

les commandes cisco

Chapitre 1 : La Configuration de Base “Switch - Router”

Partie 1 : Configuration de base d'un routeur

Modes et invites de commande

Mode	Invite de commande
Mode utilisateur	Router>
Mode privilégié	Router#
Mode de configuration globale	Router(config)#
Mode de configuration d'interface	Router(config-if)#
Mode de configuration de ligne	Router(config-line)#
Mode de configuration du routeur	Router(config-router)#

Configuration de base du routeur dans Cisco IOS

a) Changer le nom du routeur

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

b) Protéger le mode privilégié

- Mot de passe non chiffré :

```
R1(config)# enable password 123
```

- Mot de passe chiffré :

```
R1(config)# enable secret 12345
```

c) Définir un nom de domaine

```
R1(config)# ip domain-name TRI.ma
```

d) Désactiver la recherche DNS , "Domain Name System" , "Système de Noms de Domaine"

```
R1(config)# no ip domain-lookup
```

La commande `no ip domain-lookup` empêche le périphérique de tenter une résolution DNS lorsqu'une commande est mal saisie, ce qui accélère l'affichage du message d'erreur.

e) Configurer la bannière du jour (Message of the Day)

```
R1(config)# banner motd #Bienvenue sur le routeur R1#
```

f) Configurer l'interface console

```
R1(config)# line console 0
R1(config-line)# password 123
R1(config-line)# logging synchronous
R1(config-line)# login
R1(config-line)# exec-timeout 5
R1(config-line)# exit
```

- Explication de " `logging synchronous` " :

Utilisé pour désactiver les messages non sollicités sur un routeur ou un switch Cisco :

Empêcher l'interruption des commandes

```
Router(config-line)# line console 0  
Router(config-line)# logging synchronous
```

- **Explication de " exec-timeout 5 " :**

Cette commande définit la durée d'inactivité d'une session (console ou VTY) avant la déconnexion automatique de l'utilisateur.

<aside>



5 signifie que la session expirera après 5 minutes d'inactivité.

Pour désactiver cette temporisation (c'est-à-dire ne jamais déconnecter automatiquement), vous pouvez utiliser :

```
R1(config-line)# exec-timeout 0 0
```

</aside>

g) Configuration de Telnet

```
R1(config)# line vty 0 15  
R1(config-line)# password 1234567  
R1(config-line)# login  
R1(config-line)# exit
```

Vérification sur un PC via Telnet "sur :commandes prompte de pc " :

```
Pc > telnet 192.168.1.1
```

h) Configuration de SSH

```
Router(config)# hostname R1  
R1(config)# ip domain-name TRI.ma  
R1(config)# username abdo password 12345678  
R1(config)# ip ssh version 2  
R1(config)# ip ssh authentication-retries 3  
R1(config)# crypto key generate rsa  
**Entrer la valeur "512"**  
R1(config)# line vty 0 3
```

```
R1(config-line)# transport input ssh  
R1(config-line)# login local  
R1(config-line)# exit  
R1(config)# ip ssh time-out 120
```

explication :

- `R1(config)# ip domain-name TRI.ma` : Définir le nom de domaine sur "TRI.ma".
- `R1(config)# username abdo password 12345678` : Créer un utilisateur "abdo" avec le mot de passe "12345678".
- `R1(config)# ip ssh authentication-retries 3` : Limiter le nombre de tentatives d'authentification SSH à 3.
- `R1(config)# crypto key generate rsa` : Générer une clé RSA pour sécuriser la connexion.
- `Entrer la valeur "512"` : Saisir la longueur de la clé à 512 bits.
- `R1(config-line)# transport input ssh` : Autoriser uniquement SSH pour l'accès à distance.
- `R1(config-line)# login local` : Activer l'authentification locale.
- `R1(config)# ip ssh time-out 120` : Définir le délai d'attente SSH à 120 secondes.

Accès SSH depuis un PC :

```
Pc > ssh -l abdo 192.168.1.2  
Password: (mot de passe utilisateur)
```

i) Chiffrement des mots de passe

```
R1(config)# service password-encryption
```

j) Réinitialisation des paramètres du routeur

Commandes :

```
erase startup-config  
reload
```

1 **erase startup-config**

- Supprime le fichier **startup-config** stocké dans la **NVRAM**.
- Toutes les configurations sauvegardées disparaissent.

2 **reload**

- Redémarre le routeur ou switch.
- Après le redémarrage, le périphérique démarre avec **les paramètres par défaut**.

k) Enregistrer les modifications

```
R1(config)# do write  
ou  
R1# write memory  
ou  
R1# copy running-config startup-config
```

running-config

✖ Définition :

Configuration actuelle du périphérique stockée dans la **RAM**.

- Active immédiatement après modification.
- Perdue après redémarrage si non sauvegardée.

startup-config

✖ Définition :

Configuration sauvegardée dans la **NVRAM**.

- Chargée automatiquement au démarrage.
- Conservée après redémarrage.

Configuration de base du routeur dans les interfaces :

a) Configurer une interface "GigabitEthernet - Serial"

```
R1(config)# interface GigabitEthernet0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

```
R1(config)# interface serial 0/0
R1(config-if)# ip address 44.44.44.1 255.255.255.224
R1(config-if)# clock rate 64000
R1(config-if)# description "connected to router X"
R1(config-if)# no shutdown
```

b) La commande **show running-config**

Est utilisée sur les équipements réseau Cisco (et d'autres fabricants) pour afficher la configuration en cours d'utilisation dans la mémoire vive (RAM).

Utilisation :

```
Router# show running-config
```

c) **show ip interface brief**

➤ Affiche un résumé : interfaces, adresses IP et état (up/down).

```
Routeur# show ip interface brief
```

Partie 2 : Configuration de base d'un switch

Configuration de base du switch dans Cisco IOS

a) Changer le nom du switch

```
Switch> enable  
Switch# configure terminal  
Switch(config)# hostname S1
```

b) Protéger le mode privilégié

- Mot de passe non chiffré :

```
S1(config)# enable password 123
```

- Mot de passe chiffré :

```
S1(config)# enable secret 12345
```

c) Définir un nom de domaine

```
S1(config)# ip domain-name TRI.ma
```

d) Désactiver la recherche DNS , "Domain Name System" , "Système de Noms de Domaine"

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

La commande `no ip domain-lookup` empêche le périphérique de tenter une résolution DNS lorsqu'une commande est mal saisie, ce qui accélère l'affichage du message d'erreur.

e) Configurer la bannière du jour (Message of the Day)

```
S1(config)# banner motd #Bienvenue sur le switch S1#
```

f) Configurer l'interface console

```
S1(config)# line console 0  
S1(config-line)# password 123
```

```
S1(config-line)# logging synchronous  
S1(config-line)# login  
S1(config-line)# exec-timeout 5  
S1(config-line)# exit
```

g) Configuration de Telnet

```
S1(config)# line vty 0 15  
S1(config-line)# password 1234567  
S1(config-line)# login  
S1(config-line)# exit
```

h) Configuration ssh sur un Switch

```
Switch(config)# hostname SW1  
SW1(config)# ip domain-name TRI.ma  
SW1(config)# username abdo password 12345678  
SW1(config)# username superabdo privilege 15 password 12345678  
SW1(config)# ip ssh version 2  
SW1(config)# ip ssh authentication-retries 3  
SW1(config)# crypto key generate rsa  
**Entrer la valeur "1024"**  
SW1(config)# line vty 0 3  
SW1(config-line)# transport input ssh  
SW1(config-line)# login local  
SW1(config-line)# exit  
SW1(config)# ip ssh time-out 120
```

- L'utilisateur "**abdo**" a le privilège par défaut **1** avec des droits limités, tandis que "**superabdo**" a le privilège **15**, lui accordant un accès complet à toutes les commandes administratives.
- Le niveau de **privilège 15** accorde un accès complet à toutes les commandes de configuration et d'exécution sur les appareils Cisco.

Accès SSH depuis un PC :

```
Pc > ssh -l abdo 192.168.1.2  
Password: (mot de passe utilisateur)
```

i) Chiffrement des mots de passe

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

j) Réinitialisation des paramètres du routeur

Commandes :

```
erase startup-config  
reload
```

1 erase startup-config

- Supprime le fichier **startup-config** stocké dans la **NVRAM**.
- Toutes les configurations sauvegardées disparaissent.

2 reload

- Redémarre le routeur ou switch.
- Après le redémarrage, le périphérique démarre avec **les paramètres par défaut**.

k) Enregistrer les modifications

```
S1# write memory  
ou  
S1# copy running-config startup-config
```

Configuration de base du switch dans les interfaces :

Configuration d'une VLAN sur un switch

Avantages du concept de VLAN

Avantages	Description
Domaines de Diffusion Plus Petits	La division du réseau local réduit le nombre de domaines de diffusion
Sécurité optimisée	Seuls les utilisateurs du même VLAN peuvent communiquer ensemble
Efficacité accrue des IT	Les VLAN peuvent regrouper des appareils ayant des exigences similaires, par exemple professeurs contre étudiants
Réduction des coûts	Un commutateur peut prendre en charge plusieurs groupes ou VLAN
Meilleures performances	Les domaines de diffusion plus petits réduisent le trafic et améliorent la bande passante
Gestion simplifiée	Des groupes similaires auront besoin d'applications similaires et d'autres ressources réseau

1. Création d'un VLAN

```
S1(config)# vlan 10
S1(config-vlan)# name Sales
S1(config-vlan)# exit
```

2. Assigner un VLAN à un port

```
S1(config)# interface FastEthernet0/2
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
```

3. Assigner un VLAN à un port

```
Switch(config)# interface range fa0/1 - 5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# no shutdown
Switch(config-if-range)# exit
```

4. Configuration de l'adresse IP du switch

```
S1(config)# interface vlan 10  
S1(config-if)# ip address 192.168.1.2 255.255.255.0  
S1(config-if)# no shutdown  
S1(config-if)# exit
```

5. Définir la passerelle par défaut

```
Switch(config)# ip default-gateway 192.168.1.1
```

6. Afficher et configurer l'horloge du switch

```
Switch# show clock  
Switch# clock set 16:32:00 31 aug 2025
```

7. Modifier le SDM pour activer IPv6 (si nécessaire)

```
Switch(config)# sdm prefer dual-ipv4-and-ipv6 default  
Switch(config)# end  
Switch# reload
```

commande pour afficher la liste des VLANs sur un switch :

```
Switch# show vlan
```

notion importante sur VLAN

1 Définition des VLAN

- **VLAN (Virtual Local Area Network)** = réseau local virtuel sur un même switch ou plusieurs switches.
- Fonctionne au niveau **Layer 2 (Data Link)** et **isole les domaines de broadcast**.
- Chaque VLAN a généralement un **subnet (réseau IP) indépendant**.

2 Objectif principal des VLAN

- Isolation des broadcasts :

Empêche les messages broadcast de passer d'un VLAN à un autre.

- Organisation du réseau :

Division du réseau selon les départements (Clients, Administration, Serveurs...).

- Facilitation de la gestion :

Gestion simplifiée des DHCP, ACL, QoS, et extension facile du réseau.

- Amélioration partielle de la sécurité :

L'isolation au niveau Layer 2 empêche les appareils de communiquer directement entre VLANs, mais **la sécurité réelle nécessite Layer 3 + ACLs/Firewalls**.

3 Règles importantes pour les VLAN

1. Chaque VLAN = subnet indépendant.
2. Un même VLAN doit conserver le même subnet si étendu sur plusieurs switches.
3. La communication entre VLANs nécessite un routeur ou un switch Layer 3 (Inter-VLAN Routing).
4. Les ports Access appartiennent à un seul VLAN.
5. Les liens Trunk permettent de transporter plusieurs VLANs entre switches.
6. Noms clairs pour les VLANs afin d'éviter la confusion dans les grands réseaux.
7. Le VLAN ne bloque pas le trafic après activation de l'Inter-VLAN Routing
→ la sécurité se fait au niveau Layer 3.

4 Scénarios réels

- Entreprise :

- VLAN10 → Clients

- VLAN20 → Administration
- VLAN30 → Serveurs
- Chaque département isolé au Layer 2, communication contrôlée via Routeur + ACL.

- **École ou bâtiment :**

- VLAN1 → Étudiants
- VLAN2 → Enseignants
- VLAN3 → Administration
- L'isolation protège le réseau et réduit le trafic broadcast inutile.

5 Sécurité

- **Le VLAN n'est pas un pare-feu !**
- L'isolation Layer 2 empêche la communication directe, mais **avec l'Inter-VLAN Routing, les appareils peuvent communiquer si aucune ACL n'est appliquée.**
- La sécurité réelle = **Routing + ACL + Firewalls.**

6 Conseils pratiques

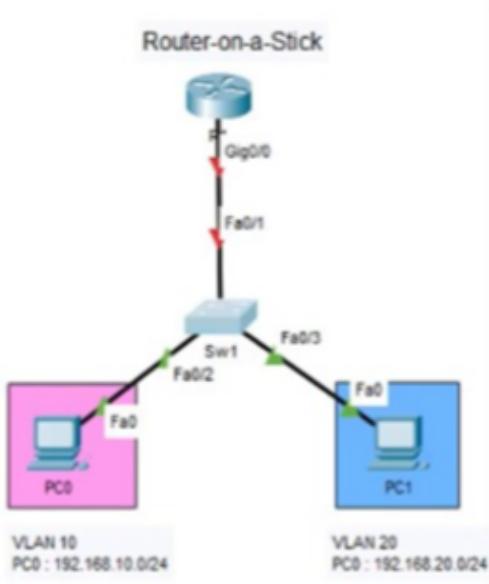
1. Planifier les subnets avant de créer les VLANs.
2. Documenter l'ID, le nom et la fonction de chaque VLAN.
3. Utiliser les liens Trunk avec précaution et définir les VLANs autorisés.
4. Activer les SVI ou Router-on-a-Stick pour l'Inter-VLAN Routing si nécessaire.
5. Mettre en place des ACL pour limiter les communications entre VLANs.
6. Surveiller les broadcasts et les tables MAC pour éviter les boucles.

💡 Conclusion clé :

Un VLAN sert à organiser le réseau et isoler les broadcasts, mais ce n'est pas un mécanisme de sécurité complet. La communication entre VLANs se

fait uniquement via Layer 3, et la sécurité réelle se met en place avec le routage et les politiques (ACLs, Firewalls).

configuration Router-on-a-Stick "inter-vlan"



Ce réseau utilise un **routeur-on-a-stick**, un **switch** et deux **PC** connectés à deux VLANs différents (VLAN 10 et VLAN 20).

1 Configuration du Switch

Entrez en mode privilégié :

```
Switch> enable  
Switch# configure terminal
```

Créer les VLANs :

```
Switch(config)# vlan 10  
Switch(config-vlan)# name VLAN10  
Switch(config-vlan)# exit
```

```
Switch(config)# vlan 20
```

```
Switch(config-vlan)# name VLAN20  
Switch(config-vlan)# exit
```

Configurer les ports d'accès pour les PC :

```
Switch(config)# interface FastEthernet 0/2  
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport access vlan 10  
Switch(config-if)# exit
```

```
Switch(config)# interface FastEthernet 0/3  
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport access vlan 20  
Switch(config-if)# exit
```

Configurer le port Trunk vers le routeur :

```
Switch(config)# interface FastEthernet 0/1  
Switch(config-if)# switchport mode trunk  
Switch(config-if)# switchport trunk encapsulation dot1q  
Switch(config-if)# exit
```

Sauvegarder la configuration :

```
Switch(config)# end  
Switch# write memory
```

2 Configuration du Routeur

Entrez en mode privilégié :

```
Router> enable  
Router# configure terminal
```

Activer l'interface principale :

```
Router(config)# interface GigabitEthernet 0/0  
Router(config-if)# no shutdown
```

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

Créer les sous-interfaces pour les VLANs :

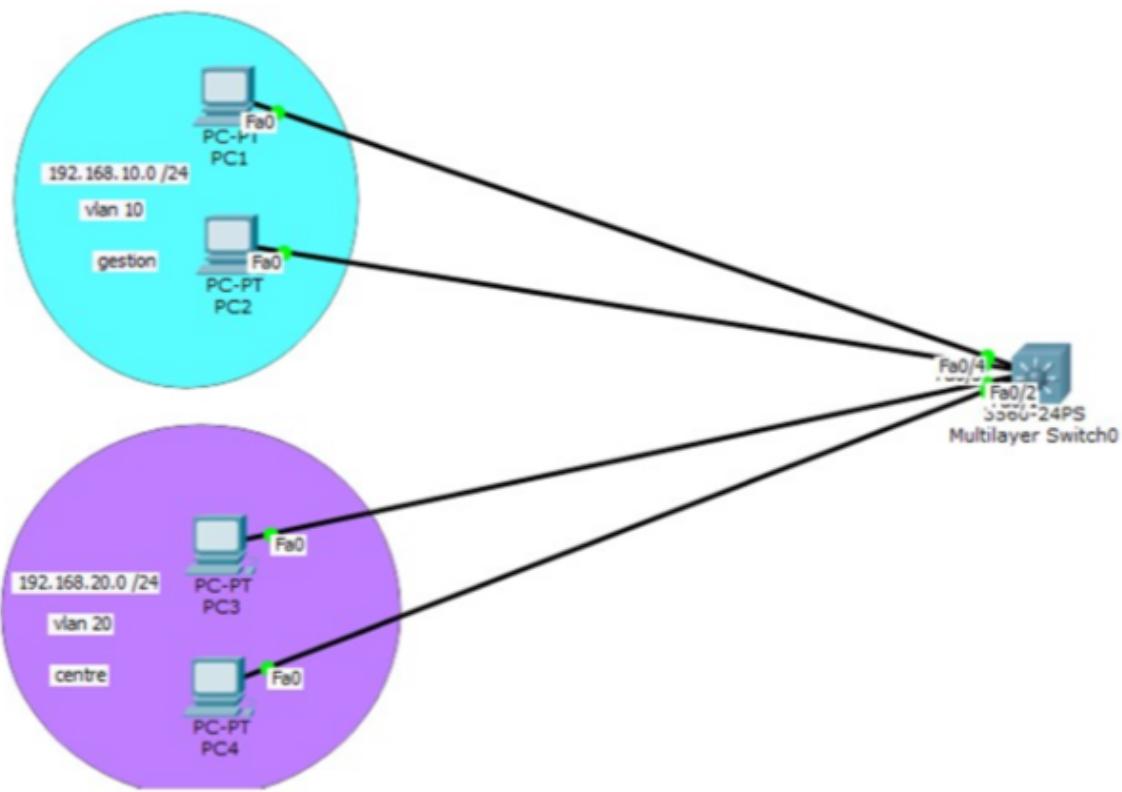
```
Router(config)# interface GigabitEthernet 0/0.10
Router(config-subif)# encapsulation dot1Q 10
Router(config-subif)# ip address 192.168.10.1 255.255.255.0
Router(config-subif)# exit
```

```
Router(config)# interface GigabitEthernet 0/0.20
Router(config-subif)# encapsulation dot1Q 20
Router(config-subif)# ip address 192.168.20.1 255.255.255.0
Router(config-subif)# exit
```

Sauvegarder la configuration :

```
Router(config)# end
Router# write memory
```

��置多层交换机以实现VLAN间路由



1 Objectif

- PC1 & PC2 dans **VLAN 10**
- PC3 & PC4 dans **VLAN 20**
- Un switch multilayer pour gérer le routage entre VLANs

2 Configuration des VLANs sur le Switch

📌 Crédit de VLANs

```

Switch> enable
Switch# configure terminal

# VLAN 10
Switch(config)# vlan 10
Switch(config-vlan)# name VLAN10
Switch(config-vlan)# exit

# VLAN 20
Switch(config)# vlan 20

```

```
Switch(config-vlan)# name VLAN20
Switch(config-vlan)# exit
```

✖ Attribution des ports aux VLANs

```
# PC1 → VLAN 10
Switch(config)# interface FastEthernet0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

# PC2 → VLAN 10
Switch(config)# interface FastEthernet0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# exit

# PC3 → VLAN 20
Switch(config)# interface FastEthernet0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit

# PC4 → VLAN 20
Switch(config)# interface FastEthernet0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 20
Switch(config-if)# exit
```

3 Activation du Routage Inter-VLAN

```
Switch(config)# ip routing
```

✖ Configuration des interfaces VLAN

```
# VLAN 10 (Passerelle : 192.168.10.1)
Switch(config)# interface Vlan10
Switch(config-if)# ip address 192.168.10.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit

# VLAN 20 (Passerelle : 192.168.20.1)
Switch(config)# interface Vlan20
Switch(config-if)# ip address 192.168.20.1 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
```

4 Configuration du Trunk (Si un autre switch est utilisé)

```
Switch(config)# interface GigabitEthernet0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 10,20
Switch(config-if)# exit
```

5 Enregistrement de la Configuration

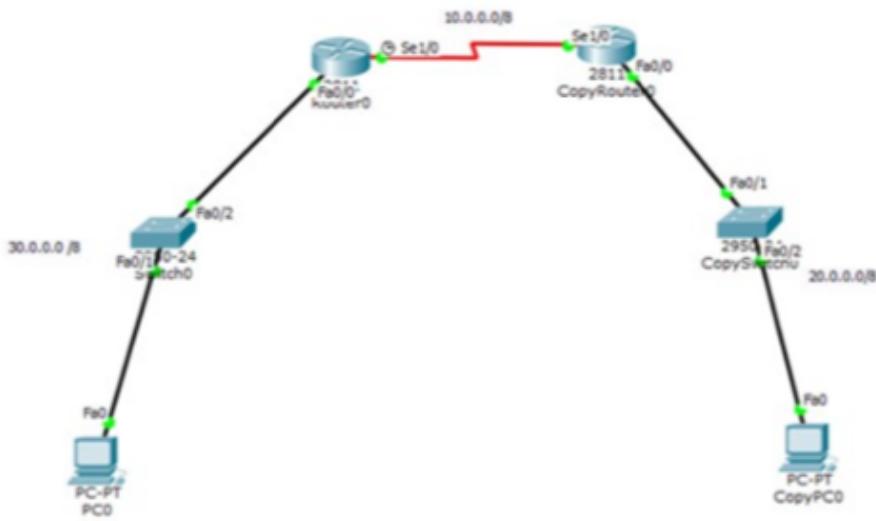
```
Switch(config)# end
Switch# write memory
```

6 Configuration des PC (Adresses IP statiques)

PC	VLAN	Adresse IP	Passerelle
PC1	10	192.168.10.2/24	192.168.10.1
PC2	10	192.168.10.3/24	192.168.10.1
PC3	20	192.168.20.2/24	192.168.20.1
PC4	20	192.168.20.3/24	192.168.20.1

partie 3 : Routage Statique IPv4

EXERCICE 1 :



1 - Configuration des PC

PC	Adresse IP	Masque	Passerelle
PC0	30.0.0.2	255.0.0.0	30.0.0.1
PC1	20.0.0.2	255.0.0.0	20.0.0.1

2 - Configuration des interfaces des routeurs

Router0

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 30.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config)# interface Serial1/0
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router# write memory
```

Router1

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet0/0
Router(config-if)# ip address 20.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config)# interface Serial1/0
Router(config-if)# ip address 10.0.0.2 255.0.0.0
Router(config-if)# no shutdown
Router# write memory
```

3 - Configuration du routage statique

a) Avec Next-Hop

Router0 → Router1

```
Router(config)# ip route 20.0.0.0 255.0.0.0 10.0.0.1
Router# write memory
```

Router1 → Router0

```
Router(config)# ip route 30.0.0.0 255.0.0.0 10.0.0.2
Router# write memory
```

b) Avec l'Interface de Sortie

Router0 → Router1

```
Router(config)# ip route 20.0.0.0 255.0.0.0 s1/0
Router# write memory
```

Router1 → Router0

```
Router(config)# ip route 30.0.0.0 255.0.0.0 s1/0  
Router# write memory
```

c) Routage par défaut

Router0

```
Router(config)# ip route 0.0.0.0 0.0.0.0 s1/0  
Router# write memory
```

Router1

```
Router(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2  
Router# write memory
```

Distance Administrative (AD)

- **Définition :** La distance administrative est une valeur numérique utilisée par un routeur pour indiquer la **fiabilité d'une source de routage**.
- **Principe :** Plus la valeur est petite → plus la route est fiable et prioritaire.
- **Rôle :** Lorsqu'un routeur reçoit plusieurs routes vers le même réseau (RIP, OSPF, EIGRP, statique...), il choisit **celle avec la plus petite distance administrative** et l'insère dans la table de routage.

Valeurs par défaut (Cisco) :

Méthode / Protocole	AD
Connecté directement	0
Statique	1
EIGRP interne	90
OSPF	110
RIP	120

Méthode / Protocole	AD
EIGRP externe	170
Route invalide	255

✖ Routage Flottant (Floating Static Route)

- **Définition :** Un routage flottant est une **route statique de secours** utilisée uniquement si la route principale devient indisponible.
- **Fonctionnement :**
 - La route principale a une **petite AD** (ex. 1).
 - La route de secours a une **AD plus élevée** (ex. 200).
 - Si la route principale échoue, le routeur active automatiquement la route flottante.

Exemple :

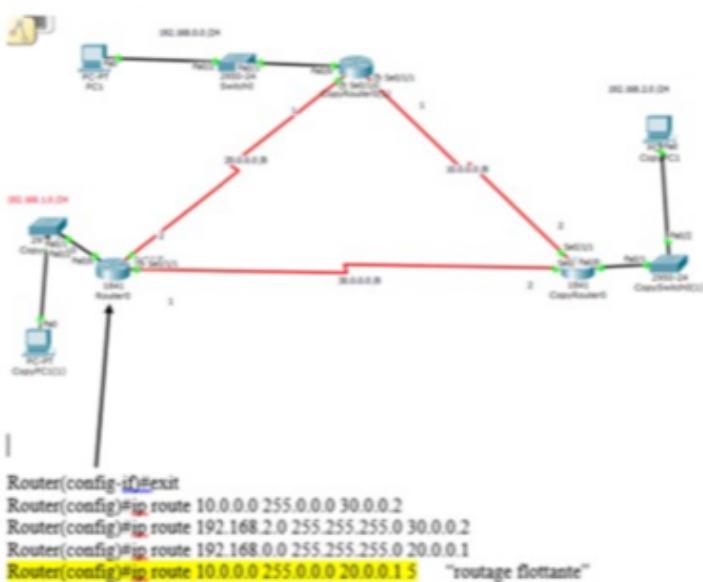
- Route principale :

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1 1
```

- Route flottante (backup) :

```
ip route 0.0.0.0 0.0.0.0 192.168.2.1 200-
```

d) Routage statique flottante



4 - Vérification de la table de routage

```
Router# show ip route
```

5 - Suppression d'une Route

```
Router(config)# no ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

partie 4 : ROUTAGE Dynamique ipv4

1 - Configuration de RIP (Routing Information Protocol)

Types de routage

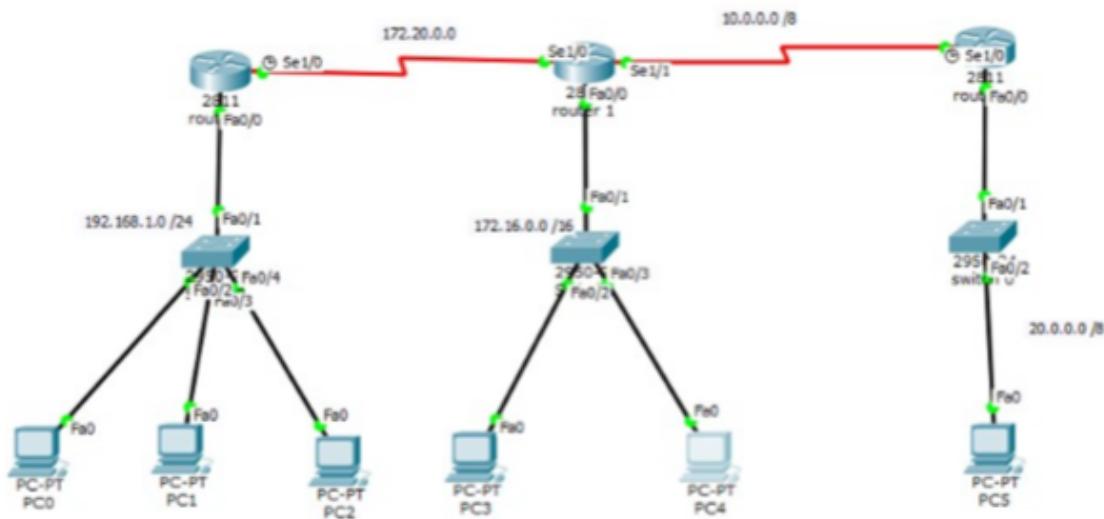
- **Statique** : configuration manuelle des tables de routage par l'administrateur.
- **Dynamique** : les routeurs construisent automatiquement leurs tables via des protocoles de routage.

1. Présentation de RIP

RIP est un protocole de routage à vecteur de distance. Il existe en deux versions :

- **RIP v1** : Classful
- **RIP v2** : Classless, prend en charge VLSM

2. Configuration de RIP



Sur Router0 :

```
Router0> enable
Router0# configure terminal
Router0(config)# router rip
Router0(config-router)# version 2
Router0(config-router)# network 10.0.0.0
Router0(config-router)# network 20.0.0.0
Router0(config-router)# no auto-summary
Router0(config-router)# exit
Router0(config)# exit
Router0# write memory
```

Sur Router1 :

```
Router1> enable
Router1# configure terminal
Router1(config)# router rip
Router1(config-router)# version 2
Router1(config-router)# network 10.0.0.0
Router1(config-router)# network 172.16.0.0
Router1(config-router)# network 172.20.0.0
Router1(config-router)# no auto-summary
Router1(config-router)# exit
Router1(config)# exit
Router1# write memory
```

Sur Router2 :

```
Router2> enable
Router2# configure terminal
Router2(config)# router rip
Router2(config-router)# version 2
Router2(config-router)# network 172.20.0.0
Router2(config-router)# network 192.168.1.0
Router2(config-router)# no auto-summary
Router2(config-router)# exit
Router2(config)# exit
Router2# write memory
```

- **no auto-summary** : Désactive le résumé automatique des routes pour permettre le VLSM.

4. Configuration d'une route par défaut et propagation dans RIP

```
Router1(config)# ip route 0.0.0.0 0.0.0.0 172.20.0.2
Router1(config)# router rip
Router1(config-router)# default-information originate
Router1(config-router)# exit
```

- **default-information originate** : Permet d'annoncer une route par défaut aux autres routeurs du réseau.

5. Vérification de la table de routage RIP

```
Router# show ip route
```

6. Désactivation des mises à jour RIP sur une interface

```
Router(config)# router rip  
Router(config-router)# passive-interface <interface>
```

7. la distance administrative

- **Distance administrative** : Valeur définissant la priorité des protocoles de routage. Plus elle est faible, plus le protocole est prioritaire.
- **Exemples de distances administratives**

Protocole de Routage	Distance Administrative (AD)	Fiabilité
Route connectée directement	0	✓✓✓ Très fiable
Route statique	1	✓✓✓ Très fiable
EIGRP (interne)	90	✓✓ Fiable
OSPF	110	✓ Moyen
RIP	120	✗ Peu fiable

Modification de la Distance Administrative (Administrative Distance) pour RIP

◆ Commande :

```
router rip  
distance 80
```

✓ Rôle :

- Modifie la **distance administrative** du protocole **RIP**, qui est par défaut **120**, pour la définir à **80**.
- Cela donne à **RIP** une **priorité plus élevée** par rapport aux autres protocoles ayant une distance supérieure à **80**, comme **OSPF (110)** et **EIGRP (90)**.
- **Configuration des minuteries du protocole de routage**

```
timers basic 45 120 120 130
```

Rôle : Définit les minuteries du protocole de routage :

- **45** secondes : Intervalle entre les mises à jour.
- **120** secondes : Délai avant de considérer une route comme invalide.
- **120** secondes : Temps d'attente avant de purger une route obsolète.
- **130** secondes : Temps total avant de supprimer une route de la table de routage.

Désactivation de Split Horizon sur un routeur Cisco

- **Split Horizon** empêche un routeur d'envoyer des mises à jour de routage sur la même interface par laquelle il les a reçues, afin d'éviter les boucles.
- Pour le désactiver sur une interface spécifique :

```
R1(config)# interface Serial0/0  
R1(config-if)# no ip split-horizon  
R1(config-if)# exit
```

- **Affichage des paramètres et protocoles de routage en cours**

```
show ip protocols
```

Rôle : Affiche les détails des protocoles de routage activés, les minuteries, les interfaces participant au routage et les routes apprises.

2 - Configuration d'OSPF pour IPv4

Routeur 1 :

```
Router(config)# router ospf 1  
Router(config-router)# network 12.0.0.0 0.255.255.255 area 0  
Router(config-router)# network 192.168.0.0 0.0.0.31 area 0  
Router(config-router)# network 30.0.0.0 0.0.0.3 area 0
```

```
Router(config-router)# exit  
Router# write memory
```

Routeur 2 :

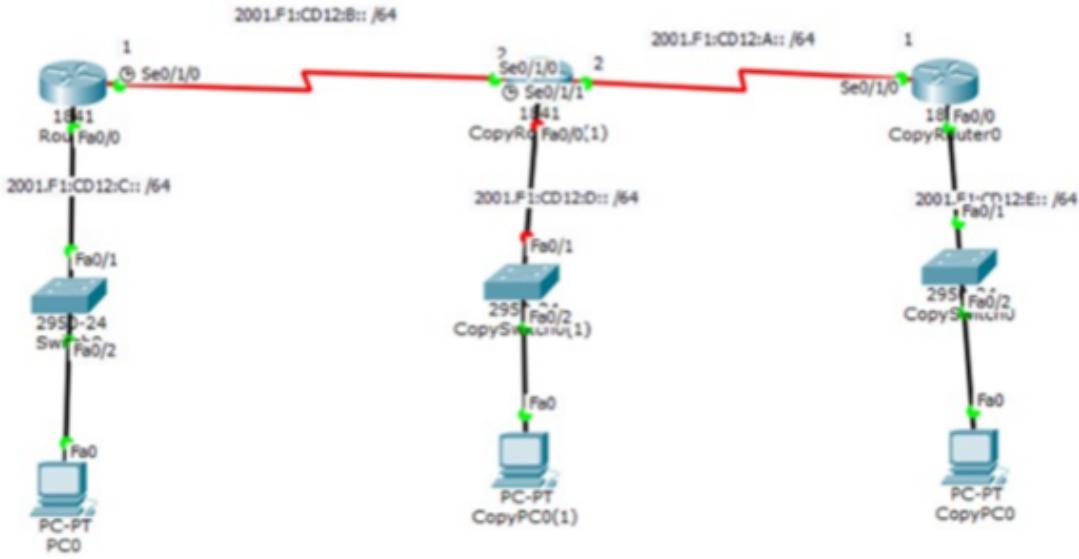
```
Router(config)# router ospf 1  
Router(config-router)# network 192.168.0.0 0.0.0.31 area 0  
Router(config-router)# network 20.0.0.0 0.0.0.3 area 0  
Router(config-router)# network 30.0.0.0 0.0.0.3 area 0  
Router(config-router)# exit  
Router# write memory
```

La commande **router-id** est utilisée pour définir un identifiant unique et statique pour le routeur, comme indiqué dans la commande suivante :

```
R_Tanger(config-router)#router-id 1.1.1.1
```

partie 5 : Routage Statique IPv6

exercice 1 :



1 - Configuration des interfaces des routeurs

Routeur 1

```
Router> enable
Router# configure terminal
Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 address 2001:F1:CD12:C::1/64
Router(config-if)# no shutdown
Router(config)# interface serial 0/1/0
Router(config-if)# ipv6 address 2001:F1:CD12:B::1/64
Router(config-if)# clock rate 64000
Router(config-if)# no shutdown
Router# write memory
```

Routeur 2

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0/1/0
Router(config-if)# ipv6 address 2001:F1:CD12:B::2/64
Router(config-if)# no shutdown
Router(config)# interface serial 0/1/1
Router(config-if)# ipv6 address 2001:F1:CD12:A::2/64
Router(config-if)# clock rate 64000
Router(config-if)# no shutdown
Router# write memory
```

Routeur 3

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0/1/0
Router(config-if)# ipv6 address 2001:F1:CD12:A::1/64
Router(config-if)# no shutdown
Router(config)# interface fastEthernet 0/0
Router(config-if)# ipv6 address 2001:F1:CD12:E::1/64
```

```
Router(config-if)# no shutdown  
Router# write memory
```

Affichage des informations des interfaces IPv6 :

Commande :

```
show ipv6 interface brief
```

2 - Configuration du routage statique ipv6 :

a) Activation du routage unicast :

"Dans tous les routeurs "

```
Router> enable  
Router# configure terminal  
Router(config)# ipv6 unicast-routing
```

b) Configuration du routage statique IPv6

Routeur 1

```
Router(config)# ipv6 route 2001:F1:CD12:E::/64 SE0/1/0  
Router(config)# ipv6 route 2001:F1:CD12:A::/64 SE0/1/0  
Router(config)# ipv6 route 2001:F1:CD12:D::/64 SE0/1/0  
Router# write memory
```

Routeur 2

```
Router(config)# ipv6 route 2001:F1:CD12:C::/64 SE0/1/0  
Router(config)# ipv6 route 2001:F1:CD12:E::/64 SE0/1/1  
Router# write memory
```

Routeur 3

```
Router(config)# ipv6 route 2001:F1:CD12:C::/64 SE0/1/0
Router(config)# ipv6 route 2001:F1:CD12:B::/64 SE0/1/0
Router(config)# ipv6 route 2001:F1:CD12:D::/64 SE0/1/0
Router# write memory
```

c) Vérification de la table de routage IPv6

```
Router# show ipv6 route
```

d) Routage statique IPv6 par défaut

```
Router(config)# ipv6 route ::/0 interface_de_sortie
```

3) Configuration de RIPng pour IPv6

Sur Router1 :

```
Router1> enable
Router1# configure terminal
Router1(config)# ipv6 unicast-routing
Router1(config)# ipv6 router rip test
Router1(config-rtr)# exit
Router1(config)# interface G0/0
Router1(config-if)# ipv6 rip test enable
Router1(config-if)# exit
Router1(config)# interface S0/0/0
Router1(config-if)# ipv6 rip test enable
Router1(config-if)# exit
Router1# write memory
```

Vérification :

```
show ipv6 database
```

4) Configuration d'OSPFv3 pour IPv6

a) Activation du routage IPv6

Cette commande doit être exécutée sur **chaque routeur** pour activer le routage IPv6 :

```
R1 > enable  
R1# configure terminal  
R1(config)# ipv6 unicast-routing
```

b) Configuration d'OSPFv3

◆ Sur R1

```
R1(config)# ipv6 router ospf 10  
R1(config-rtr)# router-id 1.1.1.1  
  
R1(config)# interface g0/0  
R1(config-if)# ipv6 ospf 10 area 0  
  
R1(config)# interface se0/0/0  
R1(config-if)# ipv6 ospf 10 area 0  
  
R1(config)# interface se0/0/1  
R1(config-if)# ipv6 ospf 10 area 0
```

◆ Sur R2

```
R2(config)# ipv6 router ospf 10  
R2(config-rtr)# router-id 2.2.2.2  
  
R2(config)# interface g0/0  
R2(config-if)# ipv6 ospf 10 area 0  
  
R2(config)# interface se0/0/0
```

```
R2(config-if)# ipv6 ospf 10 area 0
```

```
R2(config)# interface se0/0/1
```

```
R2(config-if)# ipv6 ospf 10 area 0
```

◆ Sur R3

```
R3(config)# ipv6 router ospf 10
```

```
R3(config-rtr)# router-id 3.3.3.3
```

```
R3(config)# interface g0/0
```

```
R3(config-if)# ipv6 ospf 10 area 0
```

```
R3(config)# interface se0/0/0
```

```
R3(config-if)# ipv6 ospf 10 area 0
```

```
R3(config)# interface se0/0/1
```

```
R3(config-if)# ipv6 ospf 10 area 0
```

c) Vérification du fonctionnement d'OSPFv3

Commandes utiles pour vérifier la configuration OSPFv3 :

```
show ipv6 route
```

```
show ipv6 ospf neighbor
```

5 - Calcul de l'adresse IPv6 Link-Local avec EUI-64

✖ Exemple avec une adresse MAC donnée :

Supposons que nous ayons l'adresse MAC suivante :

```
00:1A:2B:3C:4D:5E
```

1 Diviser l'adresse MAC en deux parties :

00:1A:2B 3C:4D:5E

2 Insérer FF:FE au milieu :

00:1A:2B:FF:FE:3C:4D:5E

3 Modifier le 7^e bit du premier octet :

- Conversion du premier octet (00) en binaire :

0000 0000

- Inversion du 7^e bit (le deuxième bit en partant de la gauche, de 0 à 1) :

0000 0010 = 02 (en hexadécimal)

Le premier octet devient 02, donc l'adresse devient :

02:1A:2B:FF:FE:3C:4D:5E

4 Conversion en format IPv6 :

- Regroupement en segments de 16 bits :

021A:2BFF:FE3C:4D5E

- Ajout du préfixe FE80::/10 pour générer l'adresse Link-Local :

FE80::21A:2BFF:FE3C:4D5E

✓ Résultat final :

Adresse IPv6 Link-Local calculée :

FE80::21A:2BFF:FE3C:4D5E

6 - Configuration d'une adresse IPv6 Link-Local sur trois routeurs Cisco :

Objectif :

Configurer des adresses **Link-Local** pour permettre la communication locale entre eux.

1 Configuration sur le premier routeur (Router 1) :

1. Accéder à la configuration :

```
Router> enable  
Router# configure terminal  
Router(config)# interface GigabitEthernet0/0  
Router(config-if)# ipv6 address FE80::1 link-local
```

2. Vérifier la configuration de l'interface :

```
Router# show ipv6 interface brief
```

2 Configuration sur le deuxième routeur (Router 2) :

1. Accéder à la configuration :

```
Router> enable  
Router# configure terminal  
Router(config)# interface GigabitEthernet0/0  
Router(config-if)# ipv6 address FE80::2 link-local
```

2. Vérifier la configuration de l'interface :

```
Router# show ipv6 interface brief
```

3 Configuration sur le troisième routeur (Router 3) :

1. Accéder à la configuration :

```
Router> enable  
Router# configure terminal  
Router(config)# interface GigabitEthernet0/0  
Router(config-if)# ipv6 address FE80::3 link-local
```

2. Vérifier la configuration de l'interface :

```
Router# show ipv6 interface brief
```

Note :

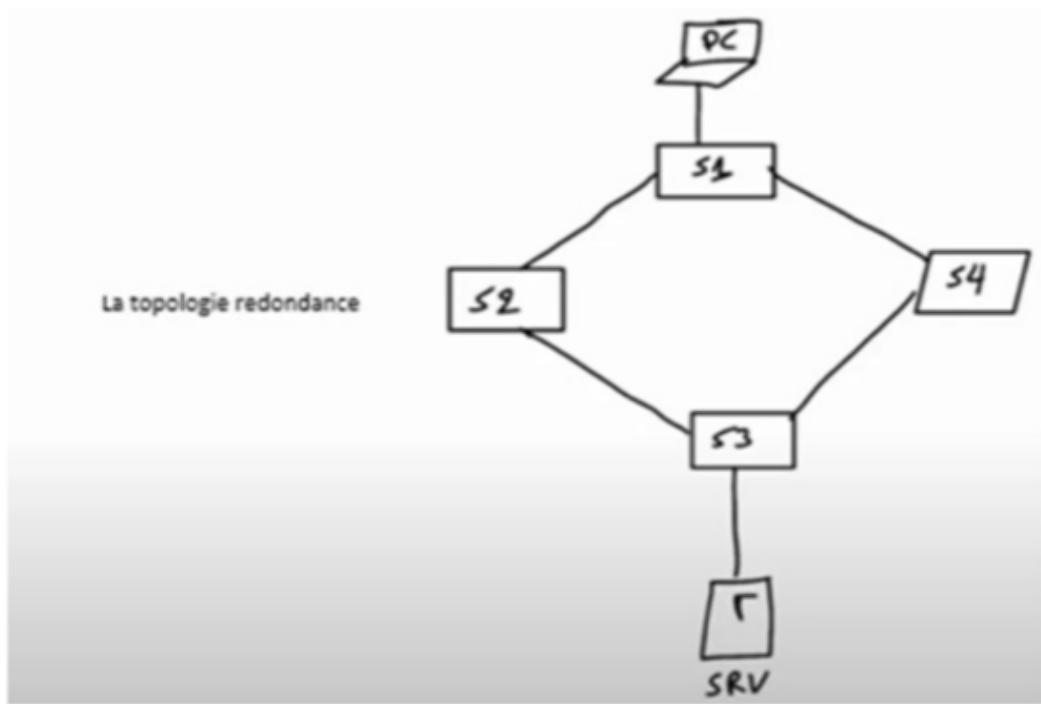
Chaque interface sur le même routeur a une adresse Link-Local unique basée sur l'adresse MAC de l'interface. L'adresse est générée à l'aide de EUI-64 avec le préfixe **FE80::/10**.

partie 6 : Protocole Spanning Tree (STP) :

1. Fonctionnement d'un commutateur

- Apprentissage des adresses MAC
- Prise de décision de transfert
- Prévention des boucles de commutation

Problèmes de redondance dans une topologie sans STP



2 - Problèmes de redondance dans une topologie sans STP.

- Boucles de commutation (Switching Loops)
- Tempête de diffusion (Broadcast Storm)
- Duplication des trames (Duplicate Frames)
- Instabilité de la table des adresses MAC
- Consommation excessive des ressources réseau



Solution : Utilisation du protocole STP

Protocole Spanning Tree (STP)

Le **Spanning Tree Protocol (STP)** est un protocole de la **couche 2** qui empêche les boucles en bloquant certains chemins redondants.

Les 4 étapes du STP.

1. Élection du pont racine (Root Bridge)
2. Sélection des ports racine (Root Ports)

3. Définition des ports désignés (Designated Ports)

4. Blocage des ports alternatifs (Blocked Ports)

Tableau des coûts STP selon le type de câble.

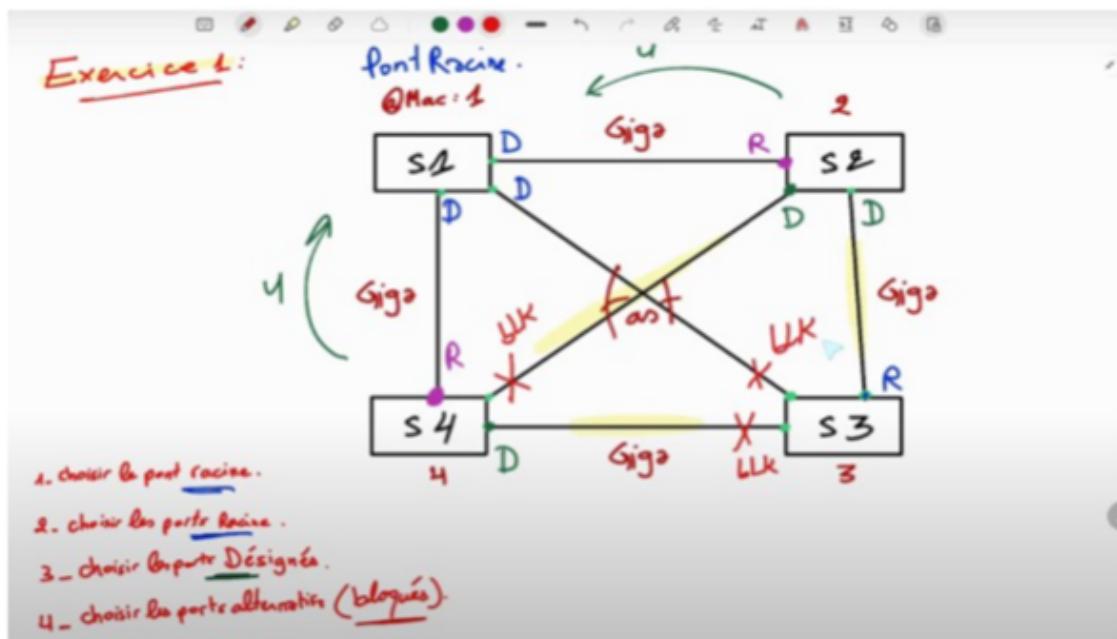
Bande passante	Coût du chemin (Path Cost)
10 Mbps (Ethernet)	100
100 Mbps (Fast Ethernet)	19
1 Gbps (Gigabit Ethernet)	4
10 Gbps (10-Gigabit Ethernet)	2

◆ Règle pour calculer le nombre de ports bloqués

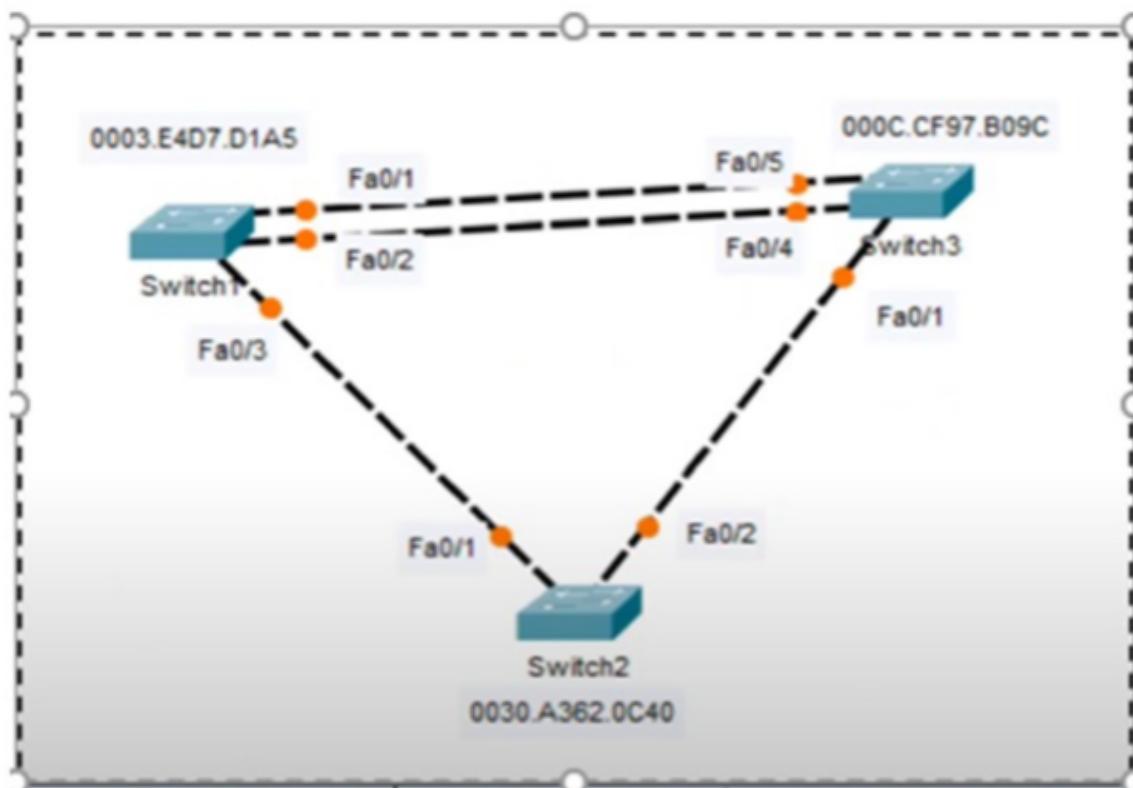
◆ Formule :

$$\text{Nombre de ports bloqués} = (\text{Nombre de câbles} - \text{Nombre de switches}) + 1$$

exercice 1 :



💡 Exercice :



Le commutateur	La priorité	L'adresse MAC
Switch 1	32769	0003.E4D7.D1A5
Switch 2	32769	0030.A362.0C40
Switch 3	32769	000C.CF97.B09C

- 1- Déterminer le pont racine.
- 2- Déterminer les ports racines.
- 3- Déterminer les ports désignés et les ports alternatifs.
- 4- Quelle est la commande qui permet d'afficher les informations ci-dessus ?

1 Sélection du pont racine (Root Bridge)

Le Root Bridge est déterminé en fonction de la plus petite valeur du **Bridge ID (BID)**.

Composition du BID :

- ✓ **Priorité** : Par défaut, tous les commutateurs ont la même valeur (32769).
- ✓ **Adresse MAC** : En cas d'égalité de priorité, le commutateur avec l'adresse MAC la plus faible est sélectionné.

Comparaison des adresses MAC :

Commutateur	Adresse MAC	Sélectionné ?
Switch 1	0003.E4D7.D1A5	(Adresse MAC la plus faible)
Switch 2	0030.A362.0C40	
Switch 3	000C.CF97.B09C	

→ Switch 1 est donc élu Root Bridge.

2 Détermination des ports racines (Root Ports - RP)

Le **port racine** est celui qui a le coût le plus faible pour atteindre le **Root Bridge** (Switch 1).

☛ **Coût du chemin (Path Cost) selon la vitesse du port :**

Vitesse du port	Coût par défaut
10 Mbps	100
100 Mbps (Fast Ethernet)	19
1 Gbps (Gigabit Ethernet)	4

◆ Tous les ports sont en FastEthernet (100 Mbps), donc le coût de chaque liaison est de 19.

✓ Détermination des ports racines :

- **Switch 2** a deux connexions avec le **Root Bridge** (Switch 1) :
 - Fa0/1 (direct vers Switch 1) → Coût = 19
 - Fa0/2 (via Switch 3 → Switch 1) → Coût = 38 (19 + 19)

→ Fa0/1 est choisi comme port racine de Switch 2.
- **Switch 3** a trois connexions :
 - Fa0/5 (direct vers Switch 1 via Fa0/1) → Coût = 19
 - Fa0/4 (direct vers Switch 1 via Fa0/2) → Coût = 19
 - Fa0/1 (via Switch 2 → Switch 1) → Coût = 38 (19 + 19)

→ Pourquoi Fa0/5 est-il choisi comme port racine ?

✓ Fa0/4 et Fa0/5 ont le même coût (19).

- ✓ On compare alors le numéro du port sur le Root Bridge (Switch 1).
- ✓ Si Fa0/5 a un numéro inférieur à Fa0/4 sur Switch 1, alors Fa0/5 est choisi. ✓
- ✓ Le port Fa0/4 est mis en mode Blocking pour éviter les boucles.

3 Détermination des ports désignés et alternatifs

✓ Ports désignés (Designated Ports - DP) :

- ✓ Tout port du Root Bridge est automatiquement désigné.
- ✓ Tout port qui constitue le seul chemin actif vers un segment est désigné.
- ◆ Liste des ports désignés :
 - ✓ Tous les ports de Switch 1 (car c'est le Root Bridge).
 - ✓ Fa0/2 sur Switch 2 (seul chemin actif pour Switch 3).
 - ✓ Fa0/4 sur Switch 3 (seul chemin actif pour Switch 2).

🚫 Ports bloqués (Alternate/Blocking Ports - BP) :

- ✓ Les ports qui créent une boucle sont bloqués.
- ◆ Liste des ports bloqués :
 - Fa0/1 sur Switch 3 → Bloqué pour éviter une boucle via Switch 2.

4 Commande pour afficher les informations STP

█ Commande CLI :

```
show spanning-tree
```

- ◆ Cette commande affiche :
 - ✓ Le pont racine (Root Bridge)
 - ✓ Les ports racines (Root Ports)
 - ✓ Les ports désignés (Designated Ports)
 - ✓ Les ports bloqués (Blocking Ports)

5 Configuration du Root Bridge principal et secondaire

1. Modifier la priorité du switch

Pour modifier la **priorité du switch** dans **Packet Tracer** avec le **Spanning Tree Protocol (STP)**, suivez ces étapes :

```
Switch> enable
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 priority 4096
Switch(config)# exit
Switch# write memory
```

◆ Explication :

Plus la valeur de la priorité est **faible**, plus il est probable que ce switch devienne le Root Bridge.

2. Définir le Root Bridge principal

■ Commande CLI :

```
router> enable
router# configure terminal
router(config)# spanning-tree vlan 1 root primary
```

- ✓ Définit le switch comme **Root Bridge principal pour le VLAN 1**.
- ✓ Réduit automatiquement la priorité pour s'assurer qu'il devienne le Root Bridge.

3. Définir le Root Bridge secondaire

■ Commande CLI :

```
router> enable
router# configure terminal
router(config)# spanning-tree vlan 1 root secondary
```

Avantages et inconvénients du STP

Avantages :

- Évite les boucles, améliore la stabilité.
- Assure la redondance intelligemment.
- S'adapte automatiquement aux changements.

Inconvénients :

- Peut induire un retard d'adaptation.
- Nécessite une configuration précise.

Pour configurer RSTP sur un switch :

1. Activer RSTP :

```
switch> enable  
switch# configure terminal  
switch(config)# spanning-tree mode rapid-pvst
```

partie 7 : etherchannel

Modes EtherChannel sur Cisco

Cisco propose plusieurs modes de configuration d'EtherChannel, regroupés en modes de négociation et mode statique.

PAgP (Port Aggregation Protocol - Protocole propriétaire Cisco)

Protocole propriétaire Cisco permettant une négociation dynamique de l'agrégation des liens.

- **Auto** : Attente d'une proposition de l'autre équipement.
- **Desirable** : Envoi actif de demandes d'agrégation.

LACP (Link Aggregation Control Protocol - IEEE 802.3ad)

Protocole **standard** permettant l'agrégation de liens en mode **Active** ou **Passive**.

- **Active** : Le switch **tente activement** de négocier l'agrégation.
- **Passive** : Le switch **attend** qu'un autre équipement lance la négociation.

3 Mode statique (On)

Aucune négociation n'est effectuée, l'agrégation est configurée manuellement sur les deux équipements.

Modes de fonctionnement PAgP

S1 Mode	S2 Mode	Négociation	Agrégation
Auto	Auto	✗ Non	✗ Pas d'agrégation
Auto	Desirable	✓ Oui	✓ Agrégation
Desirable	Auto	✓ Oui	✓ Agrégation
Desirable	Desirable	✓ Oui	✓ Agrégation

Modes de fonctionnement LACP

S1 Mode	S2 Mode	Négociation	Agrégation
Passive	Passive	✗ Non	✗ Pas d'agrégation
Passive	Active	✓ Oui	✓ Agrégation
Active	Passive	✓ Oui	✓ Agrégation
Active	Active	✓ Oui	✓ Agrégation

PRATIQUE :



Configuration d'EtherChannel sur Switch 1

```
Switch> enable
Switch# configure terminal

Switch(config)# interface range fastEthernet 0/1-4
Switch(config-if-range)# channel-group 1 mode auto
Switch(config)# exit

Switch(config)# interface port-channel 1

Switch(config-if)# switchport mode trunk
```

Pour Afficher les informations du Spanning Tree Protocol (STP)

```
Switch# show spanning-tree
```

Pour Afficher et configurer l'équilibrage de charge d'EtherChannel

```
Switch# show etherchannel load-balance
Switch(config)# port-channel load-balance dst-mac
```

Configuration d'EtherChannel sur Switch 2

```
Switch> enable
Switch# configure terminal

Switch(config)# interface range fastEthernet 0/1-4
Switch(config-if-range)# channel-group 1 mode desirabl
Switch(config)# exit

Switch(config)# interface port-channel 1

Switch(config-if)# switchport mode trunk
```

partie 8 : VTP (VLAN Trunking Protocol)

1 - Qu'est-ce que le VTP ?

Le **VTP** est un protocole développé par **Cisco** pour gérer les **VLANs** dans les réseaux utilisant des **switches**.

2 - Modes de VTP et leurs différences

Mode VTP	Serveur (par défaut)	Client	Transparent (local)
Création des VLANs	<input checked="" type="checkbox"/> Oui	<input type="checkbox"/> Non	<input checked="" type="checkbox"/> Oui (localemement)
Suppression des VLANs	<input checked="" type="checkbox"/> Oui	<input type="checkbox"/> Non	<input checked="" type="checkbox"/> Oui (localemement)
Modification des VLANs	<input checked="" type="checkbox"/> Oui	<input type="checkbox"/> Non	<input checked="" type="checkbox"/> Oui (localemement)
Envoi des VLANs	<input checked="" type="checkbox"/> Oui	<input type="checkbox"/> Non (un cas)	<input type="checkbox"/> Non
Synchronisation des VLANs	<input checked="" type="checkbox"/> Oui	<input type="checkbox"/> Non	<input type="checkbox"/> Non
Transmission des VLANs	<input checked="" type="checkbox"/> Oui	<input checked="" type="checkbox"/> Oui	<input checked="" type="checkbox"/> Oui

3 - Configuration du VTP et gestion du numéro de révision

1. Changer le nom du domaine VTP

Utilisez la commande suivante pour modifier le nom du domaine VTP :

```
Switch(config)# vtp domain CISCO  
Changing VTP domain name from NULL to CISCO
```

2. Changer le mode VTP

Afficher les options disponibles pour le mode VTP :

```
Switch(config)# vtp mode ?  
client    Set the device to client mode.  
server    Set the device to server mode.  
transparent Set the device to transparent mode.
```

1 - Passer en mode server:

```
Switch(config)# vtp mode server
```

2 - Passer en mode Transparent :

```
Switch(config)# vtp mode transparent
```

3 - Passer ensuite en mode Client :

```
Switch> enable  
Switch# configure terminal  
Switch(config)# vtp mode client
```

3 - Vérifier les VLANs autorisés sur un trunk

```
show interfaces trunk
```

Remarque :

Les switches doivent être dans le **même domaine réseau** et la liaison entre eux doit être en **mode trunk** pour permettre le passage des données entre plusieurs VLANs.

partie 9 : Configuration de la redistribution entre RIP et OSPF

exercice :

Pour permettre la communication entre les deux réseaux (**RIP** et **OSPF**), il faut configurer la **redistribution des routes** sur le routeur intermédiaire (**R2**). Voici la configuration requise :



Configuration de la redistribution entre RIP et OSPF sur R2

1. Accéder au routeur R2 :

```
Router> enable  
Router# configure terminal  
Router(config)#
```

2. Activer la redistribution entre les protocoles :

- Redistribuer RIP vers OSPF :

```
Router(config)# router ospf 1  
Router(config-router)# redistribute rip subnets  
Router(config-router)# exit
```

- Redistribuer OSPF vers RIP :

```
Router(config)# router rip  
Router(config-router)# redistribute ospf 1 metric 5  
Router(config-router)# exit
```

partie 9 : Configuration du DHCP (DHCP serveur & DHCP routeur)

Le DHCP (Dynamic Host Configuration Protocol) attribue automatiquement des adresses IP aux dispositifs sur un réseau local. Il utilise le port 67 pour le

serveur et le port 68 pour les clients.

Types d'adresses IP :

1. **STATIQUE** – Adresse IP attribuée manuellement.
2. **DHCP** – Adresse IP attribuée automatiquement par un serveur DHCP.
3. **ALTERNATE** – Adresse alternative utilisée en cas d'absence de DHCP.
4. **APIPA** – Adresse IP automatique en cas d'échec du DHCP (plage 169.254.x.x).

Processus d'attribution d'une adresse IP via DHCP (Processus DORA) :

1. **DHCP DISCOVER** – L'appareil envoie une requête pour trouver un serveur DHCP.
2. **DHCP OFFER** – Le serveur répond avec une offre d'adresse IP disponible.
3. **DHCP REQUEST** – L'appareil demande la confirmation de l'adresse proposée.
4. **DHCP ACK** – Le serveur valide la demande et attribue l'adresse IP.

Que se passe-t-il en l'absence d'un serveur DHCP ?

- Si aucun serveur DHCP n'est disponible, l'appareil obtient une adresse APIPA (169.254.x.x), ce qui empêche la connexion correcte au réseau.

1 Configuration du DHCP sur un serveur

◆ Étapes :

1. Ajouter un serveur DHCP depuis **End Devices**.
2. Aller dans **Services → DHCP** et activer le service.
3. Créer un **nouveau pool DHCP** en spécifiant :
 - **Passerelle par défaut (Gateway)** : **192.168.1.1**
 - **Serveur DNS** : **8.8.8.8**
 - **Plage d'adresses** : **192.168.1.100 – 192.168.1.200**
 - **Masque de sous-réseau** : **255.255.255.0**

- Nombre maximum d'utilisateurs : 50

4. Cliquer sur "Add" pour enregistrer la configuration.

2 Configuration du DHCP sur un routeur

◆ Étapes :

1. Accéder au mode de configuration via l'interface CLI du routeur :

```
enable  
configure terminal
```

2. Créer un pool DHCP et définir les paramètres :

```
ip dhcp pool MON_POOL  
network 192.168.1.0 255.255.255.0  
default-router 192.168.1.1  
dns-server 8.8.8.8  
lease 86400
```

3. Exclure certaines adresses IP réservées (ex: pour les équipements critiques) :

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
```

4. Configurer l'interface du réseau local :

```
interface GigabitEthernet0/0  
ip address 192.168.1.1 255.255.255.0  
no shutdown  
exit
```

5. Si le serveur DHCP est externe, activer le relais DHCP :

```
ip helper-address 192.168.1.2 # Adresse IP du serveur DHCP
```

3 Vérifications et tests

- Sur le **serveur DHCP** : vérifier les adresses attribuées dans **Services → DHCP**.
- Sur le **routeur** :

```
show ip dhcp binding
```

- Sur un **PC client** : tester la connectivité avec la commande :

```
ping 192.168.1.1
```

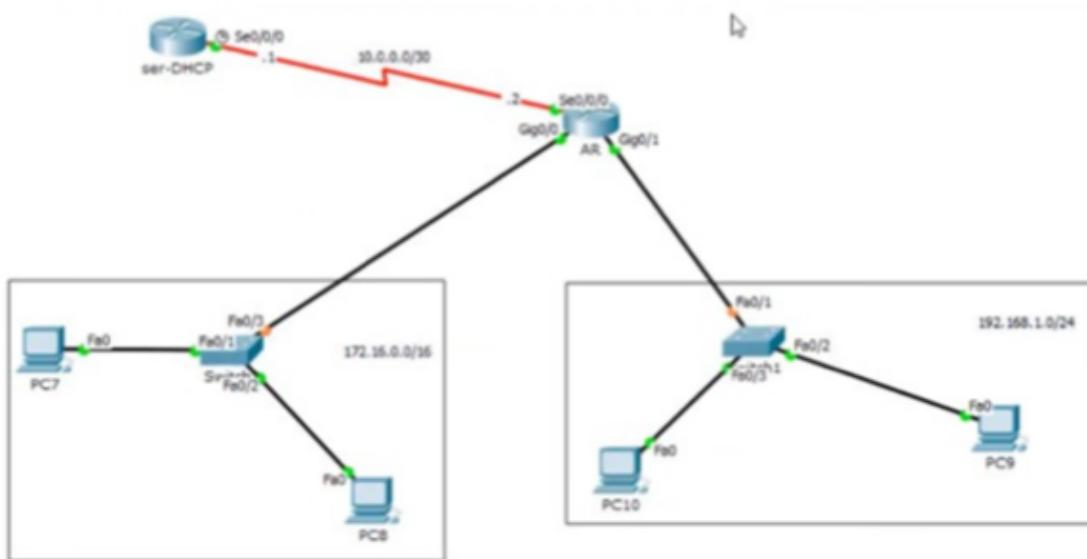
Commandes pour gérer le DHCP via l'invite de commande (CMD) :

- Pour renouveler l'adresse IP :

```
ipconfig /renew
```

- Pour libérer l'adresse IP :

```
ipconfig /release
```



Pour permettre aux ordinateurs connectés au routeur **AR** d'obtenir des adresses IP à partir du routeur **SER DHCP**, il faut configurer **AR** comme un **Relais DHCP (DHCP Relay)**. Cela se fait en utilisant la commande suivante sur

AR (si c'est un routeur prenant en charge le **DHCP Relay**, comme les routeurs Cisco) :

Commande pour activer le relais DHCP sur le routeur AR :

```
ip helper-address [adresse_IP_DE ROUTER SER-DHCP ]
```

partie 10 : les ACL "Access Control List"

1. ACL dans les Réseaux

les ACL sont des listes de règles appliquées aux **routeurs, pare-feu (firewall) et switches** pour autoriser ou bloquer le trafic .

Types d'ACL :

1- ACL standard (Numéros : 1-99 et 1300-1999)

- Filtrage basé uniquement sur l'adresse **IP source**.
- Exemple : Bloquer tout trafic venant de **192.168.1.10**

Voici les commandes en mode **Configuration** sur un routeur Cisco :

```
Router> enable  
Router# configure terminal  
Router(config)# access-list 10 deny 192.168.1.10  
Router(config)# access-list 10 permit any
```

Si vous souhaitez appliquer la liste d'accès **access-list 10** à une interface spécifique, par exemple **FastEthernet 0/0** :

```
Router# configure terminal  
Router(config)# interface FastEthernet 0/0  
Router(config-if)# ip access-group 10 in  
Router(config-if)# exit
```

Explication des commandes :

- `access-list 10 deny 192.168.1.10` → Bloque l'adresse `192.168.1.10`.
- `access-list 10 permit any` → Autorise tout le reste du trafic.
- `ip access-group 10 in` → Applique la liste d'accès à l'interface pour le trafic entrant.

2- ACL étendue (Numéros : 100-199 et 2000-2699)

- Filtrage basé sur **IP source et destination, protocole, port, etc.**
- Exemple : Autoriser uniquement le trafic HTTP depuis `192.168.1.0/24` vers `10.0.0.1`

```
access-list 100 permit tcp 192.168.1.0 0.0.0.255 host 10.0.0.1 eq 80
```

3- ACL nommées

- Permettent une gestion plus lisible en utilisant des **noms** au lieu de numéros.
- Exemple :

```
ip access-list extended WebAccess  
permit tcp 192.168.1.0 0.0.0.255 any eq 80  
deny ip any any
```

📌 Liste des Protocoles Utilisant TCP et UDP

Protocole	Description	Port Courant	TCP ou UDP ?
HTTP	Navigation Web non sécurisée	80	TCP
HTTPS	Navigation Web sécurisée	443	TCP
FTP	Transfert de fichiers	21 (Contrôle) / 20 (Données)	TCP

Protocole	Description	Port Courant	TCP ou UDP ?
SSH	Accès sécurisé à distance	22	TCP
Telnet	Accès à distance non sécurisé	23	TCP
SMTP	Envoi d'e-mails	25	TCP
POP3	Réception d'e-mails	110	TCP
POP3S	Réception d'e-mails sécurisée	995	TCP
DNS	Service de résolution des noms de domaine	53	UDP (Requêtes) / TCP (Transfert de zone)
DHCP	Attribution automatique des adresses IP	67 (Serveur) / 68 (Client)	UDP
RIP	Protocole de routage dynamique	520	UDP

Création de listes de contrôle d'accès étendues

Exemples :

1. Autorisation de connexion spécifique

```
access-list 101 permit ip host 192.168.1.1 193.1.1.0 0.0.0.255
```

- Cette règle permet à la machine **192.168.1.1** de se connecter au réseau **193.1.1.0** en utilisant le protocole IP.

2. Interdiction de Telnet (TCP 23) vers une machine spécifique

```
access-list 102 deny tcp any host 10.1.1.1 eq 23
```

- Bloque toute tentative de connexion **Telnet (TCP 23)** vers la machine **10.1.1.1**.

3. Interdiction des connexions TCP sur des ports supérieurs à 1023

```
access-list 102 deny tcp 1.0.0.0 0.255.255.255 44.1.x.x gt 1023
```

- Empêche les connexions **TCP** avec des ports **supérieurs à 1023** entre le réseau **1.0.0.0** et **44.1.x.x**.

4. Autorisation du trafic après les restrictions

```
access-list 102 permit ip any any
```

- Cette règle est essentielle pour **autoriser le reste du trafic**, sinon tout est bloqué par défaut à cause du **deny implicite**.

5. Interdiction du ping (ICMP echo) depuis un réseau spécifique

```
access-list 151 deny icmp 33.1.2.0 0.0.0.255 44.1.x.x echo
```

```
access-list 151 permit ip any any
```

- Bloque les requêtes **ping (ICMP echo)** du réseau **33.1.2.0** vers **44.1.x.x**, tout en permettant les autres types de trafic.

information :

Métrique : Valeur numérique utilisée par les protocoles de routage pour choisir le meilleur chemin (plus elle est petite, meilleure est la route).

Configuration des ACLs IPv6 Étendues (Extended)

Création d'une ACL Nommée

```
Router(config)# ipv6 access-list Nom_Acl
```

1. Si le Protocole est ICMP ou IPv6 :

```
{deny|permit} protocole ipv6-source/CIDR ipv6-destination/CIDR
```

- **deny** : Bloquer le trafic
- **permit** : Autoriser le trafic

2. Si le Protocole est UDP ou TCP :

```
{deny|permit} protocole ipv6-source/CIDR ipv6-destination/CIDR [{eq|neq|gt|lt|range} port]
```

- **eq** : Égal à un port spécifique
- **neq** : Différent d'un port spécifique
- **gt** : Supérieur à un port donné
- **lt** : Inférieur à un port donné
- **range** : Plage de ports

3. Pour une Adresse Hôte Unique :

```
{deny|permit} protocole host ipv6-source host ipv6-destination
```

- **host** : Identifier une adresse IP spécifique

4. Pour Toutes les Adresses :

```
{deny|permit} protocole any any
```

- **any** : Appliquer la règle à toutes les adresses IPv6

5. Activation d'une ACL sur une Interface :

```
Router(config)# interface type numéro
```

```
Router(config-if)# ipv6 traffic-filter Nom_Acl {in|out}
```

- **in** : Appliquer l'ACL pour le trafic entrant
- **out** : Appliquer l'ACL pour le trafic sortant

VLSM IPV6

Exemple d'adressage IPv6 - Subnetting

Adresse de Base

- 2001:DB8:CAFE:1::

Allocation des Sous-Réseaux et des Hôtes

Nombre d'Hôtes	Puissance de 2	Préfixe CIDR	Adresse Utilisée
120 Hôtes	$2^7 = 128$	/121	2001:DB8:CAFE:1::/121
60 Hôtes	$2^6 = 64$	/122	2001:DB8:CAFE:2::/122
20 Hôtes	$2^5 \approx 32$	/123	2001:DB8:CAFE:3::/123
2 Hôtes	$2^1 = 2$	/127	2001:DB8:CAFE:4::/127
2 Hôtes	$2^1 = 2$	/127	2001:DB8:CAFE:5::/127

Explication

- **N = Nombre de bits pour les hôtes**
- **128 - N = Longueur du préfixe CIDR**
- Plus le préfixe CIDR est grand, moins il y a d'adresses disponibles pour les hôtes.
- Ce type de segmentation est couramment utilisé pour maximiser l'utilisation des adresses IPv6 tout en optimisant l'adressage pour différents besoins réseau.

Questions et Réponses

1. Différence entre la Running Configuration et la Startup Configuration (2 Pts)

- **Running Configuration** : Il s'agit de la configuration en cours d'exécution dans la mémoire RAM du routeur. Toute modification y est appliquée immédiatement.
 - **Startup Configuration** : Il s'agit de la configuration sauvegardée dans la mémoire NVRAM. Elle est utilisée pour charger la configuration lors du redémarrage du routeur.
-

2. Avantages du Routage Dynamique (1 Pt)

- Adaptation automatique aux changements du réseau.
 - Moins d'intervention manuelle.
 - Calcul automatique des meilleurs chemins.
 - Évolutivité pour les grands réseaux.
-

3. Avantages du Routage Dynamique par Rapport au Routage Statique (1 Pt)

- Moins d'effort administratif.
 - Détection automatique des pannes et des modifications de topologie.
 - Convergence rapide après un changement réseau.
-

Avantages de l'Adressage IPv6

- **Grand Nombre d'Adresses IP** : Grâce à ses 128 bits, IPv6 offre un espace d'adressage énorme.
 - **Suppression du Broadcast** : IPv6 n'utilise pas de Broadcast, ce qui améliore les performances réseau.
 - **Correction des Erreurs** : Mécanismes intégrés pour détecter et corriger les erreurs.
 - **Auto-Configuration** : IPv6 prend en charge la configuration automatique des interfaces (SLAAC).
-

Adresses IPv6 - Caractéristiques

- **Longueur** : 128 bits (16 octets), offrant un espace d'adressage plus vaste qu'IPv4.

Types d'Adresses IPv6

1. Unicast :

- **Globale** : Utilisée pour l'accès à Internet (Commence par `2000::/3`).
- **Lien Local (Link-local)** : Utilisée pour la communication locale (Commence par `FE80::/10`).
- **Site Local** : Obsolète, remplacée par `FC00::/7`.

2. Multicast :

- Permet l'envoi de paquets à un groupe d'interfaces.

3. Anycast :

- Le paquet est envoyé à l'interface la plus proche appartenant à un groupe d'interfaces.

Traduction d'IPv4 vers IPv6

- **IPv4** : `192.168.1.3`
- **Conversion en Hexadécimal** :
 - 192 → C0
 - 168 → A8
 - 1 → 01
 - 3 → 03
- **Adresse IPv6** : `::C0A8-0103` ou `::C0A8:103`
- **Adresse IPv4 Mappée** : `::FFFF:192.168.1.3`

Types d'Adresses IPv6 - Récapitulatif

- `2000::/3` : Unicast routable sur Internet.
- `FC00::/7` : Locales uniques, non routables (équivalentes aux adresses privées IPv4).
- `FE80::/10` : Link-local, non routables (pour les communications locales).

- `::FFFF:a.b.c.d` : IPv4 mappée pour la compatibilité.
- `FF00::/8` : Multicast (comme `224.0.0.0` en IPv4).
- `::1/128` : Loopback/localhost (équivalent à `127.0.0.1` en IPv4).
- `::` : Adresse réservée (adresse nulle).

Exemples de Multicast

- `FF02::1` : Tous les équipements du sous-réseau.
- `FF02::2` : Tous les routeurs.

تابعوني على:

Instagram: [@aauam.net](#)

LinkedIn: [linkedin.com/in/Aauam_Net](#)