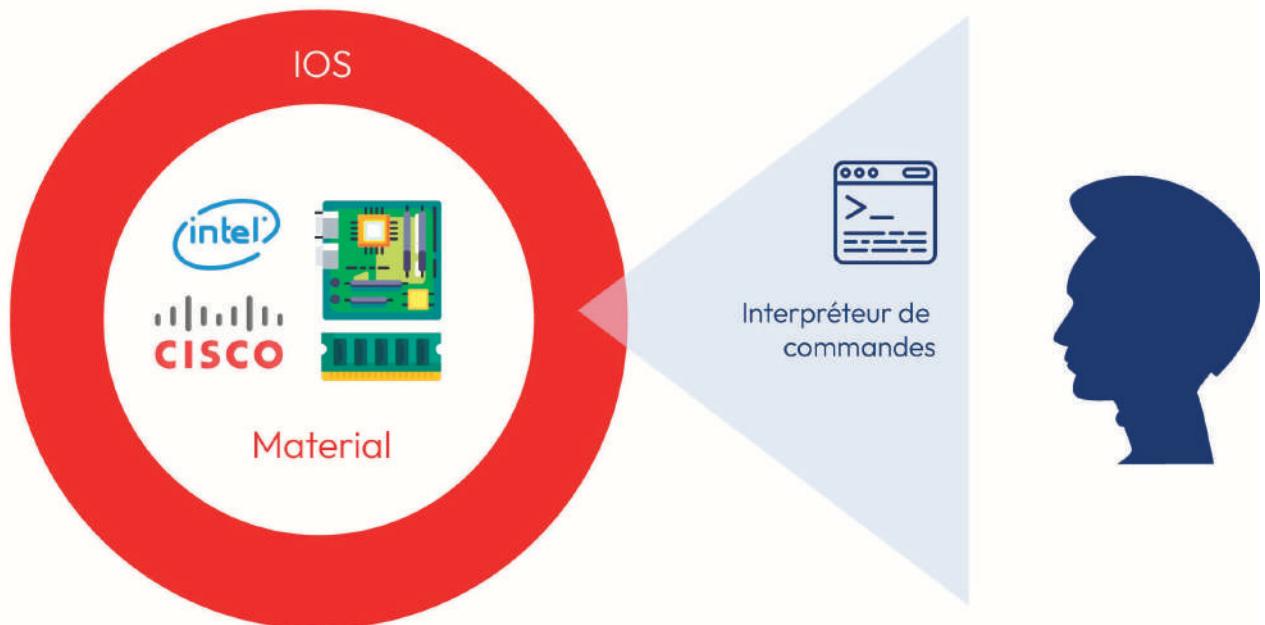


2

LES CONCEPTS DE LA COMMUTATION

2.1. Composants d'un équipement réseau



2.1.1. Composants matériels :

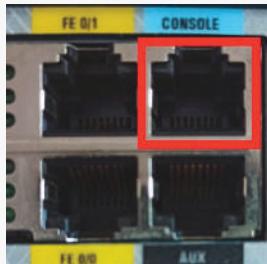
MÉMOIRES :

TYPES DE MÉMOIRES	
	La mémoire Flash La mémoire Flash est une mémoire non volatile qui contient le système d'exploitation appelé « IOS » : nom_IOS.bin
	La mémoire RAM La mémoire RAM est une mémoire volatile qui contient le fichier de configuration en cours : Running-config
	La mémoire NVRAM La mémoire NVRAM est une mémoire non volatile qui contient le fichier de configuration initiale (De démarrage) : Startup-config
	La mémoire ROM La mémoire ROM est une mémoire non volatile qui contient : <ul style="list-style-type: none">• Code permettant de tester le matériel de l'équipement réseau.• Code d'amorçage permettant de localiser l'IOS de l'équipement réseau.• Un outil de diagnostic ROMMON pour le dépannage.

LES INTERFACES D'UN ÉQUIPEMENT RÉSEAU :

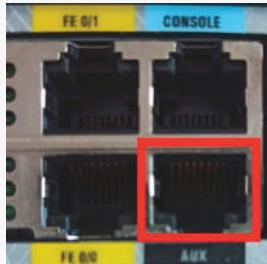


PORT CONSOLE



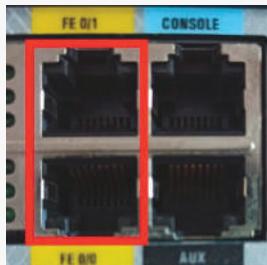
Le port console est un port utilisé pour la configuration d'un équipement réseau à l'aide d'un câble console

PORT AUXILIAIRE



Le port auxiliaire est un port utilisé pour la configuration d'un équipement réseau à distance en passant par un MODEM.

INTERFACES RÉSEAU



Interfaces LAN

Les interfaces LAN sont des interfaces permettant de connecter l'équipement réseau aux périphériques du réseau local LAN



Interfaces WAN

Les interfaces WAN (Série) sont des interfaces utilisées pour connecter l'équipement réseau (Routeur généralement) au réseau étendu WAN (Site distant)

2.1.2. Composants logiciels :

LE SYSTÈME D'EXPLOITATION RÉSEAU IOS

```
Switch>enable
Switch# show flash:
Directory of flash:/

 1 -rw- 4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
```

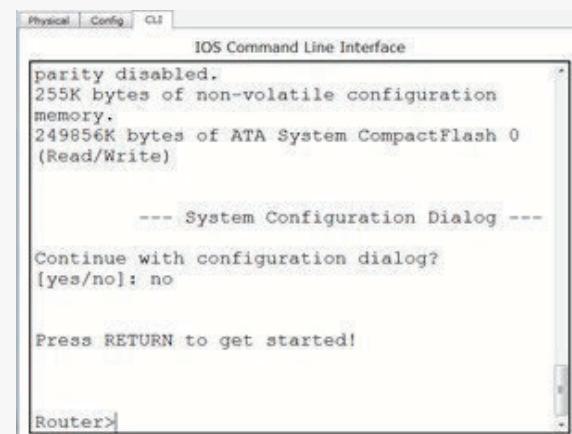
L'IOS d'un équipement réseau se trouve dans la mémoire Flash

LE FICHIER DE CONFIGURATION INITIALE

```
S1#show startup-config
Using 1076 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
```

Le fichier de configuration initiale (de démarrage) se trouve dans la mémoire NVRAM et il contient toute la configuration de l'équipement réseau.

CLI



IOS Command Line Interface

```
parity disabled.
255K bytes of non-volatile configuration
memory.
249856K bytes of ATA System CompactFlash 0
(Read/Write)

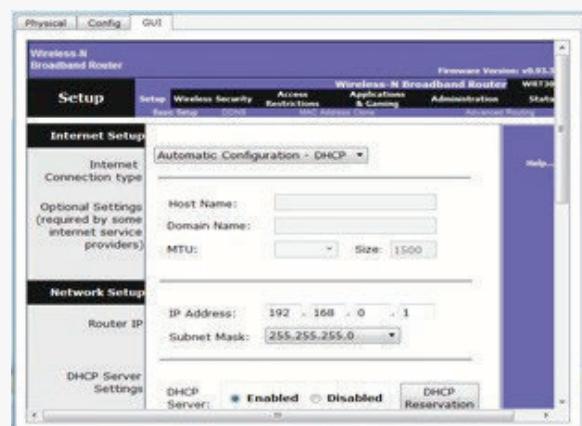
--- System Configuration Dialog ---

Continue with configuration dialog?
[yes/no]: no

Press RETURN to get started!

Router>
```

INTERFACE GRAPHIQUE



2.2. Processus de démarrage d'un équipement réseau

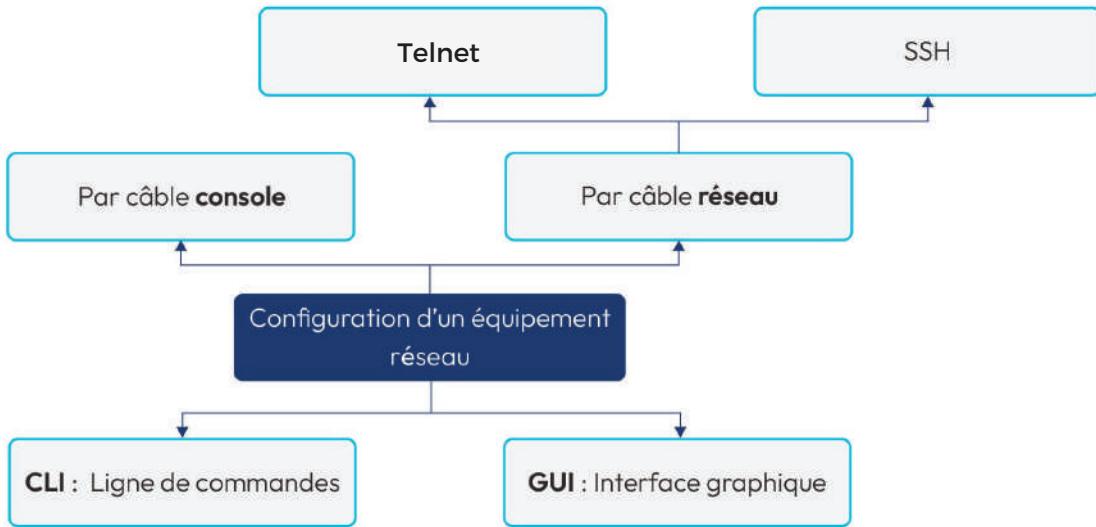


2.3. Méthodes de configuration d'un équipement réseau

Pour configurer un équipement réseau :

- ➊ Du point de vue matériel, on utilise un câble console ou un câble réseau
- ➋ Du point de vue logiciel, on utilise l'interface graphique GUI ou l'invite de commandes CLI





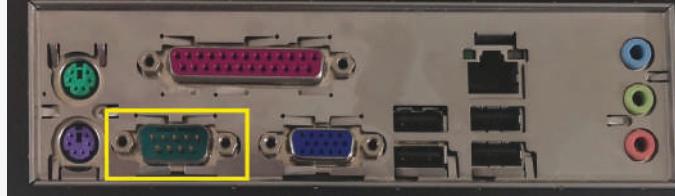
2.3.1. Configuration à l'aide d'un câble console

La configuration par câble console est généralement nécessaire lorsqu'on utilise un équipement réseau pour la première fois. Et ce, dans le but de personnaliser certains paramètres réseau pour pouvoir le configurer ensuite par un câble réseau.

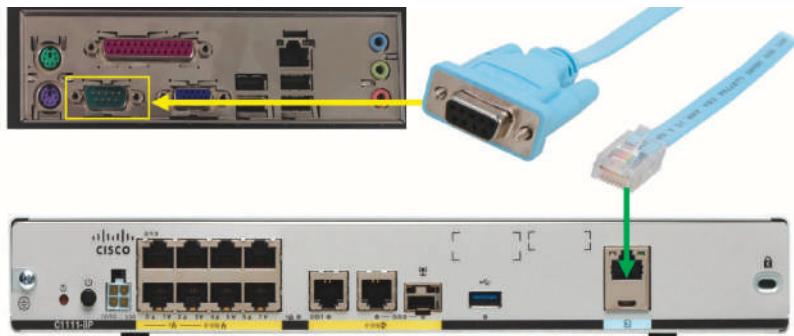


OUTILS ET MATÉRIELS NÉCESSAIRES :

CONFIGURATION PAR CÂBLE CONSOLE

Ordinateur avec un port série DB9 mâle (RS232 mâle)	
Câble console	
Équipement réseau	

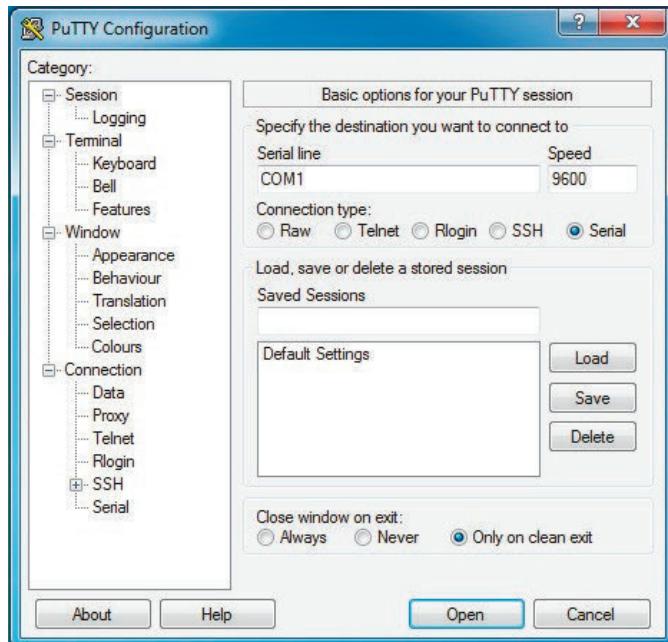
CÂBLAGE :



Remarque :

Dans le cas où l'ordinateur n'est pas muni d'un port série RS232, on utilise un adaptateur USB-RS232

OUTILS ET LOGICIELS NÉCESSAIRES : UN TERMINAL



Putty est un programme utilisé pour se connecter à des serveurs à distance, ou bien des équipements réseau, en utilisant le protocole sécurisé SSH.

- ➊ **Choix de l'option :** « Serial » pour la configuration par câble console.
- ➋ **Choix du port série :** COM1 dans la plupart des cas
- ➌ **Choix de la vitesse :** par défaut 9600 pour un nouvel équipement Cisco

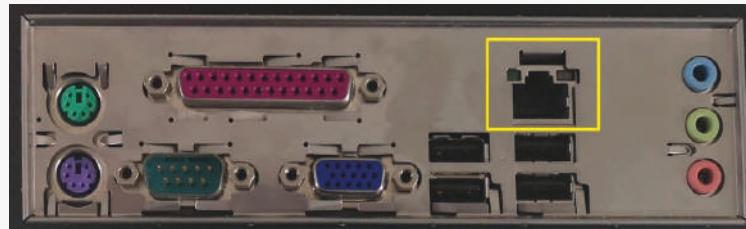


2.3.2. Configuration à l'aide d'un câble réseau

OUTILS ET MATÉRIELS NÉCESSAIRES :

CONFIGURATION PAR CÂBLE CONSOLE

Ordinateur avec un port réseau



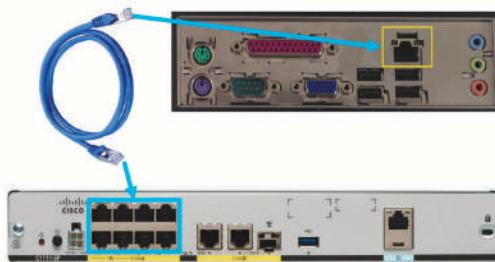
Câble réseau



Équipement réseau

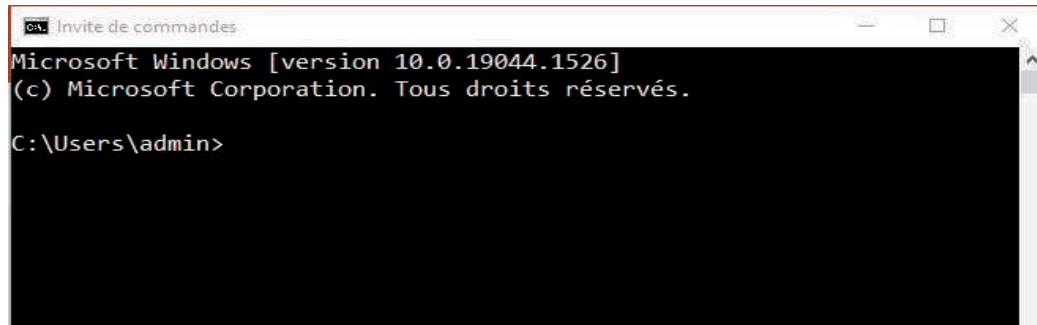


CÂBLAGE



OUTILS LOGICIELS :

Pour la configuration par réseau, il suffit d'utiliser le terminal du système d'exploitation ou un autre terminal.



```
Microsoft Windows [version 10.0.19044.1526]
(c) Microsoft Corporation. Tous droits réservés.

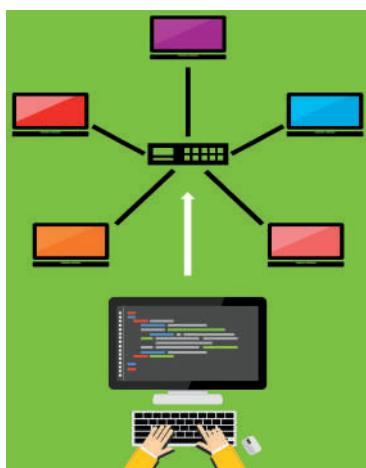
C:\Users\admin>
```

PROTOCOLES RÉSEAU :

Telnet SSH

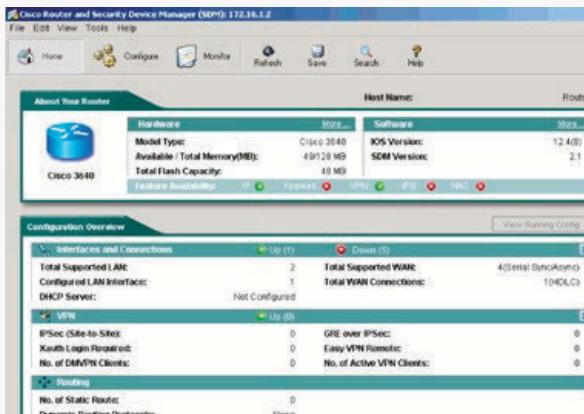
Le protocole « **Telnet** » n'est pas sécurisé, car il envoie les données en clair (**non recommandé**)

Le protocole « **SSH** » est sécurisé, car il envoie les données d'une manière chiffrée (**Recommandé**)

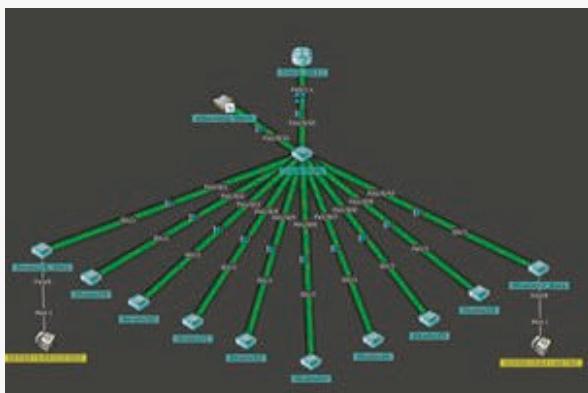


2.3.3. Configuration à l'aide de l'interface graphique

CONFIGURATION PAR INTERFACE GRAPHIQUE



Cisco Router and Security Device Manager



CNA pour les commutateurs



Cisco Configuration Professional (CCP)

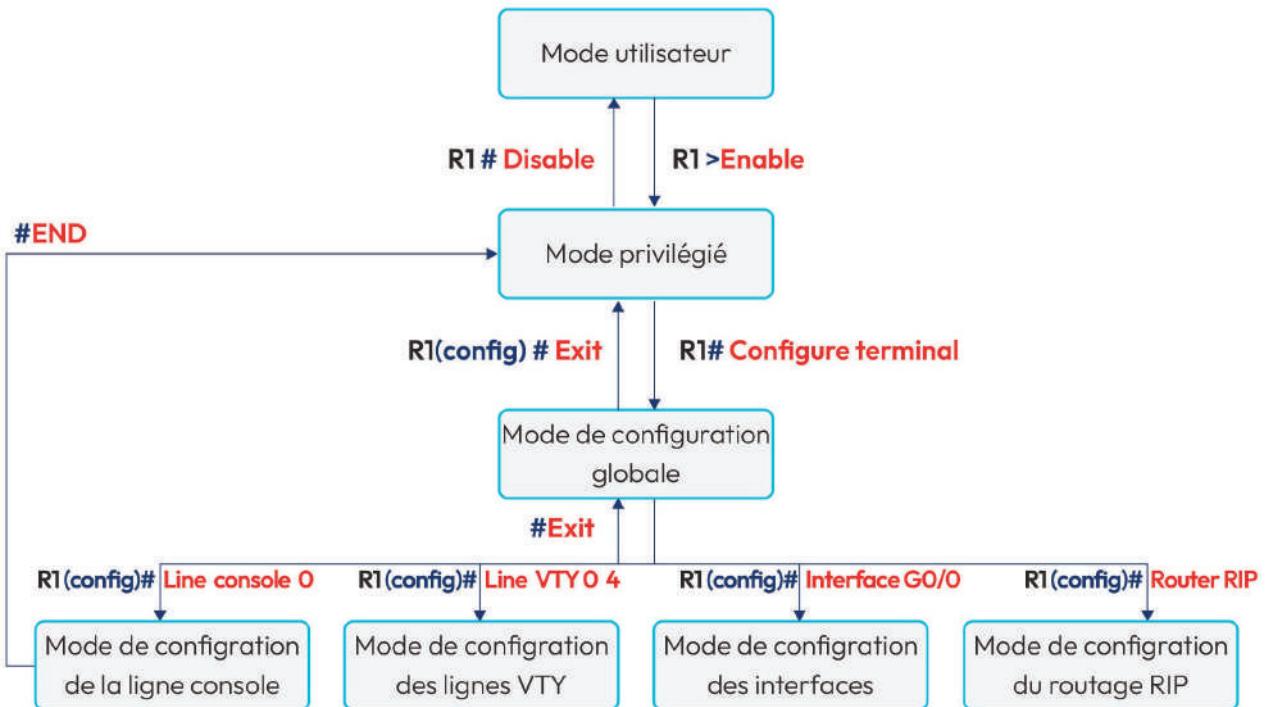
2.3.4. Configuration à l'aide de la ligne de commandes CLI

La configuration de l'équipement réseau se fait à l'aide d'un terminal.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#
```

2.4. Configuration de base d'un équipement réseau

2.4.1. Modes de configuration :



Router>**enable**

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**line console 0**

Mode utilisateur

Router(config-line)#**exit**

Mode d'exécution privilégiée

Router(config)#**line vty 0 4**

Mode de configuration globale

Router(config-line)#**exit**

Mode de configuration de la console

Router(config)#**interface G0/0**

Mode de configuration VTY

Router(config-if)#**exit**

Mode de configuration de l'interface G0/0

Router(config)#**router rip**

Mode de configuration du routage RIP

Router(config-router)#**exit**

Mode de configuration du routage RIP

Router(config)#**exit**

Mode de configuration du routage RIP

Router#

2.4.2. L'aide CLI :

UTILISATION DU POINT D'INTERROGATION « ? »

Cas 1 : Utilisation du « ? » au début

S1#?

Exec commands:

clear	Reset functions
clock	Manage the system clock
configure	Enter configuration mode
connect	Open a terminal connection
copy	Copy from one file to another
debug	Debugging functions (see also 'undebug')
delete	Delete a file
dir	List files on a filesystem
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
erase	Erase a filesystem
exit	Exit from the EXEC
logout	Exit from the EXEC
more	Display the contents of a file
no	Disable debugging informations

Le point d'interrogation « ? » utilisé au début d'un mode de configuration, affiche toutes les commandes disponibles dans ce mode ainsi que leurs descriptions.

Cas 2 : Utilisation du « ? » après une commande

```
S1#clock ?
  set Set the time and date
S1#clock set ?
  hh:mm:ss Current Time
S1#clock set 20:40:00 ?
  <1-31> Day of the month
  MONTH Month of the year
S1#clock set 20:40:00 March ?
  <1-31> Day of the month
S1#clock set 20:40:00 March 02 ?
  <1993-2035> Year
S1#clock set 20:40:00 March 02 2022
```

Le point d'interrogation, utilisé après une commande, affiche toutes les options disponibles pour cette commande :

- ⌚ **Clock ?** : affiche l'option « set »
- ⌚ **Clock set ?** : affiche l'option qui indique le format de l'heure « **hh:mm:ss** »
- ⌚ **Clock set 20:40:00 ?** : affiche deux options
 - Le jour
 - Le nom du mois (c'est l'option choisie)
- ⌚ **Clock set 20:40:00 March ?** : affiche l'option qui indique la saisie du jour du mois
- ⌚ **Clock set 20:40:00 March 02 ?** : affiche l'option qui indique la saisie de l'année
- ⌚ **Clock set 20:40:00 March 02 2022** est la commande finale

Cas 3 : Utilisation du « ? » attaché à une chaîne

```
S1#cl?  
clear clock  
S1#clo?  
clock
```

Le point d'interrogation, attaché à une chaîne de caractères, affiche toutes les commandes qui commencent par cette dernière.

L'AUTOCOMPLÉTION :

```
S1#con  
S1#conf  
S1#configure t  
S1#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
S1(config)#li  
S1(config)#line c  
S1(config)#line console 0  
S1(config-line)#ex  
S1(config-line)#exi  
S1(config-line)#exit  
S1(config)#+
```

Quand on tape une partie de la commande suivie de la touche "tabulation", la commande s'affiche complètement si la partie saisie correspond à une commande unique.

LES MESSAGES D'ERREUR

```
S1(config)#c
% Ambiguous command: "c" 1
S1(config)#clock
% Incomplete command. 2
S1(config)#clok
^
% Invalid input detected at '^' marker. 3
S1(config)#
```

- ⌚ Cas 1 : Commande ambiguë (plusieurs commandes qui commencent par « c »)
- ⌚ Cas 2 : Commande incomplète
- ⌚ Cas 3 : commande erronée

2.4.3. Les commandes de configuration de base :

COMMANDES DE BASE :

Configuration du nom du commutateur « S1 » :

La commande hostname permet de définir un nom d'hôte. Cela permet de lui donner une identité unique sur le réseau.

```
Switch(config)#hostname S1
S1(config)#
```

Rétablissement du nom par défaut :

De manière générale, l'utilisation de "**no**" dans la configuration d'un équipement de réseau vous permet de désactiver ou de supprimer des paramètres précédemment définis.

```
S1(config)#no hostname
Switch(config)#
```

Configuration d'une bannière d'un message du jour (message_of-the-day) :

La commande "**banner motd**" (Message Of The Day) permet de configurer un message qui sera affiché chaque fois qu'un utilisateur se connecte à l'équipement réseau.

Ce message peut être utilisé pour informer les utilisateurs de l'état du réseau ou pour afficher des informations importantes.

```
Router(config)# banner motd #L'électricité du bâtiment sera coupée de  
6h00 à 7h00 mercredi prochain.#
```



Note : le symbole "#" marque le début et la fin du message.

Configuration d'une bannière de connexion (login) :

La commande "**banner login**" permet de configurer un message qui sera affiché chaque fois qu'un utilisateur essaie de se connecter à l'équipement réseau de la marque Cisco en utilisant un nom d'utilisateur et un mot de passe.

Ce message peut être utilisé pour informer les utilisateurs de l'état du réseau ou pour afficher des informations importantes, comme des politiques de confidentialité ou des informations de contact en cas de problème.

```
Router(config)# banner login #Bienvenue sur le réseau de notre  
entreprise. En accédant à ce réseau, vous acceptez de respecter notre  
politique de confidentialité et notre charte d'utilisation responsable.  
Toute utilisation non autorisée de ce réseau sera considérée comme une  
violation de cette charte et des sanctions appropriées seront  
appliquées.#
```



La principale différence entre ces deux commandes, c'est le moment où le message est affiché :

- "**banner motd**" affiche le message une fois que l'utilisateur est connecté
- Tandis que "**banner login**" affiche le message avant qu'un utilisateur ne soit connecté.

Désactivation de la recherche DNS :

La commande "**no ip domain-lookup**" est utilisée pour désactiver la fonction de recherche de domaine sur un équipement réseau.

Cela signifie que lorsqu'un utilisateur tape une commande qui inclut un nom de domaine plutôt qu'une adresse IP, l'équipement n'essaiera pas de résoudre ce nom de domaine en une adresse IP en utilisant un serveur DNS...

Cela peut être utile dans les situations où l'on souhaite limiter l'accès à internet ou éviter les temps de réponse lents lors de la résolution de noms de domaine.

```
S1(config)# no ip domain-lookup
```

Activation de la recherche DNS :

Activer la recherche DNS permet de traduire un nom d'hôte (par exemple www.google.com) en une adresse IP (par exemple 216.58.215.110).

Cela rend plus facile pour les utilisateurs de se connecter aux serveurs et de naviguer sur le Web en utilisant des noms de domaine au lieu d'adresses IP.

```
S1(config)# ip domain-lookup
```

Ajout d'une entrée à la table des noms d'hôtes IP :

La commande "**ip host**" permet de configurer un nom d'hôte et son adresse IP associée sur un équipement réseau.

Cela permet d'accéder à l'hôte en utilisant son nom au lieu de son adresse IP.

Par exemple, pour configurer un hôte nommé "**serveur**" avec l'adresse IP "**192.168.1.10**", vous pouvez utiliser la commande suivante :

```
S1(config)# ip host serveur 192.168.1.10
```

Configuration d'un mot de passe (en clair) à l'accès ENABLE :

La commande "**enable password**" permet de définir un mot de passe pour accéder à la configuration avancée (mode enable) d'un équipement réseau.

Par exemple, pour définir le mot de passe "**abc123**" pour accéder au mode enable, on peut utiliser la commande suivante :

```
S1(config)# enable password abc123
```

Configuration du mot de passe chiffré du mode privilégié « F@ormip2 » :

La commande "**enable secret**" permet aussi de configurer un mot de passe afin de protéger l'accès au mode enable d'un équipement réseau.

La différence, c'est que ce mot de passe est **chiffré**.

Par exemple, pour configurer le mot de passe "**cisco123**" pour l'accès au mode enable, vous pouvez utiliser la commande suivante :

```
S1(config)# enable secret cisco123
```



Il est important de noter que le mot de passe "**enable secret**" **remplacera le mot de passe "enable"** s'il est déjà configuré sur l'équipement.

De plus, il est **recommandé** d'utiliser la commande "**enable secret**" plutôt que "enable password", car le mot de passe "**enable secret**" est **chiffré et plus sécurisé**.

Configuration du mot de passe des lignes VTY :

La commande "**line vty**" est utilisée pour configurer **les connexions à distance** à l'équipement réseau.

La commande "**password**" est utilisée pour définir un mot de passe pour **la connexion à distance**.

Et la commande "**login**" permet d'activer l'authentification par mot de passe pour les connexions VTY (Virtual Teletype)

```
S1(config)# line vty 0 4
S1(config-line)# password cisco123
S1(config-line)# login
```

Ces commandes activent l'authentification par mot de passe pour les connexions VTY sur les interfaces de ligne virtuelle 0 à 4.



Le "**0**" compte comme une connexions VTY

Configuration du mot de passe de la ligne "console 0":

La commande "**line console 0**" permet de configurer un mot de passe pour l'accès physique d'un équipement réseau. C'est-à-dire en utilisant un câble console.

```
S1(config)# line console 0
S1(config-line)# password cisco123
S1(config-line)# login
```

Activation du service de chiffrement des mots de passe :

La commande "**service password-encryption**" permet de chiffrer l'ensemble des mots de passe qui sont configurés sur l'équipement.

```
S1(config)# service password-encryption
```

Configuration d'une adresse IP sur l'interface d'un routeur

La commande "**interface**" permet de spécifier l'interface sur laquelle la configuration doit être appliquée.

La commande "**ip address**" permet de configurer l'adresse IP et le masque de sous-réseau qui seront utilisés par l'interface pour communiquer sur le réseau.

```
Router(config)# interface G0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
```



Il est important de noter que la commande "**interface**" doit être suivie du nom de l'interface sur laquelle la configuration doit être appliquée.
Tandis que la commande "**ip address**" doit être suivie de l'adresse IP et du masque de sous-réseau à configurer.



Ces deux commandes sont souvent utilisées conjointement pour configurer les interfaces de communication de l'équipement.

Activation/désactivation d'une interface d'un routeur :

La commande "**no shutdown**" permet de mettre en ligne une interface qui a été précédemment mise hors ligne en utilisant la commande "**shutdown**".

```
Router(config)# interface G0/1
Router(config-if)# shutdown
Router(config-if)# no shutdown
```



Ces deux commandes sont utilisées pour contrôler **l'état de l'interface** et permettent de **mettre en ligne ou hors ligne l'interface de communication de l'équipement**.

Configuration d'une description d'une interface :

La commande "**description**" permet aux administrateurs réseau de décrire de manière plus précise l'utilisation ou le rôle de l'interface dans le réseau.

```
Router(config)# interface G0/1
Router(config-if)# description Connexion au serveur de fichiers
```



Il est important de noter que la commande "**description**" est facultative et n'a pas d'impact sur le fonctionnement de l'interface.



Elle sert simplement à fournir une description **plus précise** de l'interface et de **son rôle dans le réseau**.

Configuration de l'adresse IP d'une interface de gestion d'un commutateur :

La commande "**interface vlan**" permet de créer et de configurer des réseaux locaux virtuels sur l'équipement.

```
Router(config)# interface vlan 1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

La commande "**ip address 192.168.1.1 255.255.255.0**" configure l'adresse IP de l'**interface VLAN 1** en tant qu'adresse IP **192.168.1.1** et le masque de sous-réseau en **255.255.255.0**.

Cette configuration permet à l'**interface VLAN 1** de communiquer avec d'autres équipements sur le réseau en utilisant l'**adresse IP et le masque de sous-réseau spécifiés**.



Les **interfaces VLAN** permettent de créer plusieurs réseaux locaux virtuels sur un même équipement de réseau, ce qui peut être utile pour **séparer** les différents trafics de réseau et améliorer la sécurité et la performance du réseau.

Affichage de la configuration IP de toutes les interfaces :

La commande "**show ip interface brief**" permet d'afficher un résumé des interfaces de communication de l'équipement.

Elle permet aux administrateurs réseau de voir rapidement **l'état et les paramètres de chaque interface de l'équipement**.

Router# show ip interface brief					
Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.0.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

Dans cet exemple, la sortie de la commande "**show ip interface brief**" affiche le nom, l'adresse IP, l'état de configuration, l'état de l'interface et le protocole de chaque interface de l'équipement.

On peut voir que l'interface GigabitEthernet 0/1 est configurée manuellement et est en ligne, tandis que les interfaces GigabitEthernet 0/0, 0/2 et le Vlan 1 ne sont pas configurées et sont hors ligne (Administrativement coupé).



Il est important de noter que la commande "**show ip interface brief**" est une commande en lecture seule qui ne modifie pas la configuration de l'équipement de réseau.

Configuration du mode "Duplex":

La commande "duplex" permet de configurer le mode de duplex de communication d'une interface de réseau.

Elle permet de définir si l'interface fonctionne en mode :

- duplex simple
- duplex intégral
- ou duplex auto

```
S1(config)# interface G0/1
S1(config-if)# duplex half
S1(config-if)# duplex full
S1(config-if)# duplex auto
```

❷ Dans le premier exemple, la commande "**duplex half**" configure l'interface GigabitEthernet 0/1 en **mode duplex simple**.

Cela signifie que l'interface peut envoyer et recevoir des données, mais pas simultanément.

Le mode duplex simple (half) est souvent utilisé sur les interfaces de réseau à bas débit, comme les interfaces de réseau de données (RDD) ou les interfaces téléphoniques (POTS).

❷ Dans le deuxième exemple, la commande "**duplex full**" configure l'interface GigabitEthernet 0/1 en **mode duplex intégral**.

Cela signifie que l'interface peut envoyer et recevoir des données simultanément.

Le mode duplex intégral est souvent utilisé sur les interfaces de réseau à haut débit, comme les interfaces Ethernet.

❷ Dans le troisième exemple, la commande "**duplex auto**" configure l'interface GigabitEthernet 0/1 en **mode duplex automatique**.

Cela signifie que l'interface peut s'adapter automatiquement au mode de duplex utilisé par l'équipement auquel elle est connectée.

Le mode duplex automatique est souvent utilisé pour éviter les conflits de mode de duplex entre les équipements de réseau.

Affichage du mode Duplex d'une interface :

```
S1#show interface G0/1
```

```
GigabitEthernet0/1 is down, line protocol is down (disabled)
Hardware is Lance, address is 0001.9716.4019 (bia 0001.9716.4019)
BW 1000000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Half-duplex, 1000Mb/s
```

Affichage de la configuration en cours (RAM) :

Le fichier de configuration "**running-config**" est un fichier de configuration **en cours d'exécution** sur l'équipement.

Il contient tous les paramètres de configuration qui sont actuellement appliqués sur l'équipement et qui sont utilisés pour contrôler son fonctionnement.

La commande "**show running-config**" permet aux administrateurs réseau de voir quelles configurations sont actuellement appliquées sur l'équipement et de vérifier que les paramètres de configuration sont corrects.

```
S1#show running-config
```

```
Building configuration...
Current configuration : 1210 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
```

Affichage de la configuration initiale (NVRAM), c'est à dire de démarrage :

Le fichier de configuration "**startup-config**" est un fichier de configuration de démarrage sur l'équipement.

Il contient tous les paramètres de configuration qui sont chargés lorsque l'équipement démarre et qui sont utilisés pour contrôler son fonctionnement.

S1#**show startup-config**

```
Using 1076 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname S1
!
```



Il est important de noter que le fichier de configuration "**startup-config**" est en général utilisé pour enregistrer la configuration de l'équipement de manière permanente, de sorte qu'elle soit chargée chaque fois que l'équipement démarre.

En effet, cela permet aux administrateurs de réseau de configurer une fois l'équipement et de ne pas avoir à reconfigurer chaque fois qu'il redémarre...

Il est également possible de sauvegarder le fichier de configuration "**running-config**" dans le fichier de configuration "**startup-config**" à l'aide de la commande "**copy running-config startup-config**".

Cette commande permet de mettre à jour le fichier de configuration "**startup-config**" avec la configuration actuelle de l'équipement, de sorte que les modifications apportées à la configuration en cours d'exécution soient conservées lorsque l'équipement redémarre.

En général, les fichiers de configuration "**running-config**" et "**startup-config**" sont utilisés conjointement pour configurer et enregistrer la configuration de l'équipement réseau, de manière permanente.

Ils permettent aux administrateurs réseau de **configurer et de gérer** l'équipement de manière efficace et de résoudre rapidement les problèmes de réseau.

Affichage du contenu de la mémoire Flash :

La commande "**show flash:**" permet de lister le contenu de la carte flash de l'équipement réseau.

La mémoire flash est une mémoire de stockage non volatile utilisée par l'équipement afin d'enregistrer des fichiers tels que les images de système d'exploitation et les fichiers de configuration.

La commande "**show flash:**" affiche les noms et les tailles de tous les fichiers enregistrés dans la mémoire, ainsi que l'espace libre et l'espace total disponibles.

```
Switch# show flash:
Directory of flash:/

 1 -rw-  4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin

64016384 bytes total (59345929 bytes free)
```

Envoi d'une requête ICMP à une adresse IP :

La commande "**ping**" est utilisée dans le but de tester la connectivité réseau entre deux appareils. Elle envoie des paquets ICMP de données à destination de l'appareil cible et attend une réponse.

- ⌚ Si l'appareil cible répond, cela signifie qu'il y a une connexion réseau active entre les deux appareils et que les données peuvent être transmises correctement.
- ⌚ Si l'appareil cible ne répond pas, cela peut indiquer un problème de connectivité réseau.

```
S1#ping 192.168.0.11
```

Traçage de la route vers une adresse IP :

La commande "**traceroute**" (ou "tracert" sous Windows) permet de suivre le chemin emprunté par les données à travers le réseau entre deux appareils.

Elle envoie des paquets de données à destination de l'appareil cible et enregistre chaque appareil traversé par les données sur le chemin.

```
S1#traceroute 192.168.0.11
```

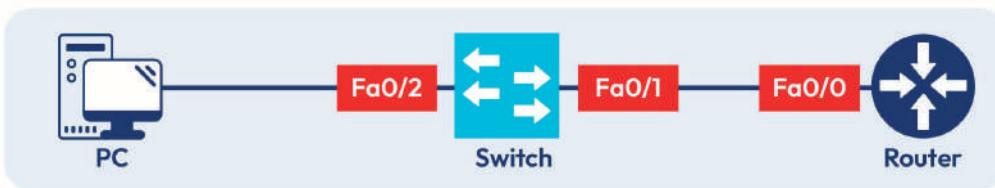
Connexion à distance à l'aide du protocole Telnet à une adresse IP :

La commande "telnet" permet de se connecter à distance à un appareil réseau via une connexion réseau.

Elle permet de se connecter à l'interface de ligne de commande (CLI) d'un appareil et d'exécuter des commandes à distance, comme si vous étiez physiquement connecté à l'appareil en utilisant un terminal ou une invite de commandes.

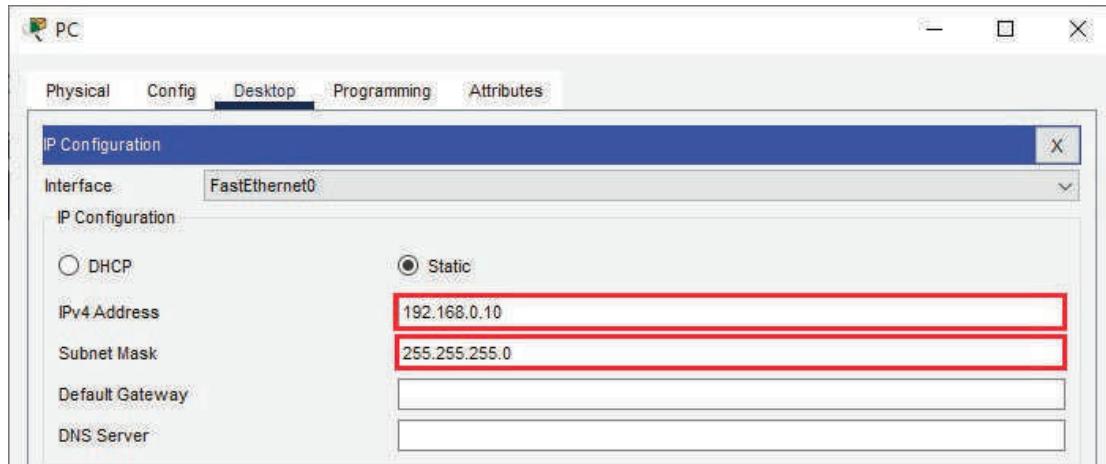
S1#**telnet** 192.168.0.11

CONFIGURATION DE L'ACCÈS À DISTANCE AVEC TELNET :



Étape 1 : Au niveau du PC

Tout d'abord, il faut configurer l'adresse IP du PC, qui jouera le rôle de "client Telnet".



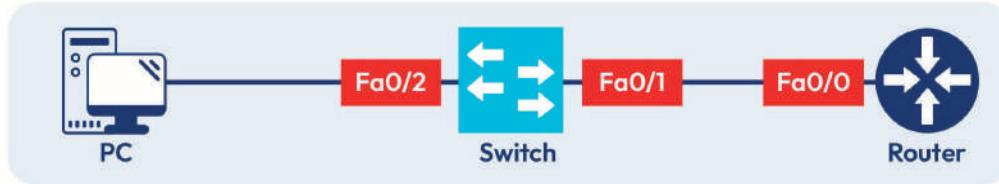
Le client Telnet est disponible sur **Packet Tracer**.

Packet Tracer est un logiciel de simulation de réseaux informatiques.

Il permet de créer virtuellement des réseaux informatiques et de les simuler afin de comprendre comment ils fonctionnent et comment ils sont configurés.

C'est un outil précieux pour l'apprentissage des réseaux informatiques

Étape 2 : Au niveau du routeur.



```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret Formip1
R1(config)#line vty 0 15
R1(config-line)#password Formip2
R1(config-line)#login
R1(config-line)#exit
R1(config)# Interface Fa0/0
R1(config-if)#ip address 192.168.0.1 255.255.255.0
R1(config-if)#no shutdown
```

Étape 3 : Vérification de l'accès à distance par Telnet

```
C:\>telnet 192.168.0.1
Trying 192.168.0.1 ...Open

User Access Verification

Password: ← Mot de passe VTY
Router>enable
Password: ← Mot de passe
d'exécution privilégiée
Router#
Router#
```

2.5. Fonctionnement d'un commutateur

Un **commutateur** est un appareil réseau qui permet de connecter plusieurs ordinateurs et appareils ensemble, au sein d'un réseau local (LAN).

Le **commutateur** utilise des câbles dans le but d'envoyer et recevoir des données à des vitesses très rapides entre les différents appareils connectés.

- ➲ Lorsqu'un appareil (comme un ordinateur) a besoin d'envoyer ou de recevoir des données à un autre appareil (comme une imprimante), il envoie d'abord une demande au commutateur.
- ➲ Le commutateur lit cette demande et décide où envoyer les données en utilisant ce que l'on appelle une **table de commutation**.
- ➲ La **table de commutation** est comme une liste qui dit au commutateur où envoyer les données en fonction de l'adresse de l'appareil cible.

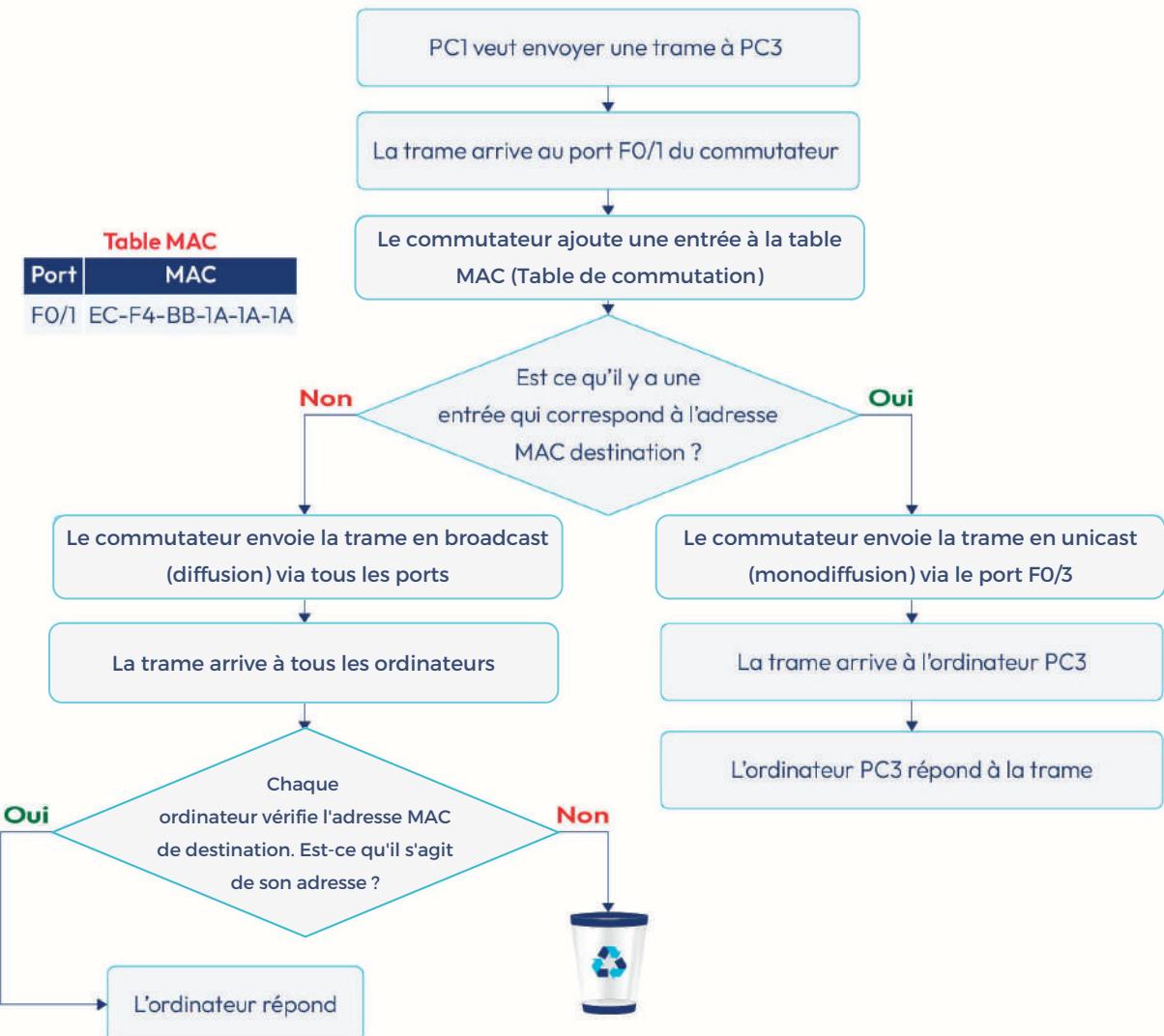
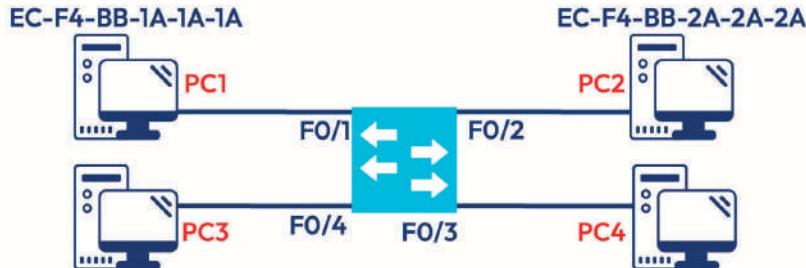
Un commutateur se base donc sur la **table de commutation** (Table MAC) pour commuter les trames vers leurs destinations.

La **table MAC** peut être affichée en utilisant la commande : **show mac-address-table**

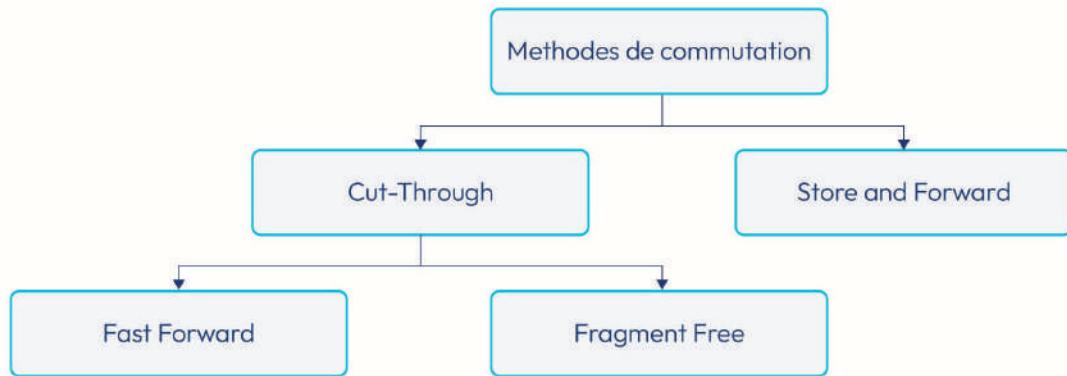
S1# show mac address-table			
Mac Address Table			
Vlan	Mac Address	Type	Ports
1	0001.631e.5220	DYNAMIC	Fa0/3
1	0001.9609.6692	DYNAMIC	Fa0/1

- ➲ Si une trame est destinée à un ordinateur dont l'adresse MAC est **0001.631e.5220**, la trame sera envoyée via le port **F0/3**
- ➲ Si une trame est destinée à un ordinateur dont l'adresse MAC est **0001.9609.6692**, la trame sera envoyée via le port **F0/1**

Exemple : Trame de PC1 vers PC3

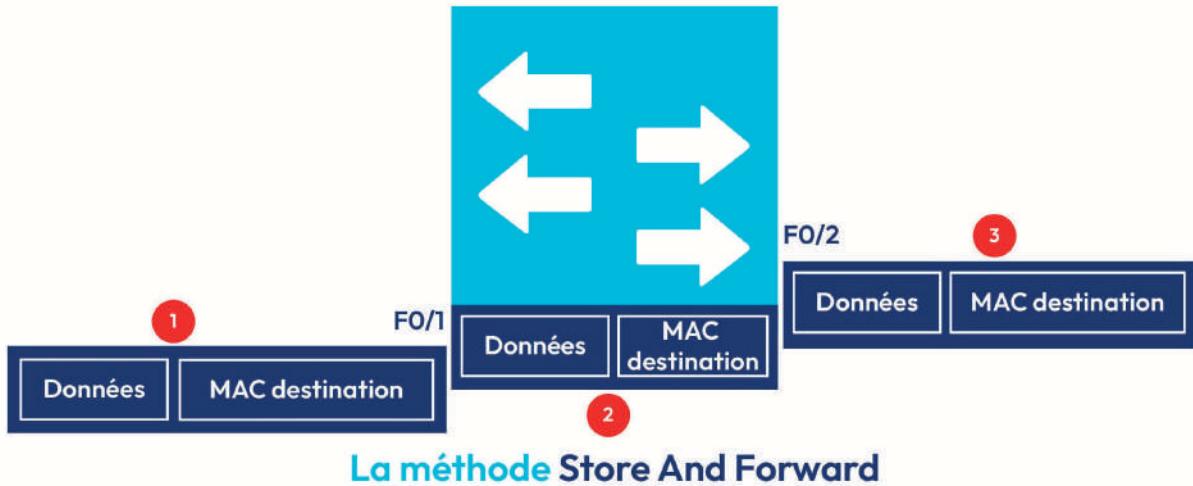


2.6. Modes de commutation :



2.6.1. Store And Forward

Quand le commutateur utilise la méthode « **Store And Forward** », il attend la réception de la totalité de la trame avant de faire la commutation.



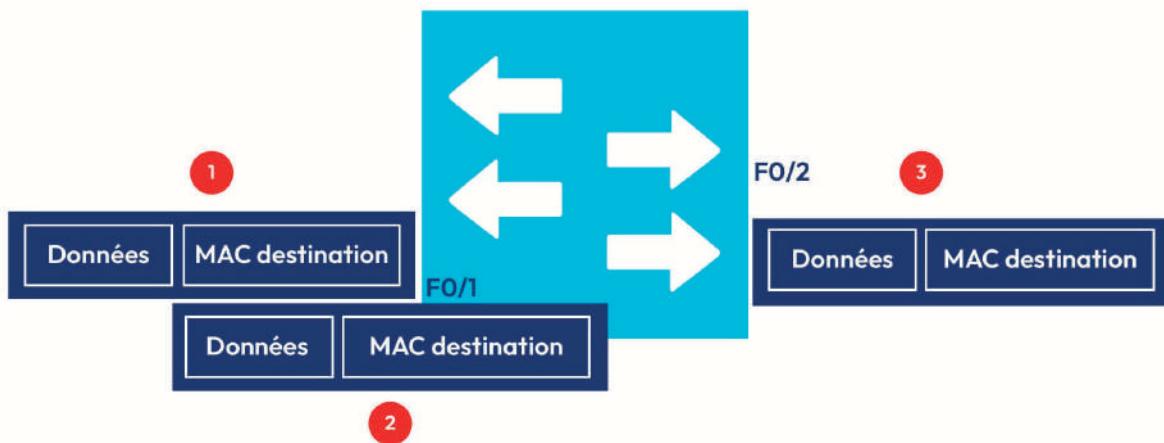
2.6.2. Cut-Through

Quand le commutateur utilise la méthode Cut-Through, il commence l'envoi de la trame après la réception d'une partie de cette dernière.

FAST FORWARD

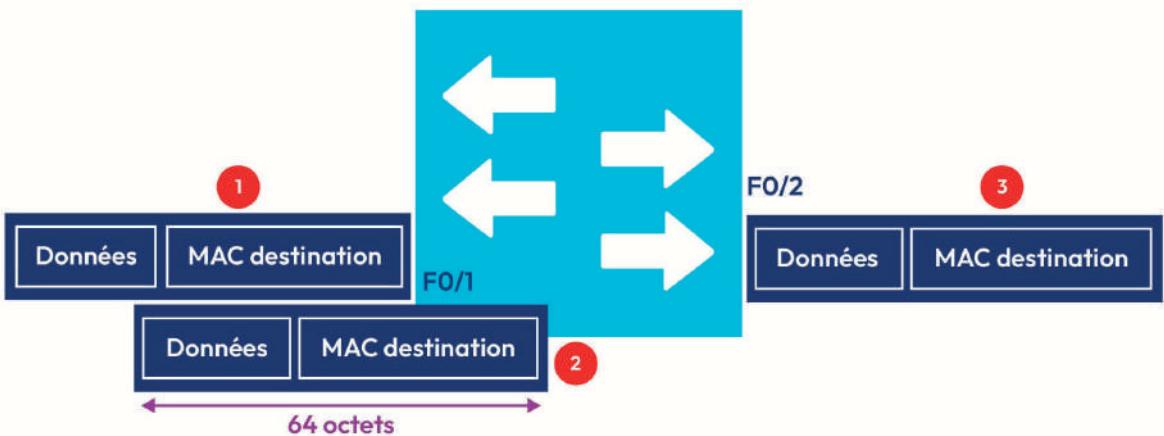
Quand le commutateur utilise la méthode « **Fast Forward** », il commence l'envoi de la trame dès la réception de l'adresse MAC de destination.

- Méthode très rapide par rapport aux autres méthodes
- Beaucoup d'erreurs, car la trame n'est pas vérifiée avant la commutation



La méthode Fast Forward

FRAGMENT FREE

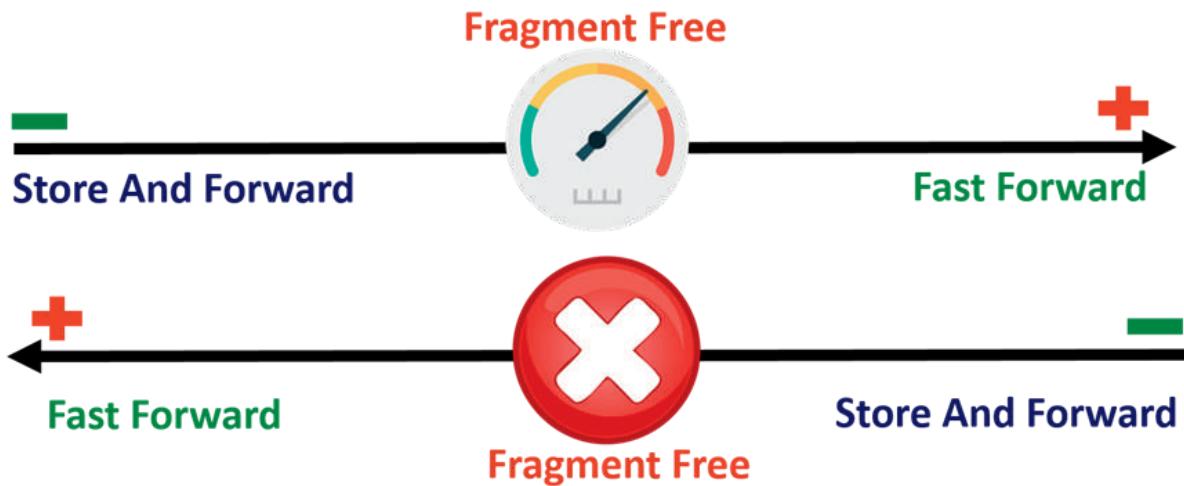


La méthode Fragment Free

Quand le commutateur utilise la méthode « Fragment Free », il attend la réception des 64 premiers octets de la trame avant de commencer la commutation, car la plupart des erreurs et des collisions sur le réseau surviennent au niveau de ces 64 premiers octets.

- ➊ Méthode plus rapide que la méthode « **Store And Forward** » et moins rapide que la méthode « **Fast Forward** »
- ➋ Quelques d'erreurs, car la trame n'est vérifiée que partiellement avant la commutation

Pour résumer :



2.7. Sécurité d'un commutateur

2.7.1. Accès à distance à un commutateur

ACCÈS NON SÉCURISÉ VIA TELNET

192.168.0.100/24



PCI

192.168.0.10/24



S1

```
S1>enable
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret Formip1
S1(config)#line vty 0 15
S1(config-line)#password Formip2
S1(config-line)#transport input telnet
S1(config-line)#login
S1(config-line)#exit
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.0.10 255.255.255.0
S1(config-if)#no shutdown
```

```
C:\>telnet 192.168.0.10
Trying 192.168.0.10 ...Open
User Access Verification

Password: Formip2
Switch>enable
Password: Formip1
Switch#
```

ACCÈS SÉCURISÉ VIA SSH



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret Formip321
S1(config)#ip domain-name formip.com
S1(config)#username Formip secret Formip123
S1(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: S1.formip.com
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:3:52.987: %SSH-5-ENABLED: SSH 1.99 has been enabled
S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#ip ssh version 2
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.0.10 255.255.255.0
S1(config-if)#no shutdown
```

```
C:\>SSH -l Formip 192.168.0.10
Password: Formip123
S1>enable
Password: Formip321
S1#
```

2.7.2. Sécurité des ports d'un commutateur

DÉSACTIVATION DES PORTS NON UTILISÉS

Désactivation des ports inutilisés (de F0/5 à F0/24) :

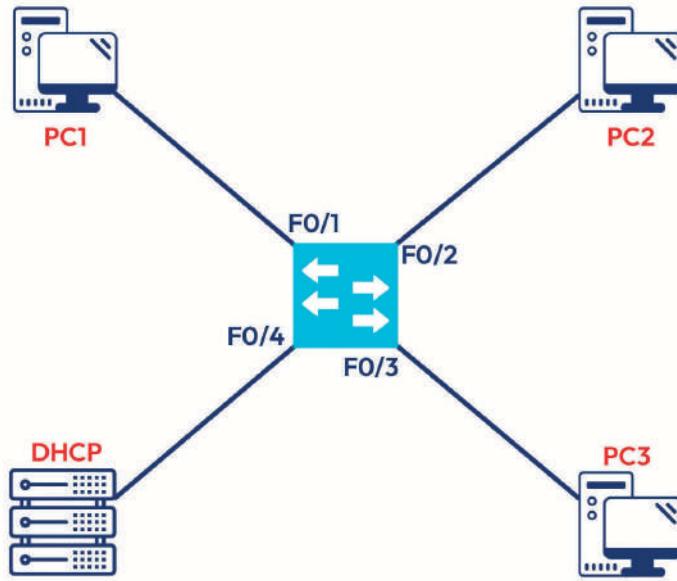
La commande "**interface range**" permet de configurer plusieurs interfaces de manière groupée. Cela signifie que vous pouvez appliquer une commande de configuration à plusieurs interfaces **en une seule fois**, au lieu de devoir la répéter pour chaque interface individuellement.

```
S1(config)# interface range F0/5-F0/24
S1(config-if)# shutdown
```

SURVEILLANCE DHCP

La surveillance DHCP permet de limiter les attaques DHCP :

- ➊ Épuisement des ressources DHCP
- ➋ Faux serveur DHCP



Activation de la surveillance DHCP:

Le **DHCP spoofing** est une attaque dans laquelle un attaquant envoie des paquets DHCP falsifiés dans un réseau, dans le but de rediriger les clients vers des serveurs DHCP malveillants ou de leur attribuer des adresses IP incorrectes.

Cela peut entraîner une **perte de connectivité** pour les clients ou même une **fuite de données sensibles** si les clients sont redirigés vers des serveurs malveillants.

```
S1(config)# ip dhcp snooping
```

Activation de la surveillance DHCP pour les VLANs 1, 10 et 20

```
S1(config)# ip dhcp snooping vlan 1,10,20
```

Configuration du port connecté au serveur DHCP comme port fiable :

```
S1(config)# interface F0/4
S1(config-if)# ip dhcp snooping trust
```

Par défaut, les autres ports du commutateur seront des ports non fiables.

Limitation de la fréquence à laquelle un pirate peut transmettre de fausses requêtes DHCP au serveur DHCP via des ports non fiables (5 requêtes par seconde) :

```
S1(config)# interface F0/4
S1(config-if)# ip dhcp snooping limit rate 5
```

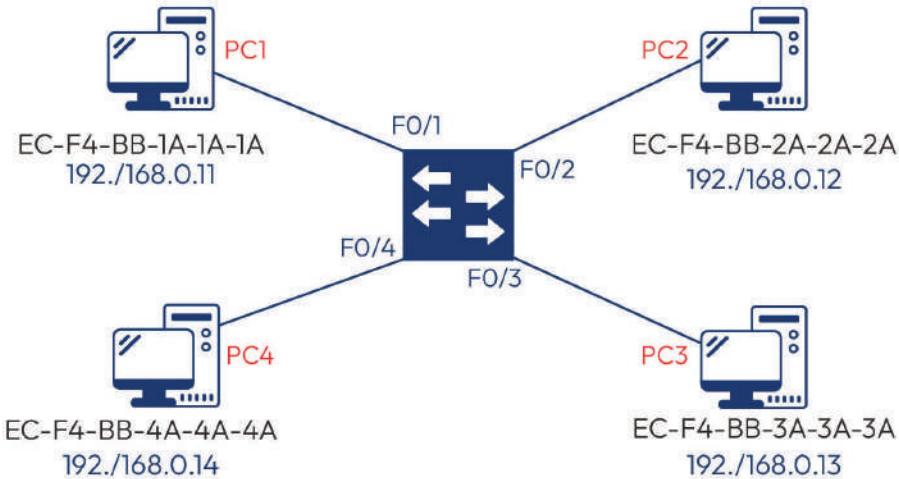
La commande "ip dhcp snooping" permet de configurer le DHCP snooping sur un équipement Cisco. Lorsque le DHCP snooping est activé, l'équipement Cisco inspecte tous les paquets DHCP entrant et vérifie qu'ils proviennent d'un serveur DHCP légitime. Si un paquet DHCP est détecté comme étant falsifié, il est rejeté et le client ne reçoit pas l'adresse IP incorrecte.

SÉCURITÉ DES PORTS

La sécurité des ports est utilisée pour lutter contre les attaques **CAM OverFlow**.

Une attaque **CAM Overflow** est une attaque qui vise à dépasser la capacité de stockage de la table d'adressage MAC d'un commutateur réseau (CAM, pour Content Addressable Memory).

L'attaquant envoie de nombreux paquets avec des adresses MAC aléatoires au commutateur, ce qui peut entraîner une perte de connectivité et rendre le réseau instable.



Scénario 1 : Configuration manuelle

PC1 est le seul ordinateur associé au port F0/1 :

Configuration du port F0/1 comme port d'accès :

```
S1(config)# interface F0/1  
S1(config-if)# switchport mode access
```

Activation de la sécurité au niveau du port F0/1 :

La commande "switchport port-security" est utilisée pour configurer la sécurité des ports sur un équipement Cisco.

Elle permet de limiter le nombre d'adresses MAC qui peuvent être associées à un port donné, ce qui peut aider à protéger contre les attaques de type MAC spoofing ou CAM Overflow.

```
S1(config)# interface F0/1  
S1(config-if)# switchport port-security
```

Association de l'adresse MAC du PC1 au port F0/1 :

```
S1(config)# interface F0/1  
S1(config-if)# switchport port-security mac-address EC-F4-BB-1A-1A-1A
```

Configuration du mode de violation :

Il existe 3 modes :

RESTRICT	PROTECT	SHUTDOWN
Rejette silencieusement les paquets offensifs	Rejette les paquets offensifs ET donne des alertes	Rejette les paquets offensifs ET place le port dans un état de désactivation (Shutdown)

Restrict :

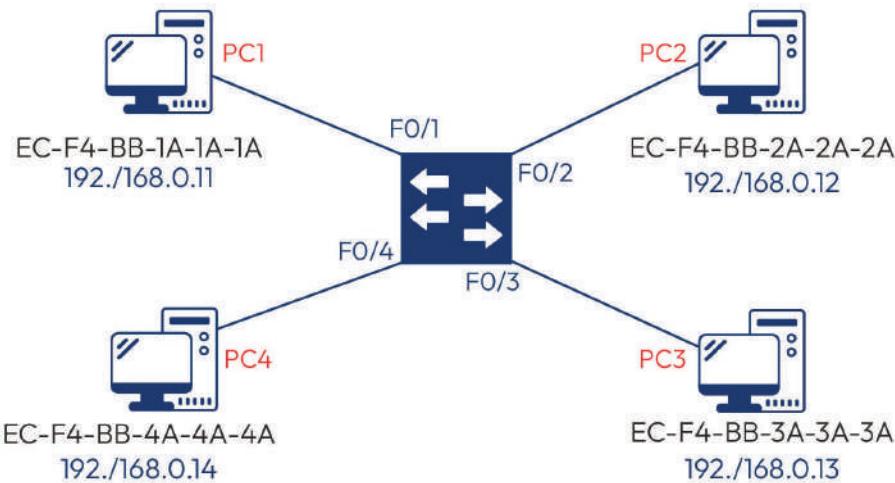
```
S1(config)# interface F0/1  
S1(config-if)# switchport port-security violation restrict
```

Protect :

```
S1(config)# interface F0/1  
S1(config-if)# switchport port-security violation protect
```

Shutdown :

```
S1(config)# interface F0/1  
S1(config-if)# switchport port-security violation shutdown
```



Scénario 2 : Configuration dynamique

3 ordinateurs au maximum seront associés au port F0/2 :

Configuration du port F0/2 comme port d'accès :

```
S1(config)# interface F0/2
S1(config-if)# switchport mode access
```

Activation de la sécurité au niveau du port F0/2 :

```
S1(config)# interface F0/2
S1(config-if)# switchport port-security
```

Configuration du nombre maximal d'adresses MAC autorisées sur le port F0/2 :

```
S1(config)# interface F0/2
S1(config-if)# switchport port-security maximum 3
```

Activation de l'apprentissage dynamique des adresses MAC des ordinateurs :

```
S1(config)# interface F0/2
S1(config-if)# switchport port-security mac-address sticky
```

Cette commande active la fonctionnalité **sticky MAC** sur le port en cours de configuration.

Toutes les adresses MAC qui sont associées au port seront automatiquement ajoutées à la liste d'adresses MAC autorisées pour ce port.

Reste plus qu'à configurer le mode de violation :

Restrict :

```
S1(config)# interface F0/2
S1(config-if)# switchport port-security violation restrict
```

Protect :

```
S1(config)# interface F0/2
S1(config-if)# switchport port-security violation protect
```

Shutdown :

```
S1(config)# interface F0/2
S1(config-if)# switchport port-security violation shutdown
```

Remarque :

	ACHEMINEMENT DU TRAFIC	ENVOI DES MESSAGES SYSLOG	INCREMENTATION DU COMPTEUR DE VIOLATION	ARRÊT DU PORT
Shutdown	Non	Oui	Oui	Oui
Restrict	Non	Oui	Oui	Non
Protect	Non	Non	Non	Non

Commandes de vérification :

Vérification de la configuration de la sécurité des ports au niveau du port F0/1 :

```
S1# show port-security interface F0/1
```

Vérification des adresses MAC sécurisées :

```
S1# show port-security address
```

Affichage de l'état du port F0/1

```
S1# show interface F0/1 status
```