

3 Concepts et configuration de base de la commutation

3.1 Configuration de la sécurité des commutateurs

3.1.1 Outils de sécurité

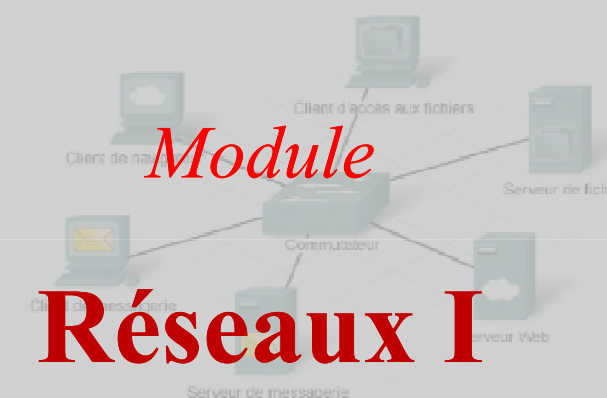
**Fonctions des outils de sécurité réseau**

Un réseau sécurisé est véritablement un processus et non un produit. Vous ne pouvez pas simplement activer un commutateur et dire que le tour est joué. Pour affirmer que votre réseau est sécurisé, vous devez disposer d'un programme de sécurité réseau exhaustif qui définit comment vous pouvez vérifier régulièrement que votre réseau est capable de faire face aux dernières attaques malveillantes. Le caractère évolutif des risques de sécurité implique le recours impératif à des outils d'audit et de pénétration que vous pouvez mettre à jour face aux risques les plus récents. Les fonctions courantes d'un outil de sécurité réseau moderne incluent notamment les éléments suivants :

- Identification de service : les outils sont utilisés dans le but de cibler des hôtes au moyen des numéros de ports [IANA Internet Assigned Numbers Authority](#). Ces outils doivent également être capables de détecter un serveur FTP exécuté sur un port non standard ou sur un serveur Web fonctionnant sur le port 8080. Ils doivent pouvoir aussi tester tous les services en cours d'exécution sur un hôte.
- Prise en charge des services SSL : évaluation

CCNA Exploration

Commentation de réseau local et réseau local sans fil



**Module**

**Réseaux I**

Placez le pointeur de la souris sur les différents services client et serveur pour en afficher une brève description.

**Fatma Rouissi**

Cisco Networking Academy<sup>®</sup>

Mind Wide Open<sup>™</sup>



## *Chapitre 3*

# **Concepts de base et configuration des commutateurs**



# Généralités sur les réseaux locaux

---



- **Fonctionnalités d'un commutateur**
- **Fonctions d'un commutateur dans un réseau hiérarchique**
- **Commutateurs pour petites & moyennes entreprises**
- **Transmission de trames au moyen d'un commutateur**
- **Configuration de la gestion des commutateurs**
- **Configuration de la sécurité des commutateurs**



# Chapitre 2

---



## Fonctionnalités d'un commutateur

## Commutateurs de configuration fixe

- Configuration **fixe**
- Pas d'options supplémentaire
- Différents choix de configuration selon le nombre et les types de ports inclus

Commutateurs de configuration fixe



## Commutateurs modulaires

- Plus de **souplesse** dans leur configuration
- livrés avec des **châssis** de différentes tailles, qui permettent l'installation de plusieurs cartes d'interface modulaires, pour l'extension du réseau.

Commutateurs de configuration modulaire



## Commutateurs empilables

- interconnectés à l'aide d'un câble spécial appelé fond de panier, qui fournit un débit de bande passante élevé entre les commutateurs.
  - Technologie « **StackWise** » permet d'interconnecter jusqu'à 9 commutateurs
- Des câbles connectant les commutateurs en chaîne, fonctionnent comme un **unique commutateur** plus important
- utilisent un **port spécial** pour les interconnexions et pas de ports de ligne pour les connexions entre commutateurs.
- Recommandés en cas de tolérance aux pannes, disponibilité de bande passante, et limitation des ressources matérielles (commutateur modulaire très cher)

Commutateurs de configuration empilable



# Performances d'un commutateur (1)

- Étroitement liée à la capacité du commutateur à prendre en charge les exigences en matière de densité des ports, débit de transfert et bande passante du réseau.

## Densité des ports

- Correspond au **nombre de ports disponibles** sur un commutateur
- Densité de ports **élevée**  $\Leftrightarrow$  **meilleure** utilisation de l'espace et de l'alimentation électrique limités.
- Les commutateurs modulaires peuvent prendre en charge des densités de ports très élevées via l'ajout de plusieurs cartes d'interface de port de commutateur

- ❑ **Exemple : Catalyst 6500** prend en charge plus de **1000 ports** sur un seul périphérique.

Commutateur modulaire comportant jusqu'à 1000 ports ou plus



Commutateur à 24 ports



Commutateur à 48 ports



# Performances d'un commutateur (2)

## Débit de transfert

- Correspond à la capacité de traitement d'un commutateur  $\equiv$  la **quantité de données** pouvant être traitée par seconde par le commutateur.
- Si débit de transfert **trop faible**, il ne peut pas convenir à une communication à la vitesse du câble à travers l'ensemble de ses ports
  - ❑ **Vitesse du câble**  $\equiv$  débit de données que chaque port peut atteindre  
(Fast Ethernet : 100 Mbits/s, Gigabit Ethernet : 1000 Mbits/s)

Commutateur Gigabit Ethernet à 24 ports



- Commutation de trafic à 24 Go/s possible

Commutateur Gigabit Ethernet à 48 ports



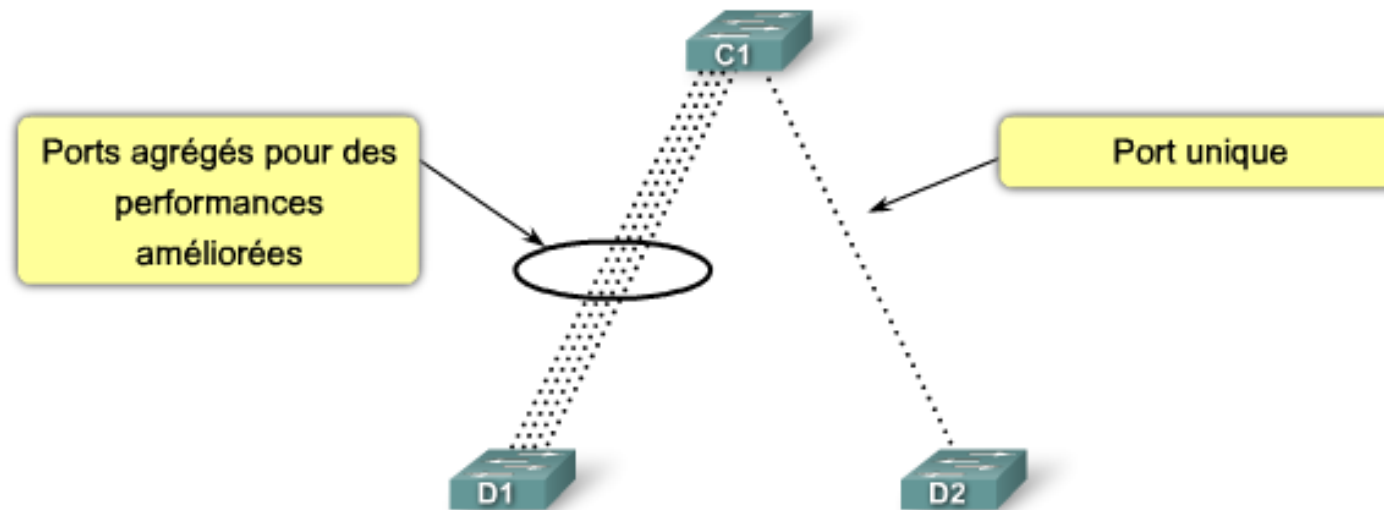
- Commutation de trafic à 48 Go/s possible



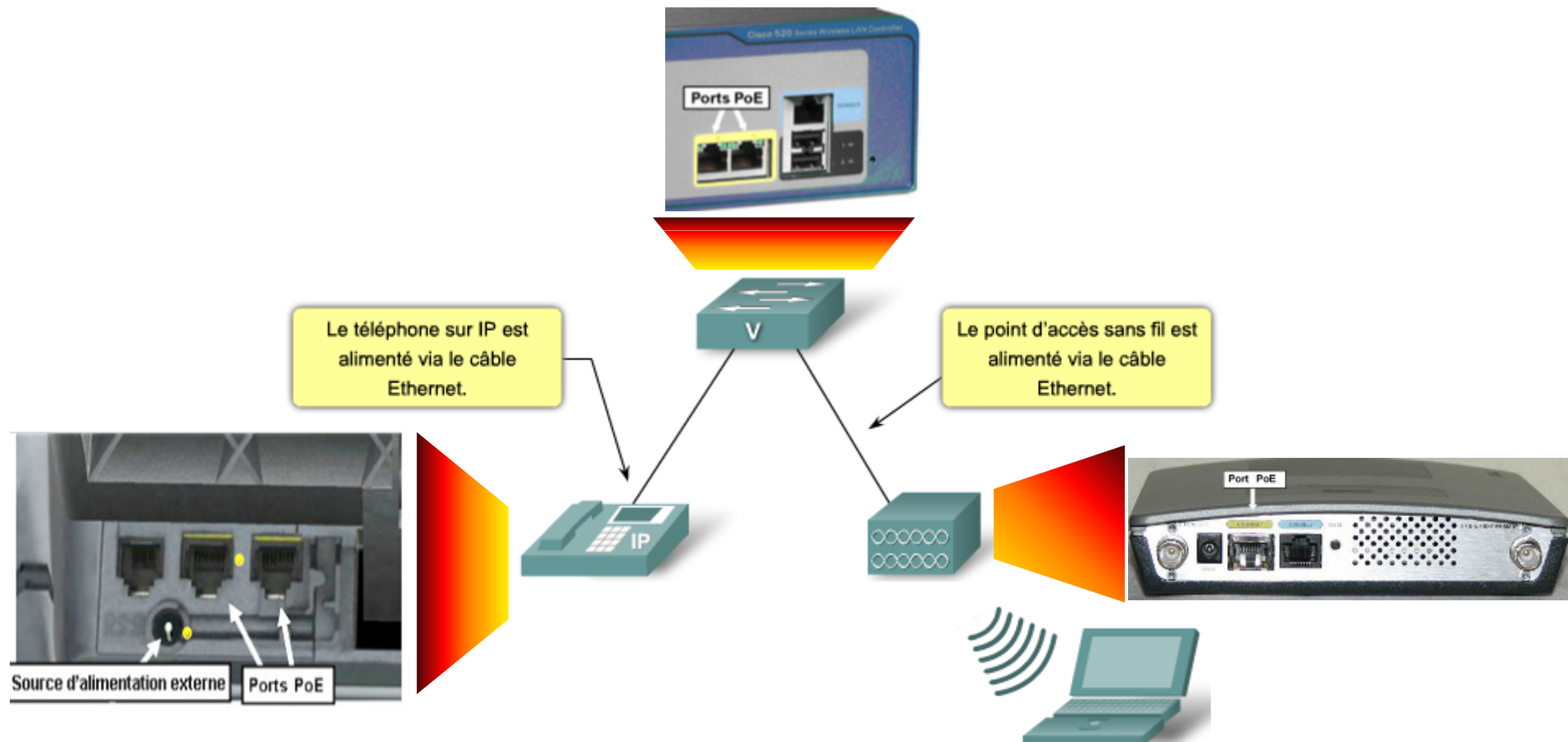
# Performances d'un commutateur (3)

## Agrégation de liaisons

- Déterminer si un commutateur à agréger dispose **d'assez de ports** pour prendre en charge la bande passante requise
  - ❑ **Exemple** : port Gigabit Ethernet, peut traiter jusqu'à 1 Gbits/s  $\Rightarrow$  si commutateur à 24 ports, possibilité de générer jusqu'à 24 Gbits/s
- L'agrégation de liaisons aide à réduire les goulots d'étranglement de trafic en associant jusqu'à 8 ports de commutateur pour les communications de données.

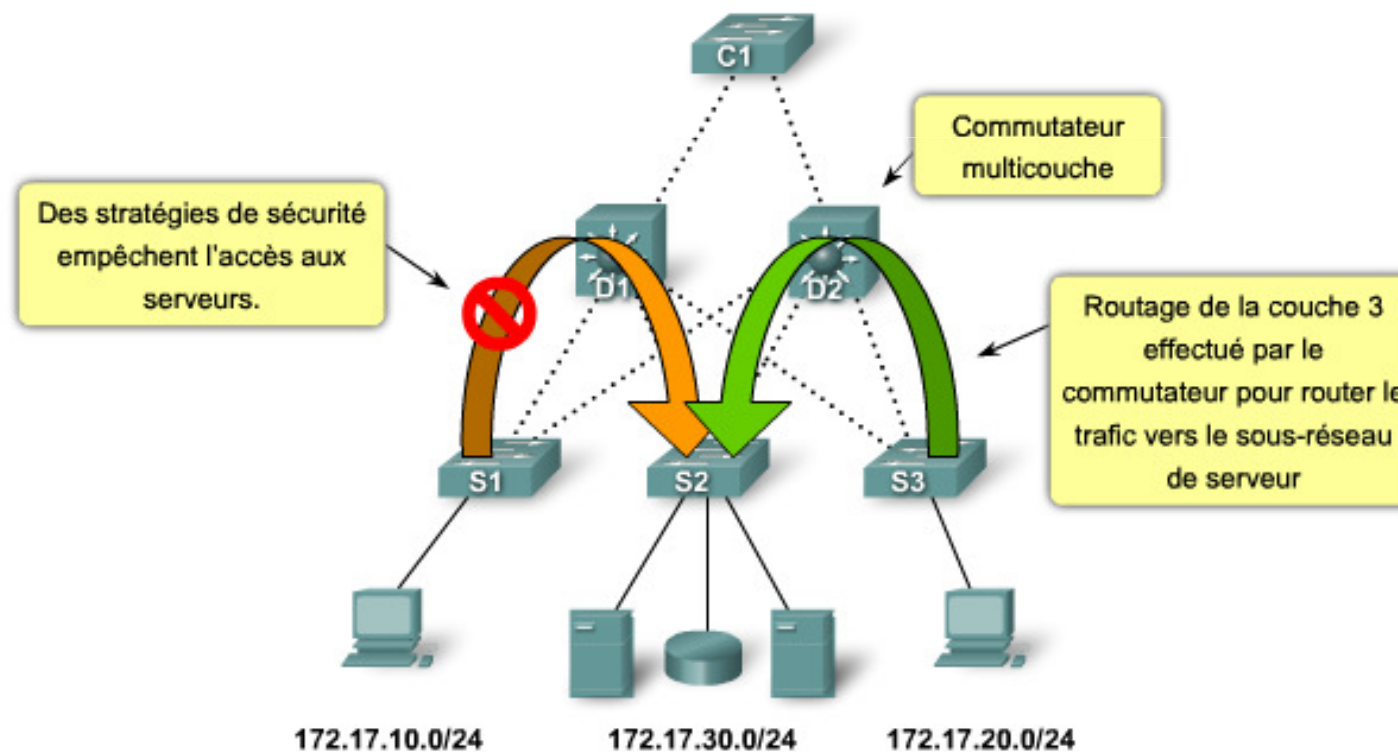


- Technologie qui permet au commutateur de fournir une alimentation à un périphérique à travers le câblage Ethernet existant ⇒ **augmente le coût du commutateur**
- Utilisé par les **téléphones sur IP** et les **points d'accès** pour plus de souplesse d'installation



# Fonctions de couche 3 pour un commutateur

- Commutateurs multicouches  $\equiv$  commutateurs de couche 3, qui offrent un ensemble de fonctionnalités supplémentaires :
  - Routage et acheminement de paquets en fonction d'adresses IP
  - Filtrage de paquets en vue de sécuriser le réseau

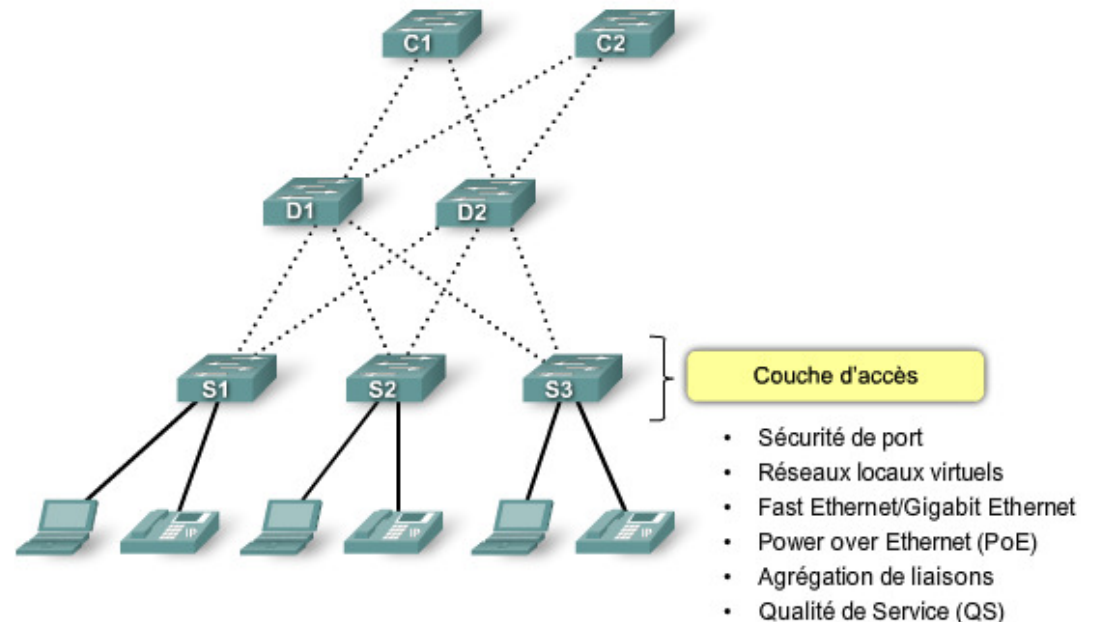




## **Fonctions d'un commutateur dans un réseau hiérarchique**

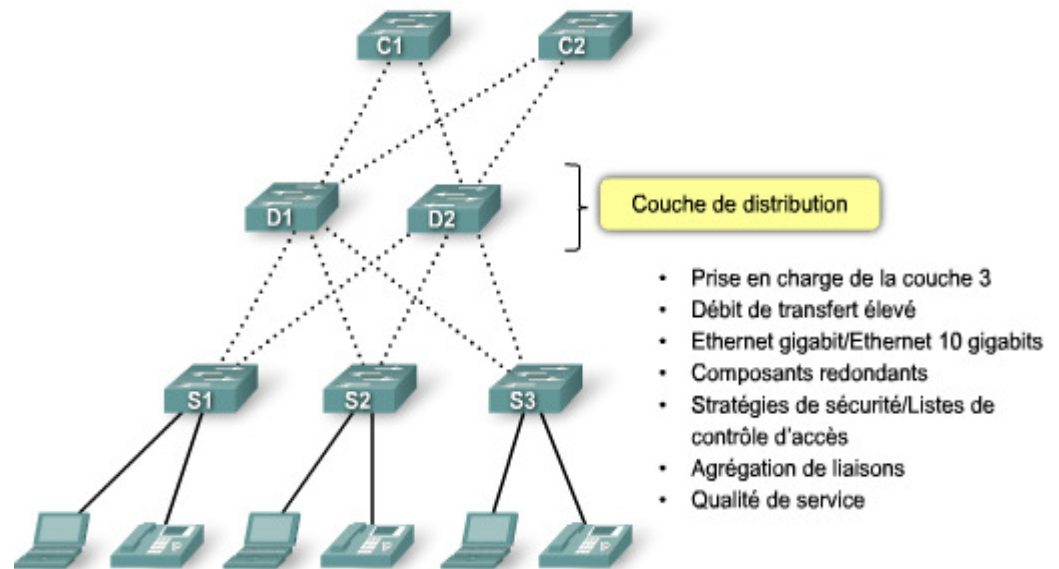
# Fonctions d'un commutateur de la couche d'accès

- Réseau **hiérarchique**  $\Rightarrow$  composé de 3 couches de base : accès, distribution & cœur
- Utilité d'identifier les besoins du commutateur selon la couche de laquelle il fait partie
- Les commutateurs de couche d'accès facilitent la connexion des nœuds d'extrémités :
- Prise en charge de :
  - **Sécurité des ports**  $\Rightarrow$  décider du nombre et des périphériques autorisés à se connecter
  - **Réseaux locaux virtuels**  $\Rightarrow$  distinguer des réseaux spécifiques pour différents types de trafic
  - **PoE**  $\Rightarrow$  ajouter une souplesse de positionnement des points d'accès et réduire le coût d'installation de l'alimentation
  - **Agrégation de liaisons**
  - **Qualité de service (Qos)**  $\Rightarrow$  conserver la hiérarchisation du trafic (priorité)



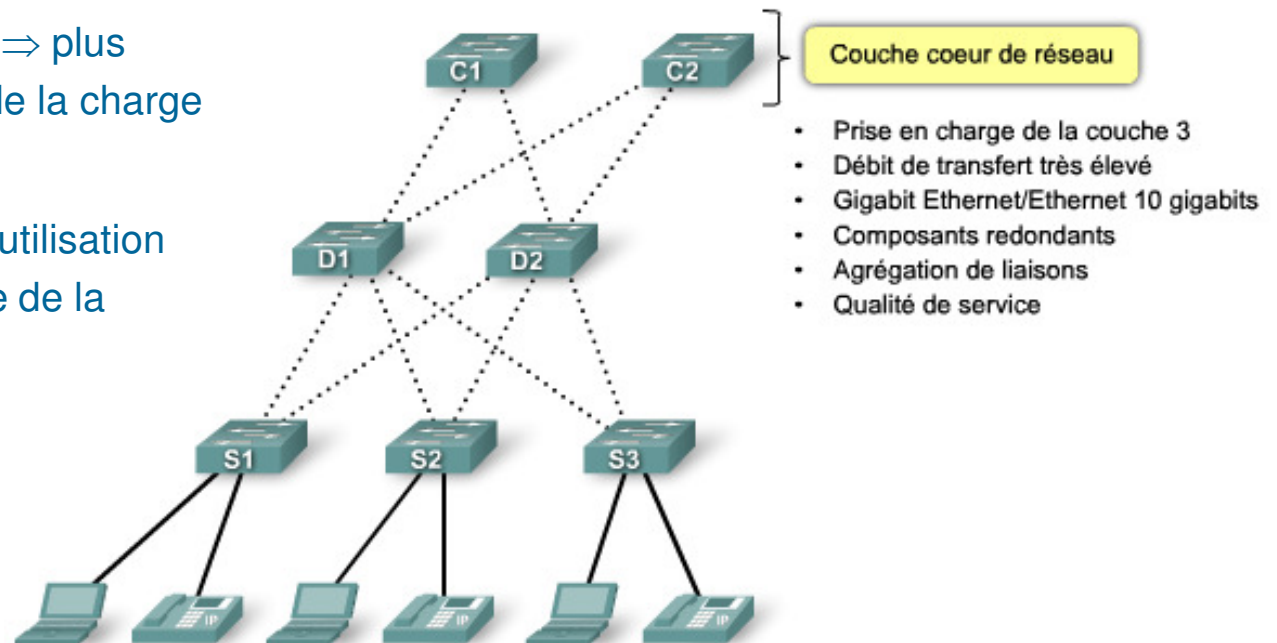
# Fonctions d'un commutateur de la couche de distribution

- Les commutateurs de couche de distribution collectent les données à partir de tous les commutateurs de la couche d'accès et les transmettent vers ceux de la couche cœur
- Prise en charge de :
  - **Routage entre VLAN** ⇒ assurer leur communication sans consommer inutilement de la bande passante.
  - **Stratégies de sécurité** ⇒ utilisation de listes de contrôle d'accès (ACL)
  - **Qualité de service** ⇒ assurer aux communications audio et vidéo l'attribution d'une bande passante adéquate
  - **Redondance** ⇒ assurer la disponibilité du réseau
  - **Agrégation de liaisons** ⇒ vers les commutateurs de couche cœur



# Fonctions d'un commutateur de la couche cœur

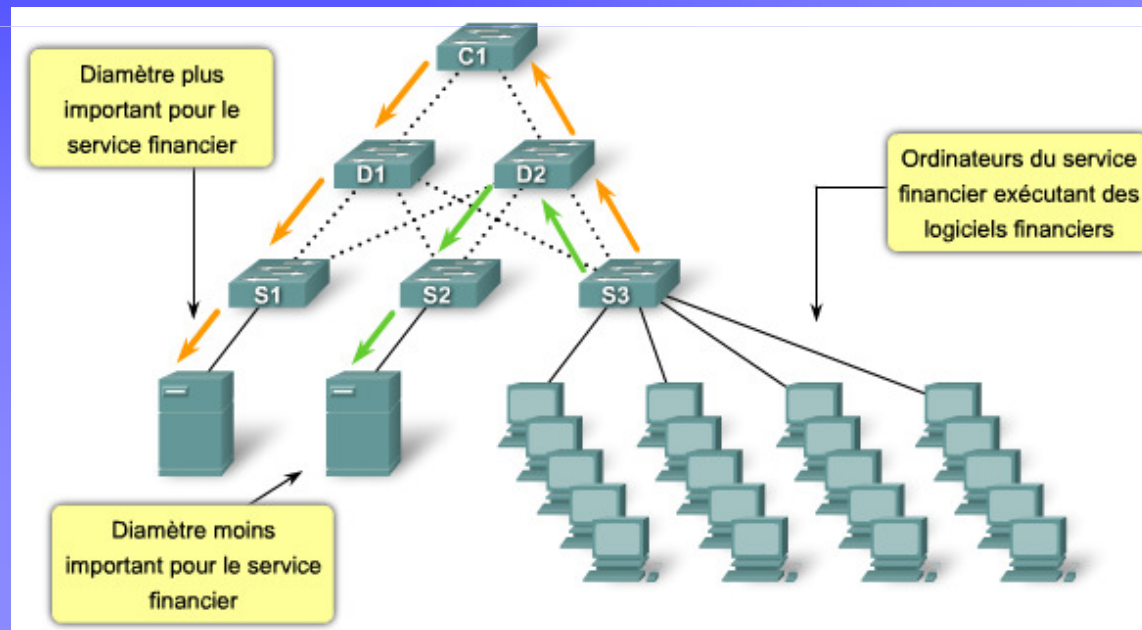
- Les commutateurs de la couche cœur doivent gérer des débits de transfert très élevés (réseau fédérateur)
- Prise en charge de :
  - **Agrégation de liaisons**  $\Rightarrow$  connexion 10 Gbits/s Ethernet agrégées est la plus rapide disponible.
  - **Redondance**  $\Rightarrow$  convergence plus rapide en cas de panne que la couche 2.
  - **Option de ventilation**  $\Rightarrow$  plus sophistiquées en vue de la charge de travail élevée
  - **Qualité de service**  $\Rightarrow$  utilisation optimale et différenciée de la bande passante





# Remarques relatives aux commutateurs sur un réseau hiérarchique (1)

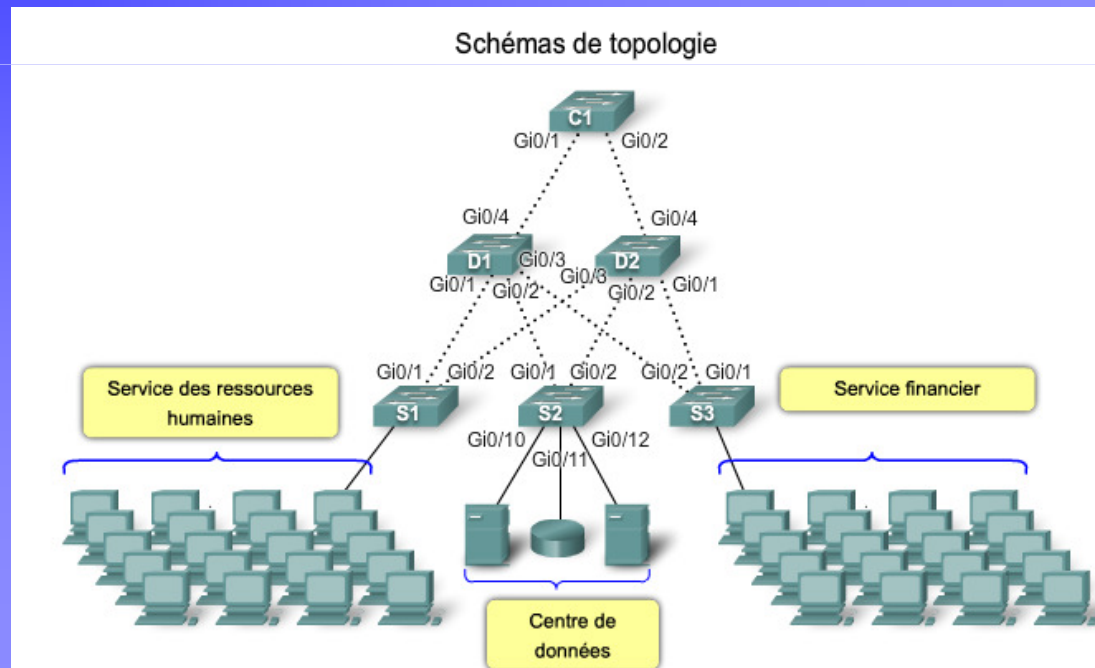
- La sélection d'un commutateur approprié à une couche nécessite les détails suivants :
  - Les flux de trafic cibles  $\Rightarrow$  l'analyse du flux de trafic permet de mesurer la bande passante à utiliser pour les données à transmettre, de régler les performances et planifier les capacités par amélioration du matériel
  - Les communautés d'utilisateurs  $\Rightarrow$  identifier les groupes d'utilisateurs et leurs impact sur les performances du réseau





# Remarques relatives aux commutateurs sur un réseau hiérarchique (1)

- Analyse de magasins et serveurs de données ⇒ serveurs, réseaux de stockage SAN, stockage en réseau NAS, unités de sauvegarde... afin de tenir compte du trafic type client-serveur, ou serveur-serveur
- Schéma de topologie ⇒ étudier la manière dont les commutateurs sont interconnectés, et configurés, la densité des périphériques et les communautés d'utilisateur, ainsi que les goulots d'étranglement





# Chapitre 2

---



## **Commutateurs pour petites et moyennes entreprises**



# Fonctions des commutateurs

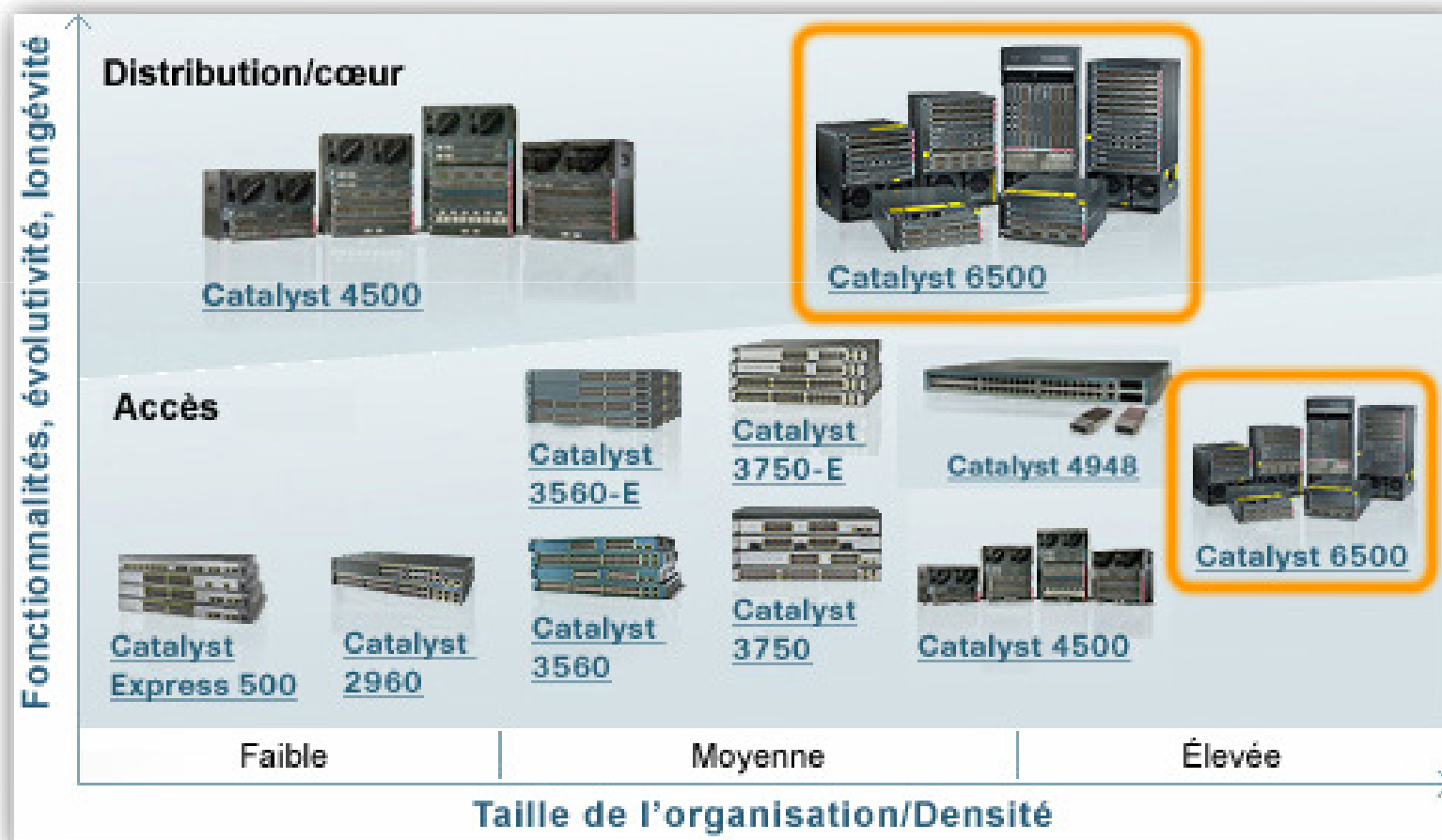
## Cisco Catalyst (1)



- Sept gammes de commutateurs proposées par Cisco  $\Leftrightarrow$  dépendance avec les exigences fonctionnelles du réseau :
  - ❑ **Catalyst Express 500**  $\Rightarrow$  des débits de transfert de **8,8 Gbits/s** à **24 Gbits/s**, et des ports jusqu'à **24**
  - ❑ **Catalyst 2960**  $\Rightarrow$  des débits de transfert **entre 16 et 32 Gbits/s**, ILC Cisco et gestion basé sur le web, et jusqu'à **48 ports 10/100 ou 10/100/1000**
  - ❑ **Catalyst 3560**  $\Rightarrow$  des débits **entre 32 et 128 Gbits/s**, fonctions réseau avancée telles que Qos et ACL,
  - ❑ **Catalyst 3750**  $\Rightarrow$  pour des organisation de taille moyenne et succursales d'entreprises
  - ❑ **Catalyst 4500**  $\Rightarrow$  des débits de transfert **jusqu'à 136 Gbits/s**, **384 ports** à liaison montante sur fibre Fast Ethernet, des fonctions réseau avancées telles que commutation multi couche, routage IP Assisté par matériel, Qos et ACLs
  - ❑ **Catalyst 4900**  $\Rightarrow$  optimisés pour la commutation de serveur et les centre de données en leur permettant de bénéficier de débits de transfert très élevés, solution idéale pour le principal matériel de téléphonie sur IP
  - ❑ **Catalyst 6500**  $\Rightarrow$  des débits de transfert **jusqu'à 720 Gbits/s**, **1152 ports 10/100**, **577 ports 10/100/1000**, **410 ports Gigabit Ethernet SFP** (Small Form factor Pluggable), ou **64 ports 10 Gigabit Ethernet**

# Fonctions des commutateurs Cisco Catalyst (2)

## Fonctions des commutateurs Cisco Catalyst





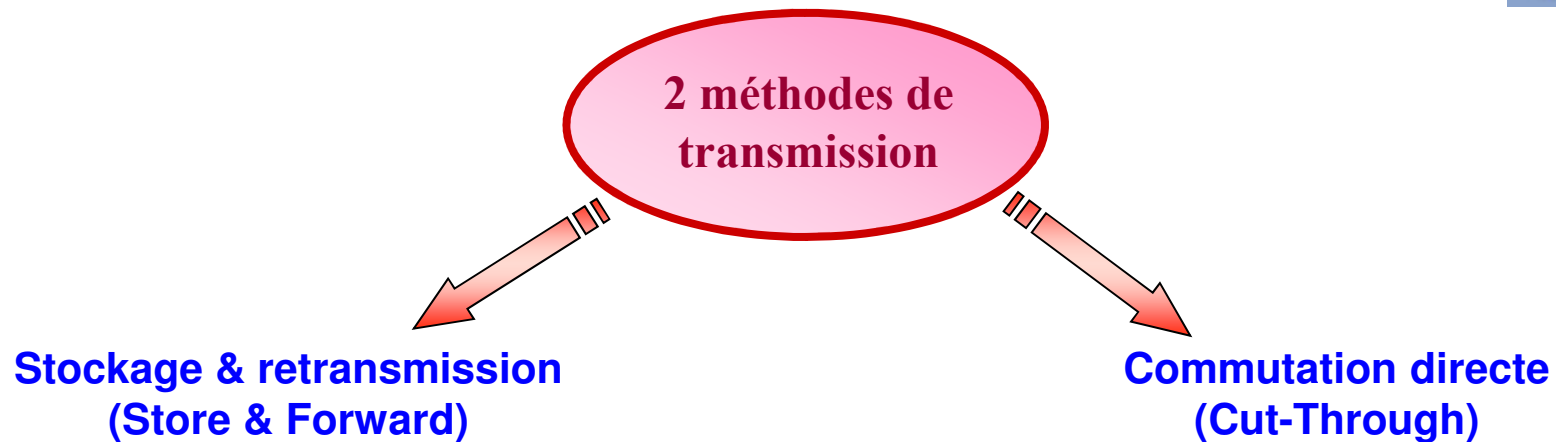
# Chapitre 2

---



## **Transmission de trames au moyen d'un commutateur**

# Méthodes de transmission par commutateur (1)



Store and Forward



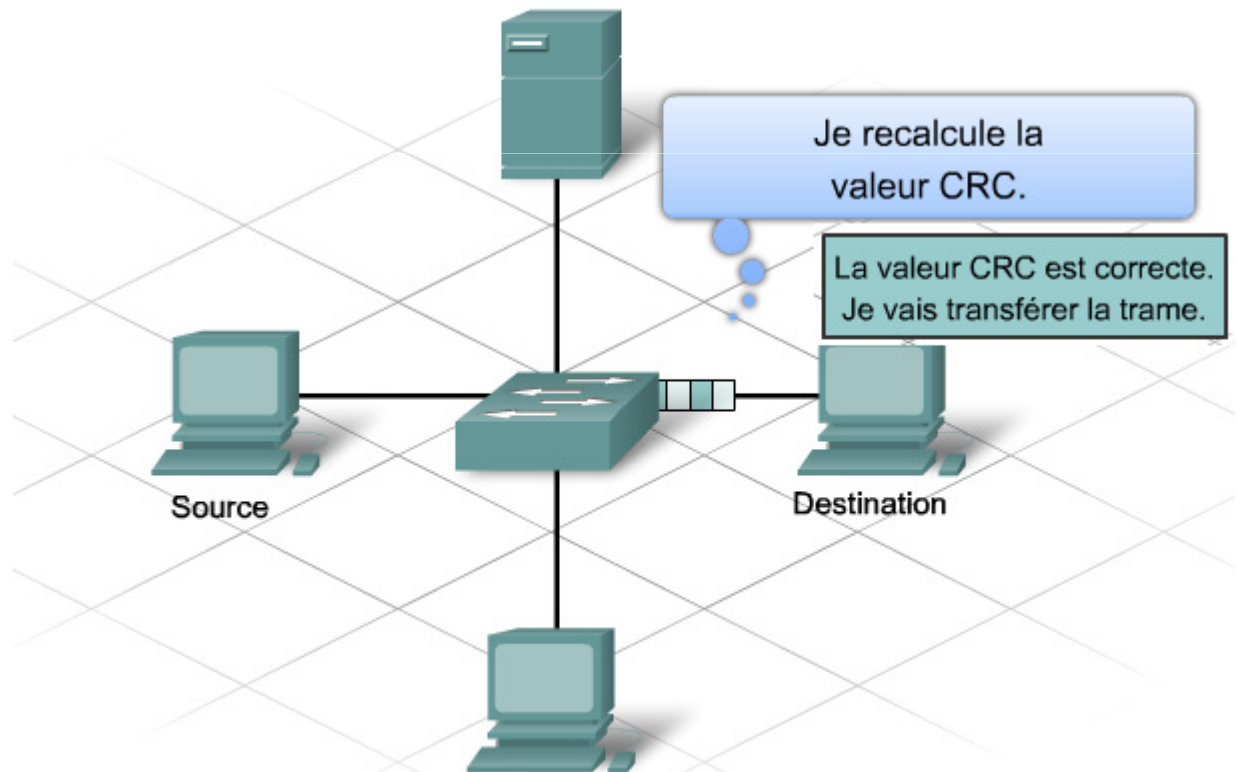
Un commutateur Store and Forward reçoit la trame entière, calcule le contrôle par redondance cyclique (CRC) et vérifie la longueur de la trame. Si le CRC et la longueur de la trame sont admis, le commutateur recherche l'adresse de destination qui détermine l'interface de sortie. La trame est ensuite acheminée par le port approprié.

Cut-through



Un commutateur cut-through achemine la trame avant qu'elle ne soit entièrement reçue. Au minimum, l'adresse de destination de la trame doit être lue avant que celle-ci ne soit retransmise.

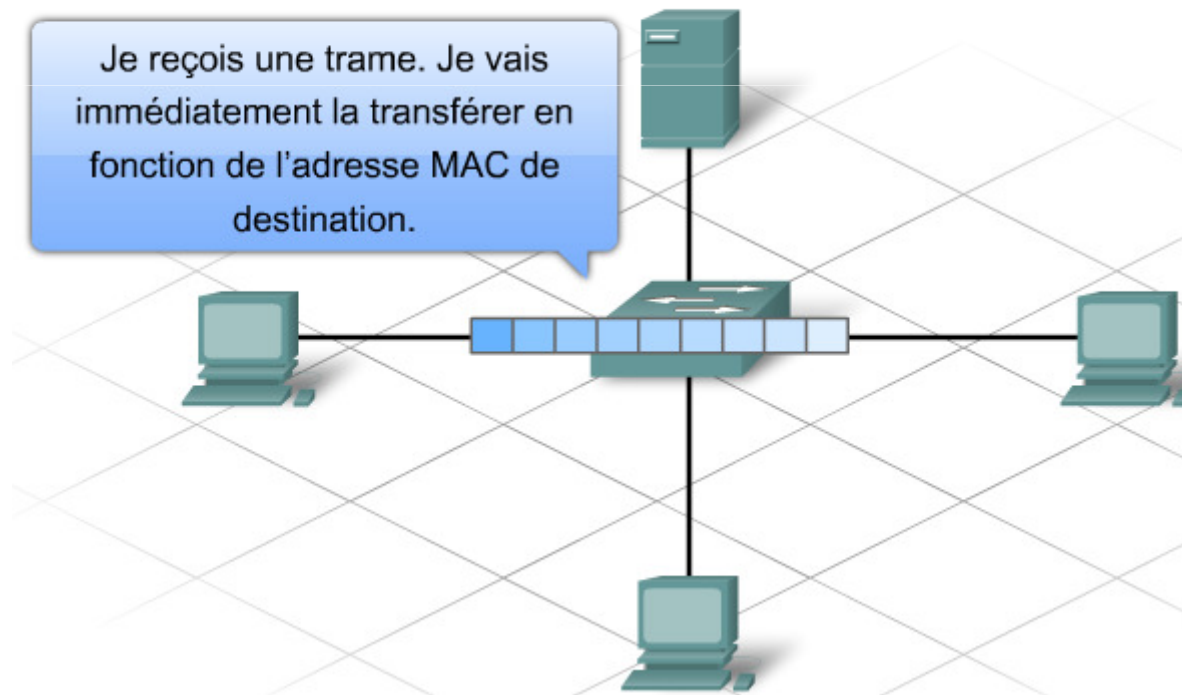
- Stocker les données dans la **mémoire tampon** du commutateur, jusqu'à la réception de la totalité de la trame
- Calcul du **CRC** et vérification avec l'en-queue de la trame Ethernet :
  - ❑ Si l'**intégralité** de la trame **confirmée** ⇒ le commutateur recherche l'**@Des** en consultant la **table MAC**, et la trame est ensuite acheminée par le port approprié
  - ❑ Si **erreur** ⇒ trame ignorée
- Nécessaire pour l'analyse de la Qos sur des réseaux convergeant où la classification des trames pour la priorité du trafic est indispensable
  - ❑ **Exemple** : flux de données de voix est prioritaire sur trafic Web



- 2 variantes : Fast-Forward & Fragment-Free

## Fast-Forward

- Transmettre immédiatement suite à la lecture de l'*@Dest*
- Niveau de latence très faible
- Aucun contrôle d'erreur (la destination ignore la trame si erronée)

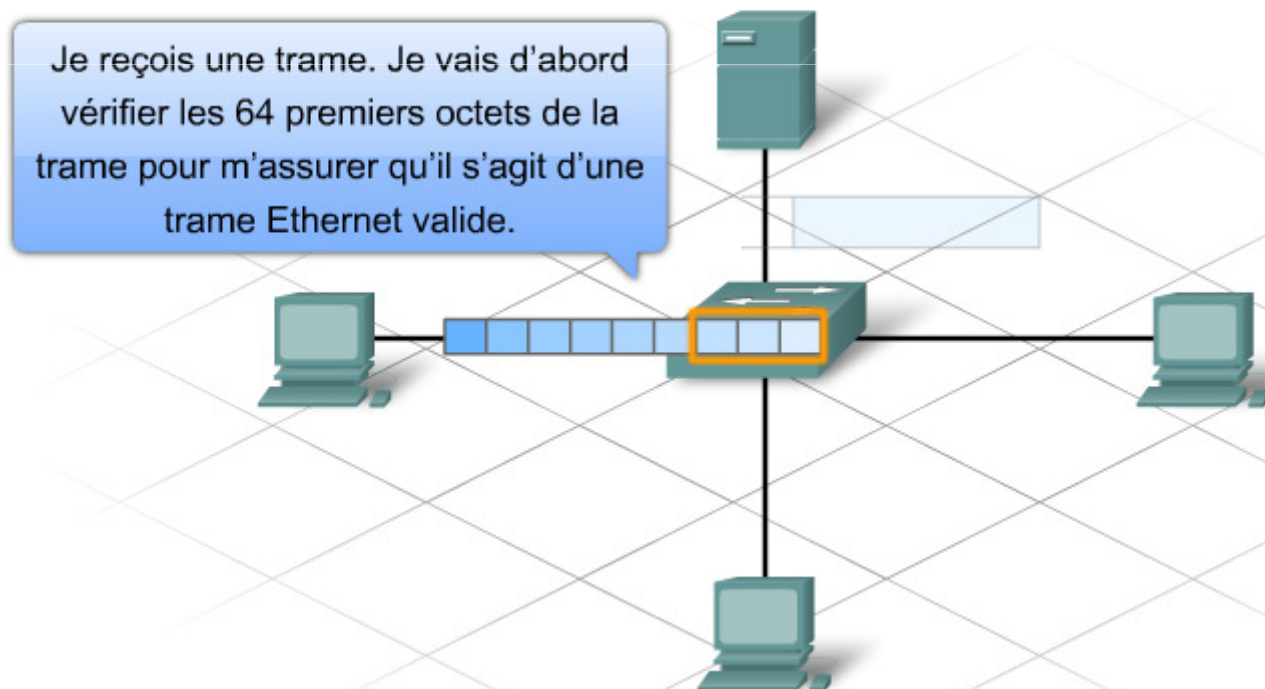




- 2 variantes : Fast-Forward & Fragment-Free

## Fragment-Free

- Stocker les 64 premiers octets avant de transmettre
- Contrôler l'erreur uniquement sur ces 64 premiers octets (où plus de possibilité d'erreurs)
- Compromis entre Store & Forward et Cut-Through



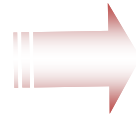


# Commutation symétrique/asymétrique (1)



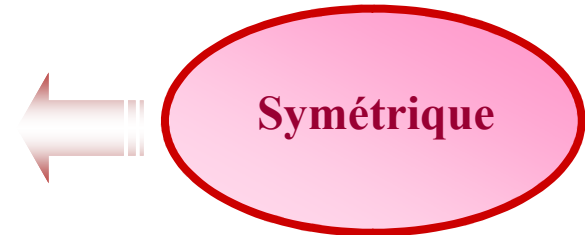
- La manière la bande passante aux ports du commutateur

Asymétrique



- Faire correspondre divers débits de données sur des ports différents,
- Dédier un volume de bande passante plus important au port de commutateur d'un serveur afin d'éviter tout goulot d'étranglement.
  - Trafic plus fluide si plusieurs clients communiquent simultanément avec le même serveur
- Conservation des trames entières dans la mémoire tampon et déplacement vers le port l'une après l'autre selon les besoins.

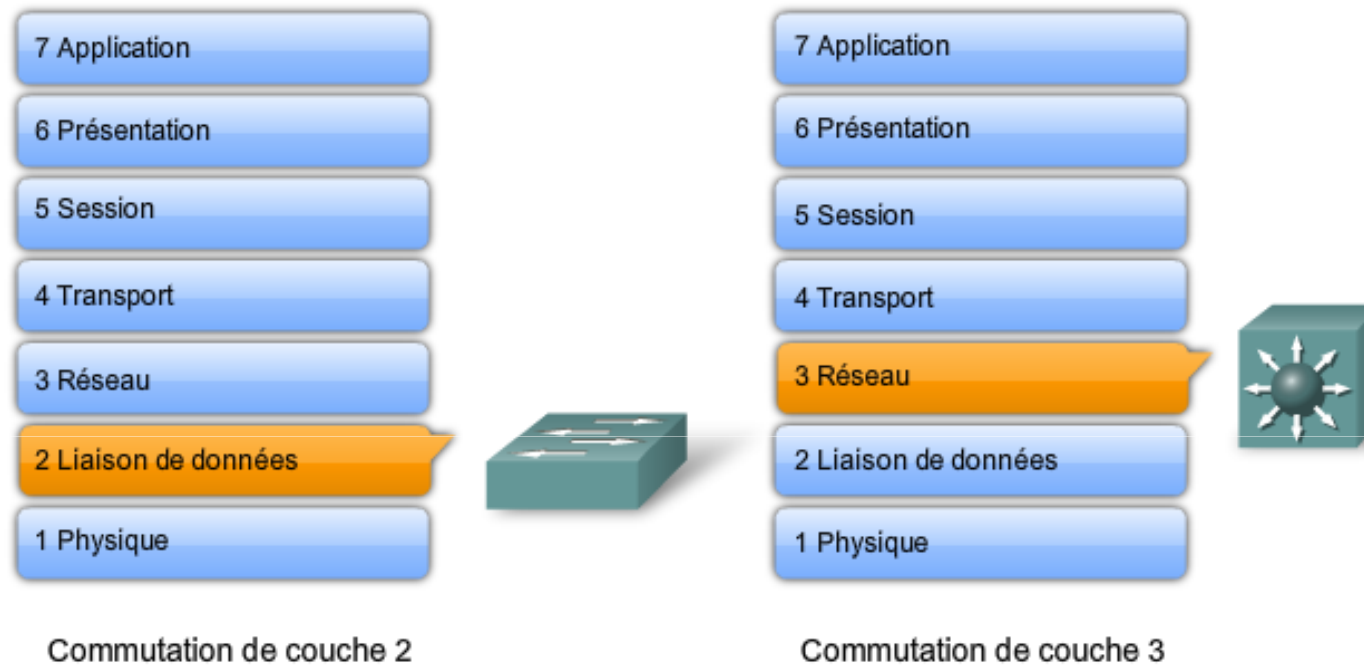
- Tous les ports disposent de la même bande passante
- Optimisée pour une charge de trafic raisonnablement distribuée
  - ❑ Exemple : environnement Peer-to-Peer



- Deux méthodes de mise en mémoire tampon :
  - **Axée sur les ports** ⇒ les trames sont stockées dans des files d'attente liés à des ports entrants et sortant spécifiques
  - **Mémoire partagée** ⇒ les trames sont stockées dans une mémoire commune à tous les ports
    - Permet la réception d'une trame sur un port et sa transmission sur un autre, sans avoir à le déplacer vers une autre file d'attente
    - Existence d'une carte de liaison entre trames et ports, indiquant l'emplacement vers lequel la trame doit être acheminé
    - Taille de mémoire limitée ⇒ transmission de plus grandes trames en en supprimant un minimum

Mémoire axée sur les ports	Dans le cas de la mise en mémoire tampon axée sur les ports, les trames sont stockées dans des files d'attente liées à des ports entrants et sortants spécifiques.
Mémoire partagée	La mise en mémoire tampon partagée stocke toutes les trames dans une mémoire tampon commune à tous les ports du commutateur.

# Commutation sur les couches 2 & 3 (1)



- Commutation et filtrage en se basant uniquement sur l'**@MAC**
- transparent
- Peut exploiter les **@IP** pour décision de transmission
- Peut exécuter des **fonctions de routage**



# Commutation sur les couches 2 & 3 (2)



Caractéristique	Commutateur de couche 3	Routeur
Routage de couche 3	Compatible	Compatible
Gestion du trafic	Compatible	Compatible
Cartes WIC		Compatibles
Protocoles de routage avancés		Compatibles
Routage à vitesse filaire	Compatible	



# Chapitre 2

---



## **Configuration de la gestion des commutateurs**



# Utilisation des modes d'interface de ligne de commande (1)



**Mode d'exécution  
utilisateur & privilégié**

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passez du mode d'exécution utilisateur au mode d'exécution privilégié.	switch> <b>enable</b>
Si vous avez défini un mot de passe en mode d'exécution privilégié, le système vous demande de le saisir.	Password: <b>password</b>
L'invite # désigne le mode d'exécution privilégié.	switch#
Passez du mode d'exécution privilégié au mode d'exécution utilisateur.	switch# <b>disable</b>
L'invite > désigne le mode d'exécution utilisateur.	switch>



# Utilisation des modes d'interface de ligne de commande (2)



## Consultation des modes de configuration

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passez du mode d'exécution privilégié au mode de configuration globale.	switch# <b>configure terminal</b>
L'invite (config)# signifie que le commutateur est en mode de configuration globale.	switch(config) #
Passez du mode de configuration globale au mode de configuration d'interface pour l'interface Fast Ethernet 0/1.	switch(config) # <b>interface fastethernet 0/1</b>
L'invite (config-if)# signifie que le commutateur est en mode de configuration d'interface.	switch(config-if) #
Passez du mode de configuration d'interface en mode de configuration globale.	switch(config-if) # <b>exit</b>
L'invite (config)# signifie que le commutateur est en mode de configuration globale.	switch(config) #
Passez du mode de configuration globale au mode d'exécution privilégié.	switch(config) # <b>exit</b>
L'invite # signifie que le commutateur est en mode d'exécution privilégié.	switch#





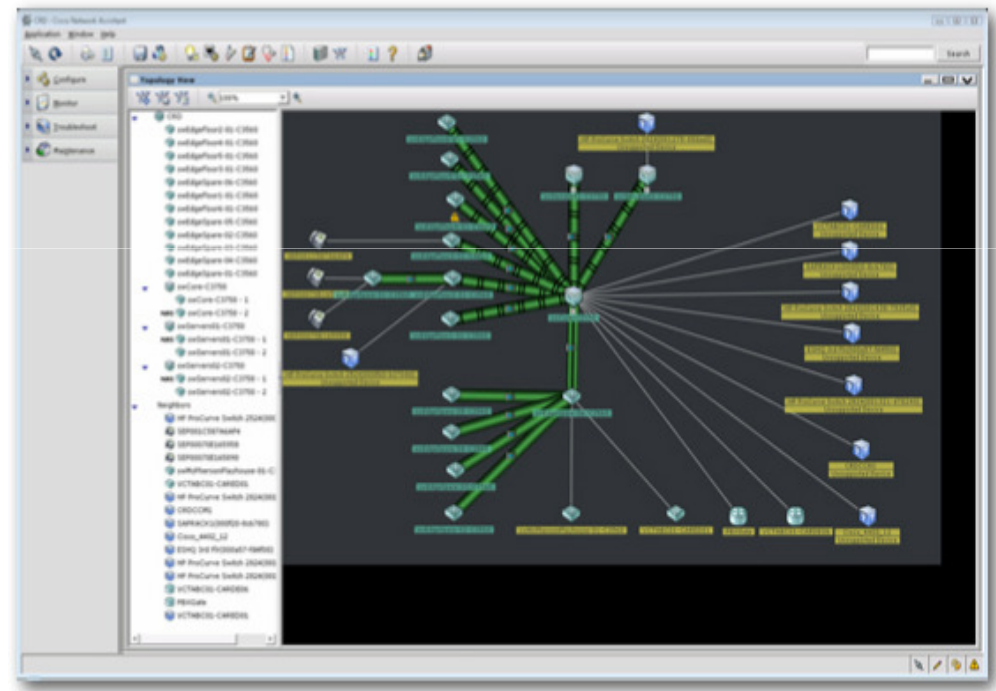
# Solutions de l'interface graphique utilisateur par rapport à l'ILC (1)



- D'autres solutions de gestion graphique pour la gestion d'un commutateur  $\Rightarrow$  solution de gestion et de configuration des commutateurs qui ne demande **aucune connaissance** approfondie de l'ILC Cisco :

## ❑ Cisco Network Assistant

- interface d'administration réseau pour PC optimisée,
- conçue pour les réseaux locaux de petite et moyenne taille.
- Permet de configurer et gérer des groupes de commutateurs ou des commutateurs autonomes.
- Disponible gratuitement et peut être téléchargé sur le site Web de Cisco



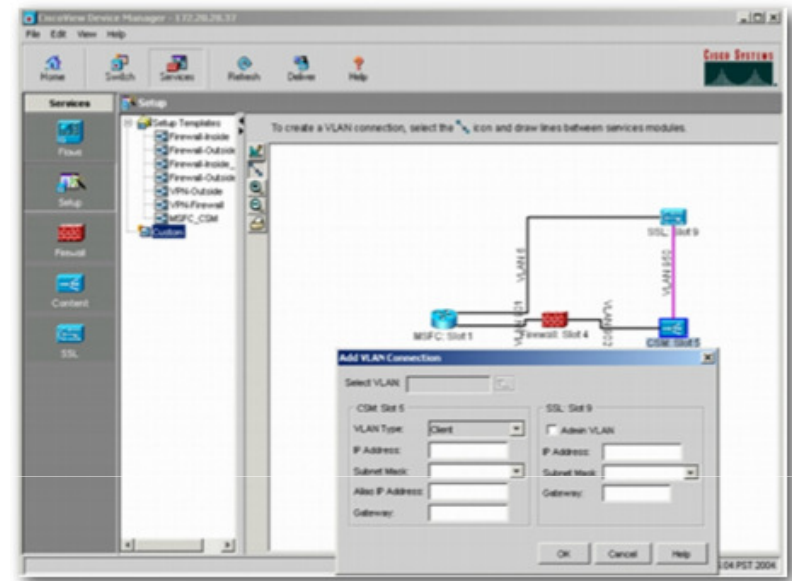


# Solutions de l'interface graphique utilisateur par rapport à l'ILC (2)



## ❑ CiscoView

- Application de gestion de périphériques avec interface qui fournit des données dynamiques sur l'état, et la configuration des périphériques Cisco
- Offre des fonctions de surveillance de périphériques et des fonctions élémentaires de dépannage
- Peut être intégré à plusieurs plateformes de gestion de réseau SNMP



## ❑ Cisco Device Manager

- Outil logiciel Web stocké dans la mémoire du commutateur.
- Permet de configurer et gérer des commutateurs.



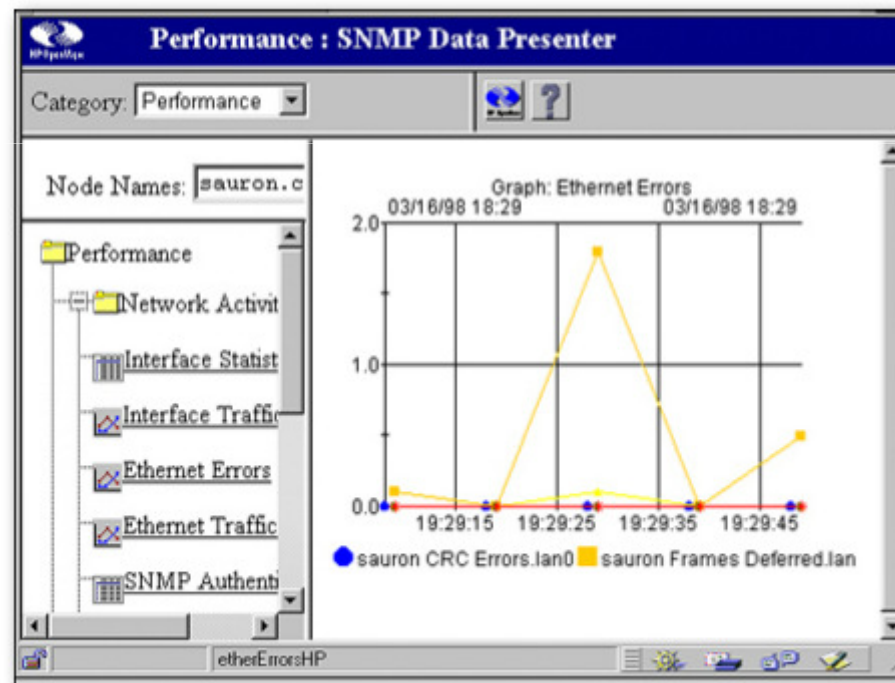


# Solutions de l'interface graphique utilisateur par rapport à l'ILC (3)



## ❑ Gestion de réseau SNMP

- Gestion des commutateurs à partir d'une station de gestion compatible SNMP, telle que HP OpenView.
- La gestion de réseau SNMP est bien plus fréquente dans des réseaux d'entreprise de très grande taille.



## Aide contextuelle

Syntaxe des commandes sur un commutateur Cisco	
Exemple d'invite de commandes. Dans cet exemple, la fonction d'aide fournit une liste des commandes disponibles dans le mode actuel qui commencent par cl.	switch#cl? clear clock
Exemple de commande incomplète.	switch#clock % Incomplete command.
Exemple de traduction symbolique.	switch#colck % Unknown command or computer name, or unable to find computer address
Exemple d'invite de commandes. Vous avez remarqué l'espace ? Dans cet exemple, la fonction d'aide fournit une liste des sous-commandes associées à la commande clock.	switch#clock ? set Set the time and date
Dans cet exemple, la fonction d'aide fournit une liste des arguments de commande requis avec la commande clock set.	switch#clock set ? hh:mm:ss Current Time

Exemple de message d'erreur	Signification	Comment obtenir de l'aide
switch#cl % Ambiguous command: "cl"	Vous n'avez pas entré suffisamment de caractères pour permettre à votre périphérique de reconnaître la commande.	Entrez à nouveau la commande suivie d'un point d'interrogation (?) sans espace intermédiaire. Les mots clés que vous pouvez entrer avec la commande s'affichent.
switch#clock % Incomplete command.	Vous n'avez pas entré tous les mots clés ou les valeurs nécessaires pour cette commande.	Entrez à nouveau la commande suivie d'un point d'interrogation (?) avec un espace intermédiaire.
switch#clock set aa:12:23 ^ % Invalid input detected at '^' marker.	Vous avez mal entré la commande. L'accent circonflexe (^) marque la position de l'erreur.	Entrez un point d'interrogation (?) pour afficher toutes les commandes ou tous les paramètres disponibles.

## Messages d'erreur de la console



# Accès à l'historique des commandes



- Fonction d'historique « **show history** » permet de :
  - afficher le contenu de la mémoire tampon des commandes
  - définir la taille de la mémoire tampon de l'historique des commandes
  - rappeler les commandes entrées précédemment et stockées dans la mémoire tampon de l'historique
- mémoire tampon pour chaque mode de configuration

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Active l'historique du terminal. Vous pouvez exécuter cette commande en mode utilisateur ou en mode d'exécution privilégié.	switch# <b>terminal history</b>
Configure la taille de l'historique du terminal. L'historique du terminal peut conserver entre 0 et 256 lignes de commande.	switch# <b>terminal history size 50</b>
Rétablit la taille de l'historique du terminal d'après sa valeur par défaut, soit 10 lignes de commande.	switch# <b>terminal no history size</b>
Désactive l'historique du terminal.	switch# <b>terminal no history</b>



# Séquence d'amorçage des commutateurs



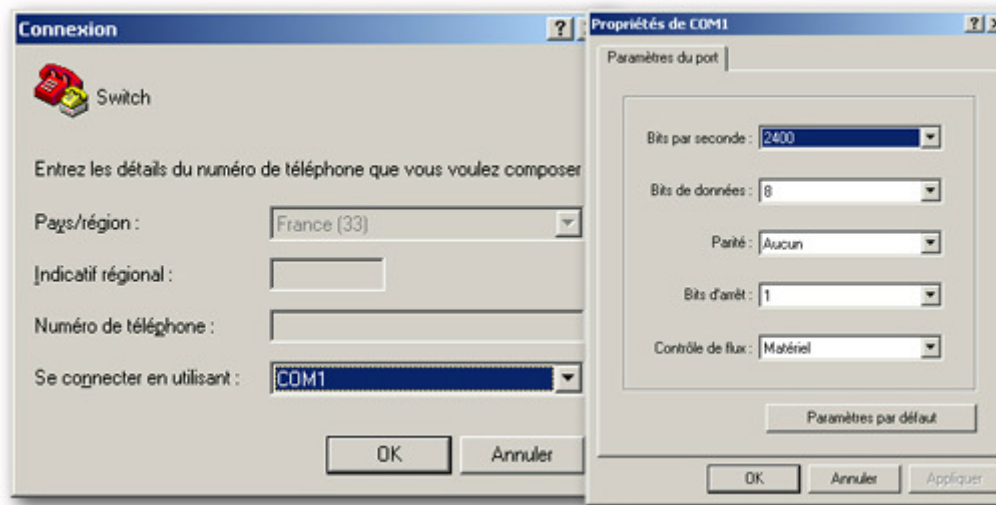
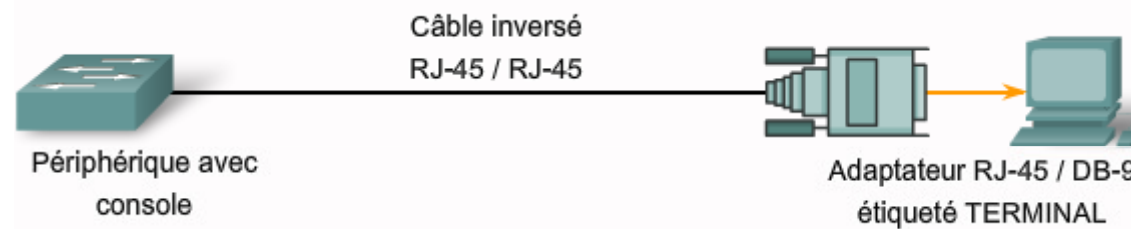
- Le commutateur exécute le logiciel du chargeur d'amorçage à partir de la **mémoire vive non volatile (NVRAM)**
- Le chargeur d'amorçage effectue les opérations suivantes :
  - **initialisation** de l'unité centrale (UC) à un faible niveau
  - Test automatique de mise sous tension (**POST**) pour le sous-système de l'UC
  - **Initialisation** du système de fichiers flash sur la carte système
  - **Chargement** de **l'image du logiciel** de système d'exploitation par défaut dans la mémoire et **amorçage** du commutateur
- Le système d'exploitation est exécuté à l'aide du fichier « **config.txt** » stocké dans la **mémoire flash** du commutateur
- Le chargeur d'amorçage facilite **la récupération** après une panne du système d'exploitation :
  - **Accès au commutateur** si le système d'exploitation est défaillant
  - **Accès aux fichiers stockés** dans la mémoire flash avant le chargement du système d'exploitation
  - **Appel à la ligne de commande** du chargeur d'amorçage pour procéder à des opérations de récupération



# Préparation de la configuration du commutateur (1)

## Etapes de démarrage d'un commutateur

- **Etape 1 :** vérification des câbles réseau, de la connexion du terminal au port de la console et de la configuration du logiciel émulateur



Configuration de l'**HyperTerminal**

# Préparation de la configuration du commutateur (2)

## Etapes de démarrage d'un commutateur

- **Etape 2 :** branchement de la fiche du câble d'alimentation dans la prise d'alimentation électrique du commutateur (les Cisco Catalyst 2960 ne disposent pas de boutons d'alimentation.)
- **Etape 3 :** observation de la séquence d'amorçage : Lorsque le commutateur est activé, le test POST démarre, où les LED clignotent tandis qu'une série de tests détermine que le commutateur fonctionne correctement, ensuite, le LED SYST clignote rapidement en vert. Si le commutateur échoue au test POST, le LED SYST devient orange. Lorsqu'un commutateur échoue au test POST, il est nécessaire de le réparer.

```
Copyright (c) 1986-2006 by Cisco Systems, Inc.  
Compiled Fri 28-Jul-06 04:33 by yenan  
Image text-base: 0x00003000, data-base: 0x00AA2F34  
flashfs[1]: 602 files, 19 directories  
flashfs[1]: 0 orphaned files, 0 orphaned directories  
flashfs[1]: Total bytes: 32514048  
flashfs[1]: Bytes used: 7715328  
flashfs[1]: Bytes available: 24798720  
flashfs[1]: flashfs fsck took 1 seconds.  
flashfs[1]: Initialization complete....done Initializing  
flashfs.  
  
POST: CPU MIC register Tests : Begin  
POST: CPU MIC register Tests : End, Status Passed  
  
POST: PortASIC Memory Tests : Begin  
POST: PortASIC Memory Tests : End, Status Passed  
  
POST: CPU MIC PortASIC interface Loopback Tests : Begin  
POST: CPU MIC PortASIC interface Loopback Tests : End, Status
```



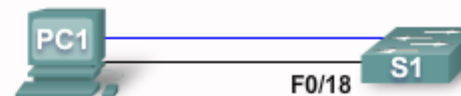
# Configuration de la connectivité IP (1)

## Considérations de gestion de l'interface

- Objectif: gérer un commutateur à distance à l'aide de TCP/IP

↳ Un commutateur de couche d'accès ressemble beaucoup à un PC ⇒ configuration d'une adresse IP, un masque de sous-réseau et une passerelle par défaut.

- **Méthode par défaut** : utilisation du réseau VLAN 1
- **Méthode recommandée** : utilisation d'un autre VLAN (exemple : VLAN 99)



### PC1 :

- Adresse IP : 172.17.99.12
- Connexion au port de console
- Connexion au port F0/18 sur le commutateur S1

### S1 :

- VLAN 99
- Réseau local virtuel de gestion
- Adresse IP : 172.17.99.11
- Port F0/18 affecté au VLAN 99

- Une adresse de couche 3 doit être affectée au commutateur pour la gestion TCP/IP.
- Le réseau local virtuel (VLAN) 1 est l'interface de gestion par défaut pour tous les commutateurs.
- L'utilisation du réseau local virtuel 1 présente des risques.
- Créez un autre réseau local virtuel (par exemple, VLAN 99 ou 150).
- Affectez ce réseau local virtuel à un port approprié (par exemple, F0/18).



# Configuration de la connectivité IP (2)



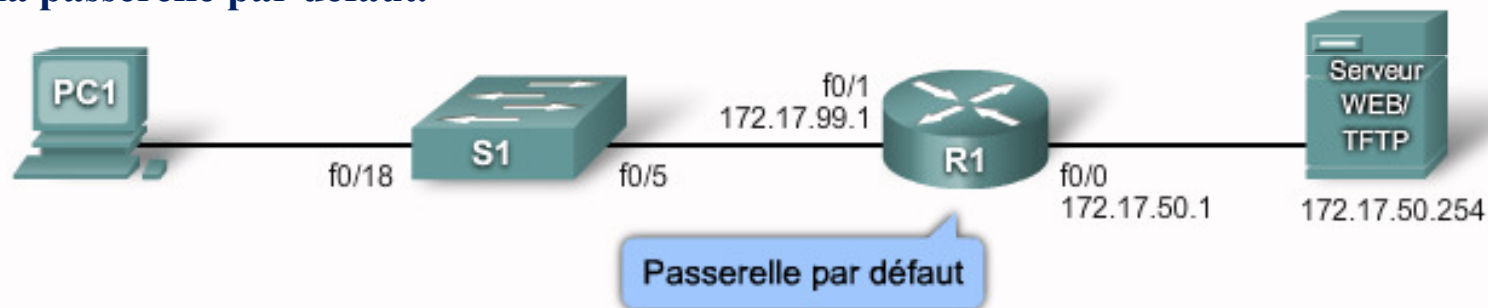
## Configuration de l'interface de gestion

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>S1#configure terminal</code>
Passer en mode de configuration d'interface pour l'interface du VLAN 99.	<code>S1(config)#interface vlan 99</code>
Configurer l'adresse IP de l'interface.	<code>S1(config-if)#ip address 172.17.99.11 255.255.255.0</code>
Activer l'interface.	<code>S1(config-if)#no shutdown</code>
Repasser en mode d'exécution privilégié.	<code>S1(config-if)#end</code>
Passer en mode de configuration globale.	<code>S1#configure terminal</code>
Entrer dans l'interface pour affecter le réseau local virtuel.	<code>S1(config)#interface fastethernet 0/18</code>
Définir le mode d'appartenance du port à un réseau local virtuel.	<code>S1(config-if)#switchport mode access</code>
Affecter le port à un réseau local virtuel.	<code>S1(config-if)#switchport acces vlan 99</code>
Repasser en mode d'exécution privilégié.	<code>S1(config-if)#end</code>
Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.	<code>S1#copy running-config startup-config</code>

# Configuration de la connectivité IP (3)

## Configuration de la passerelle par défaut

- La configuration de la passerelle par défaut permet transmettre les paquets IP à des réseaux distants.
- Le commutateur transmet des paquets IP avec des adresses IP de destination, externes au réseau local, à la passerelle par défaut.



Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Configurer la passerelle par défaut sur le commutateur.	<code>S1(config)#ip default-gateway 172.17.99.1</code>
Repasser en mode d'exécution privilégié.	<code>S1(config)#end</code>
Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.	<code>S1#copy running-config startup-config</code>

# Configuration de la connectivité IP (4)

## Vérification de la configuration

```
S1#show running-config
...
!
interface FastEthernet0/18
  switchport access vlan 99
  switchport mode access
...
!
interface Vlan99
  ip address 172.17.99.11 255.255.255.0
  no ip route-cache
!
```

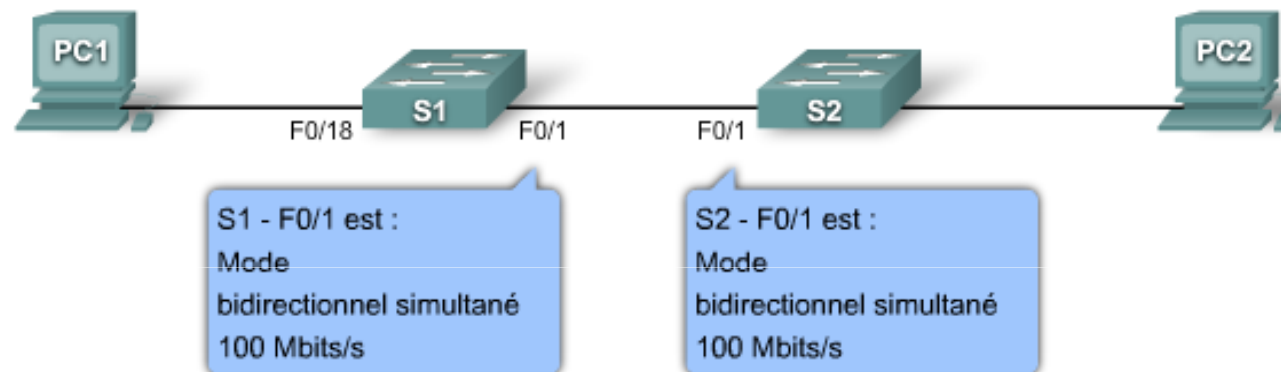
VLAN 99 configuré sur le port F0/18

```
S1#show ip interface brief
Interface          IP-Address  OK?  Method  Status
Protocol
...
Vlan99             172.17.99.11 YES   manual  up       up
...
FastEthernet0/18    unassigned  YES   unset   up       up
FastEthernet0/19    unassigned  YES   unset   down     down
...
GigabitEthernet0/2  unassigned  YES   unset   down     down
S1#
```

État du VLAN 99 et du port F0/18

# Configuration du mode bidirectionnel et de la vitesse

- Cas de deux commutateurs disposant des mêmes paramètres bidirectionnels et même vitesse



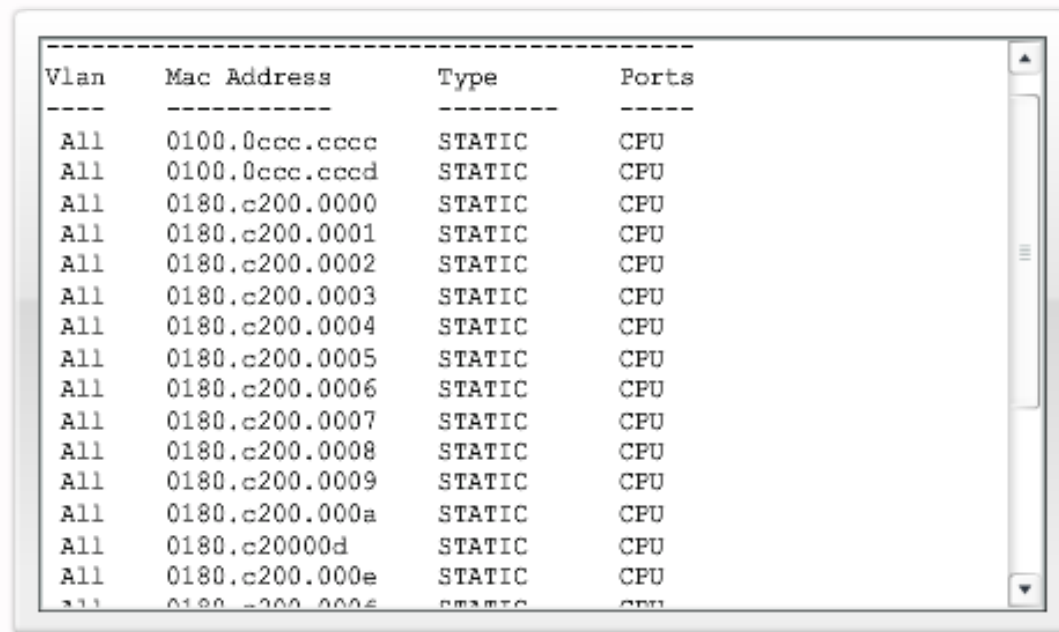
Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	S1# <b>configure terminal</b>
Passer en mode de configuration d'interface.	S1 (config) # <b>Interface fastethernet 0/1</b>
Configurer le mode birectionnel d'interface pour activer la configuration bidirectionnelle automatique.	S1 (config-if) # <b>duplex auto</b>
Configurer la vitesse bidirectionnelle d'interface et activer la configuration de vitesse automatique.	S1 (config-if) # <b>speed auto</b>
Revenir au mode d'exécution privilégié.	S1 (config-if) # <b>end</b>
Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.	S1# <b>copy running-config startup-config</b>

- Commutateurs Cisco modernes  $\Rightarrow$  présence d'outils de configuration Web (interface utilisateur du navigateur Web Cisco, SDM ...)
- ⇒ Nécessité de configurer le commutateur en tant que serveur HTTP.



Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>S1#configure terminal</code>
Configurer l'interface du serveur HTTP pour le type d'authentification enable. Les autres options disponibles sont les suivantes : enable : utilisation du mot de passe actif, soit la méthode par défaut pour l'authentification utilisateur du serveur HTTP. local : utilisation de la base de données utilisateur telle que définie sur le routeur Cisco ou le serveur d'accès. tacacs : utilisation du serveur TACACS.	<code>S1 (config) #ip http authentication enable</code>
Activer le serveur HTTP.	<code>S1 (config) #ip http server</code>
Revenir au mode d'exécution privilégié.	<code>S1 (config) #end</code>
Enregistrer la configuration en cours dans la configuration de démarrage du commutateur.	<code>S1#copy running-config startup-config</code>

- Visualiser la table d'adresses MAC (adresses statiques et dynamiques) ⇒ « **show mac-address-table** »
- Créer un mappage statique dans la table MAC ⇒ commande “**mac-address-table static** *<adresse\_MAC>* **vlan {1-4096, ALL}** **interface id\_interface**”.
- Supprimer un mappage statique ⇒ commande “**no mac-address-table static** *<adresse\_MAC>* **vlan {1-4096, ALL}** **interface id\_interface**”.



Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU



Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Affiche l'état et la configuration d'une ou de l'ensemble des interfaces disponibles sur le commutateur.	<code>show interfaces [interface-id]</code>
Affiche le contenu de la configuration de démarrage.	<code>show startup-config</code>
Affiche la configuration actuelle.	<code>show running-config</code>
Affiche des informations sur le système de fichiers flash.	<code>show flash:</code>
Affiche l'état du logiciel et du matériel système.	<code>show version</code>
Affiche l'historique des commandes de session.	<code>show history</code>
Affiche des informations IP. L'option d'interface dévoile l'état et la configuration de l'interface IP. L'option http affiche les données HTTP relatives au gestionnaire de périphériques exécuté sur le commutateur. L'option arp affiche la table ARP IP.	<code>show ip {interface   http   arp}</code>
Affiche la table de transmission MAC.	<code>show mac-address-table</code>

## Exemples

```

S1#show running-config
Building configuration...

Current configuration : 1664 bytes
!
version 12.2
...
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
.....
!
interface Vlan99
 ip address 172.17.99.11 255.255.0.0
 no ip route-cache
!
 ip default-gateway 172.17.50.1
 ip http server

```

```

S1#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Fast Ethernet, address is 0019.aa9e.b001 (bia 0019.aa9e.b001)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts (0 multicast)

```





# Sauvegarde et restauration des configurations des commutateurs (1)



## Sauvegarde des configurations

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Version officielle de la commande de copie de Cisco IOS. Confirmez le nom du fichier de destination. Appuyez sur la touche Entrée pour valider et sur les touches Ctrl+C pour annuler.	<pre>S1#copy system:running-config flash:startup-config Destination filename [ startup-config]?</pre>
Version non officielle de la commande de copie. Il est supposé alors que la configuration en cours est exécutée sur le système et que le fichier de configuration de démarrage sera stocké dans la mémoire vive non volatile flash. Appuyez sur la touche Entrée pour valider et sur les touches Ctrl+C pour annuler.	<pre>S1#copy running-config startup-config Destination filename [ startup-config]?</pre>
Sauvegardez la configuration de démarrage dans un fichier stocké dans la mémoire vive non volatile flash. Confirmez le nom du fichier de destination. Appuyez sur la touche Entrée pour valider et sur les touches Ctrl+C pour annuler.	<pre>S1#copy startup-config flash:config.bak1 Destination filename [ config.bak1]?</pre>

- Sauvegarder les fichiers sur un serveur TFTP ⇒ «**copy system:running-config tftp:[[/[/emplacement]/répertoire]/nom\_fichier]**»



# Sauvegarde et restauration des configurations des commutateurs (2)



## Restauration des configurations

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Copiez le fichier config.bak1 stocké dans la mémoire flash dans la configuration de démarrage qui doit être stockée dans la mémoire flash. Appuyez sur la touche Entrée pour valider et sur les touches Ctrl+C pour annuler.	<pre>S1#copy flash:config.bak1 startup-config Destination filename [ startup-config]?</pre>
Demandez à Cisco IOS de redémarrer le commutateur. Si vous avez modifié le fichier de configuration en cours, le système vous demande de l'enregistrer. Confirmez par un 'y' (oui) ou un 'n' (non). Pour confirmer le rechargement, appuyez sur la touche Entrée pour valider ou sur les touches Ctrl+C pour annuler.	<pre>S1#reload  System configuration has been modified. Save? [ yes/no] : n Proceed with reload? [ confirm]?</pre>



# Sauvegarde et restauration des configurations des commutateurs (3)



## Sauvegarde et restauration depuis un serveur TFTP

- Sauvegarder les fichiers sur un serveur TFTP ⇒ « **#copy system:running-config tftp:[[/emplacement]/répertoire/nom\_fichier]** »
- Restaurer (télécharger) le fichier depuis le serveur TFTP ⇒ « **copy tftp:[[/emplacement]/répertoire/nom\_fichier] system:running-config** »

```
S1#copy system:running-config tftp://172.16.2.155/tokyo-config
Write file tokyo-config on host 172.16.2.155? [confirm] y
Writing tokyo-config!!! [OK]
```



# Suppression des paramètres de configuration



- Effacer le contenu de la configuration de démarrage ⇒ « **erase nvram** » ou « **erase startup-config** »
- Supprimer un fichier stocké dans la mémoire flash ⇒ « **delete flash:nom\_fichier** »

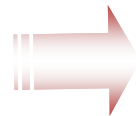
```
S1#erase nvram:
Erasing the nvram filesystem will remove all configuration
files!
Continue? [confirm]
[OK]
Erase of nvram: complete
S1#
```



## **Configuration de la sécurité des commutateurs**

# Configurations des options des mots de passe (1)

## Configuration de mot de passe d'accès à la console



Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>Sl#configure terminal</code>
Passer du mode de configuration globale au mode de configuration de ligne pour la console 0.	<code>Sl (config)#line con 0</code>
Définir cisco en tant que mot de passe pour la ligne de console 0 sur le commutateur.	<code>Sl (config-line)#password cisco</code>
Définir la ligne de console pour exiger la saisie du mot de passe avant l'octroi de l'accès.	<code>Sl (config-line)#login</code>
Quitter le mode de configuration de ligne et revenir en mode d'exécution privilégié.	<code>Sl (config-line)#end</code>

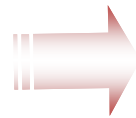
Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>Sl#configure terminal</code>
Passer du mode de configuration globale au mode de configuration de ligne pour les lignes vty 0 à 4.	<code>Sl (config)#line vty 0 4</code>
Définir cisco en tant que mot de passe pour les lignes vty sur le commutateur.	<code>Sl (config-line)#password cisco</code>
Définir la ligne vty pour exiger la saisie du mot de passe avant l'octroi de l'accès.	<code>Sl (config-line)#login</code>
Quitter le mode de configuration de ligne et revenir en mode d'exécution privilégié.	<code>Sl (config-line)#end</code>



## Configuration de mot de passe d'accès au terminal virtuel

# Configurations des options des mots de passe (2)

## Configuration de mot de passe en mode d'exécution



Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	S1#configure terminal
Configurer la commande <b>enable password</b> pour le passage en mode d'exécution privilégié.	S1(config)#enable password mot_de_passe
Configurer le mot de passe <b>enable secret</b> pour le passage en mode d'exécution privilégié.	S1(config)#enable secret mot_de_passe
Quitter le mode de configuration de ligne et revenir en mode d'exécution privilégié.	S1(config)#end

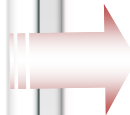
## Activation de la récupération de mot de passe (Cisco 2960)

- **Etape 1 :** branchement du commutateur au Terminal et démarrage du logiciel d'émulation
- **Etape 2 :** Appuie sur le bouton Mode pendant 15 secondes jusqu'à ce que le LED système devienne verte
- **Etape 3 :** initialisation du système de fichier ⇒ commande « **flash\_init** »
- **Etape 4 :** Chargement de tous les fichiers ⇒ commande « **load\_helper** »
- **Etape 5 :** affichage du contenu de la mémoire flash ⇒ commande « **dir flash** »
- **Etape 6 :** modification du nom de fichier de configuration ⇒ commande « **rename flash:config.text flash:config.text.old** »
- **Etape 7 :** Démarrage du système ⇒ commande « **boot** »

# Configurations des options des mots de passe (3)

## Configuration des mots de passe chiffrés

```
...
line con 0
password cisco
login
line vty 0 4
password cisco
no login
line vty 5 15
password cisco
no login
!
end
S1#config terminal
S1(config)#service password-encryption
S1(config)#end
```



```
S1#Show running-config
...
control-plane
!
line con 0
password 7 030752180500
login
line vty 0 4
password 7 1511021F0725
no login
line vty 5 15
password 7 1511021F0725
no login
!
end
```



## Configuration d'une bannière de connexion

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>S1#configure terminal</code>
Configurer une bannière de connexion.	<code>S1(config)#banner login "Personnel autorisé uniquement"</code>

## Bannière MOTD

- **Bannière de message de jour (MOTD) :** affiche tous les terminaux connectés à la connexion et transmet des messages à tous les utilisateurs du réseau
  - ❑ **Exemple :** avertissement d'un arrêt imminent du système.
- apparaît avant la configuration de la bannière de connexion.

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passer du mode d'exécution privilégié au mode de configuration globale.	<code>S1#configure terminal</code>
Configurer une bannière MOTD.	<code>S1(config)#banner motd "La maintenance du périphérique aura lieu vendredi."</code>

Deux choix pour l'accès distant à un terminal virtuel (vty) sur un commutateur Cisco.

Telnet	SSH (Secure SHell)
Méthode d'accès la plus courante	Devrait être la méthode d'accès la plus fréquente à utiliser
Envoie des flux de messages en texte clair	Envoie des flux de messages chiffrés
Méthode non sécurisé	Méthode sécurisée

## Configuration de Telnet

- Le mode de transport par défaut
- En cas de commutation vers le mode SSH, la réactivation de Telnet :

```
S1(config)#line vty 0 15
S1(config-line)#transport input telnet
```

## Configuration de SSH

- La prise en charge des versions 1 (SSHv1) et 2 (SSHv2) par le commutateur, en tant que serveur, et de la version 1 (SSHv1) en tant que client
- Configuration d'un serveur SSH :

```
(config)#ip domain-name mydomain.com
(config)#crypto key generate rsa
(config)#ip ssh version 2
(config)#line vty 0 15
(config-line)#transport input SSH
```

Configuration de domaine hôte

Activation de l'authentification en utilisant des clés RSA

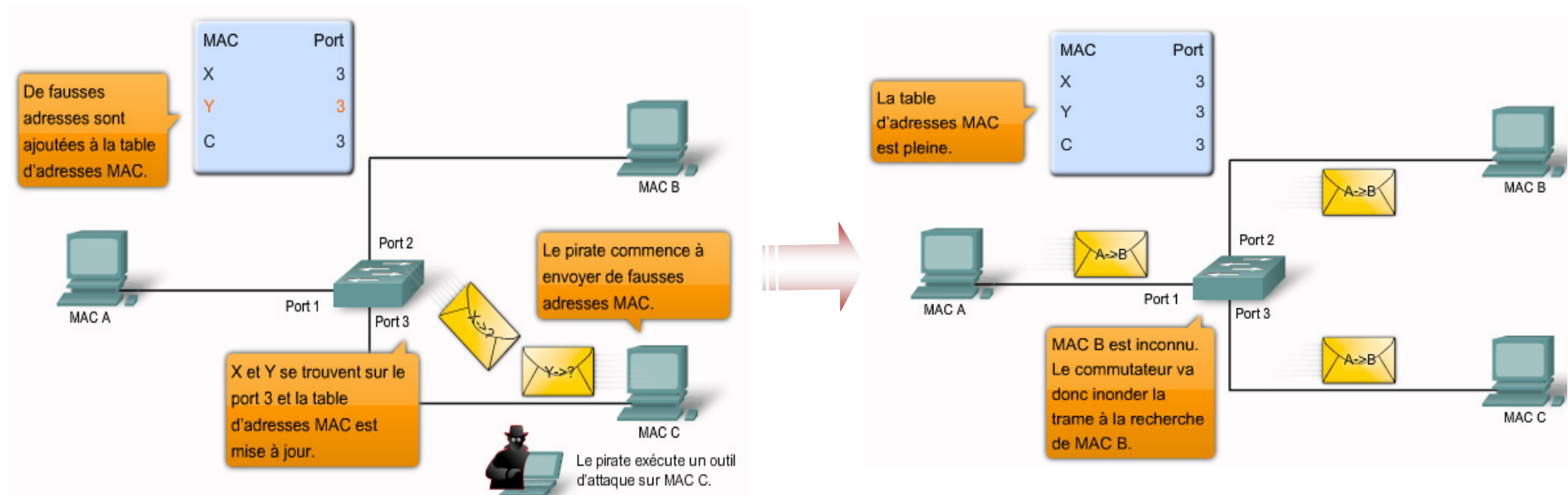
Activation SSH

# Menaces fréquentes en terme de sécurité (1)

## Inondations d'adresses MAC

- Ou attaques par dépassement de table MAC, de taille limitée
  - submerger le commutateur de fausses adresses MAC source jusqu'à ce que la table d'adresses MAC de ce dernier soit saturée.
- ⇒ Le commutateur passe alors en mode fail-open, commence à agir en qualité de hub (concentrateur) et diffuse des trames à tous les hôtes du réseau.

⇒ voir toutes les trames transmises de l'hôte attaqué vers un autre hôte sans une entrée de la table d'adresses MAC.

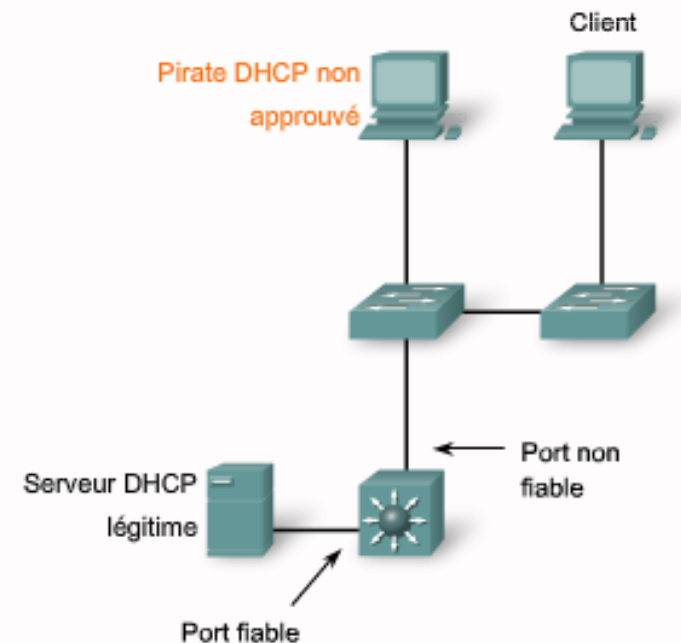


## Attaques par mystification

- Un périphérique de mystification DHCP répond aux requêtes DHCP clientes: le pirate active un serveur DHCP sur un segment de réseau
- Il répond avant le serveur DHCP légitime en procurant des paramètres IP définis par le pirate (passerelle par défaut et/ou serveur DNS)
- Les paquets hôtes sont redirigés vers l'adresse du pirate qui les transmet, à son tour vers la destination voulu

## Surveillance DHCP

- Permet de configurer des ports comme :
  - ☐ **fiables** ⇒ transmettent les requêtes et réponses DHCP
  - ☐ **non fiables** ⇒ transmettent uniquement les requêtes DHCP
- Créer une **table de liaison DHCP** chargée de mapper une @MAC cliente, une @IP, un VLAN et un ID de port





# Menaces fréquentes en terme de sécurité (3)

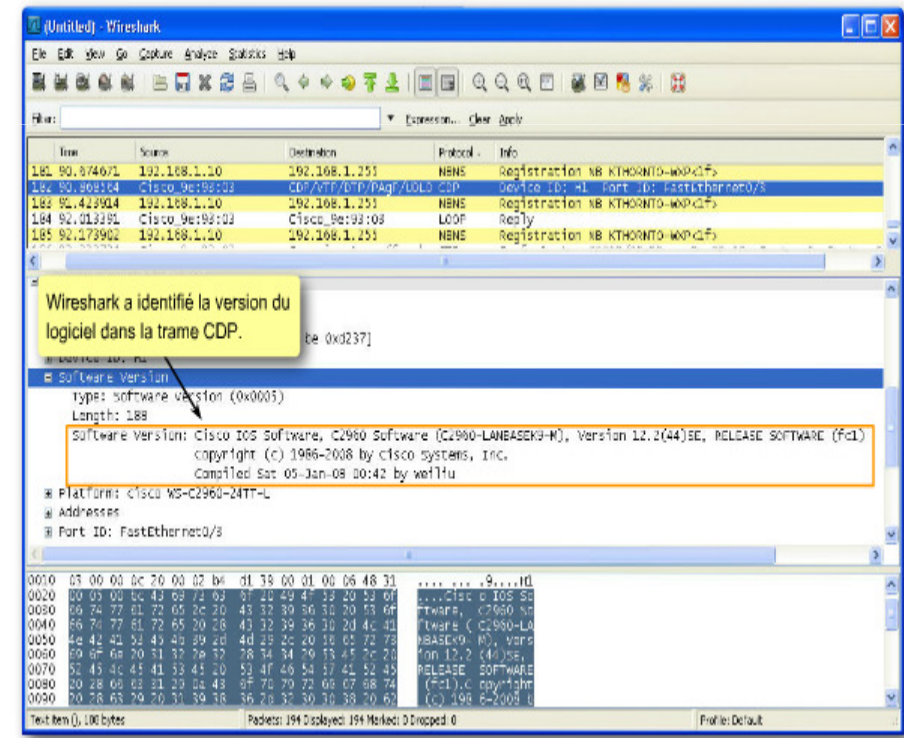


## Etapes de configuration de la surveillance DHCP

- ❑ **Etape 1** : Activer la surveillance DHCP  $\Rightarrow$  commande de configuration globale « **ip dhcp snooping** ».
- ❑ **Etape 2** : Activer la surveillance DHCP pour des VLANs spécifiques  $\Rightarrow$  commande « **ip dhcp snooping vlan number [nombre]** ».
- ❑ **Etape 3** : Définir, au niveau de l'interface, les ports comme étant fiables  $\Rightarrow$  commande « **ip dhcp snooping trust** ».
- ❑ **Etape 4** : (Facultatif) Pour limiter la fréquence à laquelle un pirate peut perpétuellement transmettre de fausses requêtes DHCP au serveur DHCP via des ports non fiables  $\Rightarrow$  commande « **ip dhcp snooping limit rate fréquence** ».

## Attaques CDP

- **CDP (Cisco Discovery Protocol)** ≡ protocole activé sur les routeurs et commutateurs Cisco, qui détecte tous les autres périphériques Cisco bénéficiant d'une connexion directe
- Les messages CDP ne sont pas chiffrés
- renferme des informations sur le périphérique ( @ IP, version du logiciel, plateforme, fonctions et le VLAN)
  - ↳ Si ces informations sont connues par un pirate, il peut les exploiter pour attaquer le réseau (**DoS**)
- Le paquet CDP renferme la version du logiciel Cisco IOS utilisé par le périphérique
  - ↳ Permet au pirate de rechercher et d'identifier quelques points vulnérables en matière de sécurité
- CDP n'est pas authentifié
  - ↳ Permet au pirate peut concevoir de faux paquets CDP et les transmettre via le périphérique Cisco connecté directement dont il dispose.





# Menaces fréquentes en terme de sécurité (5)



## Attaques Telnet

- Attaques de **mot de passe en force** (force brute)
- Attaque **DoS** (déni de service)

## Protection contre la force brute

- Modification régulière de mots de passe
- Utilisation de mots de passe forts
- Limitation des personnes à communiquer via des lignes VTY

## Protection contre DoS

- Mise à jour avec la nouvelle version du logiciel Cisco IOS





- **Audits de sécurité réseau :**
  - Révéler le type d'information dont le pirate est en mesure de rassembler et utiliser dans ses attaques
  - Évaluer la quantité idéale d'adresses MAC usurpées à supprimer
  - Déterminer la période d'obsolescence de la table d'adresses MAC
- **Tests de pénétration réseau :**
  - Identifier les faiblesses dans la configuration des périphériques réseau
  - Éviter tout impact sur les performances du réseau





# Configuration de la sécurité des ports (1)



## Objectifs de la sécurité des ports

- Préciser une seule adresse MAC ou un groupe d'adresses MAC autorisées sur un port
- ↳ Préciser que le port s'arrête automatiquement si des adresses MAC non autorisées sont détectées

## Types d'adresses MAC sécurisées

- **Adresses MAC sécurisées statiques** ≡ configurées **manuellement** ⇒ commande de configuration d'interface « **switchport port-security mac-address *adresse\_mac*** »
- **Adresses MAC sécurisées dynamiques** ≡ assimilées de manière **dynamique** et stockées uniquement dans la table d'adresses. Les adresses MAC configurées ainsi sont supprimées au redémarrage du commutateur.
- **Adresses MAC rémanentes** ≡ assimilées de manière **dynamique** et stockées dans la table d'adresses, mais aussi dans la configuration en cours (les conserver lors du redémarrage de commutateur)

# Configuration de la sécurité des ports (2)

## Modes de violation de la sécurité

- Violation dans les situations suivantes :
  - Une station dont l'adresse MAC ne figure pas dans la table d'adresses tente d'accéder à l'interface lorsque la table est saturée
  - Une adresse est en cours d'utilisation dans deux interfaces sécurisées sur le même VLAN
- Modes de violation de sécurité ⇒ actions à entreprendre en cas de violation de la sécurité
- 3 modes de violation : **Protect**, **restrict**, **shutdown**

Mode de violation	Acheminement du trafic	Envoi d'un message syslog	Affichage d'un message d'erreur	Incrémentation du compteur de violation	Arrêt du port
Protect	Non	Non	Non	Non	Non
Restrict	Non	Oui	Non	Oui	Non
Shutdown	Non	Oui	Non	Oui	Oui



# Configuration de la sécurité des ports (3)



## Paramètres par défaut de la sécurité des ports

Fonction	Paramètre par défaut
Sécurité des ports	Désactivée sur un port
Nombre maximal d'adresses MAC sécurisées	1
Mode de violation	Shutdown. Le port se ferme en cas de dépassement du nombre maximal d'adresses MAC sécurisées et une notification d'interruption SNMP est transmise.
Apprentissage des adresses rémanentes	Désactivé

## Configuration de la sécurité des ports dynamiques

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passez en mode de configuration globale. Utilisez la commande Cisco IOS :	<code>Sl#configure terminal</code>
Précisez le type et le numéro de l'interface physique à configurer (par exemple, fastEthernet F0/18) et passez en mode de configuration d'interface. Utilisez la commande Cisco IOS :	<code>Sl(config)#interface fastEthernet 0/18</code>
Définissez le mode d'interface en accès. Vous ne pouvez pas configurer une interface en tant que port sécurisé selon le mode dynamique par défaut approprié. Utilisez la commande Cisco IOS :	<code>Sl(config-if)#switchport mode access</code>
Activez la sécurité des ports sur l'interface. Utilisez la commande Cisco IOS :	<code>Sl(config-if)#switchport port-security</code>
Revenez au mode d'exécution privilégié. Utilisez la commande Cisco IOS :	<code>Sl(config-if)#end</code>



# Configuration de la sécurité des ports (4)



## Configuration de la sécurité des ports rémanents

Syntaxe de commande de l'interface de ligne de commande Cisco IOS	
Passez en mode de configuration globale. Utilisez la commande Cisco IOS :	<code>SI#configure terminal</code>
Précisez le type et le numéro de l'interface physique à configurer. Utilisez la commande Cisco IOS :	<code>SI(config)#interface fastEthernet 0/18</code>
Définissez le mode d'interface en accès. Utilisez la commande Cisco IOS :	<code>SI(config-if)#switchport mode access</code>
Activez la sécurité des ports sur l'interface. Utilisez la commande Cisco IOS :	<code>SI(config-if)#switchport port-security</code>
Définissez le nombre maximal d'adresses sécurisées à 50. Utilisez la commande Cisco IOS :	<code>SI(config-if)#switchport port-security maximum 50</code>
Activez l'apprentissage rémanent. Utilisez la commande Cisco IOS :	<code>SI(config-if)#switchport port-security mac-address sticky</code>
Revenez au mode d'exécution privilégié. Utilisez la commande Cisco IOS :	<code>SI(config-if)#end</code>

# Configuration de la sécurité des ports (5)

Vérification des paramètres de sécurité des ports

```
switch#show port-security interface fastEthernet 0/18
Port Security           : Enabled
Port Status             : Secure-down
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Vérification des adresses MAC sécurisées

```
switch#show port-security address
Secure Mac Address Table
-----
Vlan  Mac Address      Type                Ports    Remaining Age (mins)
99    0050.BAA6.06CE    SecureConfigured    Fa0/18   -
-----
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8320
```

Désactivation des ports inutilisés afin de les sécuriser ⇒ commande « **shutdown** »

```
...  
interface FastEthernet0/4  
  shutdown  
!  
interface FastEthernet0/5  
  shutdown  
!  
interface FastEthernet0/6  
  shutdown  
...  
!  
interface FastEthernet0/18  
  switchport mode access  
  switchport port-security  
...
```