Partie B : Les notions de base sur la commutation

2.1 Présentation de l'IOS :

Tous les périphériques électroniques nécessitent un système d'exploitation.

- Windows, Mac et Linux pour les PC et ordinateurs portables
- Apple iOS et Android pour les Smartphones et tablettes
- Cisco IOS pour les périphériques réseau (par exemple : les commutateurs, les routeurs, les points d'accès sans fil, le pare-feu, etc.).

- Les périphériques Cisco utilisent le **système d'exploitation interréseau Cisco (IOS)**.

Rôle du système d'exploitation

- L'utilisation d'une interface graphique permet à un utilisateur d'effectuer les opérations suivantes :
  - Utiliser une souris pour faire des sélections et exécuter des programmes ;
  - Entrer des commandes textuelles ;
- L'utilisation d'une interface de ligne de commande sur un commutateur ou un routeur Cisco IOS permet à un technicien réseau d'effectuer les opérations suivantes :
  - Utiliser un clavier pour exécuter des programmes réseau basés sur CLI ;
  - Utiliser un clavier pour entrer des commandes textuelles ;
- Il existe de nombreuses versions différentes de Cisco IOS :
  - IOS pour les commutateurs, les routeurs et les autres périphériques réseau Cisco
  - Versions numérotées d'IOS pour un périphérique réseau Cisco donné
- Tous les périphériques sont livrés avec un IOS et un jeu de fonctionnalités par défaut. Il est possible de mettre à niveau la version ou un ensemble de fonctionnalités de l'IOS.
- Un IOS peut être téléchargé à partir de cisco.com. Toutefois, un compte Cisco Connection Online (CCO) est requis.

Remarque : ce cours sera axé sur la version 15.x de Cisco IOS.

Méthodes d'accès

- Les trois façons les plus courantes d'accéder à IOS sont les suivantes :
  - **Port de console :** port série hors bande utilisé principalement à des fins de gestion comme la configuration initiale du routeur.
  - **Secure Shell (SSH) :** méthode intrabande pour établir à distance et en toute sécurité une session CLI sur un réseau. Les informations d'authentification des utilisateurs, les mots de passe et les commandes envoyés sur le réseau sont chiffrés. Il est fortement conseillé d'utiliser SSH plutôt que Telnet dans la mesure du possible.
  - **Telnet :** interfaces intrabandes permettant d'établir une session CLI à distance via une interface virtuelle sur un réseau. Les informations d'authentification des utilisateurs, les mots de passe et les commandes sont envoyés sur le réseau en clair.

Remarque : le port AUX est une méthode plus ancienne pour établir une session CLI à distance via une connexion téléphonique commutée utilisant un modem.

Programme d'émulation de Terminal

- Quelle que soit la méthode d'accès, un programme d'émulation de terminal sera nécessaire. Les programmes d'émulation de terminal les plus populaires comprennent PuTTY, Tera Term, SecureCRT, et OS X Terminal.

Modes de fonctionnement de Cisco IOS

- Les modes Cisco IOS utilisent une structure de commande hiérarchique.
- Chaque mode présente une invite distincte et permet d'effectuer des tâches particulières grâce à des commandes spécifiques disponibles uniquement dans ce mode.

Principaux modes de commande

- Le mode d'exécution utilisateur n'autorise qu'un nombre limité de commandes de surveillance de base.
  - Il est souvent qualifié de mode de « visualisation seule » pour cette raison.
  - Par défaut, aucune authentification n'est requise pour accéder au mode d'exécution utilisateur, mais cela doit être sécurisé.
- Le mode d'exécution privilégié permet d'exécuter des commandes de configuration et de gestion.
  - Il est souvent appelé « mode actif » parce qu'il nécessite la commande d'exécution utilisateur **enable**.
  - Par défaut, aucune authentification n'est requise pour accéder au mode d'exécution privilégié, mais cela doit être sécurisé.

Mode de commande	Invite du périphérique par défaut	ordre	Pour passer d'un mode au mode suivant	Pour revenir à un mode précédant
Mode d'exécution utilisateur	Switch> Router>	1	Switch>enable Router>enable	
Mode d'exécution Privilégié	Switch# Router#	2	Switch#config t Router#config t	Switch#disable ou Router#exit
Modes de configuration Globale	Switch(config)# Router(config)#	3		Switch(config)#exit Router(config)#end

Modes de commande de configuration

- Le principal mode de configuration est appelé mode de **configuration globale** ou simplement **config. globale**.
  - Utilisez la commande **configure terminal** pour y accéder.
  - Les modifications apportées affectent le fonctionnement du périphérique.
- **Il est possible d'accéder à des sous-modes de configuration spécifiques à partir du mode de configuration globale.** Chacun de ces modes permet de configurer une partie ou une fonction spéciale du périphérique IOS.
  - **Mode interface** : pour configurer l'une des interfaces réseau.
  - **Mode ligne** : configurer l'accès par la console, par SSH, par Telnet, ou l'accès AUX.

Mode Interface	Mode Line	Mode Router
Switch(config)#interface F0/1 Router(config)# interface G0/1	Switch(config)#line console 0 Router(config)# line vty 0 4	Router(config)# router rip
Switch(config-if)# Router(config-if)#	Switch(config-line)# Router(config-line)#	Router(config-router)#

Pour revenir au mode de configuration globale, taper: **exit**

Et pour revenir au mode d'exécution privilégié, taper : **end**

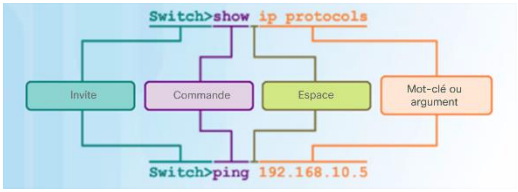
Structure des commandes IOS de base

Un périphérique Cisco IOS prend en charge de nombreuses commandes. Chaque commande IOS a un format ou une syntaxe spécifique et ne peut être exécutée que dans le mode approprié.

La syntaxe d'une commande est constituée de la commande suivie des mots-clés et des arguments appropriés.

- **Mot-clé** : il s'agit d'un paramètre spécifique défini dans le système d'exploitation (dans la figure, **protocoles IP**)
- **Argument** : non prédéfini ; il s'agit d'une valeur ou d'une variable définie par l'utilisateur (dans la figure, **192.168.10.5**)

Après avoir tapé une commande complète suivie des mots-clés et des arguments adéquats, appuyez sur la touche **Entrée** pour la soumettre à l'interpréteur de commandes.



Fonctionnalités d'aide d'IOS

- Aide contextuelle IOS :
  - L'aide contextuelle fournit une liste de commandes et les arguments associés à ces commandes dans le contexte du mode actuel.
  - Pour afficher l'aide contextuelle tapez un point d'interrogation (**?**) à une invite quelconque.
- Vérification de la syntaxe des commandes IOS :
  - L'interpréteur de ligne de commande vérifie une commande saisie de gauche à droite pour déterminer quelle action est demandée.
  - Si l'interpréteur comprend la commande, IOS exécute l'action demandée et l'invite appropriée reparaît dans l'environnement ILC.
  - Si l'interpréteur détecte une erreur, IOS renvoie généralement des informations telles que « Commande ambiguë », « Commande incomplète », ou « Commande incorrecte ».

2.2 Configuration de base des périphériques

Noms des périphériques

- La première étape lors de la configuration d'un commutateur consiste à lui attribuer un nom de périphérique unique, ou nom d'hôte.
  - Les noms d'hôte apparaissent dans les invites de la CLI, peuvent être utilisés dans différents processus d'authentification entre les périphériques et doivent être utilisés dans les diagrammes de topologie.
  - Sans nom d'hôte, les périphériques réseau sont difficiles à identifier à des fins de configuration.
- La commande de configuration globale **hostname *nom*** sert à attribuer un nom.

Limitation de l'accès au périphérique

- **Étape 1** : sécurisez les périphériques réseau pour limiter physiquement l'accès en les plaçant dans des armoires de répartition et des racks verrouillés.
- **Étape 2** : appliquez des mots de passe sécurisés, car ils constituent la principale défense contre l'accès non autorisé aux périphériques réseau.

Configuration des mots de passe

- Sécurisez l'accès au mode d'exécution privilégié, en utilisant la commande de config. globale **enable secret *mot_de_passe***.
- Sécurisez l'accès au mode d'exécution utilisateur en configurant **la console** de ligne

Sécuriser le mode d'exécution utilisateur	Description
`Switch(config)#` **line console 0**	La commande passe en mode de configuration de console de ligne.
`Switch(config-line)#` **password** *password*	La commande spécifie le mot de passe de console de ligne.
`Switch(config-line)#` **login**	Cette commande configure le commutateur pour demander le mot de passe.

- Sécurisez l'accès Telnet ou SSH à distance en configurant les lignes VTY (terminal virtuel)

Sécurisation intrabande et horsbande	Description
`Switch(config)#` **line vty 0 15**	Les commutateurs Cisco prennent généralement en charge jusqu'à 16 lignes VTY numérotées de 0 à 15.
`Switch(config-line)#` **password** *password*	La commande spécifie le mot de passe de la ligne VTY.
`Switch(config-line)#` **login**	Cette commande configure le commutateur pour demander le mot de passe.

- Les fichiers **startup-config** et **running-config** affichent la plupart des mots de passe en clair. C'est une menace à la sécurité, car n'importe quel utilisateur peut voir les mots de passe s'il a accès à ces fichiers.
- Utilisez la commande de configuration globale **service password-encryption** pour chiffrer tous les mots de passe.
- La commande applique un chiffrement simple à tous les mots de passe non chiffrés.

Messages de bannière

Les bannières sont des messages qui s'affichent lorsqu'une personne tente d'accéder à un périphérique. Les bannières sont une partie importante du processus légal dans le cas où quelqu'un est poursuivi pour avoir pénétré par effraction dans un périphérique.
Configuré à l'aide de la commande **banner motd délimiteur *message* délimiteur** à partir du mode de configuration globale.
Vous pouvez utiliser comme délimiteur n'importe quel caractère tant qu'il est unique et ne figure pas dans le message (par exemple, #$%^&*).

Enregistrer le fichier de configuration en cours

Les périphériques Cisco utilisent un fichier de **configuration en cours** et un fichier de **configuration de démarrage**.

- Le fichier de configuration en cours est stocké dans la mémoire vive et contient la configuration en cours sur un périphérique Cisco IOS.
- Les modifications de configuration sont stockées dans ce fichier.
- Si l'alimentation est interrompue, la configuration en cours d'exécution est perdue.
- Utilisez la commande **show startup-config** pour afficher le contenu.
- Le fichier de configuration initiale est stocké dans la mémoire vive non volatile et contient la configuration qui sera utilisée par le périphérique au redémarrage.
- En général, la configuration en cours est enregistrée en tant que la configuration de démarrage.
- Si l'alimentation est interrompue, elle n'est ni perdue ni effacée.
- Utilisez la commande **show running-config** pour afficher le contenu.
- Utilisez la **commande copy running-config startup-config** pour enregistrer la configuration en cours.

Modifier le fichier de configuration en cours

- Si les modifications de configuration n'ont pas l'effet désiré, elles peuvent être supprimées individuellement ou le périphérique peut être redémarré sur la dernière configuration enregistrée en utilisant la commande **reload** en mode d'exécution privilégié.
  - La commande permet de restaurer la configuration initiale.
  - Dans l'affirmative, IOS affiche une invite vous demandant s'il doit enregistrer les modifications. Pour abandonner les modifications, entrez **n** ou **no**.
- Par ailleurs, si des modifications indésirables ont été enregistrées dans la configuration de démarrage, il peut être nécessaire d'effacer toutes les configurations à l'aide de la commande **erase startup-config** en mode d'exécution privilégié.

Exemple :

Attribuer le nom 'Sw-Floor-1' au commutateur	Switch(config)# **hostname** Sw-Floor-1
Sécuriser le mode d'exécution privilégié avec le mot de passe 'class'	Sw-Floor-1(config)# **enable secret class**
Sécuriser le mode d'exécution utilisateur (console) avec le mot de passe 'cisco'	Sw-Floor-1(config)# **line console 0** Sw-Floor-1(config-line)# **password cisco** Sw-Floor-1(config-line)# **login** Sw-Floor-1(config-line)# **exit**

Sécurisation le mode d'exécution utilisateur (16 premières lignes VTY) avec le mot de passe 'cisco'	Sw-Floor-1(config)# **line vty 0 15** Sw-Floor-1(config-line)# **password cisco** Sw-Floor-1(config-line)# **login**
Chiffrer tous les mots de passe	`Sw-Floor-1(config)# service password-encryption`
Définir une bannière avec délimiteur ' !'	`Sw-Floor-1(config)#banner motd ! acces restraint !`

Enregistrer la configuration en cours sur le mode d'exécution privilégié	`Sw-Floor-1#write`
	Ou
	`Sw-Floor-1# copy running-config startup-config`

2.3 Schémas d'adressage

Présentation de l'adressage IP

- Chaque périphérique final d'un réseau (PC, ordinateurs portables, serveurs, imprimantes, téléphones VoIP, caméras de sécurité, etc.) nécessite une configuration IP composée des éléments suivants :
  - **Adresse IP**
  - **Masque de sous-réseau**
  - **Passerelle par défaut** (en option pour certains périphériques)

Les adresses IPv4 sont affichées en format décimal à point composé de :

- 4 nombres décimaux 0 et 255
- Séparés par des points décimaux (points)
- Par exemple, 192.168.1.10, 255.255.255.0, 192.168.1.1

Interfaces et ports

- **Les commutateurs Cisco IOS de couche 2 sont équipés de ports physiques pour permettre à des périphériques de s'y connecter. Cependant, ces ports ne prennent pas en charge les adresses IP de couche 3.**
- **Pour se connecter à distance et gérer un commutateur de couche 2, il doit être configuré avec une ou plusieurs interfaces virtuelles de commutateur (SVI).**
- **Chaque commutateur possède un VLAN 1 SVI par défaut.**

Remarque : un commutateur de couche 2 ne nécessite pas d'adresse IP pour fonctionner. L'adresse IP SVI sert uniquement à gérer à distance un commutateur.

Interface virtuelle du commutateur

- Pour gérer à distance un commutateur, il doit également être configuré avec une configuration IP :
  - Toutefois, un commutateur n'est pas une interface Ethernet physique qui peut être configurée.
  - Au lieu de cela, vous devez configurer l'**interface virtuelle du commutateur (SVI)** de VLAN 1.

L'interface SVI de VLAN 1 doit être configurée avec :

- **Adresse IP** : identifie de façon unique le commutateur sur le réseau
- **Masque de sous-réseau :** identifie la partie réseau et hôte de l'adresse IP
- **Activée :** en utilisant la commande **no shutdown**.
- Utilisez la commande **show ip interface brief** en mode d'exécution privilégié pour vérifier.

Vérification de la connectivité

La commande **ping** peut être utilisée pour tester la connectivité vers un autre périphérique sur le réseau, un site web ou Internet.

Exemple : ping 8.8.8.8

Vérification de l'adressage de l'interface

- La configuration IP sur un hôte Windows est vérifiée à l'aide de la commande **ipconfig**.

- Pour vérifier les interfaces et les réglages d'adresse des périphériques intermédiaires tels que les commutateurs et les routeurs, utilisez la commande **show ip interface brief** en mode d'exécution privilégié.

Initiation aux réseaux commutés

Les commutateurs :

Facteur de forme

Quelques aspects qu'il faut tenir compte lors du choix des commutateurs :

- **Coût :** le coût d'un commutateur dépend du nombre et de la rapidité des interfaces, des fonctionnalités prises en charge et de sa capacité d'extension.
- **Densité :** nombre des ports.
- **Alimentation :** Supporte la technologie PoE(Power over Ethernet) qui permet d'alimenter les points d'accès, les téléphones IP et même des commutateurs compacts au moyen de la technologie PoE (Power over Ethernet).
  Certains commutateurs sur châssis prennent en charge des alimentations redondantes.
- **Fiabilité :** le commutateur doit fournir un accès permanent au réseau.
- **Vitesse des ports :** 10 ; 100 ; 1000mb/s ou plus.
- **Tampons de trames :** Taille de la mémoire qui enregistre les trames.
- **Évolutivité :** le commutateur doit donc comporter des possibilités de croissance.

Pour sélectionner le type d'un commutateur, le concepteur de réseau doit choisir une configuration fixe ou modulaire, et empilable ou non empilable et l'épaisseur du commutateur (en nombre d'unités de rack xU).

- ✓ **Commutateurs de configuration fixe :** Les commutateurs de configuration fixe prennent en charge uniquement les fonctionnalités et les options fournies d'origine avec le commutateur.
- ✓ **Commutateurs de configuration modulaire :** les commutateurs de configuration modulaire sont livrés avec des châssis de différentes tailles, qui permettent l'installation de plusieurs cartes d'interface modulaires. Ces cartes d'interface contiennent les ports.
- ✓ **Commutateurs de configuration empilable :** Les commutateurs de configuration empilable peuvent être interconnectés à l'aide d'un câble spécial fournissant un débit de bande passante élevé entre les commutateurs.

Transfert de trame

La décision du commutateur est basée sur le port d'entrée et sur l'adresse de destination du message.
Un commutateur LAN gère une table qu'il utilise pour déterminer l'acheminement du trafic.

Remplissage dynamique de la table d'adresses MAC d'un commutateur

Pour qu'un commutateur sache vers quel port transférer une trame, il doit tout d'abord apprendre quels périphériques existent sur chaque port.
Il remplit une table appelée **table d'adresses MAC ou table CAM (Content Addressable Memory, mémoire adressable par contenu)**.
Un commutateur renseigne la table d'adresses MAC sur la base des adresses MAC source des trames qu'il reçoit.

Le commutateur utilise les informations de la table d'adresses MAC pour envoyer des trames destinées à un périphérique donné au port qui a été attribué à ce périphérique.

Remarque :

- ✓ Lorsqu'un commutateur reçoit une trame entrante avec une adresse MAC de destination qui ne figure pas dans la table d'adresses MAC, il transfère la trame à tous les ports (inondation) sauf au port d'entrée de la trame.
- ✓ Il est possible que la table d'adresses MAC contient plusieurs adresses MAC pour un seul port connecté aux autres commutateurs (le cas ou ce port est connecté à un autre commutateur)

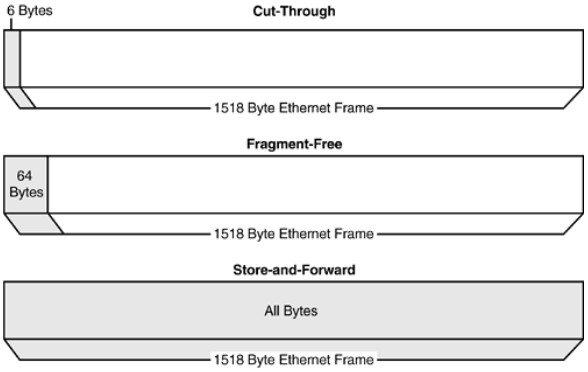
Méthodes de transfert par commutateur

- ➢ **La méthode par stockage et retransmission (Store and Forward)** décide de transférer une trame après avoir reçu la trame complète et contrôlé l'absence d'erreurs (Le dernier champ de la trame contient une

séquence de contrôle de trame (FCS, frame check séquence), que le commutateur compare avec ses propres calculs de FCS et s'il trouve une différence il abandonne la trame sinon il l'envoi vers le port qui convient).

La mise en tampon des ports d'entrée, prend en charge toute combinaison de vitesses Ethernet. Par exemple, le traitement d'une trame arrivant sur un port Ethernet 100 Mbit/s et à transférer sur une interface 1 Gbit/s ; dans ce cas-là aussi on utilise cette méthode de commutation.

- **La méthode cut-through** lance le processus de transfert dès que l'adresse MAC de destination d'une trame entrante et le port de sortie sont déterminés.



Cette méthode risque de transférer des trames non valides car il n'effectue aucun contrôle FCS.
Elle comporte deux caractéristiques principales :

- ✓ **Transmission rapide des trames** (FastForward)

Un commutateur cut-through peut décider de transférer une trame dès qu'il a trouvé l'adresse MAC de destination de la trame dans sa table d'adresses MAC.
En cas de taux d'erreur élevé dans le réseau (trames non valides), la commutation cut-through risque d'encombrer la bande passante avec des trames endommagées et incorrectes.

- ✓ **Fragment Free** : le commutateur attend la fin de la réception de la fenêtre de collision (64 octets) avant de transférer la trame. Elle assure un meilleur contrôle des erreurs que la méthode FastForward.

Domaines de commutation

Domaines de collision

- Dans les segments Ethernet basés sur des **concentrateurs**, les périphériques réseau sont en concurrence pour le support, car ils doivent transmettre à tour de rôle. Les segments de réseaux partageant la même bande passante entre périphériques sont appelés **des domaines de collision.**
- En effet, lorsque deux périphériques de ce segment, ou plus, tentent de communiquer au même moment, des collisions peuvent se produire.
- **Les routeurs et commutateurs sont utilisés pour segmenter les domaines de collision.**
- **Chaque nouveau segment devient un nouveau domaine de collision.**

Domaines de diffusion

Un ensemble de commutateurs interconnectés constitue un domaine de diffusion unique.
Lorsqu'un commutateur reçoit une trame de diffusion, il la transfère à tous ses ports, sauf au port d'entrée où elle a été reçue.
Seul un périphérique de couche réseau, tel qu'un routeur, peut diviser un domaine de diffusion de couche 2.
Les routeurs sont utilisés pour segmenter les domaines de collision et les domaines de diffusion.
Un nombre de diffusions et une charge de trafic trop élevés sur un réseau peuvent entraîner un encombrement, c'est-à-dire un ralentissement des performances réseau.

Partie 2 : Concepts et configuration de base de la commutation

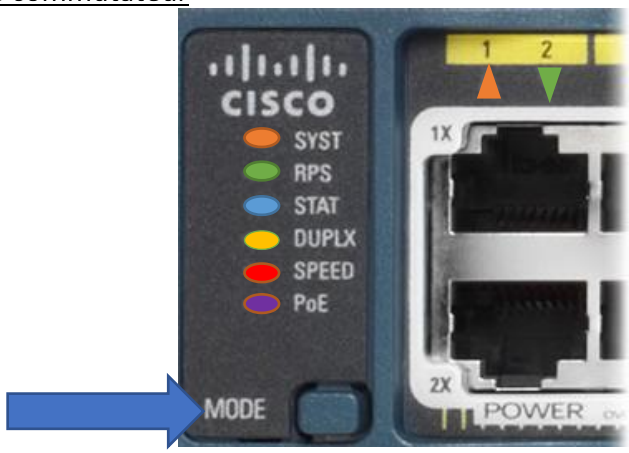
Configuration de commutateur de base

Séquence d'amorçage de commutateur

Dès qu'un commutateur est mis sous tension, il exécute la séquence de démarrage suivante :

1. D'abord, le commutateur exécute un programme de **Power-On Self Test (POST)** stocké dans la mémoire ROM. Le POST contrôle le sous-système du processeur. Il teste le processeur, la mémoire vive dynamique et la partie du périphérique flash qui compose le système de fichiers flash.
2. Le commutateur **exécute ensuite le bootloader**. Le bootloader est un petit programme stocké dans la mémoire morte et exécuté immédiatement après la réussite du POST.
3. Il effectue **l'initialisation de bas niveau du processeur**. Il initialise les registres du processeur qui contrôlent l'emplacement auquel la mémoire physique est mappée, la quantité de mémoire et sa vitesse.
4. Le **bootloader initialise le système de fichiers flash** sur la carte système.
5. Enfin, **il localise et charge une image de logiciel du système d'exploitation IOS** par défaut dans la mémoire et transfère le contrôle du commutateur à l'IOS.

Voyants LED de commutateur



Les commutateurs Cisco Catalyst ont plusieurs témoins lumineux LED. Vous pouvez utiliser les LED du commutateur pour surveiller rapidement l'activité et les performances du commutateur.
La fonction des indicateurs LED, ainsi que leur code couleur :

- **LED système (SYST) :**

Verte	Le système est bien alimenté et s'il fonctionne correctement
Orange	Le système est sous tension mais ne fonctionne pas correctement
Éteinte	Le système est hors tension

- **LED système d'alimentation redondante (RPS) :**

Verte	le système RPS est connecté et prêt à fournir l'alimentation de secours
Éteinte	le système RPS est éteint ou n'est pas correctement connecté

- **LED état port (stat) : lorsque LED de ce mode est verte ; et le LED du Port est :**

éteinte	aucune liaison n'est établie ou le port a été arrêté administrativement
verte	une liaison est établie
verte et clignote	la liaison est active et le port envoie ou reçoit des données
orange	le port est bloqué (temporairement)

- **LED de bidirectionnalité du port (duplex)** :

Verte	le port est en mode bidirectionnel simultané
Éteinte	le port en mode bidirectionnel non simultané

- **LED de vitesse de port** (speed) :

Verte	le port fonctionne à 100 Mbit/s
verte et clignote	le port fonctionne à 1 000 Mbit/s
Éteinte	le port fonctionne à 10 Mbit/s

Configuration de base du commutateur :

Switch(config)#**hostname S**1	Définir le nom en « S1 »
S1(config)#**enable secret** MotPassPriv	Définir mot de passe pour accès au mode privilégié
S1(config)#**line console 0** S1(config-line)#**password** MPConsol S1(config-line)#**login** S1(config-line)#exit	Définir mot de passe pour accès au port console
S1(config)#**line vty 0 15** S1(config-line)#**password** MPDistance S1(config-line)#**login** S1(config-line)#exit	Définir mot de passe pour accès à distance (via l'adresse IP)
S1(config)#**banner motd** !BANNIERE A AFFICHER LORS DE L ACCES AU COMUTATEUR VIA CONSOLE OU A DISTANCE !	Définir un message lors de l'accès au port console ou a distance.
S1(config)#**service password-encryption**	Activer le cryptage des mots de passe
S1#**write** ou	Sauvegarder la configuration en cours vers la mémoire NVRAM
S1(config)# **copy running-config startup-config**	

Préparation à la gestion de commutateur de base

Pour préparer l'accès à la gestion à distance d'un commutateur, il est nécessaire de configurer une adresse IP et un masque de sous-réseau sur le commutateur. Et pour administrer le commutateur depuis un réseau distant, le commutateur doit être configuré avec une passerelle par défaut.
L'interface virtuelle du commutateur (SVI) sur le commutateur doit se voir attribuer une adresse IP.
Une interface SVI est une interface virtuelle, et non un port physique du commutateur.
Une interface SVI est un concept relatif aux VLAN. (voir chapitre suivant)
Par défaut, le commutateur est configuré de telle sorte que sa gestion est régie par le VLAN 1.
Tous les ports sont assignés à VLAN 1 par défaut.
NB : Ces paramètres IP sont uniquement utilisés pour l'accès à la gestion à distance du commutateur.
Les paramètres IP ne permettent pas au commutateur de router des paquets de couche 3.

Préparation à la gestion de commutateur de base

Étape 1. Configuration de l'interface de gestion

Les commandes pour configurer l'interface de gestion du commutateur S1 sont comme suit :

```
S1(config)# vlan vlan_id
S1(config-vlan)# name vlan_name
S1(config-vlan)# exit
S1(config)# Interface vlan vlan_id
S1(config-if)# ip address adresseIP Masque
S1(config-if)# no shutdown
```

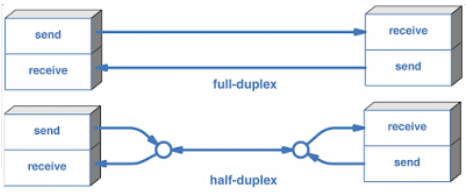
Étape 2. Configuration de la passerelle par défaut

Le commutateur doit être configuré avec une passerelle par défaut s'il doit être géré à distance depuis des réseaux connectés indirectement.

```
S1(config)# ip default-gateway Adresse_IP_de_interface_du_routeur
```

Configuration des ports de commutateur

Les communications **bidirectionnelles simultanées(full-duplex)** 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 (half-duplex)** sont unidirectionnelles. L'envoi et la réception de données n'ont jamais lieu simultanément.



Configuration des ports de commutateur au niveau de la couche physique

Mode bidirectionnel et vitesse

Pour configurer mode bidirectionnel et vitesse des ports :

Config (switch-if)#**duplex** full | half | auto Config (switch-if)#speed 10 | 100 | ~~1000~~ | auto

Fonction auto-MDIX

Jusqu'à récemment, il était nécessaire d'utiliser certains types de câble (droit ou croisé) pour connecter les périphériques. **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.
Les commandes permettant d'activer la fonctionnalité auto-MDIX ~~sont :~~

S1(switch-if)# mdix auto

Vérification de la configuration du port de commutateur

La commande **show** se révéler utiles pour vérifier les fonctionnalités configurables les plus courantes des commutateurs.

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

Concepts du routage

Pourquoi le routage ?

- **Le but d'un routeur est de relier un réseau à un autre.**
- **La communication entre les réseaux serait impossible sans un routeur pour déterminer le meilleur chemin vers la destination et transférer le trafic vers le prochain routeur sur ce chemin. Le routeur est responsable du routage du trafic entre les réseaux.**
- **Lorsqu'un paquet arrive sur une interface de routeur, le routeur utilise sa table de routage pour déterminer comment atteindre le réseau de destination.**

Les routeurs sont des ordinateurs

Un routeur est à un ordinateur spécialisé. Il a besoin d'un processeur et d'une mémoire pour stocker temporairement et définitivement des données lui permettant d'exécuter les instructions du système d'exploitation, telles que l'initialisation du système, les fonctions de routage et de commutation.

Les périphériques Cisco utilise le logiciel système **Internetwork Operating System (IOS).**

Les routeurs stockent des données à l'aide des éléments suivants :

Mémoire vive (RAM)	Volatile*	stockage temporaire pour des applications et processus divers : IOS actuel, le fichier de configuration en cours, différentes tables (par exemple, table de routage IP, table ARP Ethernet) et les tampons pour le traitement des paquets.
Mémoire morte (ROM)	Non volatile	Les instructions de démarrage, du logiciel de diagnostic de base et d'une version limitée de l'IOS au cas où le routeur ne peut pas charger l'IOS complet. La mémoire morte est un firmware.
Mémoire vive non volatile	Non volatile	Garantit le stockage permanent du fichier de configuration initiale (startup-config).
Flash	Non volatile	Offre le stockage permanent de l'IOS et d'autres fichiers liés au système. L'IOS est copié de la mémoire Flash vers la mémoire vive lors du processus de démarrage.

*Volatile : elle perd son contenu lors de la mise hors tension

Les routeurs sont équipés de ports spécialisés et de cartes réseau pour interconnecter les périphériques à d'autres réseaux.

Les routeurs interconnectent les réseaux

Un routeur relie plusieurs réseaux, c'est-à-dire qu'**il dispose de plusieurs interfaces appartenant chacune à un réseau IP différent.** Lorsqu'un routeur **reçoit un paquet IP sur une interface**, **il détermine quelle interface utiliser pour transférer le paquet vers sa destination**. L'interface qu'utilise le routeur pour transférer le paquet peut être la destination finale, mais aussi un réseau connecté à un autre routeur utilisé pour atteindre le réseau de destination.

Chaque réseau auquel un routeur se connecte nécessite généralement une interface séparée.

Ces interfaces servent à accueillir une combinaison de réseaux locaux (LAN) et de réseaux étendus (WAN).

- Les réseaux locaux sont généralement des réseaux **Ethernet** comportant des périphériques tels que PC, imprimantes et serveurs.
- Les réseaux étendus sont utilisés pour relier des réseaux dans une zone géographique vaste. Par exemple, une connexion WAN est souvent utilisée pour relier un réseau local au réseau du fournisseur d'accès Internet (FAI).

Les routeurs choisissent les meilleurs chemins

Les principales fonctions d'un routeur sont les suivantes :

- **Détermine le meilleur chemin pour l'envoi des paquets**
- **Transférer les paquets vers leur destination**

Le routeur utilise sa table de routage pour déterminer le meilleur chemin à utiliser pour transférer un paquet.

Mécanismes de transfert des paquets

Les routeurs prennent en charge trois mécanismes de transfert des paquets :

- **Commutation de processus** : Lorsqu'un paquet arrive sur une interface, il est transféré au plan de contrôle où le processeur ***fait correspondre l'adresse de destination avec une entrée de sa table de routage***, puis détermine l'interface de sortie et transmet le paquet. **Il est important de comprendre que le routeur effectue cette opération pour chaque paquet, même si la destination est identique pour une série de paquets**.
- **Commutation rapide** : utilise **un cache à commutation rapide** pour stocker les informations de tronçon suivant. Lorsqu'un paquet arrive sur une interface, il est transféré au plan de contrôle où le processeur recherche ***une correspondance dans le cache à commutation rapide***. S'il ne trouve rien, le paquet est commuté par le processus et transféré à l'interface de sortie et stockes ces informations dans le cache à commutation rapide pour un autre paquet ayant la même destination.
- **CEF (Cisco Express Forwarding)** : Comme la commutation rapide, le protocole CEF génère une table FIB et une table de contiguïté. Cependant, à la différence de la commutation rapide, ***les entrées de table ne sont pas déclenchées par les paquets, mais par les modifications***, comme en cas de changement dans la topologie du réseau.

Voici une analogie courante permettant de décrire les trois mécanismes de transfert des paquets :

- La commutation de processus résout un problème en effectuant un calcul à la main, même si un problème identique s'est déjà posé.
- La commutation rapide résout un problème en effectuant un calcul à la main et mémorise la solution pour les problèmes identiques suivants.
- Le protocole CEF résout à l'avance tous les problèmes possibles dans un tableur.

Brancher les périphériques

Passerelles par défaut

Pour activer l'accès au réseau, les périphériques doivent être configurés avec les informations d'adresse IP permettant d'identifier les éléments corrects suivants :

- **Adresse IP** : identifie un hôte unique sur un réseau local.
- **Masque de sous-réseau** : identifie avec quel sous-réseau l'hôte peut communiquer.
- **Passerelle par défaut** : identifie le routeur auquel envoyer un paquet lorsque la destination n'est pas sur le même sous-réseau de réseau local.

La passerelle par défaut est généralement l'adresse de l'interface du routeur connecté au réseau local.

LED des périphériques

Les périphériques de l'infrastructure réseau utilisent souvent plusieurs voyants LED pour donner un aperçu rapide de leur état.

Port	Led	Couleur	Description
GE0/0	S (vitesse)	1 clignotement + pause	Le port fonctionne à 10 Mb/s
		2 clignotements + pause	Le port fonctionne à 100 Mb/s
		3 clignotements + pause	Le port fonctionne à 1000 Mb/s
	L (Liaison)	Vert	La liaison est active
		Désactiver	La liaison est inactive

Accès à la console

Dans un environnement de production, des périphériques d'infrastructure sont couramment utilisés à distance à l'aide de Secure Shell (SSH) ou du protocole de transfert hypertexte sécurisé (HTTPS). **L'accès à la console n'est vraiment nécessaire que lors de la configuration initiale d'un périphérique, ou si l'accès distant échoue**.

L'accès à la console nécessite :

- **Câble de console** : câble de console RJ-45 vers DB-9 (port série)
- **Logiciel d'émulation de terminal** : Tera Term, PuTTY, HyperTerminal

Le câble est connecté entre le port série ou USB de l'hôte et le port de console du périphérique.

Paramètres de base d'un routeur

Configuration des paramètres de base du routeur

Les routeurs Cisco et les commutateurs Cisco ont beaucoup de points communs. Ils prennent en charge le même système d'exploitation de modes, les mêmes structures de commandes et comptent de nombreuses commandes similaires. En outre, les deux périphériques présentent des étapes de configuration initiale similaires.

Lors de la configuration d'un commutateur ou d'un routeur Cisco, les tâches de base suivantes doivent d'abord être exécutées :

- **Nommer le périphérique** : le distingue des autres routeurs.

```
Router#configure terminal
Router(config)#hostname R1
```

- **Sécuriser l'accès à la gestion** : sécurise le mode d'exécution privilégié, le mode d'exécution utilisateur et l'accès Telnet, et chiffre les mots de passe à leur niveau le plus élevé.

```
R1(config)#enable secret ofpptP
```
Définir un MP pour accéder au mode Privilégié

```
R1(config)#line console 0
R1(config-line)#password ofpptC
R1(config-line)#login
R1(config-line)#exit
```
Définir un MP pour accéder au port console

```
R1(config)#line vty 0 15
R1(config-line)#password ofpptV
R1(config-line)#login
R1(config-line)#exit
```
Définir un MP pour accéder à distance au routeur

```
R1(config)#service password-encryption
```
Chiffrer les mots de passe

- **Configurer une bannière** - rédige les mentions légales de tout accès non autorisé.

```
R1(config)#banner motd $ Acces autorise seulement! $
```

Remarque : enregistrez toujours les modifications sur un routeur et vérifiez la configuration de base et le fonctionnement du routeur.

```
R1#copy running-config startup-config
```

```
Ou
R1#write
```

Configuration d'une interface du routeur IPv4

Pour être disponible, une interface doit être :

- **Si vous utilisez IPv4, configurée avec une adresse et un masque de sous-réseau**.
- **Activée**. Par défaut, les interfaces LAN et WAN ne sont pas activées (**shutdown**). Pour activer une interface, utilisez la commande **no shutdown**.
- En option, l'interface peut également être configurée avec une courte description. Il est recommandé de configurer une description sur chaque interface.

Selon le type d'interface, des paramètres supplémentaires peuvent être nécessaires. Par exemple, dans un environnement de test, l'interface série se connectant à l'extrémité du câble série étiqueté DCE doit être configurée à l'aide de la commande **clock rate**.

Exemple :

```
R1(config)#interface GigabitEthernet0/0

R1(config-if)#description lien vers salleAdmin

R1(config-if)#ip address 192.168.1.1 255.255.255.0

R1(config-if)#no shutdown
```

Configuration d'une interface du routeur IPv6

La configuration d'une interface IPv6 est semblable à celle d'une interface pour IPv4.

Une interface IPv6 doit être :

- **Configurée avec l'adresse IPv6 et longueur de préfixe**. Utilisez la commande de configuration d'interface **ipv6 address** *ipv6-address/prefix-length* **[link-local | eui-64]**.
- **Activée.** L'interface doit être activée à l'aide de la commande **no shutdown**.

Remarque : une interface peut générer sa propre adresse link-local IPv6 sans adresse de monodiffusion globale à l'aide de la commande de configuration d'interface **ipv6 enable**.

Contrairement à l'adressage IPv4, les interfaces IPv6 ont généralement plus d'une adresse IPv6.

Les commandes suivantes peuvent être utilisées pour créer de manière statique une adresse de monodiffusion globale ou link-local IPv6 :

- **ipv6 address** *ipv6-address / prefix-length* - Crée une adresse IPv6 de monodiffusion globale comme indiqué.
- **ipv6 address** *ipv6-address / prefix-length* **eui-64** - Configure une adresse IPv6 de monodiffusion globale à l'aide d'un identificateur d'interface (ID) dans les 64 bits de poids faible de l'adresse IPv6 au moyen du processus EUI-64.
- **ipv6 address** *ipv6-address / prefix-length* **link-local** - Configure une adresse link-local statique sur l'interface utilisée à la place de l'adresse link-local qui est automatiquement configurée.

Exemples :

```
R1(config)#ipv6 unicast-routing
R1(config)#interface gigabitEthernet 0/0
R1(config-if)#description lien vers siteVente
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#no shutdown
```

Configuration d'une interface de bouclage IPv4

Une autre configuration courante des routeurs Cisco IOS consiste à activer une interface de bouclage.

L'interface de bouclage est une interface logique interne au routeur. Elle n'est pas affectée à un port physique et ne peut donc jamais être connectée à un autre périphérique.

L'interface de bouclage est utile en cas de test et de gestion d'un périphérique Cisco IOS.

L'activation et l'attribution d'une adresse de bouclage sont simples :

```
Router(config)# interface loopback numéro
Router(config-if)# ip address ip-address subnet-mask
```

Plusieurs interfaces de bouclage peuvent être activées sur un routeur. L'adresse IPv4 de chaque interface de bouclage doit être unique et ne doit pas être utilisée par une autre interface.

Exemple :

```
R1(config)#interface loopback 0

R1(config-if)#ip address 10.0.0.1 255.255.255.0
```

Vérification des paramètres d'interface (R#)

Il existe plusieurs commandes **show** permettant de vérifier le fonctionnement et la configuration d'une interface.

Les trois commandes suivantes sont particulièrement utiles pour identifier rapidement l'état d'une interface :

- **show ip interface brief** - Affiche un résumé de toutes les interfaces, notamment l'adresse IPv4 de l'interface et son état de fonctionnement actuel.
- **show ip route** - Affiche le contenu de la table de routage IPv4 stocké dans la mémoire vive.
- **show running-config interface** *interface-id* - Affiche les commandes configurées sur l'interface spécifiée.

Les deux commandes suivantes permettent de recueillir des informations plus détaillées sur l'interface :

- **show interfaces** - Affiche des informations sur l'interface et le nombre de flux de paquets pour toutes les interfaces du périphérique.
- **show ip interface** - Affiche des informations sur IPv4 relatives à toutes les interfaces d'un routeur.

Vérification des paramètres d'interface IPv6

Les commandes permettant de vérifier la configuration de l'interface IPv6 sont semblables aux commandes utilisées pour IPv4, **il suffit de remplacer ip par ipv6.**

Parmi les autres commandes utiles pour la vérification IPv6, citons :

- **show ipv6 interface brief**
- **show ipv6 route**

Protocole ARP Protocole de résolution d'adresse

- Les périphériques Ethernet consulte une table ARP (ou au cache ARP) dans sa mémoire (c'est-à-dire la mémoire vive) pour connaître l'adresse MAC qui est mappée à l'adresse IPv4.
- **Un périphérique recherche dans sa table ARP une adresse IPv4 de destination et une adresse MAC correspondante.**
    - **Si l'adresse IPv4 de destination du paquet appartient au même réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de destination dans sa table ARP.**
    - **Si l'adresse IPv4 de destination du paquet appartient à un autre réseau que l'adresse IPv4 source, le périphérique recherche l'adresse IPv4 de la passerelle par défaut dans sa table ARP.**
- **Une requête ARP est une trame de diffusion envoyée lorsqu'un périphérique a besoin d'une adresse MAC associée à une adresse IPv4 qui ne figure pas dans sa table ARP.**
- **Les messages ARP sont encapsulés directement dans une trame Ethernet.**
  Il n'existe pas d'en-tête IPv4.
- **Le message de la requête ARP contient les éléments suivants :**
    - **Adresse IPv4 cible**
    - **Adresse MAC cible**
- **Seul le périphérique dont l'adresse IPv4 correspond à l'adresse IPv4 cible de la requête ARP envoie une réponse ARP.**
- **Le message de réponse ARP contient les éléments suivants :**
    - **Adresse IPv4 de l'expéditeur**
    - **Adresse MAC de l'expéditeur**
    - **Les entrées de la table ARP sont horodatées. Si le périphérique ne reçoit pas de trame d'un périphérique précis avant expiration de l'horodatage, l'entrée correspondant à ce périphérique précis est supprimée du tableau ARP.**
- **Lorsqu'un hôte crée un paquet pour une destination, il compare l'adresse IPv4 de destination à sa propre adresse IPv4 pour déterminer si celles-ci se situent sur le même réseau de couche 3.**
- **Si l'hôte de destination ne se situe pas sur le même réseau, l'hôte source cherche dans sa table ARP l'adresse IPv4 de la passerelle par défaut.**
- **Si l'entrée n'existe pas, il fait appel au processus ARP pour déterminer l'adresse MAC de la passerelle par défaut.**

Suppression

- Chaque périphérique possède un compteur de cache ARP qui supprime les entrées ARP qui n'ont pas été utilisées pendant une période donnée.

Messages ICMP

Le protocole ICMP est disponible pour IPv4 et IPv6. ICMPv4 est le protocole de message des réseaux IPv4. ICMPv6 fournit également ces services pour l'IPv6, en ajoutant d'autres fonctionnalités.

Les types de messages ICMP, et les raisons pour lesquelles ils sont envoyés, sont nombreux. Les messages ICMP communs à ICMPv4 et à ICMPv6 sont notamment les suivants :

- Accessibilité de l'hôte
- Destination or Service Unreachable (destination ou service inaccessible)
- Time exceeded (Délai dépassé)

Accessibilité de l'hôte

Un message d'écho ICMP peut être utilisé pour tester l'accessibilité d'un hôte sur un réseau IP. L'hôte local envoie un message ICMP Echo Request (Demande d'écho) à un autre hôte. Si l'hôte est disponible, l'hôte de destination répond en envoyant une réponse d'écho. Sur la figure ci-contre, cliquez sur le bouton Lecture pour lancer une animation sur les requêtes et les réponses d'écho ICMP. Cette utilisation des messages ICMP Echo est à la base de l'utilité **ping**.

Destination ou service inaccessible

Lorsqu'un hôte ou une passerelle ne peut pas acheminer un paquet reçu, il ou elle peut utiliser un message ICMP de destination inaccessible pour avertir la source que la destination ou le service est inaccessible. Ce message comprend un code indiquant pourquoi le paquet n'a pas pu être acheminé.

Certains des codes de destination inaccessible pour l'ICMPv4 sont:

- 0 - Réseau inaccessible
- 1 - Hôte inaccessible
- 2 - Protocole inaccessible
- 3 - Port inaccessible

Délai dépassé

Un message de dépassement de délai ICMPv4 est utilisé par un routeur pour indiquer qu'il ne peut pas transférer un paquet, car le champ TTL de durée de vie du paquet a atteint 0. Si un routeur reçoit un paquet et décrémente le champ TTL de durée de vie du paquet IPv4 jusqu'à atteindre zéro, il abandonne le paquet et envoie un message de dépassement de délai à l'hôte source.

Note:Les messages Temps dépassé sont utilisés par l' **traceroute** outil.

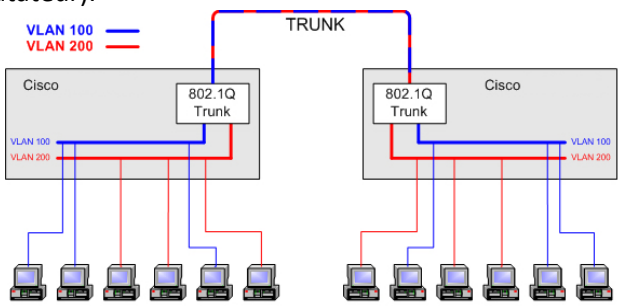
VLAN

Introduction :

- ✓ Les VLANs permettent à un administrateur de segmenter les réseaux en fonction de facteurs tels que la fonction, l'équipe de projet ou l'application, quel que soit l'emplacement physique de l'utilisateur ou du périphérique.
- ✓ Les périphériques d'un VLAN se comportent comme s'ils se trouvaient chacun sur leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLAN.
- ✓ N'importe quel port de commutateur peut appartenir à un VLAN. Les paquets monodiffusion, diffusion et multidiffusion sont transférés et diffusés uniquement à des stations finales dans le VLAN dont proviennent les paquets.
- ✓ Chaque VLAN est considéré comme un réseau logique distinct et les paquets destinés aux stations n'appartenant pas au VLAN doivent être transférés par un périphérique qui prend en charge le routage.
- ✓ Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments de réseau local physique. Les VLANs améliorent les performances réseau en divisant de vastes domaines de diffusion en domaines plus petits. Les VLANs permettent la mise en œuvre des stratégies d'accès et de sécurité en fonction de groupes d'utilisateurs précis.
- ✓ Chaque port de commutateur peut être attribué à un seul VLAN (à l'exception des ports connectés à un téléphone IP ou à un autre commutateur).

Avantages des VLAN

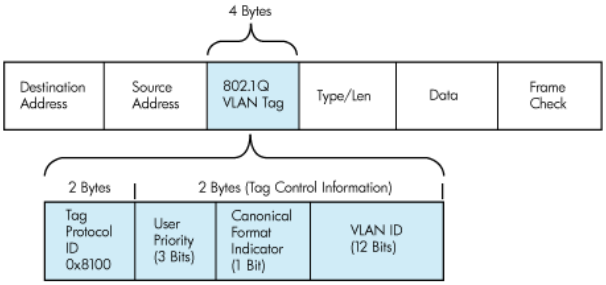
- ✓ ***Sécurité*** *:*
- ✓ ***Réduction des coûts*** *:*
- ✓ ***Meilleures performances***
- ✓ ***Réduction des domaines de diffusion*** *:*
- ✓ ***Efficacité accrue du personnel informatique*** *:*
- ✓ ***Gestion simplifiée de projets et d'applications*** *:*



NB : Chaque VLAN d'un réseau commuté correspond à un réseau IP ; par conséquent, la conception VLAN doit tenir compte de la mise en œuvre d'un système d'adressage hiérarchique.

Types de VLAN

- ***VLAN de données*** : Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Un VLAN de données est parfois appelé un ***VLAN utilisateur***. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques.
- ***VLAN par défaut*** : Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Le VLAN par défaut pour les commutateurs Cisco est VLAN 1. Tous les ports sont assignés au VLAN 1 par défaut.
- **Le VLAN 1 ne peut pas être renommé ni supprimé. Par défaut, tout le trafic de contrôle de couche 2 est associé au VLAN 1.**
- ***VLAN natif*** : **Un réseau local virtuel natif est affecté à un port trunk 802.1Q**,
- ***VLAN de gestion*** : Un VLAN de gestion est un réseau local virtuel configuré pour gérer un commutateur à distance. Pour créer le VLAN de gestion, l'interface virtuelle du commutateur (SVI) de ce VLAN se voit attribuer une adresse IP et un masque de sous-réseau, ce qui permet de gérer le commutateur via HTTP, Telnet, SSH ou SNMP.
- ***VLAN voix*** : Un VLAN distinct est nécessaire pour prendre en charge la voix sur IP (VoIP).



Trunks de VLAN

Un trunk est une liaison point à point entre deux périphériques réseau qui transporte plusieurs VLAN. Un trunk de VLAN permet d'étendre les VLAN à l'ensemble d'un réseau. Cisco prend en charge la norme **IEEE 802.1Q** pour la coordination des trunks.

Étiquetage des trames Ethernet pour l'identification des VLAN

Lorsque les trames sont placées sur un trunk, il convient d'ajouter les informations relatives au VLAN dont elles dépendent. Ce processus, appelé **étiquetage(tagging)**, s'effectue à l'aide de l'en-tête **IEEE 802.1Q**. L'en-tête 802.1Q inclut une étiquette de 4 octets insérée dans l'en-tête d'origine de la trame Ethernet.

Lorsque le commutateur reçoit une trame sur un port configuré en mode d'accès et associé à un VLAN, il insère une étiquette VLAN dans l'en-tête de trame, recalcule la séquence de contrôle de trame, puis envoie la trame étiquetée par un port **trunk**.

VLAN natifs et étiquetage 802.1Q

Certaines trames véhiculées sur un Trunk ne sont pas marquées d'un tag dot1q (pas d'ID VLAN) vu qu'ils ne sont pas envoyé d'un port en mode Access ! par exemple les messages envoyés entre commutateurs (CDP par exemple). Dès lors il faut pouvoir les placer quelque part. C'est là qu'intervient le vlan natif.

Le vlan natif, est le vlan dans lequel sont véhiculées les trames non taguées dot1q. Donc si un switch reçoit sur une interface trunk une trame ethernet standard, il la placera dans ce vlan natif, en quelque sorte, un vlan par défaut (de marquage).

Implémentations de VLAN

Plages VLAN sur les commutateurs Catalyst

- VLAN à plage normale
  - Identifiés par un ID de VLAN compris entre 1 et 1005.
  - Les configurations sont stockées dans un fichier de base de données VLAN nommé vlan.dat qu'on le trouve dans la mémoire Flash du commutateur.
  - Le protocole VTP (VLAN Trunking Protocol), qui permet de gérer les configurations VLAN entre les commutateurs, peut uniquement découvrir et stocker les VLAN à plage normale.
- VLAN à plage étendue :
  - ✓ Sont identifiés par un ID de VLAN compris entre 1006 et 4094.
  - ✓ Sont par défaut enregistrés dans le fichier de configuration en cours.
  - ✓ Le protocole VTP ne prend pas en compte les VLAN à plage étendue.

Création d'un VLAN

Créez un VLAN avec un numéro d'identité valide.	S1(config)# **vlan** vlan-id
Indiquez un nom unique pour identifier le VLAN.	S1(config-vlan)# **name** vlan-name

NB : Pour créer plusieurs sur une seule ligne (mais sans indiquer leurs noms)
S1(config)# **vlan 100, 102, 105-107**

Affectation de ports à des VLAN

Un port d'accès peut appartenir **à un seul VLAN à la fois**. (sauf si ce port connecté à un téléphone IP).
Pour définir un port d'accès et de l'affecter à un VLAN. La commande :
S1(config)#**interface** fa0/X
S1(config-if)# **switchport mode access**
S1(config-if)#**switchport access vlan** *VlanID*

Remarque : utilisez la commande **interface range fa0/X-Y** pour configurer simultanément plusieurs interfaces (fa0/X au FA0/Y)

Modification de l'appartenance des ports aux VLAN

Pour faire passer un port de commutateur en appartenance VLAN 1 :
S1(config-if)#**no switchport access vlan**

Suppression de VLAN

S1(config)#no vlan *vlan-id*
La commande est utilisée pour supprimer le VLAN.
Attention : avant de supprimer un VLAN, réattribuez d'abord tous les ports lui appartenant à un autre VLAN. Sinon les hôtes appartenant au vlan supprimé ne pourront plus communiquer avec d'autres hôtes.
Le fichier **vlan.dat** peut aussi être entièrement supprimé à l'aide de la commande, pour supprimer tous les vlan.
S1#**delete flash:vlan.dat**.

Vérification des informations VLAN

- ✓ Les configurations VLAN peuvent être validées à l'aide des commandes **show** de Cisco IOS.

Exemples : **show vlan** et **show interfaces**.

- ✓ **show vlan name NomVLAN** produit un résultat difficile à interpréter. Il est préférable d'utiliser la commande **show vlan brief**.
- ✓ La commande **show vlan summary** affiche tous les VLAN configurés.

Trunks de VLAN

Configuration des liaisons trunk IEEE 802.1Q

Pour configurer un port de commutateur sur l'extrémité d'une liaison trunk, utilisez la commande :

S1(config-if)#**switchport mode trunk**.

Utilisez la commande **switchport trunk allowed vlan** *vlan-list* de CISCO IOS pour préciser la liste des VLAN à autoriser sur la liaison trunk.

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

Réinitialisation du trunk à l'état par défaut

Passer en mode de configuration d'interface pour SVI.	S1(config)# **interface** interface_id
Définir le trunk de sorte qu'il autorise tous les VLAN.	S1(config-if)# **no switchport trunk allowed** vlan
Redéfinir le VLAN natif sur les paramètres par défaut.	S1(config-if)# **no switchport trunk native** vlan

Vérification de la configuration du trunk

La configuration est vérifiée à l'aide de la commande **show interfaces** *interface-ID* **switchport**.

Protocole VTP

Le protocole de jonction VLAN (VTP) réduit la gestion dans un réseau commuté. Quand vous configurez un nouveau VLAN sur un serveur VTP, le VLAN est distribué par tous les commutateurs dans le domaine. Ceci réduit la nécessité de configurer le même VLAN partout.

Modes VTP

- ***Serveur*** —vous pouvez créer, modifier, et supprimer des VLAN et spécifier d'autres paramètres de configuration, tels que la version VTP. Les serveurs VTP annoncent leur configuration VLAN à d'autres commutateurs dans le même domaine VTP. NB : Le Serveur VTP est le mode par défaut.
- ***Client*** —vous ne pouvez pas créer, changer, ou supprimer des VLAN sur un client VTP.
- ***Transparent*** — Les commutateurs VTP transparents ne participent pas à VTP. Mais transmettent des annonces VTP qu'ils reçoivent par leurs ports de jonction dans VTP Version 2.

Mot de passe VTP
Mot de passe pour l'authentification des données VTP entre commutateurs.

Configuration VTP :

Définir domaine VTP	S1config)#**vtp domain TEST**
Définir le mode VTP	S1(config)#**vtp mode** server |**client**|~~transparent~~
Configurer Mot de passe VTP « cisco123 »	S1(config)#**vtp password cisco123**
Activer la version 2 ou 3	S1(config)#**vtp version** 2|3

Vérification VTP :

Vérification de la configuration globale du VTP	S#**show vtp status**
Vérification des compteurs des messages VTP envoyés et reçus	S#**show vtp counters**
Visualisation du mot de passe configuré	S#**show vtp password**

Routage Inter-Vlan :

Pour relier plusieurs Vlans, on doit utiliser un routeur, et pour le configurer ; il existe deux méthodes :

- **Classique** : lier chaque interface du routeur avec un vlan ; en reliant chaque interface du routeur avec un port (mode Access) du commutateur appartenant à un vlan X.
  Cette méthode nécessite que le routeur doive avoir le même nombre d'interfaces que de VLAN. (Càd si on veut créer 4 vlan on doit avoir sur le routeur 4 interfaces ; etc.)
- **Router-on-a-Stick** : Cette méthode consiste à utiliser les sous interfaces (interfaces virtuelle relié à une seule interface physique), on peut créer le nombre qu'on veut des sous interfaces pour relier les VLAN.

Routage inter-VLAN (Router-on-a-Stick):

Au niveau du routeur :

Pour configurer les sous interfaces ;

R(config)#**interface** G0/0.X	X : numéro de VLAN ; G0/0 est seulement à titre d'exemple.
R(config-if)#**encapsulation dot1q** X	On définit le type de protocole utilisé pour trunking ; et le N° VLAN
R(config-if)#**ip address** A.B.C.D M.A.S.K	On donne l'adresse IP et Masque
R(config)#**interface** G0/0 R(config-if)#**no shutdown**	Pour l'interface physique on doit seulement l'activer :

Au niveau du Commutateur :

Le port relié au routeur doit être définit en mode « Trunk ».

Voir paragraphe (Configuration des liaisons trunk IEEE 802.1Q)

Sécurité du commutateur : gestion et implémentation

Accès à distance sécurisé

Secure Shell (SSH) est un protocole qui permet d'établir une connexion sécurisée (chiffrée) pour la gestion des périphériques distants. SSH permet de sécuriser les connexions distantes grâce à une méthode de chiffrement fort pour l'authentification des périphériques (nom d'utilisateur et mot de passe), mais également pour la transmission des données entre les périphériques de communication. SSH est attribué au port TCP 22.

Configuration de SSH

Switch(config)#**hostname** S1	Configurer le commutateur avec un nom d'hôte unique
s1(config)# **ip domain-name cisco.com**	**Configuration du domaine IP (exemple cisco.com)**
s1(config)# **crypto key generate rsa**[1]	**Générez des paires de clés RSA.**
s1(config)# **username util1 secret ABC123**	**Configurez l'authentification utilisateur (exemple login : util1 et Mot de passe : ABC123)**
s1(config)# **ip ssh version 2**	Pour activer uniquement la version 2 de SSH
s1(config)#**line vty** 0 15 s1(config-line)# **transport input ssh**.	Autoriser seulement le protocole SSH sur les lignes VTY
s1(config-line)# **login local**	Pour exiger l'authentification locale des connexions SSH

Remarque : pour supprimer la paire de clés RSA, utilisez la commande de configuration globale **crypto key zeroize rsa**. Une fois la paire de clés RSA supprimée, le serveur SSH est automatiquement désactivé.

Vérification de SSH

Sur un PC, un client SSH, par exemple PuTTY, est utilisé pour établir une connexion à un serveur SSH.

S1#show ip ssh	Pour vérifier que le commutateur prend en charge SSH ou afficher les données de version ou de configuration SSH du périphérique configuré en tant que serveur SSH
S1# **show ssh**	Pour vérifier les connexions SSH vers le périphérique

NB : Les mêmes commandes peuvent être utilisé pour configurer SSH sur un routeur Cisco.

Problèmes de sécurité dans les LAN

Attaques de sécurité courantes : inondation d'adresse MAC

Inondation d'adresses MAC

La taille des tables d'adresses MAC est limitée. L'inondation d'adresses MAC profite de cette limite pour submerger le commutateur de fausses adresses MAC source jusqu'à ce que la table d'adresses MAC de ce dernier soit saturée.

Attaques de sécurité courantes : usurpation de DHCP

Deux types d'attaques DHCP peuvent être menées contre un réseau commuté : l'épuisement des ressources DHCP et l'usurpation de DHCP.

Dans les attaques d'épuisement des ressources DHCP, un pirate inonde le serveur DHCP de requêtes DHCP afin d'utiliser toutes les adresses IP disponibles sur le serveur DHCP. Une fois que toutes les adresses IP ont été émises, le serveur ne peut plus fournir d'autre adresse. alors les clients ne peuvent obtenir un accès au réseau.

[1] Lors de la génération de clés RSA, l'administrateur est invité à saisir une longueur de module ; pour utiliser SSHv2 il est recommandé de saisir au minimum 1024.

Dans les attaques par usurpation de DHCP, un pirate configure un faux serveur DHCP sur le réseau pour affecter des adresses DHCP aux clients. Cette attaque a généralement pour but de forcer les clients à utiliser un faux système de noms de domaine (DNS) ou Windows Internet Naming Service (WINS) et d'utiliser le serveur du pirate, ou une machine contrôlée par ce dernier, comme passerelle par défaut.

Attaques de sécurité courantes : utiliser le protocole CDP

CDP (Cisco Discovery Protocol) est un protocole propriétaire que tous les périphériques Cisco peuvent utiliser. Le protocole CDP détecte tous les autres périphériques Cisco connectés directement, ce qui leur permet de procéder à la configuration automatique de leur connexion.

CDP renferme des informations sur le périphérique, notamment son adresse IP, la version du logiciel IOS, la plate-forme, les fonctions et le VLAN natif. Ces informations peuvent être utilisées par un pirate afin d'attaquer le réseau, généralement par une attaque de déni de service (DoS).

Il est recommandé de **désactiver le protocole CDP** sur les périphériques ou les ports sur lesquels il n'est pas requis, à l'aide de la commande de mode de configuration globale **no cdp run**. Le CDP peut être désactivé port par port.

Attaque de mot de passe en force

La première phase de ce type d'attaque consiste pour le pirate à utiliser une liste de mots de passe courants, ainsi qu'un programme conçu pour tenter d'établir une session Telnet au moyen de chaque mot figurant dans la liste du dictionnaire. Si le mot de passe n'est pas découvert lors de la première phase, une seconde phase débute. Lors de la deuxième phase de l'attaque en force, le pirate fait appel à un programme chargé de créer des combinaisons de caractères séquentielles pour tenter de deviner le mot de passe. Lorsque le pirate dispose de suffisamment de temps, une attaque en force permet de décoder quasiment tous les mots de passe employés.

Pour vous prémunir contre les attaques en force, utiliser des mots de passe forts et changez-les régulièrement. L'accès aux lignes vty peut également être limité à l'aide d'une liste de contrôle d'accès.

Sécurité des ports de commutateur

Sécurisation des ports inutilisés

Une méthode simple à laquelle nombre d'administrateurs ont recours pour mieux protéger le réseau contre tout accès non autorisé est de désactiver tous les ports qui ne sont pas exploités sur un commutateur.

```
Switch(config)# interface range type module/premier nombre – dernier nombre
Switch(config-if)# shutdown
```

Sécurité des ports : fonctionnement

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.

Pour Activer la sécurité des ports :

S1(config-if)#**switchport port-security**

Types d'adresses MAC sécurisées

Il existe plusieurs façons de configurer la sécurité des ports. Le type d'adresse sécurisée est basé sur la configuration et peut être l'un des types suivants :

- **Adresses MAC sécurisées statiques** : adresses MAC configurées manuellement sur un port à l'aide de la commande de mode de configuration globale **switchport port-security mac-address** *adresse-mac*. Les adresses MAC configurées de cette manière sont stockées dans la table d'adresses et sont ajoutées à la configuration en cours sur le commutateur.

- **Adresses MAC sécurisées dynamiques** : adresses MAC apprises de manière dynamique et stockées uniquement dans la table d'adresses. Les adresses MAC configurées ainsi sont supprimées au redémarrage du commutateur.

- **Adresses MAC sécurisées rémanentes (sticky)**: adresses MAC pouvant être apprises de manière dynamique ou configurées manuellement, puis stockées dans la table d'adresses et ajoutées à la configuration en cours.

  Pour activer l'apprentissage rémanent sur une interface, exécutez la commande de mode de configuration d'interface **switchport port-security mac-address sticky**.

Sécurité des ports : modes de violation

Il y a violation de la sécurité lorsque 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.

Lors de la détection d'une violation : aucune communication n'est possible sur le port.

Une interface peut être configurée pour l'un des trois modes de violation, en spécifiant les actions à entreprendre en cas de violation. Les modes de violation de sécurité sont :

- **Protect:** Aucune notification n'indique qu'une violation de sécurité s'est produite.
- **Restrict :** Dans ce mode, une notification indique qu'une violation de sécurité s'est produite Et le compteur de violation est incrémenté.
- **Shutdown :** dans ce mode (le mode par défaut), toute violation de sécurité de port entraîne immédiatement la désactivation du port. Et le compteur de violation est incrémenté.
  Pour réactiver le port, il faut faire **shutdown** et après **no shutdown**.

Pour configurer la sécurité des ports :

S1(Config-if)# **switchport mode access**
S1(Config-if)# **switchport port-security**
S1(Config-if)# **switchport port-security violation** {protect | restrict | shutdown}.
S1(Config-if)# **switchport port-security maximum X**[2]
S1(Config-if)# **switchport port-security mac-address** sticky

Sécurité des ports : Vérification

Vérification de la sécurité des ports

Pour afficher les paramètres de sécurité des ports du commutateur ou de l'interface spécifiée, utilisez la commande **:**
S1#show port-security [interface *interface-id***]**.

Surveillance DHCP

La surveillance DHCP est une fonction de Cisco Catalyst qui détermine quels ports du commutateur sont en mesure de répondre aux requêtes DHCP. Les ports sont identifiés comme étant fiables et non fiables. Les ports fiables peuvent obtenir tous les messages DHCP. Les ports non fiables peuvent

[2] *Nombre d'adresses MAC à retenir*

uniquement obtenir les demandes. Les ports fiables hébergent un serveur DHCP ou peuvent offrir une liaison montante vers le serveur DHCP.

S1(config)# **ip dhcp snooping**	Activez la surveillance DHCP
S1(config)# **ip dhcp snooping vlan** *nombre*	Activez la surveillance DHCP pour des VLAN spécifiques
S1(config-if)# **ip dhcp snooping trust**	Au niveau de l'interface, définissez les ports comme étant fiables en définissant les ports fiables

Urpation arp

- **Les cybercriminels peuvent répondre aux requêtes et prétendre être des prestataires de services.**
- **Un type d'attaque par usurpation ARP utilisé par les pirates consiste à répondre à une requête ARP pour la passerelle par défaut. Dans la figure, l'hôte A demande l'adresse MAC de la passerelle par défaut. L'hôte C répond à la requête ARP. L'hôte A reçoit la réponse et met à jour sa table ARP. Il envoie ensuite des paquets destinés à la passerelle par défaut à l'hôte pirate C.**
- **Les commutateurs destinés aux grandes entreprises offrent des méthodes de limitation de ce risque appelées inspection ARP dynamique.**

Protocole NTP

L'utilisation d'une heure correcte sur un réseau est particulièrement importante. Des horodatages corrects sont nécessaires pour suivre avec précision les événements réseau tels que les violations de sécurité. Par ailleurs, la synchronisation des horloges est critique pour la bonne interprétation des événements au sein des fichiers de données Syslog, ainsi que pour les certificats numériques.

Le protocole NTP est un protocole utilisé pour synchroniser les horloges des systèmes informatiques appartenant à un réseau de données à paquets commutés et à latence variable.

Le protocole NTP permet aux périphériques réseau de synchroniser leurs paramètres de temps avec un serveur NTP. Un groupe de clients NTP qui obtient des informations d'heure et de date depuis une source unique présentera davantage de cohérence dans ses paramètres de temps.

Un périphérique réseau peut être configuré comme serveur ou comme client NTP. Pour permettre à l'horloge logicielle de se synchroniser à un serveur de temps NTP : **R(config)#ntp server** *adresse-ip*.

Pour configurer un périphérique comme disposant d'une horloge NTP maître à laquelle les pairs peuvent se synchroniser eux-mêmes : **R(config)#ntp master**

Pour afficher des informations telles que l'état de la synchronisation NTP, l'homologue avec lequel le périphérique est synchronisé et la strate sur laquelle le périphérique fonctionne : R#**show ntp status**