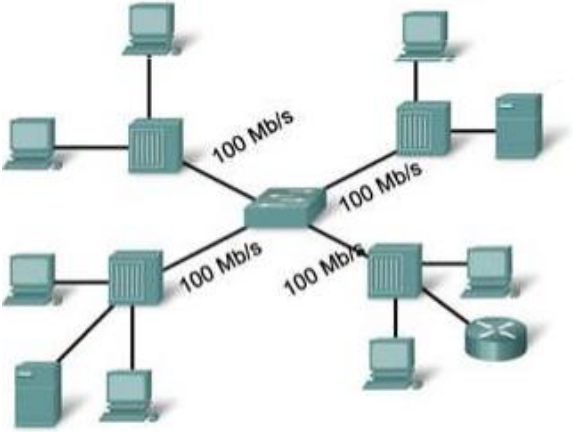
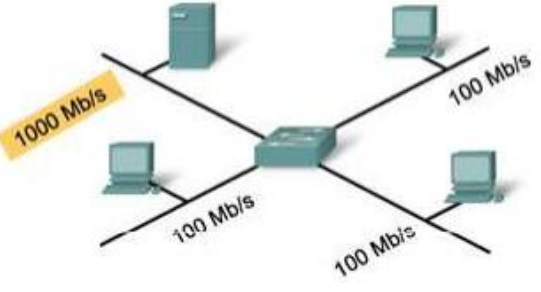


Chapitre 01**Maîtriser les concepts de la commutation****1. Quelques notions sur la commutation****1.1. Méthodes de transmission des trames**

Cut through	Le commutateur lit juste l' adresse du matériel et transmet la trame telle quelle. Aucune détection d'erreur n'est réalisée avec cette méthode. La trame est acheminée par le commutateur avant d'être entièrement reçue.
Store and forward	Le commutateur met en tampon (mémoire temporaire), et le plus souvent, réalise une opération de checksum (vérification des trames) sur chaque trame avant de l'envoyer. La trame complète est reçue puis acheminée.
Fragment free	Les paquets sont passés à un débit fixé, permettant de réaliser une détection d'erreur simplifiée. C'est un compromis entre les méthodes Cut through et Store and forward.
Adaptive switching	Un mode automatique. En fonction des erreurs constatées, le commutateur utilise une des trois méthodes précédentes.

1.2. Commutation symétrique et asymétrique

<p>Commutation symétrique : la commutation est réalisée entre les ports ont la même vitesse.</p>	
<p>Commutation asymétrique : la commutation est réalisée entre des ports qui ont des vitesses différentes.</p>	

2. Configurer les périphériques réseaux

2.1. Configurer les paramètres d'un commutateur/routeur

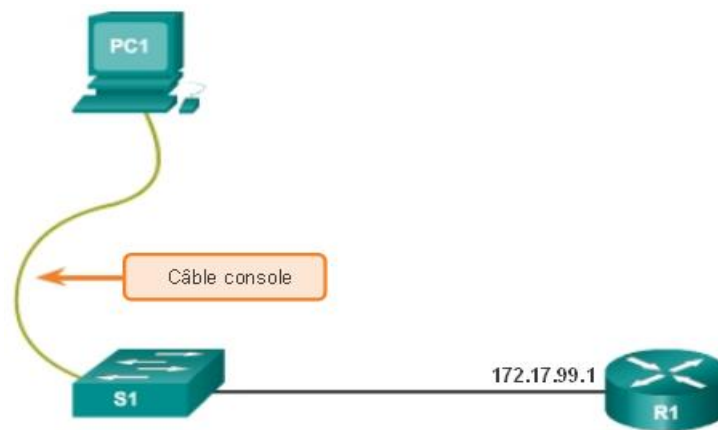
- Les commutateurs sont utilisés pour connecter plusieurs périphériques sur un même réseau.
- Dans un réseau, les commutateurs LAN ont pour fonction de diriger et de contrôler le flux de données au niveau de la couche d'accès des ressources mises en réseau.
- Voici les modes de commandes du commutateur (et du routeur) et comment basculer entre ces modes :

Mode utilisateur	Switch >
Mode privilégié	Switch #
Mode de configuration globale	Switch (config)#
Mode de configuration de l'interface	Switch (config-if)#
Mode de configuration de la ligne	Switch (config-line)#
Basculer du mode utilisateur en mode privilégié	Switch > enable
Basculer du mode privilégié en mode de configuration globale.	Switch # configure terminal Switch(config) #
Basculer du mode de configuration globale en mode de configuration de l'interface pour l'interface Fa0/1.	Switch(config) # interface Fa0/1 Switch(config-if) #
Basculer du mode de configuration globale en mode de configuration de la ligne pour la ligne Console 0.	Switch(config) # line console 0 Switch(config-line) #

- Les paramètres de base qu'il faut savoir configurer sont :
 - Nom d'hôte du périphérique (commande **hostname**)
 - Bannière de connexion (commande **banner motd**)
 - Réglage de la date et l'heure
 - Adresses IPv4 et IPv6 des interfaces (commande **ip address**)
 - Désactiver/activer la résolution DNS (commande **no ip domain-lookup**)
 - Mots de passe du mode privilégié (commandes **enable password** et **enable secret**)
 - Sécuriser les lignes console et VTY
 - Chiffrer tous les mots de passe (commande **service password-encryption**)
 - Etc.

2.2. Configurer l'accès à distance au commutateur

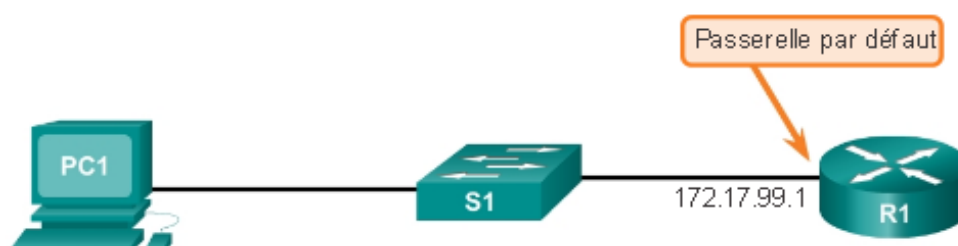
- Pour un accès distant à un commutateur, il est nécessaire de configurer **une adresse IP et un masque de sous-réseau** sur celui-ci.
- Pour configurer un commutateur, un câble console est utilisé.



- L'accès à distance au commutateur se fait à travers l'**interface virtuelle du commutateur** appelée **SVI** (Switched Virtual Interface). Cette dernière doit se voir attribuer une adresse IP et un masque.
- Il faut noter que SVI est une **interface virtuelle**, et non un port physique du commutateur.
- Par défaut, le commutateur est configuré de telle sorte que sa gestion est régie par le **VLAN 1**. Tous les ports sont par défaut assignés à VLAN 1. Pour des raisons de sécurité, il est recommandé d'utiliser un VLAN de gestion autre que le VLAN 1.
- Voici les commandes de configuration d'une SVI :

Création d'un VLAN pour l'associer à SVI.	S1 (config) # vlan 99 S1 (config-vlan) # name Gestion
Passer en mode de configuration d'interface SVI.	S1 (config) # interface vlan 99
Configurer l'@IP/masque de l'interface SVI.	S1 (config-if) # ip address 172.17.99.11 255.255.0.0
Associer le VLAN a un port du commutateur	S1 (config-if) # interface Fa0/2 S1 (config-if) # switchport access vlan 99
Activer l'interface SVI.	S1 (config-if) # no shutdown
Vérifier la configuration de SVI	S1# show ip interface brief

- Remarque : L'interface SVI n'apparaît comme **up/up** qu'une fois le VLAN associé est créé et qu'un périphérique est connecté à un port de commutateur associé à ce VLAN.
- Le commutateur doit être configuré avec une **passerelle par défaut** s'il doit être **géré à distance depuis des réseaux connectés indirectement**.
- La passerelle par défaut est le routeur auquel le commutateur est connecté directement.



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
Repassez 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

2.3. Sécuriser l'accès à distance au commutateur

- Le protocole **SSH** (Secure Shell) est un protocole permettant d'établir une connexion sécurisée (chiffrée) pour la gestion des périphériques distants comme les commutateurs.
- SSH remplace **Telnet** pour les connexions de gestion.
- SSH utilise le port par défaut **TCP 22**.
- Voici les commandes de configuration de SSH pour un accès à distance sécurisé au commutateur (ou routeur):

Vérifier que le commutateur prend en charge SSH.	S1# show ip ssh
Configurer le nom de domaine IP du réseau.	S1(config)# ip domain-name id.com
Générer les paires de clés RSA. La génération d'une paire de clés RSA active automatiquement le serveur SSH. Pour supprimer la paire de clés RSA on utilise crypto key zeroize rsa . Une fois la paire de clés RSA supprimée, le serveur SSH est automatiquement désactivé .	S1(config)# crypto key generate rsa
Configurer l'authentification utilisateur (nom d'utilisateur et mot de passe).	S1(config)# username stag secret sec123
Activer le protocole SSH sur les lignes VTY. Cette configuration permet d'interdire toute connexion autre que SSH (par exemple Telnet). La commande login local permet d'exiger l'authentification locale des connexions SSH provenant d'une base de données de noms d'utilisateur locale.	S1(config)# line vty 0 4 S1(config-line)# transport input ssh S1(config-line)# login local
Tester l'accès à distance depuis un client SSH (ex. poste de travail)	pc> SSH -I stag 192.168.1.10

- Exemple : configuration de SSH pour la gestion à distance du commutateur

```

S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jq/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVN1QhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfA
P3fyzKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q--

S1# show ssh
Connection Version Mode Encryption Hmac State Username
0 2.0 IN aes256-cbc hmac-sha1 Session started admin
0 2.0 OUT aes256-cbc hmac-sha1 Session started admin
%No SSHv1 server connections running.

```

```

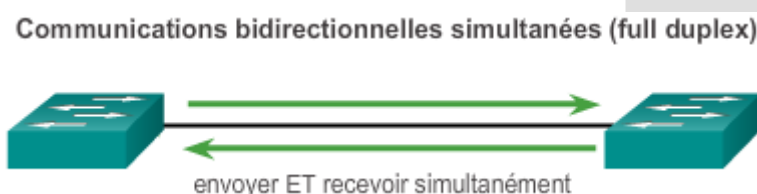
S1# configure terminal
S1(config)# ip domain-name cisco.com
S1(config)# crypto key generate rsa
The name for the keys will be: S1.cisco.com
...
How many bits in the modulus [512]: 1024
...
S1(config)# username admin secret ccna
S1(config-line)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
S1(config)# ip ssh version 2

```

2.4. Configurer des ports de commutateur

a) Communications bidirectionnelles simultanées (full duplex)

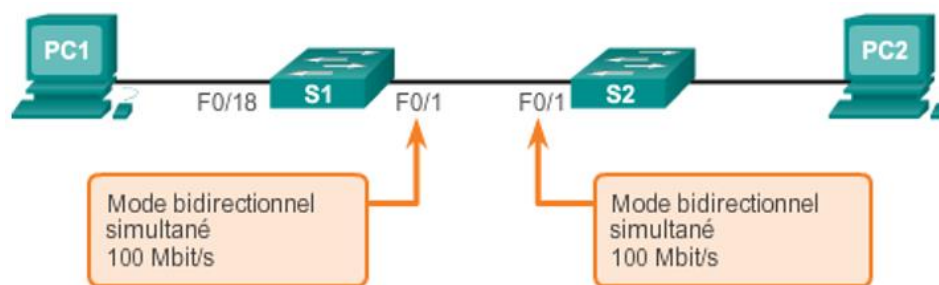
- Les communications bidirectionnelles simultanées **augmentent la bande passante réelle** car les deux extrémités de la connexion transmettent et reçoivent simultanément des données. On parle également de **bidirectionnalité**.



- Les communications bidirectionnelles non simultanées sont unidirectionnelles. L'envoi et la réception de données n'ont jamais lieu simultanément. Les communications bidirectionnelles non simultanées entraînent des problèmes de performances car les données ne peuvent circuler que dans un sens à la fois, ce qui se traduit souvent par des collisions.



- Voici les commandes pour configurer le mode bidirectionnel et la vitesse :



Passer en mode de configuration d'interface	S1(config)# interface Fa0/1
Configurer le mode bidirectionnel d'interface	S1(config-if)# duplex full
Configurer la vitesse d'interface	S1(config-if)# speed 100

b) Auto-MDIX

- Jusqu'à récemment, il était nécessaire d'utiliser certains types de câble Ethernet (droit ou croisé) pour connecter les périphériques (deux commutateurs ou un commutateur et un routeur).
- La **fonctionnalité d'interface croisée dépendante du support (auto-MDIX)** d'une interface permet d'éliminer ce problème.
- Lorsque la fonction auto-MDIX est activée, l'interface détecte automatiquement le type de câble requis pour la connexion (droit ou croisé) et configure la connexion en conséquence.
- Remarque : Lorsque la fonctionnalité auto-MDIX est utilisée sur une interface, la vitesse de l'interface et le mode de bidirectionnalité doivent être réglés sur **auto** pour un fonctionnement correct.
- Voici les commandes pour activer la fonction auto-MDIX :



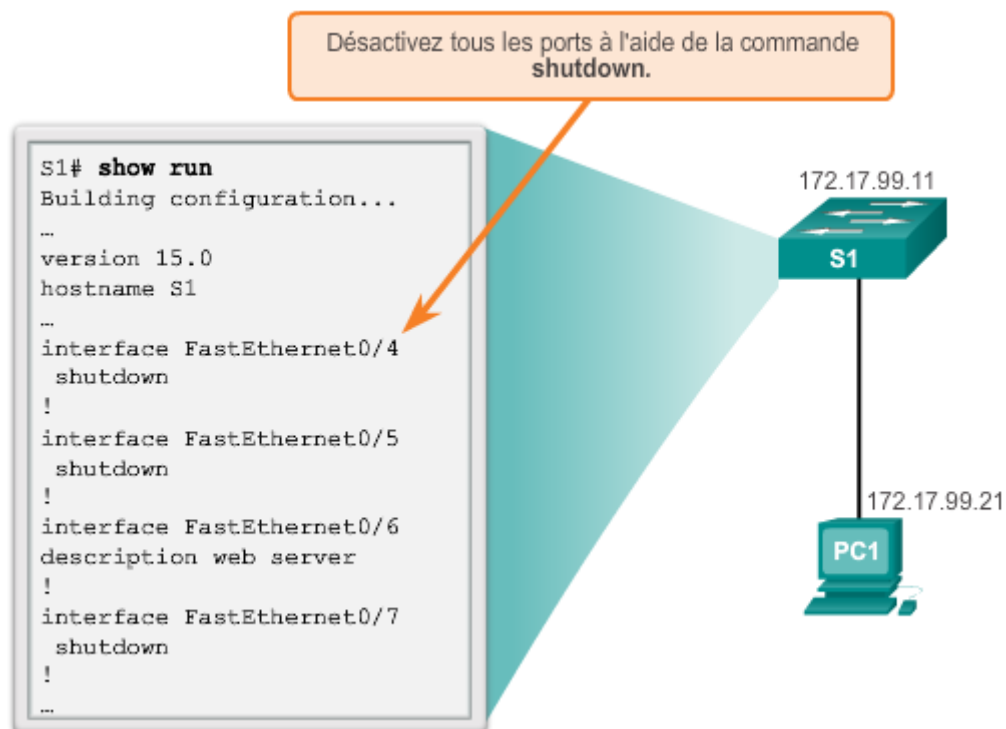
Passer en mode de configuration d'interface	S1(config)# interface Fa0/1
Configurer l'interface de sorte à négocier automatiquement les paramètres bidirectionnels et de vitesse avec le périphérique connecté.	S1(config-if)# duplex auto S1(config-if)# speed auto
Activer la fonction auto-MDIX sur l'interface	S1(config-if)# mdix auto

c) Vérification de la configuration des ports du commutateur

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

3. Sécurité des ports du commutateur**3.1. Sécuriser les ports inutilisés**

- **Désactiver les ports du commutateur inutilisés** est une méthode simple mais efficace à laquelle les administrateurs ont recours pour mieux protéger le réseau contre tout accès non autorisé.



- Il est possible de désactiver une plage de ports sur un commutateur en utilisant la commande **interface range**.

3.2. Implémenter la sécurité des ports

- Tous les ports (interfaces) de commutateur doivent être sécurisés avant le déploiement du commutateur en production.
- L'une des méthodes de sécurisation des ports consiste à implémenter une fonctionnalité appelée **sécurité des ports**.
- La sécurité des ports restreint le nombre d'adresses MAC autorisées sur un port. Les adresses MAC des périphériques légitimes sont ainsi autorisées. Toutes les autres adresses MAC sont refusées.
- La sécurité des ports peut être configurée pour autoriser une ou plusieurs adresses MAC. Si le nombre d'adresses MAC autorisées sur un port est limité à **un**, seul le périphérique disposant de **cette adresse MAC** spécifique peut se connecter au port.
- Types d'adresses MAC sécurisées :

Adresses MAC sécurisées statiques	Adresses MAC configurées manuellement sur un port avec la commande switchport port-security mac-address <i>adresse-mac</i> . Elles sont stockées dans la table d'adresses MAC et sont ajoutées à la configuration en cours sur le commutateur (fichier running-config).
Adresses MAC sécurisées dynamiques	Adresses MAC apprises de manière dynamique. Elles sont stockées uniquement dans la table d'@MAC et supprimées au redémarrage du commutateur.
Adresses MAC sécurisées rémanentes	Adresses MAC pouvant être apprises de manière dynamique ou configurées manuellement. Elles sont stockées dans la table d'@MAC et ajoutées à la configuration en cours.

- Il y a violation de la sécurité lorsque l'une des situations suivantes se présente :
 - Le nombre maximal d'adresses MAC sécurisées a été ajouté dans la table d'adresses de l'interface et une station dont l'adresse MAC ne figure pas dans la table d'adresses tente d'accéder à l'interface.
 - Une adresse assimilée ou configurée dans une interface sécurisée est visible sur une autre interface sécurisée dans le même VLAN.
- Une interface peut être configurée pour l'un des **trois modes de violation**, en spécifiant les actions à entreprendre en cas de violation :

Modes de violation de sécurité				
Mode de violation	Acheminement du trafic	Envoi d'un message syslog	Incrémentatio n du compteur de violation	Arrêt du port
Protect	Non	Non	Non	Non
Restrict	Non	Oui	Oui	Non
Shutdown	Non	Oui	Oui	Oui

- Paramètres par défaut de la sécurité 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

- Exemple : configuration de la sécurité des ports dynamiques



Commandes de l'interface en ligne de commande de CiscoIOS	
Spécifiez l'interface à configurer pour la sécurité des ports.	S1(config)# interface fastethernet 0/18
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

- Exemple : configuration de la sécurité des ports rémanents



Commandes de l'interface en ligne de commande de CiscoIOS	
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

- Vérification des adresses MAC sécurisées, dynamiques et rémanentes :

S1# **show port-security interface fastethernet 0/18**

```
Port Security           : Enabled
Port Status             : Secure-up
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 : 0025.83e6.4b01:1
Security Violation Count : 0
```

S1# **show port-security interface fastethernet 0/19**

```
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 10
Total MAC Addresses     : 1
Configured MAC Addresses : 0
Sticky MAC Addresses     : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```

S1# **show run | begin FastEthernet 0/19**

```
interface FastEthernet0/19
  switchport mode access
  switchport port-security maximum 10
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security mac-address sticky 0025.83e6.4b02
```

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	-