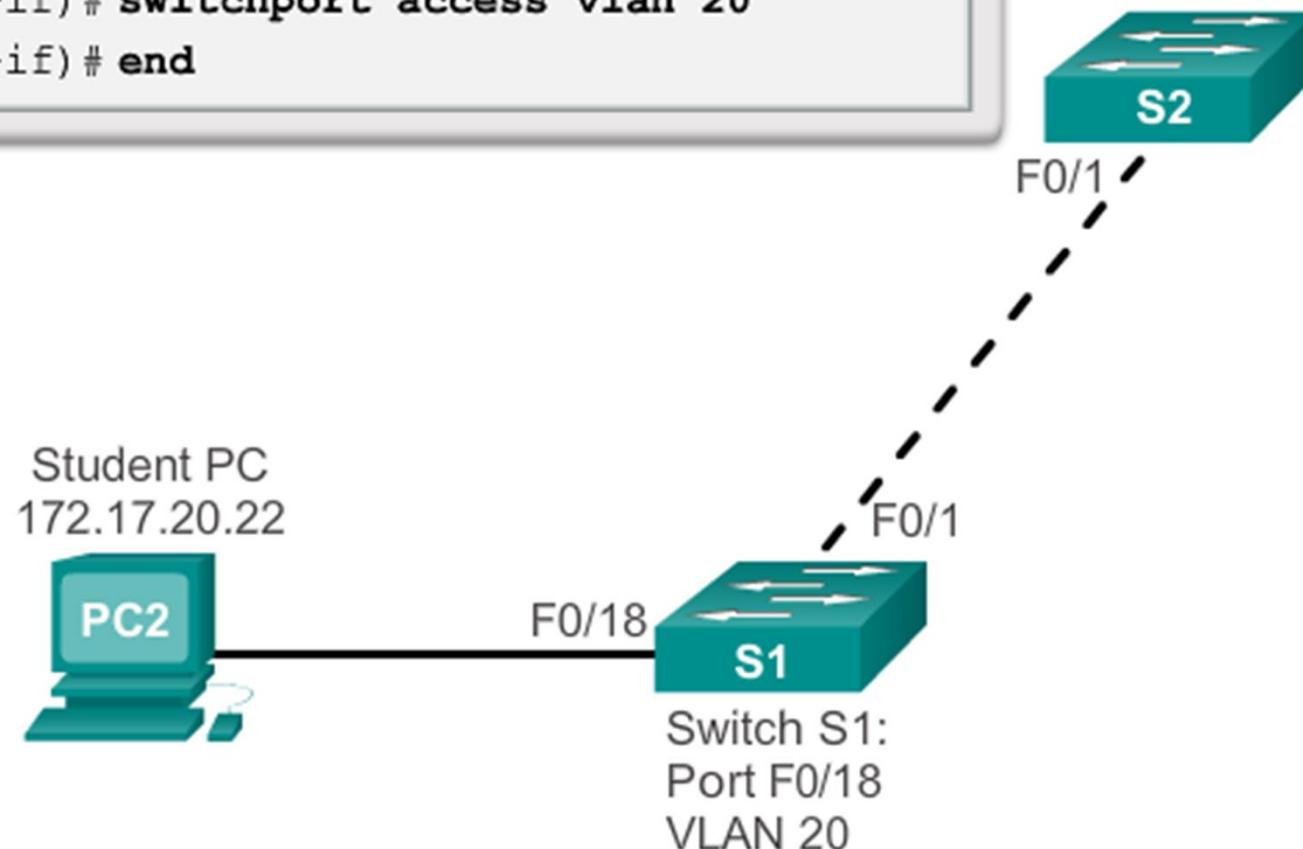
Attribution de ports aux VLAN

Commandes IOS de commutateur Cisco

Passez en mode de configuration globale.	S1# configure terminal
Passez en mode de configuration d'interface pour SVI.	S1 (config)# interface interface_id
Définissez le port en mode d'accès.	S1 (config-if) # switchport mode access
Affectez le port à un réseau local virtuel.	S1 (config-if) # switchport access vlan vlan_id
Repassiez en mode d'exécution privilégié.	S1 (config-if) # end

Attribution de ports aux VLAN

```
s1# configure terminal  
s1(config)# interface F0/18  
s1(config-if)# switchport mode access  
s1(config-if)# switchport access vlan 20  
s1(config-if)# end
```



Modification de l'appartenance des ports aux VLAN

```
S1# config t
S1(config)# int fa0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
S1#
S1# show vlan brief

VLAN Name          Status      Ports
---- -----
1    default        active     Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/12, Fa0/13
                           Fa0/14, Fa0/15, Fa0/16, Fa0/17
                           Fa0/18, Fa0/19, Fa0/20, Fa0/21
                           Fa0/22, Fa0/23, Fa0/24, Gi0/1
                           Gi0/2
20   student         active     Fa0/11
1002 fddi-default   act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default   act/unsup
S1#
```

Suppression de VLAN

```
S1# conf t  
S1(config)# no vlan 20  
S1(config)# end  
S1#  
S1# sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	
	S1#		

Vérification des informations VLAN

```

S1# show vlan name student

VLAN Name                               Status    Ports
-----+-----+-----+-----+-----+-----+-----+-----+-----+
20   student                            active   Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----+-----+-----+-----+-----+-----+-----+-----+-----+
20   enet     100020 1500   -      -      -      -      -      0      0

Remote SPAN VLAN
-----
Disabled

Primary Secondary Type          Ports
-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

S1# show vlan summary

Number of existing VLANs	:	7
Number of existing VTP VLANs	:	7
Number of existing extended VLANs	:	0

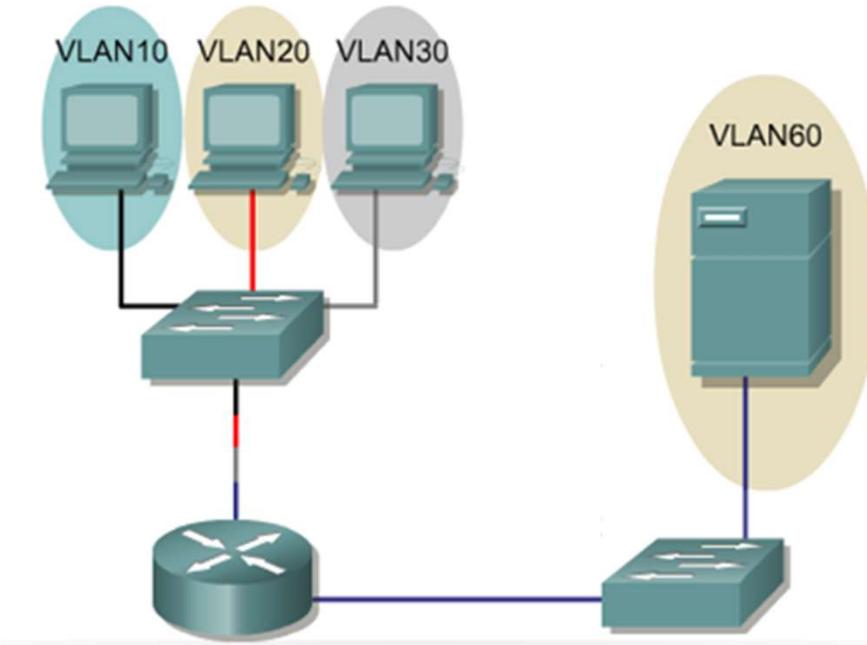
Configuration des liaisons trunk IEEE 802.1q

Commandes IOS de commutateur Cisco

Passer en mode de configuration globale.	S1# configure terminal
Passer en mode de configuration d'interface pour SVI.	S1(config)# interface interface_id
Forcer la liaison à devenir une liaison trunk.	S1(config-if)# switchport mode trunk
Indiquer un VLAN natif pour les trunks 802.1Q non étiquetés.	S1(config-if)# switchport trunk native vlan vlan_id
Indiquer la liste des VLAN autorisés sur la liaison trunk.	S1(config-if)# switchport trunk allowed vlan vlan-list
Repasser en mode d'exécution privilégié.	S1(config-if)# end

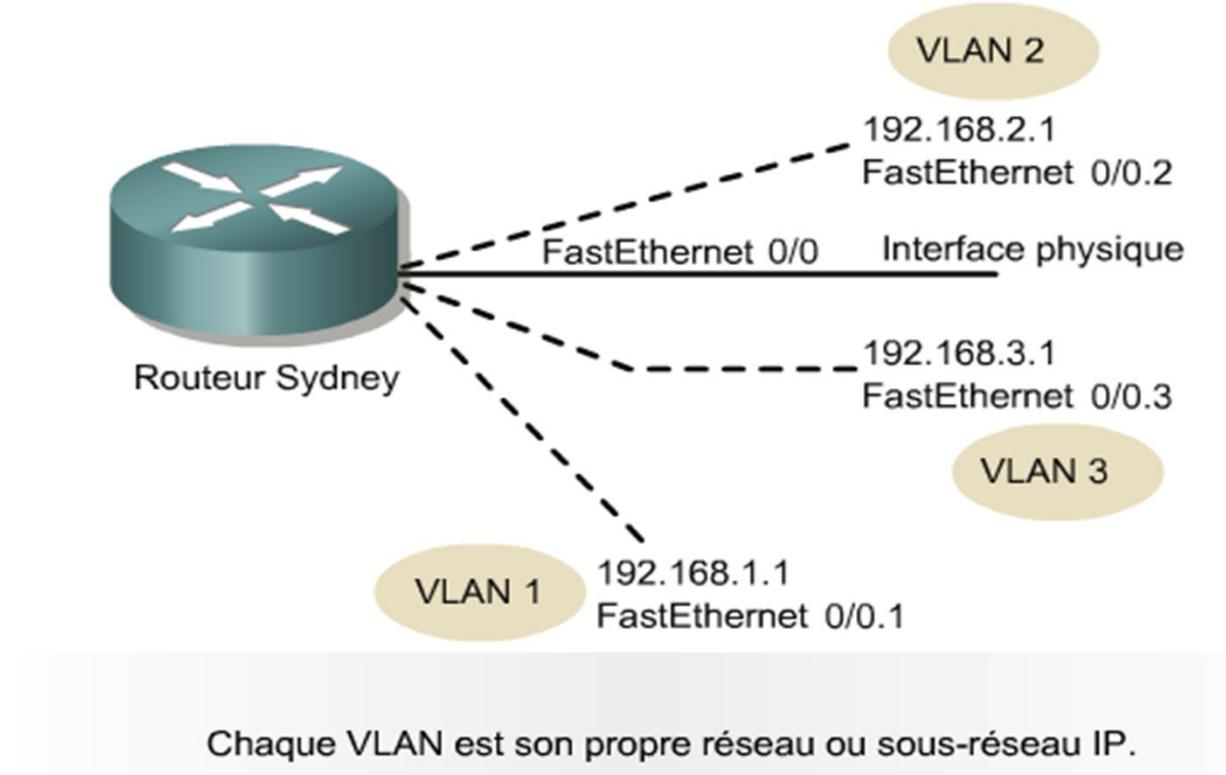
```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Routage Inter-Vlan



Une liaison agrégée 802.1Q prend en charge plusieurs Vlans en utilisant une seule interface physique mais plusieurs interfaces logiques

Sous interfaces et Vlans



Comparaison d'interface et de sous interfaces de routeur

Interface physique	Sous-interface
Une interface physique par VLAN	Une interface physique pour de nombreux VLAN
Aucun conflit de bande passante	Conflit de bande passante
Connectée au port de commutateur en mode d'accès	Connectée au port de commutateur en mode d'agrégation
Plus coûteuse	Moins coûteuse
Configuration de connexion plus complexe	Configuration de connexion moins complexe

Configuration de sous-interface d'un routeur

Routeur R1

```
R1(config)# interface g0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0
R1(config-subif)# exit
```

```
R1(config)# interface g0/1.20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0
R1(config-subif)# exit
```

```
R1(config)# interface g0/1
R1(config-if)# no shutdown
```