SRWE : Switching, Routing, and Wireless Essentials — Guide Complet

Guide complet du cours SRWE (Cisco CCNA) : configuration des réseaux commutés, VLANs, routage inter-VLAN, STP, EtherChannel, DHCPv4/v6, FHRP, sécurité LAN, WLAN, routage statique et dépannage. 16 chapitres avec travaux pratiques.

Réseau Systèmes 120 min de lecture Niveau Intermédiaire

Document généré le 25/05/2026 à 20h09 · nouvy.fr/wiki/srwe-switching-routing-wireless-essentials

Sommaire

117 section(s) · 120 min de lecture

Objectifs du cours

Table des matières

Chapitre 1 : Configuration de base des périphériques

↳ 1.1 Accès aux périphériques Cisco

↳ 1.2 Configuration de base d'un switch

↳ 1.3 Configuration de base d'un routeur

↳ 1.4 Vérification de la configuration

↳ 1.5 Configuration SVI (Switch Virtual Interface)

↳ □ TP Chapitre 1 : Configuration de base

Chapitre 2 : Principes de commutation

↳ 2.1 Fonctionnement d'un switch

↳ 2.2 Méthodes de commutation

↳ 2.3 Domaines de collision et de diffusion

↳ 2.4 Types de trames Ethernet

↳ 2.5 Auto-MDIX

↳ □ TP Chapitre 2 : Observation de la commutation

Chapitre 3 : VLANs

↳ 3.1 Concepts des VLANs

↳ 3.2 Création et gestion des VLANs

↳ 3.3 Assignation des ports aux VLANs (mode Access)

↳ 3.4 Configuration des Trunks (802.1Q)

↳ 3.5 Sécurisation des VLANs

↳ □ TP Chapitre 3 : Configuration des VLANs et Trunks

Chapitre 4 : Routage Inter-VLAN

↳ 4.1 Pourquoi le routage Inter-VLAN ?

↳ 4.2 Router-on-a-Stick

↳ 4.3 Routage Inter-VLAN avec Switch L3 (SVI)

↳ 4.4 Vérification du routage Inter-VLAN

↳ 4.5 Dépannage du routage Inter-VLAN

↳ □ TP Chapitre 4 : Routage Inter-VLAN

Chapitre 5 : STP (Spanning Tree Protocol)

↳ 5.1 Problème des boucles de commutation

↳ 5.2 Fonctionnement de STP (802.1D)

↳ 5.3 Versions de Spanning Tree

↳ 5.4 Configuration de STP

↳ 5.5 Vérification de STP

↳ □ TP Chapitre 5 : Configuration de STP

Chapitre 6 : EtherChannel

↳ 6.1 Concepts d'EtherChannel

↳ 6.2 Protocoles de négociation

↳ 6.3 Configuration d'EtherChannel

↳ 6.4 Vérification et dépannage d'EtherChannel

↳ □ TP Chapitre 6 : Configuration d'EtherChannel

Chapitre 7 : DHCPv4

↳ 7.1 Fonctionnement de DHCPv4

↳ 7.2 Configuration d'un serveur DHCPv4 sur un routeur

↳ 7.3 DHCP Relay Agent

↳ 7.4 Configuration du client DHCP sur un routeur

↳ 7.5 Vérification et dépannage DHCPv4

↳ □ TP Chapitre 7 : Configuration DHCPv4

Chapitre 8 : Concepts SLAAC et DHCPv6

↳ 8.1 Attribution d'adresses IPv6

↳ 8.2 SLAAC (Stateless Address Auto-Configuration)

↳ 8.3 Configuration SLAAC sur le routeur

↳ 8.4 DHCPv6 Stateless

↳ 8.5 DHCPv6 Stateful

↳ 8.6 DHCPv6 Relay Agent

↳ 8.7 Vérification DHCPv6

↳ □ TP Chapitre 8 : Configuration SLAAC et DHCPv6

Chapitre 9 : Principes FHRP (First Hop Redundancy Protocols)

↳ 9.1 Problème de la passerelle unique

↳ 9.2 Protocoles FHRP
↳ 9.3 HSRP (Hot Standby Router Protocol)
↳ 9.4 HSRP pour IPv6
↳ 9.5 Vérification FHRP
↳ TP Chapitre 9 : Configuration HSRP

Chapitre 10 : Principes de sécurité LAN

↳ 10.1 Menaces sur les réseaux locaux
↳ 10.2 Attaque MAC Flooding
↳ 10.3 Attaques DHCP
↳ 10.4 Attaque ARP Spoofing
↳ 10.5 Attaque VLAN Hopping
↳ 10.6 Attaque STP
↳ TP Chapitre 10 : Identification des menaces LAN

Chapitre 11 : Configuration de la sécurité des commutateurs

↳ 11.1 Port Security
↳ 11.2 DHCP Snooping — Configuration complète
↳ 11.3 Dynamic ARP Inspection (DAI) — Configuration complète
↳ 11.4 IP Source Guard
↳ 11.5 Protection contre les attaques CDP/LLDP
↳ 11.6 Récapitulatif des protections
↳ TP Chapitre 11 : Sécurisation d'un switch

Chapitre 12 : Principes WLAN

↳ 12.1 Fondamentaux du Wi-Fi
↳ 12.2 Composants WLAN
↳ 12.3 Topologies WLAN
↳ 12.4 Processus de connexion Wi-Fi
↳ 12.5 Sécurité WLAN
↳ 12.6 Architecture WLAN d'entreprise
↳ 12.7 Menaces WLAN
↳ TP Chapitre 12 : Analyse des réseaux WLAN

Chapitre 13 : Configuration WLAN

↳ 13.1 Configuration d'un AP autonome (routeur Wi-Fi Cisco)

↳ 13.2 Configuration d'un WLC (Wireless LAN Controller)
↳ 13.3 Configuration WPA2-Enterprise avec RADIUS
↳ 13.4 Configuration du routeur Wi-Fi domestique (interface GUI)
↳ 13.5 Bonnes pratiques de sécurité WLAN
↳ TP Chapitre 13 : Configuration WLAN

Chapitre 14 : Principes de routage

↳ 14.1 Fonctionnement d'un routeur
↳ 14.2 La table de routage
↳ 14.3 Décision de routage
↳ 14.4 Routage IPv4 vs IPv6
↳ 14.5 Routage statique vs dynamique
↳ TP Chapitre 14 : Exploration de la table de routage

Chapitre 15 : Routage IP statique

↳ 15.1 Types de routes statiques
↳ 15.2 Configuration des routes statiques IPv4
↳ 15.3 Route par défaut
↳ 15.4 Route statique flottante
↳ 15.5 Routes statiques IPv6
↳ 15.6 Routes statiques résumées
↳ 15.7 Vérification des routes statiques
↳ TP Chapitre 15 : Configuration du routage statique

Chapitre 16 : Dépannage des routes statiques et par défaut

↳ 16.1 Méthodologie de dépannage
↳ 16.2 Problèmes courants et solutions

Objectifs du cours

À l'issue de ce guide, vous serez capable de :

- **Configurer et dépanner** les réseaux commutés (switches, VLANs, trunks)
- **Mettre en œuvre** des protocoles de routage inter-VLAN et statique
- **Renforcer la sécurité** des réseaux locaux (port security, DHCP snooping, DAI)
- **Configurer les protocoles** STP, EtherChannel, DHCP, FHRP
- **Déployer et sécuriser** des réseaux sans fil (WLAN)
- **Dépanner** les routes statiques et par défaut

Table des matières

Chapitre	Titre	Thème
1	Configuration de base des périphériques	Fondamentaux
2	Principes de commutation	Switching
3	VLANs	Switching
4	Routage Inter-VLAN	Routing
5	STP (Spanning Tree Protocol)	Switching
6	EtherChannel	Switching
7	DHCPv4	Services
8	Concepts SLAAC et DHCPv6	Services IPv6
9	Principes FHRP	Redondance
10	Principes de sécurité LAN	Sécurité
11	Configuration de la sécurité des commutateurs	Sécurité
12	Principes WLAN	Sans fil
13	Configuration WLAN	Sans fil
14	Principes de routage	Routing
15	Routage IP statique	Routing
16	Dépannage des routes statiques et par défaut	Dépannage

Chapitre 1 : Configuration de base des périphériques

1.1 Accès aux périphériques Cisco

Modes d'accès

Mode	Invite	Accès
Utilisateur	`Switch>`	Commandes de base, monitoring
Privilégié	`Switch#`	Toutes les commandes show
Configuration globale	`Switch(config)#`	Configuration du périphérique
Configuration d'interface	`Switch(config-if)#`	Configuration d'une interface
Configuration de ligne	`Switch(config-line)#`	Configuration console/VTY

Navigation entre les modes

```
Switch> enable
Switch# configure terminal
Switch(config)# interface fastEthernet 0/1
Switch(config-if)# exit
Switch(config)# line console 0
Switch(config-line)# end
Switch#
```

Copier

1.2 Configuration de base d'un switch

Nom d'hôte et bannière

```
Switch(config)# hostname S1
S1(config)# banner motd #Accès autorisé uniquement. Toute intrusion sera poursuivie.#
```

Copier

Sécurisation des accès

```
! Mot de passe enable (chiffré)
S1(config)# enable secret Class123

! Sécuriser la console
S1(config)# line console 0
S1(config-line)# password Cisco123
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exec-timeout 5 0

! Sécuriser les lignes VTY (accès SSH/Telnet)
S1(config)# line vty 0 15
S1(config-line)# password Cisco123
S1(config-line)# login local
S1(config-line)# transport input ssh

! Chiffrer tous les mots de passe en clair
S1(config)# service password-encryption

! Créer un utilisateur local
S1(config)# username admin privilege 15 secret Admin123
```

Copier

Configuration SSH

```
S1(config)# ip domain-name example.com
S1(config)# crypto key generate rsa general-keys modulus 2048
S1(config)# ip ssh version 2
S1(config)# ip ssh time-out 60
S1(config)# ip ssh authentication-retries 3
```

Copier

1.3 Configuration de base d'un routeur

Configuration des interfaces du routeur

```
Router(config)# hostname R1

! Interface GigabitEthernet vers le LAN
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# description Lien vers LAN
R1(config-if)# no shutdown

! Interface série vers le WAN
R1(config)# interface Serial 0/1/0
R1(config-if)# ip address 10.0.0.1 255.255.255.252
R1(config-if)# clock rate 128000
R1(config-if)# no shutdown

! Interface Loopback (pour tests)
R1(config)# interface Loopback 0
R1(config-if)# ip address 1.1.1.1 255.255.255.255
```

Copier

1.4 Vérification de la configuration

```
! Afficher la configuration en cours
S1# show running-config

! Afficher la configuration de démarrage
S1# show startup-config

! Afficher les interfaces et leur état
S1# show ip interface brief
S1# show ipv6 interface brief

! Sauvegarder la configuration
S1# copy running-config startup-config
S1# write memory
```

Copier

1.5 Configuration SVI (Switch Virtual Interface)

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shutdown
S1(config)# ip default-gateway 192.168.1.1
```

Copier

□ TP Chapitre 1 : Configuration de base

Objectif : Configurer un switch et un routeur avec les paramètres de base.

Topologie :

```
[PC1] --- [S1] --- [R1] --- [S2] --- [PC2]
```

Copier

Étapes :

1. Configurer les noms d'hôte sur S1, S2 et R1
2. Sécuriser les accès console, VTY et enable
3. Configurer SSH sur tous les périphériques
4. Configurer les interfaces du routeur R1
5. Configurer les SVI sur S1 et S2
6. Vérifier la connectivité de bout en bout avec `ping`

Vérification :

```
S1# show ip interface brief
R1# show ip interface brief
PC1> ping 192.168.2.10
```

Copier

Chapitre 2 : Principes de commutation

2.1 Fonctionnement d'un switch

Table d'adresses MAC (table CAM)

Le switch apprend les adresses MAC source des trames reçues et les associe au port d'entrée.

Étape	Action
1	Le switch reçoit une trame sur un port
2	Il enregistre l'adresse MAC source + numéro de port dans la table MAC
3	Il vérifie l'adresse MAC destination dans sa table
4a	**Si trouvée** → Forwarding vers le port correspondant
4b	**Si inconnue** → Flooding vers tous les ports (sauf celui de réception)

Afficher la table MAC

```
S1# show mac address-table
S1# show mac address-table dynamic
S1# show mac address-table address 00A1.B2C3.D4E5
S1# clear mac address-table dynamic
```

Copier

2.2 Méthodes de commutation

Méthode	Description	Latence	Vérification CRC
Store-and-Forward	Reçoit toute la trame avant de la transmettre	Élevée	□ Oui
Cut-Through	Transmet dès que l'adresse MAC dest. est lue	Faible	□ Non
Fragment-Free	Lit les 64 premiers octets avant de transmettre	Moyenne	Partielle

> ***Note** : Les switches Cisco Catalyst utilisent par défaut le mode **Store-and-Forward**.*

2.3 Domaines de collision et de diffusion

Concept	Description	Séparé par
Domaine de collision	Zone où les trames peuvent entrer en collision	Switch (chaque port = 1 domaine)
Domaine de diffusion	Zone atteinte par une trame broadcast	Routeur ou VLAN

Fonctionnement en Full-Duplex

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# duplex full
S1(config-if)# speed 100
```

Copier

> *En **full-duplex**, il n'y a pas de collision. Chaque direction (envoi/réception) a son propre canal.*

2.4 Types de trames Ethernet

Type	Adresse MAC Destination	Description
Unicast	Adresse MAC spécifique	Trame pour un seul destinataire
Broadcast	FF:FF:FF:FF:FF:FF	Trame pour tous les hôtes du réseau
Multicast	01:00:5E:xx:xx:xx	Trame pour un groupe d'hôtes

2.5 Auto-MDIX

La fonctionnalité **Auto-MDIX** détecte automatiquement le type de câble (droit ou croisé) et ajuste la connexion.

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# mdix auto
```

Copier

TP Chapitre 2 : Observation de la commutation

Objectif : Observer le comportement du switch et sa table MAC.

Étapes :

1. Connecter 3 PCs au switch S1
2. Effacer la table MAC : `clear mac address-table dynamic`
3. Depuis PC1, effectuer un `ping` vers PC2
4. Afficher la table MAC : `show mac address-table dynamic`
5. Observer les entrées apprises dynamiquement
6. Envoyer un broadcast depuis PC1 et observer le comportement

---

Chapitre 3 : VLANs

3.1 Concepts des VLANs

Un **VLAN (Virtual Local Area Network)** est un réseau logique qui segmente un réseau physique en plusieurs domaines de diffusion distincts.

Avantages des VLANs

Avantage	Description
Sécurité	Isolation du trafic entre les groupes
Performance	Réduction des domaines de diffusion
Flexibilité	Regroupement logique indépendant de la localisation physique
Gestion	Administration simplifiée des réseaux
Coût	Moins besoin de routeurs pour segmenter

Types de VLANs

Type	Description	Exemple
VLAN de données	Transporte le trafic utilisateur	VLAN 10 (Ventes)
VLAN voix	Optimisé pour le trafic VoIP (QoS)	VLAN 150
VLAN de gestion	Accès à la gestion du switch (SSH/Telnet)	VLAN 99
VLAN natif	VLAN pour les trames non taguées sur le trunk	VLAN 99
VLAN par défaut	VLAN 1 — tous les ports y sont assignés par défaut	VLAN 1

> ⚠ ***Bonne pratique*** *: Ne jamais utiliser le VLAN 1 en production. Créer un VLAN de gestion dédié.*

3.2 Création et gestion des VLANs

Créer des VLANs

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

S1(config)# vlan 20
S1(config-vlan)# name Ingenierie
S1(config-vlan)# exit

S1(config)# vlan 30
S1(config-vlan)# name Direction
S1(config-vlan)# exit

S1(config)# vlan 99
S1(config-vlan)# name Gestion
S1(config-vlan)# exit

S1(config)# vlan 150
S1(config-vlan)# name VoIP
S1(config-vlan)# exit
```

Copier

Vérification des VLANs

```
S1# show vlan brief

VLAN Name                   Status    Ports
---- ---------------------- --------- -------------------------------
1    default                active    Fa0/1, Fa0/2, ... (tous par défaut)
10   Ventes                 active
20   Ingenierie             active
30   Direction              active
99   Gestion                active
150  VoIP                   active
```

Copier

3.3 Assignation des ports aux VLANs (mode Access)

```
! Assigner un port au VLAN 10
S1(config)# interface FastEthernet 0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10

! Assigner une plage de ports
S1(config)# interface range FastEthernet 0/1-10
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 10

! Configurer un port voix
S1(config)# interface FastEthernet 0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# switchport voice vlan 150
```

Copier

3.4 Configuration des Trunks (802.1Q)

Un **trunk** transporte le trafic de plusieurs VLANs entre les switches en ajoutant un tag 802.1Q à chaque trame.

Structure d'une trame 802.1Q

```
+----------+----------+------+------+---------+-----+
| Dest MAC | Src MAC  | TPID | TCI  | Type/Len| Data|
+----------+----------+------+------+---------+-----+
                       |    Tag 802.1Q    |
                       | TPID = 0x8100    |
                       | PRI (3 bits)     |
                       | CFI (1 bit)      |
                       | VLAN ID (12 bits)|
```

Copier

Configurer un trunk

```
! Configurer un port en mode trunk
S1(config)# interface GigabitEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99,150

! Vérifier la configuration du trunk
S1# show interfaces trunk
S1# show interfaces GigabitEthernet 0/1 switchport
```

Copier

Négociation DTP (Dynamic Trunking Protocol)

Mode du port	Description
`switchport mode trunk`	Force le mode trunk
`switchport mode access`	Force le mode access
`switchport mode dynamic auto`	Devient trunk si l'autre côté le demande
`switchport mode dynamic desirable`	Tente de négocier un trunk
`switchport nonegotiate`	Désactive DTP

> ⚠ ***Bonne pratique*** *: Toujours désactiver DTP et forcer le mode trunk ou access.*

```
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

Copier

3.5 Sécurisation des VLANs

```
! Désactiver les ports non utilisés
S1(config)# interface range FastEthernet 0/20-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown

! Créer un VLAN "trou noir" pour les ports inutilisés
S1(config)# vlan 999
S1(config-vlan)# name TrouNoir
```

Copier

TP Chapitre 3 : Configuration des VLANs et Trunks

Objectif : Créer des VLANs, assigner des ports et configurer des trunks.

Topologie :

```
[PC1 VLAN10] --Fa0/1-- [S1] --Gi0/1(trunk)-- [S2] --Fa0/1-- [PC3 VLAN10]
[PC2 VLAN20] --Fa0/2-- [S1]                   [S2] --Fa0/2-- [PC4 VLAN20]
```

Copier

Plan d'adressage :

Périphérique	VLAN	Adresse IP	Masque
PC1	VLAN 10	192.168.10.10	255.255.255.0
PC2	VLAN 20	192.168.20.10	255.255.255.0
PC3	VLAN 10	192.168.10.20	255.255.255.0
PC4	VLAN 20	192.168.20.20	255.255.255.0

Étapes :

1. Créer les VLANs 10, 20 et 99 sur S1 et S2
2. Assigner les ports aux VLANs correspondants
3. Configurer le trunk entre S1 et S2
4. Vérifier : PC1 peut pinger PC3 (même VLAN)
5. Vérifier : PC1 ne peut **pas** pinger PC2 (VLAN différent)
6. Afficher `show vlan brief` et `show interfaces trunk`

Chapitre 4 : Routage Inter-VLAN

4.1 Pourquoi le routage Inter-VLAN ?

Les VLANs créent des domaines de diffusion séparés. Pour que les hôtes de VLANs différents communiquent, un **routeur** ou un **switch L3** est nécessaire.

Méthodes de routage Inter-VLAN

Méthode	Description	Avantages	Inconvénients
Legacy	1 interface physique par VLAN	Simple	Coûteux, non scalable
Router-on-a-Stick	Sous-interfaces sur 1 interface physique	Économique	Goulot d'étranglement
Switch L3 (SVI)	Routage directement sur le switch	Performant, scalable	Switch plus coûteux

4.2 Router-on-a-Stick

Le routeur utilise une seule interface physique divisée en **sous-interfaces**, chacune associée à un VLAN.

Configuration du trunk sur le switch

```
S1(config)# interface GigabitEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# no shutdown
```

Copier

Configuration des sous-interfaces sur le routeur

```
R1(config)# interface GigabitEthernet 0/0/1
R1(config-if)# no shutdown

! Sous-interface pour VLAN 10
R1(config)# interface GigabitEthernet 0/0/1.10
R1(config-subif)# description Passerelle VLAN 10 - Ventes
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip address 192.168.10.1 255.255.255.0

! Sous-interface pour VLAN 20
R1(config)# interface GigabitEthernet 0/0/1.20
R1(config-subif)# description Passerelle VLAN 20 - Ingenierie
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip address 192.168.20.1 255.255.255.0

! Sous-interface pour VLAN 30
R1(config)# interface GigabitEthernet 0/0/1.30
R1(config-subif)# description Passerelle VLAN 30 - Direction
R1(config-subif)# encapsulation dot1Q 30
R1(config-subif)# ip address 192.168.30.1 255.255.255.0

! Sous-interface pour le VLAN natif
R1(config)# interface GigabitEthernet 0/0/1.99
R1(config-subif)# description Passerelle VLAN natif 99
R1(config-subif)# encapsulation dot1Q 99 native
R1(config-subif)# ip address 192.168.99.1 255.255.255.0
```

Copier

4.3 Routage Inter-VLAN avec Switch L3 (SVI)

Activer le routage IP sur le switch L3

```
MLS1(config)# ip routing

! Créer les VLANs
MLS1(config)# vlan 10
MLS1(config-vlan)# name Ventes
MLS1(config)# vlan 20
MLS1(config-vlan)# name Ingenierie

! Configurer les SVI
MLS1(config)# interface vlan 10
MLS1(config-if)# ip address 192.168.10.1 255.255.255.0
MLS1(config-if)# no shutdown

MLS1(config)# interface vlan 20
MLS1(config-if)# ip address 192.168.20.1 255.255.255.0
MLS1(config-if)# no shutdown

! Configurer un port routé (vers un routeur)
MLS1(config)# interface GigabitEthernet 0/1
MLS1(config-if)# no switchport
MLS1(config-if)# ip address 10.0.0.2 255.255.255.252
MLS1(config-if)# no shutdown
```

Copier

4.4 Vérification du routage Inter-VLAN

```
! Vérifier les sous-interfaces
R1# show ip interface brief
R1# show ip route
R1# show interfaces GigabitEthernet 0/0/1.10

! Vérifier les SVI sur un switch L3
MLS1# show ip interface brief
MLS1# show ip route
MLS1# show interfaces vlan 10

! Tests de connectivité
PC1-VLAN10> ping 192.168.20.10
PC1-VLAN10> tracert 192.168.20.10
```

Copier

4.5 Dépannage du routage Inter-VLAN

Problème	Vérification	Solution
Sous-interface down	`show ip interface brief`	`no shutdown` sur l'interface physique
Pas de connectivité inter-VLAN	`show ip route`	Vérifier encapsulation dot1Q
VLAN natif mismatch	`show interfaces trunk`	Même VLAN natif des deux côtés
Trunk non formé	`show interfaces trunk`	Vérifier mode trunk
Mauvais VLAN sur le port	`show vlan brief`	Réassigner le port au bon VLAN

🧪 TP Chapitre 4 : Routage Inter-VLAN

Objectif : Configurer le routage inter-VLAN avec Router-on-a-Stick et switch L3.

Topologie :

```
[PC1 VLAN10] --Fa0/1-- [S1] --Gi0/1(trunk)-- [R1] Gi0/0/1
[PC2 VLAN20] --Fa0/2-- [S1]
[PC3 VLAN30] --Fa0/3-- [S1]
```

Copier

Étapes :

1. Configurer les VLANs et le trunk sur S1
2. Configurer les sous-interfaces sur R1
3. Configurer les passerelles par défaut sur les PCs
4. Vérifier la communication inter-VLAN : PC1 → PC2 ✅
5. Utiliser `tracert` pour observer le passage par le routeur

Chapitre 5 : STP (Spanning Tree Protocol)

5.1 Problème des boucles de commutation

Sans STP, les réseaux avec des liens redondants créent des **boucles** qui provoquent :

Problème	Description
Tempête de broadcast	Les trames broadcast circulent indéfiniment
Instabilité de la table MAC	Le switch reçoit la même MAC sur différents ports
Trames en double	Les hôtes reçoivent plusieurs copies de la même trame

5.2 Fonctionnement de STP (802.1D)

STP élit un **Root Bridge** et place certains ports en état **Blocking** pour éliminer les boucles.

Élection du Root Bridge

Le switch avec le **Bridge ID (BID) le plus bas** devient le Root Bridge.

```
BID = Priorité (4 bits) + Extended System ID (VLAN ID) + Adresse MAC
     Par défaut : 32768 + VLAN ID + MAC
```

Copier

États des ports STP

État	Durée	Envoie BPDU	Apprend MAC	Transmet données
Blocking	20s (max age)	❌	❌	❌
Listening	15s (forward delay)	✅	❌	❌
Learning	15s (forward delay)	✅	✅	❌
Forwarding	-	✅	✅	✅
Disabled	-	❌	❌	❌

> ***Convergence STP 802.1D** : 30 à 50 secondes (Listening → Learning → Forwarding)*

Rôles des ports STP

Rôle	Description
Root Port	Port le plus proche du Root Bridge (1 par switch non-root)
Designated Port	Port qui transmet le trafic vers le segment (1 par segment)
Alternate Port	Port bloqué (sauvegarde du Root Port)
Backup Port	Port bloqué (sauvegarde du Designated Port)

5.3 Versions de Spanning Tree

Version	Standard	Convergence	Instances
STP	802.1D	30-50 sec	1 pour tous les VLANs
PVST+	Cisco	30-50 sec	1 par VLAN
RSTP	802.1w	1-2 sec	1 pour tous les VLANs
Rapid PVST+	Cisco	1-2 sec	1 par VLAN
MSTP	802.1s	1-2 sec	Groupes de VLANs

5.4 Configuration de STP

Changer le Root Bridge

```
! Méthode 1 : Définir la priorité manuellement
S1(config)# spanning-tree vlan 10 priority 24576

! Méthode 2 : Macro root primary / secondary
S1(config)# spanning-tree vlan 10 root primary
S2(config)# spanning-tree vlan 10 root secondary
```

Copier

> *La priorité doit être un multiple de **4096** : 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768*

Configurer Rapid PVST+

```
S1(config)# spanning-tree mode rapid-pvst
```

Copier

Configurer PortFast et BPDU Guard

```
! PortFast sur les ports d'accès (vers les hôtes)
S1(config)# interface FastEthernet 0/1
S1(config-if)# spanning-tree portfast
S1(config-if)# spanning-tree bpduguard enable

! Activer PortFast globalement sur tous les ports access
S1(config)# spanning-tree portfast default

! Activer BPDU Guard globalement
S1(config)# spanning-tree portfast bpduguard default
```

Copier

> ⚠ ***PortFast** : uniquement sur les ports connectés à des hôtes (PCs, serveurs, imprimantes). Jamais sur les ports connectés à d'autres switches.*

5.5 Vérification de STP

```
S1# show spanning-tree
S1# show spanning-tree vlan 10
S1# show spanning-tree summary
S1# show spanning-tree interface FastEthernet 0/1
S1# show spanning-tree root
```

Copier

🧪 TP Chapitre 5 : Configuration de STP

Objectif : Observer le fonctionnement de STP et manipuler l'élection du Root Bridge.

Topologie (triangle de switches) :

```
        [S1]
       /    \
   Gi0/1   Gi0/2
     /        \
  [S2]------[S3]
      Gi0/1
```

Copier

Étapes :

1. Connecter les 3 switches en triangle

2. Observer le Root Bridge élu : `show spanning-tree`
3. Identifier les ports Root, Designated et Blocked
4. Forcer S1 comme Root Bridge : `spanning-tree vlan 1 root primary`
5. Activer Rapid PVST+ sur tous les switches
6. Configurer PortFast et BPDU Guard sur les ports d'accès

Chapitre 6 : EtherChannel

6.1 Concepts d'EtherChannel

EtherChannel agrège plusieurs liens physiques en un seul lien logique, augmentant la bande passante et offrant de la redondance.

Avantages

Avantage	Description
Bande passante	Agrégation de 2 à 8 liens physiques
Redondance	Si un lien tombe, les autres continuent
STP	STP voit un seul lien logique → pas de blocage
Load Balancing	Répartition du trafic sur les liens

6.2 Protocoles de négociation

Protocole	Standard	Modes
PAgP (Port Aggregation Protocol)	Cisco propriétaire	`desirable` / `auto`
LACP (Link Aggregation Control Protocol)	IEEE 802.3ad	`active` / `passive`
Static	-	`on` / `on`

Compatibilité des modes

PAgP :

	desirable	**auto**
desirable	✅ EtherChannel	✅ EtherChannel
auto	✅ EtherChannel	❌ Pas de channel

LACP :

	active	**passive**
active	✅ EtherChannel	✅ EtherChannel
passive	✅ EtherChannel	❌ Pas de channel

6.3 Configuration d'EtherChannel

Avec LACP (recommandé)

```
! Sur S1
S1(config)# interface range GigabitEthernet 0/1-2
S1(config-if-range)# channel-group 1 mode active
S1(config-if-range)# exit

S1(config)# interface Port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99

! Sur S2
S2(config)# interface range GigabitEthernet 0/1-2
S2(config-if-range)# channel-group 1 mode passive
S2(config-if-range)# exit

S2(config)# interface Port-channel 1
S2(config-if)# switchport mode trunk
S2(config-if)# switchport trunk native vlan 99
S2(config-if)# switchport trunk allowed vlan 10,20,30,99
```

Copier

Avec PAgP

```
! Sur S1
S1(config)# interface range GigabitEthernet 0/1-2
S1(config-if-range)# channel-group 1 mode desirable

! Sur S2
S2(config)# interface range GigabitEthernet 0/1-2
S2(config-if-range)# channel-group 1 mode auto
```

Copier

EtherChannel L3 (entre switches L3)

```
MLS1(config)# interface range GigabitEthernet 0/1-2
MLS1(config-if-range)# no switchport
MLS1(config-if-range)# channel-group 1 mode active
MLS1(config-if-range)# exit

MLS1(config)# interface Port-channel 1
MLS1(config-if)# no switchport
MLS1(config-if)# ip address 10.0.0.1 255.255.255.252
```

Copier

6.4 Vérification et dépannage d'EtherChannel

```
! Vérifier l'état de l'EtherChannel
S1# show etherchannel summary
S1# show etherchannel port-channel
S1# show etherchannel detail

! Vérifier les interfaces membres
S1# show interfaces Port-channel 1
S1# show interfaces GigabitEthernet 0/1 etherchannel

! Méthode de load balancing
S1# show etherchannel load-balance
S1(config)# port-channel load-balance src-dst-mac
```

Copier

Résolution de problèmes courants

Problème	Cause	Solution
Channel non formé	Modes incompatibles	Vérifier active/passive ou desirable/auto
Channel en suspend	Paramètres différents	Même speed, duplex, VLAN, trunk sur tous les ports
Port en err-disabled	Mauvaise config	`shutdown` puis `no shutdown` après correction

> ⚠ ***Règle importante*** *: Tous les ports d'un EtherChannel doivent avoir* ***exactement*** *la même configuration (speed, duplex, mode trunk/access, VLANs autorisés).*

TP Chapitre 6 : Configuration d'EtherChannel

Objectif : Configurer un EtherChannel LACP entre deux switches.

Topologie :

```
[S1] ==Gi0/1==Gi0/2== [S2]
      (Port-channel 1)
```

Copier

Étapes :

1. Configurer LACP : S1 en `active`, S2 en `passive`
2. Configurer le Port-channel en trunk
3. Vérifier avec `show etherchannel summary` → flags SU (Layer2, In Use)
4. Débrancher un câble et vérifier que le trafic continue
5. Tester avec un EtherChannel PAgP sur un autre groupe de ports
6. Comparer les résultats des deux protocoles

Chapitre 7 : DHCPv4

7.1 Fonctionnement de DHCPv4

Le protocole **DHCP (Dynamic Host Configuration Protocol)** attribue automatiquement des adresses IP et d'autres paramètres réseau aux clients.

Processus DORA

Étape	Message	Direction	Description
1	**Discover**	Client → Broadcast	Le client cherche un serveur DHCP
2	**Offer**	Serveur → Broadcast/Unicast	Le serveur propose une adresse IP
3	**Request**	Client → Broadcast	Le client accepte l'offre
4	**Acknowledge**	Serveur → Broadcast/Unicast	Le serveur confirme l'attribution

Ports utilisés

Rôle	Port UDP
Serveur DHCP	**67**
Client DHCP	**68**

7.2 Configuration d'un serveur DHCPv4 sur un routeur

```
! Exclure les adresses statiques (passerelles, serveurs, etc.)
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)# ip dhcp excluded-address 192.168.10.254

! Créer le pool DHCP pour le VLAN 10
R1(config)# ip dhcp pool VLAN10-POOL
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 8.8.8.8 8.8.4.4
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# lease 7

! Créer le pool DHCP pour le VLAN 20
R1(config)# ip dhcp pool VLAN20-POOL
R1(dhcp-config)# network 192.168.20.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.20.1
R1(dhcp-config)# dns-server 8.8.8.8 8.8.4.4
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# lease 7
```

Copier

7.3 DHCP Relay Agent

Quand le serveur DHCP est sur un réseau différent des clients, le routeur doit relayer les messages DHCP broadcast.

```
! Sur l'interface du routeur côté client
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip helper-address 10.0.0.10
```

Copier

> *Le `ip helper-address` redirige les broadcasts DHCP (et autres services UDP) vers le serveur DHCP à l'adresse 10.0.0.10.*

Services relayés par ip helper-address

Service	Port UDP
DHCP/BOOTP	67, 68
TFTP	69
DNS	53
Time	37
NetBIOS	137, 138
TACACS	49

7.4 Configuration du client DHCP sur un routeur

```
! Configurer une interface comme client DHCP
R2(config)# interface GigabitEthernet 0/0/0
R2(config-if)# ip address dhcp
R2(config-if)# no shutdown
```

Copier

7.5 Vérification et dépannage DHCPv4

```
! Vérifier les pools DHCP
R1# show ip dhcp pool

! Voir les baux DHCP actifs
R1# show ip dhcp binding

! Voir les statistiques DHCP
R1# show ip dhcp server statistics

! Vérifier les conflits d'adresses
R1# show ip dhcp conflict

! Libérer un bail côté client (Windows)
C:\> ipconfig /release
C:\> ipconfig /renew
C:\> ipconfig /all

! Debug DHCP
R1# debug ip dhcp server events
```

Copier

Dépannage DHCP

Problème	Cause possible	Solution
Client n'obtient pas d'IP	Pas de pool configuré	Vérifier `show ip dhcp pool`
Adresse dans un mauvais réseau	Pool incorrect	Vérifier le network du pool
Client sur un autre réseau	Pas de relay agent	Configurer `ip helper-address`
Conflit d'adresses	Adresse déjà utilisée	Vérifier `ip dhcp excluded-address`

TP Chapitre 7 : Configuration DHCPv4

Objectif : Configurer un serveur DHCPv4 sur un routeur avec relay agent.

Topologie :

```
[PC1] --S1-- [R1] --WAN-- [R2] --S2-- [PC2]
          Gi0/0/0      Gi0/0/1
      192.168.10.0/24      192.168.20.0/24
```

Copier

Étapes :

1. Configurer le pool DHCP pour le réseau 192.168.10.0/24 sur R1
2. Configurer le pool DHCP pour le réseau 192.168.20.0/24 sur R1
3. Configurer `ip helper-address` sur R2 (vers R1)
4. Vérifier que PC1 obtient une IP automatiquement
5. Vérifier que PC2 obtient une IP via le relay
6. Consulter `show ip dhcp binding`

Chapitre 8 : Concepts SLAAC et DHCPv6

8.1 Attribution d'adresses IPv6

En IPv6, il existe trois méthodes d'attribution d'adresses :

Méthode	Description	Flag RA
SLAAC	Auto-configuration sans serveur	A=1, O=0, M=0
SLAAC + DHCPv6 Stateless	SLAAC pour l'IP + DHCPv6 pour DNS, etc.	A=1, O=1, M=0
DHCPv6 Stateful	Le serveur attribue toute la config	A=0, O=0, M=1

8.2 SLAAC (Stateless Address Auto-Configuration)

Le client génère son adresse IPv6 en combinant le **préfixe réseau** (reçu via Router Advertisement) et un **identifiant d'interface** (EUI-64 ou aléatoire).

Processus SLAAC

1. Le client envoie un **Router Solicitation (RS)** en multicast (FF02::2)
2. Le routeur répond avec un **Router Advertisement (RA)** contenant le préfixe
3. Le client construit son adresse : Préfixe + Interface ID

Méthodes de génération de l'Interface ID

Méthode	Description
EUI-64	Basé sur l'adresse MAC (avec insertion de FF:FE au milieu)
Aléatoire	Identifiant généré aléatoirement (vie privée)

Exemple EUI-64

```
MAC : 00:1A:2B:3C:4D:5E
  ↓ Inversion du 7ème bit
  ↓ Insertion de FF:FE au milieu
EUI-64 : 021A:2BFF:FE3C:4D5E

Adresse complète : 2001:DB8:ACAD:1::021A:2BFF:FE3C:4D5E/64
```

Copier

8.3 Configuration SLAAC sur le routeur

```
R1(config)# ipv6 unicast-routing

R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)# ipv6 address FE80::1 link-local
R1(config-if)# no shutdown
```

Copier

> *Avec `ipv6 unicast-routing`, le routeur envoie automatiquement des **RA** avec les flags par défaut (SLAAC pur).*

8.4 DHCPv6 Stateless

Le client utilise SLAAC pour l'adresse IP, mais obtient d'autres informations (DNS, domaine) via DHCPv6.

```
! Configuration du serveur DHCPv6 Stateless
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)# dns-server 2001:DB8:ACAD::CAFE
R1(config-dhcpv6)# domain-name example.com

R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
```

Copier

8.5 DHCPv6 Stateful

Le serveur DHCPv6 gère l'attribution complète des adresses.

```
! Configuration du serveur DHCPv6 Stateful
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)# address prefix 2001:DB8:ACAD:1::/64
R1(config-dhcpv6)# dns-server 2001:DB8:ACAD::CAFE
R1(config-dhcpv6)# domain-name example.com

R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# ipv6 nd prefix default no-autoconfig
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
```

Copier

8.6 DHCPv6 Relay Agent

```
R2(config)# interface GigabitEthernet 0/0/0
R2(config-if)# ipv6 dhcp relay destination 2001:DB8:ACAD:A::1
```

Copier

8.7 Vérification DHCPv6

```
R1# show ipv6 dhcp pool
R1# show ipv6 dhcp binding
R1# show ipv6 interface GigabitEthernet 0/0/0

! Côté client (Windows)
C:\> ipconfig /all
C:\> ipconfig /release6
C:\> ipconfig /renew6
```

Copier

TP Chapitre 8 : Configuration SLAAC et DHCPv6

Objectif : Configurer SLAAC, DHCPv6 Stateless et DHCPv6 Stateful.

Étapes :

1. Configurer SLAAC sur R1 et vérifier l'auto-configuration sur PC1
2. Ajouter DHCPv6 Stateless pour fournir le DNS
3. Convertir en DHCPv6 Stateful et vérifier les baux
4. Comparer les trois méthodes

Chapitre 9 : Principes FHRP (First Hop Redundancy Protocols)

9.1 Problème de la passerelle unique

Si la passerelle par défaut tombe en panne, tous les hôtes du réseau perdent l'accès aux réseaux distants, même si un chemin alternatif existe.

```
Situation sans FHRP :
[PC] → [R1 (passerelle)] ✖ → [Internet]
                              [R2 (backup)] ← inutilisé !

Situation avec FHRP :
[PC] → [IP virtuelle] → [R1 (actif)] → [Internet]
                      ↘ [R2 (standby)] → bascule automatique si R1 tombe
```

Copier

9.2 Protocoles FHRP

Protocole	Standard	Adresse IP virtuelle	Préemption
HSRP (Hot Standby Router Protocol)	Cisco	IP virtuelle partagée	Configurable
VRRP (Virtual Router Redundancy Protocol)	IEEE	IP virtuelle partagée	Par défaut
GLBP (Gateway Load Balancing Protocol)	Cisco	IP virtuelle + load balancing	Configurable

9.3 HSRP (Hot Standby Router Protocol)

États HSRP

État	Description
Initial	Le routeur vient de démarrer
Learn	Le routeur n'a pas encore reçu l'IP virtuelle
Listen	Le routeur connaît l'IP virtuelle, attend
Speak	Le routeur participe à l'élection
Standby	Le routeur est le backup
Active	Le routeur est le routeur actif (transmet le trafic)

Configuration HSRP

```
! Routeur R1 (Active - priorité haute)
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip address 192.168.10.2 255.255.255.0
R1(config-if)# standby version 2
R1(config-if)# standby 10 ip 192.168.10.1
R1(config-if)# standby 10 priority 110
R1(config-if)# standby 10 preempt
R1(config-if)# standby 10 timers 1 3

! Routeur R2 (Standby - priorité par défaut)
R2(config)# interface GigabitEthernet 0/0/0
R2(config-if)# ip address 192.168.10.3 255.255.255.0
R2(config-if)# standby version 2
R2(config-if)# standby 10 ip 192.168.10.1
R2(config-if)# standby 10 preempt
R2(config-if)# standby 10 timers 1 3
```

Copier

> *Les PCs utilisent **192.168.10.1** comme passerelle par défaut (adresse IP virtuelle HSRP).*

Paramètres HSRP

Paramètre	Valeur par défaut	Description
Priorité	100	Plus la valeur est haute, plus le routeur est prioritaire
Hello timer	3 secondes	Intervalle entre les messages Hello
Hold timer	10 secondes	Temps avant de déclarer le routeur actif down
Préemption	Désactivée	Permet au routeur prioritaire de reprendre le rôle actif

9.4 HSRP pour IPv6

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# standby version 2
R1(config-if)# standby 10 ipv6 autoconfig
R1(config-if)# standby 10 priority 110
R1(config-if)# standby 10 preempt
```

Copier

9.5 Vérification FHRP

```
R1# show standby
R1# show standby brief
R1# show standby GigabitEthernet 0/0/0

! Résultat attendu
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Gi0/0/0     10   110 P Active   local           192.168.10.3    192.168.10.1
```

Copier

🧪 TP Chapitre 9 : Configuration HSRP

Objectif : Configurer HSRP pour assurer la redondance de la passerelle.

Topologie :

```
            [Internet]
              |    |
           [R1]  [R2]
          .2  \  / .3
              [S1]
           .1 (VIP HSRP)
              |
            [PC1]
```

Copier

Étapes :

1. Configurer R1 comme routeur HSRP actif (priorité 110)
2. Configurer R2 comme routeur HSRP standby
3. Adresse IP virtuelle : 192.168.10.1
4. Vérifier avec `show standby brief`
5. Débrancher R1 → observer la bascule vers R2
6. Reconnecter R1 → observer la préemption

Chapitre 10 : Principes de sécurité LAN

10.1 Menaces sur les réseaux locaux

Menace	Description	Couche
MAC Flooding	Inondation de la table MAC du switch → le switch se comporte comme un hub	L2
DHCP Spoofing	Faux serveur DHCP fournissant de mauvaises configurations	L2-L3
DHCP Starvation	Épuisement de toutes les adresses DHCP disponibles	L2-L3
ARP Spoofing/Poisoning	Faux messages ARP pour intercepter le trafic (MITM)	L2-L3
VLAN Hopping	Accès non autorisé à un VLAN via double tagging	L2
STP Manipulation	Envoi de BPDU malveillants pour devenir Root Bridge	L2
CDP/LLDP Reconnaissance	Découverte d'informations sur les périphériques réseau	L2

10.2 Attaque MAC Flooding

Principe

L'attaquant envoie un grand nombre de trames avec des adresses MAC source aléatoires. La table CAM du switch se remplit et le switch commence à inonder le trafic sur tous les ports (comme un hub).

```
Outil d'attaque : macof (partie de dsniff)
$ macof -i eth0 -n 100000
```

Copier

Protection : Port Security (voir Chapitre 11)

10.3 Attaques DHCP

DHCP Starvation

L'attaquant épuise toutes les adresses IP du pool DHCP en envoyant de multiples requêtes DHCP Discover avec des adresses MAC différentes.

DHCP Spoofing

L'attaquant déploie un faux serveur DHCP qui répond aux clients avec :

- Une fausse passerelle par défaut (vers l'attaquant → MITM)
- Un faux serveur DNS (pour du phishing)

Protection : DHCP Snooping

```
! Activer DHCP Snooping globalement
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20,30

! Configurer le port vers le serveur DHCP légitime comme trusted
S1(config)# interface GigabitEthernet 0/1
S1(config-if)# ip dhcp snooping trust

! Les ports d'accès restent untrusted par défaut
! Limiter le débit DHCP sur les ports d'accès
S1(config)# interface range FastEthernet 0/1-24
S1(config-if-range)# ip dhcp snooping limit rate 6
```

Copier

10.4 Attaque ARP Spoofing

Principe

L'attaquant envoie de fausses réponses ARP (ARP Reply gratuits) pour associer sa propre adresse MAC à l'adresse IP de la passerelle dans la table ARP des victimes.

```
Victime pense : IP passerelle 192.168.10.1 → MAC de l'attaquant
Résultat : tout le trafic passe par l'attaquant (Man-in-the-Middle)
```

Copier

Protection : Dynamic ARP Inspection (DAI)

```
! Prérequis : DHCP Snooping doit être activé
S1(config)# ip arp inspection vlan 10,20,30

! Port trunk vers un autre switch → trusted
S1(config)# interface GigabitEthernet 0/1
S1(config-if)# ip arp inspection trust

! Limiter le débit ARP sur les ports d'accès
S1(config)# interface range FastEthernet 0/1-24
S1(config-if-range)# ip arp inspection limit rate 15
```

Copier

10.5 Attaque VLAN Hopping

Double Tagging Attack

L'attaquant envoie une trame avec **deux tags 802.1Q**. Le premier switch retire le tag natif, et la trame arrive dans le VLAN cible.

Protection

```
! Changer le VLAN natif (ne pas utiliser VLAN 1)
S1(config-if)# switchport trunk native vlan 99

! Forcer le tagging du VLAN natif
S1(config)# vlan dot1q tag native

! Désactiver DTP
S1(config-if)# switchport nonegotiate

! Mettre les ports inutilisés dans un VLAN trou noir
S1(config)# interface range Fa0/20-24
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
S1(config-if-range)# shutdown
```

Copier

10.6 Attaque STP

L'attaquant envoie des BPDU avec une priorité plus basse pour devenir Root Bridge et intercepter le trafic.

Protection : BPDU Guard et Root Guard

```
! BPDU Guard – désactive le port si un BPDU est reçu
S1(config)# interface FastEthernet 0/1
S1(config-if)# spanning-tree bpduguard enable

! Root Guard – empêche un port de devenir Root Port
S1(config)# interface GigabitEthernet 0/2
S1(config-if)# spanning-tree guard root
```

Copier

TP Chapitre 10 : Identification des menaces LAN

Objectif : Comprendre et identifier les menaces de sécurité sur un LAN.

Étapes :

1. Observer le comportement d'un switch lors d'un MAC flooding (simulation)
2. Identifier les risques d'un faux serveur DHCP
3. Documenter les contre-mesures pour chaque attaque
4. Préparer la mise en œuvre des protections (Chapitre 11)

Chapitre 11 : Configuration de la sécurité des commutateurs

11.1 Port Security

Port Security limite le nombre d'adresses MAC autorisées sur un port et définit l'action à prendre en cas de violation.

Modes de violation

Mode	Trafic illégitime	Compteur violation	Notification	État du port
protect	Bloqué	Non incrémenté	❌	Up
restrict	Bloqué	Incrémenté	✅ (syslog/SNMP)	Up
shutdown	Bloqué	Incrémenté	✅ (syslog/SNMP)	err-disabled

Configuration Port Security

```
! Configuration de base
S1(config)# interface FastEthernet 0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 2
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# switchport port-security mac-address sticky

! Configuration avec adresse MAC statique
S1(config-if)# switchport port-security mac-address 00A1.B2C3.D4E5
```

Copier

Récupération d'un port en err-disabled

```
! Vérifier les ports en err-disabled
S1# show interfaces status err-disabled

! Récupération manuelle
S1(config)# interface FastEthernet 0/1
S1(config-if)# shutdown
S1(config-if)# no shutdown

! Récupération automatique (après 300 secondes par défaut)
S1(config)# errdisable recovery cause psecure-violation
S1(config)# errdisable recovery interval 300
```

Copier

11.2 DHCP Snooping — Configuration complète

```
! Activer DHCP Snooping
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20,30
S1(config)# no ip dhcp snooping information option

! Port trusted (vers serveur DHCP ou routeur)
S1(config)# interface GigabitEthernet 0/1
S1(config-if)# ip dhcp snooping trust

! Ports untrusted (vers les clients) — limiter le rate
S1(config)# interface range FastEthernet 0/1-24
S1(config-if-range)# ip dhcp snooping limit rate 6
```

Copier

Vérification DHCP Snooping

```
S1# show ip dhcp snooping
S1# show ip dhcp snooping binding
S1# show ip dhcp snooping statistics
```

Copier

11.3 Dynamic ARP Inspection (DAI) — Configuration complète

```
! Activer DAI (nécessite DHCP Snooping)
S1(config)# ip arp inspection vlan 10,20,30

! Port trusted (uplink vers switch/routeur)
S1(config)# interface GigabitEthernet 0/1
S1(config-if)# ip arp inspection trust

! Validation supplémentaire
S1(config)# ip arp inspection validate src-mac dst-mac ip

! Pour les hôtes avec IP statique : ARP ACL
S1(config)# arp access-list STATIC-ARP
S1(config-arp-nacl)# permit ip host 192.168.10.100 mac host 00A1.B2C3.D4E5
S1(config)# ip arp inspection filter STATIC-ARP vlan 10
```

Copier

Vérification DAI

```
S1# show ip arp inspection
S1# show ip arp inspection vlan 10
S1# show ip arp inspection statistics
S1# show ip arp inspection interfaces
```

Copier

11.4 IP Source Guard

IP Source Guard filtre le trafic basé sur la table DHCP Snooping binding pour empêcher l'usurpation d'adresses IP.

```
S1(config)# interface FastEthernet 0/1
S1(config-if)# ip verify source
```

Copier

11.5 Protection contre les attaques CDP/LLDP

```
! Désactiver CDP globalement
S1(config)# no cdp run

! Désactiver CDP sur des interfaces spécifiques
S1(config)# interface FastEthernet 0/1
S1(config-if)# no cdp enable

! Désactiver LLDP globalement
S1(config)# no lldp run
```

Copier

11.6 Récapitulatif des protections

Menace	Protection	Commande clé
MAC Flooding	Port Security	`switchport port-security`
DHCP Spoofing	DHCP Snooping	`ip dhcp snooping`
DHCP Starvation	DHCP Snooping + Port Security	`ip dhcp snooping limit rate`
ARP Spoofing	DAI	`ip arp inspection vlan`
VLAN Hopping	Trunk hardening	`switchport nonegotiate`
STP Attack	BPDU Guard	`spanning-tree bpduguard enable`
Reconnaissance	Désactiver CDP/LLDP	`no cdp run`

TP Chapitre 11 : Sécurisation d'un switch

Objectif : Mettre en œuvre toutes les protections de sécurité sur un switch.

Étapes :

1. Configurer Port Security (max 2 MAC, mode shutdown, sticky)
2. Activer DHCP Snooping sur les VLANs 10, 20 et 30
3. Configurer DAI sur les mêmes VLANs
4. Vérifier avec `show port-security`, `show ip dhcp snooping binding`, `show ip arp inspection`
5. Tester : connecter un 3ème appareil → observer le port en err-disabled
6. Récupérer le port et ajuster la configuration

Chapitre 12 : Principes WLAN

12.1 Fondamentaux du Wi-Fi

Standards IEEE 802.11

Standard	Fréquence	Débit max	Portée	Nom commercial
802.11a	5 GHz	54 Mbps	~35m	Wi-Fi 2
802.11b	2.4 GHz	11 Mbps	~100m	Wi-Fi 1
802.11g	2.4 GHz	54 Mbps	~70m	Wi-Fi 3
802.11n	2.4/5 GHz	600 Mbps	~70m	Wi-Fi 4
802.11ac	5 GHz	6.93 Gbps	~35m	Wi-Fi 5
802.11ax	2.4/5/6 GHz	9.6 Gbps	~70m	Wi-Fi 6/6E

Bandes de fréquences

Bande	Canaux	Avantages	Inconvénients
2.4 GHz	1-14 (3 non chevauchants : 1, 6, 11)	Meilleure portée, traverse mieux les murs	Interférences (micro-ondes, Bluetooth)
5 GHz	36-165 (23 non chevauchants)	Moins d'interférences, plus de canaux	Portée réduite

12.2 Composants WLAN

Composant	Description
STA (Station)	Client Wi-Fi (PC, téléphone, tablette)
AP (Access Point)	Point d'accès Wi-Fi
BSS (Basic Service Set)	Un AP avec ses clients associés
ESS (Extended Service Set)	Plusieurs BSS connectés (roaming)
SSID	Nom du réseau Wi-Fi
BSSID	Adresse MAC de l'AP
DS (Distribution System)	Réseau filaire reliant les APs

12.3 Topologies WLAN

Mode	Description	Utilisation
Ad-hoc (IBSS)	Communication directe entre STAs	Partage de fichiers temporaire
Infrastructure	Communication via un AP	Réseaux d'entreprise
Mesh	APs interconnectés sans fil	Couverture étendue

12.4 Processus de connexion Wi-Fi

Étapes d'association

Étape	Description
1. **Découverte**	Le client scanne les canaux (passif = écoute des Beacons / actif = envoi de Probe Requests)
2. **Authentification**	Open System Authentication (802.11) ou Shared Key
3. **Association**	Le client s'associe à l'AP (Association Request → Association Response)
4. **Authentification 802.1X**	(Optionnel) Authentification EAP via RADIUS

Trames de gestion 802.11

Trame	Description
Beacon	Annonce périodique de l'AP (SSID, canal, débit, sécurité)
Probe Request	Client recherche un réseau spécifique
Probe Response	AP répond à la demande du client
Authentication	Échange d'authentification
Association Request	Client demande à s'associer
Association Response	AP confirme l'association
Disassociation	Déconnexion propre
Deauthentication	Forçage de la déconnexion

12.5 Sécurité WLAN

Protocole	Chiffrement	Authentification	Sécurité
WEP	RC4 (64/128 bits)	Clé partagée	□ Obsolète — facilement crackable
WPA	TKIP + RC4	PSK ou 802.1X	⚠ Amélioré mais vulnérable
WPA2	AES-CCMP	PSK ou 802.1X	□ Standard actuel
WPA3	AES-GCMP-256	SAE ou 802.1X	□ Le plus sécurisé

Modes d'authentification

Mode	Description	Utilisation
Personal (PSK)	Clé pré-partagée	Réseaux domestiques/petites entreprises
Enterprise (802.1X)	Serveur RADIUS	Réseaux d'entreprise

12.6 Architecture WLAN d'entreprise

Type d'AP	Description	Gestion
Autonomous AP	AP indépendant, configuré individuellement	Gestion locale
Lightweight AP (LAP)	AP géré centralement par un WLC	CAPWAP/LWAPP
Cloud-Managed AP	AP géré via le cloud (Cisco Meraki)	Dashboard cloud

Architecture WLC (Wireless LAN Controller)

```
[Clients Wi-Fi] ↔ [LAP 1] ↔ [WLC] ↔ [Réseau filaire]
                  [LAP 2] ↗
                  [LAP 3] ↗

Protocole CAPWAP (Control and Provisioning of Wireless Access Points) :
- Port UDP 5246 : contrôle (chiffré DTLS)
- Port UDP 5247 : données
```

Copier

12.7 Menaces WLAN

Menace	Description
Rogue AP	AP non autorisé connecté au réseau
Evil Twin	AP malveillant imitant un AP légitime (même SSID)
Deauthentication Attack	Envoi de trames deauth pour déconnecter les clients
MITM Wi-Fi	Interception du trafic entre client et AP
Wardriving	Recherche de réseaux Wi-Fi non sécurisés

TP Chapitre 12 : Analyse des réseaux WLAN

Objectif : Identifier les composants WLAN et analyser la sécurité.

Étapes :

1. Identifier les réseaux Wi-Fi disponibles et leur sécurité
2. Analyser les trames Wi-Fi avec Wireshark (mode monitor)
3. Comparer WPA2-Personal et WPA2-Enterprise
4. Identifier un Rogue AP dans un environnement de test
5. Documenter les bonnes pratiques de sécurité WLAN

Chapitre 13 : Configuration WLAN

13.1 Configuration d'un AP autonome (routeur Wi-Fi Cisco)

Configuration de base du WLAN

```
! Accéder à l'interface radio
Router(config)# interface Dot11Radio 0
Router(config-if)# ssid ENTREPRISE-WIFI
Router(config-if-ssid)# authentication open
Router(config-if-ssid)# authentication key-management wpa version 2
Router(config-if-ssid)# wpa-psk ascii MonMotDePasse123!
Router(config-if-ssid)# guest-mode
Router(config-if-ssid)# exit
Router(config-if)# encryption mode ciphers aes-ccm
Router(config-if)# channel 6
Router(config-if)# power local 50
Router(config-if)# no shutdown
```

Copier

13.2 Configuration d'un WLC (Wireless LAN Controller)

Accès initial au WLC

```
Connexion via navigateur web : https://192.168.1.100
Ou via CLI (console/SSH)

(Cisco Controller) > show sysinfo
(Cisco Controller) > show wlan summary
(Cisco Controller) > show ap summary
```

Copier

Création d'un WLAN sur le WLC

Paramètre	Valeur
WLAN ID	1
Profile Name	Corp-WLAN
SSID	ENTREPRISE
Sécurité L2	WPA2 + AES
Auth	PSK ou 802.1X
Interface/VLAN	VLAN 10

```
(Cisco Controller) > config wlan create 1 Corp-WLAN ENTREPRISE
(Cisco Controller) > config wlan security wpa akm psk set-key ascii MonMotDePasse123! 1
(Cisco Controller) > config wlan interface 1 vlan10
(Cisco Controller) > config wlan enable 1
```

Copier

13.3 Configuration WPA2-Enterprise avec RADIUS

Sur le WLC

```
! Configurer le serveur RADIUS
(Cisco Controller) > config radius auth add 1 10.0.0.50 1812 ascii SharedSecret123

! Appliquer 802.1X au WLAN
(Cisco Controller) > config wlan security wpa akm 802.1x enable 1
(Cisco Controller) > config wlan radius_server auth add 1 1
```

Copier

Sur le switch (pour le VLAN dédié au WLAN)

```
S1(config)# vlan 10
S1(config-vlan)# name WLAN-Corp

S1(config)# interface FastEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# description Vers AP
```

Copier

13.4 Configuration du routeur Wi-Fi domestique (interface GUI)

Sur un routeur Wi-Fi domestique (Linksys, Netgear, etc.) accessible via l'interface web :

Paramètre	Configuration recommandée
SSID	Nom personnalisé (pas le nom par défaut)
Sécurité	WPA2-Personal (AES) minimum, WPA3 si disponible
Mot de passe	12+ caractères, complexe
Canal	Auto ou canal le moins encombré (1, 6, ou 11 en 2.4 GHz)
Broadcast SSID	Activé (le masquer n'améliore pas la sécurité)
Firmware	Toujours à jour
Accès admin	Mot de passe fort, HTTPS
WPS	Désactivé (vulnérable)

13.5 Bonnes pratiques de sécurité WLAN

Pratique	Description
Utiliser **WPA3** ou **WPA2-AES**	Jamais WEP ou WPA-TKIP
802.1X en entreprise	Authentification individuelle via RADIUS
Segmentation VLAN	WLAN invité sur un VLAN séparé
Désactiver WPS	Vulnérable aux attaques brute-force
Filtrage MAC	Couche supplémentaire (facilement contournable)
IDS/IPS Wi-Fi	Détection de Rogue AP et attaques
Réduire la puissance	Limiter la portée au strict nécessaire
Mise à jour firmware	Correctifs de sécurité réguliers

TP Chapitre 13 : Configuration WLAN

Objectif : Configurer un réseau sans fil sécurisé.

Scénario Packet Tracer :

```
[PC sans fil] ↔Wi-Fi→ [AP/Routeur Wi-Fi] ↔Fa0→ [S1] ↔Gi0/1→ [R1] → Internet
```

Copier

Étapes :

1. Configurer le SSID et WPA2-PSK sur le routeur Wi-Fi
2. Connecter un PC sans fil au réseau
3. Vérifier la connectivité (ping vers la passerelle)
4. Créer un second SSID pour les invités (VLAN séparé)
5. Vérifier l'isolation entre les deux réseaux

Chapitre 14 : Principes de routage

14.1 Fonctionnement d'un routeur

Le routeur prend des décisions de transfert basées sur la **table de routage** :

1. Le routeur reçoit un paquet
2. Il examine l'adresse IP destination
3. Il consulte sa table de routage pour trouver la meilleure route
4. Il transfère le paquet vers l'interface de sortie appropriée

14.2 La table de routage

```
R1# show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF,
       D - EIGRP, B - BGP, L - local

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L    192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
C    10.0.0.0/30 is directly connected, Serial0/1/0
L    10.0.0.1/32 is directly connected, Serial0/1/0
S    192.168.20.0/24 [1/0] via 10.0.0.2
S*   0.0.0.0/0 [1/0] via 10.0.0.2
```

Copier

Types de routes

Code	Type	Description
C	Connected	Réseau directement connecté
L	Local	Adresse IP de l'interface du routeur (/32)
S	Static	Route configurée manuellement
S*	Static default	Route par défaut statique
R	RIP	Route apprise par RIP
O	OSPF	Route apprise par OSPF
D	EIGRP	Route apprise par EIGRP

14.3 Décision de routage

Le routeur sélectionne la route en suivant ces critères :

Critère	Description
1. **Longest prefix match**	La route avec le masque le plus spécifique l'emporte
2. **Distance administrative**	Plus la valeur est basse, plus la source est fiable
3. **Métrique**	Coût du chemin (spécifique au protocole)

Distance administrative (AD)

Source de la route	AD
Directement connectée	0
Route statique	1
EIGRP (résumé)	5
BGP externe	20
EIGRP interne	90
OSPF	110
IS-IS	115
RIP	120
EIGRP externe	170
BGP interne	200

14.4 Routage IPv4 vs IPv6

```
! Activer le routage IPv6
R1(config)# ipv6 unicast-routing

! Vérifier la table de routage IPv6
R1# show ipv6 route

IPv6 Routing Table - 5 entries
C   2001:DB8:ACAD:1::/64 [0/0] via GigabitEthernet0/0/0
L   2001:DB8:ACAD:1::1/128 [0/0] via GigabitEthernet0/0/0
S   2001:DB8:ACAD:2::/64 [1/0] via 2001:DB8:ACAD:A::2
```

Copier

14.5 Routage statique vs dynamique

Caractéristique	Statique	Dynamique
Configuration	Manuelle	Automatique
Scalabilité	Faible	Élevée
Adaptation	Aucune (manuelle)	Automatique (convergence)
Bande passante	Aucun overhead	Overhead des mises à jour
Sécurité	Plus sécurisé	Risque de manipulation
Utilisation	Petits réseaux, routes par défaut	Grands réseaux

□ TP Chapitre 14 : Exploration de la table de routage

Objectif : Comprendre la table de routage et la prise de décision.

Étapes :

1. Configurer les interfaces de R1 et R2
2. Afficher la table de routage : `show ip route`
3. Identifier les routes C (connected) et L (local)
4. Ajouter des routes statiques
5. Observer le longest prefix match avec `traceroute`

Chapitre 15 : Routage IP statique

15.1 Types de routes statiques

Type	Syntaxe	Utilisation
Standard	`ip route réseau masque next-hop`	Route vers un réseau spécifique
Par défaut	`ip route 0.0.0.0 0.0.0.0 next-hop`	Route catch-all
Flottante	`ip route réseau masque next-hop AD`	Backup (AD plus élevée)
Résumée	`ip route réseau masque_résumé next-hop`	Agrégation de routes

15.2 Configuration des routes statiques IPv4

Route statique standard (next-hop)

```
R1(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.2
```

Copier

Route statique vers une interface de sortie

```
R1(config)# ip route 192.168.20.0 255.255.255.0 Serial 0/1/0
```

Copier

Route statique complète (interface + next-hop)

```
R1(config)# ip route 192.168.20.0 255.255.255.0 GigabitEthernet 0/0/1 10.0.0.2
```

Copier

> ***Bonne pratique** : Pour les réseaux **point-à-point** (série), l'interface de sortie suffit. Pour les réseaux **multi-accès** (Ethernet), spécifier le next-hop ou les deux.*

15.3 Route par défaut

```
! Route par défaut IPv4
R1(config)# ip route 0.0.0.0 0.0.0.0 10.0.0.2

! Route par défaut IPv6
R1(config)# ipv6 route ::/0 2001:DB8:ACAD:A::2

! Vérifier
R1# show ip route static
R1# show ip route 0.0.0.0
```

Copier

15.4 Route statique flottante

Une route flottante a une **distance administrative plus élevée** que la route principale. Elle ne s'active que si la route principale disparaît.

```
! Route principale via Serial 0/1/0 (AD = 1 par défaut)
R1(config)# ip route 192.168.20.0 255.255.255.0 10.0.0.2

! Route flottante de backup via Serial 0/1/1 (AD = 5)
R1(config)# ip route 192.168.20.0 255.255.255.0 10.0.1.2 5
```

Copier

> *La route flottante (AD=5) n'apparaît dans la table de routage que si la route principale (AD=1) est indisponible.*

15.5 Routes statiques IPv6

```
! Route statique standard
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 2001:DB8:ACAD:A::2

! Route statique via interface de sortie
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 Serial 0/1/0

! Route statique via link-local (nécessite l'interface de sortie)
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 Serial 0/1/0 FE80::2

! Route par défaut
R1(config)# ipv6 route ::/0 2001:DB8:ACAD:A::2

! Route flottante IPv6
R1(config)# ipv6 route 2001:DB8:ACAD:2::/64 2001:DB8:ACAD:B::2 5
```

Copier

15.6 Routes statiques résumées

Au lieu de créer plusieurs routes :

```
R1(config)# ip route 192.168.16.0 255.255.255.0 10.0.0.2
R1(config)# ip route 192.168.17.0 255.255.255.0 10.0.0.2
R1(config)# ip route 192.168.18.0 255.255.255.0 10.0.0.2
R1(config)# ip route 192.168.19.0 255.255.255.0 10.0.0.2
```

Copier

On peut résumer avec un supernet :

```
R1(config)# ip route 192.168.16.0 255.255.252.0 10.0.0.2
```

Copier

> *Calcul : 192.168.16.0 à 192.168.19.0 = 4 réseaux → /22 (255.255.252.0)*

15.7 Vérification des routes statiques

```
R1# show ip route static
R1# show ip route 192.168.20.0
R1# show running-config | section ip route

R1# show ipv6 route static
R1# show ipv6 route 2001:DB8:ACAD:2::/64
```

Copier

□ TP Chapitre 15 : Configuration du routage statique

Objectif : Configurer des routes statiques IPv4 et IPv6 dans un réseau multi-routeurs.

Topologie :

```
[PC1]         [PC2]         [PC3]
  |             |             |
[S1]          [S2]          [S3]
  |             |             |
[R1]---WAN---[R2]---WAN---[R3]
 .1  10.0.0.0/30  .1  10.0.1.0/30
192.168.10.0   192.168.20.0   192.168.30.0
```

Copier

Plan d'adressage :

Lien	Réseau	R1	R2	R3
R1-R2	10.0.0.0/30	.1	.2	-
R2-R3	10.0.1.0/30	-	.1	.2
LAN R1	192.168.10.0/24	.1	-	-
LAN R2	192.168.20.0/24	-	.1	-
LAN R3	192.168.30.0/24	-	-	.1

Étapes :

1. Configurer les interfaces sur R1, R2 et R3
2. Configurer les routes statiques sur R1 vers les réseaux 20 et 30
3. Configurer les routes statiques sur R3 vers les réseaux 10 et 20
4. Configurer R2 avec les routes vers les réseaux 10 et 30
5. Ajouter les routes par défaut vers Internet (simulé)
6. Configurer une route flottante de backup
7. Répéter avec IPv6
8. Vérifier la connectivité complète avec `ping` et `traceroute`

Chapitre 16 : Dépannage des routes statiques et par défaut

16.1 Méthodologie de dépannage

Approche structurée

Étape	Action
1	**Identifier le problème** : ping, traceroute, show ip route
2	**Isoler la cause** : quel tronçon pose problème ?
3	**Vérifier couche par couche** : L1 → L2 → L3
4	**Corriger et tester**
5	**Documenter**

Commandes de diagnostic essentielles

```
! Test de connectivité de base
R1# ping 192.168.20.1
R1# ping 192.168.20.1 source 192.168.10.1

! Tracer le chemin
R1# traceroute 192.168.20.1

! Vérifier la table de routage
R1# show ip route
R1# show ip route 192.168.20.0

! Vérifier les interfaces
R1# show ip interface brief
R1# show interfaces GigabitEthernet 0/0/0

! Vérifier la configuration
R1# show running-config | section ip route
R1# show running-config interface GigabitEthernet 0/0/0
```

Copier

16.2 Problèmes courants et solutions

Problème 1 : Interface down

```
R1# show ip interface brief
Interface           IP-Address      OK?  Method  Status  Protocol
Gi0/0/0             192.168.10.1    YES  manual  down    down
```

Copier

Causes possibles :

- Câble non connecté (L1)
- Interface administrativement désactivée
- Problème matériel