

# Module 1: Conception de réseau



# 1.1 Réseaux hiérarchiques

# La nécessité de faire évoluer le réseau

Les organisations s'appuient de plus en plus sur leur infrastructure réseau pour offrir des services critiques.

Les organisations en évolution ont besoin de réseaux capables d'évoluer et de soutenir:

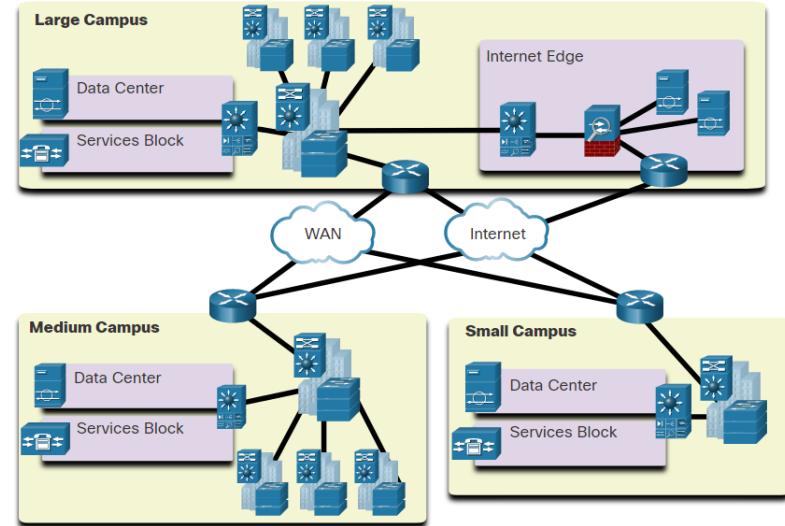
- Trafic réseau convergent
- Applications critiques
- Des besoins métier variés
- Contrôle administratif centralisé

Les conceptions de réseaux sur les campus vont des petits réseaux utilisant un seul commutateur LAN à des très grands réseaux comptant des milliers de connexions.

# Réseaux commutés sans frontières

Le réseau commuté sans frontières est une architecture de réseau qui permet de connecter tout le monde, à tout moment, où qu'ils se trouvent et quel que soit l'appareil utilisé, d'une manière à la fois sûre, fiable et fluide.

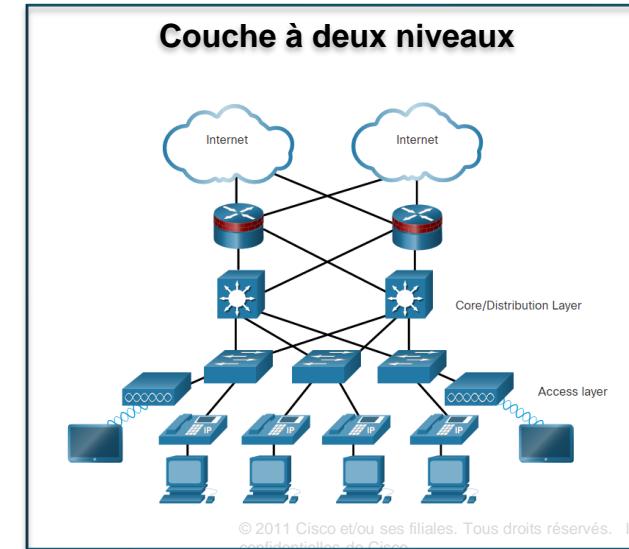
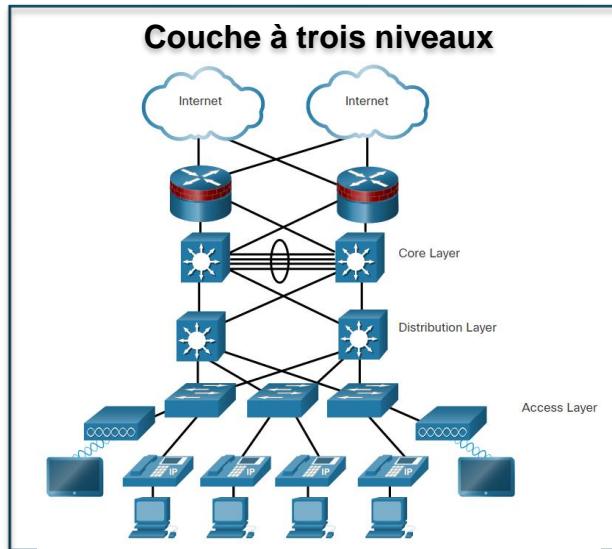
- Il fournit le cadre pour unifier l'accès filaire et sans fil, construit sur une infrastructure matérielle hiérarchique évolutive et résiliente.
- Les réseaux commutés sans frontières sont hiérarchiques, modulaires, résilients et flexibles.



# La hiérarchie du réseau commuté sans frontières

Les réseaux hiérarchiques utilisent une conception à plusieurs niveaux d'accès, de distribution et de couches centrales, chaque couche jouant un rôle bien défini dans le réseau du campus.

Il existe deux cadres de conception hiérarchique éprouvés pour les réseaux de campus.



# Fonctions des couches d'accès, de distribution et de cœur de réseau

## Couche d'accès

- La couche d'accès offre un accès réseau à l'utilisateur.
- La figure présente un commutateur de couche d'accès connecté à deux commutateurs de couche de distribution.

## Couche de distribution

- La couche de distribution implémente le routage, la qualité du service et la sécurité.
- Il regroupe les réseaux de placards de câblage à grande échelle et limite les domaines de diffusion de couche 2.
- Les commutateurs de couche de distribution se connectent aux commutateurs de couche d'accès et de couche cœur de réseau.

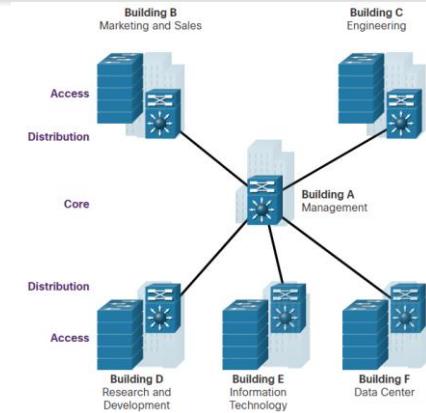
## Couche cœur de réseau

- La couche cœur de réseau est l'épine fédératrice du réseau et connecte plusieurs couches du réseau.
- La couche cœur de réseau fournit la localisation de défauts et la connectivité au fédératrice à haute vitesse.

# Exemples à trois niveaux et à deux niveaux

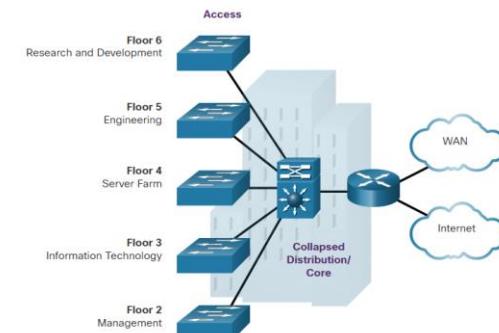
### Réseau de campus à trois niveaux

- Utilisé par les organisations nécessitant un accès, une distribution et des couches de cœur de réseau.
- Il est recommandé d'établir une topologie de réseau physique en étoile étendue, depuis un bâtiment centralisé vers tous les autres bâtiments du campus.



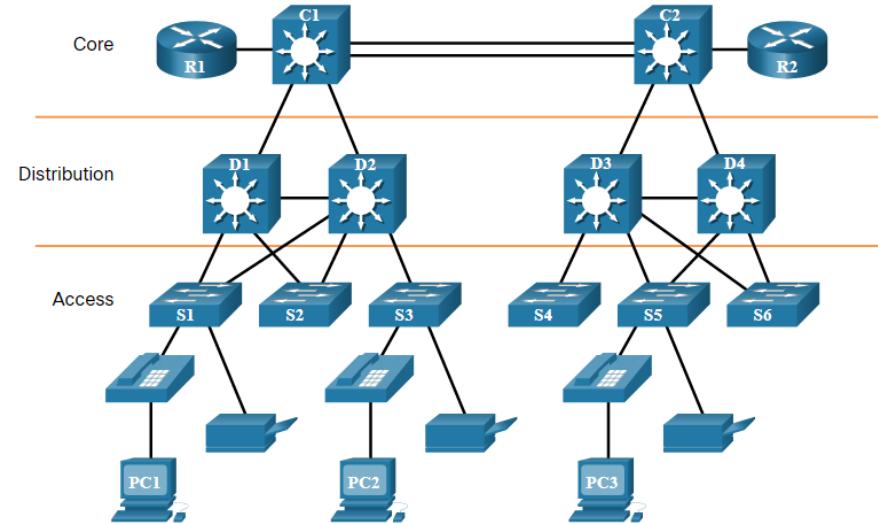
### Réseau de campus à deux niveaux

- Utilisé lorsque des couches de distribution et de cœur réseau séparées n'est pas nécessaire.
- Utile pour les emplacements de campus plus petits, ou sur les sites de campus constitués d'un seul bâtiment.
- Également connu sous le nom de conception de réseau *cœur de réseau sont regroupés*.



# Le rôle des réseaux commutés

- Les réseaux ont fondamentalement changé, pour devenir des réseaux locaux commutés dans un réseau hiérarchique.
- Un réseau local commuté permet une flexibilité supplémentaire, la gestion du trafic, la qualité de service et la sécurité.
- Un réseau local commuté peut également prendre en charge la mise en réseau sans fil et d'autres technologies telles que le téléphone IP et les services de mobilité.



# 1.2 Réseaux évolutifs

# Conception pour l'évolutivité

L'évolutivité est le terme d'un réseau qui peut se développer sans perdre la disponibilité et la fiabilité.

Les concepteurs de réseaux doivent élaborer des stratégies pour permettre au réseau d'être disponible et de s'étendre efficacement et facilement.

Ceci est accompli en utilisant:

- Redondance
- Liens multiples
- Protocole de routage évolutif
- Connectivité sans fil

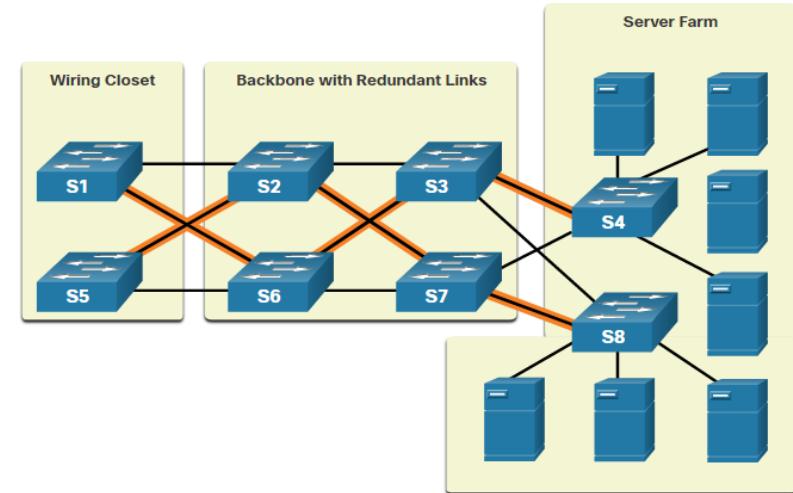
# Planification pour la redondance

La redondance peut prévenir l'interruption des services de réseau en minimisant la possibilité d'un seul point de défaillance par:

- Installer un équipement en double
- Fournir des services de basculement sur incident pour les périphériques critiques

Les chemins redondants offrent des chemins physiques alternatifs pour que les données traversent le réseau en favorisant la haute disponibilité.

- Toutefois, les chemins d'accès redondants dans un réseau Ethernet peuvent entraîner à la fois des boucles logiques de couche 2.
- Par conséquent, le protocole STP (Spanning Tree) est nécessaire.



# Réduire la taille du domaine défaillant

Un réseau bien conçu contrôle le trafic et limite la taille des domaines de défaillance (c'est-à-dire la zone d'un réseau qui est affectée lorsque le réseau rencontre des problèmes).

- Dans le modèle de conception hiérarchique, les domaines d'échec sont terminés à la couche de distribution.
- Chaque routeur fonctionne comme une passerelle pour un nombre limité d'utilisateurs de la couche d'accès.

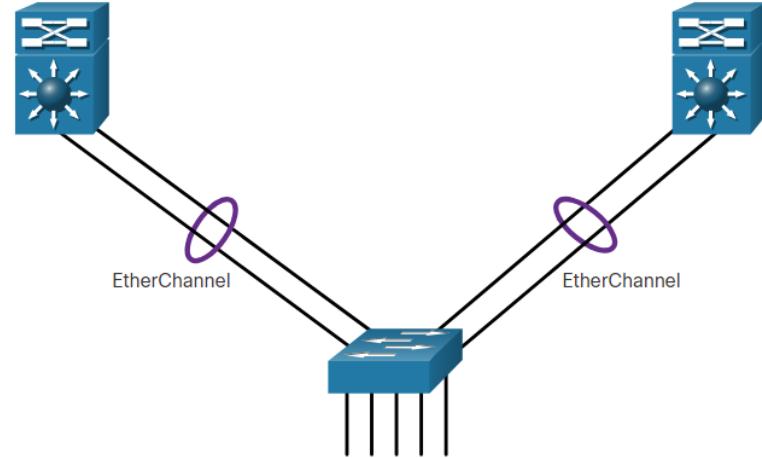
Les routeurs, ou les commutateurs multicouches, sont généralement déployés par paires dans une configuration appelée bloc de commutateur de bâtiment ou de service.

- Chaque bloc de commutateur est indépendant.
- Ainsi, lorsqu'un périphérique tombe en panne, l'ensemble du réseau continue à fonctionner normalement.

# Augmentation de la bande passante

L'agrégation de liens (comme EtherChannel) permet à un administrateur d'augmenter le volume de bande passante entre les appareils en créant un lien logique constitué de plusieurs liens physiques.

- EtherChannel combine les ports de commutateurs existants en un lien logique utilisant une interface Port Channel.
- La plupart des tâches de configuration sont réalisées sur l'interface Port Channel (plutôt que sur chaque port), ce qui assure la cohérence de la configuration sur tous les liens.
- EtherChannel peut équilibrer la charge entre les liens.



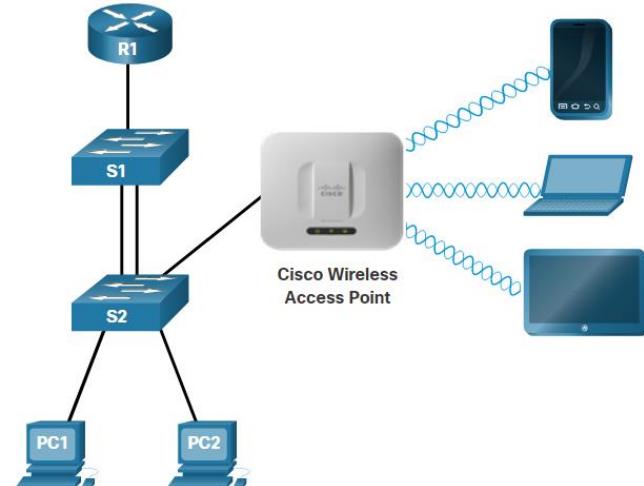
# Extension de la couche d'accès

Une option de plus en plus populaire pour étendre la connectivité de la couche d'accès est le sans fil.

- Les LAN sans fil offrent une plus grande flexibilité, des coûts réduits, sans oublier la possibilité de se développer et de s'adapter à l'évolution des besoins professionnels.
- Pour communiquer sans fil, les périphériques terminaux nécessitent une carte réseau sans fil pour se connecter à un routeur sans fil ou à un point d'accès sans fil (AP).

Voici quelques considérations lors de la mise en œuvre d'un réseau sans fil:

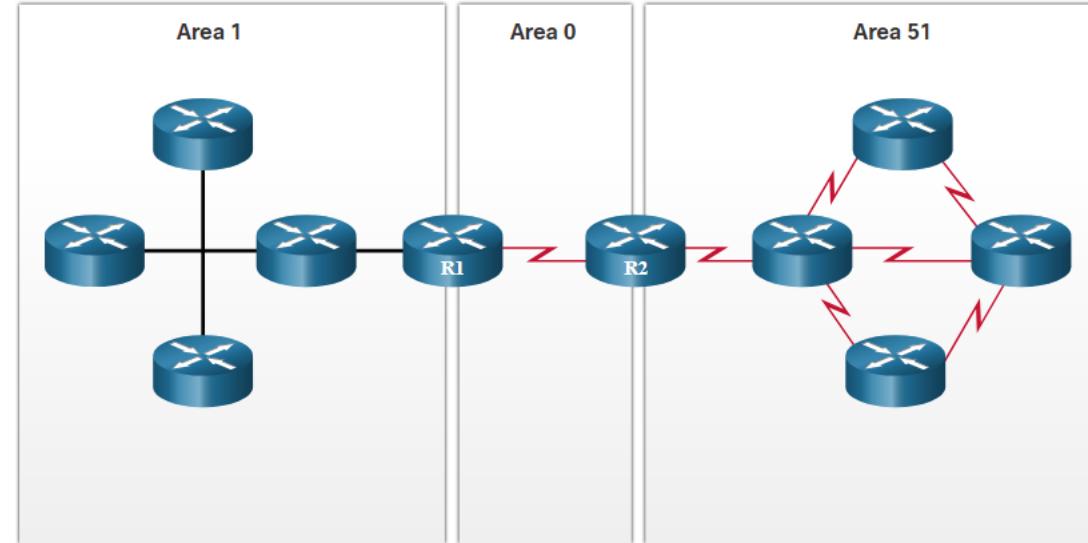
- Types de périphériques sans fil se connectant au WLAN
- Exigences de couverture sans fil
- Éléments à prendre en compte pour éviter les interférences
- Considérations relatives à la sécurité



# Précisions sur les protocoles de routage

Des protocoles de routage avancés, tels que l'OSPF (Open Shortest Path First), sont utilisés dans les grands réseaux.

- OSPF est un protocole de routage d'état de liaison qui utilise des zones pour prendre en charge un réseau hiérarchique.
- Les routeurs OSPF établissent et maintiennent une ou des contiguïtés de voisinage avec d'autres routeurs OSPF connectés.
- Les routeurs OSPF synchronisent leur base de données d'état de liaison.
- Lorsqu'un changement de réseau se produit, des mises à jour de l'état des liens sont envoyées, informant les autres routeurs OSPF du changement et établissant un nouveau meilleur chemin, si un tel chemin est disponible.  

# 1.3 Matériel de commutateur

## Places-formes de commutateur

Il existe une variété de plates-formes de commutateur, de facteurs de forme et d'autres fonctionnalités qui doivent être pris en compte avant de choisir un commutateur. Lors de la conception d'un réseau, il est important de sélectionner le matériel approprié aux besoins actuels, tout en prévoyant la croissance du réseau. Au sein d'un réseau d'entreprise, les commutateurs et les routeurs jouent un rôle essentiel dans la communication réseau.

Les commutateurs LAN Campus, tels que la série Cisco 3850 illustrée ici, prennent en charge des concentrations élevées de connexions utilisateur avec une vitesse et une sécurité appropriées pour le réseau d'entreprise.



# Places-formes de commutateur (Suite)

Les commutateurs d'accès gérés dans le cloud Meraki de Cisco permettent l'empilage virtuel des commutateurs. Ils permettent de surveiller et de configurer des milliers de ports de commutation sur le web, sans aucune intervention du personnel informatique sur le site.

La plate-forme Cisco Nexus encourage l'évolutivité de l'infrastructure, la continuité opérationnelle et la flexibilité du transport dans le data center.



## Places-formes de commutateur (Suite)

Les commutateurs d'accès Ethernet pour fournisseurs de services apportent surveillance des applications, services unifiés, virtualisation, sécurité intégrée et gestion simplifiée.



Les plates-formes de commutation de réseaux virtuels Cisco Nexus apportent des services multilocataires sécurisés en ajoutant une technologie d'intelligence de virtualisation au réseau de Data center.



## Facteurs de forme de commutateur

Lorsqu'ils sélectionnent un commutateur, les administrateurs réseau doivent déterminer ses facteurs de forme. Cela comprend la configuration fixe, la configuration modulaire, empilable ou non empilable

Les caractéristiques et les options des commutateurs à configuration fixe sont limitées à celles qui sont fournies à l'origine avec le commutateur.

Le châssis des commutateurs modulaires accepte les cartes de ligne remplaçables sur le terrain.



# Facteurs de forme de commutateur (Suite)

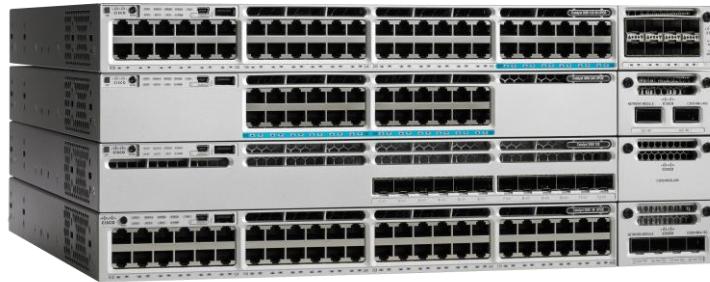
Les commutateurs empilables, connectés à l'aide d'un câble spécial, fonctionnent comme un seul commutateur de grande taille.



L'épaisseur du commutateur, exprimée en nombre d'unités de rack, est également importante pour les commutateurs montés dans un rack. Par exemple, les commutateurs à configuration fixe illustrés dans la figure sont tous d'une unité de rack (1U) ou de 1,75 pouces (44,45 mm) de hauteur.

# Densité du ports

La densité de ports d'un commutateur fait référence au nombre de ports disponibles sur un commutateur unique.



Les commutateurs à configuration fixe prennent en charge diverses configurations de densité de ports. Le Cisco Catalyst 3850 est disponible en configurations 12, 24, 48 ports.



Les commutateurs modulaires peuvent prendre en charge des densités de ports très élevées grâce à l'ajout de plusieurs cartes de lignes de ports de commutateur. Le commutateur modulaire Catalyst 9400 prend en charge 384 interfaces de port de commutateur.

## Débit de transfert

Les taux de réacheminement désignent la capacité de traitement d'un commutateur en mesurant la quantité de données que ce commutateur peut traiter par seconde.

- Les gammes de produits de commutateur sont classées par débits de transfert.
- Le débit de transfert des commutateurs bas de gamme est inférieur à celui des commutateurs d'entreprise.

Si le débit de transfert de commutateur est trop faible, il ne peut pas convenir à une communication à la vitesse du câble à travers l'ensemble de ses ports de commutation.

- Le débit filaire correspond au débit de données que chaque port Ethernet du commutateur peut atteindre.
- Les débits de données peuvent être de 100 Mbps, 1 Gbps, 10 Gbps ou 100 Gbps.
- Les commutateurs de la couche d'accès n'ont généralement pas besoin de fonctionner au débit filaire, car ils sont physiquement limités par leurs liaisons ascendantes vers la couche de distribution.

## Power over Ethernet (PoE)

La technologie PoE (Power over Ethernet) permet au commutateur de fournir une alimentation à un périphérique (par exemple, Phone IP, AP, Camera) à travers le câblage Ethernet existant.

Un administrateur réseau doit s'assurer que les fonctionnalités PoE sont réellement nécessaires pour une installation donnée, car les commutateurs qui supportent le PoE sont coûteux.

## La commutation multicouche

Les commutateurs multicouches sont généralement déployés dans les couches principales et de distribution du réseau commuté d'une entreprise.

- Ils prennent en charge certains protocoles de routage et transmettent les paquets IP à un rythme proche de celui de la transmission de la couche 2.
- Les commutateurs multicouches prennent souvent en charge du matériel spécialisé, tels que des circuits intégrés spécifiques ASIC (Application Specific Integrated Circuits).
- Les ASIC, associés à des structures de données logicielles dédiées, peuvent rationaliser le réacheminement de paquets IP indépendamment du processeur.

# Considérations commerciales pour la sélection du commutateur

Considération	Description
Coût	Le coût d'un commutateur dépend du nombre et de la rapidité des interfaces, des fonctionnalités prises en charge et de sa capacité d'extension.
Densité des ports	Les commutateurs de réseau doivent prendre en charge le nombre approprié d'appareils sur le réseau.
Alimentation	Il est maintenant courant d'alimenter les points d'accès, les téléphones IP et les commutateurs compacts par l'intermédiaire de l'alimentation par Ethernet (PoE). Outre les aspects PoE, certains commutateurs sur châssis prennent en charge des alimentations redondantes.
Fiabilité	Le commutateur doit fournir un accès permanent au réseau.
Vitesse du port	La vitesse de la connexion au réseau est une préoccupation essentielle des utilisateurs finaux.
Tampons de trames	Il est important qu'un commutateur enregistre les trames, dans les réseaux susceptibles d'encombrement des ports vers des serveurs ou d'autres parties du réseau.
Évolutivité	Le nombre d'utilisateurs d'un réseau évolue généralement au fil du temps ; le commutateur doit donc comporter des possibilités de croissance.

# 1.4 Matériel de routeur

## Spécifications des routeurs

Les routeurs utilisent la partie du réseau (préfixe) de l'adresse IP de destination pour envoyer des paquets vers la destination appropriée.

- Ils choisissent un chemin alternatif si un lien tombe en panne.
- Tous les hôtes d'un réseau local spécifient dans leur configuration IP l'adresse IP de l'interface du routeur local comme leur passerelle par défaut.

Les routeurs remplissent également d'autres fonctions bénéfiques, comme suit :

- Ils assurent le confinement des émissions en limitant les diffusions au réseau local.
- Ils relient entre eux des lieux géographiquement séparés.
- Les utilisateurs regroupés logiquement par application ou département au sein d'une entreprise, qui ont des besoins de commandement ou qui ont besoin d'accéder aux mêmes ressources.
- Ils offrent une sécurité accrue en filtrant le trafic indésirable au moyen de listes de contrôle d'accès.

## Routeurs Cisco

Les routeurs de filiale, illustrés dans la figure, optimisent les services des filiales sur une plate-forme unique tout en offrant une expérience applicative optimale dans les infrastructures des filiales et du réseau étendu. Les routeurs de la série 4000 de Cisco ISR (Integrated Services Router) sont présentés.



# Routeurs Cisco (Suite)

Les routeurs de périphérie de réseau, illustrés dans la figure, permettent à la périphérie de réseau de fournir des services haute performance, hautement sécurisés et fiables qui unissent les réseaux de campus, de Data center et de réseaux de filiale. Les routeurs de la série 9000 de Cisco ASR (Aggregation Services Routers) sont représentés.



## Routeurs Cisco (Suite)

Les routeurs de fournisseurs de services, illustrés dans la figure, fournissent des solutions évolutives de bout en bout et des services adaptés aux abonnés. Les routeurs de la série 6000 du Cisco NCS (Network Convergence System) sont illustrés.



Door Closed



Door Open

# Routeurs Cisco (Suite)

Les routeurs industriels, tels que ceux illustrés dans la figure, sont conçus pour fournir des fonctionnalités de classe entreprise dans des environnements robustes et difficiles. Les routeurs industriels à services intégrés de la série Cisco 1100 sont illustrés.



## Facteurs de forme du routeur

**Séries Cisco 900:** Il s'agit d'un petit routeur de filiale. Il combine des options de connexion WAN, de commutation, de sécurité et de connectivité avancées dans une plate-forme compacte et sans ventilateur pour les petites et moyennes entreprises.



# Facteurs de forme du routeur

**Routeurs Cisco ASR 9000 et 1000:** Ces routeurs fournissent densité et résilience avec programmabilité, pour une périphérie réseau évolutive.



# Facteurs de forme du routeur

**Routeurs de séries Cisco 5500 NCS (Network Convergence System):** ces routeurs sont conçus pour évoluer efficacement entre les grands centres de données et les grands réseaux d'entreprise, le Web et les réseaux WAN et d'agrégation des fournisseurs de services.

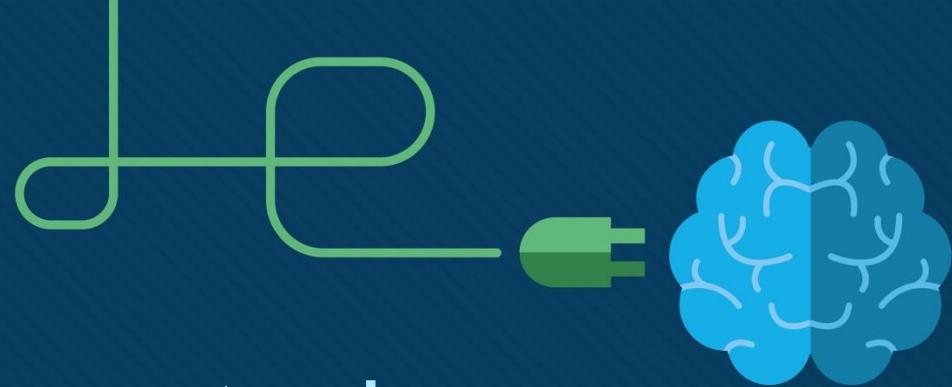


confidentielles de Cisco

## Facteurs de forme du routeur

**Routeur Cisco 800 ISR (Industrial Integrated Services Router):** Ce routeur est compact et conçu pour les environnements difficiles.





# Module 2 : Concepts de commutation



# Objectifs de ce module

**Titre du module:** Concepts de commutation

**Objectif du module :** Expliquer comment la couche 2 permet de transférer des données.

<b>Titre du rubrique</b>	<b>Objectif du rubrique</b>
<b>Transfert de trame</b>	Expliquer comment les trames sont transmises sur un réseau commuté.
<b>Domaines de commutation</b>	Comparer un domaine de collision à un domaine de diffusion.

# 2.1 Transfert de trame

# Commutation dans la mise en réseau

Deux termes sont associés à des trames entrant ou sortant d'une interface:

- **Ingress (entrer)** - entrer dans l'interface
- **Egress (sortie)** — sortie de l'interface

Un commutateur de transfert basé sur l'interface d'entrée et l'adresse MAC de destination.

Un commutateur utilise sa table d'adresses MAC pour prendre des décisions de transmission.

**Remarque:** Un commutateur ne permettra jamais de transférer le trafic sur l'interface où il a reçu le trafic.



Port Table	
Destination Addresses	Port
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

## Le tableau d'adresses MAC du commutateur

Un commutateur utilisera l'adresse MAC de destination pour déterminer l'interface de sortie.

Avant qu'un commutateur puisse prendre cette décision, il doit savoir quelle interface se trouve la destination.

Un commutateur construit une table d'adresses MAC, également appelée table CAM (Content Addressable Memory), en enregistrant l'adresse MAC source dans la table avec le port qu'il a reçu.

# La méthode d'apprentissage et de transmission du commutateur

Le commutateur utilise un processus en deux étapes:

## Étape 1. Apprendre - Examiner l'adresse source

- Ajoute le MAC source si ce n'est pas dans la table
- Réinitialise le réglage du délai d'arrêt à 5 minutes si la source est dans le tableau

## Étape 2. Transfert - Examiner l'adresse de destination

- Si le MAC de destination se trouve dans la table d'adresses MAC, il est transféré hors du port spécifié.
- Si un MAC de destination n'est pas dans la table, il est inondé de toutes les interfaces sauf celle qu'il a reçue.

## Les méthodes de transmission du commutateur

Les commutateurs utilisent des logiciels sur des circuits intégrés spécifiques à l'application (ASIC) pour prendre des décisions très rapides.

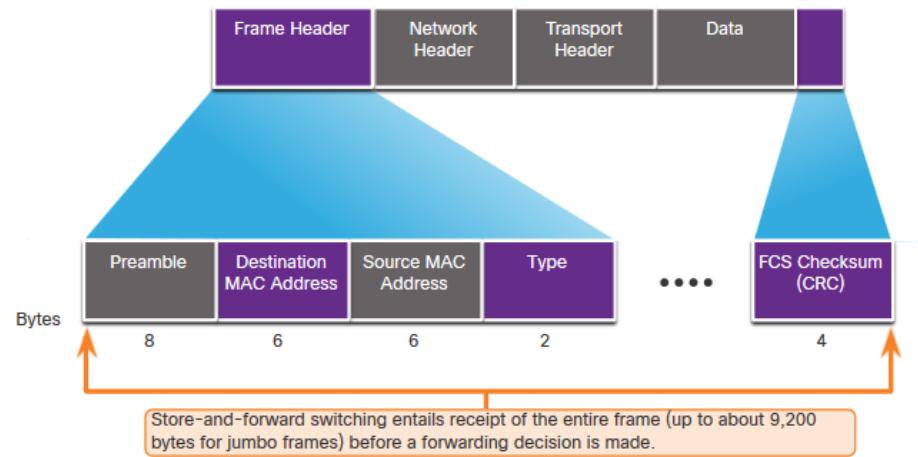
Un commutateur utilisera l'une des deux méthodes pour prendre des décisions de transfert après avoir reçu une trame:

- **Commutation de stockage et de transfert** - Reçoit la trame entière et assure la validité de la trame. La commutation par stockage et retransmission est la méthode de commutation LAN principale de Cisco.
- **Commutation par coupure (cut-through)** - Transfère la trame immédiatement après avoir déterminé l'adresse MAC de destination d'une trame entrante et le port de sortie.

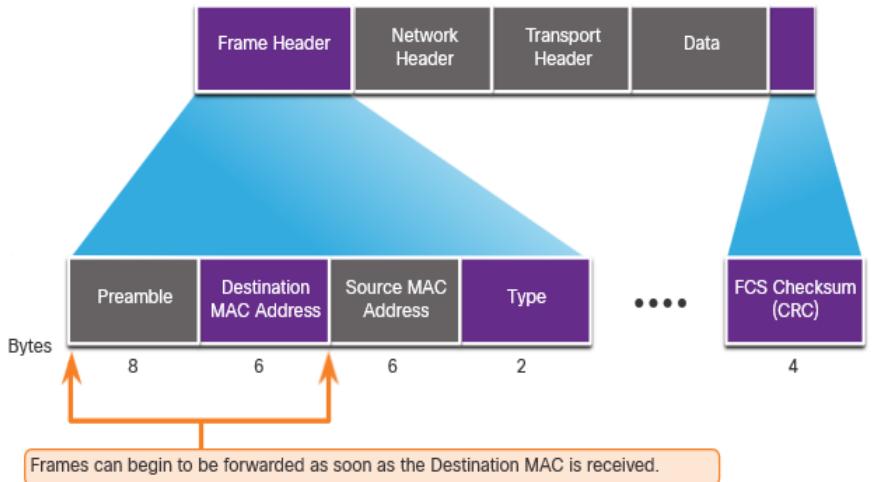
# Commutation par stockage et retransmission (Store-and-Forward)

Le stockage et le transfert présentent deux caractéristiques principales :

- Vérification des erreurs — Le commutateur vérifie la séquence de vérification de trame (FCS) pour les erreurs CRC. Les trames défectueux seront jetés.
- Mise en mémoire tampon - L'interface d'entrée met en mémoire tampon la trame pendant qu'elle vérifie le FCS. Cela permet également au commutateur de s'adapter à une éventuelle différence de vitesse entre les ports d'entrée et de sortie.



# Commutation par coupure (Cut-Through)



- La coupure transmet la trame immédiatement après avoir déterminé le MAC de destination.
- La méthode Fragment (Frag) Free permet de vérifier la destination et de s'assurer que la trame est d'au moins 64 octets. Cela éliminera les runts.

Concepts de la commutation cut-through :

- convient aux commutateurs dont la latence doit être inférieure à 10 microsecondes
- Ne vérifie pas le FCS, il peut donc propager des erreurs
- Peut entraîner des problèmes de largeur de bande si le commutateur propage trop d'erreurs
- Ne peut pas prendre en charge les ports dont les vitesses varient de l'entrée à la sortie

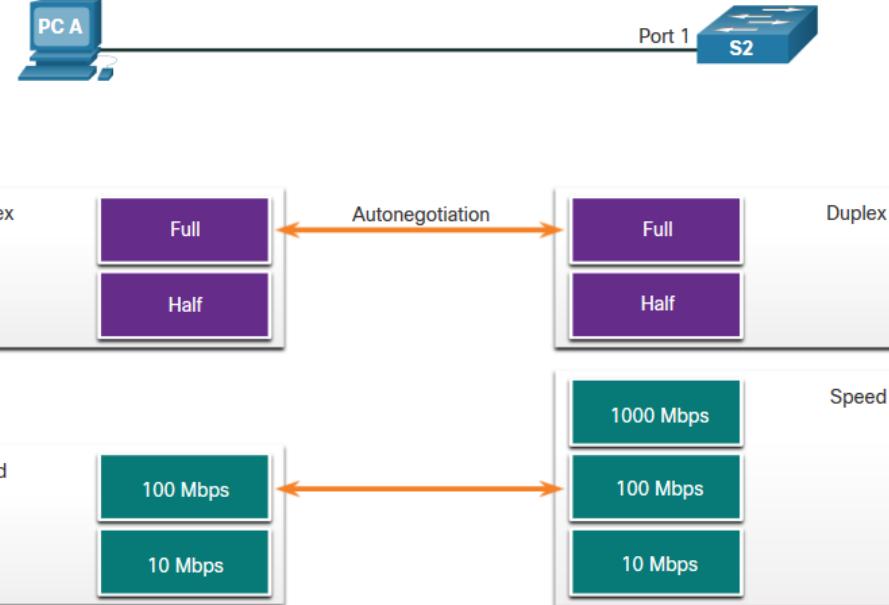
## 2.2 Domaines de commutation

## Domaines de commutation

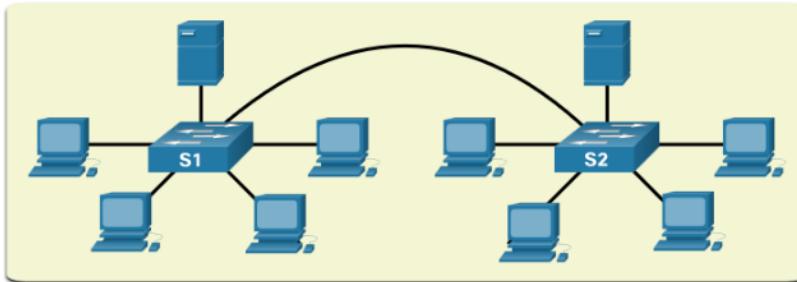
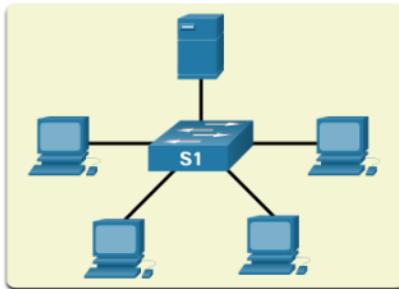
# Domaines de collision

Les commutateurs éliminent les domaines de collision et réduisent la congestion.

- Lorsqu'il y a duplex intégral sur le lien, les domaines de collision sont éliminés.
- Lorsqu'il y a un ou plusieurs périphériques en semi-duplex, il y aura désormais un domaine de collision.
  - Il y aura maintenant un conflit pour la bande passante.
  - Les collisions sont maintenant possibles.
- La plupart des appareils, y compris Cisco et Microsoft, utilisent l'auto-négociation comme paramètre par défaut pour le duplex et la vitesse.



# Domaines de diffusion



- Un domaine de diffusion s'étend sur tous les périphériques de couche 1 ou 2 d'un réseau local.
  - Seul un périphérique de couche 3 (routeur) brisera le domaine de diffusion, également appelé domaine de diffusion MAC.
  - Le domaine de diffusion MAC est constitué de tous les périphériques du réseau local qui reçoivent les trames de diffusion provenant d'un hôte.
- Lorsque le commutateur de couche 2 reçoit la diffusion, il l'inondera toutes les interfaces à l'exception de l'interface d'entrée.
- Trop de diffusions peuvent causer de la congestion et des performances réseau médiocres.
- L'augmentation des périphériques au niveau de la couche 1 ou de la couche 2 entraîne le développement du domaine de diffusion.

# Réduction de la congestion des réseaux

Les commutateurs utilisent la table d'adresses MAC et le duplex intégral pour éliminer les collisions et éviter la congestion.

Les caractéristiques de l'interrupteur qui soulagent la congestion sont les suivantes:

Protocole	Fonction
Vitesse de port rapide	Selon le modèle, les commutateurs peuvent avoir des vitesses de port allant jusqu'à 100 Gbit/s.
Commutation interne rapide	Cela utilise un bus interne rapide ou une mémoire partagée pour améliorer les performances.
Grands tampons de trame	Cela permet un stockage temporaire lors du traitement de grandes quantités de trames.
Nombre de ports élevé	Cela fournit de nombreux ports pour les périphériques à connecter au réseau local à moindre coût. Cela permet également d'augmenter le trafic local avec moins de congestion.

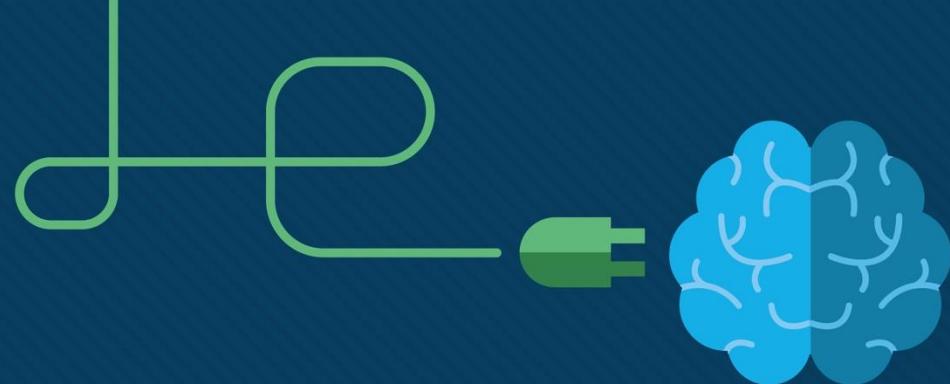
# Qu'est-ce que j'ai appris dans ce module?

## Transfert de trame

- Ingress est le port d'entrée, egress est le port de sortie.
- Le commutateur construit une table d'adresses MAC pour transférer les trames sur le réseau local.
- Le commutateur peut utiliser soit la méthode du stockage et de la retransmission, soit la méthode de la retransmission par coupure.

## Domaines de commutation

- Les ports Ethernet en semi-duplex font partie d'un domaine de collision.
- Le duplex intégral éliminera les domaines de collision.
- Un commutateur va inonder toutes les interfaces sauf le port d'entrée si la trame est une diffusion ou si le MAC de destination monodiffusion est inconnu.
- Les domaines de diffusion peuvent être fragmentés par un périphérique de couche 3, comme un routeur.
- Les commutateurs étendent les domaines de diffusion, mais peuvent éliminer les domaines de collision et soulager la congestion.



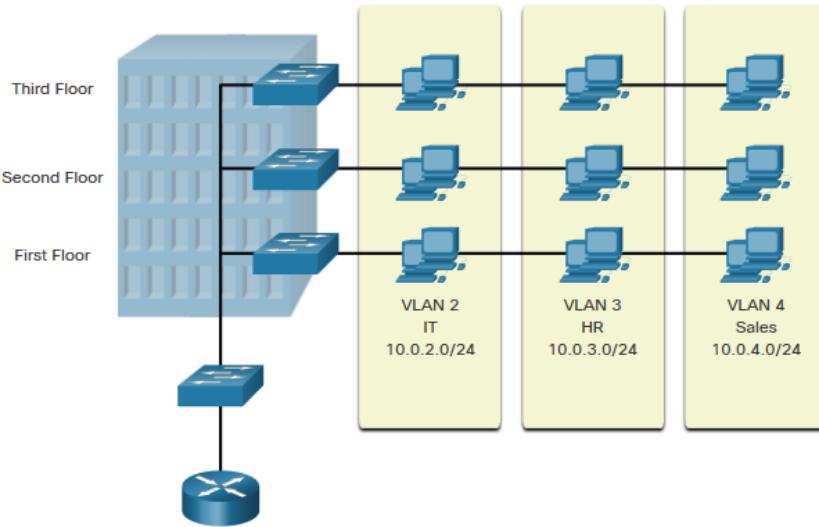
# Module 3: Les VLAN



# 3.1 Présentation des VLAN

# Présentation des VLAN

## Définitions des VLAN



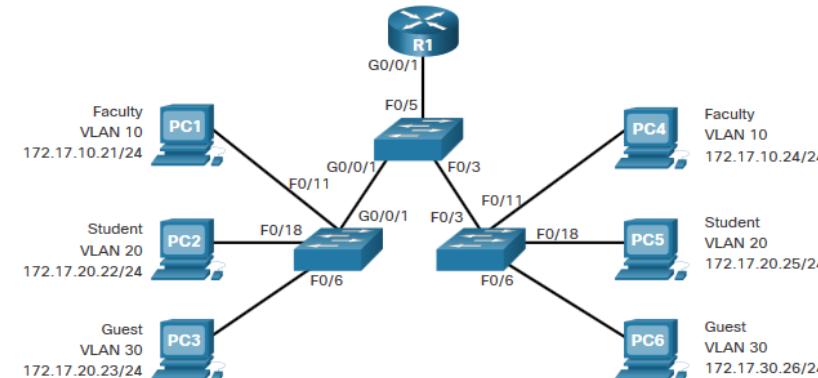
Les VLAN sont des connexions logiques avec d'autres périphériques similaires.

Le placement de périphériques dans divers VLAN présente les caractéristiques suivantes:

- Fournir la segmentation des différents groupes de périphériques sur les mêmes commutateurs
- Fournir une organisation plus facile à gérer
  - Les diffusions, les multidiffusions et les monodiffusions sont isolées dans le VLAN individuel
  - Chaque VLAN aura sa propre plage d'adressage IP unique
  - Domaines de Diffusion Plus Petits

# Avantages du concept de VLAN

Les avantages des VLAN sont les suivants:



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

## Types de VLAN

### VLAN par défaut

VLAN 1 est le suivant:

- Le VLAN par défaut
- Le VLAN natif par défaut
- VLAN de gestion par défaut
- Impossible de supprimer ou de renommer

**Remarque :** Bien que nous ne puissions pas supprimer VLAN1, Cisco recommandera d'attribuer ces caractéristiques par défaut à d'autres VLAN

Switch# show vlan brief			
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default		act/unsup
1003	token-ring-default		act/unsup
1004	fddinet-default		act/unsup
1005	trnet-default		act/unsup

# Types de VLAN (Suite)

### VLAN de données

- Dédié au trafic généré par l'utilisateur (trafic e-mail et web).
- VLAN 1 est le VLAN de données par défaut car toutes les interfaces sont attribuées à ce VLAN.

### VLAN natif

- Ceci est utilisé uniquement pour les liaisons de trunk.
- Toutes les trames sont marquées sur une liaison de trunk 802.1Q, à l'exception de celles sur le VLAN natif.

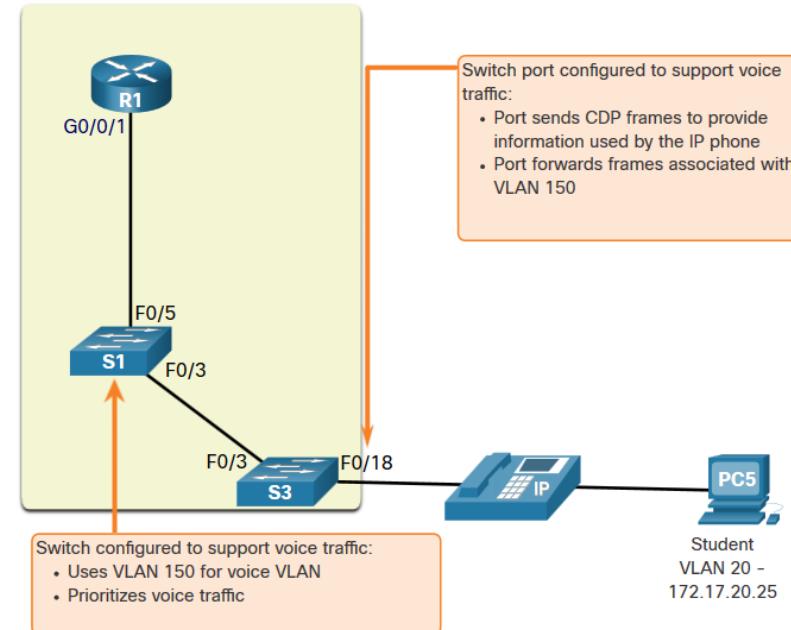
### VLAN de gestion

- Ceci est utilisé pour le trafic SSH/TelNet VTY et ne doit pas être transporté avec le trafic d'utilisateur final.
- Généralement, le VLAN qui est le SVI pour le commutateur de couche 2.

## Types de VLAN (Suite)

### VLAN voix

- Un VLAN distinct est requis car le trafic de voix nécessite:
  - La bande passante consolidée
  - La priorité de QOS élevée
  - La capacité d'éviter la congestion
  - Le délai inférieur à 150 ms de la source à la destination
- L'ensemble du réseau doit être conçu pour prendre en charge la voix.



# Packet Tracer - Qui entend la diffusion?

Dans cette activité Packet Tracer, vous allez:

- Observer le trafic de diffusion dans une implémentation VLAN
- Compléter les questions de révision

# 3.2 Les VLAN dans un environnement à plusieurs commutateurs

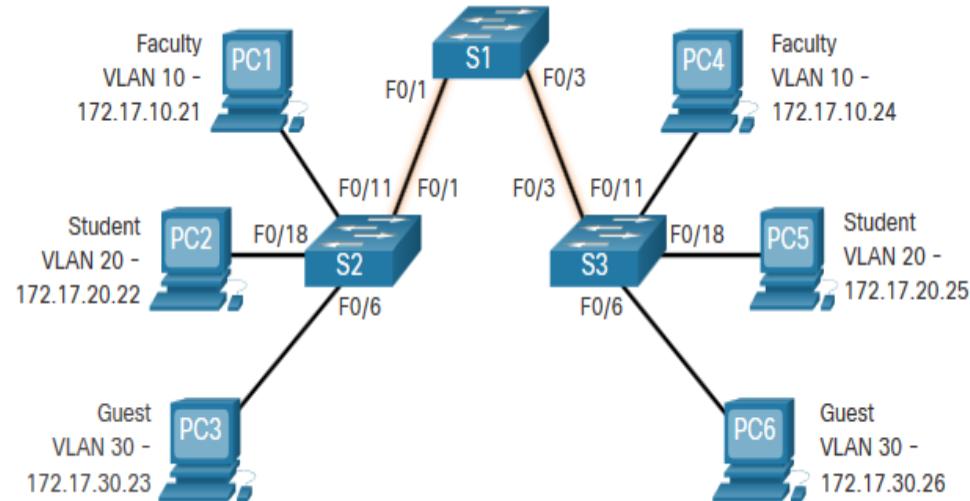
VLAN dans un environnement à plusieurs commutateurs

## Définir les trunks de VLAN

Un trunk est une liaison point à point entre deux périphériques réseau.

Fonctions du trunk Cisco :

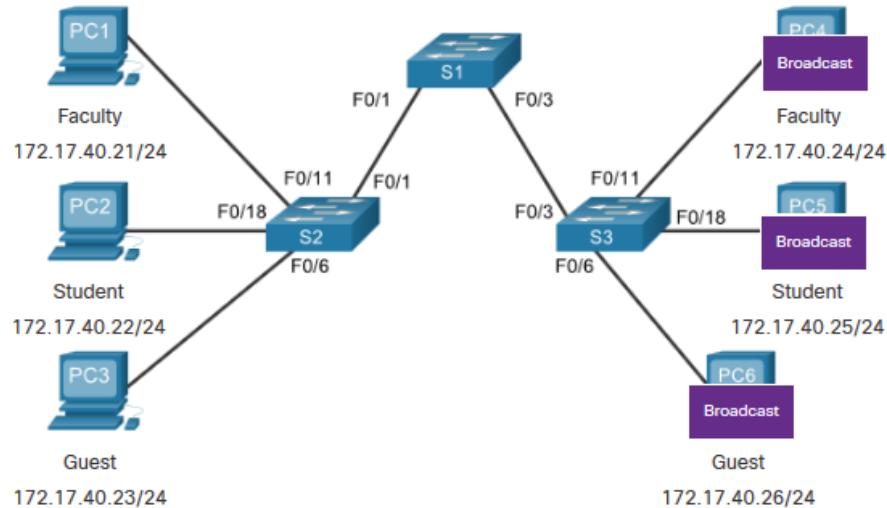
- Autoriser plusieurs VLAN
- Étendre le VLAN sur l'ensemble du réseau
- Par défaut, il prend en charge tous les VLAN
- Il prend en charge trunking 802.1Q



## Les VLAN dans un environnement à plusieurs commutateurs

# Réseaux sans VLAN

Sans VLAN, tous les périphériques connectés aux commutateurs recevront tout le trafic de monodiffusion, de multidiffusion et de diffusion.

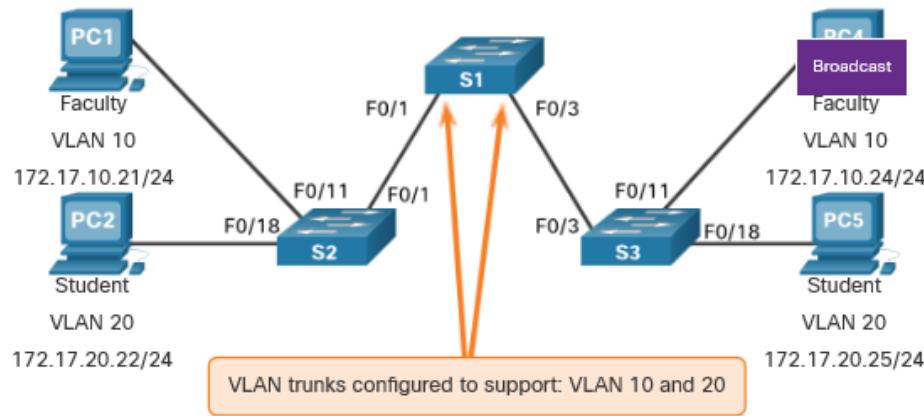


PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.

VLAN dans un environnement à plusieurs commutateurs

## Réseaux sans VLAN

Avec les VLAN, le trafic de monodiffusion, de multidiffusion et de diffusion est limité à un VLAN. Sans un périphérique de couche 3 permettant de connecter les VLAN, les périphériques de différents VLAN ne peuvent pas communiquer.



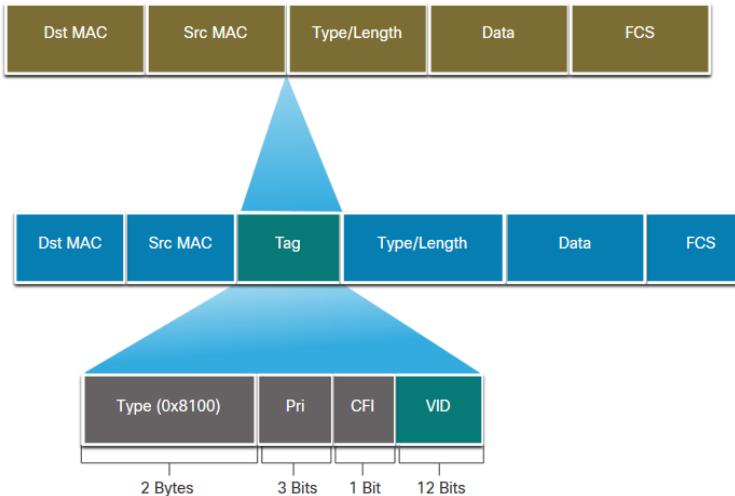
PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

ses filiales. Tous droits réservés. Informations  
isco

## VLAN dans un environnement à plusieurs commutateurs

### Identification du VLAN avec une étiquette

- L'en-tête IEEE 802.1Q est de 4 octets
- Lorsque l'étiquette est créée, le FCS doit être recalculé.
- Lorsqu'elle est envoyée aux périphériques terminaux, cette étiquette doit être supprimée et le FCS doit être recalculé pour retourner à son numéro d'origine.



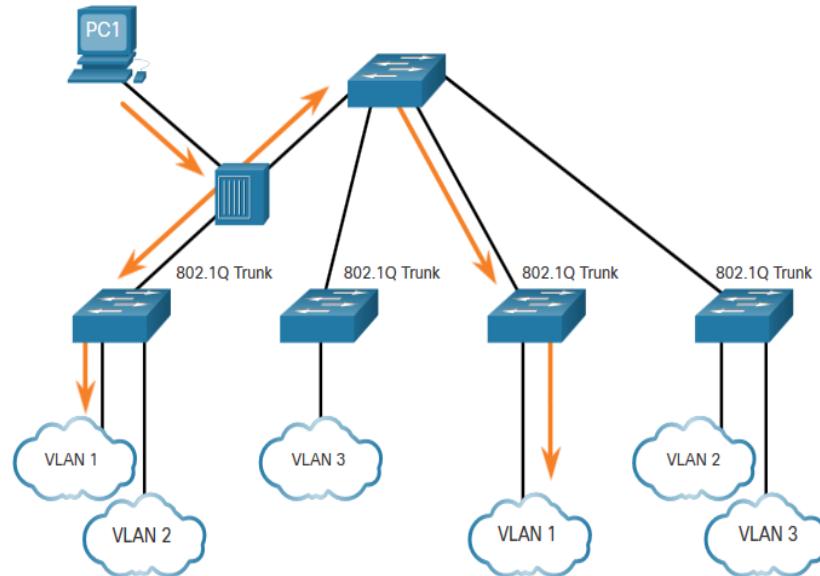
Champ d'étiquette VLAN 802.1Q	Fonction
Type	<ul style="list-style-type: none"><li>• Champ de 2 octets avec hexadécimal 0x8100</li><li>• Ceci est appelé TPID (Tag Protocol ID)</li></ul>
Priorité Utilisateur	<ul style="list-style-type: none"><li>• Valeur de 3 bits prenant en charge</li></ul>
CFI (Canonical Format Identifier)	<ul style="list-style-type: none"><li>• Identificateur de 1 bit qui prend en charge les trames Token Ring sur des liaisons Ethernet</li></ul>
ID de VLAN (VID)	<ul style="list-style-type: none"><li>• Numéro d'identification VLAN de 12 bits qui prend en charge jusqu'à 4096 ID de VLAN.</li></ul>

VLAN dans un environnement à plusieurs commutateurs

## VLAN natifs et étiquetage 802.1Q

trunk de base 802.1Q:

- Étiquetage est généralement effectué sur tous les VLAN.
- L'utilisation d'un VLAN natif a été conçue pour une utilisation ancienne, comme le concentrateur dans l'exemple.
- Moins qu'il ne soit modifié, VLAN1 est le VLAN natif.
- Les deux extrémités d'une liaison trunk doit être configurées avec le même VLAN natif.
- Chaque trunk est configuré séparément, il est donc possible d'avoir un VLAN natif différent sur des trunks séparés.



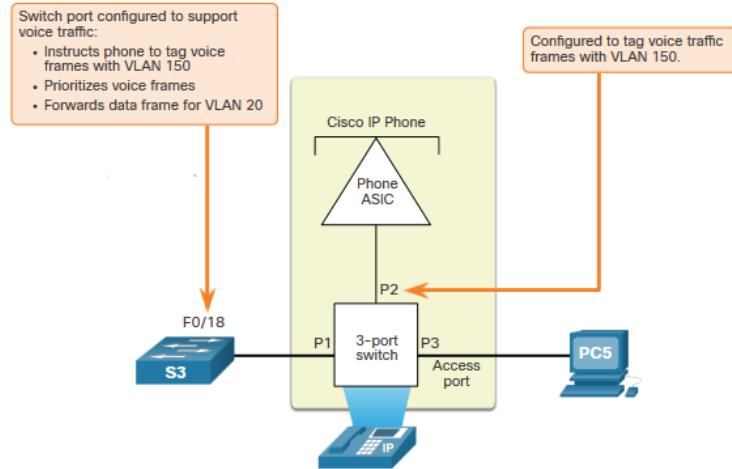
# VLAN dans un environnement à plusieurs commutateurs

## L'étiquetage du VLAN voix

Le téléphone VoIP est un commutateur à trois ports:

- Le commutateur utilisera CDP pour informer le téléphone du VLAN voix.
- Le téléphone marquera son propre trafic (Voix) et peut définir le coût du service (CoS). CoS est QoS pour la couche 2.
- Le téléphone peut ou non étiqueter les trames du PC.

Traffic	Fonction d'étiquetage
Étiquetage VLAN voix	avec une valeur appropriée de priorité CoS (Class of Service) de couche2
VLAN d'accès	peut également être étiqueté avec une valeur de priorité CoS de couche 2
VLAN d'accès	n'est pas étiqueté (pas de valeur de priorité CoS de couche2)



VLAN dans un environnement à plusieurs commutateurs

## Exemple de vérification d'un VLAN voix

La commande **show interfaces fa0/18 switchport** peut nous montrer à la fois les VLAN de données et de voix attribués à l'interface.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

# 3.3 Configuration de VLAN

## Configuration de VLAN

# Plages de VLAN sur les commutateurs Catalyst

Les commutateurs Catalyst 2960 et 3560 prennent en charge plus de 4000 VLAN.

Switch# show vlan brief			
VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

### Réseaux locaux virtuels (VLAN) à plage normale compris entre 1 et 1005

Utilisé dans les petites et moyennes entreprises

la plage entre 1002 et 1005 sont réservés aux VLAN anciens

La plage entre 1, 1002 et 1005 sont créés automatiquement et ne peuvent pas être supprimés

Stocké dans le fichier `vlan.dat` en flash

VTP peut synchroniser entre les commutateurs

### Réseaux locaux virtuels (VLAN) à plage étendue comprise entre 1006 et 4095

Utilisé par les Fournisseurs de Services

Sont dans `running-config`

Prend en charge moins de caractéristiques de VLAN

Configuration VTP requise

## Configuration de VLAN

# Commandes de création de VLAN

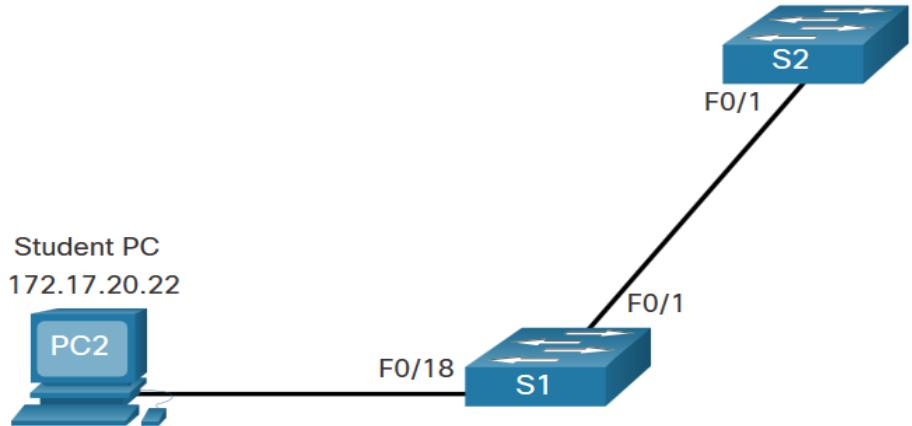
Les détails du VLAN sont stockés dans le fichier `vlan.dat`. Vous créez des VLAN en mode de configuration globale.

Tâche	Commande IOS
Passez en mode de configuration globale.	Switch# <b>configure terminal</b>
Créez un VLAN avec un numéro d'identité valide.	Switch(config)# <b>vlan vlan-id</b>
Indiquez un nom unique pour identifier le VLAN.	Switch(config-vlan)# <b>name vlan-name</b>
Repassiez en mode d'exécution privilégié.	Switch(config-vlan) # <b>end</b>
Passez en mode de configuration globale.	Switch# <b>configure terminal</b>

## Configuration de VLAN

# Exemple de création de VLAN

- Si le PC d'étudiant doit être en VLAN 20, nous allons d'abord créer le VLAN, puis le nommer.
- Si vous ne le nommez pas, le Cisco IOS lui donnera un nom par défaut de `vlan` et le numéro à quatre chiffres du VLAN. Par exemple, `vlan 0020` pour VLAN 20.



Invite	Commande
S1#	Configure terminal
S1(config)#	vlan 20
S1(config-vlan)#	name student
S1(config-vlan)#	end

# Commandes d'attribution de port à des VLAN

Une fois le VLAN est créé, nous pouvons alors l'attribuer aux interfaces correctes.

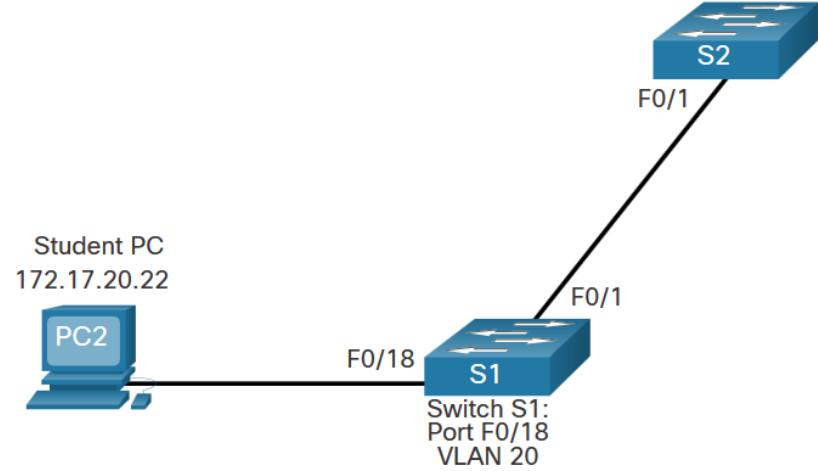
Tâche	Commande
Passez en mode de configuration globale.	Switch# <b>configure terminal</b>
Passez en mode de configuration d'interface.	Switch(config)# <b>interface interface-id</b>
Définissez le port en mode d'accès.	Switch(config-if)# <b>switchport mode access</b>
Affectez le port à un réseau local virtuel.	Switch(config-if)# <b>switchport access vlan vlan-id</b>
Repassiez en mode d'exécution privilégié.	Switch(config-if)# <b>end</b>

## Configuration de VLAN

# Exemples d'attribution de port à des

Nous pouvons attribuer le VLAN à l'interface du port.

- Une fois le VLAN est attribué au périphérique, le périphérique final aura besoin des informations d'adresse IP pour ce VLAN
- Ici, le PC de l'étudiant reçoit 172.17.20.22

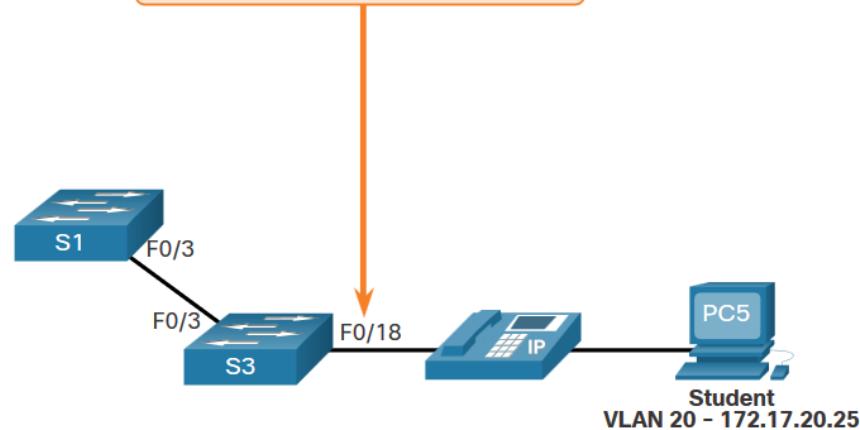


Invite	Commande
S1#	Configure terminal
S1(config)#	Interface fa0/18
S1(config-if)#	Switchport mode access
S1(config-if)#	Switchport access vlan 20
S1(config-if)#	end

# VLAN de données et de voix

Un port d'accès ne peut être attribué qu'à un seul VLAN. Cependant, il peut également être attribué à un VLAN voix lorsqu'un téléphone et un périphérique terminal sont hors du même port de commutation.

Switchport must support VLAN traffic for:  
• Voice traffic to the IP phone  
• Data traffic to PC5



# Exemple de VLAN de données et de voix

- Nous voulons créer et nommer à la fois les VLAN de données et de voix.
- En plus d'attribuer le VLAN de données, nous allons également attribuer le VLAN de voix et activer la QoS pour le trafic de voix à l'interface.
- Le commutateur catalyst le plus récent crée automatiquement le VLAN, s'il n'existe pas déjà, lorsqu'il est affecté à une interface.

**Remarque:** l'implémentation de la QoS dépasse le cadre de ce cours. Ici, nous montrons l'utilisation de la commande **mls qos trust [cos | device cisco-phone | dscp | ip-precedence]**.

```
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# vlan 150
S1(config-vlan)# name VOICE
S1(config-vlan)# exit
S1(config)# interface fa0/18
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# mls qos trust cos
S1(config-if)# switchport voice vlan 150
S1(config-if)# end
```

```
% Access VLAN does not exist. Creating vlan 30
```

# Configuration de VLAN

## Vérifier les informations sur les VLAN

Utiliser la commande **show vlan**.

La syntaxe complète est :

```
show vlan [brief | id vlan-id | name  
          vlan-name | summary]
```

```
S1# show vlan summary
Number of existing VLANs : 7
Number of existing VTP VLANs : 7
Number of existing extended VLANs : 0
```

```
S1# show interface vlan 20
Vlan20 is up, line protocol is up
  Hardware is EtherSVI, address is 001f.6ddb.3ec1 (bia 001f.6ddb.3ec1)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set

(Output omitted)
```

Tâche	Option de commande
Afficher une ligne pour chaque VLAN comportant le nom du VLAN, son état et ses ports.	<b>brief</b>
Afficher des informations sur un VLAN identifié par un ID de VLAN.	<b>id <i>vlan-id</i></b>
Afficher des informations sur un VLAN identifié par un nom de VLAN. Le <i>nom de VLAN</i> est une chaîne ASCII de 1 à 32 caractères de long.	<b>name <i>vlan-name</i></b>
Afficher les informations récapitulatives sur le VLAN.	<b>résumé</b>

# Configuration de VLAN

## Modification de l'appartenance des ports aux VLAN

Il existe plusieurs façons de modifier l'appartenance des ports aux VLAN:

- saisissez à nouveau la commande **switchport access vlan *vlan-id***
- utilisez la commande **no switchport access vlan** pour replacer l'interface sur VLAN 1

Utilisez les commandes **show vlan brief** ou **show interface fa0/18 switchport** pour vérifier l'association correcte de VLAN.

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# show vlan brief
VLAN Name          Status    Ports
---- -
1    default        active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                           Gi0/1, Gi0/2
20   student         active
1002 fddi-default    act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default   act/unsup
```

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

# Suppression de VLAN

Supprimez les VLAN avec la commande **no vlan *vlan-id***.

**Attention:** Avant de supprimer un VLAN, réaffectez tous les ports membres à un autre VLAN.

- Supprimez tous les VLAN avec les commandes **delete flash:vlan.dat** ou **delete vlan.dat** .
- Rechargez le commutateur lors de la suppression de tous les VLAN.

**Remarque:** Pour restaurer la valeur par défaut d'usine, débranchez tous les câbles de données, effacez la configuration de démarrage et supprimez le fichier *vlan.dat*, puis rechargez le périphérique.

# Packet Tracer - Configuration de VLAN

Dans cette activité Tracer de paquets, vous allez effectuer les opérations suivantes:

- Vérifier la configuration des réseaux locaux virtuels (VLAN) par défaut
- Configurer les VLAN
- Attribuer les VLAN aux ports
- LAB01.1-VLAN
- LAB01.2-VLAN

# 3.4 Agrégations de VLAN

# Commandes de configuration de trunk

Configurez et vérifiez les trunks VLAN. Les trunks sont de couche 2 et transportent le trafic pour tous les VLAN.

Tâche	Commande IOS
Passez en mode de configuration globale.	Switch# <b>configure terminal</b>
Passez en mode de configuration d'interface.	Switch(config)# <b>interface interface-id</b>
Réglez le port en mode de liaison permanent.	Switch(config-if)# <b>switchport mode trunk</b>
Choisissez un VLAN natif autre que le VLAN 1	Switch(config-if)# <b>switchport trunk native vlan vlan-id</b>
Indiquez la liste des VLAN autorisés sur la liaison trunk.	Switch(config-if)# <b>switchport trunk allowed vlan vlan-list</b>
Repassiez en mode d'exécution privilégié.	Switch(config-if)# <b>end</b>

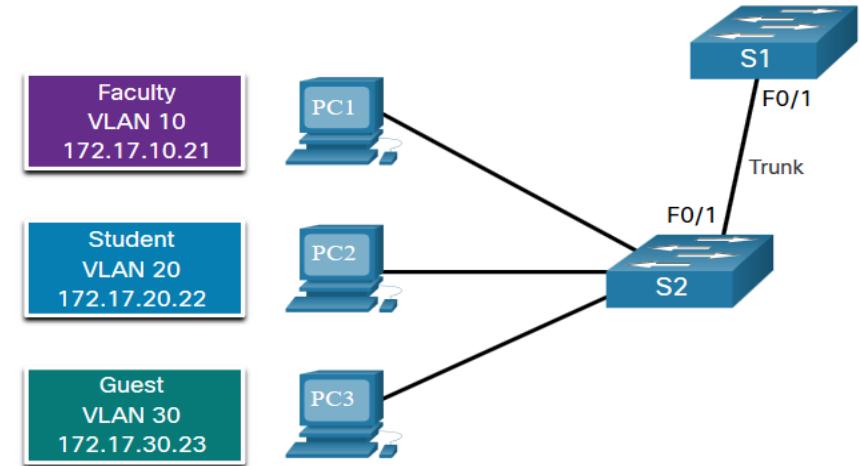
# Exemple de configuration de trunk

Les sous-réseaux associés à chaque VLAN sont:

- VLAN 10 - Faculté/Personnel - 172.17.10.0/24
- VLAN 20 - Étudiants - 172.17.20.0/24
- VLAN 30 - Invités - 172.17.30.0/24
- VLAN 99 - Natif - 172.17.99.0/24

Le port F0/1 sur S1 est configuré en tant que port de trunk.

**Remarque :** Ceci suppose un commutateur 2960 utilisant l'étiquetage 802.1q. Les commutateurs de couche 3 nécessitent que l'encapsulation soit configurée avant le mode trunk.



Invite	Commande
S1(config)#	Interface fa0/1
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)#	end

## Vérifier la configuration du trunk

Définissez le mode de trunk et le vlan natif.

Remarquez la commande **sh int fa0/1 switchport** :

- Est défini sur le trunk administrativement
- Est défini comme trunk opérationnel (fonctionnement)
- L'encapsulation est dot1q
- VLAN natif défini sur VLAN 99
- Tous les VLAN créés sur le commutateur transmettront le trafic sur ce trunk

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

# Réinitialisation du trunk à l'état par défaut

- Réinitialisez les paramètres de trunk par défaut avec la commande "no".
- Tous les VLAN sont autorisés à transmettre le trafic
- VLAN natif = VLAN 1
- Vérifiez les paramètres par défaut à l'aide de la commande **sh int fa0/1 switchport**.

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

# Réinitialisation du trunk à l'état par défaut (Suite)

Réinitialisez le trunk à un mode d'accès à l'aide de la commande **switchport mode access** :

- Est défini sur une interface d'accès administrativement
- Est défini comme une interface d'accès opérationnelle (fonctionnement)

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
(output omitted)
```

## Packet Tracer - Configuration de trunk

Dans cette activité Packet Tracer, vous allez effectuer les opérations suivantes:

- Vérifier des VLAN
- Configurer des trunks
- **LAB02-VLAN**

# 3.5 Protocole DTP (Dynamic Trunking Protocol)

# Présentation au protocole DTP

Le protocole DTP (Dynamic Trunking Protocol) est un protocole de Cisco propriétaire.

Les caractéristiques de protocole DTP sont les suivantes:

- Activé par défaut sur les commutateurs Catalyst 2960 et 2950
- Dynamic-auto est par défaut sur les commutateurs 2960 et 2950
- Peut être désactivé avec la commande `nonegotiate`
- Peut être réactivé en réglant l'interface sur `dynamic-auto`
- La définition d'un commutateur sur un trunk statique ou un accès statique évitera les problèmes de négociation avec la commande **switchport mode trunk** ou **switchport mode access** .

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

```
S1(config-if)# switchport mode dynamic auto
```

# Modes d'interface négociés

La commande **switchport mode** comporte des options supplémentaires.

Utilisez la commande de configuration d'interface **switchport nonegotiate** pour arrêter la négociation DTP.

Option	Description
accès	Mode d'accès permanent et négocie pour convertir le lien voisin en un lien d'accès
Dynamique Automatique	l'interface devient un trunk si l'interface voisine est configurée en mode trunk inconditionnel ou souhaitable.
dynamique souhaitable	Cherche activement à devenir un trunk en négociant avec d'autres interfaces automatiques ou souhaitables
trunk	Mode de trunking permanent avec négociation pour convertir le liaison voisin en liaison trunk

# Résultats d'une configuration du protocole DTP

Les options de configuration du protocole DTP sont les suivantes:

	Dynamique Automatique	Dynamique souhaitable	Trunk	Accès
Dynamique Automatique	Accès	Trunk	Trunk	Accès
Dynamique souhaitable	Trunk	Trunk	Trunk	Accès
Trunk	Trunk	Trunk	Trunk	Connectivité limitée
Accès	Accès	Accès	Connectivité limitée	Accès

# Vérifier le mode du protocole DTP

La configuration du protocole DTP par défaut dépend de la version et de la plate-forme de Cisco IOS.

- Utilisez la commande **show dtp interface** pour déterminer le mode DTP actuel.
- La meilleure pratique recommande que les interfaces soient configurées pour l'accès ou le trunk et pour passer au PAO

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

## Packet Tracer - Configuration de protocole DTP

Dans cette activité Packet Tracer, vous allez effectuer les opérations suivantes:

- Configurer le trunking statique
- Configurer et vérifier le protocole DTP
- **LAB03.1-DTP**
- **LAB03.2-DTP**
-

# 3.6 Module pratique et questionnaire

## Qu'est-ce que j'ai appris dans ce module?

- Les VLAN reposent sur des connexions logiques au lieu de connexions physiques.
- Les VLAN peuvent segmenter des réseaux selon la fonction de l'équipe ou de l'application.
- Chaque VLAN est considéré comme un réseau logique distinct.
- Un trunk est une liaison point à point qui porte plusieurs VLAN.
- Les champs d'étiquette VLAN comprennent le type, la priorité de l'utilisateur, la CFI et le VID.
- Un VLAN voix distinct est nécessaire pour prendre en charge la voix sur IP (VoIP).
- Les configurations VLAN de plage normale sont stockées dans le fichier vlan.dat en flash.
- Un port d'accès peut correspondre à un VLAN de données à la fois, mais il peut aussi avoir un VLAN voix.

## Qu'est-ce que j'ai appris dans ce module? (Cont.)

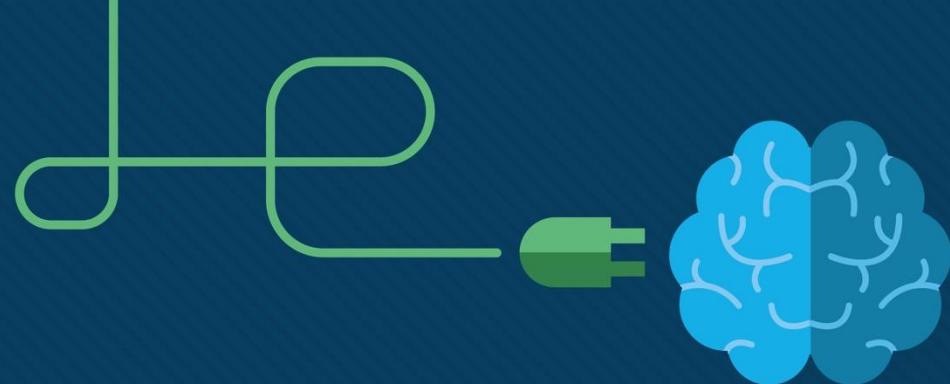
- Un trunk est une liaison de couche 2 entre deux commutateurs qui transporte le trafic pour tous les VLAN.
- Les trunks doivent être étiquetés pour les différents VLAN, généralement 802.1q.
- L'étiquetage IEEE 802.1q prévoit un VLAN natif qui ne sera pas étiqueté.
- Une interface peut être définie sur "trunking" ou "non-trunking".
- La négociation de trunk est gérée par le protocole DTP (Dynamic Trunking Protocol).
- Le protocole DTP est un protocole propriétaire de Cisco qui gère la négociation des trunks.

# Nouveaux termes et commandes

- |  |   |
|--|---|
| <ul style="list-style-type: none"><li>• VLAN</li><li>• Domaine de diffusion logique</li><li>• VLAN de données</li><li>• VLAN par défaut</li><li>• VLAN natif</li><li>• VLAN de gestion</li><li>• <b>show vlan brief</b></li><li>• VLAN voix</li><li>• Trunk de VLAN</li><li>• Segmentation d'un VLAN</li><li>• IEEE 802.1Q</li><li>• Balisage VLAN</li><li>• CFI (Canonical Format Identifier)</li></ul> | <ul style="list-style-type: none"><li>• Priorité utilisateur</li><li>• ID du réseau local virtuel</li><li>• Type</li><li>• <b>show interfaces <i>int</i> switchport</b></li></ul> |
|--|---|

# Nouveaux termes et commandes

- |   |  |  |
|---|--|--|
| <ul style="list-style-type: none"><li>• Réseaux locaux virtuels à plage normale</li><li>• Réseaux locaux virtuels à plage étendue</li><li>• <b>vlan <i>vlan-id</i></b></li><li>• <b>name <i>vlan-name</i></b></li><li>• <b>switchport mode access</b></li><li>• <b>switchport access vlan <i>vlan-id</i></b></li><li>• <b>gamme d'interfaces</b></li><li>• <b>no switchport access vlan <i>vlan-id</i></b></li><li>• <b>no vlan <i>vlan-id</i></b></li><li>• <b>delete flash:vlan.dat</b></li></ul> | <ul style="list-style-type: none"><li>• <b>delete vlan.dat</b></li><li>• <b>show vlan</b></li><li>• <b>show interfaces</b></li><li>• <b>show vlan summary</b></li><li>• <b>show interfaces vlan <i>vlan_id</i></b></li><li>• <b>switchport mode trunk</b></li><li>• <b>switchport trunk allowed vlan <i>vlan_list</i></b></li><li>• <b>switchport trunk native vlan <i>vlan_id</i></b></li><li>• <b>no switchport trunk allowed vlan</b></li></ul> | <ul style="list-style-type: none"><li>• <b>no switchport trunk native vlan</b></li><li>• <b>show interfaces switchport</b></li><li>• <b>no switchport access vlan <i>vlan_id</i></b></li><li>• <b>show interfaces trunk</b></li><li>• <b>show interfaces <i>int_id</i> trunk</b></li></ul> |
|---|--|--|



## Module 4 : Routage inter-VLAN



# Objectifs du module

**Titre du module :** Routage inter-VLAN

**Objectif du module:** Dépanner le routage inter-VLAN sur les appareils de couche 3

Titre du Rubrique	Objectif du Rubrique
<b>Fonctionnement du routage inter VLAN</b>	Décrire les options permettant de configurer le routage inter VLAN.
<b>Routage inter-VLAN avec la méthode router-on-a-stick</b>	Configurer le routage Inter-VLAN avec la méthode «Router-on-a-stick».
<b>Routage inter-VLAN à l'aide de commutateurs de couche 3</b>	Configurer le routage inter-VLAN à l'aide de la commutation de couche 3.
<b>Dépannage du routage inter-VLAN</b>	Dépanner les problèmes courants de configuration inter-VLAN

# 4.1 Fonctionnement du routage inter-VLAN

# Qu'est-ce que le routage inter-VLAN?

Les VLANs sont utilisés pour segmenter des réseaux de couche 2 commutés pour diverses raisons. Quelle que soit la raison, les hôtes d'un VLAN ne peuvent pas communiquer avec les hôtes d'un autre VLAN sauf s'il existe un routeur ou un commutateur de couche 3 pour fournir des services de routage.

Le routage inter-VLAN est un processus d'acheminement du trafic réseau d'un VLAN à un autre.

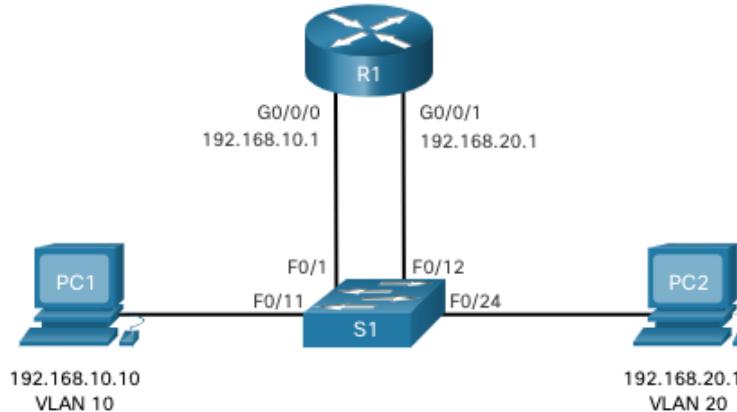
Il existe 3 options de routage inter-VLAN:

- **Routage inter-VLAN hérité** - Il s'agit d'une solution héritée. Il n'est pas bien dimensionné.
- **Router-on-a-Stick** - C'est une solution acceptable pour un réseau de petite à moyenne taille.
- **Commutateur de couche 3 utilisant des interfaces virtuelles commutées (SVI)** - Il s'agit de la solution la plus évolutive pour les moyennes et grandes entreprises.

# Fonctionnement du routage inter-VLAN

## Routage inter-VLAN hérité

- La première solution de routage inter-VLAN reposait sur l'utilisation d'un routeur avec plusieurs interfaces Ethernet. Chaque interface de routeur était connectée à un port de commutateur dans différents VLANs. Les interfaces de routeur ont servi de passerelles par défaut vers les hôtes locaux du sous-réseau VLAN.
- L'ancien routage inter-VLAN utilisant des interfaces physiques fonctionne, mais il présente une limitation importante. Il n'est pas raisonnablement évolutif car les routeurs ont un nombre limité d'interfaces physiques. La nécessité de posséder une interface de routeur physique par VLAN épuise rapidement la capacité du routeur.
- **Remarque:**Cette méthode de routage inter-VLAN n'est plus implémentée dans les réseaux commutés et est incluse à des fins d'explication uniquement.



# Routage inter VLAN Router-on-a-Stick

La méthode de routage inter-VLAN 'router-on-a-stick' surmonte la limite de la méthode de routage inter-VLAN héritée. Il ne nécessite qu'une seule interface Ethernet physique pour acheminer le trafic entre plusieurs VLANs sur un réseau.

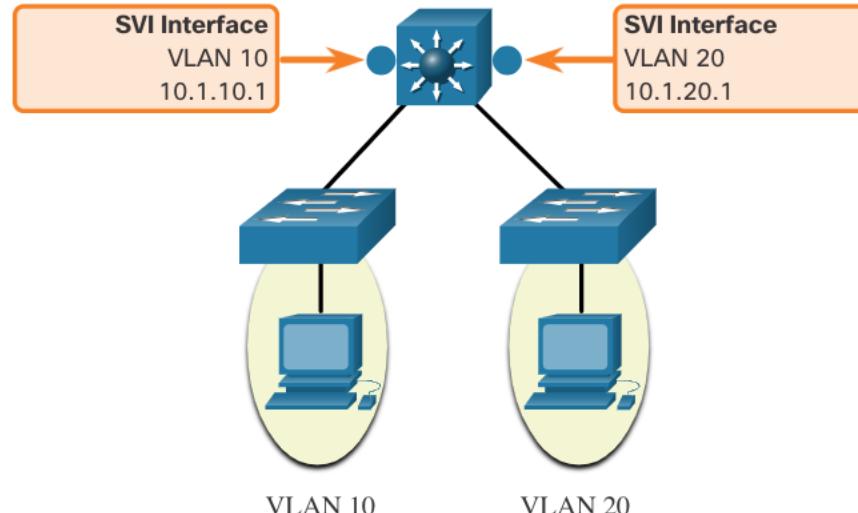
- Une interface Ethernet de routeur Cisco IOS est configurée comme un trunk 802.1Q et connectée à un port de trunk sur un commutateur de couche 2. Plus précisément, l'interface du routeur est configurée à l'aide de sous-interfaces pour identifier les VLANs routables.
- Les sous-interfaces configurées sont des interfaces virtuelles logicielles. Chacune est associée à une seule interface Ethernet physique. Les sous-interfaces sont configurées dans un logiciel sur un routeur. Chaque sous-interface est configurée indépendamment avec sa propre adresse IP et une attribution VLAN. Les sous-interfaces sont configurées pour différents sous-réseaux correspondant à une attribution VLAN. Cela facilite le routage logique.
- Lorsque le trafic balisé VLAN entre dans l'interface du routeur, il est transféré à la sous-interface VLAN. Une fois qu'une décision de routage est prise en fonction de l'adresse du réseau IP de destination, le routeur détermine l'interface de sortie du trafic. Si l'interface de sortie est configurée en tant que sous-interface 802.1q, les blocs de données sont étiquetés VLAN avec le nouveau VLAN et renvoyés vers l'interface physique

**Remarque:** la méthode router-on-a-stick de routage inter-VLAN ne va pas au-delà de 50 VLAN.

# Routage inter-VLAN sur un commutateur de couche 3

La méthode moderne d'exécution du routage inter-VLAN consiste à utiliser des commutateurs de couche 3 et des interfaces virtuelles commutées (SVI). Une interface SVI est une interface virtuelle configurée dans un commutateur de couche 3, comme illustré dans la figure.

**Remarque:** Un commutateur de couche 3 est également appelé commutateur multicouche car il fonctionne sur les couches 2 et 3. Cependant, dans ce cours, nous utilisons le terme commutateur de couche 3.



# Routage inter-VLAN sur un commutateur de couche 3 (suite)

Les SVI inter-VLAN sont créés de la même manière que l'interface VLAN de gestion est configurée. Une interface SVI est créée pour chaque VLAN existant sur le commutateur. Bien que virtuel, le SVI exécute les mêmes fonctions pour le VLAN qu'une interface de routeur le ferait. Plus précisément, il assure le traitement de couche 3 des paquets vers ou depuis tous les ports de commutateur associés à ce VLAN.

Voici les avantages de l'utilisation de commutateurs de couche 3 pour le routage inter-VLAN :

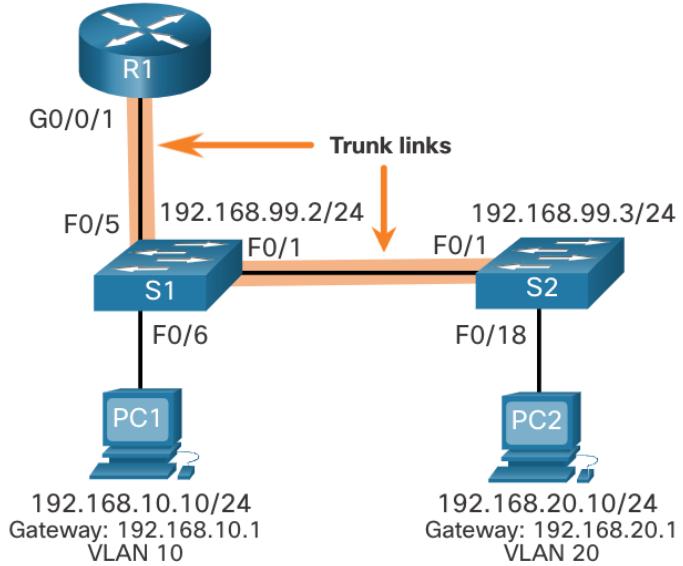
- Ils sont beaucoup plus rapides que les routeurs sur bâton car tout est commuté et acheminé par le matériel.
  - Il n'est pas nécessaire d'utiliser des liaisons externes entre le commutateur et le routeur pour le routage.
  - Ils ne sont pas limités à une liaison, car les canaux EtherChannels de couche 2 peuvent être utilisés comme liaisons de trunk entre les commutateurs pour augmenter la bande passante.
  - La latence est bien plus faible, car les données n'ont pas besoin de quitter le commutateur pour être acheminées vers un autre réseau.
  - Ils sont plus souvent déployés dans un réseau local de campus que les routeurs.
- Le seul inconvénient est que les commutateurs de couche 3 sont plus chers.

# 4.2 Routage inter-VLAN «Router-on-a-Stick»

# Router-on-a-Stick Inter-VLAN Routing

## Router-on-a-Stick Scénario

- Sur la figure, l'interface R1 GigabitEthernet 0/0/1 est connectée au port S1 FastEthernet 0/5. Le port S1 FastEthernet 0/1 est connecté au port S2 FastEthernet 0/1. Il s'agit de liaisons de trunk qui sont nécessaires pour transférer le trafic au sein des VLANs et entre ceux-ci.
- Pour router entre les VLANs, l'interface R1 GigabitEthernet 0/0/1 est logiquement divisée en trois sous-interfaces, comme indiqué dans le tableau. Le tableau indique également les trois VLANs qui seront configurés sur les commutateurs.
- Supposons que R1, S1 et S2 ont des configurations de base initiales. Actuellement, PC1 et PC2 ne peuvent pas effectuer de **ping** mutuellement parce qu'ils se trouvent sur des réseaux distincts. Seuls S1 et S2 peuvent s'envoyer des **pings** mutuellement, mais ils sont inaccessibles par PC1 ou PC2 car ils sont également sur des réseaux différents.
- Pour permettre aux périphériques de s'envoyer des pings, les commutateurs doivent être configurés avec des VLANs et des trunkings, et le routeur doit être configuré pour le routage inter-VLAN.



Sous-interfaces	VLAN	Adresse IP
G0/0/1.10	10	192.168.10.1/24
G0/0/1.20	20	192.168.20.1/24
G0/0/1.30	99	192.168.99.1/24

# Configuration du VLAN S1 et du trunking

Effectuez les étapes suivantes pour configurer S1 avec les VLANs et le trunking :

- **Étape 1.** Créez et nommez les VLANs.
- **Étape 2.** Créez l'interface de gestion.
- **Étape 3.** Configurer les ports d'accès
- **Étape 4.** Configurez les ports trunk.

# Configuration du VLAN S2 et du trunking

La configuration de S2  
est similaire à S1.

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar  1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

# Configuration de la sous-interface R1

La méthode «Router-on-a-Stick» impose de créer des sous-interfaces pour chaque VLAN routable. Une sous-interface est créée à l'aide de la commande **interface interface\_id subinterface\_id** en mode global de configuration . La syntaxe de sous-interface est l'interface physique suivie d'un point et d'un numéro de sous-interface. Bien que ce n'est pas obligatoire, il est habituel de faire correspondre le numéro de la sous-interface avec le numéro de VLAN.

Chaque sous-interface est ensuite configurée avec les deux commandes suivantes :

- **encapsulation dot1q vlan\_id [native]** - Cette commande configure la sous-interface pour répondre au trafic encapsulé 802.1Q à partir du *vlan-id* spécifié. L'option de mot-clé **natif** est uniquement ajoutée pour définir le VLAN natif sur autre chose que VLAN 1.
- **ip address ip-address subnet-mask** - Cette commande configure l'adresse IPv4 de la sous-interface. Cette adresse sert généralement de passerelle par défaut pour le VLAN identifié.

Répétez le processus pour chaque VLAN à router. Une adresse IP sur un sous-réseau unique doit être attribuée à chaque sous-interface de routeur pour que le routage se produise. Lorsque toutes les sous-interfaces ont été créées, activez l'interface physique en utilisant la commande de configuration de l'interface **no shutdown** . Si l'interface physique est désactivée, toutes les sous-interfaces sont également désactivée.

# Configuration de la sous-interface R1 (suite)

Dans la configuration, les sous-interfaces R1 G0/0/1 sont configurées pour les VLANs 10, 20 et 99.

```
R1(config)# interface G0/0/1.10
R1(config-subif)# Description Default Gateway for VLAN 10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# ip add 192.168.10.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.20
R1(config-subif)# Description Default Gateway for VLAN 20
R1(config-subif)# encapsulation dot1Q 20
R1(config-subif)# ip add 192.168.20.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1.99
R1(config-subif)# Description Default Gateway for VLAN 99
R1(config-subif)# encapsulation dot1Q 99
R1(config-subif)# ip add 192.168.99.1 255.255.255.0
R1(config-subif)# exit
R1(config)#
R1(config)# interface G0/0/1
R1(config-if)# Description Trunk link to S1
R1(config-if)# no shut
R1(config-if)# end
R1#
*Sep 15 19:08:47.015: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Sep 15 19:08:50.071: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Sep 15 19:08:51.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
R1#
```

# Vérifier la connectivité entre PC1 et PC2

La configuration du «Router-on-a-Stick» est terminée après la configuration du trunk du commutateur et des sous-interfaces du routeur. La configuration peut être vérifiée à partir des hôtes, du routeur et du commutateur.

À partir d'un hôte, vérifiez la connectivité à un hôte d'un autre VLAN à l'aide de la commande **ping**. Il est conseillé de vérifier d'abord la configuration actuelle de l'adresse IP de l'hôte à l'aide de la commande Windows host **ipconfig**.

Ensuite, utilisez **ping** pour vérifier la connectivité avec PC2 et S1, comme indiqué sur la figure. La sortie **ping** confirme avec succès le routage inter-VLAN.

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss).
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
C:\Users\PC1> ping 192.168.99.2
Pinging 192.168.99.2 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 192.168.99.2: bytes=32 time=2ms TTL=254
Reply from 192.168.99.2: bytes=32 time=1ms TTL=254
Ping statistics for 192.168.99.2:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss).
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PC1>
```

## Vérification de Routage inter-VLAN «Router-on-a-Stick»

En plus d'utiliser le **ping** entre les périphériques, les commandes **show** suivantes peuvent être utilisées pour vérifier et dépanner la configuration du «Router-on-a-Stick».

- **show ip route**
- **show ip interface brief**
- **show interfaces**
- **show interfaces trunk**

# Travaux pratiques - Configuration du routage inter-VLAN «Router-on-a-Stick»

Au cours de ces travaux pratiques, vous aborderez les points suivants:

- Partie 1: Créer le réseau et configurer les paramètres de base des périphériques
- Partie 2 : Configuration des commutateurs avec les VLANs et du trunking
- Partie 3 : Configuration du routage inter-VLAN basé sur un trunk
- **LAB04.1-Router-on-Stick**

# 4.3 Routage inter-VLAN à l'aide de commutateurs de couche 3

# Routage inter-VLAN de commutateur de couche 3

Le routage inter-VLAN utilisant la méthode router-on-a-stick est simple à mettre en œuvre pour une entreprise de petite à moyenne taille. Cependant, une grande entreprise nécessite une méthode plus rapide et beaucoup plus évolutive pour fournir le routage inter-VLAN.

Les réseaux locaux de campus d'entreprise utilisent des commutateurs de couche 3 pour fournir le routage inter-VLAN. Les commutateurs de couche 3 utilisent la commutation matérielle pour obtenir des taux de traitement de paquets plus élevés que les routeurs. Les commutateurs de couche 3 sont également couramment utilisés dans les armoires de câblage de la couche de distribution d'entreprise.

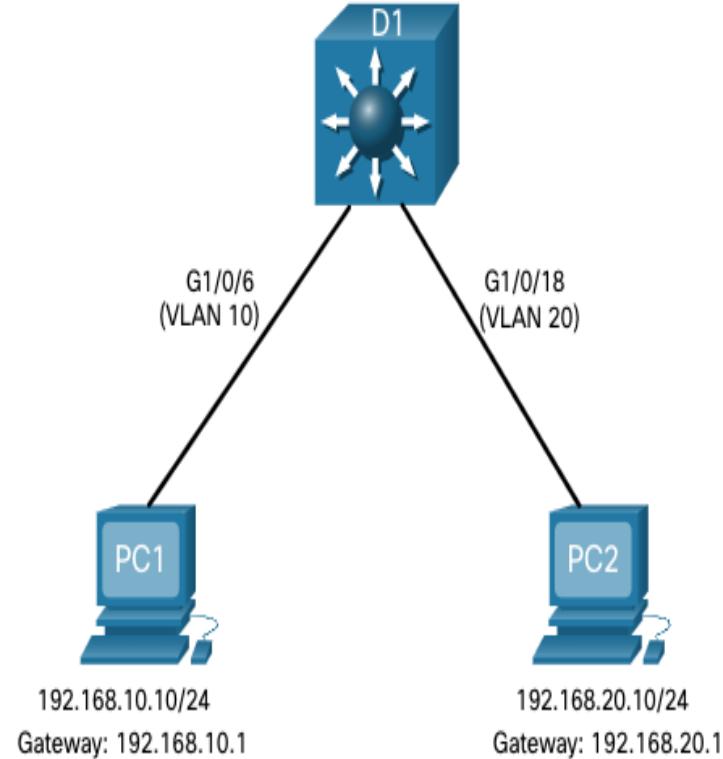
Les fonctionnalités d'un commutateur de couche 3 incluent la possibilité d'effectuer les opérations suivantes :

- Router d'un VLAN à un autre à l'aide de plusieurs interfaces virtuelles commutées (SVIs).
- Convertir un port de commutation de couche 2 en interface de couche 3 (c'est-à-dire un port routé). Un port routé est similaire à une interface physique sur un routeur Cisco IOS.
- Pour fournir le routage inter-VLAN, les commutateurs de couche 3 utilisent des SVIs. Les SVIs sont configurés à l'aide de la même commande **interface vlan *vlan-id*** utilisée pour créer le SVI de gestion sur un commutateur de couche 2. Un SVI de couche 3 doit être créé pour chacun des VLAN routables.

### Scénario de commutateur de couche 3

Sur la figure, le commutateur de couche 3, D1, est connecté à deux hôtes sur différents VLANs. PC1 est dans VLAN 10 et PC2 est dans VLAN 20, comme indiqué.

Le commutateur de couche 3 fournira des services de routage inter-VLAN vers les deux hôtes.

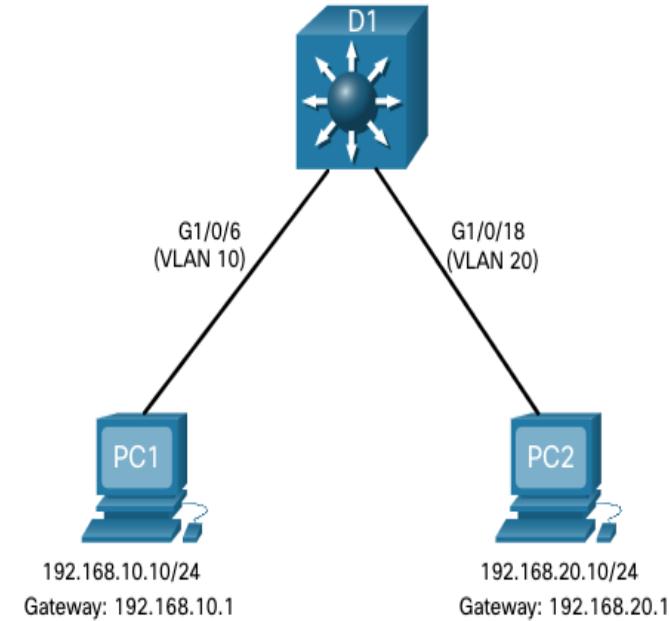


# Routage inter-VLAN à l'aide de commutateurs de couche 3

## Configuration du commutateur de couche 3

Effectuez les étapes suivantes pour configurer S1 avec les VLANs et le trunking :

- **Étape 1.** Créez les VLANs. Dans l'exemple, les VLANs 10 et 20 sont utilisés.
- **Étape 2.** Créez les interfaces VLAN SVI. L'adresse IP configurée servira de passerelle par défaut pour les hôtes du VLAN respectif.
- **Étape 3.** Configurez les ports d'accès Attribuez le port approprié au VLAN requis.
- **Étape 4.** Activez le routage IP. Émettez la commande de configuration globale **ip routing** pour permettre l'échange de trafic entre les VLANs 10 et 20. Cette commande doit être configurée pour activer le routage inter-vlan sur un commutateur de couche 3 pour IPv4.



# Vérification du routage inter-VLAN de commutateur de couche 3

Le routage inter-VLAN à l'aide d'un commutateur de couche 3 est plus simple à configurer que la méthode routeur-on-a-stick. Une fois la configuration terminée, la configuration peut être vérifiée en testant la connectivité entre les hôtes.

- À partir d'un hôte, vérifiez la connectivité à un hôte d'un autre VLAN à l'aide de la commande **ping**. Il est conseillé de vérifier d'abord la configuration actuelle de l'adresse IP de l'hôte à l'aide de la commande Windows host **ipconfig**.
- Ensuite, vérifiez la connectivité avec PC2 à l'aide de la commande Windows host **ping**. La sortie **ping** réussie confirme que le routage inter-VLAN fonctionne.

# Routage inter-VLAN à l'aide de commutateurs de couche 3

## Routage sur un commutateur de couche 3

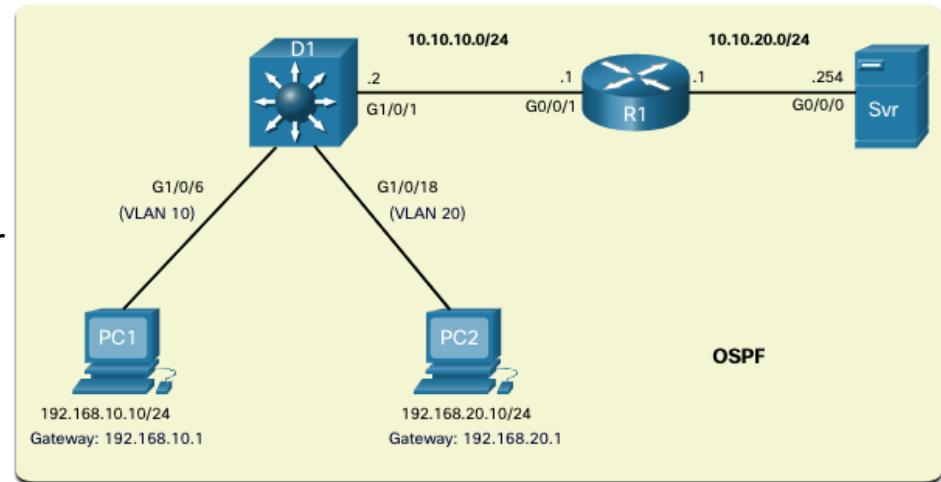
Si les VLANs doivent être accessibles par d'autres périphériques de couche 3, ils doivent être annoncés à l'aide d'un routage statique ou dynamique. Pour activer le routage sur un commutateur de couche 3, un port routé doit être configuré.

Un port routé est créé sur un commutateur de couche 3 en désactivant la fonction de port de commutation sur un port de couche 2 connecté à un autre périphérique de couche 3.

Plus précisément, la configuration de la commande de configuration de l'interface **no switchport** sur un port de couche 2 le convertit en une interface de couche 3. Ensuite, l'interface peut être configurée avec une configuration IPv4 pour se connecter à un routeur ou à un autre commutateur de couche 3.

# Scénario de routage sur un commutateur de couche 3

Dans la figure, le commutateur D1 de couche 3 configuré précédemment est maintenant connecté à R1. R1 et D1 sont tous deux dans un domaine de protocole de routage OSPF (Open Shortest Path First). Supposons qu'Inter-VLAN a été implémenté avec succès sur D1. L'interface G0/0/1 de R1 a également été configurée et activée. En outre, R1 utilise OSPF pour annoncer ses deux réseaux, 10.10.10.0/24 et 10.20.20.0/24.



**Remarque :** la configuration du routage OSPF est traitée dans un autre cours. Dans ce module, les commandes de configuration OSPF vous seront données dans toutes les activités et les évaluations. Il n'est pas nécessaire que vous compreniez la configuration pour activer le routage OSPF sur le commutateur de couche 3.

# Configuration de routage sur un commutateur de couche 3

Effectuez les étapes suivantes pour configurer D1 afin de router avec R1 :

- **Étape 1.** Configurez le port routé. Utilisez la commande **no switchport** pour convertir le port en port routé, puis attribuez une adresse IP et un masque de sous-réseau. Activez le port.
- **Étape 2.** Activez le routage. Utilisez la commande de configuration globale **ip routing** pour activer le routage.
- **Étape 3.** Configurez le routage. Utilisez une méthode de routage appropriée. Dans cet exemple, la zone unique OSPFv2 est configurée
- **Étape 4.** Vérifiez le routage. Utilisez la commande **show ip route**.
- **Étape 5.** Vérifiez la connectivité. Utilisez la commande **ping** pour vérifier l'accessibilité.

# Packet Tracer - Configurer la commutation de la couche 3 et le routage inter-VLAN

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Partie 1: Configurer la commutation de couche 3
- Partie 2: Configurer le routage inter-VLAN
- Partie 3 : Configurer le routage inter-VLAN IPv6
- **LAB04.2-Commutation\_Couche3**

# 4.4 - Dépannage du routage inter-VLAN

# Problèmes courants d'inter-VLAN

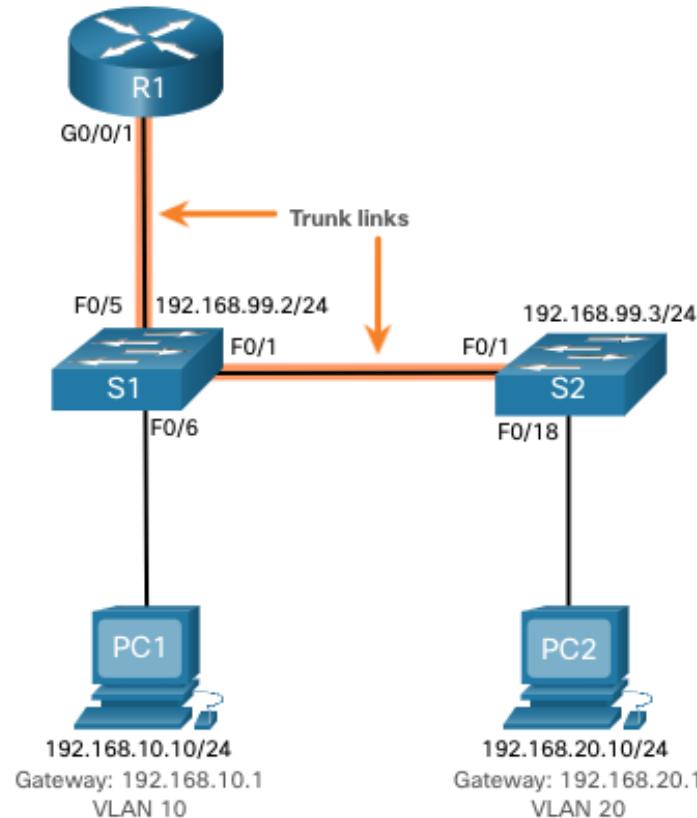
Il y a plusieurs raisons pour lesquelles une configuration inter-VLAN peut ne pas fonctionner. Tous sont liés à des problèmes de connectivité. Tout d'abord, vérifiez la couche physique pour résoudre les problèmes liés à la connexion d'un câble au mauvais port. Si les connexions sont correctes, utilisez la liste du tableau pour d'autres raisons courantes pour lesquelles la connectivité inter-VLAN peut

Type de problème	Comment réparer	Comment vérifier
VLAN manquants	<ul style="list-style-type: none"> <li>Créez (ou recréez) le VLAN s'il n'existe pas.</li> <li>Assurez-vous que le port hôte est attribué au VLAN correct.</li> </ul>	<b>show vlan [brief]</b> <b>show interfaces switchport</b> <b>ping</b>
Problèmes de port de trunk de commutateur	<ul style="list-style-type: none"> <li>Assurez-vous que les trunks sont correctement configurés.</li> <li>Assurez-vous que le port est un port de trunk et activé.</li> </ul>	<b>show interface trunk</b> <b>show running-config</b>
Problèmes liés aux ports de commutateur	<ul style="list-style-type: none"> <li>Attribuez le port au correct VLAN.</li> <li>Assurez-vous que le port est un port d'accès et activé.</li> <li>L'hôte n'est pas correctement configuré dans le mauvais sous-réseau.</li> </ul>	<b>show interfaces switchport</b> <b>show running-config interface</b> <b>ipconfig</b>
Problèmes de configuration du routeur	<ul style="list-style-type: none"> <li>L'adresse IPv4 de la sous-interface du routeur est mal configurée.</li> <li>La sous-interface du routeur est attribué à l'ID du VLAN.</li> </ul>	<b>show ip interface brief</b> <b>show interfaces</b>

# Dépanner le scénario de routage inter-VLAN

Des exemples de certains de ces problèmes de routage inter-VLAN seront maintenant abordés plus en détail. Cette topologie sera utilisée pour tous ces problèmes.

Sous-interfaces du routeur R1		
Sous-interfaces	VLAN	Adresse IP
G0/0/0.10	10	192.168.10.1/24
G0/0/0.20	20	192.168.20.1/24
G0/0/0.30	99	192.168.99.1/24



# Dépannage du routage inter-VLAN VLANs manquants

Un problème de connectivité inter-VLAN peut être causé par un VLAN manquant. Le VLAN peut être manquant s'il n'a pas été créé, s'il a été accidentellement supprimé ou s'il n'est pas autorisé sur le lien de trunk.

Lorsque vous supprimez un VLAN, tous les ports attribués à ce VLAN deviennent inactifs. Ils restent associés au VLAN (et sont par conséquent inactifs) jusqu'à ce que vous les attribuiez à un autre VLAN ou recréiez le VLAN manquant. La recréation du VLAN manquant réaffecterait automatiquement les hôtes.

Utilisez la commande **show interface *interface-id* switchport** pour vérifier l'appartenance du port à un VLAN.

CISCO

```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

# Problèmes de ports de trunk de commutation

Un autre problème pour le routage inter-VLAN inclut des ports de commutation mal configurés. Dans une solution inter-VLAN héritée, cela peut se produire lorsque le port du routeur de connexion n'est pas attribué au VLAN correct.

Cependant, avec une solution routeur sur un bâton, la cause la plus fréquente est un port de trunk mal configuré.

- Vérifiez que le port de connexion au routeur est correctement configuré en tant que lien de trunk à l'aide de la commande **show interface trunk** .
- Si ce port est absent de la sortie, examinez la configuration du port à l'aide de la commande **show running-config interface X** pour voir comment le port est configuré.

```
S1# show interface trunk
Port      Mode          Encapsulation  Status        Native vlan
Fa0/1    on            802.1q         trunking     1
Port      Vlans allowed on trunk
Fa0/1    1-4094
Port      Vlans allowed and active in management domain
Fa0/1    1,10,20,99
Port      Vlans in spanning tree forwarding state and not pruned
Fa0/1    1,10,20,99
S1#
```

# Problèmes de port d'accès au commutateur

Lorsque vous suspectez un problème avec une configuration de port d'accès du commutateur, utilisez les diverses commandes de vérification pour examiner la configuration et identifier le problème.

Un indicateur courant de ce problème est que le PC dispose de la configuration d'adresse correcte (adresse IP, masque de sous-réseau, passerelle par défaut), mais qu'il est incapable de lancer un ping sur sa passerelle par défaut.

- Utilisez la commande **show vlan brief**, **show interface X switchport** ou **show running-config interface X** pour vérifier l'attribution du VLAN de l'interface.

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

# Problèmes de configuration du routeur

Les problèmes de configuration du routeur sur un bâton sont généralement liés à des erreurs de configuration de sous-interface.

- Vérifiez l'état de la sous-interface à l'aide de la commande **show ip interface brief** .
- Vérifiez sur quel VLAN se trouve chacune des sous-interfaces. Pour ce faire, la commande **show interfaces** est utile, mais elle génère beaucoup de sortie supplémentaire non requise. La sortie de commande peut être réduite à l'aide de filtres de commande IOS. Dans cet exemple, utilisez le mot-clé **include** pour identifier que seules les lignes contenant les lettres « Gig » ou « 802.1Q »

```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```

# Packet Tracer - Dépanner le routage inter-VLAN

Dans cette activité Packet Tracer, vous remplirez les objectifs suivants:

- Partie 1: Détecter les problèmes du réseau
- Partie 2: Mettre en œuvre la solution
- Partie 3: Vérifier la connectivité réseau
- LAB04.3-Dépannage
- LAB04.4-Dépannage

# 4.5 Module pratique et questionnaire

# Qu'est-ce que j'ai appris dans ce module?

- Le routage inter-VLAN est un processus d'acheminement du trafic réseau d'un VLAN à un autre.
- Trois options comprennent le commutateur hérité, le routeur sur une clé et le commutateur de couche 3 à l'aide de SVIs.
- Pour configurer un commutateur avec VLAN et trunking, suivez les étapes suivantes : créez et nommez les VLANs, créez l'interface de gestion, configurez les ports d'accès et les ports de trunking.
- La méthode «Router-on-a-Stick» impose de créer des sous-interfaces pour chaque VLAN routable. Une sous-interface est créée à l'aide de la commande de mode global de configuration **de l'interface interface\_idsubinterface\_id**.
- Une adresse IP sur un sous-réseau unique doit être attribuée à chaque sous-interface de routeur pour que le routage se produise. Lorsque toutes les sous-interfaces ont été créées, l'interface physique doit être activée à l'aide de la commande no shutdown interface configuration.
- Les réseaux locaux de campus d'entreprise utilisent des commutateurs de couche 3 pour fournir le routage inter-VLAN. Les commutateurs de couche 3 utilisent la commutation matérielle pour obtenir des taux de traitement de paquets plus élevés que les routeurs.
- Les fonctionnalités d'un commutateur de couche 3 comprennent le routage d'un VLAN à un autre en utilisant plusieurs interfaces virtuelles commutées (SVIs) et la conversion d'un port de commutateur de couche 2 en une interface de couche 3 (c'est-à-dire un port routé).
- Pour fournir le routage inter-VLAN, les commutateurs de couche 3 utilisent des SVIs. Les SVIs sont configurés à l'aide de la même commande **interface vlan vlan-id** utilisée pour créer le SVI de gestion sur un commutateur de couche 2.

## Qu'est-ce que j'ai appris dans ce module? (Cont.)

- Pour configurer un commutateur avec VLAN et trunking, procédez comme suit : créez le VLAN, créez les interfaces VLAN SVI, configurez les ports d'accès et activez le routage IP.
- Pour activer le routage sur un commutateur de couche 3, un port routé doit être configuré. Un port routé est créé sur un commutateur de couche 3 en désactivant la fonction de port de commutation sur un port de couche 2 connecté à un autre périphérique de couche 3. L'interface peut être configurée avec une configuration IPv4 pour se connecter à un routeur ou à un autre commutateur de couche 3.
- Pour configurer un commutateur de couche 3 pour qu'il route avec un routeur, procédez comme suit : configurez le port routé, activez le routage, configurez le routage, vérifiez le routage et vérifiez la connectivité.
- Il existe un certain nombre de raisons dont la configuration inter-VLAN ne peut pas fonctionner. Tous sont liés à des problèmes de connectivité tels que des VLAN manquants, des problèmes de port de trunk de commutateur, des problèmes de port d'accès au commutateur et des problèmes de configuration du routeur.
- Un VLAN peut être manquant s'il n'a pas été créé, s'il a été supprimé accidentellement ou s'il n'est pas autorisé sur le lien de trunk.
- Un autre problème pour le routage inter-VLAN inclut des ports de commutateur mal configurés.
- Dans une solution inter-VLAN héritée, un port de commutateur mal configuré peut être causé lorsque le port du routeur de connexion n'est pas attribué au VLAN correct.

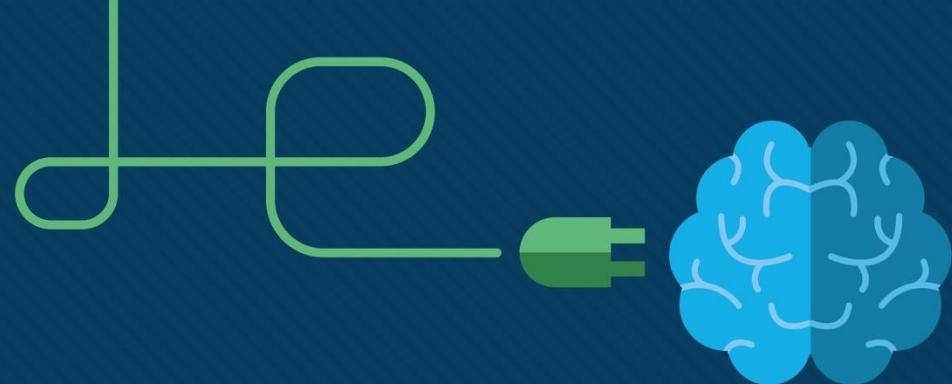


## Qu'est-ce que j'ai appris dans ce module? (Cont.)

- Avec une solution routeur sur un bâton (router-on-a-stick), la cause la plus fréquente est un port de trunk mal configuré.
- Lorsqu'un problème est suspecté avec une configuration de port d'accès de commutateur, utilisez **ping** et **show interfaces interface-id switchport** pour identifier le problème.
- Les problèmes de configuration de routeur avec les configurations de routeur sur un bâton sont généralement liés à des erreurs de configuration de sous-interface. Vérifiez l'état de la sous-interface à l'aide de la commande **show ip interface brief** .

# Nouveaux termes et commandes

- Routage inter VLAN
- Router-on-a-Stick
- **encapsulation dot1q X [ native ]**
- **no switchport**
- **router ospf**
- **ip routing**



# Module 5: Concepts du protocole STP



# Objectifs de ce module

**Titre du module:** Concepts du protocole STP

**Objectif du module:** Expliquer comment le protocole STP permet la redondance dans un réseau de couche 2.

Titre du rubrique	Objectif du rubrique
<b>Objectif du protocole STP</b>	Expliquer les problèmes courants dans un réseau commuté redondant de couche 2.
<b>Fonctionnement du protocole STP</b>	Expliquer comment le protocole STP fonctionne sur un réseau commuté.
<b>Évolution du protocole STP</b>	Expliquer le fonctionnement du protocole Rapid PVST+.

# 5.1 Objectif du protocole STP

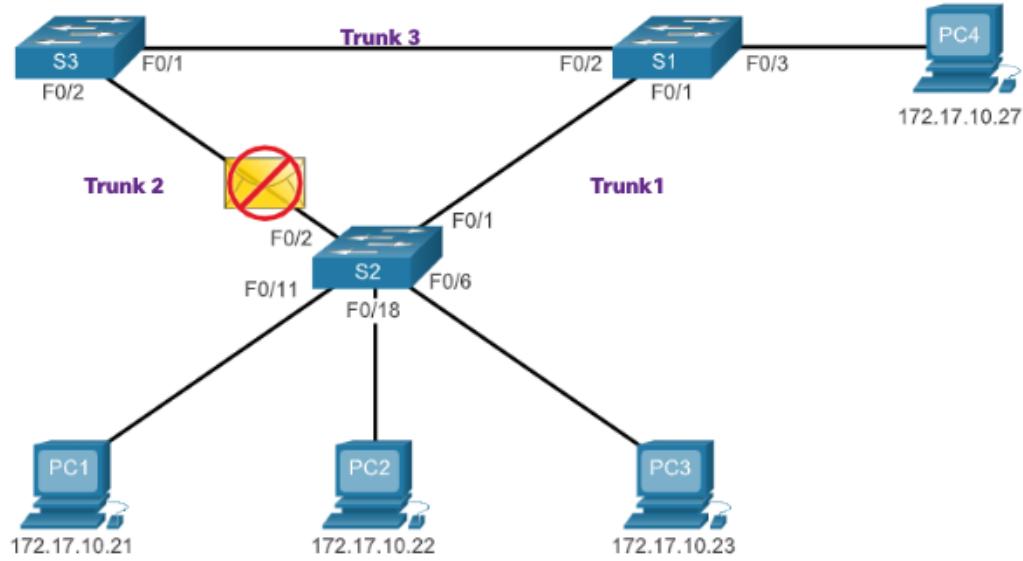
# Redondance dans les réseaux commutés de couche 2

- Cette rubrique présente les causes des boucles dans un réseau de couche 2 et explique brièvement le fonctionnement du protocole spanning tree. La redondance est un élément indispensable de la conception hiérarchique pour éviter les points de défaillance uniques et prévenir l'interruption des services de réseau fournis aux utilisateurs. Si les réseaux redondants exigent l'ajout de chemins physiques, la redondance logique doit être également intégrée à la conception. Disposer de chemins physiques alternatifs pour que les données traversent le réseau permet aux utilisateurs de toujours accéder aux ressources de ce réseau, même en cas de perturbations au niveau du chemin. Toutefois, les chemins d'accès redondants dans un réseau Ethernet commuté peuvent entraîner à la fois des boucles physiques et logiques de couche 2.
- Les réseaux locaux Ethernet nécessitent une topologie sans boucle avec un chemin unique entre deux périphériques. Une boucle dans un réseau local Ethernet peut provoquer la propagation des trames Ethernet jusqu'à ce qu'une liaison soit interrompue et rompt la boucle.

# Objectif du protocole STP

## Protocole STP (Spanning Tree Protocol)

- Le protocole STP est un protocole réseau de prévention des boucles qui permet la redondance tout en créant une topologie de couche 2 sans boucle.
- STP bloque logiquement les boucles physiques dans un réseau de couche 2, empêchant les trames d'encercler le réseau pour toujours.

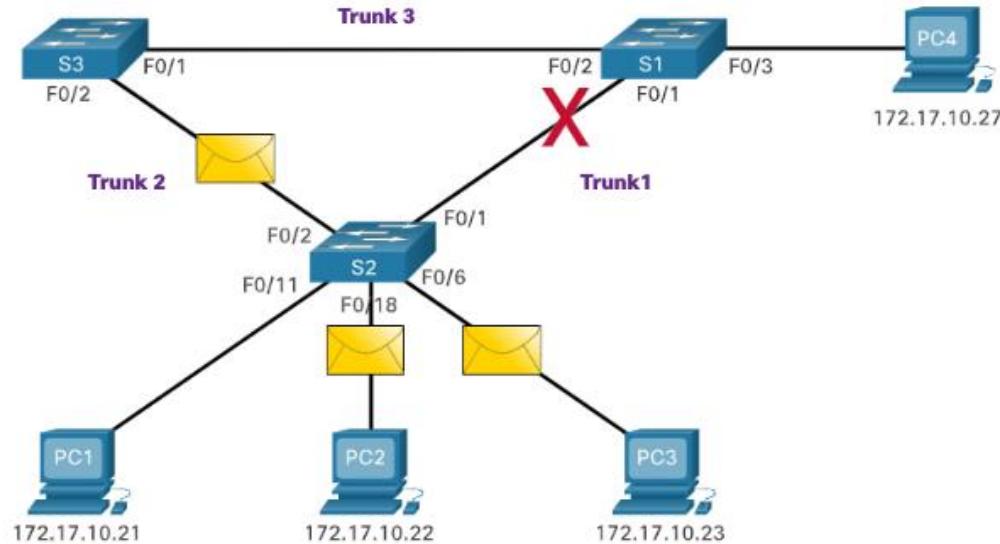


S2 drops the frame because it received it on a blocked port.

# Objectif du protocole STP

## Recalcul de STP

STP compense une défaillance du réseau en recalculant et en ouvrant les ports précédemment bloqués.



# Problèmes liés aux liaisons de commutateur redondantes

- La redondance des chemins assure de nombreux services réseau, en évitant le risque d'avoir un point de défaillance unique. Lorsqu'il existe plusieurs chemins entre deux appareils d'un réseau ethernet et que le protocole STP n'a pas été mis en œuvre sur les commutateurs, une boucle de couche 2 se produit. Une boucle de couche 2 peut entraîner l'instabilité de la table d'adresses MAC, la saturation des liaisons et une utilisation élevée de processeur sur les commutateurs et les terminaux, ce qui rend le réseau inutilisable.
- L'Ethernet de couche 2 n'intègrent pas de mécanisme pour identifier et éliminer les trames prises dans une boucle infinie. IPv4 et IPv6 comprennent tous les deux un mécanisme qui limite le nombre de fois qu'un périphérique de réseau de couche 3 est autorisé à retransmettre un paquet. Un routeur décrémentera la TTL (Time to Live) dans chaque paquet IPv4, et le champ Hop Limit dans chaque paquet IPv6. Lorsque ces champs sont décrémentés à 0, un routeur abandonne le paquet. Les commutateurs Ethernet et Ethernet n'ont pas de mécanisme comparable pour limiter le nombre de fois qu'un commutateur retransmet une trame de couche 2. Le protocole STP a été développé spécifiquement comme mécanisme de prévention des boucles pour Ethernet de couche 2.

# Boucles de couche 2

- Si le protocole STP n'est pas activé, les boucles de couche 2 peuvent se former, provoquant une boucle infinie de trames de diffusion, de multidiffusion et de monodiffusion inconnues. Cela peut faire échouer un réseau rapidement.
- Lorsqu'une boucle se produit, la table d'adresses MAC d'un commutateur changera constamment en raison des mises à jour provenant des trames de diffusion, entraînant ainsi une instabilité de la base de données MAC. Cela peut entraîner une utilisation élevée du processeur, ce qui rend le commutateur incapable de transférer des trames.
- Une trame de monodiffusion inconnue se produit lorsque le commutateur n'a pas d'adresse MAC de destination dans sa table d'adresses MAC et qu'il doit réacheminer la trame à tous les ports, sauf le port d'entrée.

# Objectif du protocole STP

## Tempête de diffusion

- Une tempête de diffusion est un nombre anormalement élevé de diffusions qui submergent le réseau pendant une durée déterminée. Les tempêtes de diffusion peuvent désactiver un réseau en quelques secondes en submergeant les commutateurs et les appareils terminaux. Les tempêtes de diffusion peuvent être provoquées par un problème matériel tel qu'une carte d'interface réseau défectueuse ou par une boucle de couche 2 dans le réseau.
- Les diffusions de couche 2 dans un réseau, telles que les demandes ARP, sont très courantes. Les multidiffusions de couche 2 sont généralement transférés de la même manière qu'une diffusion par le commutateur. Les paquets IPv6 ne soient jamais transférés en tant que diffusion de couche 2, la découverte de voisins d'ICMPv6 utilise des multidiffusions de couche 2.
- Lorsqu'un hôte est pris dans une boucle de couche 2, les autres hôtes du réseau ne peuvent pas y accéder. En outre, en raison des modifications constantes apportées à sa table d'adresses MAC, le commutateur ne sait plus à partir de quel port réacheminer les trames de monodiffusion.
- Pour empêcher ces problèmes de survenir dans un réseau redondant, un certain type de Spanning Tree doit être activé aux commutateurs. Spanning Tree est activé par défaut sur les commutateurs Cisco pour empêcher la formation de boucles de couche 2.

# L'Algorithme Spanning Tree

- STP repose sur un algorithme inventé par Radia Perlman alors qu'elle travaillait pour Digital Equipment Corporation et publié dans l'article de 1985 «An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN». Son algorithme de spanning tree (STA) crée une topologie sans boucle en sélectionnant un pont racine unique où tous les autres commutateurs déterminent un seul chemin moins coûteux.
- Le protocole STP empêche la boucle de se former en configurant un chemin sans boucle sur l'ensemble du réseau, grâce à des ports bloqués stratégiquement placés. Les commutateurs qui exécutent le protocole STP sont capables d'assurer la continuité des communications en cas de panne en débloquant dynamiquement les ports préalablement bloqués et en autorisant le trafic à emprunter les chemins de substitution.

## Objectif du protocole STP

# L'Algorithm Spanning Tree (Suite)

Comment la STA crée-t-elle une topologie sans boucle?

- **Sélection d'un pont racine:** Ce pont (commutateur) est le point de référence pour l'ensemble du réseau pour construire spanning tree.
- Les chemins redondants bloqués: Le protocole STP garantit la présence d'un seul chemin logique entre toutes les destinations sur le réseau en bloquant intentionnellement les chemins redondants susceptibles de provoquer une boucle. Un port est considéré comme bloqué lorsque les données d'utilisateur ne sont pas autorisées à entrer ou à sortir du port.
- Créer une topologie sans boucle: Un port bloqué permet de transformer ce lien en une liaison non-forwarding entre les deux commutateurs. Cela crée une topologie dans laquelle chaque commutateur n'a qu'un seul chemin vers le pont racine, semblable aux branches d'une Spanning Tree qui se connectent à la racine de Spanning Tree.
- Recalculer en cas de défaillance du lien : Les chemins physiques sont préservés pour assurer la redondance, mais ces chemins sont désactivés pour empêcher les boucles de se produire. Si le chemin est nécessaire pour compenser la défaillance d'un câble réseau ou d'un commutateur, le STP recalcule les chemins et débloque les ports nécessaires pour permettre au chemin redondant de devenir actif. Les recalculs du protocole STP peuvent également avoir lieu chaque fois qu'un nouveau commutateur ou une nouvelle liaison des commutateurs internes est ajoutée au réseau.

## Objectif du protocole STP

# Packet Tracer - Investiguer la prévention des boucles de STP

Dans cette activité Packet Tracer, vous remplirez les objectifs suivants:

- Créer et configurer un simple réseau à trois commutateurs avec STP.
- Afficher le fonctionnement du protocole STP
- Désactiver le protocole STP et afficher à nouveau l'opération.

# 5.2 Fonctionnement du protocole STP

# Étapes vers une topologie sans boucle

À l'aide de l'algorithme spanning tree (STA), le protocole STP crée une topologie sans boucle en quatre étapes:

1. Choisir le pont racine
  2. Choisir les ports racine.
  3. Choisir les ports désignés.
  4. Choisir des ports alternatifs (bloqués).
- Pendant le fonctionnement de STA et de STP, les commutateurs utilisent des BPDU (Bridge Protocol Data Units) pour partager des informations sur eux-mêmes et sur leurs connexions. Les BPDU permettent de choisir le pont racine, les ports racine, les ports désignés et les ports alternatifs.
  - Chaque trame BPDU contient un ID de pont (bridge ID) qui identifie le commutateur ayant envoyé la trame BPDU. La BID participe à la prise de nombreuses décisions STA, y compris les rôles de pont racine et de port.
  - L'ID de pont contient une valeur de priorité, l'adresse MAC du commutateur et un ID système étendu. La valeur d'ID de pont la plus basse est déterminée par une combinaison de ces trois champs.

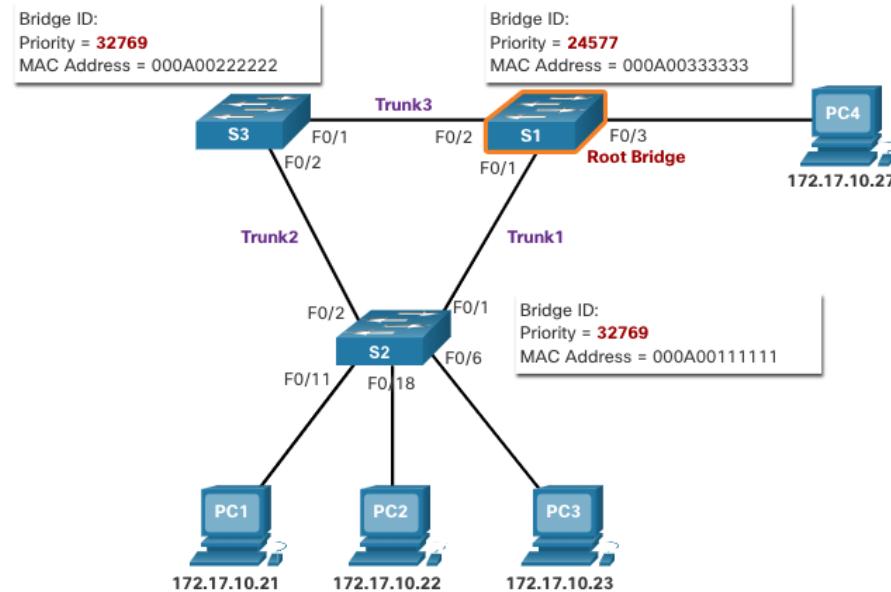
# Étapes vers une topologie sans boucle (Suite)

- **Priorité de Pont:** La valeur de priorité par défaut pour tous les commutateurs Cisco est la valeur décimale 32768. La plage va de 0 à 61440 par incrément de 4096. Une priorité de pont inférieure est préférable. Une priorité de pont de 0 a préséance sur toutes les autres priorités de pont.
- **L'ID système étendu:** La valeur de l'ID système étendu est une valeur décimale ajoutée à la valeur de priorité du pont du BID afin d'identifier le VLAN de cette BPDU.
- **Adresse MAC:** Lorsque deux commutateurs sont configurés avec la même priorité et possèdent le même ID système étendu, le commutateur dont l'adresse MAC de valeur est la plus faible, exprimée au format hexadécimal, aura le BID le plus bas.

# Fonctionnement du protocole STP

## 1. Choisir le pont racine

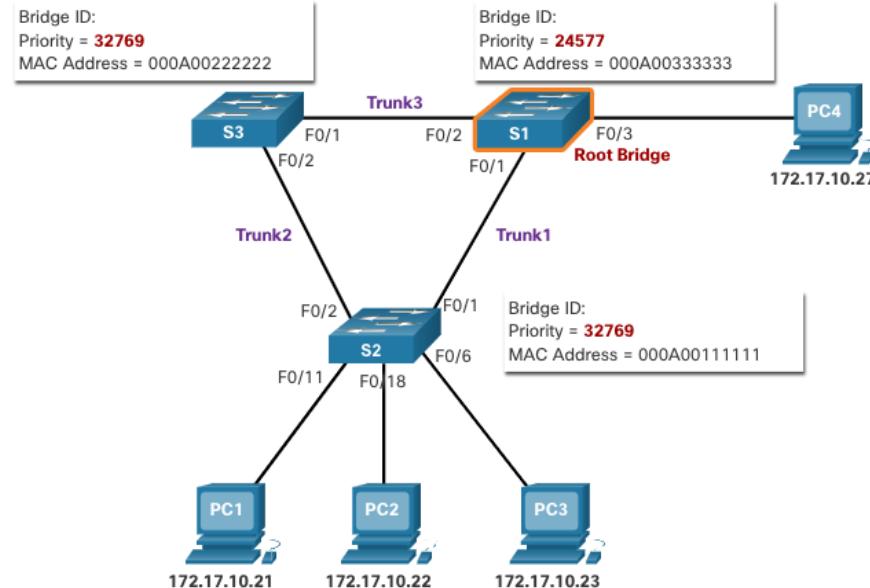
- L'algorithme STA désigne un commutateur unique comme pont racine et il l'utilise comme point de référence pour le calcul de tous les chemins. Les commutateurs échangent des BPDU pour créer la topologie sans boucle en commençant par la sélection du pont racine.
- Tous les commutateurs du domaine de diffusion participent au processus d'élection. Après son amorçage, le commutateur commence à envoyer des trames BPDU toutes les deux secondes. Ces trames BPDU contiennent la BID du commutateur d'envoi et la BID du pont racine, connue sous le nom d'ID racine.
- Le commutateur ayant l'identificateur de pont (BID) le plus bas devient le pont racine. Initialement, tous les commutateurs se déclarent en tant que pont racine avec son propre BID défini comme l'ID racine. Finalement, les commutateurs apprennent à travers l'échange de BPDU quel commutateur a la BID la plus basse et sera d'accord sur un pont racine.



## Fonctionnement du protocole STP

# Conséquences des ID de pont par défaut

- Étant donné que le BID par défaut est 32768, il est possible que deux commutateurs ou plusieurs aient la même priorité. Dans ce scénario, où les priorités sont identiques, le commutateur ayant l'adresse MAC la plus basse deviendra le pont racine. L'administrateur doit configurer le commutateur de pont racine souhaité avec une priorité inférieure.
- Dans la figure, tous les commutateurs sont configurés avec la même priorité de 32769. L'adresse MAC est alors le facteur décisif pour savoir quel commutateur deviendra le pont racine. Le commutateur dont la valeur hexadécimale est la plus basse sera choisie pour la désignation du pont racine. Dans cet exemple, S2 présente la valeur d'adresse MAC la plus basse et devient donc pont racine pour l'instance Spanning Tree.
- Remarque:** La priorité de tous les commutateurs est 32769. La valeur est basée sur la priorité de pont par défaut 32768 et l'ID système étendu (l'attribution du VLAN 1) associé à chaque commutateur (32768+1).



# Déterminer le coût du chemin racine

- Lorsque le pont racine a été choisi pour l'instance Spanning Tree, l'algorithme STA commence à déterminer des meilleurs chemins possibles vers le pont racine, depuis l'ensemble des destinations du domaine de diffusion. Les informations relatives au chemin, appelées coût du chemin racine interne, sont déterminées en additionnant les coûts de port individuels le long du chemin entre le commutateur et le pont racine.
- Lorsqu'un commutateur reçoit le BPDU, il ajoute le coût du port d'entrée du segment pour déterminer le coût de chemin racine associé.
- Les coûts du port par défaut sont définis par la vitesse de fonctionnement du port. Le tableau présente les coûts de port par défaut suggérés par IEEE. Les commutateurs Cisco utilisent par défaut les valeurs définies par la norme IEEE 802.1D, également appelée coût de chemin court, pour STP et RSTP.
- Bien qu'un coût de port par défaut soit associé aux ports des commutateurs, il est possible de configurer le coût des ports. La capacité à configurer des coûts de port individuels donne à l'administrateur la flexibilité nécessaire pour contrôler manuellement les chemins Spanning Tree vers le pont racine.

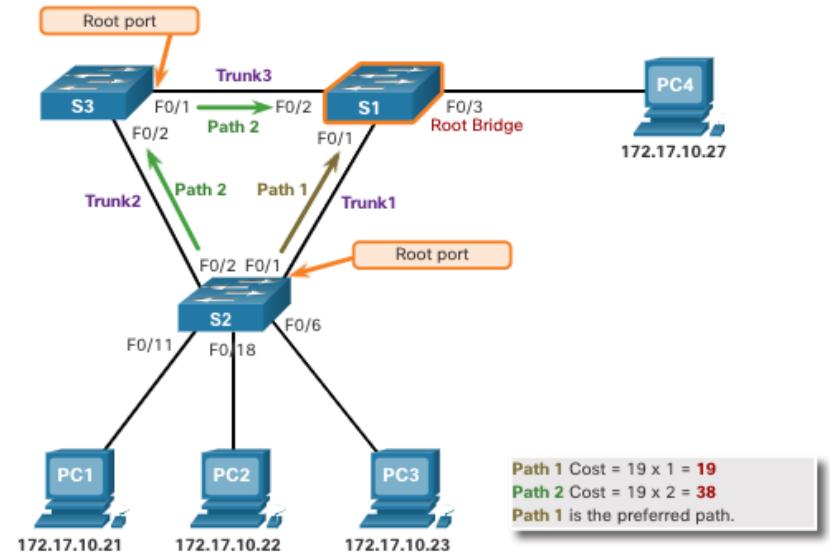
Vitesse des liens	Coût de STP: IEEE 802.1D- 1998	Coût de RSTP: IEEE 802.1w- 2004
10 Gbit/s	2	2000
1 Gbit/s	4	20000
100 Mbit/s	19	200000
10 Mbit/s	100	2000000

# Fonctionnement du protocole STP

## 2. Choisir les ports racine

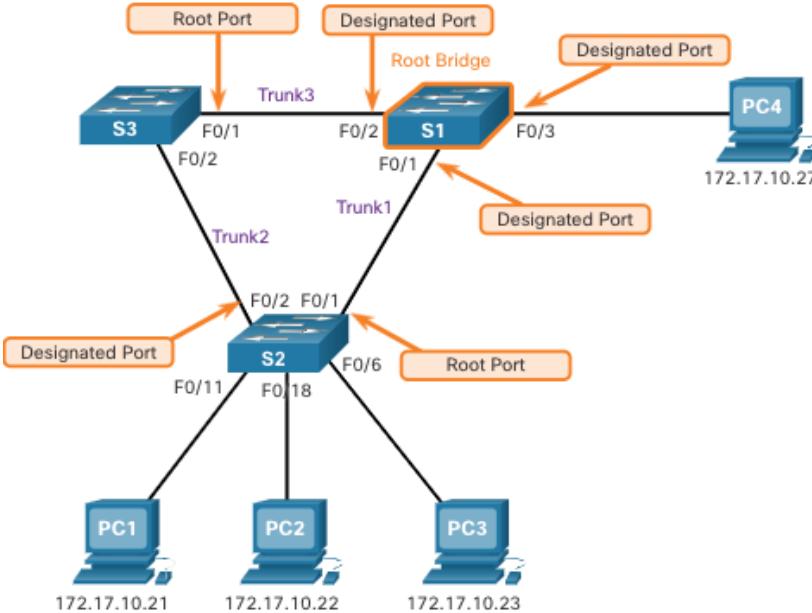
Une fois le pont racine est déterminé, l'algorithme STA est utilisé pour sélectionner le port racine. Chaque commutateur non-root sélectionnera un port racine. Le port racine est le port le plus proche du pont racine en termes de coûts généraux vers le pont racine. Ce coût global est connu sous le nom de coût du chemin racine interne.

Le coût du chemin racine interne équivaut à la somme des coûts de tous les ports le long du chemin vers le pont racine ,comme illustré sur la figure. Les chemins dont le coût est le plus bas deviennent les chemins préférés et tous les autres chemins redondants sont bloqués. Dans l'exemple, le coût du chemin racine interne de S2 au pont racine S1 sur le chemin 1 est 19 , tandis que le coût du chemin racine interne sur le chemin 2 est 38. Comme le chemin 1 a un coût de chemin global inférieur vers le pont racine, il sera choisi comme chemin principal et F0/1 devient le port racine sur S2.



### 3. Choisir les ports désignés

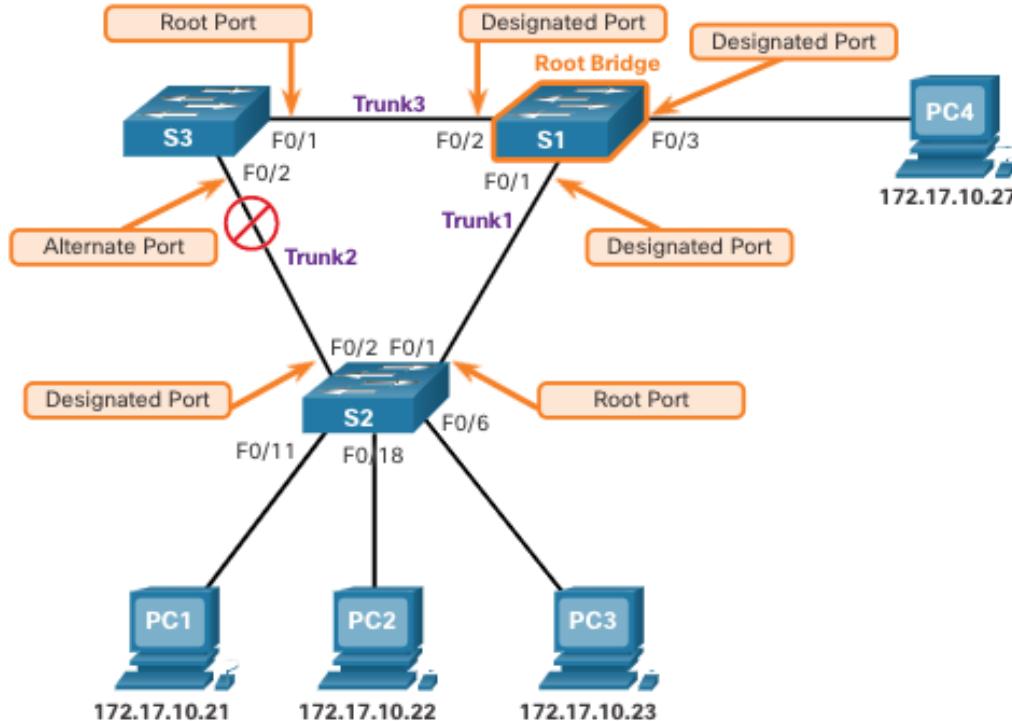
- Chaque segment entre deux commutateurs aura un port désigné. Le port désigné est un port sur le segment qui a le coût du chemin racine interne vers le pont racine. En d'autres termes, le port désigné a le meilleur chemin pour recevoir le trafic qui conduit au pont racine.
- Ce qui n'est pas un port racine ou un port désigné devient un port alternatif ou bloqué.
- Tous les ports du pont racine sont des ports désignés.
- Si l'une des extrémités d'un segment est un port racine, l'autre extrémité est un port désigné.
- Tous les ports reliés aux périphériques terminaux sont des ports désignés.
- Sur les segments entre deux commutateurs où aucun des commutateurs n'est le pont racine, le port du commutateur avec le chemin le moins coûteux vers le pont racine est un port désigné.



## 4. Choisir des ports alternatifs (bloqués)

Si un port n'est pas un port racine ou un port désigné, il devient alors un port alternatif (ou de secours). les ports alternatifs sont à l'état de suppression ou de blocage pour éviter les boucles. Dans la figure, le port Fa0/2 configuré par STA sur S3 a un rôle de port alternatif.

Le port F0/2 sur S3 est en état de blocage et ne transmet pas les trames Ethernet. Tous les autres ports inter-commutateurs sont en état de transfert. C'est la partie de STP qui permet d'empêcher la formation de boucles.



# Choisir un port racine à partir de plusieurs chemins d'accès au même coût

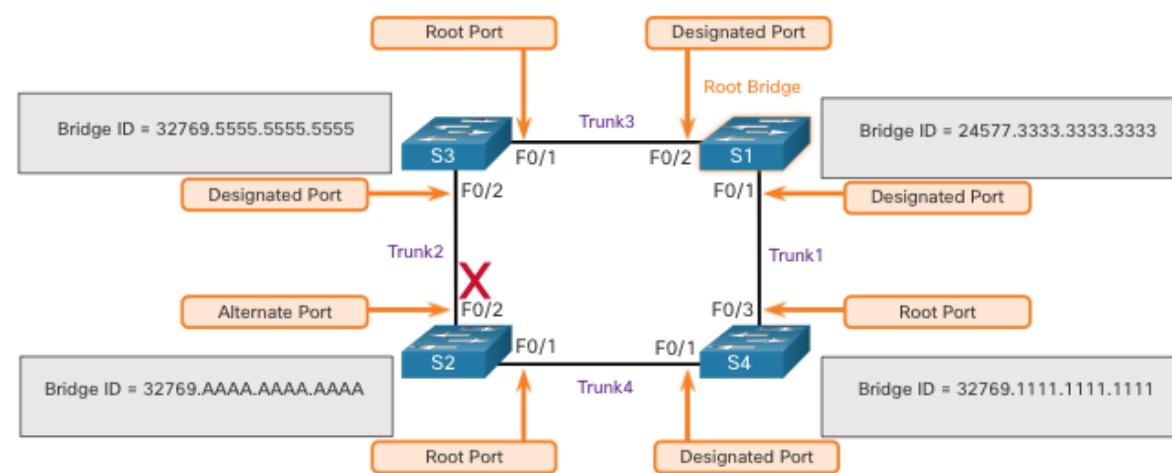
Lorsqu'un commutateur possède plusieurs chemins d'accès à coût égal vers le pont racine, le commutateur détermine un port en utilisant les critères suivants:

- ID de pont d'émetteur le plus faible
- Priorité de port le plus faible
- ID de port émetteur le plus faible

## Fonctionnement du protocole STP

# Choisir un port racine à partir de plusieurs chemins d'accès au même coût (Suite)

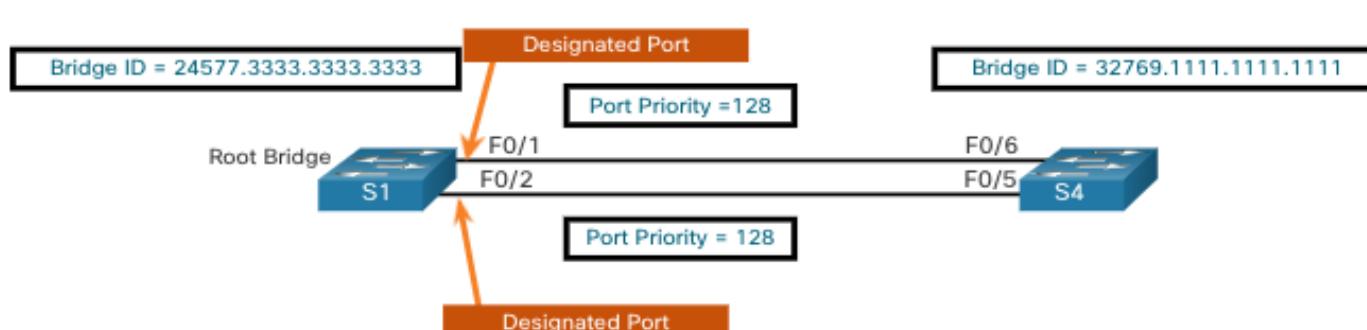
**BID d'émetteur le plus faible:** Cette topologie comporte quatre commutateurs avec le commutateur S1 comme pont racine. Le port F0/1 sur le commutateur S3 et le port F0/3 sur le commutateur S4 ont été sélectionnés comme ports racine car ils ont le coût du chemin racine vers le pont racine pour leurs commutateurs respectifs. S2 dispose de deux ports, Fa0/1 et Fa0/2, dont les chemins jusqu'au pont racine offrent le même coût. Les ID de pont des commutateurs S3 et S4 seront utilisés pour les départager. Il s'agit du BID de l'émetteur. S3 a un BID de 32769.5555.5555 et S4 a un BID de 32769.1111.1111. Puisque S4 a un BID inférieur, le port F0/1 de S2, qui est connecté à S4, sera le port racine.



# Choisir un port racine à partir de plusieurs chemins d'accès au même coût (Suite)

**Priorité de port d'émetteur le plus faible:** cette topologie comporte deux commutateurs qui sont connectés à deux chemins d'accès au même coût entre eux. S1 est le pont racine, donc ses deux ports sont des ports désignés.

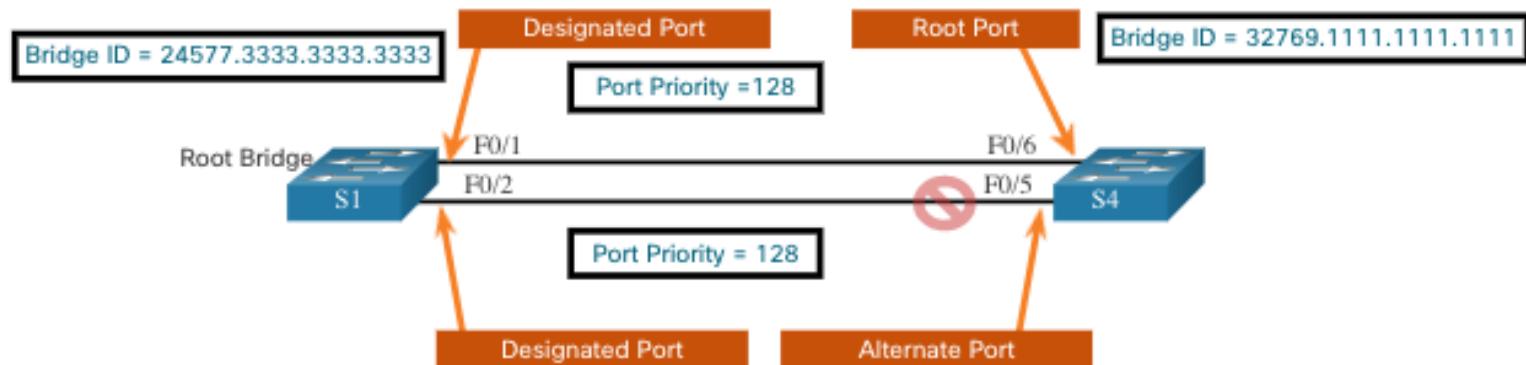
- S4 dispose de deux ports avec des chemins au même coût vers le pont racine. Comme les deux ports sont connectés au même commutateur, la BID (S1) de l'émetteur est le même. Donc, la première étape est un ex æquo.
- Ensuite, est la priorité de port de l'émetteur (S1). La priorité de port par défaut est 128, de sorte que les deux ports sur S1 ont la même priorité de port. C'est aussi un ex æquo. Toutefois, si l'un des ports de S1 était configuré avec une priorité de port inférieure, S4 mettrait son port adjacent en état de transfert. L'autre port sur S4 serait en état de blocage.



## Fonctionnement du protocole STP

# Choisir un port racine à partir de plusieurs chemins d'accès au même coût (Suite)

- **ID de port d'émetteur le plus faible:** Le dernier méthode est l'ID de port de l'émetteur le plus faible. Le commutateur S4 a reçu des BPDU du port F0/1 et du port F0/2 sur S1. La décision est basée sur l'ID de port de l'émetteur, et non sur l'ID de port du destinataire. Comme l'ID de port de F0/1 sur S1 est plus faible que du port F0/2, le port F0/6 sur le commutateur S4 sera le port racine. Il s'agit du port sur S4 qui est connecté au port Fa0/1 sur S1.
- Le port F0/5 sur S4 deviendra un port alternatif et placé dans l'état de blocage.



# STP minuteurs et les états des ports

**La convergence STP nécessite trois minuteurs, comme suit:**

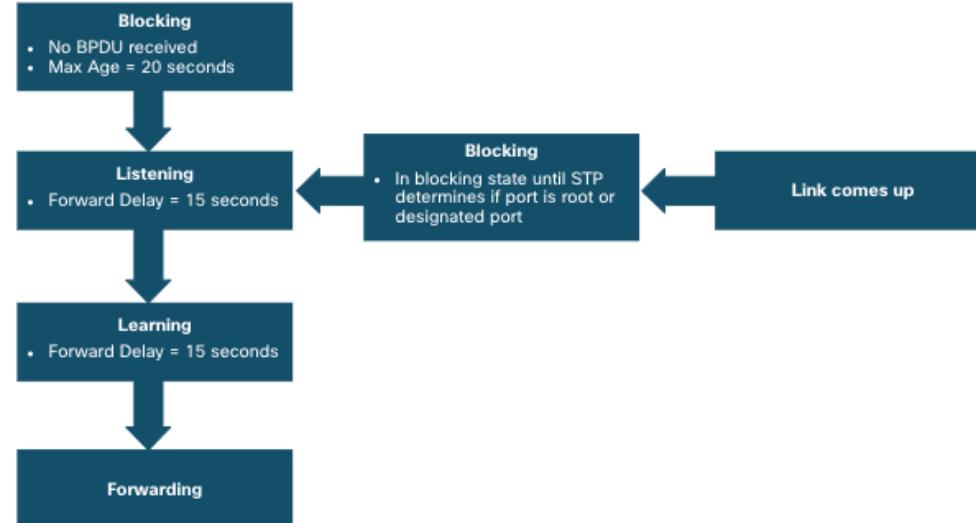
- **Minuteur Hello** -Le minuteur Hello est l'intervalle entre les BPDU. La valeur par défaut est 2 secondes, mais les valeurs autorisées peuvent être modifiées entre 1 et 10 secondes.
- **Minuteur Forward Delay** -Le minuteur Forward Delay est le temps passé à l'état d'écoute et d'apprentissage. La valeur par défaut est de 15 secondes mais peut être modifiée entre 4 et 30 secondes.
- **Minuteur Max Age** -Le minuteur Max Age est la durée maximale d'attente d'un commutateur avant de tenter de modifier la topologie STP. La valeur par défaut est 20 secondes mais peut être modifiée entre 6 et 40 secondes.

**Remarque:** Les durées par défaut peuvent être modifiées sur le pont racine, ce qui dicte la valeur de ces minuteurs pour le domaine STP.

## Fonctionnement du protocole STP

# STP minuteurs et les états des ports (Suite)

Le protocole STP facilite la mise en place d'un chemin logique sans boucle sur l'ensemble du domaine de diffusion. L'arbre recouvrant est déterminé au moyen des informations recueillies par l'échange de trames BPDU entre les commutateurs interconnectés. Si un port de commutateur passe directement de l'état de blocage à l'état de réacheminement sans informations sur la topologie complète pendant la transition, le port peut créer temporairement une boucle de données. Pour cette raison, STP compte cinq États portuaires, dont quatre sont des états des ports opérationnels, comme le montre la figure. L'état désactivé est considéré comme non opérationnel.



## Fonctionnement du protocole STP

# Détails opérationnels de chaque état du port

Le tableau récapitule les détails opérationnels de chaque état du port.

État du port	BPDU	Table d'adresses MAC	Transmission de trames de données
Blocage	Uniquement Recevoir	Pas de mise à jour	Non
Écoute	Recevoir et envoyer	Pas de mise à jour	Non
Apprentissage	Recevoir et envoyer	Mise à jour de la table	Non
Acheminement	Recevoir et envoyer	Mise à jour de la table	Oui
Désactivé	Aucun envoi ou reçu	Pas de mise à jour	Non

# Fonctionnement du protocole STP

## Spanning Tree par VLAN

STP peut être configuré pour fonctionner dans un environnement comportant plusieurs VLAN. Dans les versions de protocole PVST (Per-VLAN Spanning Tree) de STP, un pont racine est déterminé pour chaque instance Spanning Tree. Il est possible de disposer de plusieurs ponts racine distincts pour différents ensembles de réseaux VLAN.

STP exploite une instance distincte de STP pour chaque VLAN individuel. Si tous les ports de tous les commutateurs sont membres de VLAN 1, il n'y aura qu'une seule instance Spanning Tree.

# 5.3 Évolution du protocole STP

# Différentes versions de STP

- De nombreux professionnels utilisent STP (Spanning Tree Protocol) pour désigner des implémentations différentes du concept de Spanning Tree, par exemple le protocole RSTP (Rapid Spanning Tree Protocol) et le protocole MSTP (Multiple Spanning Tree Protocol). Pour pouvoir communiquer clairement sur les concepts de Spanning Tree, il est important de parler d'une implémentation ou d'une norme d'arbre recouvrant (spanning tree) dans son contexte.
- La documentation la plus récente de l'IEEE sur Spanning Tree (IEEE-802-1D-2004) indique que «STP est désormais remplacé par le protocole RSTP (Rapid Spanning Tree Protocol)». L'IEEE utilise «STP» pour faire référence à l'implémentation d'origine de Spanning Tree et «RSTP» pour décrire la version de Spanning Tree dont les spécifications figurent dans le document IEEE-802.1D-2004.
- Puisque les deux protocoles partagent en grande partie la même terminologie et les mêmes méthodes en matière de chemin sans boucle, nous mettrons principalement l'accent sur le standard actuel et les implémentations propres à Cisco de STP et de RSTP.
- Les commutateurs Cisco fonctionnant sous IOS 15.0 ou une version ultérieure exécutent PVST+ par défaut. Cette version intègre plusieurs des caractéristiques du standard IEEE 802.1D-2004, telles que les ports alternatifs au lieu des anciens ports non désignés. Les commutateurs doivent être explicitement configurés pour le mode Rapid Spanning Tree afin d'exécuter le protocole Rapid Spanning Tree.

# Évolution du protocole STP

## Différentes versions de STP (Suite)

Variété STP	Description
STP	Il s'agit de la version IEEE 802.1D d'origine (802.1D-1998 et antérieures) qui fournit une topologie dépourvue de boucle dans un réseau comportant des liaisons redondantes. Également appelé CST (Common Spanning Tree, arbre recouvrant commun) suppose une seule instance Spanning Tree pour l'ensemble du réseau ponté, quel que soit le nombre de VLAN.
PVST+	PVST+ (Per-VLAN Spanning Tree) est une version améliorée du protocole STP proposée par Cisco, qui offre une instance Spanning Tree 802.1D séparée pour chaque VLAN configuré dans le réseau. PVST+ prend en charge PortFast, UplinkFast, BackboneFast, la protection BPDU, le filtre BPDU, la protection de racine et la protection de boucle.
802.1D-2004	C'est une version mise à jour du protocole STP standard, intégrant IEEE 802.1w.
RSTP	Protocole RSTP (Rapid Spanning Tree Protocol) ou IEEE 802.1w est une version évoluée du protocole STP, qui offre une convergence plus rapide.
Rapid PVST+	Il s'agit d'une version améliorée de RSTP proposée par Cisco qui utilise PVST+ et fournit une instance distincte de 802.1w par VLAN. Chaque instance séparée prend en charge PortFast, la protection BPDU, le filtre BPDU, la protection de racine et la protection de boucle.
MSTP	MSTP (Multiple Spanning Tree Protocol) est un standard IEEE .MSTP mappe plusieurs VLAN dans une même instance Spanning Tree.
MST	Multiple Spanning Tree (MST) est l'implémentation Cisco de MSTP, elle fournit jusqu'à 16 instances du protocole RSTP et allie plusieurs VLAN avec la même topologie physique et logique au sein d'une instance courante du protocole RSTP. Chaque instance prend en charge PortFast, la protection BPDU, le filtre BPDU, la protection de racine et la protection de boucle.

# Concepts du protocole RSTP

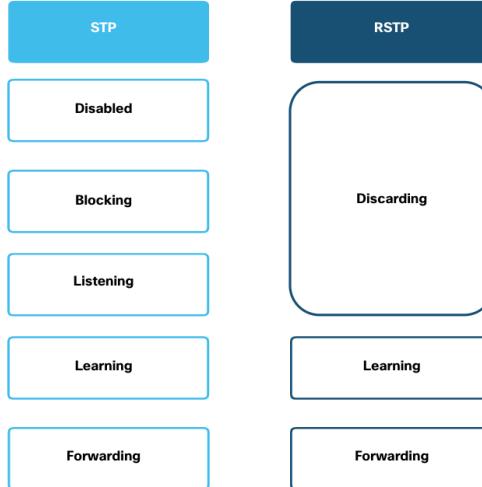
- RSTP (IEEE 802.1w) remplace le protocole 802.1D d'origine, tout en conservant la rétrocompatibilité. La terminologie du protocole STP 802.1w est essentiellement la même que celle du protocole STP IEEE 802.1D initial. La plupart des paramètres ont été conservés. les utilisateurs déjà familiarisés avec la norme STP d'origine puissent rapidement configurer le protocole RSTP. Le même algorithme de spanning tree est utilisé pour STP et RSTP pour déterminer les rôles de port et la topologie.
- Le protocole RSTP optimise le recalcul de l'arbre recouvrant (spanning tree) lorsque la topologie d'un réseau de couche 2 change. Le protocole RSTP assure un temps de convergence beaucoup plus rapide dans un réseau correctement configuré, parfois de l'ordre de quelques centaines de millisecondes. Si un port est configuré comme port alternatif, il peut passer immédiatement à l'état de transmission sans attendre que le réseau converge.

**Remarque:** Rapid PVST+ est l'implémentation de Cisco du protocole RSTP par VLAN. En utilisant le protocole Rapid PVST+ une instance indépendante s'exécute sur chaque VLAN.

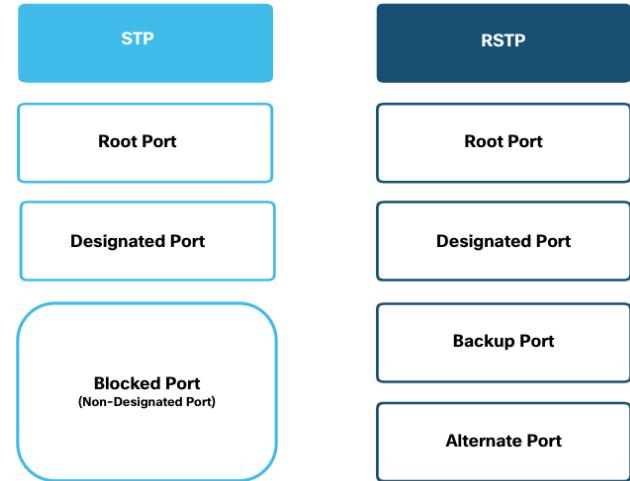
# Évolution du protocole STP

## Etats de port RSTP et rôles de port

Il n'y a que trois états de port dans le RSTP qui correspondent aux trois états opérationnels possibles dans le STP. Les états 802.1D désactivés, de blocage et d'écoute sont fusionnés en un état unique de suppression de 802.1w.

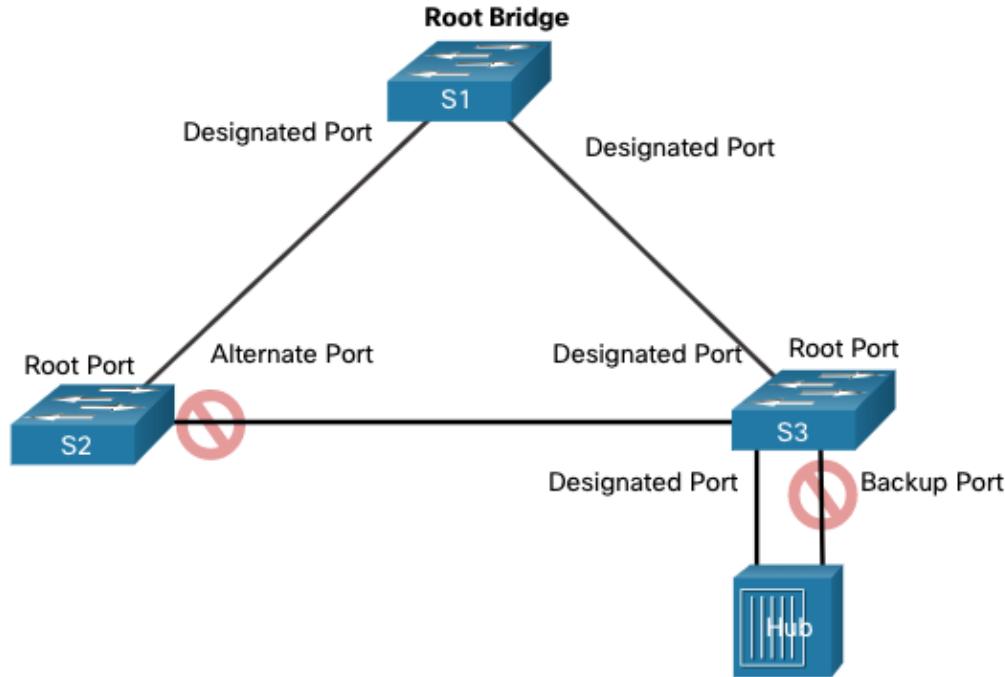


Les ports racine et les ports désignés sont les mêmes pour STP et RSTP. Toutefois, il existe deux rôles de port RSTP qui correspondent à l'état de blocage de STP. Dans STP, un port bloqué est défini comme n'étant pas le port désigné ou le port racine. RSTP a deux rôles de port à cet effet.



# Etats de port RSTP et rôles de port (Suite)

Le port alternatif a un autre chemin vers le pont racine. Le port de secours est une veille sur un support partagé, tel qu'un concentrateur. Un port de secours est moins commun car les concentrateurs sont désormais considérés comme des périphériques hérités.



# PortFast et protection BPDU

- Lorsqu'un périphérique est connecté à un port de commutateur ou lorsqu'un commutateur se met sous tension, le port de commutateur passe par les états d'écoute et d'apprentissage, chaque fois qu'il attend l'expiration de minuteur Forward Delay. Ce délai est de 15 secondes pour chaque état pour un total de 30 secondes. Cela peut présenter un problème pour les clients DHCP qui tentent de découvrir un serveur DHCP car le processus DHCP peut expirer. Le résultat est qu'un client IPv4 ne recevra pas une adresse IPv4 valide.
- Lorsqu'un port de commutateur est configuré avec PortFast, ce port passe immédiatement de l'état de blocage à l'état de transfert, en évitant ainsi le délai de 30 secondes. Vous pouvez utiliser PortFast sur les ports d'accès pour permettre aux périphériques connectés à ces ports d'accéder immédiatement au réseau. PortFast ne doit être utilisé que sur les ports d'accès. Si vous activez PortFast sur un port connecté à un autre commutateur, vous risquez de créer une boucle Spanning Tree.
- Un port de commutateur activé par PortFast ne devrait jamais recevoir de BPDU car cela indiquerait que le commutateur est connecté au port, ce qui pourrait provoquer une boucle Spanning Tree. Les commutateurs Cisco prennent en charge une fonctionnalité appelée protection BPDU. Lorsqu'elle est activée, la protection BPDU place immédiatement le port à l'état errdisabled (erreur désactivée) lors de la réception d'une trame BPDU. Cela protège contre les boucles potentielles en arrêtant efficacement le port. L'administrateur doit remettre manuellement l'interface en service.

# Alternatives au protocole STP

- Au cours des ans, les organisations ont exigé une plus grande résilience et une plus grande disponibilité dans le réseau local. Les réseaux locaux Ethernet sont passés de quelques commutateurs interconnectés connectés à un seul routeur, à une conception de réseau hiérarchique sophistiquée incluant des commutateurs d'accès, de distribution et de couche centrale.
- Selon l'implémentation, la couche 2 peut inclure non seulement la couche d'accès, mais aussi la couche de distribution ou même les couches cœur de réseau. Ces conceptions peuvent inclure des centaines de commutateurs, avec des centaines ou des milliers de VLAN. Le protocole STP s'est adapté à la redondance et à la complexité accrues grâce à des modifications dans le cadre du RSTP et du MSTP.
- Un aspect important de la conception du réseau est la convergence rapide et prévisible en cas de défaillance ou de modification de la topologie. Spanning tree n'offre pas les mêmes efficacités et prédictions que celles des protocoles de routage de la couche 3.
- Le routage de couche 3 permet des chemins et des boucles redondants dans la topologie, sans bloquer les ports. Pour cette raison, certains environnements sont en cours de transition vers la couche 3 partout, sauf lorsque les périphériques se connectent au commutateur de couche d'accès. En d'autres termes, les connexions entre les commutateurs de couche d'accès et les commutateurs de distribution seraient de couche 3 au lieu de couche 2.

# Packet Tracer - STP

**LAB05.1-STP**

**LAB05.2-STP**



# 5.4 Module pratique et questionnaire

- Module pratique et questionnaire

## Qu'est-ce que j'ai appris dans ce module?

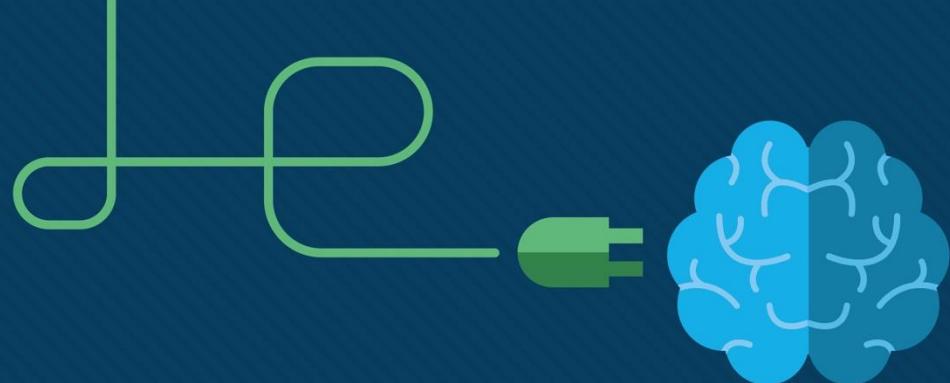
- Les chemins d'accès redondants dans un réseau Ethernet commuté peuvent entraîner à la fois des boucles physiques et logiques de couche 2.
- Une boucle de couche 2 peut entraîner l'instabilité de la table d'adresses MAC, la saturation des liaisons et une utilisation élevée de processeur sur les commutateurs et les terminaux. Il en résulte que le réseau devient inutilisable.
- Le protocole STP est un protocole réseau de prévention des boucles qui permet la redondance tout en créant une topologie de couche 2 sans boucle. Sans STP, les boucles de couche 2 peuvent se former, provoquant une boucle infinie de trames de diffusion, de multidiffusion et de monodiffusion inconnues, entraînant la défaillance d'un réseau.
- En utilisant le STA, STP établit une topologie sans boucle dans un processus en quatre étapes : élection du pont racine, élection des ports racine, élection des ports désignés et élection des ports alternatifs (bloqués).
- Pendant le fonctionnement de STA et de STP, les commutateurs utilisent des BPDU (Bridge Protocol Data Units) pour partager des informations sur eux-mêmes et sur leurs connexions. Les BPDU permettent de choisir le pont racine, les ports racine, les ports désignés et les ports alternatifs.
- Lorsque le pont racine a été choisi pour l'instance Spanning Tree, l'algorithme STA détermine des meilleurs chemins possibles vers le pont racine, depuis l'ensemble des destinations du domaine de diffusion. Les informations relatives au chemin, appelées coût du chemin racine interne, sont déterminées en additionnant les coûts de port individuels le long du chemin entre le commutateur et le pont racine.
- Une fois le pont racine est déterminé, l'algorithme STA sélectionne le port racine. Le port racine est le port le plus proche du pont racine en termes de coûts généraux qui est appelé coût du chemin racine interne.
- Après que chaque commutateur a sélectionné un port racine, les commutateurs sélectionnent les ports désignés. Le port désigné est un port sur le segment (avec deux commutateurs) qui a le coût du chemin racine interne vers le pont racine.
- Si un port n'est pas un port racine ou un port désigné, il devient alors un port alternatif (ou de secours). les ports alternatifs et de secours sont à l'état de suppression ou de blocage pour éviter les boucles.

# Qu'est-ce que j'ai appris dans ce module? (Suite)

- Lorsqu'un commutateur possède plusieurs chemins d'accès au même coût vers le pont racine, le commutateur détermine un port en utilisant les critères suivants:BID d'émetteur le plus faible, puis priorité de port d'émetteur le plus bas et enfin l'ID de port d'émetteur le plus bas.
- La convergence STP nécessite trois minuteries: le minuteur hello, le minuteur forward delay et le minuteur max age.
- Les états de port sont: blocage, écoute, apprentissage, réacheminement et désactivé.
- Dans les versions PVST de STP, un pont racine est déterminé pour chaque instance Spanning Tree. Il est possible de disposer de plusieurs ponts racine distincts pour différents ensembles de réseaux VLAN.
- STP est souvent utilisé pour faire référence aux différentes implémentations de spanning tree, telles que RSTP et MSTP.
- RSTP est une évolution de Spanning Tree qui offre une convergence plus rapide que STP.
- Les états des ports de RSTP sont mise à l'écart (discarding), apprentissage et acheminement.
- PVST+ est une version améliorée du protocole STP proposée par Cisco, qui offre une instance Spanning Tree 802.1D séparée pour chaque VLAN configuré dans le réseau. PVST+ prend en charge PortFast, UplinkFast, BackboneFast, la protection BPDU, le filtre BPDU, la protection de racine et la protection de boucle.
- Les commutateurs Cisco fonctionnant sous IOS 15.0 ou une version ultérieure exécutent PVST+ par défaut.
- Rapid PVST+ est une version améliorée de RSTP proposée par Cisco qui utilise PVST+ et fournit une instance distincte de 802.1w par VLAN.
- Lorsqu'un port de commutateur est configuré avec PortFast, ce port passe immédiatement de l'état de blocage à l'état de réacheminement, évitant ainsi les états d'écoute et d'apprentissage STP et un délai de 30 secondes.
- Vous pouvez utiliser PortFast sur les ports d'accès pour permettre aux appareils connectés à ces ports, tels que les clients DHCP, d'accéder immédiatement au réseau, plutôt que d'attendre que le STP converge sur chaque VLAN.

## Qu'est-ce que j'ai appris dans ce module? (Suite)

- Les commutateurs Cisco prennent en charge une fonctionnalité appelée Protection BPDU qui met immédiatement le port du commutateur dans un état désactivé par erreur à la réception de tout BPDU pour se protéger contre les boucles potentielles.
- Au cours des ans, les réseaux locaux Ethernet sont passés de quelques commutateurs interconnectés, reliés à un seul routeur, à une conception de réseau hiérarchique sophistiquée. Selon l'implémentation, la couche 2 peut inclure non seulement la couche d'accès, mais aussi la couche de distribution ou même les couches cœur de réseau. Ces conceptions peuvent inclure des centaines de commutateurs, avec des centaines ou des milliers de VLAN. Le protocole STP s'est adapté à la redondance et à la complexité accrues grâce à des modifications dans le cadre du RSTP et du MSTP.
- Le routage de couche 3 permet des chemins et des boucles redondants dans la topologie, sans bloquer les ports. Pour cette raison, certains environnements sont en cours de transition vers la couche 3 partout, sauf lorsque les périphériques se connectent au commutateur de couche d'accès.



# Module 6: EtherChannel



# Objectifs du Module

**Titre du module:** EtherChannel

**Objectifs du Module:** Dépanner EtherChannel sur les liaisons commutées.

Titre du rubrique	Objectif du rubrique
<b>Fonctionnement d'EtherChannel</b>	Décrire la technologie EtherChannel.
<b>Configuration d'EtherChannel</b>	Configurer la technologie EtherChannel.
<b>Vérification et dépannage d'EtherChannel</b>	Dépanner la technologie EtherChannel.

# 6.1 Fonctionnement d'EtherChannel

# Fonctionnement d'EtherChannel

## Agrégation de liaisons

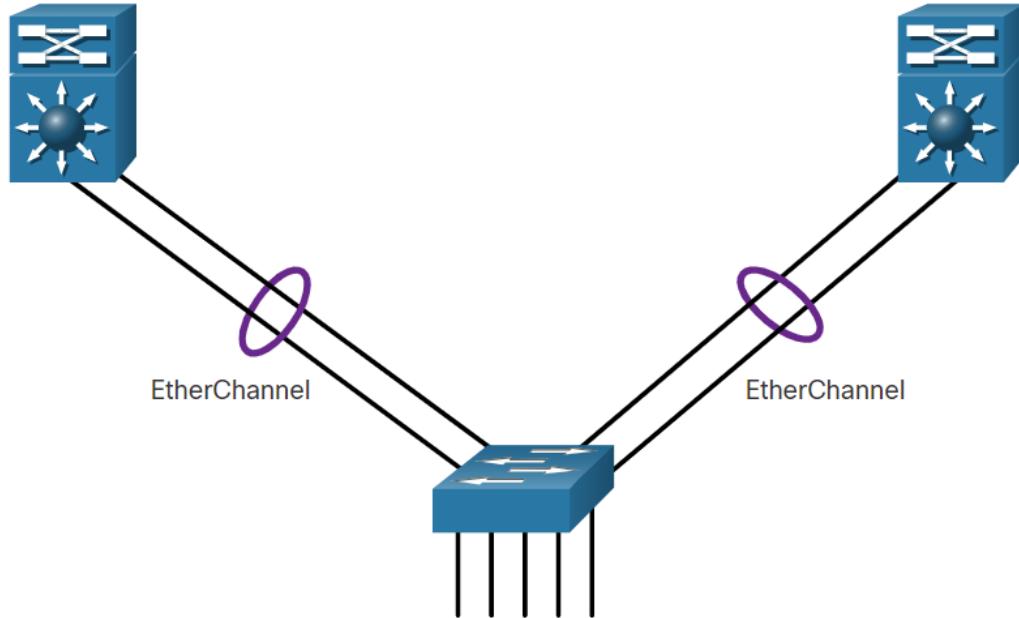
- Il existe des scénarios dans lesquels plus de bande passante ou de redondance entre les périphériques est nécessaire que ce qui peut être fourni par une liaison unique. Plusieurs liens peuvent être connectés entre les appareils pour augmenter la bande passante. Cependant, le protocole STP (Spanning Tree Protocol), qui est activé sur les périphériques de couche 2 tels que les commutateurs Cisco par défaut, bloquera les liens redondants pour empêcher les boucles de commutation.
- Une technologie d'agrégation de liens est nécessaire pour permettre des liaisons redondantes entre les périphériques qui ne seront pas bloqués par STP. Cette technologie est connue sous le nom d'EtherChannel.
- EtherChannel est une technologie d'agrégation de liens qui regroupe plusieurs liaisons Ethernet physiques en un seul lien logique. Il est utilisé pour fournir une tolérance aux pannes, un partage de charge, une bande passante accrue et une redondance entre les commutateurs, les routeurs et les serveurs.
- La technologie EtherChannel permet le nombre de liaisons physiques entre les commutateurs pour accélérer de manière globale la communication entre les commutateurs.

# Fonctionnement d'EtherChannel

## EtherChannel

La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant de regrouper plusieurs ports Fast Ethernet ou Gigabit Ethernet en un seul canal logique.

Quand un EtherChannel est configuré, l'interface virtuelle résultante est appelée un canal de port. Les interfaces physiques sont regroupées dans une interface de canal de port, comme indiqué sur la figure.



# Avantages de l'EtherChannel

La technologie EtherChannel présente de nombreux avantages, dont les suivants:

- La plupart des tâches de configuration peuvent être réalisées sur l'interface EtherChannel plutôt que sur chaque port, ce qui assure la cohérence de la configuration sur toutes les liaisons.
- Une liaison EtherChannel repose sur les ports de commutation existants. Il n'est pas nécessaire de mettre à niveau la liaison vers une connexion plus rapide et plus coûteuse pour avoir davantage de bande passante.
- L'équilibrage de la charge se fait entre les liaisons appartenant au même EtherChannel.
- EtherChannel crée une agrégation considérée comme une seule liaison logique. Quand plusieurs groupes EtherChannel existent entre deux commutateurs, STP peut bloquer l'un des groupes pour éviter les boucles de commutation. Quand STP bloque l'une des liaisons redondantes, cela bloque la totalité de l'EtherChannel. Cela bloque tous les ports appartenant à cette liaison EtherChannel. Quand il existe uniquement une liaison EtherChannel, toutes les liaisons physiques de l'EtherChannel sont actives, car STP considère une seule liaison (logique).
- EtherChannel offre de la redondance car la liaison globale est considérée comme une seule connexion logique. De plus, la perte d'un lien physique dans le canal ne crée pas de changement dans la topologie.

# Les Restrictions d'implémentation

EtherChannel a certaines restrictions d'implémentation, notamment les suivantes:

- Les types d'interfaces ne peuvent pas être associés. Par exemple, le Fast Ethernet et le Gigabit Ethernet ne peuvent pas être mélangés dans un seul EtherChannel.
- Actuellement, chaque EtherChannel peut être composé de huit ports Ethernet maximum, configurés pour être compatibles. EtherChannel fournit une largeur de bande en duplex intégral jusqu'à 800 Mbps (Fast EtherChannel) ou 8 Gbps (Gigabit EtherChannel) entre un commutateur et un autre commutateur ou hôte.
- Le commutateur Cisco Catalyst 2960 de couche 2 prend actuellement en charge jusqu'à six canaux EtherChannels.
- La configuration de chaque port du groupe EtherChannel doit être cohérente sur les deux périphériques. Si les ports physiques sont configurés en tant que trunks d'un côté, les ports physiques de l'autre côté doivent également être configurés en tant que trunks avec le même VLAN natif. En outre, tous les ports de chaque liaison EtherChannel doivent être configurés en tant que ports de couche 2.
- Chaque EtherChannel possède une interface de canal de port logique. Une configuration appliquée à l'interface de canal de port affecte toutes les interfaces physiques attribuées à cette interface.

## Protocole de négociation automatique

Des EtherChannel peuvent être formés par négociation en utilisant l'un des deux protocoles, PAgP ou LACP. Ces protocoles permettent à des ports ayant des caractéristiques similaires de former un canal grâce à une négociation dynamique avec les commutateurs attenants.

**Remarque:** Il est également possible de configurer une liaison EtherChannel statique ou inconditionnel sans PAgP ou LACP.

## Fonctionnement d'EtherChannel

# Fonctionnement de PAgP

PAgP (prononcé "Pag - P") est un protocole propriétaire de Cisco qui aide à la création automatique de liens EtherChannel. Quand une liaison EtherChannel est configurée grâce à PAgP, des paquets PAgP sont envoyés entre les ports compatibles EtherChannel pour négocier la formation d'un canal. Quand PAgP identifie des liaisons Ethernet associées, il groupe les liaisons dans une liaison EtherChannel. L'EtherChannel est ensuite ajouté à l'arbre recouvrant comme port unique.

S'il est activé, PAgP gère également l'EtherChannel. Les paquets PAgP sont envoyés toutes les 30 secondes. PAgP vérifie la cohérence de la configuration et gère les ajouts de liaison et les défaillances entre deux commutateurs. Il garantit que tous les ports ont le même type de configuration quand une liaison EtherChannel est créée.

**Remarque:** Dans l'EtherChannel, tous les ports doivent obligatoirement avoir une vitesse, un paramètre de bidirectionnalité et des informations VLAN identiques. Toute modification d'un port après la création du canal modifie également tous les autres ports du canal.

# Fonctionnement de PAgP (Suite)

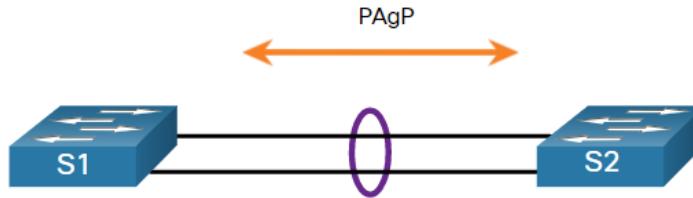
PAgP permet de créer la liaison EtherChannel en détectant la configuration de chaque côté et en assurant la compatibilité des liaisons, afin que la liaison EtherChannel puisse être activée si besoin. Les modes de PAgP sont les suivants :

- **On** - Ce mode force l'interface à établir un canal sans PAgP. Les interfaces configurées en mode On (Activé) n'échangent pas de paquets PAgP.
- **PAgP desirable (désirable)** - Ce mode PAgP place une interface dans un état de négociation actif, dans lequel l'interface entame des négociations avec d'autres interfaces en envoyant des paquets PAgP.
- **PAgP auto** - Ce mode PAgP place une interface dans un état de négociation passif, dans lequel l'interface répond aux paquets PAgP qu'elle reçoit mais n'entame pas de négociation PAgP.

Les modes doivent être compatibles de chaque côté. Si un côté est configuré pour être en mode Auto, il est placé dans un état passif et attend que l'autre côté entame la négociation EtherChannel. Si l'autre côté est également placé en mode Auto, la négociation ne commence jamais et l'EtherChannel ne se forme pas. Si tous les modes sont désactivés en utilisant la commande **no** , ou si aucun mode n'est configuré, alors l'EtherChannel est désactivé. Le mode On (Activé) place manuellement l'interface dans un EtherChannel, sans aucune négociation. Cela fonctionne uniquement si l'autre côté est également placé en mode On (Activé). Si l'autre côté est configuré pour négocier les paramètres via PAgP, aucun EtherChannel ne se forme car le côté placé en mode On (Activé) ne négocie pas. Comme il n'y a aucune négociation entre les deux commutateurs, aucun contrôle ne permet de s'assurer que toutes les liaisons de l'EtherChannel prennent fin de l'autre côté ou que l'autre commutateur prend charge le protocole PAgP.

## Fonctionnement d'EtherChannel

# Exemple de paramètres du mode PAgP



Le tableau montre les différentes combinaisons de modes PAgP sur S1 et S2 et le résultat résultant de l'établissement du canal.

S1	S2	Établissement de canal
On (activé)	Allumé	Oui
On	Desirable/Auto	Non
Desirable	Desirable	Oui
Desirable	Auto	Oui
Auto	Desirable	Oui
Auto	Auto	Non

## Fonctionnement d'EtherChannel

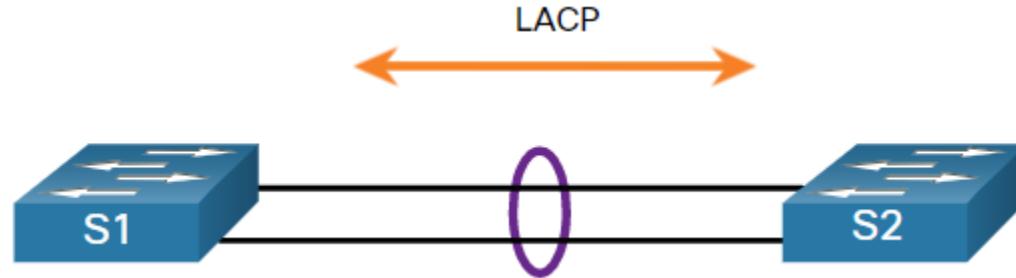
# Fonctionnement de LACP

LACP fait partie d'une spécification IEEE (802.3ad) qui permet de regrouper plusieurs ports physiques pour former un seul canal logique. LACP permet à un commutateur de négocier un paquet automatique en envoyant des paquets LACP à l'autre commutateur. Il assure une fonction semblable à celle de PAgP avec Cisco EtherChannel. LACP étant une norme IEEE, il peut être utilisé pour faciliter les EtherChannel dans des environnements multifournisseurs. Sur les périphériques Cisco, les deux protocoles sont pris en charge.

LACP offre les mêmes avantages en matière de négociation que PAgP. LACP permet de créer la liaison EtherChannel en détectant les configurations de chacun des côtés et en assurant leur compatibilité, afin que la liaison EtherChannel puisse être activée au besoin. Les modes de LACP sont les suivants:

- **On** - Ce mode force l'interface à établir un canal sans LACP. Les interfaces configurées en mode On (Activé) n'échangent pas de paquets LACP.
- **LACP active** - Ce mode LACP place un port dans un état actif de négociation. Dans cet état, le port entame des négociations avec d'autres ports en envoyant des paquets LACP.
- **LACP passive** - Ce mode LACP place un port dans un état de négociation passif. Dans cet état, le port répond aux paquets LACP qu'il reçoit, mais n'entame pas de négociation par paquet LACP.

# Exemple de paramètres du mode LACP



Le tableau montre les diverses combinaisons de modes LACP sur S1 et S2 et le résultat résultant de l'établissement du canal.

S1	S2	Établissement de canal
On (activé)	On (activé)	Oui
On	Active (Actif)/Passive (Passif)	Non
Actif	Actif	Oui
Actif	Passif	Oui
Passif	Actif	Oui
Passif	Passif	Non

# 6.2 Configurer la technologie EtherChannel.

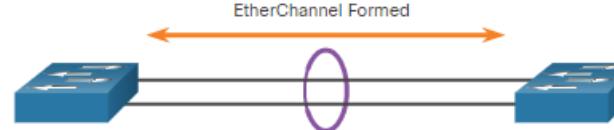
# Consignes de configuration

Les instructions et restrictions suivantes sont utiles pour la configuration d'EtherChannel:

- **Prise en charge d'EtherChannel** - Toutes les interfaces Ethernet doivent prendre en charge EtherChannel sans exigence que les interfaces soient physiquement contiguës.
- **Débit et duplex** - Configurez le même débit et le même mode duplex sur l'ensemble des interfaces d'un EtherChannel.
- **VLAN correspondant** - Toutes les interfaces d'une liaison EtherChannel doivent être attribuées au même VLAN, ou être configurées en tant que trunk (illustré dans la figure).
- **Plage de VLAN** - Une EtherChannel prend en charge la même plage autorisée de VLAN sur toutes les interfaces d'un trunk EtherChannel. Si la plage autorisée de VLAN n'est pas identique, les interfaces ne forment pas l'EtherChannel, même si elles sont définies en mode **auto** ou **desirable**.

# Consignes de Configuration (Suite)

- La figure montre une configuration qui permettrait à l'EtherChannel de se former entre S1 et S2.
- Si ces paramètres doivent être modifiés, configuez-les dans le mode de configuration de l'interface de canal de port. Toute configuration appliquée à l'interface de canal de port affecte également les autres interfaces. Cependant, les configurations appliquées à chaque interface n'affectent pas l'interface de canal de port. Par conséquent, modifier la configuration d'une interface appartenant à une liaison EtherChannel peut entraîner des problèmes de compatibilité d'interface.
- Le canal de port peut être configuré en mode d'accès, en mode trunk (le plus couramment utilisé) ou sur un port routé.



S1 Port Configurations

Speed	1 Gbps
Duplex	Full
VLAN	10

S2 Port Configurations

Speed	1 Gbps
Duplex	Full
VLAN	10

# Exemple de Configuration LACP

La configuration d'EtherChannel avec LACP nécessite les trois étapes suivantes :

- **Étape 1.** Spécifiez les interfaces qui composent le groupe EtherChannel en utilisant la commande de mode de configuration globale d'interface **interface range** Le mot-clé **range** vous permet de sélectionner plusieurs interfaces et de les configurer toutes ensemble.
- **Étape 2.** Créez l'interface de canal de port à l'aide de la commande **channel group identifier mode active** en mode de configuration de plage d'interface. L'identificateur spécifie un numéro de groupe de canaux. Les mots-clés **mode active** l'identifient comme une configuration EtherChannel LACP.
- **Étape 3.** Pour modifier les paramètres de la couche 2 de l'interface de canal de port, entrez dans le mode de configuration de l'interface de canal de port en utilisant la commande **interface port-channel** suivie de l'identifiant de l'interface. Dans l'exemple, S1 est configuré avec l'EtherChannel LACP. Le canal de port est configuré comme une interface de trunk avec les VLAN autorisés spécifiés.

```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config-if)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```

# Packet Tracer - Configuration d'EtherChannel

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Configurer les paramètres de base du commutateur
- Configurer un réseau EtherChannel avec Cisco PAgP
- Configurer et EtherChannel 802.3ad
- Configurer une liaison EtherChannel redondante
- **LAB06.1-ETHERCHANNEL**

# 6.3 Vérification et dépannage d'EtherChannel

## Vérification et dépannage d'EtherChannel

# Vérification d'EtherChannel

Comme toujours, lorsque vous configurez des périphériques sur votre réseau, vous devez vérifier votre configuration. S'il y a des problèmes, vous devrez également être en mesure de les dépanner et de les résoudre. Il existe plusieurs commandes permettant de vérifier une configuration EtherChannel:

- La commande **show interfaces port-channel** affiche l'état global de l'interface de canal de port.
- La commande **show etherchannel summary** affiche une ligne d'informations par canal de port.
- La commande **show etherchannel port-channel** affiche des informations concernant une interface de canal de port spécifique.
- La commande **show interfaces etherchannel** peut fournir des informations sur le rôle de l'interface physique des membres dans l'EtherChannel.

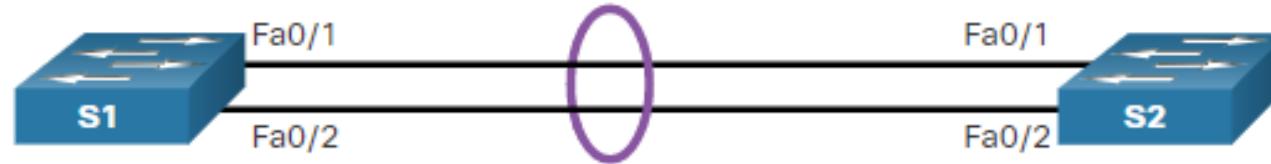
# Problèmes courants avec les configurations EtherChannel

Toutes les interfaces d'un EtherChannel doivent avoir la même configuration en matière de débit et de mode duplex, les mêmes VLAN natifs et autorisés sur les trunks, et le même VLAN d'accès sur les ports d'accès. Veiller à ce que ces configurations réduisent considérablement les problèmes réseau liés à EtherChannel. Les problèmes courants d'EtherChannel sont les suivants:

- Attribuez tous les ports du EtherChannel au même VLAN, ou configurez-les en tant que trunks. Des ports avec des VLAN natifs différents ne peuvent pas former un EtherChannel.
- Le trunking a été configuré sur certains ports qui composent l'EtherChannel, mais pas tous. Nous vous déconseillons de configurer le mode de trunking sur les ports qui composent l'EtherChannel. Lorsque vous configurez un trunk sur un EtherChannel, vérifiez le mode de trunking sur l'EtherChannel.
- Si la plage autorisée de VLAN n'est pas la même, les ports ne forment pas l'EtherChannel même lorsque le PAgP est défini sur le mode **auto** ou **desirable**.
- Les options de négociation dynamique pour le PAgP et le LACP ne sont pas configurées de manière compatible aux deux extrémités de l'EtherChannel.

# Exemple de dépannage d'EtherChannel

Dans la figure, les interfaces F0/1 et F0/2 des commutateurs S1 et S2 sont connectées à une liaison EtherChannel. Cependant, l'EtherChannel n'est pas opérationnelle.



# Exemple de dépannage d'EtherChannel

**Étape 1. Affichez les informations récapitulatives EtherChannel:** la sortie de la commande **show etherchannel summary** indique que l'EtherChannel est en panne.

```
S1# show etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3         S - Layer2
        U - in use         N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
-----+-----+-----+
 1     Po1(SD)       -      Fa0/1(D)   Fa0/2(D)
```

# Exemple de dépannage d'EtherChannel (Suite)

**Étape 2. Affichez la configuration du canal de port:** Dans le résultat de la commande **show run | begin interface port channel** la sortie plus détaillée indique qu'il existe des modes PAgP incompatibles configurés sur S1 et S2.

```
S1# show run | begin interface port-channel
interface Port-channel1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode on
!
interface FastEthernet0/2
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode on
=====
S2# show run | begin interface port-channel
interface Port-channel1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
!
interface FastEthernet0/1
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode desirable
!
interface FastEthernet0/2
switchport trunk allowed vlan 1,2,20
switchport mode trunk
channel-group 1 mode desirable
```

# Exemple de dépannage d'EtherChannel (Suite)

**Étape 3: Corrigez la mauvaise configuration:** Pour corriger le problème, le mode PAgP sur l'EtherChannel est remplacée par desirable.

**Remarque:** EtherChannel et STP doivent fonctionner ensemble. Par conséquent, l'ordre dans lequel les commandes relatives à EtherChannel sont saisies est important. Cela explique pourquoi vous voyez l'interface Port-Channel 1 supprimée puis réajoutée avec la commande **channel-group** par opposition à d'être modifiée directement. Si l'on tente de modifier directement la configuration, les erreurs STP font passer les ports associés en état de blocage ou d'erreur.

```
S1(config)# no interface port-channel 1
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
S1(config-if-range)# no shutdown
S1(config-if-range)# exit
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
S1(config-if-range)# no shutdown
S1(config-if-range)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

# Exemple de dépannage d'EtherChannel (Suite)

**Étape 4. Vérifiez que l'EtherChannel est opérationnelle:** L'EtherChannel est désormais actif comme vérifié par la sortie de la commande **show etherchannel summary** .

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone S - suspended
      H - Hot-standby (LACP only)
      R - Layer3      S - Layer2
      U - in use       N - not in use, no aggregation
      f - failed to allocate aggregator
      M - not in use, minimum links not met
      m - not in use, port not aggregated due to minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port
      A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators: 1
Group  Port-channel  Protocol    Ports
-----+-----+-----+
 1     Po1(SU)        PAgP       Fa0/1(P)   Fa0/2(P)
```

# Packet Tracer - Dépannage d'EtherChannel

Dans ce Packet Tracer, vous remplirez les objectifs suivants:

- Examen de la couche physique et correction des erreurs liées au mode du port de commutateur
- Identification et correction des erreurs d'attribution de port-channel
- **LAB06.2-ETHERCHANNEL**

# 6.4 - Module pratique et questionnaire

# Qu'est-ce que j'ai appris dans ce module?

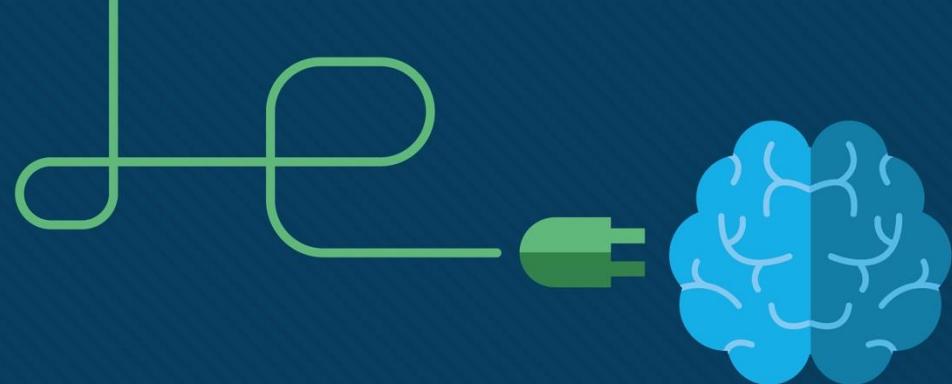
- Pour augmenter la bande passante ou la redondance, plusieurs liaisons peuvent être connectées entre les périphériques. STP bloquera les liaisons redondantes pour éviter les boucles de commutation. EtherChannel est une technologie d'agrégation de liens qui permet des liaisons redondantes entre les périphériques qui ne seront pas bloqués par STP.
- EtherChannel est une technologie d'agrégation de liens qui regroupe plusieurs liaisons Ethernet physiques en un seul lien logique. Il offre une tolérance aux pannes, un partage de charge, une bande passante accrue et une redondance entre les commutateurs, les routeurs et les serveurs.
- Quand un EtherChannel est configuré, l'interface virtuelle résultante est appelée un canal de port.
- Des EtherChannel peuvent être formés par négociation en utilisant l'un des deux protocoles, PAgP ou LACP. Ces protocoles permettent à des ports ayant des caractéristiques similaires de former un canal grâce à une négociation dynamique avec les commutateurs attenants.
- Lorsqu'une liaison EtherChannel est configurée en utilisant le PAgP propriétaire de Cisco, les paquets PAgP sont envoyés entre les ports compatibles EtherChannel pour négocier la formation d'un canal. Les modes PAgP sont On, PAgP desirable et PAgP auto.
- Il assure une fonction semblable à celle de PAgP avec Cisco EtherChannel. LACP étant une norme IEEE, il peut être utilisé pour faciliter les EtherChannel dans des environnements multifournisseurs. Les modes pour LACP sont On, LACP active et LACP passive.

# Qu'est-ce que j'ai appris dans ce module? (Suite)

- Les instructions et restrictions suivantes sont utiles pour la configuration d'EtherChannel:
  - Toutes les interfaces Ethernet sur tous les modules doivent prendre en charge EtherChannel, sans que les interfaces soient nécessairement contiguës de manière physique ou sur le même module.
  - Configurez le même débit et le même mode duplex sur l'ensemble des interfaces d'un EtherChannel.
  - Toutes les interfaces situées à l'intérieur d'un paquet EtherChannel doivent être attribuées au même VLAN ou être configurées comme un trunk.
  - Un EtherChannel prend en charge la même plage autorisée de VLAN sur toutes les interfaces d'un trunk EtherChannel.
- La configuration d'EtherChannel avec LACP nécessite trois étapes :
  - Étape 1. Spécifier les interfaces qui composent le groupe EtherChannel en utilisant la commande de mode de configuration globale d'interface **interface range** .
  - Étape 2. Créer l'interface de canal de port à l'aide de la commande **channel-group identifier mode active** en mode de configuration de plage d'interface.
  - Étape 3. Pour modifier les paramètres de la couche 2 de l'interface de canal de port, entrez dans le mode de configuration de l'interface de canal de port en utilisant la commande **interface port-channel** , suivie de l'identifiant de l'interface.

## Qu'est-ce que j'ai appris dans ce module? (Suite)

- Il existe un certain nombre de commandes pour vérifier une configuration EtherChannel, y compris **show interfaces port-channel**, **show etherchannel summary**, **show etherchannel port-channel** et **show interfaces etherchannel**.
- Les problèmes courants d'EtherChannel sont les suivants:
  - Attribution de tous les ports d'EtherChannel au même VLAN, ou les configurer en tant que trunks.
  - Des ports avec des VLAN natifs différents ne peuvent pas former un EtherChannel.
  - Le trunking a été configuré sur certains ports qui composent l'EtherChannel, mais pas tous.
  - Si la plage autorisée de VLAN n'est pas identique, les ports ne forment pas un EtherChannel, même si PAgP est défini en mode auto ou desirable.
  - Les options de négociation dynamique pour le PAgP et le LACP ne sont pas configurées de manière compatible aux deux extrémités de l'EtherChannel.



# Module 7 : Conception de sécurité LAN

Contenu Pédagogique de l'instructeur

Notions de base sur la commutation, le routage et le sans fil v7.0 (SRWE)



# Objectifs de ce module

**Titre du module:** Conception de sécurité du réseau local LAN

**Objectif du module:** Expliquez comment les vulnérabilités compromettent la sécurité du réseau local.

Titre du rubrique	Objectif du rubrique
Sécurité des terminaux	Expliquez comment utiliser la sécurité des terminaux pour atténuer les attaques.
Contrôle d'accès	Expliquez comment AAA et 802.1x sont utilisés pour authentifier les périphériques et les terminaux LAN.
Menaces de la sécurité de couche 2	Identifiez les vulnérabilités de couche 2.
Attaque du table d'adresses MAC	Expliquez comment une attaque de table d'adresses MAC compromet la sécurité du réseau LAN.
Les attaques de réseau LAN	Expliquez comment les attaques LAN compromettent la sécurité LAN.

# 7.1 La sécurité des terminaux

# Les attaques de réseau au quotidien

Les médias d'information couvrent généralement les attaques contre les réseaux d'entreprise. Recherchez simplement sur Internet les «dernières attaques réseau» pour trouver des informations à jour sur les attaques en cours. Probablement, ces attaques impliqueront un ou plusieurs les éléments suivants:

- **Déni de service distribué (DDoS)** - Il s'agit d'une attaque coordonnée de nombreux périphériques, appelés zombies, dans le but de dégrader ou d'interrompre l'accès du public au site Web et aux ressources d'une organisation.
- **Violation de données** – Il s'agit d'une attaque dans laquelle les serveurs de données ou les hôtes d'une organisation sont compromis pour voler des informations confidentielles.
- **Programme malveillant** – Il s'agit d'une attaque dans laquelle les hôtes d'une organisation sont infectés par des logiciels malveillants qui provoquent des problèmes différentes. Par exemple, un ransomware comme WannaCry chiffre les données sur un hôte et verrouille l'accès jusqu'à ce qu'une rançon soit payée.

## Les attaques de réseau au quotidien

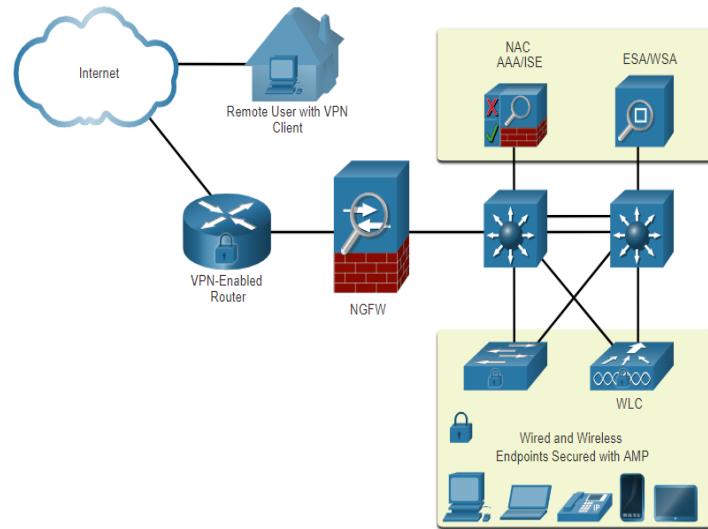
Divers appareils de sécurité du réseau sont nécessaires pour protéger le périmètre du réseau contre tout accès extérieur. Ces appareils peuvent inclure les éléments suivants:

- Un routeur activé VPN fournit une connexion sécurisée aux utilisateurs distants sur un réseau public et sur le réseau d'entreprise. Les services VPN peuvent être intégrés au pare-feu.
- Pare-feu de nouvelle génération (NGFW) - fournit une inspection des paquets avec état, une visibilité et un contrôle des applications, un système de prévention des intrusions de nouvelle génération (NGIPS), une protection avancée contre les logiciels malveillants (AMP) et un filtrage d'URL.
- Contrôle d'accès réseau (NAC) - comprend les services d'authentification, d'autorisation et de comptabilité (AAA). Dans les grandes entreprises, ces services peuvent être intégrés dans une appliance capable de gérer les politiques d'accès sur une grande variété d'utilisateurs et de types d'appareils. Le moteur de services d'identité de Cisco (ISE) est un exemple de périphérique NAC.

## Sécurité des terminaux

# Protection des terminaux

- Les terminaux sont des hôtes qui se composent généralement d'ordinateurs portables, d'ordinateurs de bureau, de serveurs et de téléphones IP, ainsi que les appareils appartenant aux employés. Les terminaux sont particulièrement sensibles aux attaques liées aux logiciels malveillants qui proviennent de la messagerie électronique ou de la navigation Web.
- Ces terminaux ont généralement utilisé des fonctionnalités de sécurité traditionnelles basées sur l'hôte, telles que l'antivirus / anti-programme malveillant, les pare-feu basés sur l'hôte et les systèmes de prévention des intrusions (HIPS) basés sur l'hôte.
- les terminaux sont mieux protégés par une combinaison de NAC, d'un logiciel AMP, d'un appliance de sécurité de messagerie (ESA) et d'un appliance de sécurité Web (WSA).



## La sécurité des terminaux

# Appliance pour la sécurité de la messagerie électronique Cisco

Cisco ESA est un appareil conçu pour surveiller le protocole SMTP (Simple Mail Transfer Protocol). Cisco ESA est constamment mis à jour par des flux en temps réel de Cisco Talos, qui détecte et corrèle les menaces et les solutions en utilisant un système de surveillance de base de données mondial. Ces données d'intelligence sur les menaces sont tiré par Cisco ESA chaque trois à cinq minutes.

Voici quelques-unes des fonctions de Cisco ESA:

- Bloquer les menaces connues
- Solution contre les logiciels malveillants furtifs qui ont échappé à la détection initiale.
- Annulez les e-mails contenant des liens incorrects
- Bloquer l'accès aux sites nouvellement infectés.
- chiffrez le contenu des e-mails sortants pour éviter la perte de données.

## Appliance pour la sécurité de la messagerie électronique Cisco

- L'appliance de sécurité Web Cisco (WSA) est une technologie d'atténuation des menaces Web. Il aide les organisations à relever les défis de la sécurisation et du contrôle du trafic Web.
- Cisco WSA combine une protection avancée contre les logiciels malveillants, la visibilité et le contrôle des applications, des contrôles de politique d'utilisation acceptable et des rapports.
- Cisco WSA offre un contrôle complet sur la façon dont les utilisateurs accèdent à Internet. Certaines fonctionnalités et applications, comme le chat, la messagerie, la vidéo et l'audio, peuvent être autorisées, limité avec le temps et de bande passante, ou bloquées, selon les besoins de l'organisation.
- Le WSA peut effectuer la liste noire des URL, le filtrage des URL, l'analyse des logiciels malveillants, la catégorisation des URL, le filtrage des applications Web et le chiffrement et le déchiffrement du trafic Web.

# 7.2 Le contrôle d'accès

# Authentification avec un mot de passe local

De nombreux types d'authentification peuvent être effectués sur des périphériques réseau, et chaque méthode offre différents niveaux de sécurité.

La méthode d'authentification d'accès à distance la plus simple est de configurer une combinaison d'identifiant et de mot de passe sur la console, les lignes vty et les ports auxiliaires.

SSH est une forme d'accès à distance plus sécurisée:

- Il nécessite un nom d'utilisateur et un mot de passe.
- Le nom d'utilisateur et le mot de passe peuvent être authentifiés locale.

La méthode de la base de données locale a certaines limites :

- Les comptes d'utilisateurs doivent être configurés localement sur chaque périphérique qui n'est pas évolutif.
- La méthode ne fournit aucune méthode d'authentification de secours.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

## Contrôle d'accès

# les Composants AAA

AAA signifie Authentification, Autorisation et Comptabilité et fournit le cadre principal pour configurer le contrôle d'accès sur un périphérique réseau.

L'AAA est un moyen de contrôle qui est autorisé à accéder à un réseau (authentifier), ce qu'ils peuvent faire pendant qu'ils sont là (autoriser), et de vérifier les actions effectuées lors de l'accès au réseau (comptabilité).

# L'authentification

L'authentification locale et l'authentification par serveur sont deux méthodes courantes de mise en œuvre de l'authentification AAA.

### L'authentification AAA locale:

- Est un méthode qui stocke les noms d'utilisateur et les mots de passe localement dans un périphérique réseau (par exemple le routeur Cisco).
- Les utilisateurs s'authentifient contre la base de données locale.
- L'authentification AAA locale est idéale pour les réseaux de petite taille.

### L'authentification AAA basée sur le serveur :

- Avec la méthode basée sur le serveur, le routeur accède à un serveur AAA central.
- Le serveur AAA contient les noms d'utilisateur et mot de passe pour tous les utilisateurs.
- Le routeur utilise les protocoles RADIUS (Service utilisateur d'accès à distance par authentification) ou TACACS+ (Contrôleur d'accès aux terminaux Système de contrôle d'accès) pour communiquer avec le serveur AAA.
- Lorsqu'il y a plusieurs routeurs et commutateurs, la méthode AAA basée sur le serveur est plus approprié.



# L'autorisation

- L'autorisation AAA est automatique et ne nécessite pas que les utilisateurs effectuent des étapes supplémentaires après l'authentification.
- L'autorisation régit ce que les utilisateurs peuvent et ne peuvent pas faire sur le réseau après leur authentification.
- L'autorisation utilise un ensemble d'attributs qui décrivent l'accès de l'utilisateur au réseau. Ces attributs sont utilisés par le serveur AAA pour déterminer les priviléges et les restrictions pour cet utilisateur.

# La comptabilité

La comptabilité AAA collecte et rapporte les données d'utilisation. Ces données peuvent être utilisées à des fins comme l'audit ou la facturation. Les données recueillies peuvent indiquer les heures de début et de fin des connexions, les commandes exécutées, le nombre de paquets et le nombre d'octets.

Une utilisation principale de la comptabilité est de la combiner avec l'authentification AAA.

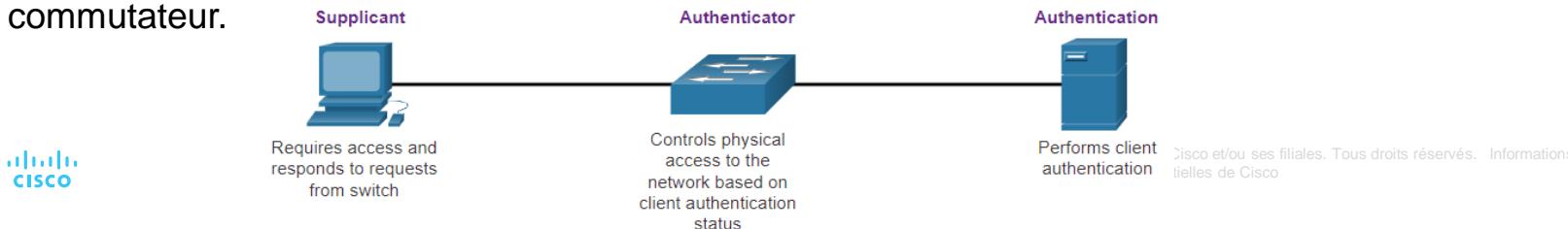
- Le serveur AAA conserve un journal détaillé de ce que l'utilisateur authentifié fait exactement sur le périphérique, comme indiqué sur la figure. Ce journal comprend toutes les commandes EXEC et les commandes de configuration exécutées par l'utilisateur.
- Il contient de nombreux champs de données, à savoir le nom d'utilisateur, la date et l'heure ainsi que les commandes saisies par l'utilisateur. Ces informations sont utiles lors du dépannage des appareils. Il fournit aussi des preuves lorsque des individus commettent des actes malveillants.

# Contrôle d'accès 802.1X

La norme IEEE 802.1X est un protocole de contrôle d'accès et d'authentification basé sur les ports. Ce protocole empêche les stations de travail non autorisées de se connecter à un réseau local via des ports de commutation accessibles au public. Avant de mettre à disposition les services offerts par le commutateur ou le LAN, le serveur d'authentification authentifie chaque station de travail connectée à un port de commutation.

Avec une authentification 802.1x basée sur les ports, les périphériques réseau ont des rôles spécifiques.

- **Le client (Demandeur)** - Il s'agit d'un appareil exécutant un logiciel client compatible 802.1X, qui est disponible pour les appareils câblés ou sans fil.
- **Le commutateur (authentificateur)** - Le commutateur peut servir d'intermédiaire entre le client et le serveur d'authentification. Il demande les informations d'identification du client, vérifie ces informations auprès du serveur d'authentification, puis transmet une réponse au client. Un autre périphérique qui pourrait faire office d'authentificateur est un point d'accès sans fil.
- **Le Serveur d'authentification** –Le serveur valide l'identité du client et informe le commutateur ou le point d'accès sans fil que le client est autorisé ou non à accéder au LAN et aux services de commutateur.



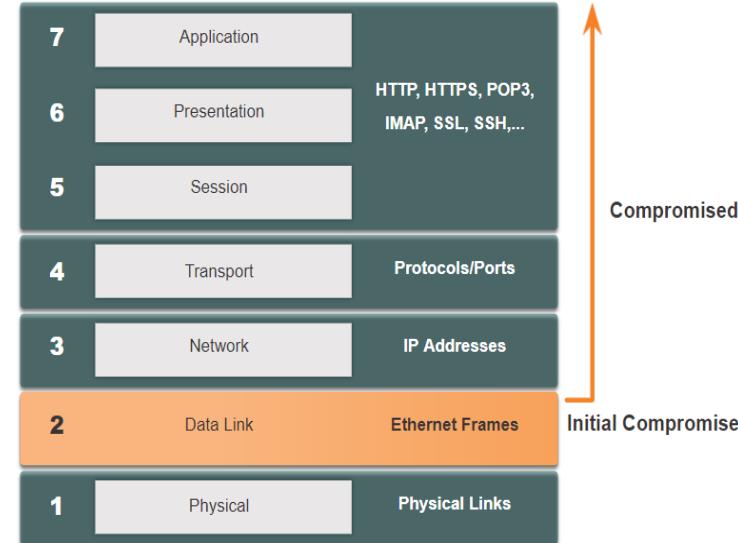
# 7.3 Menaces de sécurité de couche 2

# Vulnérabilités de couche 2

Rappelons que le modèle de référence OSI est divisé en sept couches qui fonctionnent indépendamment les unes des autres. La figure montre la fonction de chaque couche et les éléments centraux qui peuvent être exploités.

Les administrateurs du réseau implémentent régulièrement des solutions de sécurité pour protéger les éléments de la couche 3 à la couche 7. Ils utilisent des VPN, des pare-feu et des périphériques IPS pour protéger ces éléments.

Cependant, si la couche 2 est compromise, toutes les couches supérieures sont aussi affectées. Par exemple, si un acteur de menace ayant accès au réseau interne a capturé des trames de couche 2, alors toute la sécurité mise en œuvre sur les couches ci-dessus serait inutile. L'acteur de menace pourrait causer de nombreux dommages à l'infrastructure réseau LAN de couche 2.



# Les catégories d'attaque de commutateurs

La sécurité n'est aussi solide que le lien le plus faible du système, et la couche 2 est considérée comme ce lien faible. Cela est dû au fait que, les réseaux locaux étaient traditionnellement sous le contrôle administratif d'une seule organisation. Nous faisions intrinsèquement confiance à toutes les personnes et à tous les appareils connectés à notre réseau local. Aujourd'hui, avec le BYOD et des attaques plus sophistiquées, nos réseaux locaux sont devenus plus vulnérables à la pénétration.

Catégorie	Exemples
Les Attaques de table MAC	Il comprend les attaques par inondation de l'adresse MAC.
Attaques de VLAN	Il comprend les attaques par saut et par vérifier VLAN. Il aussi comprend les attaques entre les périphériques sur un VLAN commun.
Attaques DHCP	Il comprend les attaques d'insuffisance DHCP et les attaques d'usurpation DHCP.
Les attaques ARP	Il comprend les attaques d'usurpation ARP et les attaques d'empoisonnement ARP.
Attaques par usurpation d'adresse	Il comprend les attaques d'usurpation d'adresse MAC et d'adresse IP.
Les attaques STP	Il comprend les attaques de manipulation du protocole Spanning Tree.

# Les techniques d'atténuation des attaques de commutateur

La solution	Description
Sécurité des ports	Empêche de nombreux types d'attaques, y compris les attaques d'inondation d'adresses MAC et les attaques d'insuffisance DHCP.
Espionnage (snooping) DHCP	Empêche l'insuffisance DHCP et les attaques d'usurpation du DHCP.
Inspection ARP dynamique (DAI)	Empêche l'usurpation d'ARP et les attaques d'empoisonnement d'ARP.
Protection de la source IP (IPSG)	Empêche les attaques d'usurpation d'adresse MAC et IP.

Ces solutions de couche 2 ne seront pas efficaces si les protocoles de gestion ne sont pas sécurisés.

Les stratégies suivantes sont recommandées:

- Utilisez toujours des variantes sécurisées de protocoles de gestion telles que SSH, protocole de copie sécurisée (SCP), FTP sécurisé (SFTP) et couche de socket sécurisée / sécurité de la couche de transport (SSL / TLS).
- Considérez d'utiliser un réseau de gestion hors bande pour gérer les périphériques.
- Utilisez un VLAN de gestion dédié où ne réside rien d'autre que le trafic de gestion.
- Utilisez des listes de contrôle d'accès pour filtrer tout accès non indésirable.

# 7.4 Attaque du table d'adresse MAC

## Attaque du table d'adresses MAC

# Révision du fonctionnement de commutateur

Rappelez-vous cela pour prendre des décisions de transfert, un commutateur LAN de couche 2 construit un tableau basé sur les adresses MAC source dans les trames reçues. Cela s'appelle une table d'adresse MAC. Les tables d'adresses MAC sont stockées en mémoire et sont utilisées pour transmettre plus efficacement les trames.

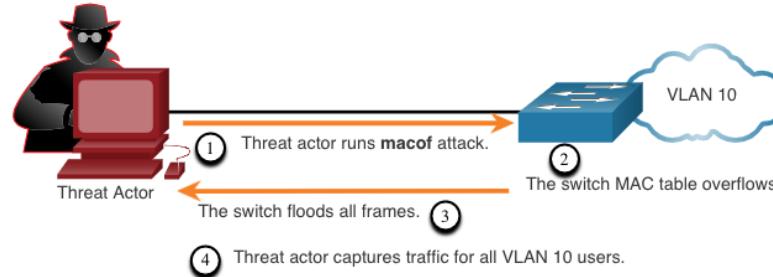
```
S1# show mac address-table dynamic
      Mac Address Table
-----
Vlan     Mac Address           Type      Ports
----     -----
  1      0001.9717.22e0        DYNAMIC   Fa0/4
  1      000a.f38e.74b3        DYNAMIC   Fa0/1
  1      0090.0c23.cea         DYNAMIC   Fa0/3
  1      00d0.ba07.8499        DYNAMIC   Fa0/2
S1#
```

# L'inondation (flooding) de table d'adresse MAC

Toutes les tables MAC ont une taille fixe et par conséquent, un commutateur peut manquer de ressources pour stocker les adresses MAC. Les attaques par inondation d'adresses MAC profitent de cette limitation en bombardant le commutateur avec de fausses adresses sources MAC jusqu'à ce que la table d'adresses MAC du commutateur soit pleine.

Lorsque cela se produit, le commutateur traite la trame comme une monodiffusion inconnue et commence à inonder tout le trafic entrant sur tous les ports du même VLAN sans référencer la table MAC. Cette condition permet désormais à un acteur de menace de capturer toutes les trames envoyées d'un hôte à un autre sur le LAN local ou le VLAN local.

**Remarque:** Le trafic n'est inondé que dans le LAN local ou le VLAN. L'acteur de menace ne peut capturer que le trafic au sein du LAN ou VLAN local auquel il est connecté.



## Attaque du table d'adresse MAC

# L'atténuation des attaques de table d'adresse MAC

Ce qui rend les outils tels que **macof** si dangereux, c'est qu'un attaquant peut créer une attaque de débordement de table MAC très rapidement. Par exemple, un commutateur Catalyst 6500 peut stocker 132,000 adresses MAC dans sa table d'adresse MAC. Un outil tel que **macof** peut inonder un commutateur avec jusqu'à 8,000 faux trames par seconde ; créant une attaque de débordement de table d'adresse MAC en quelques secondes.

Une autre raison pour laquelle ces outils d'attaque sont dangereux est qu'ils n'affectent pas seulement le commutateur local, ils peuvent aussi affecter les autres commutateurs de couche 2 connectés. Lorsque la table d'adresse MAC d'un commutateur est pleine, il commence à inonder tous les ports, y compris ceux qui sont connectés aux autres commutateurs de couche 2.

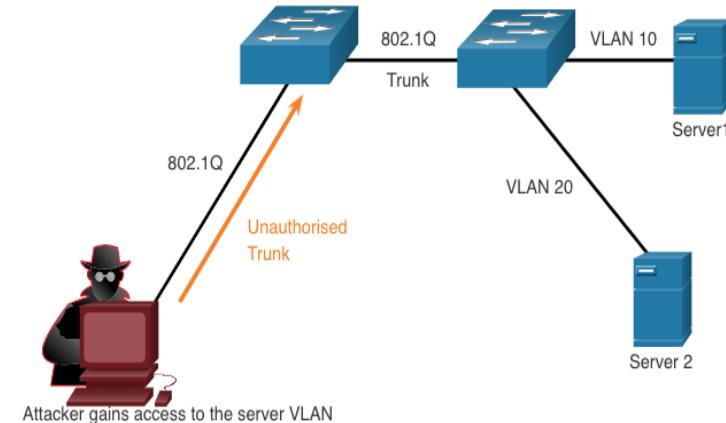
Pour atténuer les attaques de débordement de table d'adresse MAC, les administrateurs réseau doivent implémenter la sécurité des ports. La sécurité des ports ne permettra d'apprendre qu'un nombre spécifié d'adresses MAC sources sur le port. La sécurité des ports est discuté plus en détail dans un autre module.

# 7.5 Les attaques de réseau LAN

# Les attaques de saut de VLAN

Une attaque par saut de VLAN permet au trafic d'un VLAN d'être détecté par un autre VLAN sans l'aide d'un routeur. Dans une attaque de base de saut de VLAN, l'acteur de menace configure un hôte pour qu'il agisse comme un commutateur afin de profiter de la fonction de port de trunk automatique activée par défaut sur la plupart des ports de commutateur.

L'acteur de menace configure l'hôte pour usurper la signalisation 802.1Q et la signalisation DTP (Dynamic Trunking Protocol) propriétaire de Cisco pour le trunk avec le commutateur de connexion. En cas de succès, le commutateur établit une liaison de trunc avec l'hôte, comme illustré dans la figure. L'acteur de menace peut accéder tous les VLAN sur le commutateur. L'acteur de menace peut envoyer et recevoir du trafic sur n'importe quel VLAN, sautant efficacement entre les VLAN.



# Les Attaques de double étiquetage VLAN

Un acteur de menace est une situation spécifique qui pourrait incorporer une étiquette 802.1Q cachée dans la trame qui a déjà une étiquette 802.1Q. Cette balise permet à la trame d'accéder à un VLAN que l'étiquette 802.1Q d'origine n'a pas spécifié.

- **Étape 1:** L'acteur de menace envoie une trame 802.1Q double étiquetage au commutateur. L'en-tête externe a une étiquette VLAN de l'acteur de menace, qui est identique au VLAN natif du port trunc.
- **Étape 2:** La trame arrive sur le premier commutateur, qui examine la première étiquette 802.1Q de 4 octets. Le commutateur voit que la trame est destinée au VLAN natif. Le commutateur transfère le paquet sur tous les ports VLAN natifs après avoir divisé l'étiquette VLAN. La trame n'est pas réétiquetée car elle fait partie du VLAN natif. À ce stade, l'étiquette VLAN interne est toujours intacte et n'a pas été inspectée par le premier commutateur.
- **Étape 3:** La trame arrive au deuxième commutateur qui ne sait pas qu'elle était destinée au VLAN natif. Le trafic VLAN natif n'est pas étiqueté par le commutateur d'envoi selon la spécification 802.1Q. Le deuxième commutateur ne concerne que l'étiquetage 802.1Q interne que l'acteur de menace a insérée et indique que la trame est destinée au VLAN cible. Le deuxième commutateur envoie la trame à la cible ou l'inonde, selon qu'il existe une entrée de table d'adresses MAC existante pour la cible.

# Les attaques de double étiquetage VLAN (Cont.)

Une attaque de double étiquetage VLAN est unidirectionnelle et ne fonctionne que lorsque l'attaquant est connecté à un port résidant dans le même VLAN que le VLAN natif du port de trunk. L'idée est que le double étiquetage permet à l'attaquant d'envoyer des données à des hôtes ou des serveurs sur un VLAN qui autrement seraient bloqués par un certain type de configuration de contrôle d'accès.

Probablement, le trafic de retour sera aussi autorisé, ce qui donnera à l'attaquant la possibilité de communiquer avec des périphériques sur le VLAN normalement bloqué.

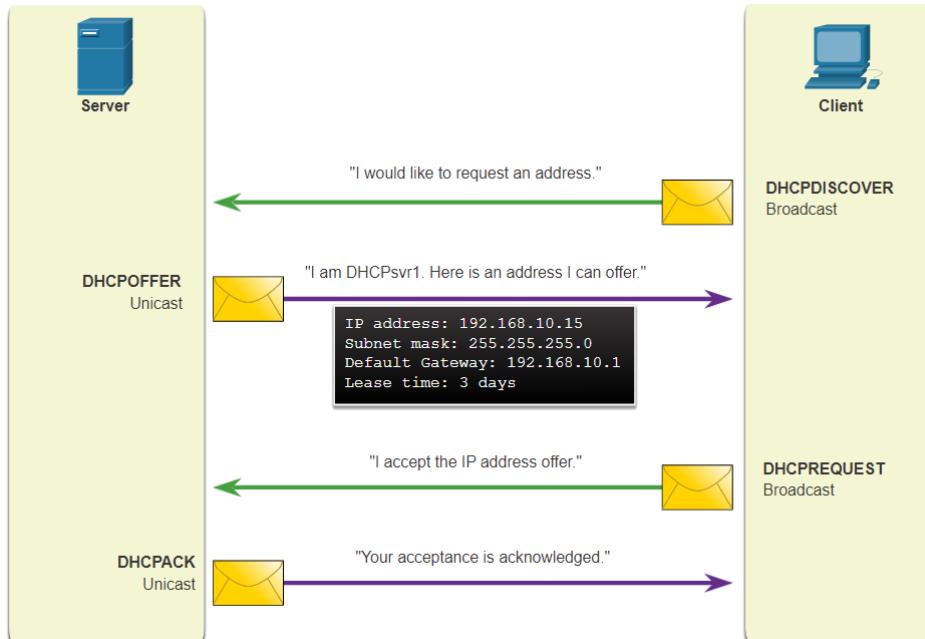
**L'attaque d'atténuation VLAN** - Les attaques de saut de VLAN et de double étiquetage VLAN peuvent être évitées en mettant en œuvre les directives de sécurité de trunk suivantes, comme indiqué dans un module précédent :

- Désactivez trunking sur tous les ports d'accès.
- Désactivez trunking automatique sur les liaisons de trunk afin que les trunks doivent être activées manuellement.
- Assurez-vous que le VLAN natif n'est utilisé que pour les liaisons de trunk.

## Les attaques de réseau LAN

# Les messages DHCP

Les serveurs DHCP fournissent aux clients les informations de configuration IP, notamment l'adresse IP, le masque de sous-réseau, la passerelle par défaut, les serveurs DNS, etc., et ce de manière dynamique. Une révision de la séquence de l'échange de messages DHCP entre le client et le serveur est illustré dans la figure.



# les attaques DHCP

Deux types d'attaques DHCP sont l'insuffisance DHCP et l'usurpation DHCP. Les deux attaques sont atténuées en mettant en œuvre l'espionnage DHCP.

- **L'attaque par insuffisance DHCP** – L'objectif d'une attaque par insuffisance DHCP est de créer un déni de service (DoS) pour connecter les clients. Les attaques par épuisement des ressources DHCP reposent sur un outil d'attaque, Gobbler, par exemple. Gobbler a la possibilité d'examiner l'intégralité des adresses IP louables et essaie de toutes les louer. Plus précisément, il crée des messages de découverte DHCP avec de fausses adresses MAC.
- **Attaque d'usurpation DHCP** – Cela se produit lorsqu'un serveur DHCP non autorisé (rogue) se connecte au réseau et fournit des paramètres de configuration IP incorrects aux clients légitimes. Un serveur non autorisé peut fournir des informations trompeuses, y compris les suivantes :
  - **Passerelle par défaut incorrecte** - Le serveur non autorisé fournit une passerelle non valide ou l'adresse IP de son hôte pour créer une attaque d'homme au milieu. Cette approche peut passer totalement inaperçue, car l'intrus intercepte le flux de données via le réseau.
  - **Serveur DNS incorrect** - Le serveur non autorisé fournit une adresse de serveur DNS incorrecte pointant l'utilisateur vers un site Web néfaste.
  - **Adresse IP incorrecte** - Le serveur non autorisé fournit une adresse IP invalide créant efficacement une attaque DoS sur le client DHCP.

### les attaques ARP

- Les hôtes diffusent des requêtes ARP pour déterminer l'adresse MAC d'un hôte avec une adresse IP de destination. Tous les hôtes du sous-réseau reçoivent et traitent la requête ARP. L'hôte dont l'adresse IP correspond à la requête ARP envoie une réponse ARP.
- Un client peut envoyer une réponse ARP non sollicitée appelé «ARP gratuite». les autres hôtes du sous-réseau stockent l'adresse MAC et l'adresse IP contenue par l'ARP gratuite dans leurs tables ARP.
- Un attaquant peut envoyer un message ARP gratuit contenant une adresse MAC usurpée à un commutateur, et le commutateur mettrait à jour sa table MAC en conséquence. Dans une attaque typique, un acteur de menace peut envoyer des réponses ARP non sollicitées à d'autres hôtes du sous-réseau avec l'adresse MAC de l'acteur de menace et l'adresse IP de la passerelle par défaut, configurant efficacement une attaque d'homme au milieu.
- Il existe de nombreux outils disponibles sur Internet pour créer des attaques ARP homme-au-milieu.
- IPv6 utilise le protocole de découverte de voisin ICMPv6 pour la résolution d'adresse de couche 2. IPv6 comprend des stratégies pour atténuer l'usurpation de publicité de voisin, de la même manière que IPv6 empêche une réponse ARP usurpée.
- L'usurpation ARP et l'empoisonnement ARP sont atténués par la mise en œuvre de l'inspection ARP dynamique (DAI).

# Les Attaques par usurpation d'adresse

- L'usurpation d'adresse IP est lorsqu'un acteur de menace détourne une adresse IP valide d'un autre périphérique sur le sous-réseau ou utilise une adresse IP aléatoire. L'usurpation d'adresse IP est difficile à atténuer, en particulier lorsqu'elle est utilisée à l'intérieur d'un sous-réseau auquel appartient l'IP.
- Les attaques d'usurpation d'adresse MAC se produisent lorsque les acteurs de menace modifient l'adresse MAC de leur hôte pour correspondre à une autre adresse MAC connue d'un hôte cible. Le commutateur remplace l'entrée de table MAC actuelle et attribue l'adresse MAC au nouveau port. Il transfère ensuite par inadvertance des trames destinées à l'hôte cible à l'hôte attaquant.
- Lorsque l'hôte cible envoie du trafic, le commutateur vérifiera l'erreur, en réalignant l'adresse MAC sur le port d'origine. Pour empêcher le commutateur de ramener l'affectation de port à son état correct, l'acteur de menace peut créer un programme ou un script qui enverra constamment des trames au commutateur afin que le commutateur conserve les informations incorrectes ou usurpées.
- Il n'y a pas de mécanisme de sécurité au couche 2 qui permet à un commutateur de vérifier la source des adresses MAC, ce qui le rend très vulnérable à l'usurpation.
- L'usurpation d'adresse IP et MAC peut être atténuée en implémentant IPSG.

## Les attaques de réseau LAN

### les attaques STP

- Les attaquants du réseau peuvent manipuler le protocole STP (Spanning Tree Protocol) pour mener une attaque en usurpant le pont racine et en modifiant la topologie d'un réseau. Les attaquants peuvent alors capturer tout le trafic pour le domaine commuté immédiat.
- Pour mener une attaque de manipulation STP, l'hôte attaquant diffuse des unités de données de protocole de pont STP (BPDU) contenant de configuration et de topologie obligera à réévaluer le spanning-tree. Les BPDU envoyés par l'hôte attaquant annoncent une priorité de pont inférieure pour tenter d'être élu pont racine.
- Cette attaque STP est atténuée par l'implémentation de BPDU Guard sur tous les ports d'accès. BPDU Guard est discuté plus en détail plus tard dans le cours.

### Reconnaissance CDP

Le protocole CDP (Cisco Discovery Protocol) est un protocole propriétaire de découverte de liaison de couche 2. Il est activé par défaut sur tous les périphériques Cisco. Les administrateurs réseau utilisent également le protocole CDP pour configurer et dépanner les périphériques réseau. les informations CDP sont envoyées sur les ports activés CDP dans des diffusions périodiques, non chiffrés et non authentifiées. Les données CDP incluent l'adresse IP du périphérique, la version logicielle IOS, la plate-forme, les fonctionnalités et le VLAN natif. Le périphérique qui reçoit le message CDP met à jour sa base de données CDP.

Pour réduire le risque d'attaque de CDP, limitez l'utilisation de ce protocole sur les périphériques et les ports. Par exemple, désactivez CDP sur les ports périphériques qui se connectent aux périphériques non fiables.

- Pour désactiver CDP globalement sur un périphérique, utilisez la commande du mode de configuration globale **no cdp run** . Pour activer CDP globalement, utilisez la commande de configuration globale **cdp run**
- Pour désactiver CDP sur un port, utilisez la commande de configuration d'interface **no cdp enable** Pour activer CDP sur un port, utilisez la commande de configuration d'interface **cdp enable**

**Remarque:** Le protocole LLDP (Link Layer Discovery Protocol) est aussi vulnérable aux attaques de reconnaissance. Configurez **no lldp run** pour désactiver LLDP globalement. Pour désactiver LLDP sur l'interface, configurez **no lldp transmite** et **no lldp receive**.

# 7.6 Pratique et questionnaire du module

# Qu'est-ce que j'ai appris dans ce module?

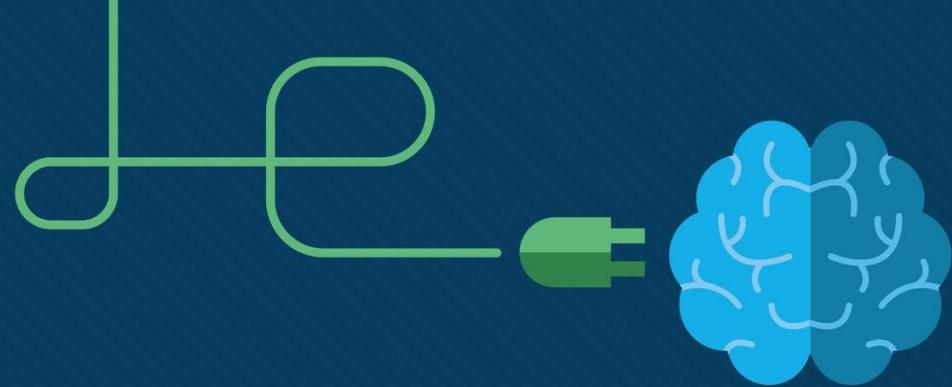
- Les terminaux sont particulièrement sensibles aux attaques liées aux logiciels malveillants qui proviennent de la messagerie électronique ou de la navigation Web, telles que DDOS, les violations de date et les logiciels malveillants. Ces terminaux ont généralement utilisé des fonctionnalités de sécurité traditionnelles basées sur l'hôte, telles que l'antivirus / anti-programme malveillant, les pare-feu basés sur l'hôte et les systèmes de prévention des intrusions (HIPS) basés sur l'hôte. Les points de terminaison sont mieux protégés par une combinaison de NAC, d'un logiciel AMP basé sur l'hôte, d'un appliance de sécurité de messagerie (ESA) et d'un appliance de sécurité Web (WSA).
- L'AAA contrôle qui est autorisé à accéder à un réseau (authentification), ce qu'il peut accomplir pendant qu'il est sur le réseau (autorisation), et pour vérifier les actions qu'il a effectuées pendant l'accès au réseau (comptabilité).
- La norme IEEE 802.1X est un protocole de contrôle d'accès et d'authentification basé sur les ports qui empêche les stations de travail non autorisées de se connecter à un LAN via des ports de commutation accessibles au public.
- Si la couche 2 est compromise, toutes les couches au-dessus sont également affectées. La première étape pour atténuer les attaques contre l'infrastructure de couche 2 consiste à comprendre le fonctionnement sous-jacentes de couche 2 et des solutions de couche 2: sécurité des ports, l'espionnage DHCP, DAI et IPSG. Ceux-ci ne fonctionneront que si les protocoles de gestion sont sécurisés.

## Qu'est-ce que j'ai appris dans ce module? (Suite)

- Les attaques par inondation d'adresses MAC bombardent le commutateur avec de fausses adresses sources MAC jusqu'à ce que la table d'adresses MAC du commutateur soit pleine.
- Une attaque par saut de VLAN permet au trafic d'un VLAN d'être détecté par un autre VLAN sans l'aide d'un routeur.
- Une attaque de double étiquetage VLAN est unidirectionnelle et ne fonctionne que lorsque l'acteur de menace est connecté à un port résidant dans le même VLAN que le VLAN natif du port de trunc.
- Les attaques par sauts et par double étiquetage de VLAN peuvent être évitées en appliquant les directives de sécurité des lignes réseau suivantes:
  - Désactivez trunking sur tous les ports d'accès.
  - Désactivez trunking automatique sur les liaisons de trunc afin que les trunks doivent être activées manuellement.
  - Assurez-vous que le VLAN natif n'est utilisé que pour les liaisons de trunc.
- Deux types d'attaques DHCP sont l'insuffisance DHCP et l'usurpation DHCP. Les deux attaques sont atténuées en mettant en œuvre l'espionnage DHCP.

# Qu'est-ce que j'ai appris dans ce module? (Suite)

- Attaque ARP: un acteur de menace envoie un message ARP gratuit contenant une adresse MAC usurpée à un commutateur, et le commutateur met à jour sa table MAC en conséquence. Désormais, l'acteur de menace envoie des réponses ARP non sollicitées à d'autres hôtes du sous-réseau avec l'adresse MAC de l'acteur de menace et l'adresse IP de la passerelle par défaut. L'usurpation ARP et l'empoisonnement ARP sont atténués par l'implémentation de DAI.
- Attaque d'usurpation d'adresse: l'usurpation d'adresse IP se produit lorsqu'un acteur de menace détourne une adresse IP valide d'un autre appareil sur le sous-réseau ou utilise une adresse IP aléatoire. Les attaques d'usurpation d'adresse MAC se produisent lorsque les acteurs de menace modifient l'adresse MAC de leur hôte pour correspondre à une autre adresse MAC connue d'un hôte cible. L'usurpation d'adresse IP et MAC peut être atténuée en implémentant IPSG.
- Attaque STP: les acteurs de menace manipulent STP pour mener une attaque en usurpant le pont racine et en changeant la topologie d'un réseau. Les attaquants peuvent faire apparaître leurs hôtes comme des ponts racine; et par conséquent, capturent tout le trafic pour le domaine commuté immédiat. Cette attaque STP est atténuée par l'implémentation de BPDU Guard sur tous les ports d'accès.
- Reconnaissance CDP: les informations CDP sont envoyées sur les ports activés CDP dans des diffusions périodiques non chiffrés. Les données CDP incluent l'adresse IP du périphérique, la version logicielle IOS, la plate-forme, les fonctionnalités et le VLAN natif. Le périphérique recevant le message CDP met à jour sa base de données CDP. les informations fournies par CDP peuvent également être utilisées par un acteur de menace pour découvrir les vulnérabilités de l'infrastructure du réseau. Pour réduire le risque d'attaque de CDP, limitez l'utilisation de ce protocole sur les périphériques et les ports.



# Module 8 : Configuration de la sécurité du commutateur



# Objectifs de ce module

**Titre du module :** Configuration de la sécurité du commutateur

**Objectif du module:** configurer la sécurité des commutateurs pour atténuer les attaques LAN

Titre du rubrique	Objectif du rubrique
<b>Mise en œuvre de la sécurité des ports</b>	Implémentez la sécurité des ports pour atténuer les attaques de table d'adresses MAC.
<b>Atténuer les attaques VLAN</b>	Expliquez comment configurer le DTP et le VLAN natif pour atténuer les attaques de VLAN.
<b>Atténuer les attaques DHCP</b>	Expliquez comment configurer la surveillance DHCP pour atténuer les attaques DHCP.
<b>Atténuer les attaques ARP</b>	Expliquez comment configurer l'inspection ARP pour atténuer les attaques ARP.
<b>Atténuer les attaques STP</b>	Expliquez comment configurer PortFast et BPDU Guard pour atténuer les attaques STP.

# 8.1 Mettre en oeuvre la sécurité des ports

## Ports inutilisés sécurisés

Les attaques de couche 2 sont parmi les plus faciles à déployer pour les pirates, mais ces menaces peuvent également être atténuées avec certaines solutions de couche 2 courantes.

- Tous les ports (interfaces) du commutateur doivent être sécurisés avant que le commutateur ne soit déployé pour une utilisation en production. La façon dont un port est sécurisé dépend de sa fonction.
- Une méthode simple que de nombreux administrateurs utilisent pour protéger le réseau contre les accès non autorisés consiste à désactiver tous les ports inutilisés d'un commutateur. Naviguez vers chaque port inutilisé et émettez la commande **shutdown** de Cisco IOS. Si un port doit être réactivé plus tard, il peut être activé avec la commande **no shutdown** .
- Pour configurer une portée de ports, utilisez la commande **interface range** .

```
Switch(config)# interface range type module/first-number - last-number
```

## Atténuer les attaques de table d'adresses MAC

La méthode la plus simple et la plus efficace pour empêcher les attaques par débordement de la table d'adresses MAC consiste à activer la sécurité des ports.

- La sécurité des ports limite le nombre d'adresses MAC valides autorisées sur un port. Il permet à un administrateur de configurer manuellement les adresses MAC d'un port ou de permettre au commutateur d'apprendre dynamiquement un nombre limité d'adresses MAC. Lorsqu'un port configuré avec la sécurité de port reçoit une trame, l'adresse MAC du source de la trame est comparée à la liste des adresses MAC des sources sécurisées qui ont été configurées manuellement ou apprises dynamiquement port à un, la sécurité du port peut être utilisée pour contrôler l'accès non autorisé sur le port.
- En limitant le nombre d'adresses MAC autorisées sur un réseau.

## Mettre en œuvre la sécurité des ports

# Activer la sécurité des ports

La sécurité des ports est activée avec la commande **switchport port-security** en mode configuration de l'interface.

Notez que dans l'exemple, la commande **switchport port-security** a été rejetée. C'est parce que, la sécurité des ports ne peut être configurée que sur des ports d'accès configurés manuellement ou des ports de trunk de réseau configurés manuellement.

Par défaut, les ports de commutateur de couche 2 sont réglés sur l'auto dynamique (trunking activée). Par conséquent, dans l'exemple, le port est configuré avec la commande **switchport mode access** en mode configuration de l'interface .

**Remarque:** la sécurité des ports trunk dépasse le cadre de ce cours.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

## Activer la sécurité des ports (Suite)

Utilisez la commande **show port-security interface** pour afficher les paramètres de sécurité de port actuels pour FastEthernet 0/1.

- Remarquez comment la sécurité des ports est activée, le mode de violation est arrêté et comment le nombre maximal d'adresses MAC est 1.
- Si un périphérique est connecté au port, le commutateur ajoute automatiquement l'adresse MAC du périphérique en tant que MAC sécurisé. Dans cet exemple, aucun périphérique n'est connecté au port.

**Remarque:** si un port actif est configuré avec la commande **switchport port-security** et que plusieurs périphériques sont connectés à ce port, le port passera à l'état désactivé par erreur.

```
S1# show port-security interface f0/1
Port Security          : Enabled
Port Status             : Secure-shutdown
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 0
Configured MAC Addresses : 0
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
S1#
```

## Activer la sécurité des ports (Suite)

Une fois la sécurité des ports est activée, d'autres spécificités de sécurité des ports peuvent être configurées, comme illustré dans l'exemple.

```
S1(config-if)# switchport port-security ?
      aging          Port-security aging commands
      mac-address   Secure mac address
      maximum        Max secure addresses
      violation      Security violation mode
      <cr>
S1(config-if)# switchport port-security
```

## Limiter et apprendre les adresses MAC

Pour définir le nombre maximal d'adresses MAC autorisées sur un port, utilisez la commande suivante:

```
Switch(config-if)# switchport port-security maximum value
```

- La valeur de sécurité du port par défaut est 1.
- Le nombre maximal d'adresses MAC sécurisées pouvant être configurées dépend du commutateur et de l'IOS.
- Dans cet exemple, le maximum est 8192.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
      <1-8192> Maximum addresses
S1(config-if)# switchport port-security maximum
```

## Limiter et apprendre les adresses MAC (Suite)

Le commutateur peut être configuré pour en savoir plus sur les adresses MAC sur un port sécurisé de trois manières:

**1. Configuration manuelle:** l'administrateur configure manuellement une ou des adresses MAC statiques à l'aide de la commande suivante pour chaque adresse MAC sécurisée sur le port:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

**2. Apprentissage dynamique:** lorsque la commande **switchport port-security** est entrée, le MAC source actuel du périphérique connecté au port est automatiquement sécurisé mais n'est pas ajouté à la configuration en cours. Si le commutateur est redémarré, le port devra réapprendre l'adresse MAC du périphérique.

**3. Apprentissage dynamique - Sticky:** l'administrateur peut activer le commutateur pour apprendre dynamiquement les adresses MAC et les «coller» à la configuration en cours en utilisant la commande suivante:

```
Switch(config-if)# switchport port-security mac-address sticky
```

L'enregistrement de la configuration en cours valide l'adresse MAC apprise dynamiquement dans la NVRAM.

# Limiter et apprendre les adresses MAC(Suite)

L'exemple illustre une configuration de sécurité de port complète pour FastEthernet 0/1.

- L'administrateur spécifie un maximum de 4 adresses MAC, configure manuellement une adresse MAC sécurisée, puis configure le port pour apprendre dynamiquement des adresses MAC sécurisées supplémentaires jusqu'à 4 adresses MAC sécurisées au maximum.
- Utilisez les commandes **show port-security interface** et **show port-security address** pour vérifier la configuration.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 4
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security          : Enabled
Port Status             : Secure-up
Violation Mode         : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses     : 1
Configured MAC Addresses : 1
Sticky MAC Addresses    : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
S1# show port-security address
               Secure Mac Address Table
-----+-----+-----+-----+-----+
Vlan  Mac Address      Type        Ports      Remaining Age
                  (mins)
-----+-----+-----+-----+-----+
1     aaaa.bbbb.1234    SecureConfigured  Fa0/1      -
-----+-----+-----+-----+-----+
Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

# Obsolescence de la sécurité des ports (suite)

L'obsolescence de la sécurité des ports peut être utilisée pour définir le temps d'obsolescence des adresses sécurisées statiques et dynamiques sur un port.

- **Absolue** - Les adresses sécurisées sur le port sont supprimées après le temps d'obsolescence spécifié.
- **Inactivité** - Les adresses sécurisées sur le port sont supprimées si elles sont inactives pendant une durée spécifiée.

Utilisez l'obsolescence pour supprimer les adresses MAC sécurisées sur un port sécurisé sans supprimer manuellement les adresses MAC sécurisées existantes.

- L'obsolescence des adresses sécurisées configurées statiquement peut être activé ou désactivé par port.

Utilisez la commande **switchport port-security aging** pour activer ou désactiver l'obsolescence statique pour le port sécurisé, ou pour définir le temps ou le type d'obsolescence.

```
Switch(config-if)# switchport port-security aging {static | time time | type {absolute | inactivity}}
```

## Obsolescence de la sécurité des ports (suite)

L'exemple montre un administrateur configurant le type d'obsolescence à 10 minutes d'inactivité.

La commande **show port-security** confirme les modifications. la commande

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security           : Enabled
Port Status              : Secure-shutdown
Violation Mode          : Restrict
Aging Time               : 10 mins
Aging Type               : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses    : 4
Total MAC Addresses       : 1
Configured MAC Addresses : 1
Sticky MAC Addresses      : 0
Last Source Address:Vlan : 0050.56be.e4dd:1
Security Violation Count : 1
```

## Modes de violation de la sécurité des ports

Si l'adresse MAC d'un périphérique connecté à un port diffère de la liste des adresses sécurisées, une violation de port se produit et le port entre dans l'état désactivé par erreur.

- Pour définir le mode de violation de sécurité du port, utilisez la commande suivante:

```
Switch(config-if)# switchport port-security violation {shutdown | restrict | protect}
```

Le tableau suivant montre comment un commutateur réagit en fonction du mode de violation configuré.

Mode	Description
<b>shutdown</b> (par défaut)	Le port passe immédiatement à l'état désactivé par erreur, éteint la LED du port et envoie un message Syslog. Il incrémente le compteur de violations. Lorsqu'un port sécurisé est dans l'état désactivé par erreur, un administrateur doit le réactiver en entrant les commandes <b>shutdown</b> and <b>no shutdown</b>
<b>restrict</b>	Le port supprime les paquets dont l'adresse source est inconnue jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées pour passer en dessous de la valeur maximale ou augmenter la valeur maximale. Ce mode entraîne l'incrémentation du compteur de violation de sécurité et génère un message syslog.
<b>protect</b>	Il s'agit du mode de violation de sécurité le moins sécurisé. Le port supprime les paquets avec des adresses source MAC inconnues jusqu'à ce que vous supprimiez un nombre suffisant d'adresses MAC sécurisées pour descendre en dessous de la valeur maximale ou augmenter la valeur maximale. Aucun message Syslog n'est envoyé.

## Modes de violation de la sécurité des ports (suite)

L'exemple montre un administrateur remplaçant la violation de sécurité par «Restreindre».

La sortie de la commande **show port-security interface** confirme que la modification a été effectuée.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security           : Enabled
Port Status              : Secure-shutdown
Violation Mode          : Restrict
Aging Time               : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 4
Total MAC Addresses      : 1
Configured MAC Addresses : 1
Sticky MAC Addresses     : 0
Last Source Address:Vlan : 0050.56be.e4dd:1
Security Violation Count : 1
S1#
```

## Mettre en œuvre la sécurité des ports

### Ports en état désactivé par erreur

Quand un port est fermé et placé dans l'état error-disabled, aucun trafic n'est envoyé ou reçu sur ce port

Une série de messages liés à la sécurité des ports s'affiche sur la console, comme illustré dans l'exemple suivant.

**Remarque:** Le protocole de port et l'état de la liaison passent à l'état bas et le voyant du port est éteint.

```
*Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting Fa0/18 in  
err-disable state  
*Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC  
address 000c.292b.4c75 on port FastEthernet0/18.  
*Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on Interface FastEthernet0/18, changed state  
to down  
*Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

# Ports en état désactivé par erreur (suite)

- Dans l'exemple, la commande **show interface** identifie l'état du port comme étant **err-disabled**. La sortie de la commande **show port-security interface** affiche désormais l'état du port comme étant **secure-shutdown**. Le compteur de violation de sécurité incrémente de 1.
- L'administrateur doit déterminer la cause de la violation de sécurité. Si un périphérique non autorisé est connecté à un port sécurisé, la menace de sécurité est éliminée avant de réactiver le port.
- Pour réactiver le port, utilisez d'abord la commande **shutdown** puis utilisez la commande **no shutdown**.

```
S1# show interface fa0/18
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)

S1# show port-security interface fa0/18
Port Security           : Enabled
Port Status              : Secure-shutdown
Violation Mode          : Shutdown
Aging Time               : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses    : 1
Total MAC Addresses       : 1
Configured MAC Addresses : 1
Sticky MAC Addresses      : 0
Last Source Address:Vlan : c025.5cd7.ef01:1
Security Violation Count : 1

S1#
```

## Mettre en œuvre la sécurité des ports

# Vérifier la sécurité des ports

Après avoir configuré la sécurité des ports sur un commutateur, vérifiez chaque interface pour vérifier que la sécurité des ports est correctement définie et assurez-vous que les adresses MAC statiques ont été correctement configurées.

Pour afficher les paramètres de sécurité des ports pour le commutateur, utilisez la commande **showport-security** .

- L'exemple indique que les 24 interfaces sont configurées avec la commande **switchport port-security** car le maximum autorisé est 1 et le mode de violation est arrêté.
- Aucun périphérique n'est connecté, par conséquent, le CurrentAddr (Count) est 0 pour chaque interface.

S1# show port-security					
Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action	
Fa0/1	1	0	0	Shutdown	
Fa0/2	1	0	0	Shutdown	
Fa0/3	1	0	0	Shutdown	
(output omitted)					
Fa0/24	1	0	0	Shutdown	
Total Addresses in System (excluding one mac per port) : 0					
Max Addresses limit in System (excluding one mac per port) : 4096					
Switch#					

## Vérifier la sécurité des ports(suite)

Utilisez la commande **show port-security interface** pour afficher les détails d'une interface spécifique, comme indiqué précédemment et dans cet exemple.

```
S1# show port-security interface fastethernet 0/18
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0025.83e6.4b01:1
Security Violation Count : 0
S1#
```

## Mettre en œuvre la sécurité des ports

# Vérifier la sécurité des ports(suite)

Pour vérifier que les adresses MAC «collent» à la configuration, utilisez la commande **show run** comme indiqué dans l'exemple pour FastEthernet 0/19.

```
S1# show run | begin interface FastEthernet0/19
interface FastEthernet0/19
switchport mode access
switchport port-security maximum 10
switchport port-security
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0025.83e6.4b02
(output omitted)
S1#
```

# Vérifier la sécurité des ports(suite)

Pour afficher toutes les adresses MAC sécurisées configurées manuellement ou apprises dynamiquement sur toutes les interfaces de commutateur, utilisez la commande **show port-security address** comme indiqué dans l'exemple.

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

```
Secure Mac Address Table
```

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
---	---	---	---	---
1	0025.83e6.4b01	SecureDynamic	Fa0/18	-
1	0025.83e6.4b02	SecureSticky	Fa0/19	-

```
Total Addresses in System (excluding one mac per port) : 0  
Max Addresses limit in System (excluding one mac per port) : 8192  
S1#
```

Mettre en œuvre la sécurité des ports

## Packet Tracer – Mettre en œuvre la sécurité des ports

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Partie 1: Configuration de la sécurité des ports
- Partie 2: Vérification de la sécurité des ports
- **LAB08.1-PortSecurity**

# 8.2 Atténuer les attaques VLAN

# Revue des attaques VLAN

Une attaque par saut de VLAN peut être lancée de trois manières:

- Usurpation des messages DTP de l'hôte attaquant pour que le commutateur passe en mode de jonction. À partir de là, l'attaquant peut envoyer du trafic étiqueté avec le VLAN cible, et le commutateur délivre ensuite les paquets à la destination.
- Présentation d'un commutateur escroc et activation de la jonction. L'attaquant peut alors accéder à tous les VLAN sur le commutateur victime à partir du commutateur non autorisé.
- Un autre type d'attaque par saut de VLAN est une attaque à double marquage (ou à double encapsulation). Cette attaque tire parti du fonctionnement du matériel sur la plupart des commutateurs.

# Étapes pour atténuer les attaques de saut de VLAN

Utilisez les étapes suivantes pour atténuer les attaques par saut de VLAN:

**Étape 1:** désactivez les négociations DTP (jonction automatique) sur les ports sans jonction à l'aide de la commande de configuration de l'interface **switchport mode access**.

**Étape 2:** désactivez les ports inutilisés et placez-les dans un VLAN inutilisé.

**Étape 3:** Activez manuellement la liaison de jonction sur un port de jonction à l'aide de la commande **switchport mode trunk**.

**Étape 4:** désactivez les négociations DTP (trunking automatique) sur les ports de jonction à l'aide de la commande **switchport nonegotiate**.

**Étape 5:** définissez le VLAN natif sur un VLAN autre que VLAN 1 à l'aide de la commande **switchport trunk native vlan vlan\_number**.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

# 8.3 Atténuer les attaques DHCP

# Revue d'attaque DHCP

Le but d'une attaque de famine DHCP est d'utiliser un outil d'attaque tel que Gobbler pour créer un déni de service (DoS) pour connecter les clients.

Rappelez-vous que les attaques de famine DHCP peuvent être efficacement atténuées en utilisant la sécurité des ports car Gobbler utilise une adresse MAC source unique pour chaque demande DHCP envoyée. Cependant, l'atténuation des attaques d'usurpation DHCP nécessite plus de protection.

Gobbler peut être configuré pour utiliser l'adresse MAC de l'interface réelle comme adresse Ethernet source, mais spécifiez une adresse Ethernet différente dans la charge utile DHCP. Cela rendrait la sécurité du port inefficace car l'adresse MAC source serait légitime.

Les attaques d'usurpation DHCP peuvent être atténuées en utilisant la surveillance DHCP sur les ports approuvés.

# Surveillance du DHCP

La surveillance DHCP filtre les messages DHCP et limite le trafic DHCP sur les ports non approuvés.

- Les périphériques sous contrôle administratif (par exemple, les commutateurs, les routeurs et les serveurs) sont des sources fiables.
- Les interfaces sécurisées (par exemple, liaisons de jonction, ports de serveur) doivent être explicitement configurées comme sécurisées.
- Les périphériques en dehors du réseau et tous les ports d'accès sont généralement traités comme des sources non fiables.

Une table DHCP est créée qui inclut l'adresse MAC source d'un périphérique sur un port non approuvé et l'adresse IP attribuée par le serveur DHCP à ce périphérique.

- L'adresse MAC et l'adresse IP sont liées ensemble.
- Par conséquent, cette table est appelée table de liaison d'espionnage DHCP.

## Étapes pour implémenter la surveillance DHCP

Utilisez les étapes suivantes pour activer la surveillance DHCP (snooping):

**Étape 1.** Activez la surveillance DHCP à l'aide de la commande de configuration globale **ip dhcp snooping** .

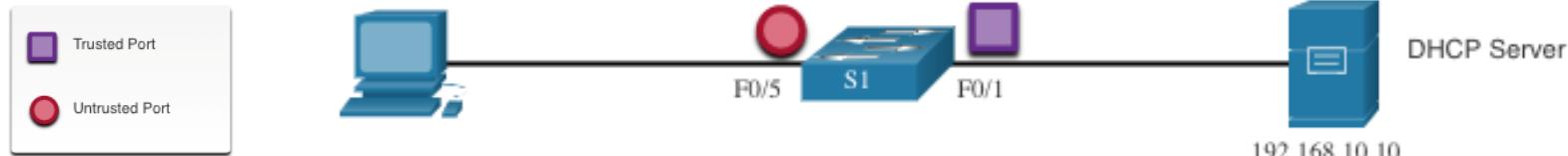
**Étape 2.** Sur les ports approuvés, utilisez la commande de configuration de l'interface **ip dhcp snooping trust** .

**Étape 3:** sur les interfaces non fiables, limitez le nombre de messages de découverte DHCP pouvant être reçus à l'aide de la commande **ip dhcpsnooping limit rate packets-per-second** en mode configuration d'interface .

**Étape 4.** Activez la surveillance DHCP par VLAN, ou par une portée de VLAN, en utilisant la commande de configuration globale **ip dhcp snooping vlan** .

# Exemple de configuration de surveillance DHCP

Reportez-vous à l'exemple de topologie de surveillance DHCP avec des ports approuvés et non approuvés.



- La surveillance DHCP est d'abord activé sur S1.
- L'interface en amont du serveur DHCP est explicitement approuvée.
- F0 / 5 à F0 / 24 ne sont pas approuvés et sont donc limités à six paquets par seconde.
- Enfin, la surveillance DHCP est activée sur les VLANS 5, 10, 50, 51 et 52.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

# Exemple de configuration de surveillance DHCP

Utilisez la commande EXEC privilégiée **show ip dhcp snooping** pour vérifier les paramètres de surveillance DHCP.

Utilisez la commande **show ip dhcp snooping binding** pour afficher les clients qui ont reçu des informations DHCP.

**Remarque:** La surveillance DHCP est également requis par l'inspection ARP dynamique (DAI).

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
    circuit-id default format: vlan-mod-port
    remote-id: 0cd9.96d2.3f80 (MAC)
option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface          Trusted      Allow option     Rate limit (pps)
-----          -----      -----          -----
FastEthernet0/1      yes        yes            unlimited
    Custom circuit-ids:
FastEthernet0/5      no         no              6
    Custom circuit-ids:
FastEthernet0/6      no         no              6
    Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress          IpAddress      Lease(sec)  Type           VLAN Interface
-----          -----          -----          -----          -----
00:03:47:B5:9F:AD  192.168.10.10  193185      dhcp-snooping  5      FastEthernet0/5
```

# 8.4 Atténuer les attaques d'ARP

# Inspection ARP dynamique

Dans une attaque ARP typique, un acteur de menace peut envoyer des réponses ARP non sollicitées à d'autres hôtes du sous-réseau avec l'adresse MAC de l'acteur de menace et l'adresse IP de la passerelle par défaut. Pour empêcher l'usurpation ARP et l'empoisonnement ARP qui en résulte, un commutateur doit garantir que seules les demandes et réponses ARP valides sont relayées.

L'inspection ARP dynamique (DAI) nécessite la surveillance DHCP et aide à prévenir les attaques ARP en:

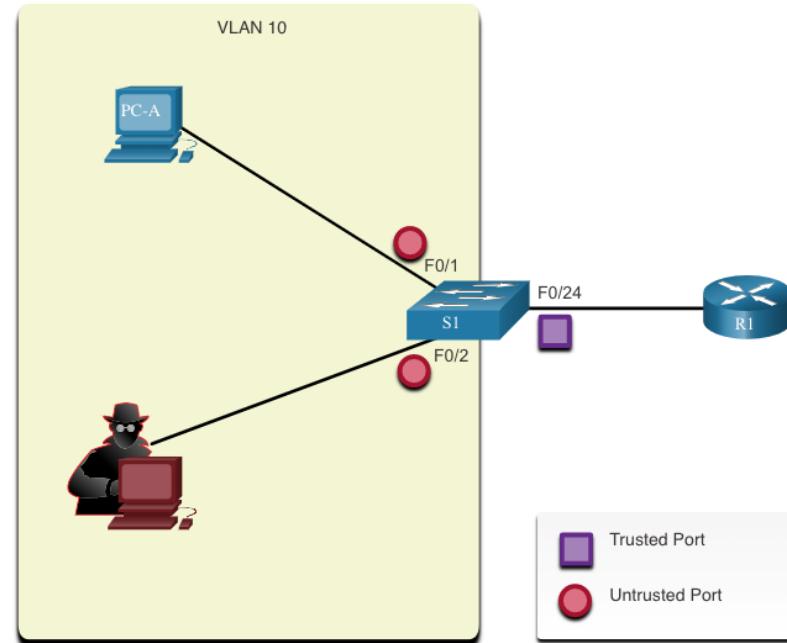
- Ne pas relayer les réponses ARP non valides ou gratuites vers d'autres ports du même VLAN.
- Interception de toutes les demandes et réponses ARP sur des ports non approuvés.
- Vérification de chaque paquet intercepté pour une liaison IP-MAC valide.
- Abandon et journalisation des réponses ARP provenant de non valides pour empêcher l'empoisonnement ARP.
- Erreur-désactivation de l'interface si le nombre DAI de paquets ARP configuré est dépassé.

# Directives d'implémentation DAI

Pour atténuer les risques d'usurpation ARP et d'empoisonnement ARP, suivez ces directives d'implémentation DAI:

- Activez globalement la surveillance DHCP.
- Activez la surveillance DHCP sur les VLAN sélectionnés.
- Activez DAI sur les VLAN sélectionnés.
- Configurez des interfaces sécurisées pour la surveillance DHCP et l'inspection ARP.

Il est généralement conseillé de configurer tous les ports de commutateur d'accès comme non approuvés et de configurer tous les ports de liaison montante qui sont connectés à d'autres commutateurs comme approuvés.



# Exemple de configuration DAI

Dans la topologie précédente, S1 connecte deux utilisateurs sur le VLAN 10.

- DAI sera configuré pour atténuer les attaques d'usurpation ARP et d'empoisonnement ARP.
- La surveillance DHCP est activée car DAI nécessite la table de liaison de surveillance DHCP pour fonctionner.
- Ensuite, la surveillance DHCP et l'inspection ARP sont activés pour les PC sur VLAN10.
- Le port de liaison montante vers le routeur est approuvé et est donc configuré comme approuvé pour la surveillance DHCP et l'inspection ARP.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

# Exemple de configuration DAI (suite)

DAI peut également être configuré pour vérifier les adresses MAC et IP de destination ou de source:

- **MAC destination** - vérifie l'adresse MAC de destination dans l'en-tête Ethernet par rapport à l'adresse MAC cible dans le corps ARP.
- **MAC source** - vérifie l'adresse MAC de source dans l'en-tête Ethernet par rapport à l'adresse MAC de l'expéditeur dans le corps ARP.
- **Adresse IP** - Vérifie le corps ARP pour les adresses IP invalides et inattendues, y compris les adresses 0.0.0.0, 255.255.255.255 et toutes les adresses de multidiffusion IP.

# Exemple de configuration DAI (suite)

La commande de configuration globale **ip arp inspection validate {[src-mac] [dst-mac] [ip]}** est utilisée pour configurer DAI pour supprimer les paquets ARP lorsque les adresses IP ne sont pas valides.

- Il peut être utilisé lorsque les adresses MAC dans le corps des paquets ARP ne correspondent pas aux adresses spécifiées dans l'en-tête Ethernet.
- Remarquez dans l'exemple suivant comment une seule commande peut être configurée.
- Par conséquent, la saisie de plusieurs commandes **ip arp inspection validate** écrase la commande précédente.
- Pour inclure plusieurs méthodes de validation, saisissez-les sur la même ligne de commande comme indiqué dans la sortie.

```
S1(config)# ip arp inspection validate ?
      dst-mac  Validate destination MAC address
      ip       Validate IP addresses
      src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#

```

# 8.5 Atténuer les attaques STP

## Atténuer les attaques STP

# PortFast et BPDU Guard

Rappelez-vous que les attaquants du réseau peuvent manipuler le protocole STP (Spanning Tree Protocol) pour mener une attaque en usurpant le pont racine et en modifiant la topologie d'un réseau. Pour atténuer les attaques STP, utilisez PortFast et Bridge Protocol Data Unit (BPDU) Guard:

### PortFast

- PortFast amène immédiatement un port à l'état de transfert à partir d'un état de blocage, en contournant les états d'écoute et d'apprentissage.
- Appliquer à tous les ports d'accès d'utilisateur final.

### BPDU Guard

- BPDU guard – Désactive immédiatement par erreur un port qui reçoit une unité BPDU.
- Comme PortFast, la protection BPDU (BPDU guard) ne doit être configurée que sur les interfaces connectées aux périphériques d'extrémité.

# Configurer PortFast

PortFast contourne les états d'écoute et d'apprentissage STP pour minimiser le temps que les ports d'accès doivent attendre pour que STP converge.

- Activez PortFast uniquement sur les ports d'accès.
- PortFast sur les liaisons inter-commutateurs peut créer une boucle de spanning-tree.

PortFast peut être activé:

- **Sur une interface** - Utilisez la commande de configuration d'interface **spanning-tree portfast**.
- **Globalement** - Utilisez la commande de configuration globale **spanning-tree portfast default** pour activer PortFast sur tous les ports d'accès.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
should now disable portfast explicitly on switched ports leading to hubs,
switches and bridges as they may create temporary bridging loops.
S1(config)# exit
```

## Configurer PortFast (suite)

Pour vérifier si PortFast est activé globalement, vous pouvez utiliser soit:

- **show running-config | begin span** commande
- **S1# show spanning-tree summary**

Pour vérifier si PortFast est activé sur une interface, utilisez la commande **show running-config interface type/number**.

La commande **spanning-tree interface type/number detail** peut également être utilisée pour la vérification.

# Configurer BPDU Guard

Un port d'accès pourrait recevoir des BPDU inattendus accidentellement ou parce qu'un utilisateur a connecté un commutateur non autorisé au port d'accès.

- Si une BPDU est reçue sur un port d'accès activé par BPDU Guard, le port est mis en état désactivé par erreur.
- Cela signifie que le port est arrêté et doit être réactivé manuellement ou récupéré automatiquement par la commande globale **errdisable recovery cause psecureViolation**.

BPDU Guard peut être activé:

- **Sur une interface** - Utilisez la commande de configuration d'interface **spanning-tree bpduguard enable**.
- **Globalement** - Utilisez la commande de configuration globale **spanning-tree portfast bpduguard default** pour activer BPDU Guard sur tous les ports d'accès.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID      is enabled
Portfast Default         is enabled
PortFast BPDU Guard Default is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default        is disabled
EtherChannel misconfig guard is enabled
UplinkFast               is disabled
BackboneFast              is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

# 8.6 Module pratique et questionnaire

# Packet Tracer - Configuration de la Sécurité de Commutateur

Dans cette activité Packet Tracer, vous allez:

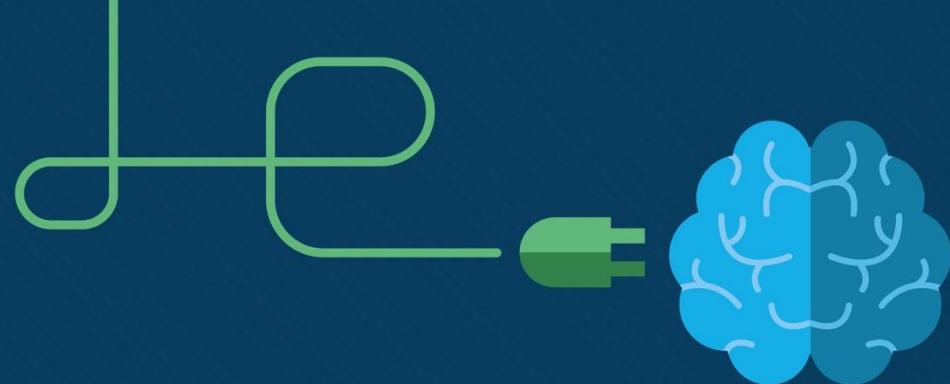
- Sécuriser les ports inutilisés
- Configurer la sécurité des ports
- Atténuer les attaques par saut de VLAN
- Atténuer les attaques DHCP
- Atténuer les attaques ARP
- Atténuer les attaques STP
- Vérifier la configuration de sécurité du commutateur
- **LAB08.2-SwitchSecurity**

## Qu'est-ce que j'ai appris dans ce module?

- Tous les ports (interfaces) du commutateur doivent être sécurisés avant que le commutateur ne soit déployé pour une utilisation en production.
- Par défaut, les ports de commutateur de couche 2 sont réglés sur l'auto dynamique (trunking activée).
- La méthode la plus simple et la plus efficace pour empêcher les attaques par débordement de la table d'adresses MAC consiste à activer la sécurité des ports.
- Le commutateur peut être configuré pour connaître les adresses MAC sur un port sécurisé de trois manières: configuré manuellement, appris dynamiquement et appris dynamiquement - collant.
- Si l'adresse MAC d'un périphérique connecté au port diffère de la liste des adresses sécurisées, une violation de port se produit. Par défaut, le port entre l'état error-disabled. Lorsqu'un port est placé dans l'état désactivé par erreur, aucun trafic n'est envoyé ou reçu sur ce port.
- Atténuez les attaques par sauts de VLAN en désactivant les négociations DTP, en désactivant les ports inutilisés, en définissant manuellement la jonction si nécessaire et en utilisant un VLAN natif autre que VLAN 1.

## Qu'est-ce que j'ai appris dans ce module? (Suite)

- L'objectif d'une attaque par insuffisance de ressources DHCP est de créer un déni de service (DoS) pour connecter les clients. Les attaques par usurpation DHCP peuvent être contrecarrées au moyen de fonctions de surveillance DHCP sur les ports de confiance.
- La surveillance DHCP détermine si les messages DHCP proviennent d'une source approuvée ou non approuvée configurée par l'administrateur. Il filtre ensuite les messages DHCP et limite le débit du trafic DHCP provenant de sources non fiables.
- L'inspection ARP dynamique (DAI) nécessite la surveillance DHCP et aide à prévenir les attaques ARP en vérifiant le trafic ARP.
- Implémentez l'inspection ARP dynamique pour atténuer l'usurpation d'identité ARP et l'empoisonnement ARP.
- Pour atténuer les attaques de manipulation du protocole Spanning Tree (STP), utilisez PortFast et Bridge Protocol Data Unit (BPDU) Guard.



# Module 9 : DHCPv4



# Objectifs de ce module

**Titre du module : DHCPv4**

**Objectif du module:** Mettre en œuvre le DHCPv4 pour opérer sur plusieurs réseaux locaux.

Titre du rubrique	Objectif du rubrique
<b>Concepts du DHCP4</b>	Expliquer comment le DHCPv4 fonctionne dans un réseau de petites et moyennes entreprises.
<b>Configurer un serveur DHCP4 Cisco IOS</b>	Configurer un routeur en tant que serveur DHCPv4.
<b>Configurer un client DHCPv4</b>	Configurer un routeur en tant que client DHCPv4.

# 9.1 Concepts du DHCPv4

# Serveur et client DHCPv4

- Le protocole DHCPv4 (Dynamic Host Configuration Protocol v4) attribue de manière dynamique les adresses IPv4 et d'autres informations de configuration du réseau. Comme les ordinateurs de bureau clients constituent la majorité des nœuds du réseau, le protocole DHCPv4 offre un gain de temps extrêmement précieux aux administrateurs réseau.
- Un serveur DHCPv4 dédié est évolutif et relativement facile à gérer. Cependant, dans le cas d'une petite filiale, d'un petit bureau ou d'un bureau à domicile, un routeur Cisco peut être configuré pour fournir les services DHCPv4, évitant ainsi l'achat d'un serveur dédié. Le logiciel IOS Cisco prend en charge un serveur optionnel DHCPv4 riche en fonctionnalités.
- Le serveur DHCPv4 attribue ou loue dynamiquement une adresse IPv4 à partir d'un pool d'adresses pendant une durée limitée définie par le serveur, ou jusqu'à ce que le client n'en ait plus besoin.
- Les clients louent les informations auprès du serveur pour la période définie par l'administrateur. Les administrateurs configurent les serveurs DHCPv4 pour que les baux dépassent le délai d'attente à différents intervalles. Le bail est généralement de 24 heures à une semaine ou plus. À l'expiration du bail, le client doit demander une autre adresse, même s'il obtient généralement la même.

# Fonctionnement DHCPv4

DHCPv4 fonctionne en mode client/serveur. Lorsqu'un client communique avec un serveur DHCPv4, le serveur attribue ou loue une adresse IPv4 à ce client.

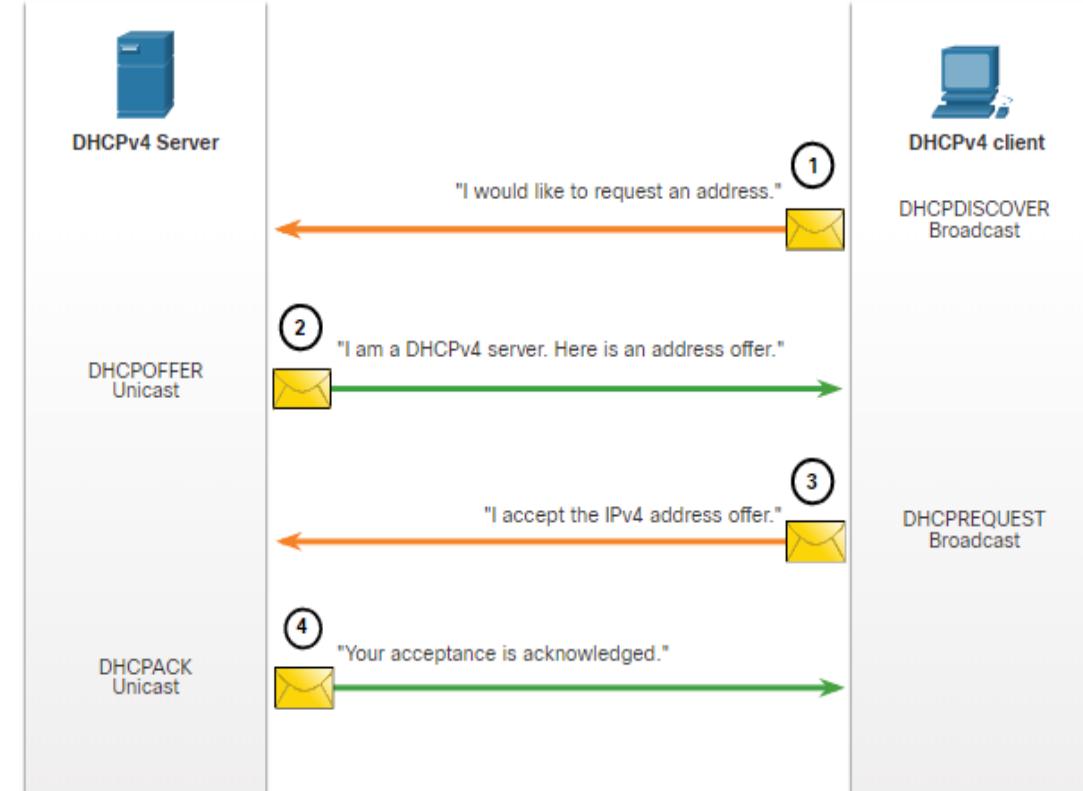
- Le client se connecte au réseau avec cette adresse IPv4 louée jusqu'à l'expiration du bail. Le client doit régulièrement contacter le serveur DHCP pour renouveler le bail.
- Ce mécanisme de bail permet de s'assurer que les clients qui sont déplacés ou qui sont mis hors tension ne conservent pas des adresses dont ils n'ont plus besoin.
- Lorsqu'un bail expire, le serveur DHCP renvoie l'adresse au pool où elle peut être réattribuée selon les besoins.

## Concepts du DHCPv4

# Etapes pour obtenir un bail

Lorsque le client démarre (ou souhaite se connecter à un réseau), il lance un processus en quatre étapes visant à obtenir un bail.

1. Détection DHCP (DHCPDISCOVER)
2. Offre DHCP (DHCPOFFER)
3. Requête DHCP (DHCPREQUEST)
4. Accusé de réception DHCP (DHCPACK)



# Etapes pour obtenir un bail

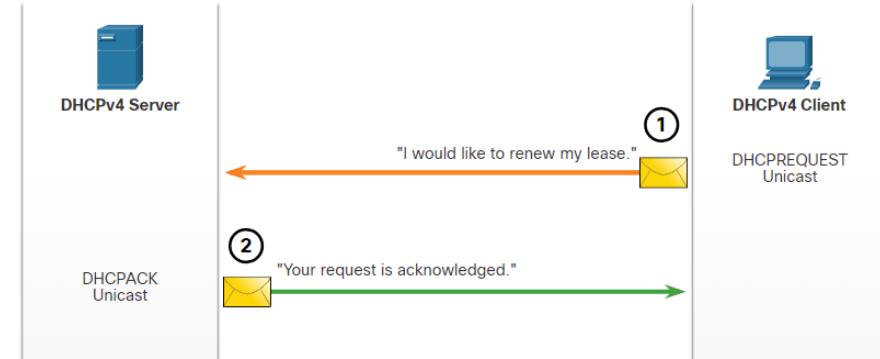
Avant l'expiration du bail, le client commence un processus en deux étapes pour renouveler le bail avec le serveur DHCPv4, comme illustré dans la figure :

## 1. Requête DHCP (DHCPREQUEST)

Avant l'expiration du bail, le client envoie un message DHCPREQUEST directement au serveur DHCPv4 qui a offert l'adresse IPv4 à l'origine. S'il ne reçoit aucun message DHCPACK dans un certain délai, le client diffuse un autre message DHCPREQUEST afin qu'un des autres serveurs DHCPv4 puisse renouveler le bail.

## 2. Accusé de réception DHCP (DHCPACK)

À la réception du message DHCPREQUEST, le serveur vérifie les informations relatives au bail en renvoyant un DHCPACK.



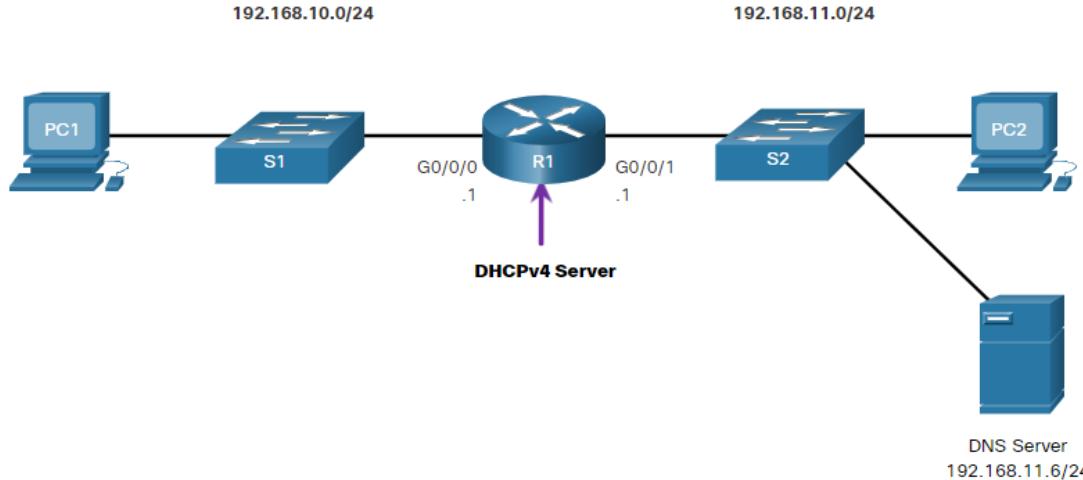
**Remarque:** ces messages (principalement DHCPOFFER et DHCPACK) peuvent être envoyés sous forme de monodiffusion ou de diffusion conformément à la spécification RFC 2131 de l'IETF.

# 9.2 Configurer un serveur Cisco IOS DHCPv4

# Configurer un serveur Cisco IOS DHCPv4

## Serveur Cisco IOS DHCPv4

Maintenant, vous avez une compréhension de base du fonctionnement de DHCPv4 et comment cela peut rendre votre travail un peu plus facile. Le logiciel Cisco IOS du routeur Cisco peut être configuré en tant que serveur DHCPv4. Le serveur DHCPv4 Cisco IOS attribue et gère les adresses IPv4 depuis les pools d'adresses spécifiés dans le routeur jusqu'aux clients DHCPv4.



## Etapes pour configurer un serveur Cisco IOS DHCPv4

Suivez les étapes suivantes pour configurer un serveur DHCPv4 Cisco IOS :

- **Étape 1.** Exclusion d'adresses IPv4 Une seule adresse ou une série d'adresses peut être exclue en spécifiant *l'adresse basse* et *l'adresse haute* de la série. Les adresses exclues doivent inclure les adresses attribuées aux routeurs, aux serveurs, aux imprimantes et aux autres périphériques qui ont été ou seront configurés manuellement. Vous pouvez également saisir la commande plusieurs fois. La commande est **ip dhcp excluded-address *low-address* [*high address*]**
- **Étape 2.** Définissez un nom de pool DHCPv4. La commande **ip dhcp pool *pool-name*** crée un pool avec le nom spécifié et met le routeur en mode de configuration DHCPv4, qui est identifié par l'invite **Router(dhcp-config)#**.

# Étapes pour configurer un serveur Cisco IOS DHCPv4 (suite.)

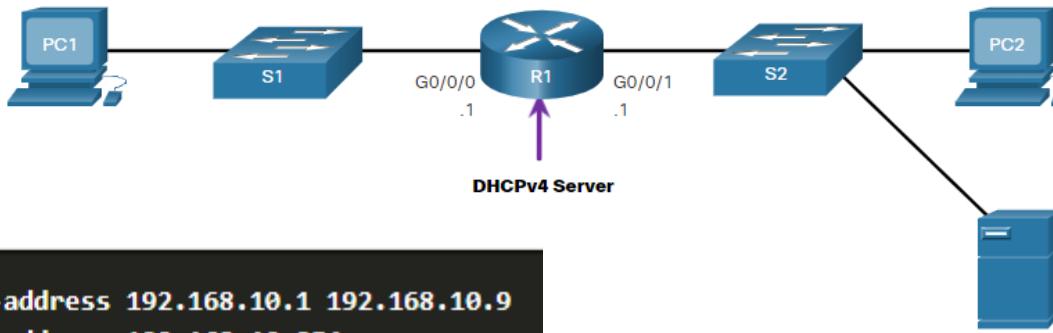
- Étape 3.** Configurez le pool DHCPv4. Le pool d'adresses et le routeur servant de passerelle par défaut doivent être configurés. Utilisez l'instruction **network** pour définir la plage d'adresses disponibles. Utilisez la commande **default-router** pour définir le routeur servant de passerelle par défaut. Ces commandes et d'autres commandes facultatives sont affichées dans le tableau.

Tâche	Commande IOS
Définir le pool d'adresses	<b>network</b> <i>network-number [mask   /prefix-length]prefix-length</i>
Définir le routeur ou la passerelle par défaut	<b>default-router</b> <i>address [ address2...address8]</i>
Définir un serveur DNS	<b>dns-server</b> <i>address [ address2...address8]</i>
Définir le nom de domaine	<b>domain-name</b> <i>domain</i>
Définir la durée du bail DHCP	<b>lease</b> { <i>days [hours [ minutes]]</i>   <b>infinite</b> }
Définir le serveur WINS NetBIOS	<b>netbios-name-server</b> <i>address [ address2...address8]</i>

# Configurer un serveur Cisco IOS DHCPv4

## Exemple de configuration

192.168.10.0/24                            192.168.11.0/24



```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
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 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

DNS Server  
192.168.11.6/24

## Vérification DHCPv4

Utilisez les commandes du tableau pour vérifier que le serveur Cisco IOS DHCPv4 est opérationnel.

Commande	Description
<b>show running-config   section dhcp</b>	Affiche les commandes DHCPv4 configurées sur le routeur.
<b>show ip dhcp binding</b>	Affiche une liste de toutes les liaisons entre les adresses IPv4 et les adresses MAC fournies par le service DHCPv4.
<b>show ip dhcp server statistics</b>	Affiche les informations de comptage concernant le nombre de messages DHCPv4 qui ont été envoyés et reçus

# Vérifiez que DHCPv4 est opérationnel

**Vérifiez la configuration DHCPv4 :** Comme le montre l'exemple, la sortie de la commande **show running-config | section dhcp** affiche les commandes DHCPv4 configurées sur R1. Le paramètre **| section** affiche uniquement les commandes liées à la configuration de DHCPv4.

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
  dns-server 192.168.11.5
  domain-name example.com
```

# Vérifiez que DHCPv4 est opérationnel (suite.)

**Vérifier les liaisons DHCPv4 :** Comme le montre l'exemple, le fonctionnement de DHCPv4 peut être vérifié en utilisant la commande **show ip dhcp binding**. Cette commande permet d'afficher la liste de toutes les liaisons entre adresse IPv4 et adresse MAC qui ont été fournies par le service DHCPv4.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
  IP address      Client-ID/          Lease expiration      Type      State       Interface
                Hardware address/
                User name
  192.168.10.10  0100.5056.b3ed.d8    Sep 15 2019 8:42 AM  Automatic  Active
  GigabitEthernet0/0/0
```

# Vérifiez que DHCPv4 est opérationnel (suite.)

## Vérifiez les statistiques du DHCPv4 :

La sortie de **show ip dhcp server statistics** est utilisée pour vérifier que les messages sont bien reçus ou envoyés par le routeur. Cette commande permet d'afficher le nombre de messages DHCPv4 envoyés et reçus.

```
R1# show ip dhcp server statistics
Memory usage          19465
Address pools          1
Database agents         0
Automatic bindings      2
Manual bindings         0
Expired bindings        0
Malformed messages      0
Secure arp entries      0
Renew messages          0
Workspace timeouts       0
Static routes           0
Relay bindings           0
Relay bindings active     0
Relay bindings terminated 0
Relay bindings selecting   0
Message                Received
BOOTREQUEST              0
DHCPDISCOVER              4
DHCPREQUEST               2
DHCPDECLINE                0
DHCPRELEASE                 0
DHCPINFORM                  0
```

# Vérifiez que DHCPv4 est opérationnel (suite)

## Vérifier l'adressage IPv4 du client

**DHCPv4** : la commande **ipconfig /all** , lorsqu'elle est émise sur PC1, affiche les paramètres TCP/IP, comme indiqué dans l'exemple. Comme PC1 était connecté au segment de réseau 192.168.10.0/24, il a automatiquement reçu un suffixe DNS, une adresse IPv4, un masque de sous-réseau, une passerelle par défaut et une adresse de serveur DNS de ce pool. Aucune configuration d'interface du routeur spécifique DHCP n'est requise.

Si un ordinateur est connecté à un segment de réseau ayant un pool DHCPv4 disponible, il peut obtenir automatiquement une adresse IPv4 du pool approprié.

```
C:\Users\Student> ipconfig /all
Windows IP Configuration
  Host Name . . . . . : ciscolab
  Primary Dns Suffix . . . . . :
  Node Type . . . . . : Hybrid
  IP Routing Enabled. . . . . : No
  WINS Proxy Enabled. . . . . : No
  Ethernet adapter Ethernet0:
    Connection-specific DNS Suffix . : example.com
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : 00-05-9A-3C-7A-00
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Lease Obtained . . . . . : Saturday, September 14, 2019 8:42:22AM
    Lease Expires . . . . . : Sunday, September 15, 2019 8:42:22AM
    Default Gateway . . . . . : 192.168.10.1
    DHCP Server . . . . . : 192.168.10.1
    DNS Servers . . . . . : 192.168.11.5
```

# Désactiver le serveur Cisco IOS DHCPv4

Le service DHCPv4 est activé par défaut. Pour désactiver le service, utilisez la commande **no service dhcp** du mode de configuration globale. Utilisez la commande **service dhcp** du mode de configuration global pour réactiver le processus du serveur DHCPv4, comme indiqué dans l'exemple. L'activation du service n'a aucun effet si les paramètres ne sont pas configurés.

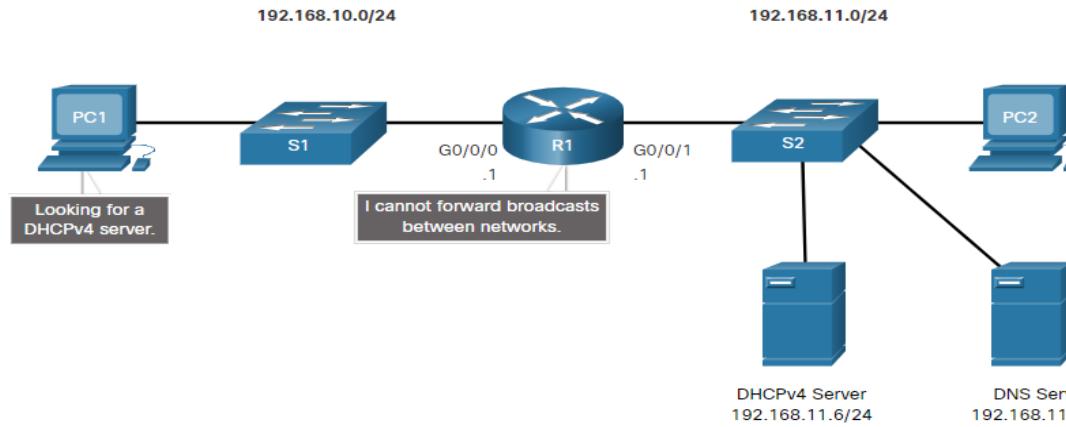
**Remarque:** l'effacement des liaisons DHCP ou l'arrêt et le redémarrage du service DHCP peuvent entraîner l'attribution temporaire d'adresses IP en double sur le réseau.

```
R1(config)# no service dhcp  
R1(config)# service dhcp  
R1(config)#
```

# Configurer un serveur Cisco IOS DHCPv4

## Relais DHCPv4

- Dans un réseau hiérarchique complexe, les serveurs d'entreprise sont généralement situés au niveau central. Ces serveurs peuvent fournir au réseau des services DHCP, DNS, TFTP et FTP. Les clients du réseau ne sont généralement pas sur le même sous-réseau que ces serveurs. Afin de localiser les serveurs et de bénéficier des services, les clients utilisent souvent des messages de diffusion.
- Dans la figure, PC1 tente d'acquérir une adresse IPv4 à partir d'un serveur DHCPv4 en utilisant un message de diffusion. Dans ce scénario, le routeur R1 n'est pas configuré en tant que serveur DHCPv4 et ne transmet pas la diffusion. Étant donné que le serveur DHCPv4 se trouve sur un autre réseau, PC1 ne peut pas recevoir d'adresse IP via DHCP. R1 doit être configuré pour relayer les messages DHCPv4 au serveur DHCPv4.



# Configurer un serveur Cisco IOS DHCPv4

## Relais DHCPv4

- Configurez R1 avec la commande de configuration de l'interface **ip helper-address address**. Cela entraînera R1 à relayer les diffusions DHCPv4 vers le serveur DHCPv4. Comme indiqué dans l'exemple, l'interface sur R1 recevant la diffusion à partir de PC1 est configurée pour relayer l'adresse DHCPv4 au serveur DHCPv4 à 192.168.11.6.
- Lorsque R1 a été configuré en tant qu'agent de relais DHCPv4, il accepte les requêtes de diffusion liées au service DHCPv4, puis transmet ces demandes en monodiffusion à l'adresse IPv4 192.168.11.6. L'administrateur réseau peut utiliser la commande **show ip interface** pour vérifier la configuration.

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
  (output omitted)
```

# Autres diffusions de service relayées

DHCPv4 n'est pas le seul service que le routeur peut relayer suite à une configuration spécifique. Par défaut, la commande **ip helper-address** transmet les huit services UDP suivants :

- Port 37: Time
- Port 49: TACACS
- Port 53: DNS
- Port 67: DHCP/BOOTP server
- Port 68: DHCP/BOOTP client
- Port 69: TFTP
- Port 137: NetBIOS name service
- Port 138: NetBIOS datagram service

# Packet Tracer - Configurer DHCPv4

Dans cette activité Packet Tracer, vous remplirez les objectifs suivants:

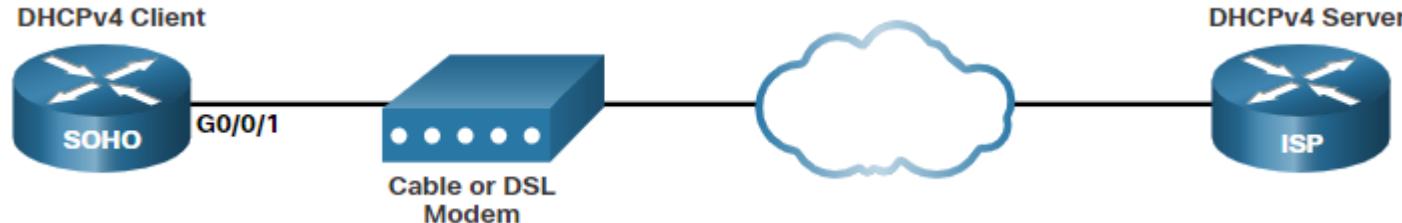
- Partie 1 : Configuration d'un routeur comme serveur DHCP
- Partie 2 : Configuration du relais DHCP
- Partie 3 : Configuration d'un routeur comme client DHCP
- Partie 4 : Vérification de DHCP et de la connectivité
- **LAB9.1-DHCP**

# 9.3 Configurer un client DHCPv4

# Routeur Cisco comme client DHCPv4

Dans certains cas, vous pourriez avoir accès à un serveur DHCP par l'intermédiaire de votre fournisseur d'accès Internet. Dans ces cas, vous pouvez configurer un routeur Cisco IOS en tant que client DHCPv4.

- Parfois, les routeurs Cisco installés dans des petites structures, des bureaux à domicile (SOHO) et des filiales doivent être configurés en tant que clients DHCPv4 de la même façon que les ordinateurs clients. La méthode utilisée dépend de l'ISP. Cependant, dans le cas de la configuration la plus simple, l'interface Ethernet est utilisée pour établir la connexion à un modem câble ou DSL.
- Pour configurer une interface Ethernet en tant que client DHCP, utilisez la commande de mode de configuration de l'interface **ip address dhcp interface**
- Dans la figure, supposons qu'un ISP ait été configuré pour fournir à certains clients des adresses IP de la gamme de réseaux 209.165.201.0/27 après que l'interface G0/0/1 ait été configurée avec la commande **ip address dhcp**.



# Configurer un client DHCPv4

## Exemple de configuration

- Pour configurer une interface Ethernet en tant que client DHCP, utilisez la commande de mode de configuration de l'interface **ip address dhcp**, comme indiqué dans l'exemple. Cette configuration suppose que le fournisseur de services Internet a été configuré pour fournir aux clients sélectionnés des informations d'adressage IPv4.
- La commande **show ip interface g0/1** confirme que l'interface est activée et que l'adresse a été allouée par un serveur DHCPv4.

```
SOHO(config)# interface G0/0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
Sep 12 10:01:25.773: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address
209.165.201.12, mask 255.255.255.224, hostname SOHO
```

```
SOHO# show ip interface g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
  (output omitted)
```

# Routeur domestique comme client DHCPv4

Les routeurs domestiques sont généralement déjà configurés pour recevoir automatiquement les informations d'adressage IPv4 d'ISP. Cela permet aux clients de configurer facilement le routeur et de se connecter à Internet.

- Par exemple, la figure montre la page de configuration WAN par défaut pour un routeur sans fil Packet Tracer. Remarquez que le type de connexion Internet est défini sur **Automatic Configuration - DHCP** (Configuration automatique - DHCP). Cette sélection est utilisée lorsque le routeur est connecté à un DSL ou à un modem câble et agit en tant que client DHCPv4, demandant une adresse IPv4 auprès de l'ISP.
- Divers fabricants de routeurs domestiques auront une configuration similaire.



# 9.4 Module pratique et questionnaire

# Travaux Pratiques - Mise en œuvre de DHCPv4

Dans ce Packet Tracer, vous aborderez les points suivants :

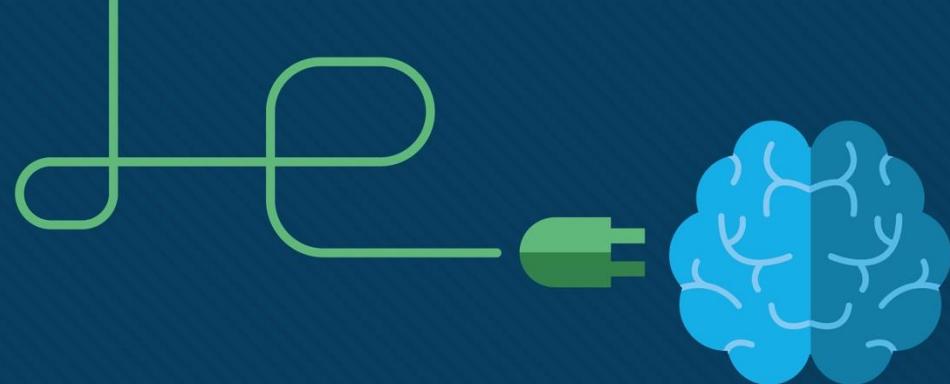
- Partie 1: Configurer un routeur comme serveur DHCP
- Partie 2: Configurer le relais DHCP
- Partie 3: Configurer un routeur comme client DHCP
- **LAB9.2-DHCP**

# Qu'est-ce que j'ai appris dans ce module?

- Le serveur DHCPv4 attribue dynamiquement, ou loue, une adresse IPv4 à un client à partir d'un pool d'adresses pour une période limitée choisie par le serveur, ou jusqu'à ce que le client n'ait plus besoin de l'adresse.
- Le processus de location DHCPv4 commence par l'envoi par le client d'un message demandant les services d'un serveur DHCP. S'il y a un serveur DHCPv4 qui reçoit le message, il répondra avec une adresse IPv4 et d'autres informations de configuration réseau possibles.
- Le client doit régulièrement contacter le serveur DHCP pour renouveler le bail. Ce mécanisme de bail permet de s'assurer que les clients qui sont déplacés ou qui sont mis hors tension ne conservent pas des adresses dont ils n'ont plus besoin.
- Lorsque le client démarre (ou souhaite rejoindre un réseau), il entame un processus en quatre étapes pour obtenir un bail : DHCPDISCOVER, puis DHCPOFFER, puis DHCPREQUEST, et enfin DHCPACK. Avant l'expiration du bail, le client entame un processus en deux étapes pour renouveler le bail avec le serveur DHCPv4: DHCPREQUEST puis DHCPACK.
- Le logiciel Cisco IOS du routeur Cisco peut être configuré en tant que serveur DHCPv4.
- Pour configurer un serveur Cisco IOS DHCPv4, procédez comme suit : excluez les adresses IPv4, définissez un nom de pool DHCPv4 et configurez le pool DHCPv4.
- Vérifiez votre configuration à l'aide des commandes **show running-config | section dhcp**, **show ip dhcp binding** et **show ip dhcp server statistics**.
- Le service DHCPv4 est activé par défaut. Pour désactiver le service, utilisez la commande **no service dhcp** du mode de configuration globale.

# Qu'est-ce que j'ai appris dans ce module? (Suite)

- Les clients réseau ne sont généralement pas sur le même sous-réseau que les serveurs d'entreprise fournissant des services DHCP, DNS, TFTP et FTP pour le réseau. Afin de localiser les serveurs et de bénéficier des services, les clients utilisent souvent des messages de diffusion. Le routeur doit être configuré pour relayer les messages DHCPv4 au serveur DHCPv4.
- L'administrateur réseau peut configurer le routeur avec la commande de configuration de l'interface **ip helper-address address** et utiliser la commande **show ip interface** pour vérifier la configuration.
- Par défaut, la commande ip helper-address transfère les huit services UDP suivants :
  - Port 37: Time
  - Port 49: TACACS
  - Port 53: DNS
  - Port 67: DHCP/BOOTP server
  - Port 68: DHCP/BOOTP client
  - Port 69: TFTP
  - Port 137: NetBIOS name service
  - Port 138: NetBIOS datagram service
- Pour configurer une interface Ethernet en tant que client DHCP, utilisez la commande de mode de configuration de l'interface **ip address dhcp**
- Les routeurs domestiques sont généralement déjà configurés pour recevoir automatiquement les informations d'adressage IPv4 d'ISP. Vérifiez que le type de connexion Internet est défini sur Configuration automatique - DHCP. Cette sélection est utilisée lorsque le routeur est connecté à un DSL ou à un modem câble et agit en tant que client DHCPv4, demandant une adresse IPv4 auprès de l'ISP.



# Module 10: Concepts ACL



# Objectifs de ce module

**Titre du module:** Concepts ACL

**Objectif du module:** Expliquer comment les listes de contrôle d'accès sont utilisées dans le cadre d'une politique de sécurité réseau.

Titre du rubrique	Objectif du rubrique
<b>Objectif des listes de contrôle d'accès</b>	Expliquer comment les listes de contrôle d'accès filtrent le trafic
<b>Masques génériques dans les listes de contrôle d'accès</b>	Expliquer comment les listes de contrôle d'accès utilisent des masques génériques.
<b>Création de listes de contrôle d'accès</b>	Expliquer comment créer des listes de contrôle d'accès.
<b>Types de listes de contrôle d'accès IPv4</b>	Comparer les listes de contrôle d'accès IPv4 standard et étendues.

# 10.1 Objectif des listes de contrôle d'accès (ACL)

# Qu'est-ce qu'une liste de contrôle d'accès?

Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. Par défaut, aucun ACL n'est configuré pour un routeur. Toutefois, lorsqu'une liste de contrôle d'accès est appliquée à une interface, le routeur évalue en outre tous les paquets réseau lorsqu'ils traversent l'interface pour déterminer s'ils peuvent être acheminés.

- Une ACL utilise une liste séquentielle de déclarations d'autorisation ou de refus, connues sous le nom d'entrées de contrôle d'accès (ACE).

**Remarque:** Les ACE sont couramment appelées des instructions de liste de contrôle d'accès.

- Lorsque le trafic réseau traverse une interface configurée avec une liste de contrôle d'accès, le routeur compare les informations du paquet à chaque ACE, dans l'ordre séquentiel, afin de déterminer si le paquet correspond à l'une des entrées ACE. C'est ce que l'on appelle le filtrage de paquet.

## Qu'est-ce qu'une liste de contrôle d'accès? (Suite)

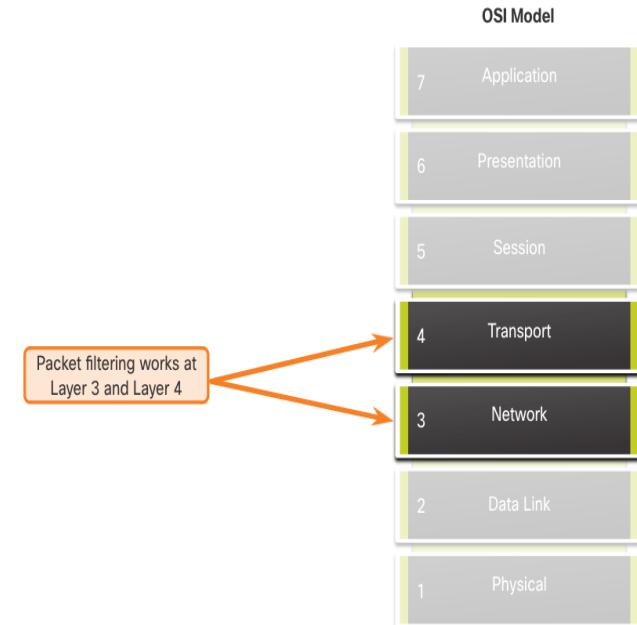
Plusieurs tâches effectuées par les routeurs nécessitent l'utilisation d'ACL pour identifier le trafic:

- Limiter le trafic du réseau pour en augmenter les performances
- Elles contrôlent le flux de trafic.
- Elles fournissent un niveau de sécurité de base pour l'accès réseau.
- Elles filtrent le trafic en fonction de son type.
- Contrôler les hôtes pour autoriser ou refuser l'accès aux services de réseau
- Donner la priorité à certaines classes de trafic réseau

# Objectif des listes de contrôle d'accès

## Filtrage des paquets

- Le filtrage de paquets contrôle l'accès à un réseau en analysant les paquets entrants et/ou sortants et en les transmettant ou en les abandonnant en fonction de critères donnés.
- Le filtrage des paquets peut être effectué au niveau de la couche 3 ou de la couche 4.
- Les routeurs Cisco prennent en charge deux types de ACLs:
  - ACL standard** - Les ACL filtrent uniquement au niveau de la couche 3 à l'aide de l'adresse IPv4 source uniquement.
  - ACL étendues** - Filtre ACL à la couche 3 à l'aide de l'adresse IPv4 source et/ou destination. Ils peuvent également filtrer au niveau de la couche 4 en utilisant les ports TCP et UDP, ainsi que des informations facultatives sur le type de protocole pour un contrôle plus fin.



## Le fonctionnement des listes de contrôle d'accès

- Les listes de contrôle d'accès définissent des règles de contrôle pour les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie.
- Les listes de contrôle d'accès peuvent être configurées pour s'appliquer au trafic entrant et au trafic sortant:

**Remarque:** Les ACL ne gèrent pas les paquets provenant du routeur lui-même.

- Un ACL entrant filtre les paquets avant qu'ils ne soient acheminés vers l'interface sortante. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet.
- Les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.



## Le fonctionnement des listes de contrôle d'accès (Suite)

Lorsqu'une ACL est appliquée à une interface, elle suit une procédure d'exploitation spécifique. Voici les étapes opérationnelles utilisées lorsque le trafic est entré dans une interface de routeur avec une ACL IPv4 standard entrante configurée:

1. Le routeur extrait l'adresse IPv4 source de l'en-tête du paquet.
2. Le routeur commence en haut de l'ACL et compare l'adresse IPv4 source à chaque ACE dans un ordre séquentiel.
3. Lorsqu'une correspondance est établie, le routeur exécute l'instruction, soit en autorisant soit en refusant le paquet, et les ACE restants dans l'ACL, le cas échéant, ne sont pas analysés.
4. Si l'adresse IPv4 source ne correspond à aucun ACE de l'ACL, le paquet est ignoré car un ACE de refus implicite est automatiquement appliqué à toutes les ACLs.

La dernière instruction d'une liste de contrôle d'accès est toujours une instruction deny implicite bloquant tout le trafic. Il est caché et non affiché dans la configuration.

**Remarque:** Une liste ACL doit avoir au moins une déclaration d'autorisation sinon tout le trafic sera refusé en raison de l'instruction ACE de refus implicite.

## Packet Tracer - Démonstration des listes de contrôle d'accès

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Partie 1: Vérifier la connectivité locale et tester la liste de contrôle d'accès
- Partie 2: supprimer la liste de contrôle d'accès et répéter le test
- **LAB10.1-ACL**

# 10.2 - Masques génériques dans les listes de contrôle d'accès

## Masques génériques dans les listes de contrôle d'accès

# Présentation de masques génériques

Un masque générique est similaire à un masque de sous-réseau en ce sens qu'il utilise le processus AND pour identifier les bits d'une adresse IPv4 à correspondre. En effet, contrairement à un masque de sous-réseau, où le chiffre binaire 1 équivaut à une correspondance et le chiffre binaire 0 à une non-correspondance, les masques génériques procèdent de façon inverse.

- Un ACE IPv4 utilise un masque générique 32 bits pour déterminer quels bits de l'adresse à examiner pour rechercher une correspondance.
- Les masques génériques respectent les règles suivantes pour faire correspondre les chiffres binaires 1 et 0:
  - **Bit 0 de masque générique** - permet de vérifier la valeur du bit correspondant dans l'adresse.
  - **Masque générique bit 1** - Ignorer la valeur du bit correspondant dans l'adresse

# Présentation de masques génériques (Suite)

Masque générique	Dernier octet (en binaire)	Signification (0 - match, 1 - ignorer)
0.0.0.0	00000000	Correspond à tous les octets.
0.0.0.63	00111111	<ul style="list-style-type: none"> <li>Faites correspondre les trois premiers octets</li> <li>Correspond aux deux bits les plus à gauche du dernier octet</li> <li>Les 6 derniers bits d'adresse sont ignorés</li> </ul>
0.0.0.15	00001111	<ul style="list-style-type: none"> <li>Faites correspondre les trois premiers octets</li> <li>Correspond aux quatre bits les plus à gauche du dernier octet</li> <li>Ignorer les 4 derniers bits du dernier octet</li> </ul>
0.0.0.248	11111100	<ul style="list-style-type: none"> <li>Faites correspondre les trois premiers octets</li> <li>Ignorer les six bits les plus à gauche du dernier octet</li> <li>Faites correspondre les deux derniers bits</li> </ul>
0.0.0.255	11111111	<ul style="list-style-type: none"> <li>Faites correspondre les trois premiers octet</li> <li>Ignorer le dernier octet</li> </ul>

# Types de masques génériques

## Caractère générique pour correspondre à un hôte:

- Supposons que l'ACL 10 ait besoin d'un ACE qui autorise uniquement l'hôte avec l'adresse IPv4 192.168.1.1. Rappelez-vous que "0" équivaut à une correspondance et "1" à une ignorance. Pour correspondre à une adresse IPv4 d'hôte spécifique, un masque générique composé de tous les zéros (c.-à-d. 0.0.0.0) est requis.
- Lorsque l'ACE est traité, le masque générique n'autorisera que l'adresse 192.168.1.1. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.1.1 0.0.0.0**.

	Décimal	Binaire
Adresse IPv4	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.0	00000000.00000000.00000000.00000000
Adresse IPv4 autorisée	192.168.1.1	11000000.10101000.00000001.00000001

# Types de masques génériques (Suite)

## Masques génériques correspondant à des sous-réseaux IPv4

- ACL 10 a besoin d'un ACE qui autorise tous les hôtes du réseau 192.168.1.0/24. Le masque générique 0.0.0.255 stipule que les trois premiers octets doivent correspondre exactement, mais pas le quatrième octet.
- Lorsqu'il est traité, le masque générique 0.0.0.255 autorise tous les hôtes du réseau 192.168.1.0/24. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.1.0 0.0.0.255**.

	Décimal	Binaire
Adresse IPv4	192.168.1.1	11000000.10101000.00000001.00000001
Masque générique	0.0.0.255	00000000.00000000.00000000.11111111
Adresse IPv4 autorisée	192.168.1.0/24	11000000.10101000.00000001.00000000

# Masques génériques dans les listes de contrôle d'accès

## Types de masques génériques (Suite)

### Masque générique pour correspondre à une plage d'adresses IPv4

- ACL 10 a besoin d'un ACE qui autorise tous les hôtes des réseaux 192.168.16.0/24, 192.168.17.0/24,..., 192.168.31.0/24.
- Lorsqu'il est traité, le masque générique 0.0.15.255 autorise tous les hôtes des réseaux 192.168.16.0/24 à 192.168.31.0/24. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.16.0 0.0.15.255**.

	Décimal	Binaire
Adresse IPv4	192.168.16.0	11000000.10101000.00010000.00000000
Masque générique	0.0.15.255	00000000.00000000.00001111.11111111
Adresse IPv4 autorisée	192.168.16.0/24 à 192.168.31.0/24	11000000.10101000.00010000.00000000 11000000.10101000.00011111.00000000

# Masques génériques dans les listes de contrôle d'accès

## Calcul de masque générique

Le calcul des masques génériques peut être complexe. La méthode la plus rapide consiste à soustraire le masque de sous-réseau de 255.255.255.255. Voici quelques exemples:

- Supposons que vous vouliez un ACE en ACL 10 pour permettre l'accès à tous les utilisateurs du réseau 192.168.3.0/24. Pour calculer le masque générique, soustrayez le masque de sous-réseau (c'est-à-dire 255.255.255.0) de 255.255.255.255. Cela génère le masque générique 0.0.0.255. L'ACE serait **access-list 10 permit 192.168.1.0 0.0.0.255**.
- Supposons que vous vouliez un ACE en ACL 10 pour permettre l'accès au réseau aux 14 utilisateurs du sous-réseau 192.168.3.32/28. Soustraire le sous-réseau (c'est-à-dire 255.255.255.240) de 255.255.255.255. Cela génère le masque générique 0.0.0.15. L'ACE serait **access-list 10 permit 192.168.3.32 0.0.0.15**
- Supposons que vous ayez besoin d'un ACE dans ACL 10 pour autoriser uniquement les réseaux 192.168.10.0 et 192.168.11.0. Ces deux réseaux pourraient être résumés comme 192.168.10.0/23 qui est un masque de sous-réseau de 255.255.254.0. Soustrayez 255.255.254.0 masque de sous-réseau de 255.255.255.255. Cela génère le masque générique 0.0.1.255.  
L'ACE serait **access-list 10 permit 192.168.10.0 0.0.1.255**.

## Les mots-clés des masques génériques

L'IOS de Cisco fournit deux mots clés pour identifier les utilisations les plus courantes du masquage générique. Les deux mots-clés sont:

- **host** - Ce mot-clé remplace le masque 0.0.0.0 Ce masque indique que tous les bits d'adresse IPv4 doivent correspondre pour pouvoir filtrer juste une adresse d'hôte.
- **any** - Ce mot clé remplace le masque 255.255.255.255 Ce masque indique qu'il convient d'ignorer l'intégralité de l'adresse IPv4 ou d'accepter n'importe quelle adresse.

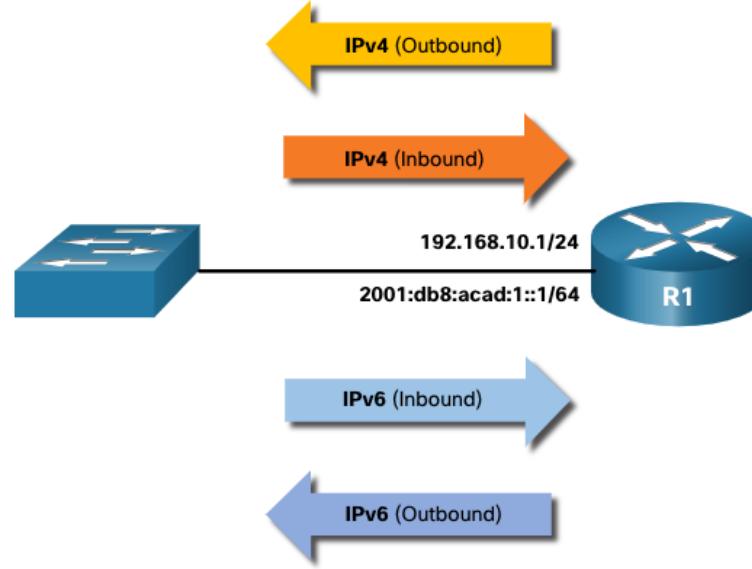
# 10.3 Directives pour la création de LCA

# Nombre limité d'ACL par interface

Le nombre de listes ACL pouvant être appliquées sur une interface de routeur est limité. Par exemple, une interface de routeur double empilée (c'est-à-dire IPv4 et IPv6) peut avoir jusqu'à quatre ACL appliquées, comme indiqué sur la figure.

Plus précisément, une interface de routeur peut avoir:

- Une liste ACL sortante IPv4.
- Une ACL IPv4 entrante.
- Une ACL IPv6 entrante.
- Une liste ACL IPv6 sortante.



**Remarque:** il n'est pas nécessaire de configurer les listes de contrôle d'accès dans les deux directions. Le nombre d'ACL et leur direction appliquée à l'interface dépendront de la stratégie de sécurité de l'organisation.

# Meilleure pratique relatives aux listes de contrôle d'accès

L'utilisation des listes de contrôle d'accès nécessite beaucoup de précision et de soin. Les erreurs peuvent vous coûter cher et se solder par des pannes de réseau, d'importants efforts de dépannage et des services réseau médiocres. Une planification de base est nécessaire avant de configurer une ACL.

Directive	Avantage
Créez vos listes de contrôle d'accès conformément à la stratégie de sécurité de votre entreprise.	Vous serez ainsi certain d'implémenter les instructions relatives à la sécurité organisationnelle.
Écrivez ce que vous voulez que l'ACL fasse.	Vous éviterez ainsi de créer d'éventuels problèmes d'accès par mégarde.
Utilisez un éditeur de texte pour créer, modifier et enregistrer les listes de contrôle d'accès.	Vous pourrez ainsi créer une bibliothèque de listes de contrôle d'accès réutilisables.
Documentez les ACL à l'aide de la commande <b>remark</b> .	Cela vous aidera (et d'autres) à comprendre le but d'un ACE.
Testez vos listes de contrôle d'accès sur un réseau de développement avant de les implémenter sur un réseau de production.	Vous éviterez ainsi de commettre des erreurs coûteuses.

# 10.4 Types d'ACL IPv4

# Listes de contrôle d'accès standard et étendues

Types de listes de contrôle d'accès IPv4

- **ACL standard** - Ces listes autorisent ou refusent les paquets basés uniquement sur l'adresse IPv4 source.
- **ACL étendues** - Ces listes autorisent ou refusent les paquets basés sur l'adresse IPv4 source et l'adresse IPv4 de destination, le type de protocole, les ports TCP ou UDP source et destination et plus encore.

# Listes de contrôle d'accès numérotées et nommées

## Listes de contrôle d'accès numérotées

- Les ACL numérotées 1-99 ou 1300-1999 sont des ACL standard, tandis que les ACL numérotées 100-199 ou 2000-2699 sont des ACL étendues.

```
R1(config)# access-list ?  
<1-99> IP standard access list  
<100-199> IP extended access list  
<700-799> 48-bit MAC address access list  
<1300-1999> IP standard access list (expanded range)  
<200-299> Protocol type-code access list  
<2000-2699> IP extended access list (expanded range)  
<700-799> 48-bit MAC address access list  
rate-limit Simple rate-limit specific access list  
template Enable IP template acls  
Router(config)# access-list
```

# Listes de contrôle d'accès numérotées et nommées (Suite)

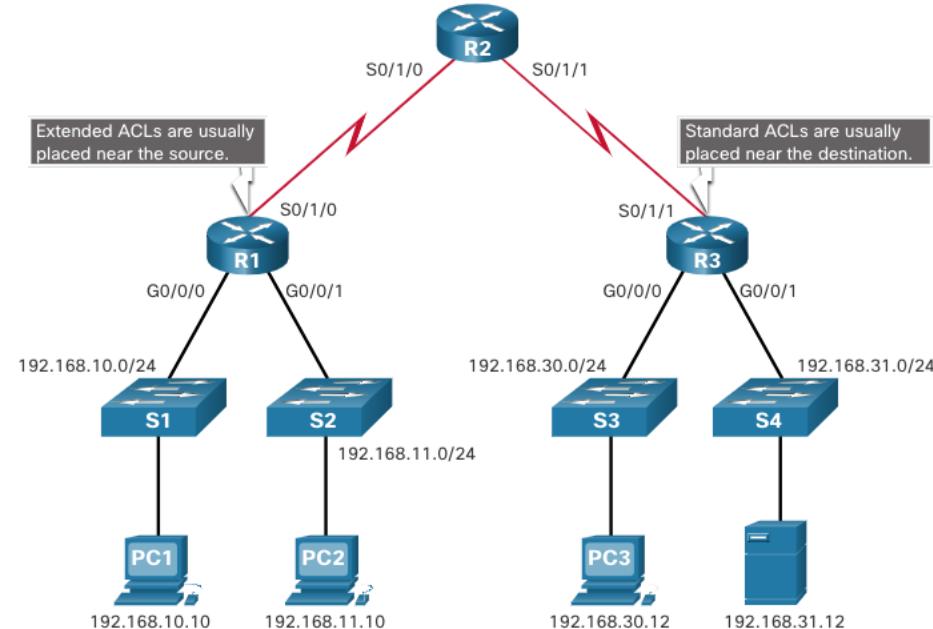
## Listes de contrôle d'accès nommées

- Les ACL nommées sont la méthode préférée à utiliser lors de la configuration des ACL. Plus précisément, les listes ACL standard et étendues peuvent être nommées pour fournir des informations sur l'objet de la liste ACL. Par exemple, nommer un ACL FTP-FILTER étendu est beaucoup mieux que d'avoir une ACL numérotée 100.
- La commande de configuration globale **ip access-list** est utilisée pour créer une liste ACL nommée, comme illustré dans l'exemple suivant.

```
R1 (config) # ip access-list extended FTP-FILTER
R1 (config-ext-nacl) # permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1 (config-ext-nacl) # permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1 (config-ext-nacl) #
```

# Où placer les listes de contrôle d'accès

- Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances.
- Les listes de contrôle d'accès étendues doivent être placées le plus près possible de la source du trafic à filtrer.
- Les listes de contrôle d'accès standard doivent être placées le plus près possible de la destination.



# Où placer les listes de contrôle d'accès (Suite)

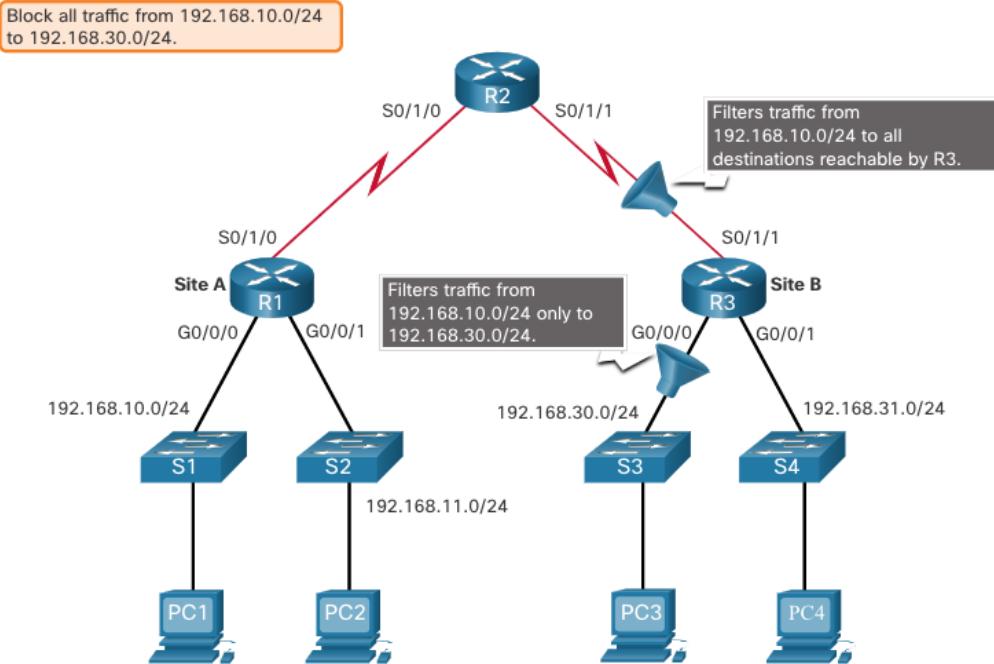
Facteurs influençant le placement des ACL	Explication
<b>L'étendue du contrôle organisationnel</b>	Le placement de l'ACL peut dépendre du fait que l'organisation contrôle ou non les réseaux source et destination.
<b>Bandé passante des réseaux concernés</b>	Il peut être souhaitable de filtrer le trafic indésirable à la source pour empêcher la transmission de trafic qui consomme de la bande passante.
<b>Simplicité de configuration</b>	<ul style="list-style-type: none"> <li>• Il peut être plus facile d'implémenter une liste ACL à destination, mais le trafic utilisera inutilement la bande passante.</li> <li>• Une liste de contrôle d'accès étendue peut être utilisée sur chaque routeur d'où provient le trafic. Cela permet d'économiser de la bande passante en filtrant le trafic à la source, mais exige de créer des listes de contrôle d'accès étendues sur plusieurs routeurs.</li> </ul>

## Types de listes de contrôle d'accès IPv4

### Exemple d'emplacement de liste de contrôle d'accès standard

Sur la figure, l'administrateur souhaite empêcher le trafic provenant du réseau 192.168.10.0/24 d'accéder au réseau 192.168.30.0/24.

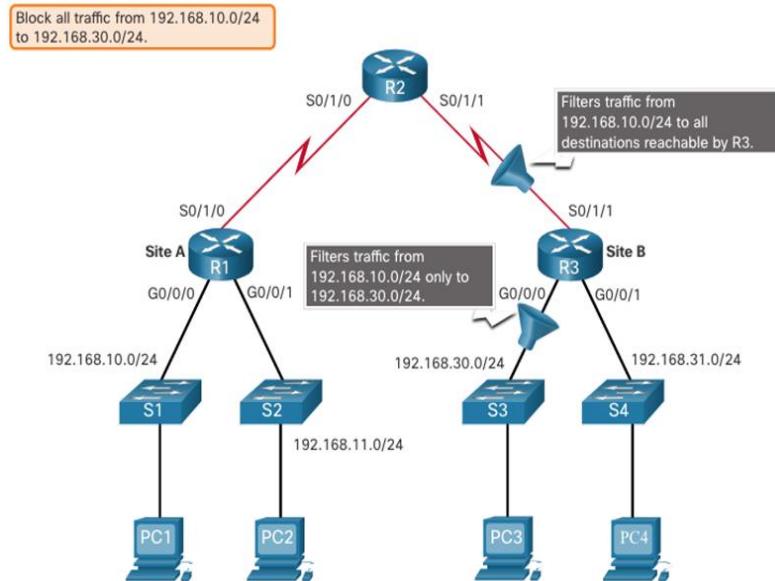
En suivant les instructions de placement de base, l'administrateur place une liste ACL standard sur le routeur R3.



## Exemple d'emplacement de liste de contrôle d'accès standard (Suite)

Il existe deux interfaces possibles sur R3 pour appliquer l'ACL standard:

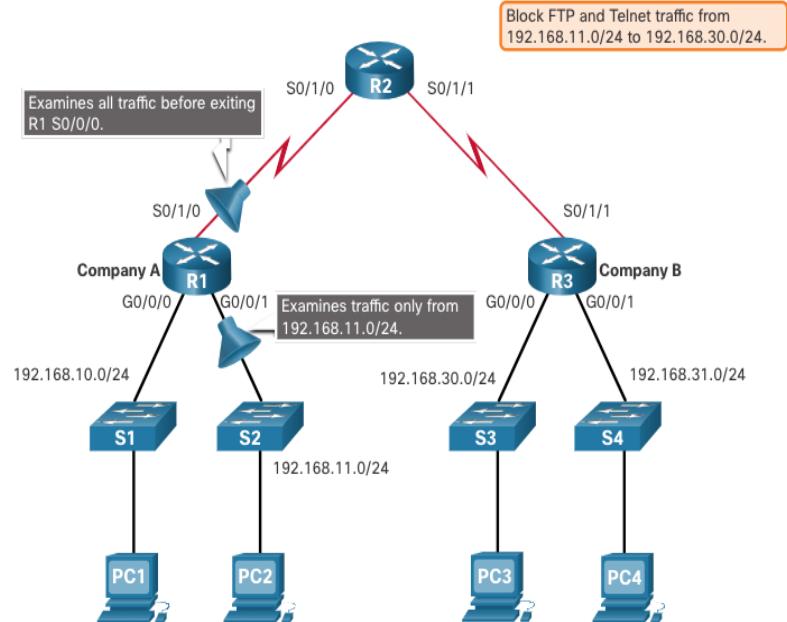
- Interface R3 S0/1/1 (entrante)** - L'ACL standard peut être appliquée entrante sur l'interface R3 S0/1/1 pour refuser le trafic à partir du réseau .10. Cependant, il filtre également le trafic .10 vers le réseau 192.168.31.0/24 (.31 dans cet exemple). Par conséquent, l'ACL standard ne doit pas être appliquée à cette interface.
- Interface R3 G0/0 (sortante)** - L'ACL standard peut être appliquée sortante sur l'interface R3 G0/0/0. Cela n'affecte pas les autres réseaux accessibles par R3. Les paquets du réseau .10 pourront toujours atteindre le réseau .31. C'est la meilleure interface pour placer la liste ACL standard pour répondre aux exigences de trafic.



## Types de listes de contrôle d'accès IPv4

### Exemple d'emplacement d'une liste de contrôle d'accès étendue

- Les ACL étendus doivent être situés aussi près que possible de la source.
- Cependant, l'organisation ne peut placer des ACL que sur les appareils qu'elle contrôle. Par conséquent, cet emplacement doit être déterminé par la portée du contrôle dont dispose l'administrateur réseau.
- Dans la figure, par exemple, la société A veut refuser le trafic Telnet et FTP au réseau 192.168.30.0/24 de la société B à partir de son réseau 192.168.11.0/24 tout en autorisant tout autre trafic.



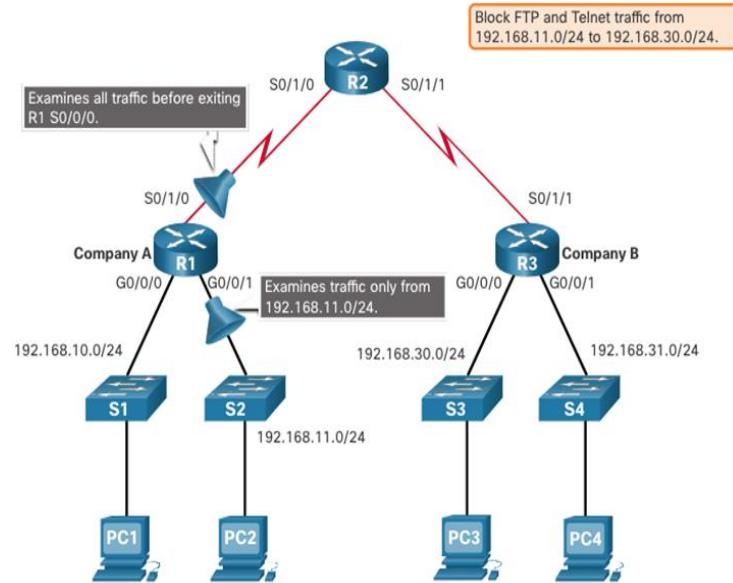
## Exemple d'emplacement d'une liste de contrôle d'accès étendue (Suite)

Un ACL étendu sur R3 permettrait d'accomplir la tâche, mais l'administrateur ne contrôle pas R3. En outre, cette solution autorise le passage du trafic indésirable sur l'ensemble du réseau avant de le bloquer lorsqu'il arrive à destination.

La solution consiste à placer une liste ACL étendue sur R1 qui spécifie à la fois les adresses source et de destination.

La figure illustre deux interfaces possibles sur R1 pour appliquer la liste de contrôle d'accès étendue:

- interface R1 S0/1/0 (sortante)** - L'ACL étendue peut être appliquée sortante sur l'interface S0/1/0. Cette solution traitera tous les paquets quittant R1 y compris les paquets de 192.168.10.0/24.
- Interface R1 G0/0/1 (entrante)** - L'ACL étendu peut être appliqué en entrée sur le G0/0/1 et seuls les paquets du réseau 192.168.11.0/24 sont soumis au traitement ACL sur R1. Puisque le filtre doit être limité aux seuls paquets quittant le réseau 192.168.11.0/24, l'application de la liste de contrôle d'accès étendue à G0/1 constitue la meilleure solution.



# 10.5 Module pratique et questionnaire

# Qu'est-ce que j'ai appris dans ce module?

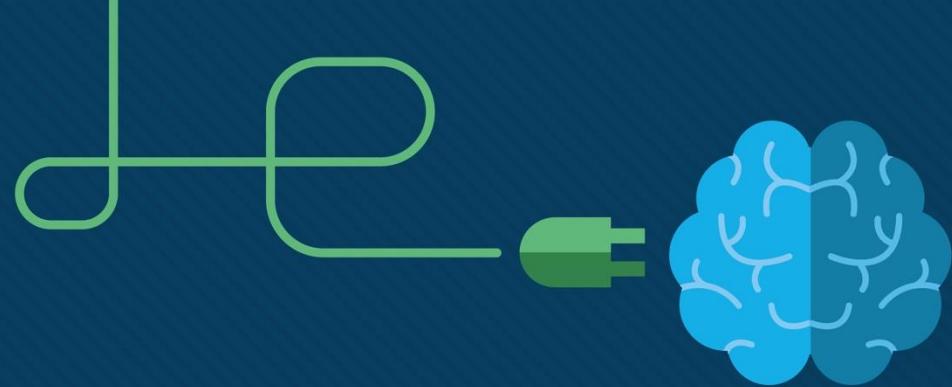
- Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet.
- Un routeur n'a pas d'ACL configuré par défaut.
- Toutefois, lorsqu'une liste de contrôle d'accès est appliquée à une interface, le routeur évalue en outre tous les paquets réseau lorsqu'ils traversent l'interface pour déterminer s'ils peuvent être acheminés.
- Une ACL utilise une liste séquentielle de déclarations d'autorisation ou de refus, connues sous le nom d'ACE.
- Les routeurs Cisco prennent en charge deux types d'ACL: ACL standard et ACL étendues.
- Un ACL entrant filtre les paquets avant qu'ils ne soient acheminés vers l'interface sortante. Si le paquet est autorisé par la liste de contrôle d'accès, il est alors traité pour le routage.
- Les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.
- Un ACE IPv4 utilise un masque générique 32 bits pour déterminer quels bits de l'adresse à examiner pour rechercher une correspondance.
- Un masque générique est similaire à un masque de sous-réseau en ce sens qu'il utilise le processus ANDing pour identifier les bits d'une adresse IPv4 à correspondre. Cependant, ils diffèrent dans la façon dont ils correspondent aux binaires 1 et 0. Masque générique bit 0 correspond à la valeur du bit correspondant dans l'adresse. Masque générique bit 1 ignore la valeur du bit correspondant dans l'adresse.

# Qu'est-ce que j'ai appris dans ce module? (Suite)

- Une autre manière de calculer un masque générique est de soustraire le masque de sous-réseau de 255.255.255.255.
- Travailler avec des représentations décimales de bits de masque générique binaire peut être simplifié en utilisant les mots-clés Cisco IOS **host** et **any** pour identifier les utilisations les plus courantes du masquage génériques.
- Le nombre de listes ACL pouvant être appliquées sur une interface de routeur est limité.
- Il n'est pas nécessaire de configurer les ACL dans les deux sens. Le nombre d'ACL et leur direction appliquée à l'interface dépendront de la stratégie de sécurité de l'organisation.
- Les ACL standard autorisent ou refusent les paquets selon l'adresse IPv4 source uniquement.
- Les ACLs étendues autorisent ou refusent les paquets en fonction de l'adresse IPv4 source et de l'adresse IPv4 de destination, du type de protocole, des ports TCP ou UDP source et destination et plus encore.
- Les ACL numérotées 1-99 ou 1300-1999 sont des ACL standard. Les ACL numérotées 100-199, ou 2000-2699, sont des ACL étendues.
- Les ACLs nommées sont la méthode préférée à utiliser lors de la configuration des ACL.
- Plus précisément, les listes ACL standard et étendues peuvent être nommées pour fournir des informations sur l'objet de la liste ACL.
- Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances.

## Qu'est-ce que j'ai appris dans ce module? (Suite)

- Les listes de contrôle d'accès étendues doivent être placées le plus près possible de la source du trafic à filtrer. De cette manière, le trafic indésirable est refusé près du réseau source et ne traverse pas l'infrastructure de réseau.
- Les listes de contrôle d'accès standard doivent être placées le plus près possible de la destination. Si une liste de contrôle d'accès standard a été placée à la source du trafic, l'instruction «permit» ou «deny» est appliquée en fonction de l'adresse source, quelle que soit la destination du trafic.
- Le placement de l'ACL peut dépendre de l'étendue du contrôle organisationnel, de la bande passante des réseaux et de la facilité de configuration.



# Module 11: Configuration de liste de contrôle d'accès pour IPv4



# Objectifs de ce module

## Module 5: Configuration de liste de contrôle d'accès pour IPv4

**Objectif du module:** Mettre en œuvre des listes de contrôle IPv4 pour filtrer le trafic et sécuriser l'accès des administrateurs.

Titre du rubrique	Objectif du rubrique
<b>Configurer les listes de contrôle d'accès IPv4 standard</b>	Configurer les listes de contrôle d'accès IPv4 standard pour filtrer le trafic afin de répondre aux besoins du réseau.
<b>Modifier les listes de contrôle d'accès IPv4</b>	Utiliser les numéros de séquence pour modifier des listes de contrôle d'accès IPv4 standard.
<b>Sécuriser les ports VTY à l'aide d'une liste de contrôle d'accès IPv4 standard</b>	Configurer une liste de contrôle d'accès standard pour sécuriser l'accès VTY
<b>Configurer les listes de contrôle d'accès IPv4 étendues</b>	Configurer les listes de contrôle d'accès IPv4 étendues pour filtrer le trafic en fonction des besoins du réseau.

# 11.1 Configurer les listes de contrôle d'accès IPv4 standard

# Créer une ACL

Toutes les listes de contrôle d'accès (ACL) doivent être planifiées. Lors de la configuration d'une ACL complexe, il est suggéré de:

- Utiliser un éditeur de texte et écrire les spécificités de la stratégie à mettre en œuvre.
- Ajouter les commandes de configuration IOS pour accomplir ces tâches.
- Inclure des remarques pour documenter l'ACL.
- Copier et coller les commandes sur le périphérique.
- Tester toujours soigneusement une liste ACL pour vous assurer qu'elle applique correctement la stratégie souhaitée.

# Syntaxe des listes de contrôle d'accès IPv4 standard numérotées

Pour créer une liste ACL standard numérotée, utilisez la commande **access-list** .

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard]  
[log]
```

Paramètre	Description
<i>access-list-number</i>	La plage de nombres est de 1 à 99 ou de 1300 à 1999
<b>deny</b>	Refuse l'accès si les conditions sont respectées.
<b>permit</b>	Autorise l'accès si les conditions sont respectées.
<b>remark <i>text</i></b>	(Facultatif) Ajoute une entrée de texte à des fins de documentation.
<b>Source</b>	Identifie l'adresse du réseau source ou de l'hôte à filtrer.
<b>source-wildcard</b>	(facultatif) Un masque générique de 32 bits qui est appliqué à la source
<b>log</b>	(Facultatif) Génère et envoie un message d'information lorsque l'ACE est apparié

Remarque : Utilisez la commande de configuration globale **no access-list *access-list-number*** pour supprimer une ACL standard numérotée.

# Syntaxe des listes de contrôle d'accès IPv4 standard nommées

Pour créer une liste ACL standard numérotée, utilisez la commande **ip access-list standard**.

- Les noms des listes de contrôle d'accès doivent contenir uniquement des caractères alphanumériques, sont sensibles à la casse et doivent être uniques.
- Vous n'êtes pas obligés de mettre des majuscules aux noms des listes de contrôle d'accès. En revanche, si vous le faites, vous les verrez bien mieux en affichant la sortie de la commande running-config.

```
Router(config)# ip access-list standard access-list-name
```

```
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# ?
Standard Access List configuration commands:
<1-2147483647> Sequence Number
default      Set a command to its defaults
deny         Specify packets to reject
exit         Exit from access-list configuration mode
no           Negate a command or set its defaults
permit        Specify packets to forward
remark       Access list entry comment
R1(config-std-nacl)#

```

## Appliquer une listes de contrôle d'accès IPv4 standard numérotées

Une fois qu'une ACL IPv4 standard est configurée, elle doit être liée à une interface ou à une fonctionnalité.

- La commande **ip access-group** est utilisée pour lier une ACL IPv4 standard numérotée ou nommée à une interface.
- Pour supprimer une ACL d'une interface, entrez d'abord la commande de configuration de l'interface **no ip access-group**

```
Router(config-if) # ip access-group {access-list-number | access-list-name} {in | out}
```

# Exemple de liste de contrôle d'accès standard numérotées

L'exemple ACL autorise le trafic à partir de l'hôte 192.168.10.10 et de tous les hôtes sur l'interface de sortie réseau 192.168.20.0/24 série 0/1/0 sur le routeur R1.

```
R1(config)# access-list 10 remark ACE permits ONLY host 192.168.10.10 to the internet
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
R1(config)#
R1(config)# access-list 10 remark ACE permits all host in LAN 2
R1(config)# access-list 10 permit 192.168.20.0 0.0.0.255
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1(config)#
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group 10 out
R1(config-if)# end
R1#
```

## Exemple de liste de contrôle d'accès standard numérotées (Suite)

- Utilisez la commande **show running-config** pour consulter la configuration.
- Utilisez la commande **show ip interface** pour vérifier que l'ACL est appliquée à la bonne interface.

```
R1# show run | section access-list
access-list 10 remark ACE permits host 192.168.10.10
access-list 10 permit 192.168.10.10
access-list 10 remark ACE permits all host in LAN 2
access-list 10 permit 192.168.20.0 0.0.0.255
R1#
```

```
R1# show ip int Serial 0/1/0 | include access list
Outgoing Common access list is not set
Outgoing access list is 10
Inbound Common access list is not set
Inbound access list is not set
R1#
```

# Exemple de liste de contrôle d'accès standard nommées

L'exemple ACL autorise le trafic à partir de l'hôte 192.168.10.10 et de tous les hôtes sur l'interface de sortie réseau 192.168.20.0/24 série 0/1/0 sur le routeur R1.

```
R1(config)# no access-list 10
R1(config)# ip access-list standard PERMIT-ACCESS
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)#
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)# remark ACE permits all hosts in LAN 2
R1(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)#
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group PERMIT-ACCESS out
R1(config-if)# end
R1#
```

# Exemple de liste de contrôle d'accès standard nommées (Suite)

- Utilisez la commande **show access-list** pour consulter la configuration.
- Utilisez la commande **show ip interface** pour vérifier que l'ACL est appliquée à la bonne interface.

```
R1# show access-lists
Standard IP access list PERMIT-ACCESS
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1# show run | section ip access-list
ip access-list standard PERMIT-ACCESS
    remark ACE permits host 192.168.10.10
    permit 192.168.10.10
    remark ACE permits all hosts in LAN 2
    permit 192.168.20.0 0.0.0.255
R1#
R1# show ip int Serial 0/1/0 | include access list
    Outgoing Common access list is not set
    Outgoing access list is PERMIT-ACCESS
    Inbound Common access list is not set
    Inbound access list is not set
R1#
```

# Packet Tracer - Configurer les listes ACL IPv4 standard numérotées

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Planifier la mise en œuvre d'une liste de contrôle d'accès
- Configurer, appliquer et vérifier une liste de contrôle d'accès standard
- **LAB11.1-ACL**

# Packet Tracer - Configurer les listes ACL IPv4 standard nommées

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Configurer, appliquer et vérifier une liste de contrôle d'accès standard
- Vérifier l'implémentation de la liste de contrôle d'accès.
- **LAB11.2-ACL**

# 11.2 Modifier les listes de contrôle d'accès IPv4

# Deux méthodes pour modifier une ACL

Une fois qu'une liste ACL est configurée, il peut être nécessaire de la modifier. Les ACL avec plusieurs ACE peuvent être complexes à configurer. Parfois, l'ACE configuré ne donne pas les comportements attendus.

Il existe deux méthodes à utiliser pour modifier une liste ACL:

- Utiliser un éditeur de texte
- Utiliser les numéros de séquence

# Méthode éditeur de texte

Les ACL avec plusieurs ACE doivent être créées dans un éditeur de texte. Cela vous permet de planifier les ACE nécessaires, de créer l'ACL, puis de la coller sur l'interface du routeur. Il simplifie également les tâches de modification et de correction d'une ACL.

Pour corriger une erreur dans une liste ACL:

- Copiez l'ACL à partir de la configuration en cours d'exécution et collez-la dans l'éditeur de texte.
- Effectuez les modifications nécessaires.
- Supprimez la liste ACL configurée précédemment sur le routeur.
- Copiez et collez la liste ACL modifiée sur le routeur.

```
R1# show run | section access-list
access-list 1 deny 19.168.10.10
access-list 1 permit 192.168.10.0 0.0.0.255
R1#
```

```
R1(config)# no access-list 1
R1(config)#
R1(config)# access-list 1 deny 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#
R1#
```

# Méthode numéros de séquence

Un ACE ACL peut être supprimé ou ajouté à l'aide des numéros de séquence ACL.

- Utilisez la commande **ip access-list standard** pour modifier une ACL.
- Les instructions ne peuvent pas être remplacées par des instructions associées à un numéro de séquence existant déjà. L'instruction actuelle doit être supprimée d'abord avec la commande **no 10**. Ensuite, le bon ACE peut être ajouté en utilisant le numéro de séquence.

```
R1# show access-lists
Standard IP access list 1
  10 deny  19.168.10.10
  20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list 1
  10 deny  192.168.10.10
  20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

# Modifier une ACL nommée Exemple

Les ACL nommées peuvent également utiliser des numéros de séquence pour supprimer et ajouter des ACE. Dans l'exemple, un ACE est ajouté pour refuser les hôtes 192.168.10.11.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny    192.168.10.10
    20 permit   192.168.10.0, wildcard bits 0.0.0.255

R1# configure terminal
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# 15 deny 192.168.10.5
R1(config-std-nacl)# end
R1#
R1# show access-lists
Standard IP access list NO-ACCESS
    15 deny    192.168.10.5
    10 deny    192.168.10.10
    20 permit   192.168.10.0, wildcard bits 0.0.0.255

R1#
```

# Statistiques des listes de contrôle d'accès

La commande **show access-lists** de l'exemple affiche des statistiques pour chaque instruction qui a été mise en correspondance.

- L'ACE de refus a été apparié 20 fois et le permis ACE a été apparié 64 fois.
- Notez que le refus implicite d'une instruction n'affiche aucune statistique. Pour suivre le nombre de paquets refusés implicitement appariés, vous devez configurer manuellement la commande **deny any**.
- Utilisez la commande **clear access-list counters** pour effacer les statistiques ACL.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny  192.168.10.10  (20 matches)
    20 permit 192.168.10.0, wildcard bits 0.0.0.255  (64 matches)
R1# clear access-list counters NO-ACCESS
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny  192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

# Packet Tracer - Configurer et modifier les listes ACL IPv4 standard

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Configurer les périphériques et vérifier la connectivité
- Configurer et vérifier les listes de contrôle d'accès numérotées et nommées standard
- Modifier une liste de contrôle d'accès standard
- **LAB11.3-ACL**

# 11.3 Sécuriser les ports VTY à l'aide d'une liste de contrôle d'accès IPv4 standard

# Sécuriser les ports VTY à l'aide d'une liste de contrôle d'accès IPv4 standard La commande access-class

Une liste ACL standard peut sécuriser l'accès administratif à distance à un périphérique à l'aide des lignes vty en implémentant les deux étapes suivantes:

- Créez une liste ACL pour identifier les hôtes administratifs qui doivent être autorisés à accéder à distance.
- Appliquez l'ACL au trafic entrant sur les lignes vty.

```
R1(config-line)# access-class {access-list-number | access-list-name} { in | out }
```

# Exemple d'accès sécurisé aux VTY

Cet exemple montre comment configurer une liste ACL pour filtrer le trafic vty.

- Tout d'abord, une entrée de base de données locale pour une utilisateur **ADMIN** et mot de passe **class** est configurée.
- Les lignes vty sur R1 sont configurées pour utiliser la base de données locale pour l'authentification, autoriser le trafic SSH et utiliser l'ACL ADMIN-HOST pour restreindre le trafic.

```
R1(config)# username ADMIN secret class
R1(config)# ip access-list standard ADMIN-HOST
R1(config-std-nacl)# remark This ACL secures incoming vty lines
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

# Vérifier la sécurité du port VTY

Une fois que la liste de contrôle d'accès aux lignes VTY est configurée, il est important de vérifier qu'elle fonctionne correctement.

Pour vérifier les statistiques ACL, exécutez la commande **show access-lists** .

- La correspondance dans la ligne d'autorisation de la sortie est le résultat d'une connexion SSH réussie par l'hôte avec l'adresse IP 192.168.10.10.
- La correspondance à l'instruction «deny» est due à l'échec de la tentative de créer une connexion SSH à partir d'un appareil sur un autre réseau.

```
R1#  
Oct  9 15:11:19.544: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 192.168.10.10]  
[localport: 23] at 15:11:19 UTC Wed Oct 9 2019  
R1# show access-lists  
Standard IP access list ADMIN-HOST  
    10 permit 192.168.10.10  (2 matches)  
    20 deny   any   (2 matches)  
R1#
```

# 11.4 Configurer les listes de contrôle d'accès IPv4 étendues

# Les ACL étendues

Les ACL étendues offrent un plus grand degré de contrôle. Ils peuvent filtrer sur l'adresse source, l'adresse de destination, le protocole (c'est-à-dire IP, TCP, UDP, ICMP) et le numéro de port.

Les ACL étendues peuvent être créées comme suit:

- **ACL étendu numérotée** - Crée à l'aide de la commande de configuration globale `access-list access-list-number`.
- **ACL étendu nommée** - Crée à l'aide de la commande `ip access-list extended access-list-name`.

# Protocoles et ports

## Options de protocole

Les ACL étendues peuvent filtrer sur protocoles et ports d'internet. Utiliser le ? pour obtenir de l'aide lors de la saisie d'un ACE complexe . Les quatre protocoles mis en évidence sont les options les plus populaires.

```
R1(config)# access-list 100 permit ?
<0-255>      An IP protocol number
ahp           Authentication Header Protocol
dvmrp          dvmrp
eigrp          Cisco's EIGRP routing protocol
esp            Encapsulation Security Payload
gre             Cisco's GRE tunneling
icmp           Internet Control Message Protocol
igmp           Internet Gateway Message Protocol
ip              Any Internet Protocol
ipinip          IP in IP tunneling
nos             KA9Q NOS compatible IP over IP tunneling
object-group   Service object group
ospf            OSPF routing protocol
pcp             Payload Compression Protocol
pim             Protocol Independent Multicast
tcp             Transmission Control Protocol
udp             User Datagram Protocol
R1(config)# access-list 100 permit
```

# Protocoles et ports (Suite)

La sélection d'un protocole influence les options de port. De nombreuses options de port TCP sont disponibles, comme indiqué dans la sortie.

```
R1(config)# access-list 100 permit tcp any any eq ?
<0-65535>  Port number
bgp          Border Gateway Protocol (179)
chargen      Character generator (19)
cmd          Remote commands (rcmd, 514)
daytime      Daytime (13)
discard      Discard (9)
domain       Domain Name Service (53)
echo          Echo (7)
exec          Exec (rsh, 512)
finger        Finger (79)
ftp           File Transfer Protocol (21)
ftp-data     FTP data connections (20)
gopher        Gopher (70)
hostname      NIC hostname server (101)
ident         Ident Protocol (113)
irc           Internet Relay Chat (194)
klogin        Kerberos login (543)
kshell        Kerberos shell (544)
login         Login (rlogin, 513)
lpd           Printer service (515)
msrpc         MS Remote Procedure Call (135)
nntp          Network News Transport Protocol (119)
onep-plain    OneP Cleartext (15001)
onep-tls      OneP TLS (15002)
pim-auto-rp   PIM Auto-RP (496)
pop2          Post Office Protocol v2 (109)
pop3          Post Office Protocol v3 (110)
smtp          Simple Mail Transport Protocol (25)
sunrpc        Sun Remote Procedure Call (111)
syslog        Syslog (514)
tacacs        TAC Access Control System (49)
talk          Talk (517)
telnet        Telnet (23)
time          Time (37)
uucp          Unix-to-Unix Copy Program (540)
whois         Nicname (43)
www           World Wide Web (HTTP, 80)
```

# Exemples de configuration de protocoles et de numéros de ports (Suite)

Les ACL étendues peuvent filtrer sur différentes options de numéro de port et de nom de port.

Cet exemple montre comment configurer une ACL 100 étendue pour filtrer le trafic HTTP. Le premier ACE utilise le nom de port **www**. Le deuxième ACE utilise le numéro de port **80**. Les deux ACE obtiennent exactement le même résultat.

```
R1(config)# access-list 100 permit tcp any any eq www  
!or...  
R1(config)# access-list 100 permit tcp any any eq 80
```

La configuration du numéro de port est requise lorsqu'aucun nom de protocole spécifique n'est répertorié tel que SSH (numéro de port 22) ou HTTPS (numéro de port 443), comme indiqué dans l'exemple suivant.

```
R1(config)# access-list 100 permit tcp any any eq 22  
R1(config)# access-list 100 permit tcp any any eq 443  
R1(config)#
```

# Appliquer une ACL IPv4 étendue numérotée

Dans cet exemple, l'ACL permet à la fois le trafic HTTP et HTTPS à partir du réseau 192.168.10.0 d'accéder à n'importe quelle destination.

Les ACL étendues peuvent être appliquées à différents endroits. Cependant, elles sont couramment appliquées près de la source. Ici ACL 110 est appliquée en entrant sur l'interface R1 G0/0/0.

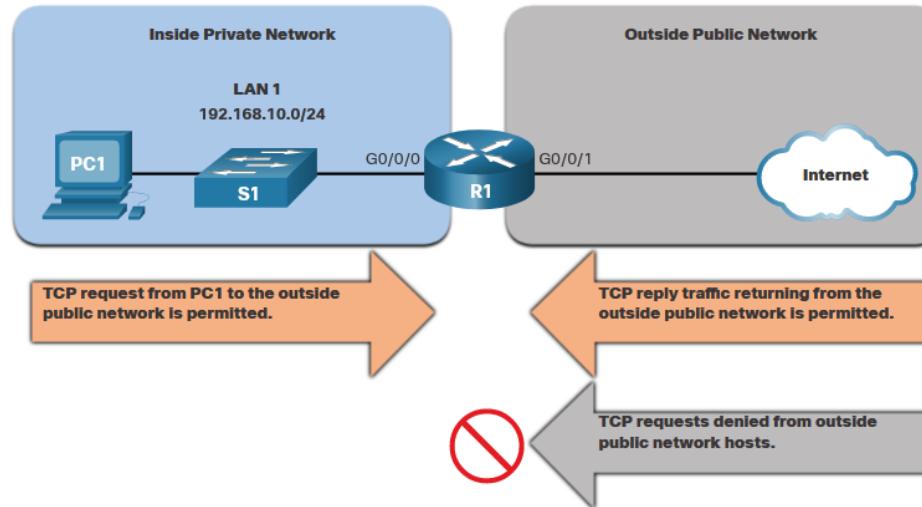
```
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 110 in
R1(config-if)# exit
R1(config)#
```

## Configurer les listes de contrôle d'accès IPv4 étendues

### ACL étendue établie par TCP

TCP peut également effectuer des services de pare-feu avec état de base à l'aide du mot-clé TCP **established**.

- Le mot-clé **established** permet au trafic intérieur de quitter le réseau privé intérieur et permet au trafic de réponse de retourner d'entrer dans le réseau privé intérieur.
- Le trafic TCP généré par un hôte externe et la tentative de communication avec un hôte interne est refusé.



# ACL étendue établie par TCP (Suite)

- ACL 120 est configurée pour autoriser uniquement le retour du trafic Web vers les hôtes internes. L'ACL est ensuite appliquée sortante sur l'interface R1 G0/0/0.
- La commande **show access-lists** indique que les hôtes internes accèdent aux ressources Web sécurisées à partir d'Internet.

**Remarque:** Il y a concordance si les bits ACK ou RST (réinitialisation) du segment TCP de retour sont définis, indiquant que le paquet appartient à une connexion existante.

```
R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 120 out
R1(config-if)# end
R1# show access-lists
Extended IP access list 110
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)
Extended IP access list 120
    10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)
R1#
```

# Syntaxe ACL étendue IPv4 nommée

Si vous attribuez un nom à une liste de contrôle d'accès, il vous sera plus facile d'en comprendre la fonction. Pour créer une liste ACL étendue nommée, utilisez la commande de configuration **ip access-list extended**.

Dans l'exemple, une liste ACL étendue nommée NO-FTP-ACCESS est créée et l'invite est modifiée en mode de configuration ACL étendue nommée. Les instructions ACE sont entrées dans le mode de sous-configuration ACL étendu nommé.

```
Router(config)# ip access-list extended access-list-name
```

```
R1(config)# ip access-list extended NO-FTP-ACCESS  
R1(config-ext-nacl)#

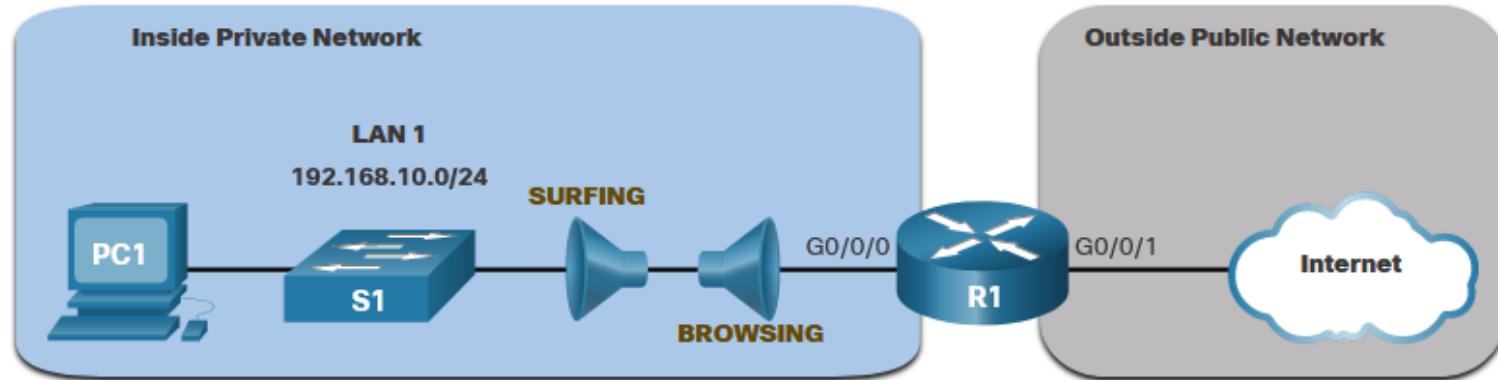
```

## Configurer les listes de contrôle d'accès IPv4 étendues

### Exemple d'ACL étendue IPv4 nommée

La topologie ci-dessous permet de démontrer la configuration et l'application de deux ACL étendues IPv4 nommées à une interface:

- SURFING - Cela permettra à l'intérieur du trafic HTTP et HTTPS de quitter l'internet.
- **BROWSING** - Cela permettra uniquement de renvoyer le trafic Web aux hôtes internes alors que tout autre trafic sortant de l'interface R1 G0/0/0 est implicitement refusé.



# Exemple de liste ACL étendue IPv4 nommée (Suite)

- L'ACL SURFING permet au trafic HTTP et HTTPS des utilisateurs internes de quitter l'interface G0/0/1 connectée à l'internet. Le trafic Web revenant de l'internet est autorisé à revenir sur le réseau privé interne par l'ACL BROWSING.
- La liste ACL SURVING est appliquée entrante et la liste ACL BROWSING est appliquée sortante sur l'interface R1 G0/0/0.

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# Remark Permits inside HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# Remark Only permit returning HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
R1(config-if)# end
R1# show access-lists
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)
R1#
```

## Configurer les listes de contrôle d'accès IPv4 étendues

# Exemple de liste ACL étendue IPv4 nommée (Suite)

**Pour vérifier les statistiques ACL, exéutez la commande `show access-lists` . Notez que les compteurs HTTPS sécurisés par permis (c.-à-d., eq 443) dans l'ACL SURFING et les compteurs de retour établis dans l'ACL BROWSING ont augmenté.**

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

# Modifier les ACL étendues

Une liste ACL étendue peut être modifiée à l'aide d'un éditeur de texte lorsque de nombreuses modifications sont nécessaires. Ou, si l'édition s'applique à un ou deux ACE, les numéros de séquence peuvent être utilisés.

### Exemple:

- Le numéro de séquence ACE 10 dans l'ACL SURFING a une adresse de réseau IP source incorrecte.

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

# Modifier les ACL étendues (Suite)

- Pour corriger cette erreur, l'instruction d'origine est supprimée avec la commande **no sequence\_#** et l'instruction corrigée est ajoutée en remplacement de l'instruction d'origine.
- La sortie de la commande **show access-lists** vérifie le changement de configuration.

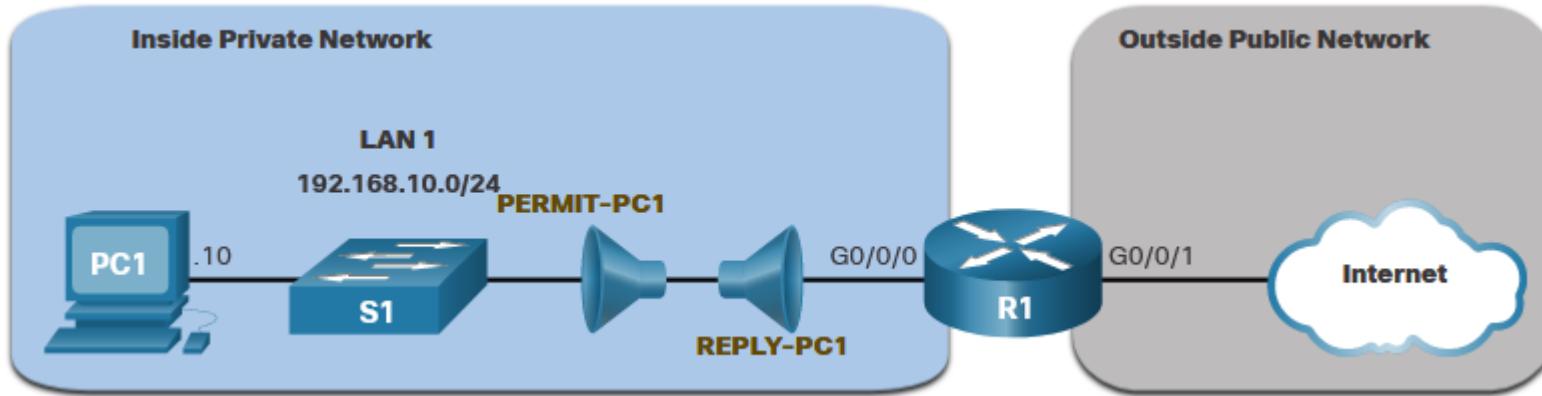
```
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config-ext-nacl)# end
```

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

# Autre exemple d'ACL étendue IPv4 nommée

Deux ACL étendues nommées seront créées:

- **PERMIT-PC1** - Cela permettra uniquement l'accès PC1 TCP à l'internet et refusera tous les autres hôtes du réseau privé.
- **REPLY-PC1** - Cela permettra uniquement le retour du trafic TCP spécifié à PC1 refuser implicitement tout autre trafic.



# Autre exemple d'ACL étendue IPv4 nommée (Suite)

- L'ACL **PERMIT-PC1** autorise PC1 (192.168.10.10) l'accès TCP au trafic FTP, SSH, Telnet, DNS, HTTP et HTTPS.
- La liste ACL **REPLY-PC1** permettra le retour du trafic vers PC1.
- La liste ACL **PERMIT-PC1** est appliquée en entrée et la liste ACL **REPLY-PC1** est appliquée en sortie sur l'interface R1 G0/0/0.

```
R1(config)# ip access-list extended PERMIT-PC1
R1(config-ext-nacl)# Remark Permit PC1 TCP access to internet
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 20
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 21
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 22
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 23
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 53
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 80
R1(config-ext-nacl)# permit tcp host 192.168.10.10 any eq 443
R1(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 any
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended REPLY-PC1
R1(config-ext-nacl)# Remark Only permit returning traffic to PC1
R1(config-ext-nacl)# permit tcp any host 192.168.10.10 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group PERMIT-PC1 in
R1(config-if)# ip access-group REPLY-PC1 out
R1(config-if)# end
R1#
```

# Vérifier les listes de contrôle d'accès étendues

La commande **show ip interface** permet de vérifier la liste de contrôle d'accès sur l'interface et la direction dans laquelle elle a été appliquée.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is REPLY-PC1
  Inbound access list is PERMIT-PC1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled

R1#
R1# show ip interface g0/0/0 | include access list
  Outgoing access list is REPLY-PC1
  Inbound access list is PERMIT-PC1

R1#
```

# Vérifier les listes de contrôle d'accès étendues (Suite)

La commande **show access-lists** peut être utilisée pour confirmer que les ACL fonctionnent comme prévu. La commande affiche les compteurs statistiques qui augmentent chaque fois qu'un ACE est apparié.

**Remarque :** Le trafic doit être généré pour vérifier le fonctionnement de l'ACL.

```
R1# show access-lists
Extended IP access list PERMIT-PC1
 10 permit tcp host 192.168.10.10 any eq 20
 20 permit tcp host 192.168.10.10 any eq ftp
 30 permit tcp host 192.168.10.10 any eq 22
 40 permit tcp host 192.168.10.10 any eq telnet
 50 permit tcp host 192.168.10.10 any eq domain
 60 permit tcp host 192.168.10.10 any eq www
 70 permit tcp host 192.168.10.10 any eq 443
 80 deny ip 192.168.10.0 0.0.0.255 any
Extended IP access list REPLY-PC1
 10 permit tcp any host 192.168.10.10 established
R1#
```

# Vérifier les listes de contrôle d'accès étendues (Suite)

La commande **show running-config** peut être utilisée pour valider ce qui a été configuré.  
La commande affiche également les remarques configurées.

```
R1# show running-config | begin ip access-list
ip access-list extended PERMIT-PC1
remark Permit PC1 TCP access to internet
permit tcp host 192.168.10.10 any eq 20
permit tcp host 192.168.10.10 any eq ftp
permit tcp host 192.168.10.10 any eq 22
permit tcp host 192.168.10.10 any eq telnet
permit tcp host 192.168.10.10 any eq domain
permit tcp host 192.168.10.10 any eq www
permit tcp host 192.168.10.10 any eq 443
deny ip 192.168.10.0 0.0.0.255 any
ip access-list extended REPLY-PC1
remark Only permit returning traffic to PC1
permit tcp any host 192.168.10.10 established
!
```

# Packet Tracer - Configurer les listes de contrôle d'accès IPv4 étendues - Scénario 1

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Configurer, appliquer et vérifier une liste de contrôle d'accès IPv4 étendue numérotée.
- Configurer, appliquer et vérifier une liste de contrôle d'accès IPv4 étendue nommée.
- LAB11.4-ACL

Configurer les listes de contrôle d'accès IPv4 étendues

# Packet Tracer - Configurer les listes de contrôle d'accès IPv4 étendues - Scénario 2

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Configurer une liste de contrôle d'accès ACL IPv4 étendue nommée
- Appliquer et vérifier la liste de contrôle d'accès IPv4 étendue
- **LAB11.5-ACL**

# Packet Tracer - Mise en œuvre de l'ACL IPv4

Dans ce Packet Tracer, vous atteindrez les objectifs suivants:

- Configurer un routeur avec des listes ACL nommées standard.
- Configurer un routeur avec des ACL nommées étendues.
- Configurer un routeur avec des ACL étendues pour répondre à des exigences de communication spécifiques.
- Configurer une liste ACL pour contrôler l'accès aux lignes de terminal de périphérique réseau.
- Configurer les interfaces de routeur appropriées avec les ACL dans la direction appropriée.
- Vérifiez le fonctionnement des ACL configurées.
- **LAB11.6-ACL**

# 11.5 Module pratique et questionnaire

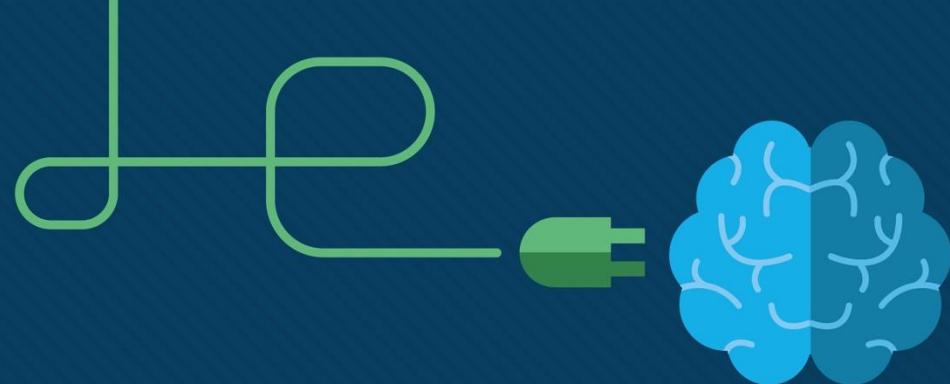
# Qu'est-ce que j'ai appris dans ce module?

- Pour créer une liste ACL standard numérotée, utilisez la commande de configuration globale **ip access-list standard access-list-name** .
- Utilisez la commande de configuration globale **no access-list access-list-number** pour supprimer une ACL standard numérotée.
- Utilisez la commande **show ip interface** pour vérifier si une ACL est appliquée à une interface.
- Pour créer une liste ACL standard nommée, utilisez la commande de configuration globale **ip access-list standard access-list-name** .
- Utilisez la commande de configuration globale **no ip access-list standard access-list-name** pour supprimer une ACL IPv4 standard nommée.
- Pour lier une ACL IPv4 standard numérotée ou nommée à une interface, utilisez la commande de configuration globale **ip access-group {access-list-number | access-list-name} { in | out }** .
- Pour supprimer une ACL d'une interface, entrez d'abord la commande de configuration de l'interface **no ip access-group**
- Pour supprimer l'ACL du routeur, utilisez la commande de configuration globale **no access-list**



# Qu'est-ce que j'ai appris dans ce module?

- Les listes de contrôle d'accès étendues peuvent filtrer sur l'adresse source, l'adresse de destination, le protocole (c'est-à-dire IP, TCP, UDP, ICMP) et le numéro de port.
- Pour créer une liste ACL étendue numérotée, utilisez la commande de configuration globale  
`Router(config)# access-list access-list-number {deny | permit | remark text} protocol source source-wildcard [operator [port]] destination destination-wildcard [operator [port]] [established] [log]`.
- Les ACL peuvent également effectuer des services de pare-feu avec état de base à l'aide du mot-clé TCP **established** .
- La commande **show ip interface** permet de vérifier la liste de contrôle d'accès sur l'interface et la direction dans laquelle elle a été appliquée.
- Pour modifier une ACL, utilisez un éditeur de texte ou utilisez des numéros de séquence.
- Un ACE ACL peut également être supprimé ou ajouté à l'aide des numéros d'ordre ACL.
- Les numéros d'ordre sont automatiquement affectés lorsqu'un ACE est entré.



# Module 12: Concepts WLAN



# Objectifs de ce module

**Titre du module:** Concepts WLAN

**Objectif du module:** expliquer comment les réseaux locaux sans fil permettent la connectivité réseau..

Titre du Rubrique	Objectif du rubrique
Introduction au sans-fil	Décrire la technologie et les normes WLAN.
Composants d'un réseau WLAN	Décrire les composants d'une infrastructure WLAN.
Fonctionnement d'un réseau WLAN	Expliquer comment la technologie sans fil permet le fonctionnement du réseau WLAN.
Fonctionnement du protocole CAPWAP	Expliquer comment un contrôleur sans fil utilise CAPWAP pour gérer plusieurs points d'accès.
Gestion des canaux	Décrire la gestion des canaux dans un réseau WLAN.
Menaces visant le réseau WLAN	Décrire les menaces visant les réseaux WLAN.
WLAN sécurisés	Décrire les mécanismes de sécurité WLAN.

# 12.1 Présentation de la technologie sans fil

## Présentation de la technologie sans fil

# Avantages du sans fil

- Un réseau local sans fil (WLAN) est un type de réseau sans fil couramment utilisé dans les maisons, les bureaux et les campus.
- Les WLAN rendent la mobilité possible dans les environnements domestiques et professionnels.
- Les infrastructures sans fil s'adaptent aux besoins et aux technologies en évolution rapide.



## Types de réseaux sans fil

- **Réseau personnel sans fil (WPAN)** - Faible consommation et courte portée (20-30 pieds ou 6-9 mètres). Basé sur la norme IEEE 802.15 et la fréquence 2,4 GHz. Bluetooth et Zigbee sont des exemples WPAN.
- **LAN sans fil (WLAN)** - Réseaux de taille moyenne jusqu'à environ 300 pieds. Basé sur la norme IEEE 802.11 et la fréquence 2,4 ou 5,0 GHz.
- **MAN sans fil (WMAN)** - Grande zone géographique telle que ville ou quartier. Utilise des fréquences sous licence spécifiques.
- **WAN sans fil (WWAN)** - Zone géographique étendue pour les communications nationales ou mondiales. Utilise des fréquences sous licence spécifiques.

# Technologies sans fil

**Bluetooth** - Norme IEEE WPAN utilisée pour l'appariement d'appareils jusqu'à une distance de 100 mètres.

- Bluetooth Low Energy (BLE) - Prend en charge la topologie maillée pour les périphériques réseau à grande échelle.
- Débit de base Bluetooth / Débit amélioré (BR / EDR) - Prend en charge les topologies point à point et est optimisé pour le streaming audio.

**WiMAX (Worldwide Interoperability for Microwave Access)** - Connexions Internet filaires à large bande alternatives. Norme WLAN IEEE 802.16 jusqu'à 30 miles (50 km).



## Technologies sans fil (suite)

**Cellulaire large bande** - Transportez à la fois la voix et les données. Utilisé par les téléphones, les automobiles, les tablettes et les ordinateurs portables.

- Global System of Mobile (GSM) - Reconnu internationalement
- CDMA (Code Division Multiple Access) - Utilisé principalement aux États-Unis.

**Satellite large bande** - Utilise une antenne parabolique directionnelle alignée sur un satellite en orbite géostationnaire. Besoin d'une ligne de site claire. Généralement utilisé dans les zones rurales où le câble et la DSL ne sont pas disponibles.



## Normes du 802.11

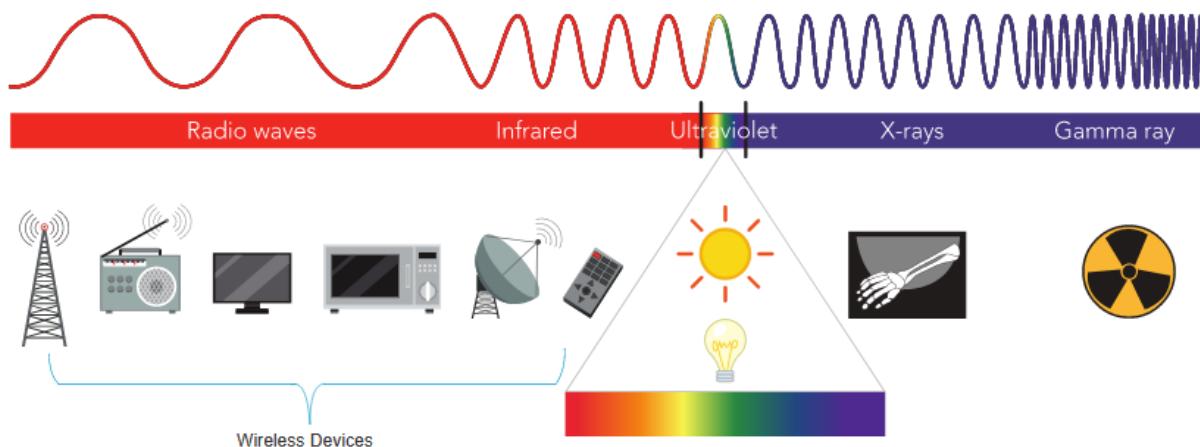
Les normes 802.11 WLAN définissent comment les fréquences radio sont utilisées pour les liaisons sans fil.

Norme IEEE	Radiofréquence	Description
802.11	2,4 GHz	Débits de données jusqu'à 2 Mb / s
802.11a	5 GHz	Débits de données jusqu'à 54 Mb / s Non interopérable avec 802.11b ou 802.11g
802.11b	2,4 GHz	Débits de données jusqu'à 11 Mb / s Portée plus longue que 802.11a et mieux à pénétrer les structures des bâtiments
802.11g	2,4 GHz	Débits de données jusqu'à 54 Mb / s Rétrocompatible avec 802.11b
802.11n	2,4 et 5 GHz	Débits de données 150 - 600 Mb / s Nécessite plusieurs antennes avec la technologie MIMO
802.11ac	5 GHz	Débits de données 450 Mb/s – 1.3 Gb/s Prend en charge jusqu'à huit antennes
802.11ax	2,4 et 5 GHz	Sans fil haute efficacité (High-Efficiency Wireless) (HEW) Capable d'utiliser des fréquences de 1 GHz et 7 GHz

## Fréquences Radio

Tous les appareils sans fil fonctionnent dans la portée du spectre électromagnétique. Les réseaux WLAN fonctionnent dans la bande de fréquences 2,4 GHz et la bande 5 GHz.

- 2,4 GHz (UHF) - 802.11b/g/n/ax
- 5 GHz (SHF) - 802.11a/n/ac/ax



## Organismes de normalisation sans fil

Les normes garantissent l'interopérabilité entre les appareils fabriqués par différents fabricants. Au niveau international, les trois organisations qui influencent les normes WLAN:

- **Union internationale des télécommunications (UIT)** - Régule l'attribution du spectre radioélectrique et des orbites de satellites.
- **Institut des ingénieurs électriciens et électroniciens (IEEE)** - Spécifie comment une fréquence radio est modulée pour transporter des informations. Il maintient les normes pour les réseaux locaux et métropolitains (MAN) avec la famille de normes IEEE 802 LAN / MAN.
- **Alliance Wi-Fi** - Favorise la croissance et l'acceptation des WLAN. Il s'agit d'une association de fournisseurs dont l'objectif est d'améliorer l'interopérabilité des produits basés sur la norme 802.11 en certifiant la conformité des fournisseurs aux normes de l'industrie et le respect des normes.

# 12.2 Composants WLAN

### NIC sans fil

Pour communiquer sans fil, les ordinateurs portables, les tablettes, les téléphones intelligents et même les dernières voitures incluent des cartes réseau sans fil intégrées qui incorporent un émetteur / récepteur radio.

Cependant, si un périphérique ne possède pas de carte réseau sans fil intégrée(NIC), un adaptateur sans fil USB peut être utilisé, comme illustré dans la figure.



# Routeur domestique sans fil

un utilisateur à domicile interconnecte généralement des périphériques sans fil à l'aide d'un petit routeur sans fil, comme illustré dans la figure.

Les routeurs sans fil sont les suivants:

- **Points d'accès** – Pour fournir un accès aux câbles
- **Commutateur** – Pour interconnecter des appareils câblés
- **Routeur** - Pour fournir une passerelle par défaut vers d'autres réseaux et Internet



## Composants WLAN

### Point d'accès sans fil

Les clients sans fil utilisent leur carte réseau sans fil pour découvrir les points d'accès (AP) à proximité.

Les clients tentent ensuite de s'associer et de s'authentifier avec un AP.

Une fois authentifiés, les utilisateurs sans fil ont accès aux ressources réseau.

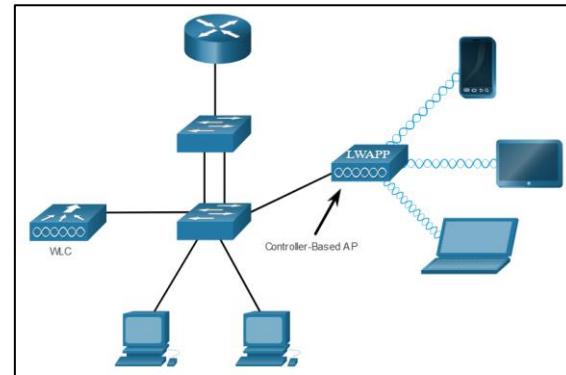
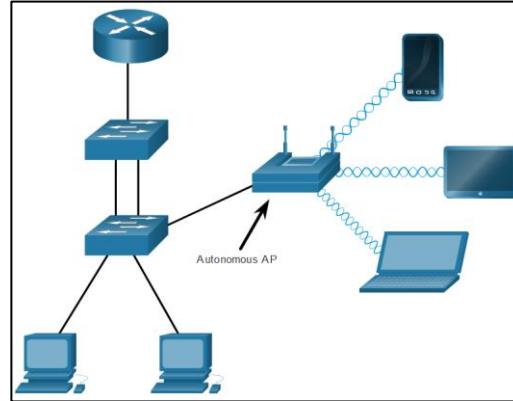


Points d'accès Cisco Meraki Go

## Catégories AP

Les points d'accès peuvent être classés comme des points d'accès autonomes ou des points d'accès basés sur un contrôleur.

- **AP autonomes** - Périphériques autonomes configurés via une interface de ligne de commande ou une interface graphique. Chaque AP autonome agit indépendamment des autres et est configuré et géré manuellement par un administrateur.
- **AP basés sur contrôleur** - Également appelés AP légers (LAP). Utilisez le protocole de point d'accès léger (LWAPP) pour communiquer avec un contrôleur LWAN (WLC). Chaque LAP est automatiquement configuré et géré par le WLC.



# Antennes sans fil

Types d'antennes externes:

- **Omnidirectionnel** - Fournit une couverture à 360 degrés. Idéal dans les maisons et les bureaux.
- **Directionnel** - Concentrez le signal radio dans une direction spécifique. Les exemples sont le Yagi et le plat parabolique.
- **Entrées multiples Sorties multiples (MIMO)** - Utilise plusieurs antennes (jusqu'à huit) pour augmenter la bande passante.



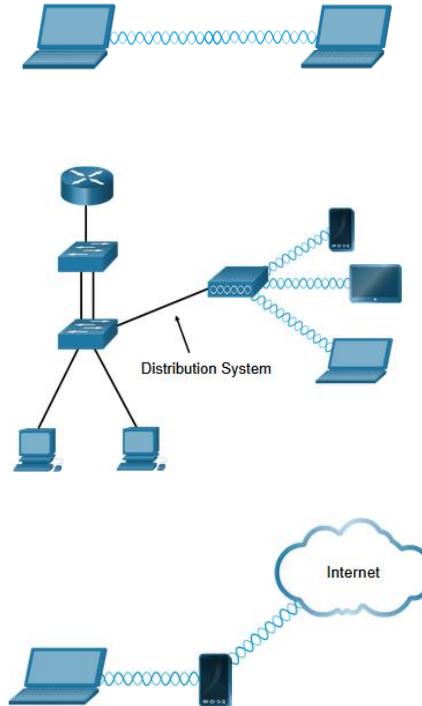
# 12.3 Fonctionnement d'un réseau WLAN

# Modes de topologie sans fil 802.11

**Mode ad hoc** - Utilisé pour connecter les clients de manière poste à poste sans point d'accès.

**Mode infrastructure** - Utilisé pour connecter les clients au réseau à l'aide d'un AP.

**Partage de connexion** - La variation de la topologie ad hoc se produit lorsqu'un téléphone intelligent ou une tablette avec accès aux données cellulaires est activé pour créer un point d'accès personnel.



## BSS et ESS

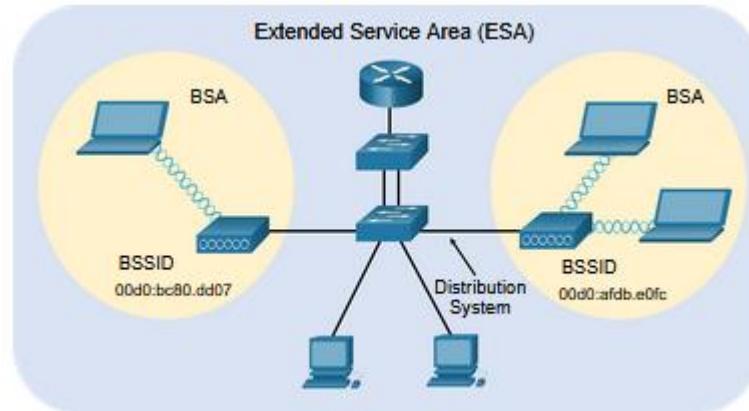
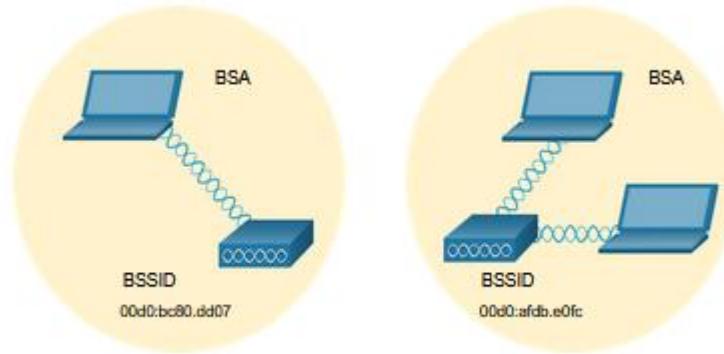
Le mode infrastructure définit deux blocs de topologie:

### Ensemble de services de base (BSS)

- Un BSS consiste en un seul AP interconnectant tous les clients sans fil associés.
- Les clients de différents BSS ne peuvent pas communiquer.

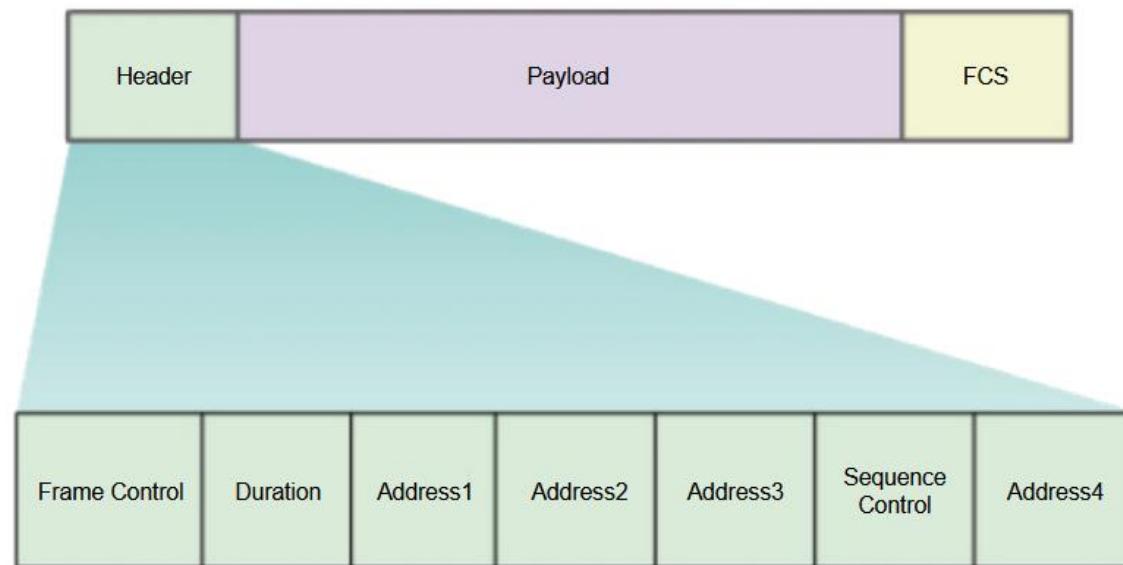
### Ensemble de service étendu (ESS)

- Union de deux ou plusieurs BSS interconnectés par un système de distribution câblé.
- Les clients de chaque BSS peuvent communiquer via l'ESS.



# Structure de trame 802.11

Le format de trame 802.11 est similaire au format de trame Ethernet, sauf qu'il contient plus de champs.



## Fonctionnement du WLAN

### CSMA/CA

Les WLAN sont semi-duplex et un client ne peut pas "entendre" pendant qu'il envoie, ce qui rend impossible de détecter une collision.

Les WLAN utilisent l'accès multiple par détection de porteuse avec évitement de collision (CSMA/CA) pour déterminer comment et quand envoyer des données. Un client sans fil effectue les opérations suivantes:

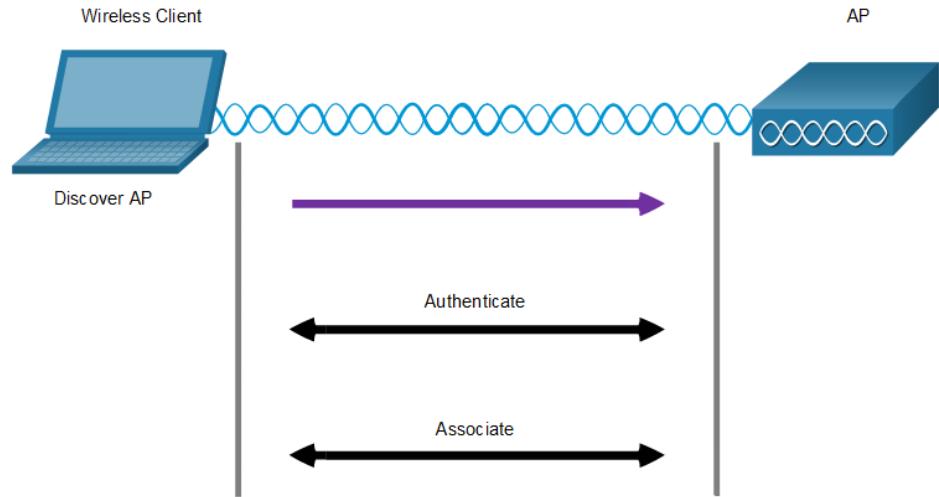
1. Écoute le canal pour voir s'il est inactif, ce qui signifie qu'il détecte qu'aucun autre trafic n'est actuellement sur le canal.
2. Envoie un message prêt à envoyer (RTS) à l'AP pour demander un accès dédié au réseau.
3. Reçoit un message clair à envoyer (CTS) de l'AP accordant l'accès à l'envoi.
4. Attend un laps de temps aléatoire avant de redémarrer le processus si aucun message CTS n'est reçu.
5. Transmet les données.
6. Reconnaît toutes les transmissions. Si un client sans fil ne reçoit pas d'accusé de réception, il suppose qu'une collision s'est produite et redémarre le processus.

# Client sans fil et Association des point d'accès

Pour que les périphériques sans fil puissent communiquer sur le réseau, ils doivent tout d'abord être associés à un point d'accès ou à un routeur sans fil.

Les appareils sans fil effectuent le processus en trois étapes suivant:

- Découvrir de nouveaux points d'accès sans fil
- S'authentifier auprès du point d'accès
- S'associer au point d'accès



## Client sans fil et Association des point d'accès (suite)

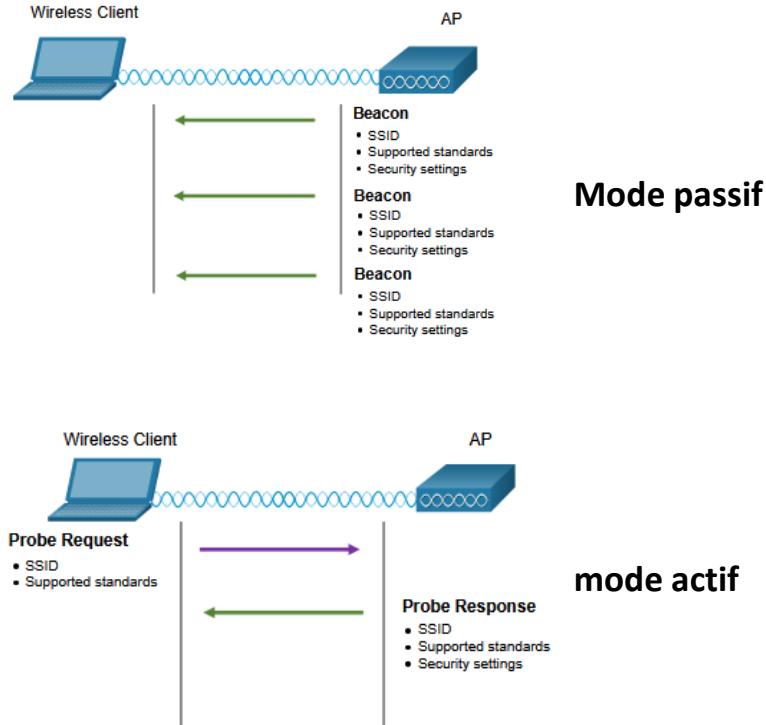
Afin d'avoir une association réussie, un client sans fil et un AP doivent se mettre d'accord sur des paramètres spécifiques.

- **SSID** – Le client doit connaître le nom du réseau pour se connecter.
- **Mot de passe** - Ceci est requis pour que le client s'authentifie auprès de l'AP.
- **Mode réseau** - La norme 802.11 utilisée.
- **Mode de sécurité** - Les réglages des paramètres de sécurité, c'est-à-dire WEP, WPA ou WPA2.
- **Paramètres des canaux** - Les bandes de fréquences utilisées.

# Mode découverte passif et actif

Les clients sans fil se connectent à l'AP à l'aide d'un processus de balayage (sondage) passif ou actif.

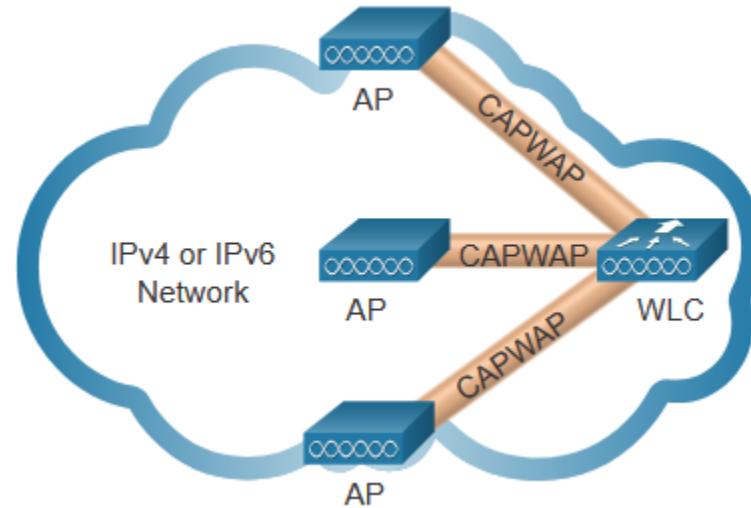
- **Mode passif** - AP annonce ouvertement son service en envoyant périodiquement des trames de balise de diffusion contenant le SSID, les normes prises en charge et les paramètres de sécurité.
- **Mode actif** - Les clients sans fil doivent connaître le nom du SSID. Le client sans fil lance le processus en diffusant une trame de demande d'enquête sur plusieurs canaux.



# 12.4 Fonctionnement du protocole CAPWAP

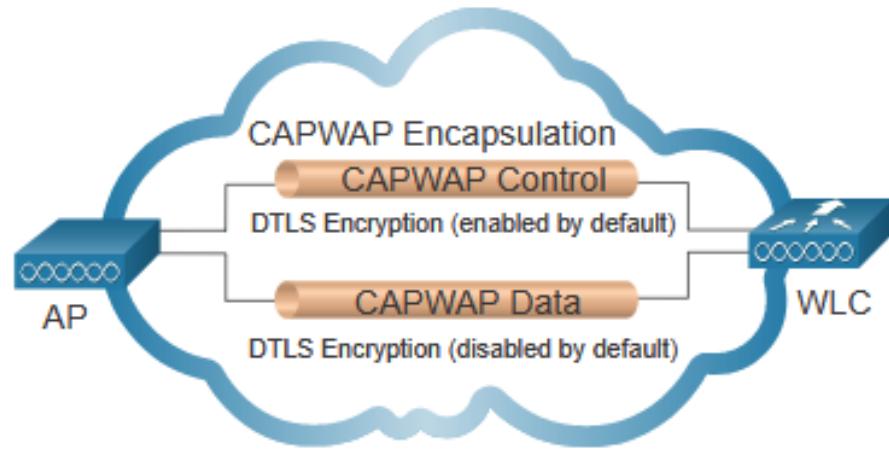
# Introduction au CAPWAP

- CAPWAP est un protocole standard IEEE qui permet à un WLC de gérer plusieurs AP et WLAN.
- CAPWAP est basé sur LWAPP mais ajoute une sécurité supplémentaire avec Datagram Transport Layer Security (DTLS).
- Encapsule et transfère le trafic client WLAN entre un AP et un WLC sur des tunnels en utilisant les ports UDP 5246 et 5247.
- Fonctionne sur IPv4 et IPv6. IPv4 utilise le protocole IP 17 et IPv6 utilise le protocole IP 136.



# Cryptage DTLS

- DTLS assure la sécurité entre l'AP et le WLC.
- Il est activé par défaut pour sécuriser le canal de contrôle CAPWAP et crypter tout le trafic de gestion et de contrôle entre AP et WLC.
- Le chiffrement des données est désactivé par défaut et nécessite qu'une licence DTLS soit installée sur le WLC avant de pouvoir être activée sur l'AP.

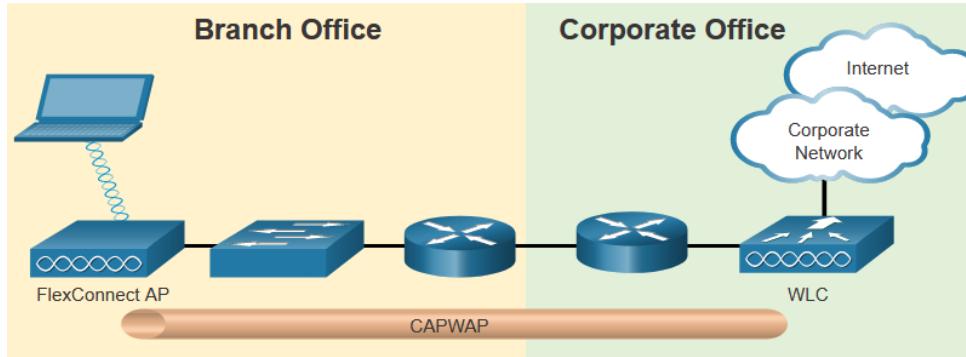


# Flex Connect APs

FlexConnect permet la configuration et le contrôle d'APs sur une liaison WAN.

Il existe deux modes d'option pour le FlexConnect AP:

- **Mode connecté** - Le WLC est accessible. Le FlexConnect AP a une connectivité CAPWAP avec le WLC via le tunnel CAPWAP. Le WLC exécute toutes les fonctions CAPWAP.
- **Mode autonome** - Le WLC est inaccessible. Le FlexConnect AP a une connectivité CAPWAP avec le WLC via le tunnel CAPWAP. Le FlexConnect AP peut assumer certaines des fonctions WLC telles que la commutation locale du trafic de données client et l'exécution de l'authentification client localement.



# 12.5 Gestion des canaux

## Saturation des canaux de fréquences

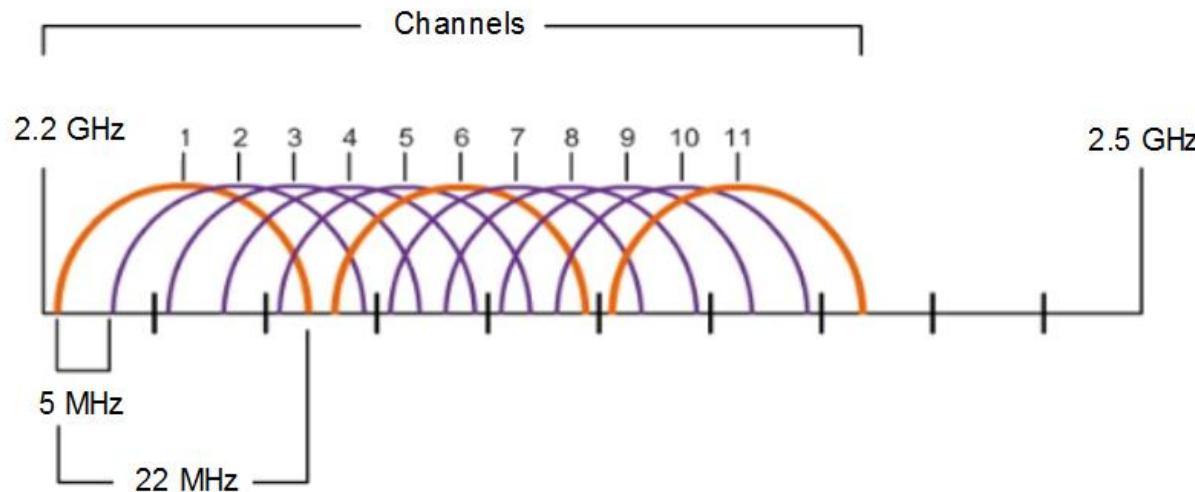
Si la demande pour un canal sans fil spécifique est trop élevée, le canal peut devenir sursaturé, dégradant la qualité de la communication.

La saturation des canaux peut être atténuée en utilisant des techniques qui utilisent les canaux plus efficacement.

- **Spectre à étalage de séquence directe (DSSS)** - Une technique de modulation conçue pour étaler un signal sur une bande de fréquences plus large. Le DSSS est utilisé par les appareils 802.11b pour éviter les interférences d'autres appareils utilisant la même fréquence 2,4 GHz.
- **Spectre étalé à saut de fréquence (FHSS)** - Transmet des signaux radio en commutant rapidement un signal porteur parmi de nombreux canaux de fréquence. L'émetteur et le récepteur doivent être synchronisés pour «savoir» sur quel canal passer. Utilisé par la norme 802.11 d'origine.
- **Multiplexage par répartition en fréquence orthogonale (OFDM)** - Sous-ensemble de multiplexage par répartition en fréquence dans lequel un seul canal utilise plusieurs sous-canaux sur des fréquences adjacentes. L'OFDM est utilisé par un certain nombre de systèmes de communication, notamment 802.11a / g / n / ac.

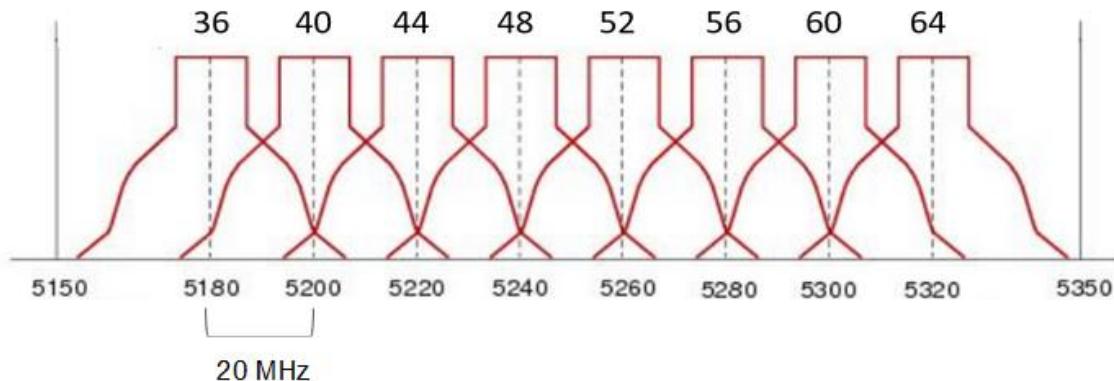
# Sélection des canaux

- La bande de 2,4 GHz est subdivisée en plusieurs canaux, chacun ayant une largeur de bande de 22 MHz et séparée du canal suivant par 5 MHz.
- Une meilleure pratique pour les WLAN 802.11b / g / n nécessitant plusieurs points d'accès est d'utiliser des canaux sans chevauchement tels que 1, 6 et 11.



# Sélection des canaux (suite)

- Pour les normes 5 GHz 802.11a / n / ac, il y a 24 canaux. Chaque canal est séparé du canal suivant de 20 MHz.
- Les canaux qui ne se chevauchent pas sont 36, 48 et 60.

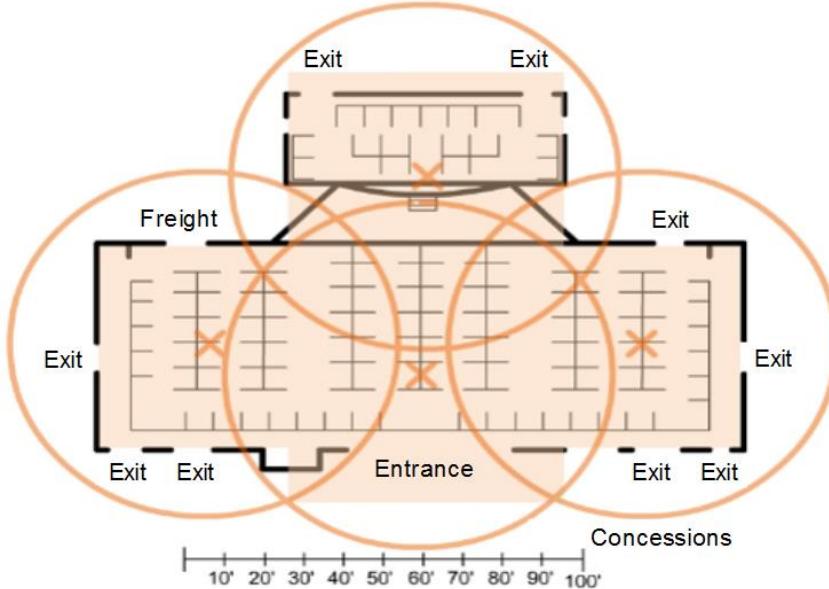


# Planifier un déploiement WLAN

Le nombre d'utilisateurs pris en charge par un WLAN dépend des éléments suivants:

- La disposition géographique de l'installation
- Le nombre de corps et d'appareils pouvant tenir dans un espace
- Les débits de données attendus par les utilisateurs
- L'utilisation de canaux sans chevauchement par plusieurs points d'accès et paramètres de puissance de transmission

Lors de la planification de l'emplacement des points d'accès, la zone de couverture circulaire approximative est importante.



# 12.6 Menaces visant le réseau WLAN

## Présentation de la sécurité sans fil

Un WLAN est ouvert à toute personne à portée d'un point d'accès et aux informations d'identification appropriées à lui associer.

Les attaques peuvent être générées par des étrangers, des employés mécontents et même involontairement par des employés. Les réseaux sans fil sont particulièrement sensibles à plusieurs menaces, notamment:

- Interception de données
- Intrus sans fil
- Attaques par déni de service (DoS)
- Points d'accès escrocs

## les Attaques DoS

Les attaques DoS sans fil peuvent être le résultat de ce qui suit:

- Périphériques mal configurés
- Un utilisateur malveillant interférant intentionnellement avec la communication sans fil
- Interférence accidentelle

Pour minimiser le risque d'une attaque DoS en raison d'appareils mal configurés et d'attaques malveillantes, renforcez tous les appareils, sécurisez les mots de passe, créez des sauvegardes et assurez-vous que toutes les modifications de configuration sont intégrées en dehors des heures d'ouverture.

## Les Points d'Accès Non Autorisés

- Un point d'accès non autorisé est un point d'accès ou un routeur sans fil qui a été connecté à un réseau d'entreprise sans autorisation explicite et conformément à la politique de l'entreprise.
- Une fois connecté, l'escroc AP peut être utilisé par un attaquant pour capturer des adresses MAC, capturer des paquets de données, accéder à des ressources réseau ou lancer une attaque de type homme-au-milieu.
- Un point d'accès au réseau personnel pourrait également être utilisé comme point d'accès non autorisé. Par exemple, un utilisateur avec un accès réseau sécurisé permet à son hôte Windows autorisé de devenir un point d'accès Wi-Fi.
- Pour empêcher l'installation de points d'accès non autorisés, les organisations doivent configurer les WLC avec des stratégies de points d'accès malveillants et utiliser un logiciel de surveillance pour surveiller activement le spectre radioélectrique des points d'accès non autorisés.

## Attaque d'Homme-au-Milieu

Dans une attaque d'homme-au-milieu (MITM), le pirate est positionné entre deux entités légitimes afin de lire ou de modifier les données qui transitent entre les deux parties. Une attaque «evil twin AP» est une attaque MITM sans fil populaire où un attaquant introduit un AP escroc et le configure avec le même SSID qu'un AP légitime

Le processus commence par l'identification des périphériques légitimes sur le WLAN. Pour ce faire, les utilisateurs doivent être authentifiés. Une fois que tous les périphériques légitimes sont connus, le réseau peut être surveillé pour détecter les périphériques ou le trafic anormaux.

# 12.7 WLAN sécurisés

# Masquage SSID et filtrage des adresses MAC

Pour faire face aux menaces de garder les intrus sans fil à l'extérieur et de protéger les données, deux premières fonctions de sécurité ont été utilisées et sont toujours disponibles sur la plupart des routeurs et des points d'accès:

## Masquage SSID

- Les points d'accès et certains routeurs sans fil permettent de désactiver la trame de balise SSID. Les clients sans fil doivent être configurés manuellement avec le SSID pour se connecter au réseau.

## Filtrage d'adresses MAC

- Un administrateur peut autoriser ou refuser manuellement l'accès sans fil des clients en fonction de leur adresse matérielle MAC physique. Dans la figure, le routeur est configuré pour autoriser deux adresses MAC. Les appareils avec des adresses MAC différentes ne pourront pas rejoindre le WLAN 2,4 GHz.

# Méthodes d'authentification d'origine du 802.11

La meilleure façon de sécuriser un réseau sans fil est d'utiliser des systèmes d'authentification et de cryptage. Deux types d'authentification ont été introduits avec la norme 802.11 d'origine:

### **L'authentification de système ouvert,**

- Aucun mot de passe requis. Généralement utilisé pour fournir un accès Internet gratuit dans les espaces publics comme les cafés, les aéroports et les hôtels.
- Le client est responsable d'assurer la sécurité, par exemple via un VPN.

### **Authentification par clé partagée**

- Fournit des mécanismes, tels que WEP, WPA, WPA2 et WPA3 pour authentifier et crypter les données entre un client sans fil et AP. Cependant, le mot de passe doit être pré-partagé entre les deux parties pour se connecter.

# Méthodes d'authentification par clé partagée

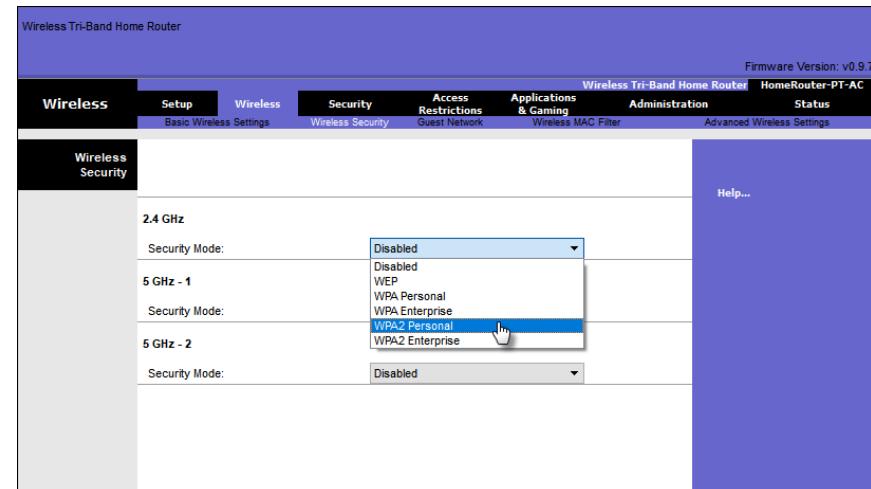
Il existe quatre techniques d'authentification par clé partagée, comme décrit dans le tableau.

Méthode d'authentification	Description
WEP (Wired Equivalent Privacy)	La spécification 802.11 originale conçue pour sécuriser les données à l'aide de la méthode de chiffrement Rivest Cipher 4 (RC4) avec une clé statique. Le WEP n'est plus recommandé et ne doit jamais être utilisé.
Fonction WPA (Wi-Fi Protected Access)	Une norme de l'Alliance Wi-Fi qui utilise le protocole WEP mais sécurise les données grâce à l'algorithme de cryptage TKIP (Temporal Key Integrity Protocol), beaucoup plus puissant. Le protocole TKIP modifie la clé pour chaque paquet, rendant très difficile son piratage.
WPA2	Il utilise le standard de cryptage avancé (AES) pour le cryptage. Le mode de chiffrement AES est actuellement considéré comme étant le protocole de chiffrement le plus puissant.
WPA3	Il s'agit de la prochaine génération de sécurité Wi-Fi. Tous les appareils compatibles WPA3 utilisent les dernières méthodes de sécurité, interdisent les protocoles hérités obsolètes et nécessitent l'utilisation de cadres de gestion protégés (PMF).

# Authentification d'un Utilisateur à Domicile

Les routeurs domestiques ont généralement deux choix pour l'authentification: WPA et WPA2.

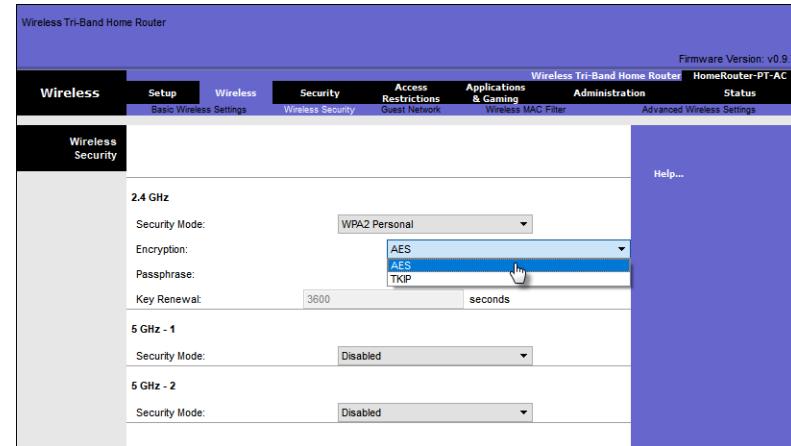
- Personnel** - Destiné aux réseaux domestiques ou de petites entreprises, les utilisateurs s'authentifient à l'aide d'une clé pré-partagée (PSK). Les clients sans fil s'authentifient auprès du routeur sans fil à l'aide d'un mot de passe pré-partagé. Aucun serveur d'authentification spécial n'est requis.
- Entreprise** - Destiné aux réseaux d'entreprise. Nécessite un serveur d'authentification RADIUS (Remote Authentication Dial-In User Service). Le périphérique doit être authentifié par le serveur RADIUS, puis les utilisateurs doivent s'authentifier à l'aide de la norme 802.1X, qui utilise le protocole EAP (Extensible Authentication Protocol) pour l'authentification.



# Méthodes de Cryptage

WPA et WPA2 incluent deux protocoles de chiffrement:

- **Protocole d'Intégrité de Clé Temporelle (TKIP)** – Utilisé par WPA et prend en charge les équipements WLAN hérités. Utilise WEP mais chiffre la charge utile de couche 2 à l'aide de TKIP.
- **Norme de Cryptage Avancée (AES)** - Utilisé par WPA2 et utilise le mode de chiffrement du compteur avec le protocole CCMP (Block Chaining Message Authentication Code Protocol) qui permet aux hôtes de destination de reconnaître si les bits cryptés et non cryptés ont été altérés.



## Authentification dans l'Entreprise

Le choix du mode de sécurité d'entreprise nécessite un serveur RADIUS d'authentification, d'autorisation et de comptabilité (AAA).

Des informations sont nécessaires:

- Adresse IP du serveur RADIUS -** Adresse IP du serveur.
- Numéros de port UDP -** Ports UDP 1812 pour l'authentification RADIUS et 1813 pour la comptabilité RADIUS, mais peuvent également fonctionner à l'aide des ports UDP 1645 et 1646.
- Clé partagée -** Utilisée pour authentifier l'AP avec le serveur RADIUS.

The screenshot shows the 'Wireless Security' configuration page for a Cisco Wireless Tri-Band Home Router. The top navigation bar includes tabs for Wireless, Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The Security tab is selected. The page displays settings for two bands: 2.4 GHz and 5 GHz - 1. Under the 2.4 GHz section, the Security Mode is set to WPA2 Enterprise, Encryption to AES, and the RADIUS Server fields are filled with values 10, 10, 10, and 100 respectively. The RADIUS Port is set to 1645, Shared Secret is J#A)a3XQnq5KsJT, and Key Renewal is 3600 seconds. Under the 5 GHz - 1 section, the Security Mode is set to WPA2 Enterprise and Encryption to AES. A 'Help...' link is located in the top right corner of the main content area.

**Remarque:** l'authentification et l'autorisation des utilisateurs sont gérées par la norme 802.1X, qui fournit une authentification centralisée sur serveur des utilisateurs finaux.

### WPA 3

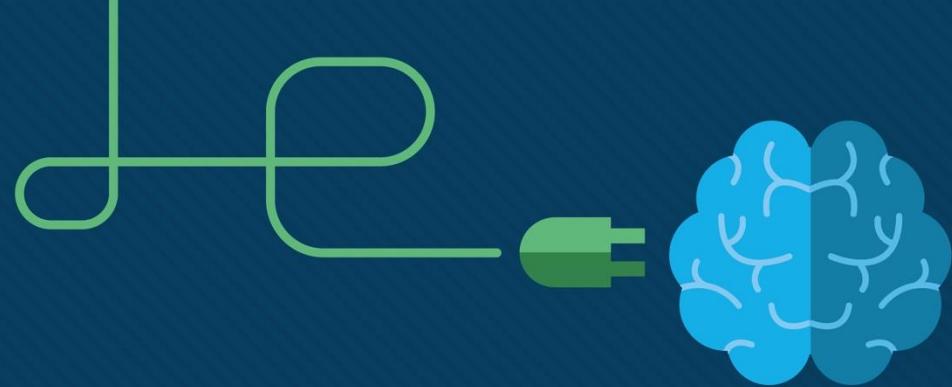
Parce que WPA2 n'est plus considéré comme sécurisé, WPA3 est recommandé lorsqu'il est disponible. WPA3 comprend quatre fonctionnalités:

- **WPA3 - Personnel:** Déjoue les attaques par force brute en utilisant l'authentification simultanée des égaux (SAE).
- **WPA3 - Entreprise:** Utilise l'authentification 802.1X / EAP. Cependant, il nécessite l'utilisation d'une suite cryptographique 192 bits et élimine le mélange des protocoles de sécurité pour les normes 802.11 précédentes.
- **Réseaux ouverts:** N'utilise aucune authentification. Cependant, ils utilisent le chiffrement sans fil opportuniste (OWE) pour chiffrer tout le trafic sans fil.
- **IoT Onboarding:** Utilise le protocole DPP (Device Provisioning Protocol) pour intégrer rapidement les appareils IoT.

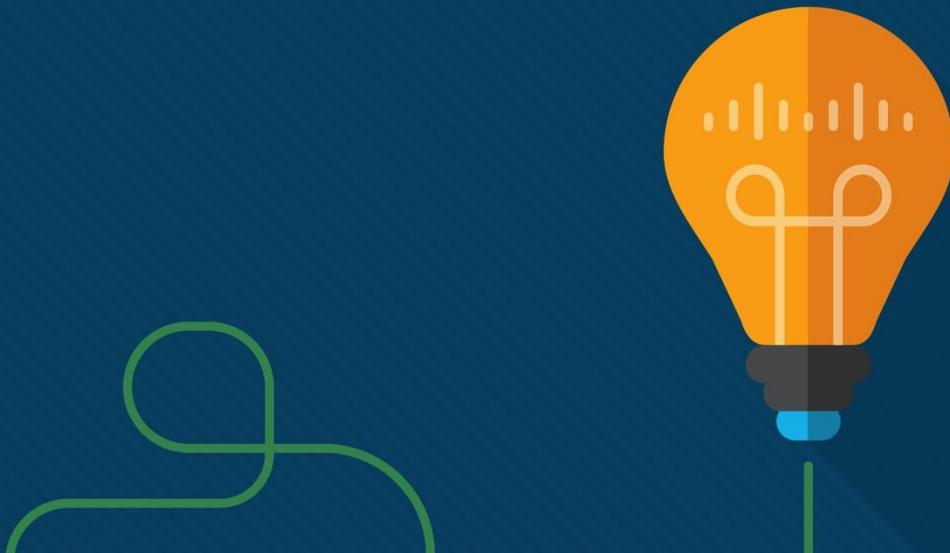
# 12.8 Module pratique et questionnaire

## Qu'est-ce que j'ai appris dans ce module?

- Les réseaux locaux sans fil (WLAN) sont basés sur les normes IEEE et peuvent être classés en quatre types principaux: WPAN, WLAN, WMAN et WWAN.
- La technologie sans fil utilise le spectre radio disponible pour envoyer et recevoir des données. Bluetooth, WiMAX, Cellular Broadband et Satellite Broadband sont des exemples de cette technologie.
- Les réseaux WLAN fonctionnent dans la bande de fréquences 2,4 GHz et la bande 5 GHz.
- Les trois organisations qui influencent les normes WLAN sont l'UIT-R, l'IEEE et la Wi-Fi Alliance.
- CAPWAP est un protocole standard IEEE qui permet à un WLC de gérer plusieurs AP et WLAN.
- DTLS est un protocole qui assure la sécurité entre l'AP et le WLC.
- Les appareils LAN sans fil ont des émetteurs et des récepteurs réglés sur des fréquences spécifiques d'ondes radio pour communiquer. Les portées sont ensuite divisées en plages plus petites appelées canaux: DSSS, FHSS et OFDM.
- Les normes 802.11b / g / n fonctionnent dans le spectre 2,4 GHz à 2,5 GHz. La bande 2,4 GHz est subdivisée en plusieurs canaux. Chaque canal se voit attribuer une bande passante de 22 MHz et est séparé du canal suivant par 5 MHz.
- Les réseaux sans fil sont sensibles aux menaces, notamment l'interception de données, les intrus sans fil, les attaques DoS et les points d'accès malveillants.
- Pour éloigner les intrus sans fil et protéger les données, deux premières fonctions de sécurité sont toujours disponibles sur la plupart des routeurs et des points d'accès: le masquage SSID et le filtrage des adresses MAC.
- Il existe quatre techniques d'authentification par clé partagée: WEP, WPA, WPA2 et WPA3.



# Module 13: Configuration WLAN



# Objectifs du module

**Le Titre de Module:** La Configuration WLAN

**Objectif du module:** Implémenter un WLAN à l'aide d'un routeur sans fil et WLC.

Titre du Rubrique	Objectif du Rubrique
Configuration d'un WLAN de site distant	Configurer un WLAN pour prendre en charge un site distant.
Configuration de WLAN de base sur le WLC	Configurer un WLC WLAN pour utiliser l'interface de gestion et l'authentification PSK WPA2.
Configurer un WPA2 d'entreprise WLAN sur le WLC	Configure un WLC WLAN pour utiliser une interface VLAN, un serveur DHCP et l'authentification WPA2 Enterprise.
Dépannage des problèmes de réseaux WLAN	Dépanner les problèmes courants de configuration sans fil.

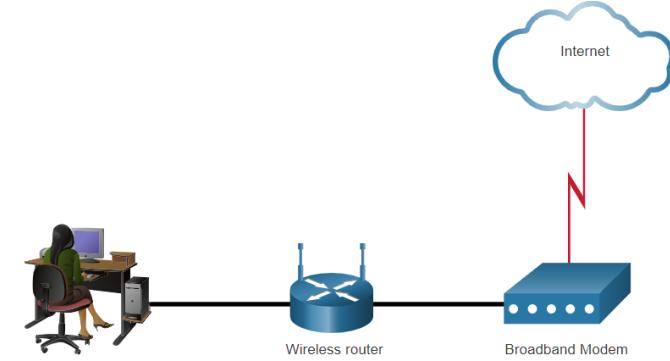
# 13.1 Configuration d'un WLAN de site distant

## Configuration d'un WLAN de site distant

### Le routeur sans fil

Les travailleurs distants, les petites filiales, et les réseaux domestiques utilisent souvent un petit bureau et un routeur domestique.

- Ces routeurs «intégrés» comprennent généralement un commutateur pour les clients câblés, un port pour une connexion Internet (parfois appelé «WAN») et des composants sans fil pour l'accès client sans fil.
- Ces routeurs sans fil offrent généralement la sécurité WLAN, les services DHCP, la traduction d'adresses de nom (NAT) intégrée, la qualité de service (QoS), ainsi que diverses autres fonctionnalités.
- L'ensemble de fonctionnalités variera en fonction du modèle de routeur.



**Remarque:** La configuration du modem câble ou DSL est généralement effectuée par le représentant du fournisseur de services sur site ou à distance.

# Connectez-vous au routeur sans fil

La plupart des routeurs sans fil sont préconfigurés pour être connectés au réseau et fournir des services.

- Les adresses IP, noms d'utilisateur et mots de passe par défaut des routeurs sans fil peuvent être facilement trouvés sur Internet.
- De ce fait, vous devez en priorité changer ces paramètres par défaut pour des raisons de sécurité.

Pour accéder à l'interface graphique de configuration du routeur sans fil

- Ouvrez un navigateur Web et entrez l'adresse IP par défaut de votre routeur sans fil.
- Cette dernière se trouve dans la documentation de votre routeur sans fil. Vous la trouverez également sur Internet.
- Le nom **admin** est communément utilisé comme nom d'utilisateur et mot de passe par défaut.

# Configuration d'un WLAN de site distant

## Configuration de base du réseau

La configuration de base du réseau comprend les étapes suivantes:

- Connectez-vous au routeur à partir d'un navigateur Web.
- Modifier le mot de passe administrateur par défaut
- Connectez-vous avec le nouveau mot de passe d'administrateur.
- Modifiez la plage d'adresses IPv4 DHCP par défaut.
- Renouvez l'adresse IP.
- Connectez-vous au routeur avec la nouvelle adresse IP.



# Configuration d'un WLAN de site distant

## Configuration de base du réseau

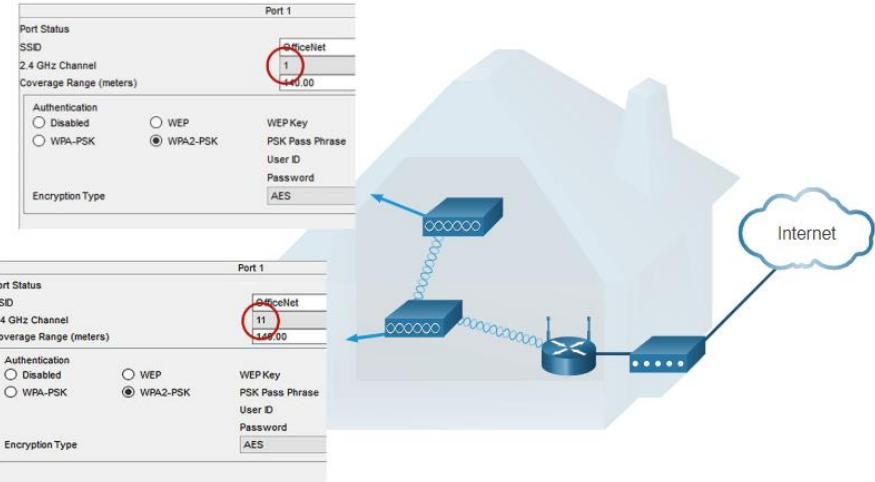
La configuration sans fil de base comprend les étapes suivantes:

- Affichez les paramètres WLAN par défaut.
- Modifiez le mode réseau en identifiant la norme 802.11 à mettre en œuvre.
- Configurez le SSID.
- Configurez le canal en vous assurant qu'il n'y a pas de canaux qui se chevauchent en cours d'utilisation.
- Configurez le mode de sécurité en sélectionnant Open, WPA, WPA2 Personal, WPA2 Enterprise, etc.
- Configurez la phrase secrète, comme requis pour le mode de sécurité sélectionné.

# Configurer un réseau maillé sans fil

Dans une petite entreprise ou chez un particulier, un routeur sans fil peut suffire à fournir un accès sans fil à tous les clients.

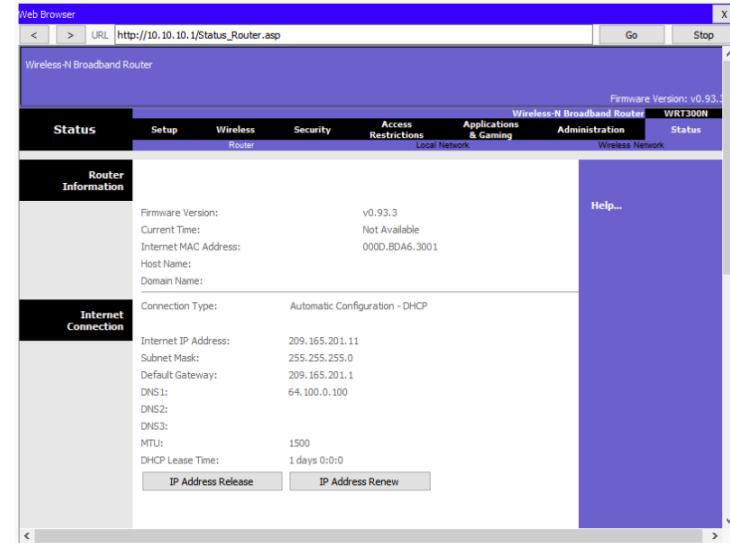
- Si vous voulez étendre la portée au-delà d'environ 45 mètres à l'intérieur et 90 mètres à l'extérieur, vous devez créer un réseau sans fil.
- Créez le maillage (mesh) en ajoutant des points d'accès avec les mêmes paramètres, sauf à utiliser des canaux différents pour éviter les interférences.
- L'extension d'un réseau local sans fil dans un petit bureau ou chez un particulier est devenue de plus en plus facile.
- Les fabricants ont développé des applications de smartphone qui permettent de créer rapidement un réseau sans fil maillé (WMN).



# Configuration d'un WLAN de site distant NAT pour IPv4

En règle générale, l'ISP attribue au routeur sans fil une adresse publiquement routable et utilise une adresse de réseau privé pour l'adressage sur le LAN.

- Pour permettre aux hôtes du LAN de communiquer avec le monde extérieur, le routeur utilisera un processus appelé traduction d'adresses réseau (NAT).
- NAT traduit une adresse IPv4 source privée (locale) en une adresse publique (globale) (le processus est inversé pour les paquets entrants).
- NAT rend possible le partage d'une adresse IPv4 publique en suivant les numéros de port source pour chaque session établie par un appareil.
- Si votre ISP a activé IPv6, vous verrez une adresse IPv6 unique pour chaque appareil.



# Configuration d'un WLAN de site distant

## Qualité de Service

De nombreux routeurs sans fil ont une option de configuration de la qualité de service (QoS).

- La configuration de la qualité de service permet d'accorder la priorité à certains types de trafic (voix ou vidéo) par rapport au trafic qui n'est pas soumis à des contraintes temporelles, notamment la messagerie et la navigation web.
- Sur certains routeurs s des ports spécifiques.

The screenshot shows a user interface for configuring Quality of Service (QoS) on a router. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' being selected. Below the tabs are two buttons: 'Cancel' and 'Apply'. On the left, a sidebar lists several setup options: 'Setup', 'Internet Setup', 'Wireless Setup', 'LAN Setup', and 'QoS Setup'. The 'QoS Setup' option is highlighted with a blue arrow pointing towards the main content area. The main area is titled 'QoS Setup' and contains a table with the following data:

#	QoS Policy	Priority	Description
1	IP Phone	High	IP Phone applications
2	Counter Strike	High	Online Gaming Counter Strike
3	Netflix	High	Online Video Streaming Netflix
4	FTP	Medium	FTP Applications
5	WWW	Medium	WWW Applications
6	Gnutella	Low	Gnutella Applications
7	SMTP	Medium	SMTP Applications

Below the table, there are buttons for 'Edit', 'Delete', and 'Delete All'. At the bottom, there is a button labeled 'Add Priority Role'.

# Redirection de Port

Les routeurs sans fil bloquent les ports TCP et UDP pour éviter les accès non autorisés au LAN internes ou externes.

- Toutefois, il faut parfois ouvrir des ports spécifiques pour permettre à certains programmes et applications de communiquer avec les périphériques de différents réseaux.
- La redirection de port est une méthode basée sur des règles qui redirige le trafic entre des périphériques situés sur des réseaux distincts.
- Le déclenchement de port autorise le routeur à transférer temporairement les données via les ports entrants vers un périphérique spécifique.
- Cela permet par exemple de transférer des données à un ordinateur uniquement lorsqu'une plage de ports désignée est utilisée pour émettre une requête sortante.

# Packet Tracer - Configurer un Réseau Sans Fil

Dans cette activité Packet Tracer, vous remplirez les objectifs suivants:

- Se connecter à un routeur sans fil
- Configurer le routeur sans fil
- Connecter un appareil filaire au routeur sans fil
- Connecter un appareil sans fil au routeur sans fil
- Ajouter un point d'accès au réseau pour étendre la couverture sans fil
- LAB13.1-WLAN

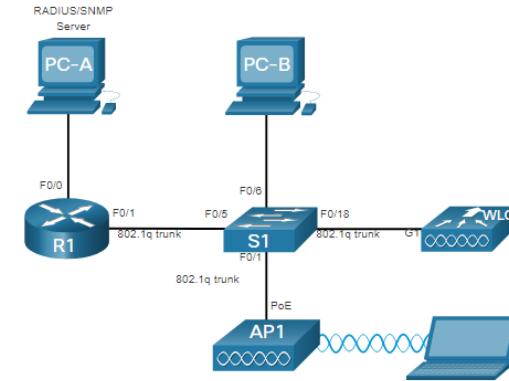
# 13.2 Configurer un WLAN de base sur le WLC

# Configurer un WLAN de base sur le WLC

## Topologie WLC

La topologie et le schéma d'adressage utilisés pour les vidéos et cette rubrique sont illustrés dans la figure et le tableau.

- Le point d'accès (AP) est un AP basé sur un contrôleur par opposition à un AP autonome, il ne nécessite donc aucune configuration initiale et est souvent appelé AP léger (LAP).
- Les LAP utilisent le Lightweight Access Point Protocol (LWAPP) pour communiquer avec un contrôleur WLAN (WLC).
- Les points d'accès basés sur un contrôleur sont utiles dans les situations où de nombreux points d'accès sont requis dans le réseau.
- En ajoutant plus d'AP, chaque AP est automatiquement configuré et géré par le WLC.



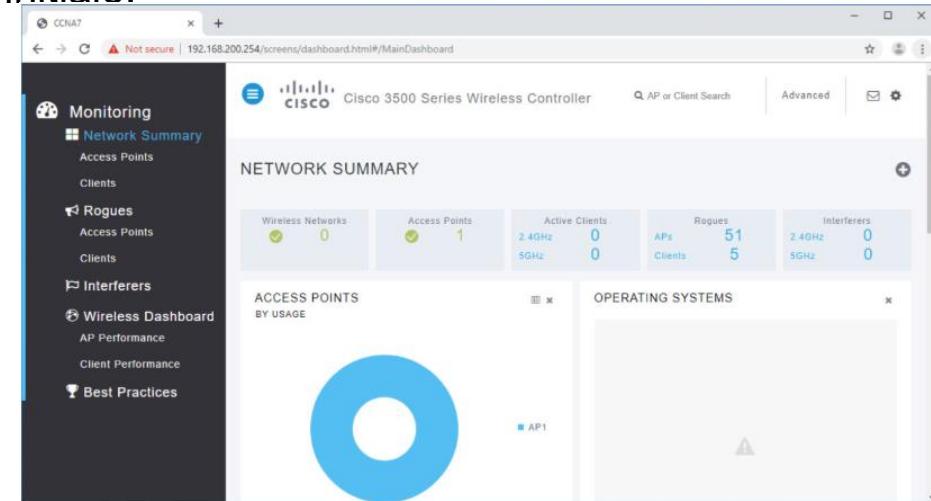
Appareil	Interface	Adresse IP	Masque de sous-réseau
R1	F0/0	172.16.1.1	255.255.255.0
R1	F0/1.1	192.168.200.1	255.255.255.0
S1	VLAN 1	le protocole DHCP	
WLC	Gestion	192.168.200.254	255.255.255.0
AP1	filaire 0	192.168.200.3	255.255.255.0
PC-A	Carte réseau (NIC)	172.16.1.254	255.255.255.0
PC-B	Carte réseau (NIC)	DHCP	
Ordinateur portable sans fil	Carte réseau (NIC)	DHCP	

# Configurer un WLAN de base sur le WLC

## Connectez-vous au WLC

La configuration d'un contrôleur LAN sans fil (WLC) n'est pas très différente de la configuration d'un routeur sans fil. Le WLC contrôle les points d'accès et fournit plus de services et de capacités de gestion.

- L'utilisateur se connecte au WLC en utilisant des informations d'identification qui ont été configurées lors de la configuration initiale.
- La page **Résumé du réseau** est un tableau de bord qui fournit un aperçu rapide des réseaux sans fil configurés, des points d'accès associés (AP) et des clients actifs.
- Vous pouvez également voir le nombre de points d'accès non autorisés et de clients.



# Configurer un WLAN de base sur le WLC

## Afficher les informations AP

Cliquez sur **Points d'accès** dans le menu de gauche pour afficher une image globale des informations système et des performances du point d'accès.

- L'AP utilise l'adresse IP 192.168.200.3.
- Étant donné que Cisco Discovery Protocol (CDP) est actif sur ce réseau, le WLC indique que l'AP est connecté au port FastEthernet 0/1 sur le commutateur.
- Cet AP dans la topologie est un Cisco Aironet 1815i, ce qui signifie que vous pouvez utiliser la ligne de commande et un ensemble limité de commandes IOS familières.

ACCESS POINT VIEW

GENERAL

AP Name: AP1

Location: default location

MAC Address: 2c:4f:52:60:37:e8

IP Address: 192.168.200.3

CDP / LLDP: Switch, FastEthernet0/1

Ethernet Speed: 100 Mbps

Model / Domain: AIR-AP1815I-B-K9 / 802.11bg:-A 802.11a:-B

Power status: PoE/Full Power

Serial Number: FCW2320NGDH

Groups: AP Group: default-group, Flex Group: default-flex-group

Mode / Sub-mode: Local / Not Configured

Max Capabilities: 802.11n 2.4GHz, 802.11ac 5GHz Spatial Streams : 2 (2.4GHz), 2 (5.0GHz) Max. Data Rate : 144 Mbps(2.4GHz), 867 Mbps(5.0GHz)

Fabric: Disabled

PERFORMANCE SUMMARY

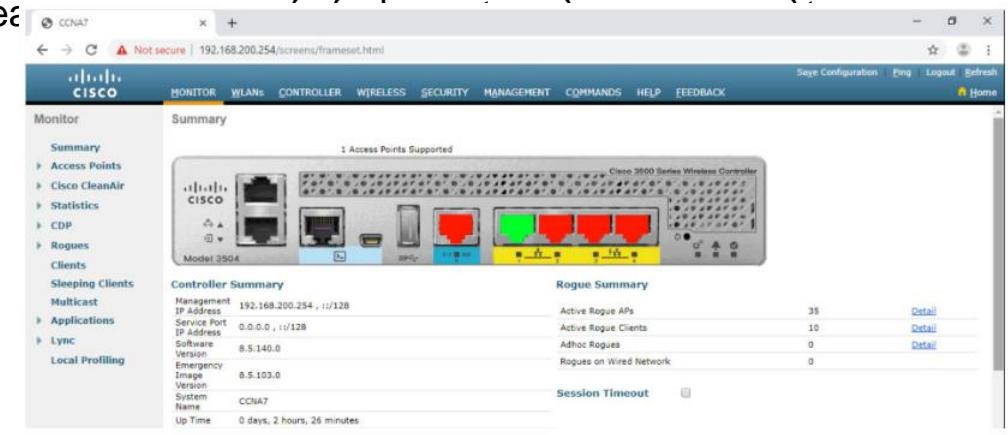
	2.4GHz	5GHz
Number of clients	1	0
Channels	11	(100, 104, 108, 112)
Configured Rate	Min: 1 Mbps, Max: 144 Min: 6 Mbps, Max: 867 Mbps	
Usage Traffic	709.4 MB	231.1 KB
Throughput	2.1 KB	0
Transmit Power	20 dBm	20 dBm
Noise	-90	-93 -95 -95 -95
Channel Utilization	9%	1%
Interference	7%	1%
Traffic	2%	0%
Air Quality	-	-
Admin Status	Enabled	Enabled
Clean Air Status	Not applicable	Not applicable

# Configurer un WLAN de base sur le WLC

## Paramètres Avancés

La plupart des WLC viennent avec des paramètres et des menus de base auxquels les utilisateurs peuvent accéder rapidement pour mettre en œuvre une variété de configurations courantes.

- Cependant, en tant qu'administrateur de réseau, vous pouvez également accéder à tous les paramètres avancés.
- Pour le contrôleur sans fil Cisco 3504, cliquez sur **Avancé** dans le coin supérieur droit pour accéder à la page **Résumé** avancée.
- De là, vous pouvez accéder à toutes les fonctionnalités du WLC.



## Configurer un WLAN de base sur le WLC

# Configurer un WLAN

Les contrôleurs LAN sans fil ont des ports de commutation de couche 2 et des interfaces virtuelles qui sont créés dans le logiciel et sont très similaires aux interfaces VLAN.

- Chaque port physique peut prendre en charge de nombreux points d'accès et WLANs.
- Les ports sur le WLC sont essentiellement des ports de jonction qui peuvent transporter le trafic de plusieurs VLAN vers un commutateur pour la distribution vers plusieurs AP.
- Chaque AP peut prendre en charge plusieurs WLAN.



## Configurer un WLAN de base sur le WLC

# Configurer un WLAN (suite)

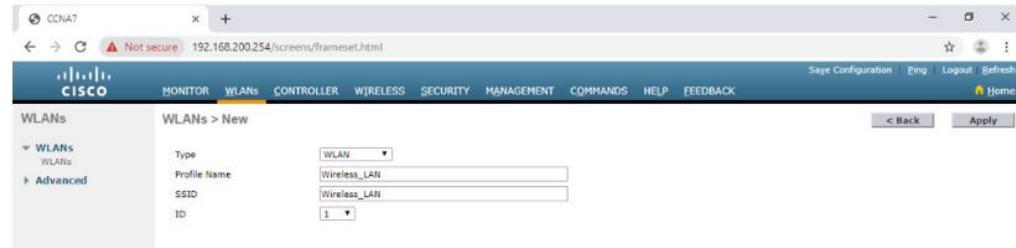
La configuration de base du WLAN sur le WLC comprend les étapes suivantes:

1. Créez le WLAN
2. Appliquez et activez le WLAN
3. Choisissez l'interface.
4. Sécurisez le WLAN
5. Vérifiez que le WLAN est opérationnel
6. Surveillez le WLAN
7. Affichez les informations du client sans fil

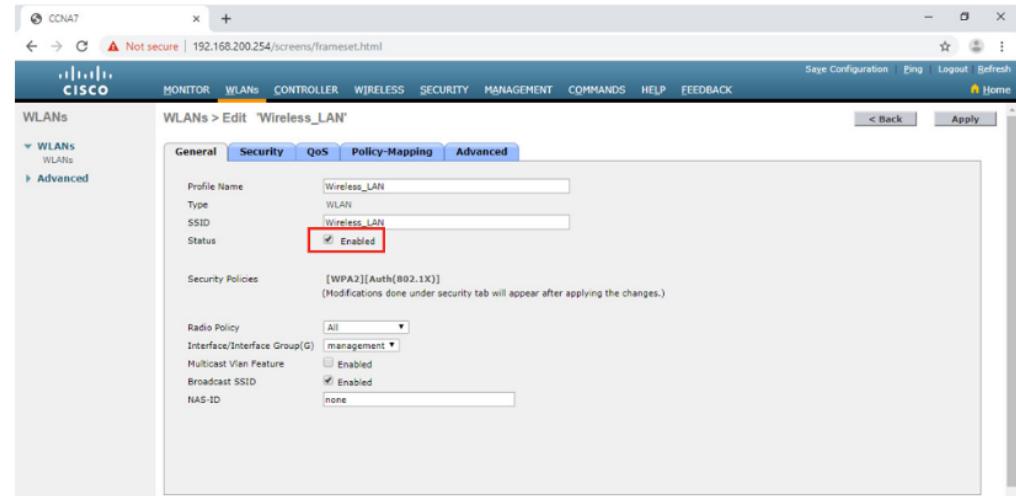
# Configurer un WLAN de base sur le WLC

## Configurer un WLAN (suite)

- Créer le WLAN:** Dans la figure, un nouveau WLAN avec un nom SSID **Wireless\_LAN** est créé.



- Appliquer et activer le WLAN:** Ensuite, le WLAN est activé, les paramètres WLAN sont configurés.



# Configurer un WLAN de base sur le WLC

## Configurer un WLAN (suite)

### 3. Sélectionner l'interface:

l'interface qui acheminera le trafic WLAN doit être sélectionnée.

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. In the top navigation bar, the 'WLANS' tab is selected. On the left, a tree view shows 'WLANS' expanded, with 'Advanced' selected. The main panel displays the 'General' tab for a WLAN profile named 'Wireless\_LAN'. The 'Interface/Interface Group(G)' dropdown menu is open, and the option 'user\_wlan' is highlighted with a red box. Other visible fields include 'Profile Name' (Wireless\_LAN), 'Type' (WLAN), 'SSID' (Wireless\_LAN), and 'Status' (Enabled). A note at the bottom states: '[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)'.

### 4. Sécuriser le WLAN: L'onglet Sécurité est utilisé pour accéder à toutes les options disponibles pour sécuriser le LAN.

The screenshot shows the 'Security' tab for the same WLAN profile 'Wireless\_LAN'. The 'PSK' checkbox is checked and highlighted with a red box. Other visible sections include 'WPA + WPA2 Parameters' (with 'WPA2 Encryption' checked and 'AES' selected), 'Authentication Key Management' (with 'PSK' checked and highlighted with a red box), and 'SuiteB-1X' (with 'Enable' checked). The 'Apply' button in the top right corner is also highlighted with a red box.

# Configurer un WLAN de base sur le WLC

## Configurer un WLAN (suite)

- 5. Vérifiez que le WLAN est opérationnel:** le menu **WLANs** à gauche est utilisé pour afficher le WLAN nouvellement configuré et ses paramètres.

- 6. Surveiller le WLAN:** L'onglet **Moniteur** est utilisé pour accéder à la page **Résumé** avancé et confirmer que le **Wireless\_LAN** a maintenant un client utilisant ses services.

# Configurer un WLAN de base sur le WLC

## Configurer un WLAN (suite)

7. Afficher les détails du client sans fil: cliquez sur **Clients** dans le menu de gauche pour afficher plus d'informations sur les clients connectés au WLAN.

The screenshot shows the Cisco Wireless Local Controller (WLC) web interface. The top navigation bar includes links for Site Configuration, Ping, Logout, Refresh, Home, MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar menu under 'Monitor' has items: Summary, Access Points, Cisco CleanAir, Statistics, CDP, and Rogues. The 'Clients' item is highlighted with a red box. The main content area is titled 'Clients' and shows one entry: Client MAC Addr 00:13:ce:57:7c:67, IP Address(Ipv4/Ipv6) 192.168.5.2, AP Name AP1. To the right, there are columns for WLAN Profile (Wireless\_LAN) and WLAN SSID (Wireless\_LAN). At the bottom right of the content area, it says 'Entries 1 - 1 of 1'. Below the content area, there are 'Change Filter' and 'Clear Filter' buttons.

## Packet Tracer – Configurer un WLAN de base sur le WLC

Dans ces travaux pratiques, vous allez explorer certaines des fonctionnalités d'un contrôleur LAN sans fil.

- Vous allez créer un nouveau WLAN sur le contrôleur et implémenter la sécurité sur ce LAN.
- Ensuite, vous allez configurer un hôte sans fil pour se connecter au nouveau WLAN via un point d'accès qui est contrôlé par le WLC.
- Enfin, vous vérifierez la connectivité.
- **LAB13.2-WLAN**

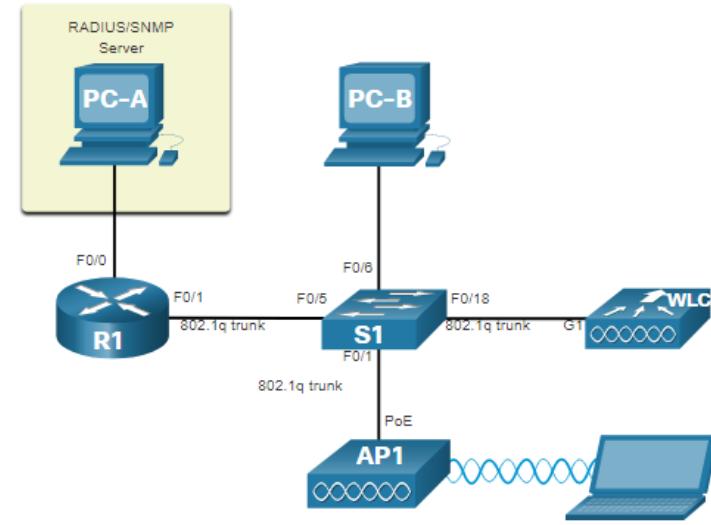
# 13.3 Configurer un WLAN WPA2 Enterprise sur le WLC

# Configurer un WLAN WPA2 Enterprise sur le WLC SNMP et RADIUS

PC-A exécute le protocole SNMP (Simple Network Management Protocol) et le logiciel serveur RADIUS (Remote Authentication Dial-In User Service).

- L'administrateur réseau veut que le WLC transfère tous les messages de journal SNMP (c'est-à-dire les interruptions) au serveur SNMP.
- L'administrateur réseau souhaite utiliser un serveur RADIUS pour les services d'authentification, d'autorisation et de comptabilité (AAA).
- Les utilisateurs entreront leurs identifiants de nom d'utilisateur et de mot de passe qui seront vérifiés par le serveur RADIUS.
- Le serveur RADIUS est requis pour les WLAN qui utilisent l'authentification WPA2 Enterprise.

**Remarque:** la configuration du serveur SNMP et du serveur RADIUS dépasse la portée de ce module.



# Configurez un WLAN WPA2 Enterprise sur le WLC

## Configurez les informations du serveur SNMP

Pour activer SNMP et configurer les paramètres:

1. Cliquez sur l'onglet **GESTION** pour accéder à une variété de fonctionnalités de gestion.
  2. Cliquez **SNMP** pour développer les sous-menus.
  3. Cliquez **Récepteurs de piège**.
  4. Cliquez **Nouveau...** pour configurer un nouveau récepteur d'interruption SNMP.
- 
- Saisissez le nom de la communauté SNMP et l'adresse IP (IPv4 ou IPv6) du serveur SNMP, puis cliquez sur **Appliquer**.
  - Le WLC va maintenant transmettre des messages de journal SNMP au serveur SNMP.



# Configurez un WLAN WPA2 Enterprise sur le WLC

## Configurez les informations de serveur RADIUS

Pour configurer le WLC avec les informations du serveur RADIUS:

1. Cliquez sur **Sécurité**.
2. Cliquez sur **RADIUS**
3. Cliquez sur **Authentification**
4. Cliquez sur **Nouveau ...** pour ajouter PC-A en tant que serveur RADIUS.
  - Entrez l'adresse IPv4 pour PC-A et le secret partagé qui sera utilisé entre le WLC et le serveur RADIUS, puis cliquez sur Appliquer.

The image contains two screenshots of the Cisco Wireless Local Controller (WLC) web interface. Both screenshots show the 'RADIUS Authentication Servers' configuration page under the 'Security' tab.

**Screenshot 1 (Top):** Shows the main configuration page for RADIUS servers. It includes fields for 'Auth Called Station ID Type' (set to 'AP MAC Address:SSID'), 'Use AES Key Wrap' (unchecked), 'MAC Delimiter' (set to 'Hyphen'), and 'Framed MTU' (set to '1500'). Below these are tabs for 'Network User', 'Management', 'Tunnel Proxy', 'Server Index', 'Server Address(Ipv4/Ipv6)', 'Port', 'IPSec', and 'Admin Status'. A sidebar on the left lists AAA components: General, RADIUS (selected), TACACS+, LDAP, Local Net Users, MAC Filtering, and Disabled Clients. A red circle labeled '1' highlights the 'SECURITY' tab in the top navigation bar. A red circle labeled '2' highlights the 'RADIUS' component in the sidebar. A red circle labeled '3' highlights the 'Authentification' link under the RADIUS component. A red circle labeled '4' highlights the 'New...' button in the top right corner.

**Screenshot 2 (Bottom):** Shows the 'RADIUS Authentication Servers > New' configuration page. It has a 'Server Index (Priority)' dropdown set to '1'. The 'Server IP Address(Ipv4/Ipv6)' field contains '172.16.1.254'. The 'Shared Secret Format' is set to 'ASCII' with the shared secret '\*\*\*\*\*'. The 'Confirm Shared Secret' field also contains '\*\*\*\*\*'. Other settings include 'Key Wrap' (unchecked), 'Port Number' (set to '1812'), 'Server Status' (set to 'Enabled'), 'Support for CoA' (set to 'Disabled'), 'Server Timeout' (set to '5 seconds'), 'Network User' (checked), 'Management' (checked), and 'Management Retransmit Timeout' (set to '5 seconds'). A red circle labeled '1' highlights the 'Server Index (Priority)' dropdown. A red circle labeled '2' highlights the 'Server IP Address(Ipv4/Ipv6)' field. A red circle labeled '3' highlights the 'Shared Secret Format' dropdown. A red circle labeled '4' highlights the 'Apply' button in the top right corner.

# Configurez un WLAN WPA2 Enterprise sur le WLC

## Configurez les informations de serveur RADIUS

Après avoir cliquer sur **Appliquer**, la liste de configuration du serveur d'authentification RADIUS est actualisée avec le nouveau serveur répertorié.

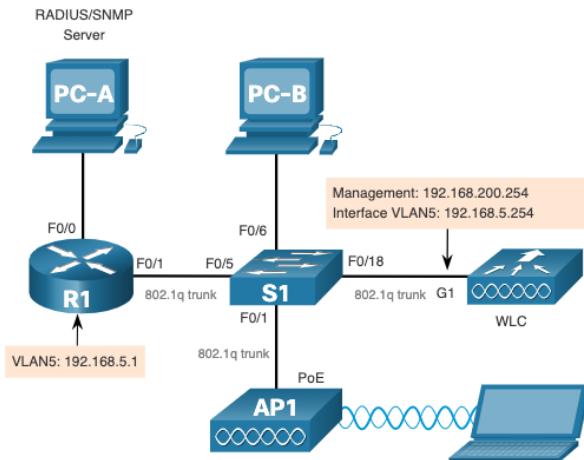
The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar includes links for Site Configuration, Log, Logout, Refresh, Home, MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (which is highlighted in orange), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar under the Security section has expanded the AAA category, showing RADIUS, TACACS+, and LDAP options. The main content area is titled "RADIUS Authentication Servers". It contains several configuration fields: "Auth Called Station ID Type" set to "AP MAC Address:SSID", "Use AES Key Wrap" with a note about FIPS compliance, "MAC Delimiter" set to "Hyphen", and "Framed MTU" set to "1300". Below these is a table titled "Radius Servers" with one row. The table columns are: Network User, Management, Tunnel Proxy, Server Index, Server Address(Ipv4/Ipv6), Port, IPSec, and Admin Status. The single row in the table has its "Server Address(Ipv4/Ipv6)" field (containing "172.16.1.254") highlighted with a red border. The "Admin Status" for this entry is "Enabled".

# Configurez un WPA2 d'entreprise WLAN sur le WLC

## Topologie avec adressage VLAN 5

Chaque WLAN configuré sur le WLC a besoin de sa propre interface virtuelle.

- Le WLC a cinq ports de données physiques qui peuvent être configurés pour prendre en charge plusieurs WLAN et une interface virtuelle.
- Le nouveau WLAN utilisera l'interface VLAN 5 et le réseau 192.168.5.0/24 et, par conséquent, R1 a été configuré pour VLAN 5 comme indiqué dans la topologie et la sortie de **show ip interface brief**.



```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    172.16.1.1     YES manual up       up
FastEthernet0/1    unassigned      YES unset  up       up
FastEthernet0/1.1  192.168.200.1  YES manual up       up
FastEthernet0/1.5  192.168.5.254  YES manual up       up
(output omitted)
R1#
```

# Configurez un WLAN WPA2 Enterprise sur le WLC

## Configurez une nouvelle interface

La configuration de l'interface VLAN sur le WLC comprend les étapes suivantes:

1. Créez une nouvelle interface
2. Configurez le nom et l'ID VLAN.
3. Configurez le port et l'adresse interface.
4. Configurez l'adresse du serveur DHCP.
5. Appliquez et confirmez.
6. Vérifiez les interfaces.

# Configurez un WPA2 d'entreprise WLAN sur le WLC

## Configurez une nouvelle interface (suite)

- Créez une nouvelle interface:  
cliquez CONTRÔLEUR>  
Interfaces> Nouveau ...

The screenshot shows the Cisco Wireless LAN Controller (WLC) web interface. The top navigation bar has tabs: MONITOR, WLAN, **CONTROLLER**, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The CONTROLLER tab is highlighted with a red box and a circled '1'. The left sidebar menu includes: General, Icons, Inventory, **Interfaces** (highlighted with a red box and circled '2'), Interface Groups, Multicast, Network Routes, and Fabric Configuration. The main content area displays a table titled 'Interfaces' with the following data:

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
management	untagged	192.168.200.254	Static	Enabled	::/128
redundancy-management	untagged	0.0.0.0	Static	Not Supported	
redundancy-roots	untagged	0.0.0.0	Static	Not Supported	
service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
virtual	N/A	192.0.2.1	Static	Not Supported	

At the bottom right of the interface, there is a 'New...' button with a circled '3'.

- Configurez le nom et l'ID du VLAN: dans l'exemple, la nouvelle interface est nommée **vlan5**, l'ID du VLAN est **5** et appliquée.

The screenshot shows the 'Interfaces > New' configuration dialog. The top navigation bar has tabs: MONITOR, WLANs, **CONTROLLER**, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The CONTROLLER tab is highlighted with a red box. The left sidebar menu includes: General, Icons, Inventory, and **Interfaces**. The main content area has two input fields: 'Interface Name' containing 'vian5' and 'VLAN Id' containing '5'. At the bottom right, there is an 'Apply' button with a circled '4'.

# Configurez un WLAN WPA2 d'entreprise sur le WLC

## Configurez une nouvelle interface (suite)

3. Configurez le port et l'adresse d'interface: Sur la page d'édition d'interface, configurez le numéro de port physique (c.-à-d., L'interface WLC G1 est le numéro de port 1 sur le WLC), l'adressage d'interface VLAN 5 (c.-à-d., 192.168.5.254/24), et la passerelle par défaut (ie, 192.168.5.1)

The screenshot shows the Cisco Wireless Local Controller (WLC) configuration interface. The top navigation bar includes 'Say Configuration', 'Ping', 'Logout', 'Refresh', 'Home', '< Back', and 'Apply'. The main menu on the left lists various controller functions: General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, Internal DHCP Server, Mobility Management, Ports, NTP, CDP, PMIPv6, Tunneling, IPv6, mDNS, and Advanced. The 'Interfaces' option is selected. The current view is 'Interfaces > Edit' for 'vlan5'. The 'General Information' section shows the Interface Name as 'vlan5' and the MAC Address as '70:18:a7:c8:cc:f1'. The 'Configuration' section includes fields for Guest Lan (unchecked), Quarantine (unchecked), Quarantine Vlan Id (set to 0), and NAS-ID (set to 'none'). The 'Physical Information' section has the Port Number set to '1' (highlighted with a red box). The 'Interface Address' section shows the VLAN Identifier as '5', the IP Address as '192.168.5.254' (highlighted with a red box), the Netmask as '255.255.255.0', and the Gateway as '192.168.5.1'.

# Configurez un WLAN WPA2 d'entreprise sur le WLC

## Configurez une nouvelle interface (suite)

### 4. Configurez l'adresse du serveur

**DHCP:** l'exemple configure un serveur DHCP principal à l'adresse IPv4 192.168.5.1, qui est l'adresse de routeur de passerelle par défaut activée en tant que serveur DHCP.

Screenshot of the Cisco WLC web interface showing the configuration of a new interface. The 'Controller' tab is selected. In the 'Interface Address' section, the 'IP Address' field is set to 192.168.5.254. In the 'DHCP Information' section, the 'Primary DHCP Server' field is highlighted with a red box and contains the value 192.168.5.1.

### 5. Appliquez et confirmez: faites défiler vers le haut et cliquez sur **Appliquer**, puis sur **OK** pour le message d'avertissement.

Screenshot of the Cisco WLC web interface showing the confirmation dialog for changing interface parameters. The message says: "Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients." There are "OK" and "Cancel" buttons at the bottom.

# Configurez un WLAN WPA2 d'entreprise sur le WLC

## Configurez une nouvelle interface (suite)

6. Vérifiez les interfaces: cliquez sur **Interfaces** pour vérifier que la nouvelle interface **vlan5** apparaît dans la liste des interfaces avec son adresse IPv4.



The screenshot shows the Cisco Wireless Local Controller (WLC) web interface. The top navigation bar includes links for 'Sayle Configuration', 'Ping', 'Logout', and 'Refresh'. On the far right, there's a 'Home' icon. The main menu on the left has several sections: 'Controller' (selected), 'General', 'Icons', 'Inventory', 'Interfaces' (selected), 'Interface Groups', 'Multicast', 'Network Routes', 'Fabric Configuration', and 'Redundancy'. The central 'Interfaces' table lists network interfaces with columns for 'Interface Name', 'VLAN Identifier', 'IP Address', 'Interface Type', 'Dynamic AP Management', and 'IPv6 Address'. The table shows seven entries, including 'management', 'redundancy-management', 'redundancy-port', 'service-port', 'user\_wlan', 'virtual', and 'vlan5'. The 'vlan5' entry has an IP address of 192.168.5.254 and is listed as Dynamic.

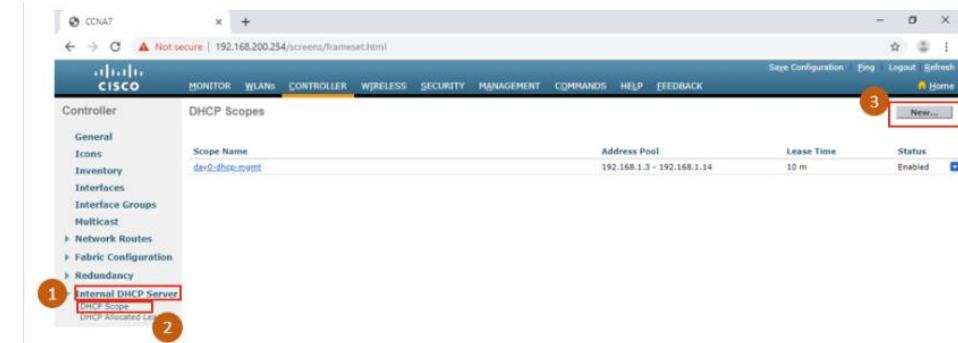
Interfaces						
	Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management	IPv6 Address
	management	untagged	192.168.200.254	Static	Enabled	::/128
	redundancy-management	untagged	0.0.0.0	Static	Not Supported	
	redundancy-port	untagged	0.0.0.0	Static	Not Supported	
	service-port	N/A	0.0.0.0	DHCP	Disabled	::/128
	user_wlan	10	192.168.10.254	Dynamic	Disabled	::/128
	virtual	N/A	1.1.1.1	Static	Not Supported	
	vlan5	5	192.168.5.254	Dynamic	Disabled	::/128

# Configurer un WLAN WPA2 Enterprise sur le WLC

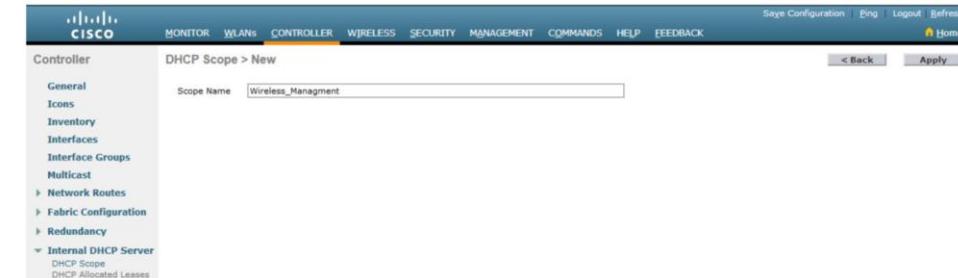
## Vidéo – Configurer une étendue DHCP (Suite)

- Créez une nouvelle étendue DHCP:  
pour configurer une nouvelle étendue DHCP, cliquez sur **Serveur DHCP interne**> **Etendue DHCP**> **Nouveau**

....



- Nommez la portée DHCP: l'étendue est nommée **Wireless\_Management** puis appliquée.



# Configurer un WLAN WPA2 Entreprise sur le WLC

## Vidéo – Configurer une étendue DHCP (suite)

### 3. Vérifiez la nouvelle étendue

DHCP: dans la page **DHCP Scope**, cliquez sur le nouveau nom d'étendue pour configurer l'étendue DHCP.

### 4. Configurez et activez la nouvelle étendue DHCP: sur l'écran Modifier pour la portée **sans fil\_de gestion**, configurez un pool d'adresses (par exemple, 192.168.200.240/24 à .249), l'adresse IPv4 par défaut du routeur (par exemple, 192.168.200.1), puis **Activé** et **Appliquer**.

Scope Name	Address Pool	Lease Time
Wireless_Management	0.0.0.0 - 0.0.0.0	1 d
	192.168.1.3 - 192.168.1.14	1 d

Scope Name: Wireless\_Management

Pool Start Address: 192.168.200.240

Pool End Address: 192.168.200.249

Network: 192.168.200.0

Netmask: 255.255.255.0

Lease Time (seconds): 86400

Default Routers: 192.168.200.1

DNS Domain Name:

DNS Servers:

Netsios Name Servers:

Status: Enabled

# Configurer un WLAN WPA2 Entreprise sur le WLC

## Vidéo – Configurer une étendue DHCP (suite)

### 5. Vérifiez la portée DHCP active:

l'administrateur réseau revient à la page **Étendues DHCP** et peut vérifier que la portée est prête à être allouée à un nouveau WLAN.

The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes links for Site Configuration, Ping, Logout, Refresh, and Home. The main menu tabs are MONITOR, WLANs, CONTROLLER (which is highlighted in orange), WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. On the left, a sidebar menu lists General, Icons, Inventory, Interfaces, Interface Groups, Multicast, Network Routes, Fabric Configuration, Redundancy, and Internal DHCP Server (which is expanded to show DHCP Scope and DHCP Allocated Leases). The central pane is titled "DHCP Scopes". It displays a table with one row for "Wireless Management" under "Scope Name". The "Address Pool" column shows two ranges: "192.168.200.240 - 192.168.200.249" and "192.168.1.3 - 192.168.1.14". The "Lease Time" column shows "1 d" for both. The right side of the interface has several status indicators and links for Site, Status, and Help.

Scope Name	Address Pool	Lease Time
Wireless Management davil-dhcp-mgmt	192.168.200.240 - 192.168.200.249 192.168.1.3 - 192.168.1.14	1 d 1 d

## Configurez un WLAN WPA2 Enterprise sur le WLC

# Configurez un WLAN WPA2 Enterprise

Par défaut, tous les WLAN qui viennent d'être créés sur le WLC utiliseront WPA2 avec AES (Advanced Encryption System).

- 802.1X est le protocole de gestion de clé par défaut utilisé pour communiquer avec le serveur RADIUS.
- Ensuite, créez un nouveau WLAN pour utiliser interface **vlan5**.

La configuration d'un nouveau WLAN sur le WLC comprend les étapes suivantes:

1. Créez un nouveau WLAN.
2. Configurez le nom WLAN et le SSID.
3. Activez le WLAN pour VLAN 5.
4. Vérifiez les valeurs par défaut AES et 802.1X.
5. Configurez la sécurité WLAN pour utiliser le serveur RADIUS.
6. Vérifiez que le nouveau WLAN est disponible.

# Configurer un WLAN WPA2 Enterprise (suite)

1. Créez un nouveau WLAN: cliquez sur l'onglet WLAN puis sur Aller pour créer un nouveau WLAN.

The screenshot shows the Cisco Wireless LAN Controller (WLC) configuration interface. The top navigation bar includes links for MONITOR, WLANs (which is highlighted with a red box), CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. Below the navigation is a search bar with 'Not secure | 192.168.200.254/screens/frameset.html'. The main content area is titled 'WLANS' and shows a table of existing WLANs. The table columns are: WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. One entry is visible: WLAN ID 1, Type WLAN, Profile Name Wireless\_Lab, WLAN SSID Wireless\_Lab, Admin Status Enabled, and Security Policies [WPA2][Auth(PSK)]. A red box highlights the 'Create New' button in the top right of the table header.

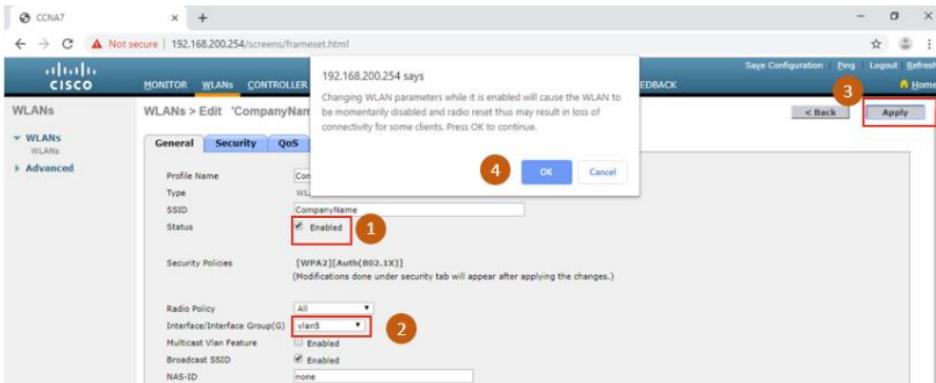
2. Configurez le nom et le SSID du WLAN: entrez le nom du profil et le SSID, choisissez un ID de 5, puis cliquez sur Appliquer pour créer le nouveau WLAN.

The screenshot shows the 'WLANs > New' configuration page. The left sidebar shows 'WLANS' selected. The main form has fields for Type (set to WLAN, highlighted with a red box), Profile Name (CompanyName), SSID (CompanyName), and ID (set to 5). A red box highlights the 'Apply' button in the bottom right corner of the form area.

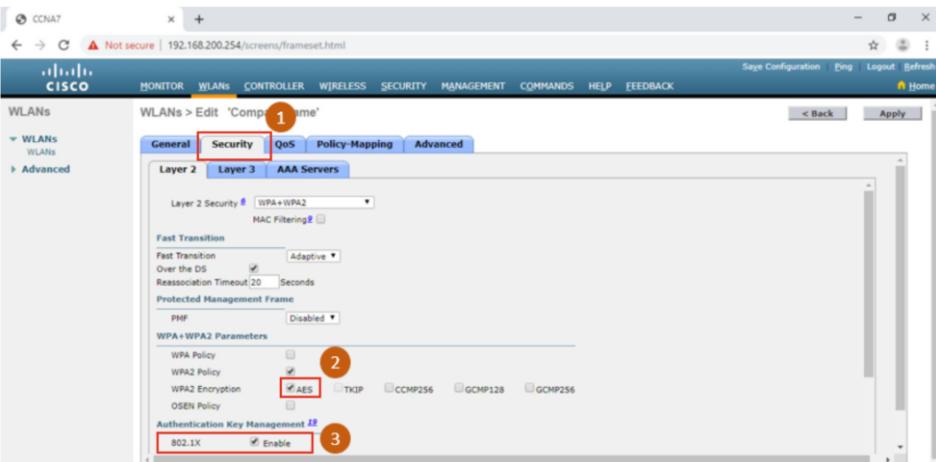
# Configurer un WLAN WPA2 Enterprise sur le WLC

## Configurer un WLAN WPA2 Enterprise (suite)

3. Activez le WLAN pour VLAN 5: Une fois le WLAN, change le statut en **Activé**, choisissez **vlan5** dans la liste déroulante Interface / Interface Group (G), puis cliquez sur **Appliquer** et sur **OK** pour accepter le message contextuel.



4. Vérifiez les valeurs par défaut AES et 802.1X: cliquez sur l'onglet **Sécurité** pour afficher la configuration de sécurité par défaut du nouveau WLAN.



# Configurer un WLAN WPA2 Enterprise (suite)

## 5. Configurez le serveur RADIUS:

Pour sélectionner le serveur RADIUS qui sera utilisé pour authentifier les utilisateurs WLAN, cliquez sur l'onglet **Serveur AAA** et dans la liste déroulante, sélectionnez le serveur RADIUS qui a été configuré sur le WLC précédemment, puis **appliquez** vos modifications.

The screenshot shows the 'AAA Servers' configuration page for a WLAN. The 'Authenticating Servers' section is highlighted with a red box. The first server entry, 'Server 1', has its IP and port fields filled with 'IP:172.16.1.254, Port:1812'. The 'Enabled' checkbox is checked. The 'Accounting Servers' and 'EAP Parameters' sections are also visible. The 'Apply' button at the top right is also highlighted with a red box.

## 6. Vérifiez que le nouveau WLAN est disponible:

Pour vérifier que le nouveau WLAN est répertorié et activé, cliquez sur le sous-menu **WLANs**.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Wireless_LAN	Wireless_LAN	Enabled	[WPA2][Auth(PSK)]
5	WLAN	CompanyName	CompanyName	Enabled	[WPA2][Auth(802.1X)]

# Packet Tracer - Configurez un WLAN WPA2 Enterprise sur le WLC

Dans cette activité, vous allez configurer un nouveau WLAN sur un contrôleur LAN sans fil (WLC), y compris l'interface VLAN qu'il utilisera. Vous allez configurer le WLAN pour utiliser un serveur RADIUS et WPA2-Enterprise pour authentifier les utilisateurs. Vous allez aussi configurer le WLC pour utiliser un serveur SNMP.

- Configurer une nouvelle interface VLAN sur un WLC.
- Configurer un nouvel WLAN sur un WLC.
- Configurer une nouvelle étendue sur le WLC interne de serveur DHCP.
- Configurer le WLC avec les paramètres SNMP.
- Configurez le WLC pour utiliser un serveur RADIUS pour authentifier les utilisateurs WLAN.
- Sécuriser un WLAN avec WPA2-Enterprise.
- Connecter les hôtes au nouvel WLC.
- **LAB13.3-WLAN**

# Packet Tracer - Configuration WLAN

Dans cette activité, vous allez configurer les deux le routeur domestique sans fil et le réseau basées sur WLC. Vous mettez en œuvre la sécurité WPA2-PSK et WPA2-Entreprise.

- Configurer un routeur domestique pour fournir une connectivité sans fil (Wi-Fi) aux différents appareils.
- Configurer la sécurité WPA2-PSK sur un routeur domestique.
- Configurer les interfaces sur un WLC.
- Configurez la sécurité WPA2-PSK sur un WLAN et connectez les hôtes au WLAN.
- Configurez la sécurité WPA2-Entreprise sur un WLAN et connectez les hôtes au WLAN.
- Vérifiez la connectivité.
- **LAB13.4-WLAN**

# 13.4 – Dépannage des problèmes de réseaux WLAN

# Dépannage des problèmes de réseaux WLAN

## Approches de Dépannage (suite)

Étape	Titre	Description
1	Identification du problème	La première étape de la procédure de dépannage consiste à identifier le problème. Si des outils peuvent être utilisés à cette étape, une conversation avec l'utilisateur est souvent très utile.
2	Élaboration d'une théorie des causes probables	Après avoir discuté avec l'utilisateur et identifié le problème, vous pouvez établir une théorie des causes probables. Cette étape fait généralement naître plusieurs causes probables.
3	Test de la théorie en vue de déterminer la cause	En fonction des causes probables, testez vos théories afin de dégager la véritable cause du problème. Un technicien peut alors appliquer une rapide procédure et voir si cela permet de résoudre le problème. Sinon, vous devrez peut-être effectuer des recherches complémentaires en vue de déterminer la cause exacte.
4	Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution	Après avoir déterminé la cause exacte du problème, établissez un plan d'action en vue de le résoudre en implantant la solution.
5	Vérification du fonctionnement de l'ensemble du système et implémentation des mesures préventives	Après avoir résolu le problème, vous devez vérifier le fonctionnement de l'ensemble du système et s'il y a lieu, implémenter des mesures préventives.
6	Documentation des résultats des recherches et des actions entreprises	Au cours de la dernière étape du processus de dépannage, vous devez documenter les résultats de vos recherches ainsi que les actions entreprises. Cette étape est très importante pour référence ultérieure.

# Le Client Sans Fil Ne Se Connecte Pas (suite)

S'il n'y a pas de connectivité, vérifiez les points suivants:

- Confirmez la configuration réseau sur le PC à l'aide de la commande **ipconfig**
- Confirmez que l'appareil peut se connecter au réseau câblé. Envoyez une requête ping à une adresse IP connue.
- Si nécessaire, rechargez les pilotes selon les besoins du client ou essayez une autre carte réseau sans fil.
- Si la carte réseau sans fil du client fonctionne, vérifiez le mode de sécurité et les paramètres de cryptage sur le client.

Si le PC est opérationnel mais que la connexion sans fil fonctionne mal, vérifiez les points suivants:

- Le PC est-il en hors de BSA?
- Vérifiez les paramètres de canal sur le client sans fil.
- Vérifiez les interférences avec la bande 2,4 GHz.

## Le Client Sans Fil Ne Se Connecte Pas (suite)

Ensuite, assurez-vous que tous les périphériques sont bien en place.

- Considérez un problème éventuel de sécurité physique.
- Tous les périphériques sont-ils alimentés et sont-ils sous tension?

Enfin, inspectez les liaisons entre les périphériques câblés à la recherche de connecteurs défectueux ou de câbles endommagés ou manquants.

- Si l'installation physique est en place, vérifiez le réseau local câblé en envoyant une requête ping aux périphériques, y compris l'AP.
- Si la connectivité est encore insuffisante à ce moment, peut-être il existe un problème avec l'AP ou sa configuration.
- Lorsque le PC de l'utilisateur est éliminé comme source du problème et que la situation physique des périphériques est confirmé, commencez à enquêter sur les performances du point d'accès.
- Vérifiez la situation d'alimentation de l'AP.

# Dépannage lorsque le réseau est lent

Pour optimiser et augmenter la bande passante des routeurs et des points d'accès bi-bande 802.11 :

- **Mettez à niveau vos clients sans fil** - les anciens appareils 802.11b, 802.11g et même 802.11n peuvent ralentir l'ensemble du WLAN. Pour de meilleures performances, tous les appareils sans fil doivent prendre en charge la même norme acceptable la plus élevée.
- **Répartir le trafic** - Le moyen le plus simple d'améliorer les performances du sans fil est de répartir le trafic sans fil entre la bande 802.11n 2,4 GHz et la bande 5 GHz. Par conséquent, 802.11n (ou mieux) peut utiliser les deux bandes comme deux réseaux sans fil distincts pour aider à gérer le trafic.

Plusieurs raisons justifient l'utilisation de méthode "split-the-traffic" :

- La bande 2,4 GHz peut convenir au trafic Internet de base qui n'est pas sensible au temps.
- La bande passante peut toujours être partagée avec d'autres WLAN à proximité.
- La bande 5 GHz est beaucoup moins encombrée que la bande 2,4 GHz; idéal pour le streaming multimédia.
- La bande 5 GHz a plus de canaux; par conséquent, le canal choisi est probablement sans interférence.

## Dépannage lorsque le réseau est lent (suite)

Par défaut, les routeurs double bande et les points d'accès utilisent le même nom de réseau sur la bande 2,4 GHz et la bande 5 GHz.

- Il peut être utile de segmenter le trafic.
- Le moyen le plus simple de segmenter le trafic consiste à renommer l'un des réseaux sans fil.

Pour améliorer la gamme d'un réseau sans fil, assurez-vous que le routeur sans fil ou l'emplacement du point d'accès ne sont pas obstrués, tels que des meubles, des luminaires et des périphériques électroménagers de grande taille.

- Ceux-ci bloquent le signal, ce qui raccourcit la gamme du WLAN.
- Si cela ne résout toujours pas le problème, un prolongateur de portée Wi-Fi ou le déploiement de la technologie sans fil CPL (Powerline wireless technology) peut être utilisé.

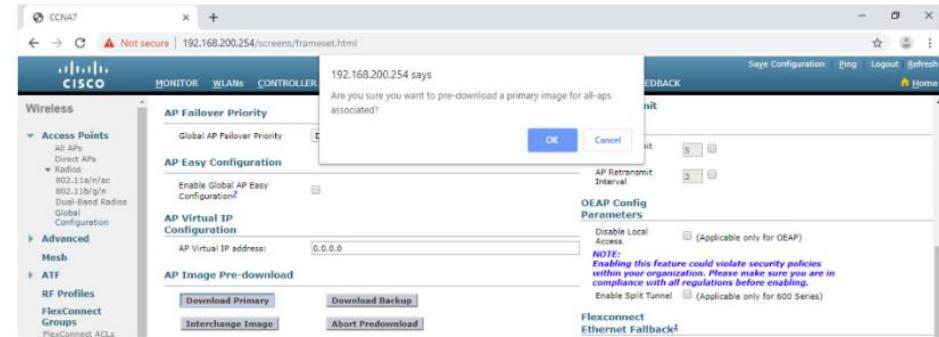
# Dépannage des problèmes de réseaux WLAN

## Mise à jour du firmware

La plupart des routeurs et points d'accès sans fil proposent un firmware (micrologiciel) mise à jour.

Sur un WLC, il y aura très probablement la possibilité de mettre à niveau le micrologiciel sur tous les points d'accès contrôlés par le WLC.

- Dans la figure suivante, l'administrateur réseau télécharge l'image du micrologiciel qui sera utilisée pour mettre à niveau tous les points d'accès.
- Sur un contrôleur sans fil Cisco 3504, cliquez sur **SANS FIL > Points d'accès > Configuration globale**, puis faites défiler vers le bas de la page pour la section de pré-téléchargement de l'image AP.



# 13.5 – Module pratique et résumé

# Qu'est-ce que j'ai appris dans ce module?

- Les travailleurs distants, les petites filiales et les réseaux domestiques utilisent souvent un routeur sans fil, qui comprend généralement un commutateur pour les clients câblés, un port pour une connexion Internet (parfois appelé «WAN») et des composants sans fil pour l'accès client sans fil.
- La plupart des routeurs sans fil sont préconfigurés pour être connectés au réseau et fournir des services. Le routeur sans fil utilise le DHCP pour fournir automatiquement des informations d'adressage aux périphériques connectés.
- Votre première priorité devrait être de changer le nom d'utilisateur et le mot de passe de votre routeur sans fil.
- Vous pouvez ajouter des points d'accès sans fil si vous souhaitez étendre la gamme au-delà de 45 mètres à l'intérieur et de 90 mètres à l'extérieur.
- Le routeur utilisera un processus appelé traduction d'adresses réseau (NAT) pour convertir les adresses IPv4 privées en adresses IPv4 routables sur Internet.
- En configurant la QoS, vous pouvez garantir que certains types de trafic, tels que la voix et la vidéo, ont la priorité sur le trafic qui n'est pas aussi sensible au temps, comme les e-mails et la navigation Web.
- Les AP Lightweight (LAPs) utilisent le Lightweight Access Point Protocol (LWAPP) pour communiquer avec un contrôleur WLAN (WLC).

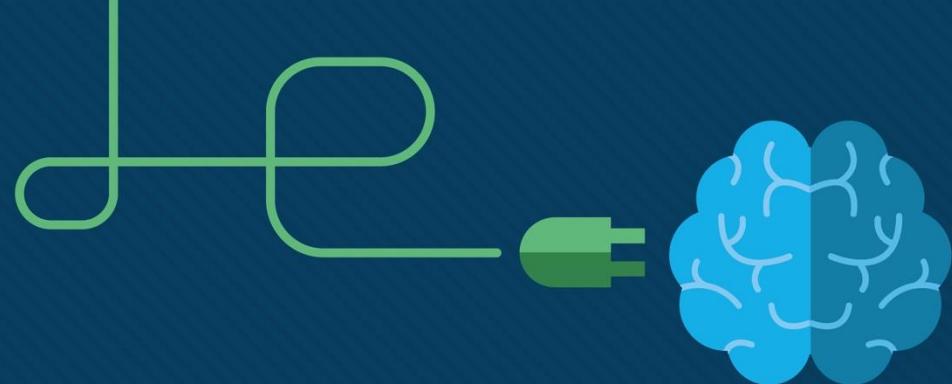
## Qu'est-ce que j'ai appris dans ce module? (Cont.)

- La Configuration de contrôleur LAN sans fil (WLC) est similaire à la Configuration de routeur sans fil, sauf qu'un WLC contrôle les points d'accès et fournit plus de services et de capacités de gestion. Utilisez l'interface WLC pour afficher une image globale des informations et des performances du système AP, pour accéder aux paramètres avancés et pour configurer un WLAN.
- SNMP est utilisé pour surveiller le réseau. le WLC transfère tous les messages de journal SNMP, appelés interruptions au serveur SNMP.
- Pour l'authentification des utilisateurs WLAN, un serveur RADIUS est utilisé pour les services d'authentification, d'autorisation et de comptabilité (AAA). L'accès des utilisateurs individuels peut être suivi et audité.
- Utilisez l'interface WLC pour configurer les informations du serveur SNMP et du serveur RADIUS, les interfaces VLAN, la portée DHCP et un WPA2-Enterprise WLAN.
- Les six étapes de la procédure de dépannage.
- Pendant le dépannage d'un WLAN, un processus d'élimination est recommandé. Les problèmes courants sont: l'absence de la connectivité et une connexion sans fil de faible performance lorsque le PC est en opération.
- Pour optimiser et augmenter la bande passante des routeurs et des points d'accès bi-bande 802.11, mettez à niveau vos clients sans fil ou divisez le trafic.
- La plupart des routeurs et points d'accès sans fil proposent un firmware mise à jour. Les différentes versions du micrologiciel peuvent contenir la résolution de problèmes courants signalés par des clients ou des failles de sécurité. Vous devriez vérifier périodiquement le routeur ou l'AP pour le firmware mise à jour.

# Nouveaux termes et commandes

- Traduction d'adresses de réseau (NAT)
- Réseau sans fil maillé (WMN)
- Transfert de port
- Déclenchement de ports





# Module 14 : Adressage IPv6



# Objectifs du Module

**Titre du module :** Adressage IPv6

**Objectif du module:** Mettre en œuvre un système d'adressage IPv6.

Titre du rubrique	Objectif du rubrique
Problèmes liés au protocole IPv4	Expliquer la nécessité de l'adressage IPv6.
Représentation de l'adresse IPv6	Expliquer comment les adresses IPv6 sont représentées.
Types d'adresses IPv6	Comparer les types d'adresses réseau IPv6.
Configuration statique GUA et LLA	Expliquer comment configurer des adresses de réseau IPv6 statiques de type monodiffusion globale et lien-local.
Adressage dynamique pour les GUA IPv6	Configurer les adresses de monodiffusion globale d'une façon dynamique.

# Objectifs du module (suite)

**Titre du module:** Adressage IPv6

**Objectif du module:** Mettre en œuvre un système d'adressage IPv6.

Titre du rubrique	Objectif du rubrique
Adressage dynamique pour les LLA IPv6	Configurez dynamiquement les adresses lien-local.
Adresses IPv6 de multidiffusion	Identifier des adresses IPv6
Sous-réseau d'un réseau IPv6	Mettre en œuvre un schéma d'adressage IPv6 divisé en sous-réseaux

# 14.1 Problèmes IPv4

## Nécessité pour IPv6

- IPv4 manque d'adresses. IPv6 est le successeur d'IPv4. Espace d'adressage de 128 bits plus grand
- Le développement d'IPv6 a également inclus des correctifs pour les limitations IPv4 et d'autres améliorations.
- Avec l'utilisation croissante d'Internet, un espace limité d'adresses IPv4, des problèmes liés à la fonction NAT et l'Internet of Everything, le moment est venu d'entamer la transition vers IPv6.



# Coexistence de l'IPv4 et de l'IPv6

IPv4 et IPv6 coexisteront dans un proche avenir et la transition prendra plusieurs années.

L'IETF a créé divers protocoles et outils pour aider les administrateurs réseau à migrer leurs réseaux vers l'IPv6. Les techniques de migration peuvent être classées en trois catégories:

- **Double pile** -les périphériques double pile exécutent les piles de protocoles IPv4 et IPv6 simultanément.
- **Tunneling** - méthode qui consiste à transporter un paquet IPv6 sur un réseau IPv4. Le paquet IPv6 est encapsulé dans un paquet IPv4.
- **Traduction** - La traduction d'adresse réseau 64 (NAT64) permet aux appareils compatibles IPv6 de communiquer avec les appareils compatibles IPv4 en utilisant une technique de traduction similaire à la NAT pour IPv4.

**Remarque:** Le tunneling et la traduction sont destinés à la transition vers IPv6 natif et ne doivent être utilisés qu'en cas de besoin. L'objectif doit être de communiquer de manière native via le protocole IPv6 depuis la source jusqu'à la destination.

# 14.2 Représentation de l'adresse IPv6

# Représentation d'adresses IPv6

## Formats d'adressage IPv6

- Les adresses IPv6 ont une longueur de 128 bits et sont écrites en hexadécimal.
- Les adresses IPv6 ne sont pas sensibles à la casse et peuvent être notées en minuscules ou en majuscules.
- le format privilégié pour noter une adresse IPv6 est x:x:x:x:x:x:x:x, où chaque «x» est constitué de quatre valeurs hexadécimales.
- Pour les adresses IPv6, « hextet » est le terme officieux qui désigne un segment de 16 bits ou de quatre valeurs hexadécimales.
- Cela présente des exemples d'adresses IPv6 au format privilégié.

2001:0db8:0000:1111:0000:0000:0000:0200

2001:0db8:0000:00a3:abcd:0000:0000:1234

# Règle 1 - Omettre le zéro de début (Leading Zero)

La première règle pour réduire la notation des adresses IPv6 consiste à omettre les zéros (0) du début.

## Exemples :

- 01ab est équivalent à 1AB
- 09f0 peut être représenté comme 9f0
- 0a00 peut être représenté comme a00
- 00ab est équivalent à ab

**Remarque:** Cette règle s'applique uniquement aux 0 de tête et NON aux 0 de queue, sinon l'adresse serait ambiguë.

Type	Format
Souhaitée	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Pas de zéros du début	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200

## Règle 2 -Double Deux Points

Une suite de double deux-points (::) peut remplacer toute chaîne unique et continue d'un ou plusieurs segments de 16 bits (hextets) comprenant uniquement des zéros.

### Exemple :

- 2001:db8:cafe:1:0:0:0:1 (les 0 principaux sont omis) pourrait être représenté par 2001:db8:cafe:1::1

**Remarque:** Le double point (::) ne peut être utilisé qu'une seule fois dans une adresse, sinon il y aurait plusieurs adresses possibles.

Type	Format
Souhaitée	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Compressée	2001:db8:0:1111::200

# 14.3 Types d'adresses IPv6

# Monodiffusion, Multidiffusion, Anycast

Il existe trois grandes catégories d'adresses IPv6 :

- **Monodiffusion** - La monodiffusion identifie de manière unique une interface sur un appareil compatible IPv6.
- **Multidiffusion** - La multidiffusion est utilisée pour envoyer un seul paquet IPv6 vers plusieurs destinations.
- **Anycast** - Il s'agit de toute adresse unicast IPv6 qui peut être attribuée à plusieurs appareils. Un paquet envoyé à une adresse anycast est acheminé vers le périphérique le plus proche ayant cette adresse.

**Remarque:** Contrairement à IPv4, IPv6 n'a pas d'adresse de diffusion. Cependant, il existe une adresse de multidiffusion destinée à tous les nœuds IPv6 et qui offre globalement les mêmes résultats.

# Longueur du préfixe IPv6

La longueur du préfixe IPv6 est utilisée pour indiquer la partie réseau de l'adresse IPv6:

La longueur de préfixe peut être comprise entre 0 et 128. La longueur du préfixe IPv6 recommandée pour les réseaux locaux et la plupart des autres types de réseaux est /64.

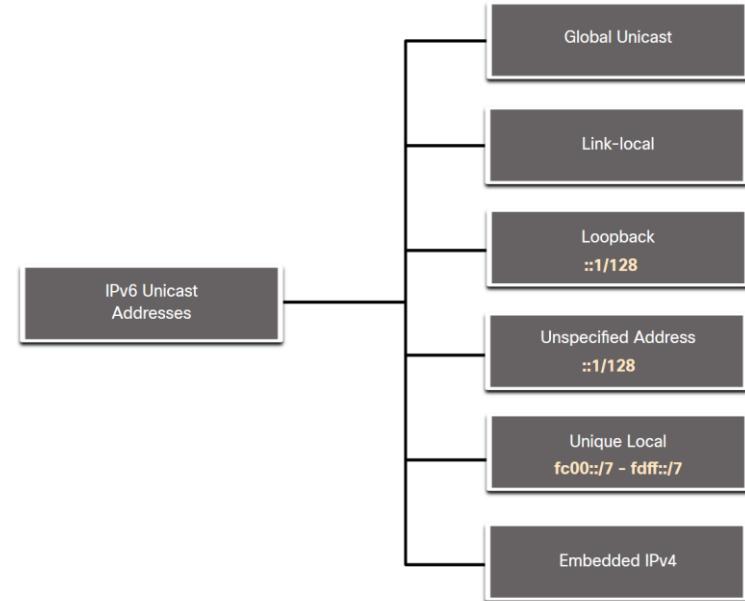


**Remarque:** Il est fortement recommandé d'utiliser un ID d'interface 64 bits pour la plupart des réseaux. En effet, la configuration automatique d'adresse sans état (SLAAC) utilise 64 bits pour l'ID d'interface. Il facilite également la création et la gestion des sous-réseaux.

# Types d'adresses IPv6 Unicast

Contrairement aux périphériques IPv4 qui n'ont qu'une seule adresse, les adresses IPv6 ont généralement deux adresses monodiffusion :

- **Global Unicast Address (GUA)** –Cette adresse est similaire à une adresse IPv4 publique. Ces adresses sont uniques au monde et routables sur Internet.
- **Adresse locale de liaison (LLA)**- Requise pour chaque appareil compatible IPv6 et utilisée pour communiquer avec d'autres appareils sur la même liaison locale. Les LLA ne sont pas routables et se limitent à une seule liaison.



## Une Remarque à propos de l'adresse locale unique

Les adresses locales uniques IPv6 (plage fc00::/7 à fdff::/7) présentent une certaine similitude avec les adresses privées RFC 1918 pour IPv4, mais il existe des différences significatives :

- Des adresses locales uniques sont utilisées pour l'adressage local au sein d'un site ou entre un nombre limité de sites.
- Les adresses locales uniques peuvent être utilisées pour les périphériques qui n'auront jamais besoin d'être accessibles sur un autre réseau.
- Les adresses locales uniques ne sont pas routées globalement ou traduites en adresse IPv6 globale.

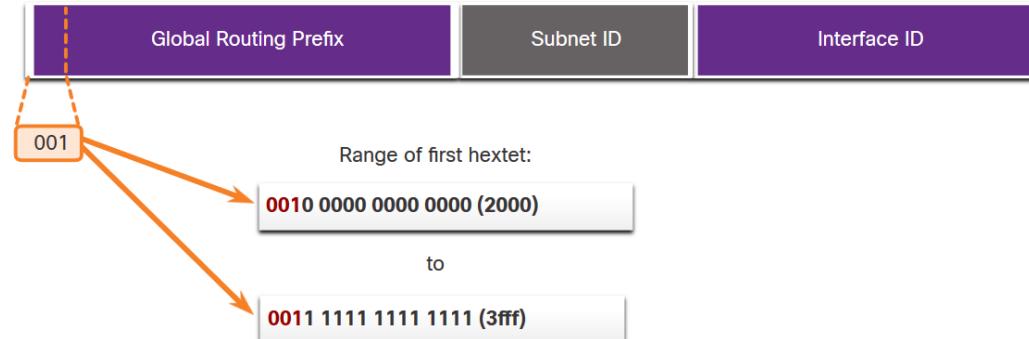
**Remarque:** de nombreux sites utilisent la nature privée des adresses RFC 1918 pour tenter de sécuriser ou de cacher leur réseau des risques potentiels de sécurité. Cela n'a jamais été l'utilisation prévue des ULA.

# Types d'adresses IPv6

## IPv6 GUA

Les adresses de diffusion globale (GUA) IPv6 sont uniques au monde et routables (Internet IPv6).

- Actuellement, seules des adresses de monodiffusion globale dont les premiers bits sont 001 ou 2000::/3 sont attribuées
- Les GUA actuellement disponibles commencent par une décimale 2 ou 3 (Ceci représente seulement 1/8ème de l'espace d'adressage IPv6 total disponible).



# IPv6 Structure GUA

### Préfixe de routage global:

- Le préfixe de routage global est le préfixe ou la partie réseau de l'adresse attribué(e) par le fournisseur (par exemple un ISP) à un client ou à un site. Le préfixe de routage global varie en fonction des stratégies du fournisseur de services Internet.

### ID de sous-réseau

- Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface. L'ID de sous-réseau est utilisé par une entreprise pour identifier les sous-réseaux au sein de son site.

### ID d'interface

- L'ID d'interface IPv6 est l'équivalent de la partie hôte d'une adresse IPv4. Dans la plupart des cas, il est fortement recommandé d'utiliser des sous-réseaux /64, qui crée un ID d'interface de 64 bits.

Remarque: IPv6 permet d'attribuer des adresses d'hôte "tout 0" et "tout 1" à un appareil. L'adresse contenant uniquement des 0 peut également être utilisée, mais elle est réservée comme adresse anycast de routeur de sous-réseau, et elle ne doit être attribuée qu'aux routeurs.

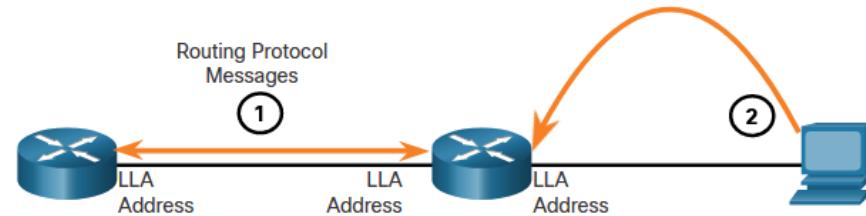


# Types d'adresses IPv6

## IPv6 LLA

Une adresse link-local IPv6 (LLA) permet à un appareil de communiquer avec d'autres appareils IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau).

- Les paquets avec un LLA source ou de destination ne peuvent pas être routés.
- Chaque interface réseau compatible IPv6 doit avoir un LLA.
- Si un LLA n'est pas configuré manuellement sur une interface, le dispositif en créera un automatiquement.
- Les IPv6 LLAs sont dans la gamme fe80::/10.



1. Routers use the LLA of neighbor routers to send routing updates.
2. Hosts use the LLA of a local router as the default-gateway.

# 14.4 Configuration statique GUA et LLA

# Configuration statique GUA sur un routeur

La plupart des commandes de configuration et de vérification IPv6 de Cisco IOS sont semblables à celles utilisées pour l'IPv4. Dans de nombreux cas, la seule différence est l'utilisation d'**ipv6** au lieu d'**ip** dans les commandes.

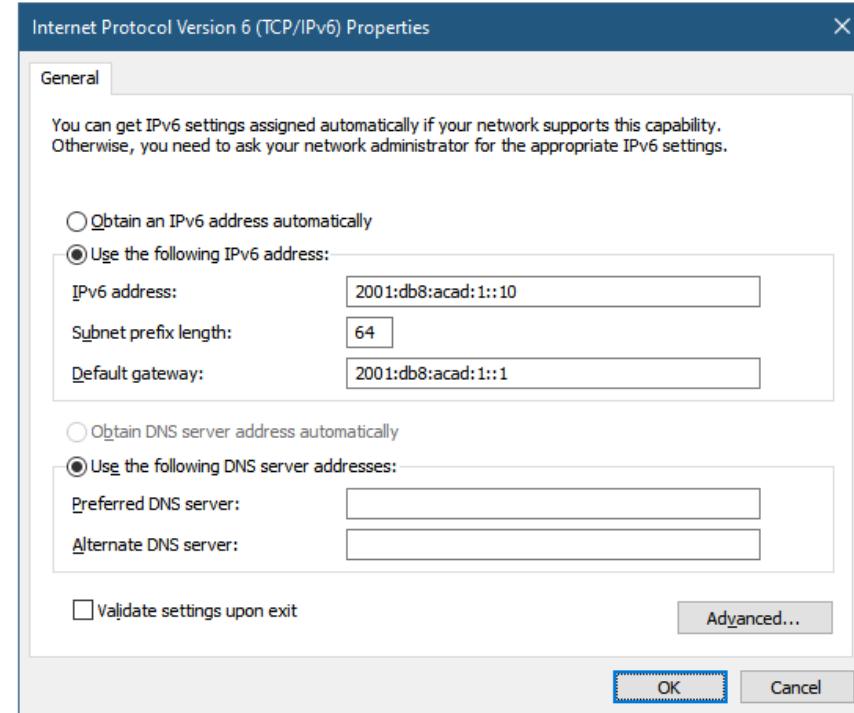
- La commande pour configurer une GUA IPv6 sur une interface est : **ipv6 adresse ipv6-adresse/prefix-length**.
- L'exemple montre les commandes pour configurer une GUA sur l'interface G0/0/0 sur R1 :

```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

# Configuration statique GUA sur un hôte Windows

- La configuration manuelle de l'adresse IPv6 sur un hôte est similaire à celle d'une adresse IPv4.
- Le GUA ou LLA de l'interface du routeur peut être utilisé comme passerelle par défaut. La meilleure pratique consiste à utiliser le LLA.

**Remarque:** lorsque le DHCPv6 ou le SLAAC est utilisé, le LLA du routeur sera automatiquement spécifié comme adresse de passerelle par défaut.



# Configuration statique d'une adresse monodiffusion Lien-Local

La configuration manuelle de l'adresse link-local permet de créer une adresse qui est reconnaissable et plus facile à mémoriser.

- Les LLA peuvent être configurés manuellement à l'aide de la commande **ipv6 address *ipv6-link-local-address* link-local** .
- L'exemple montre les commandes pour configurer un LLA sur l'interface G0/0/0 sur R1

```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

**Remarque:** la même LLA peut être configurée sur chaque lien, à condition qu'elle soit unique sur ce lien. La pratique courante consiste à créer un LLA différent sur chaque interface du routeur pour faciliter l'identification du routeur et de l'interface spécifique.

# 14.5 Adressage dynamique pour les IPv6 GUA

# Adressage dynamique pour les IPv6 GUA Messages RS et RA

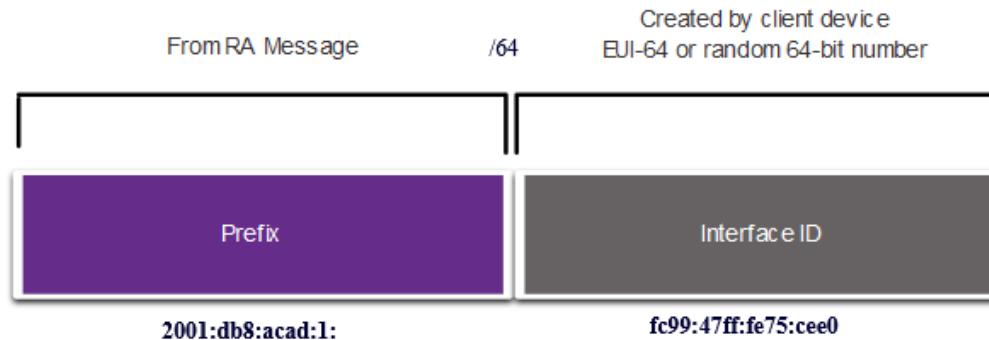
Les périphériques obtiennent des adresses GUA dynamiquement via les messages ICMPv6 (Internet Control Message Protocol version 6).

- Les messages de sollicitation de routeur (RS) sont envoyés par les périphériques hôtes pour découvrir les routeurs IPv6
- Les messages de publicité de routeur (RA) sont envoyés par les routeurs pour informer les hôtes sur la façon d'obtenir une GUA IPv6 et fournir des informations réseau utiles telles que :
  - Préfixe réseau et longueur du préfixe
  - L'adresse de la passerelle par défaut
  - Adresses DNS et nom de domaine
- L'RA peut fournir trois méthodes pour configurer une IPv6 GUA :
  - SLAAC
  - SLAAC avec serveur DHCPv6 apatride
  - DHCPv6 avec état (pas de SLAAC)



## Méthode 1: SLAAC

- SLAAC permet à un périphérique de configurer une GUA sans les services de DHCPv6.
- Les périphériques obtiennent les informations nécessaires pour configurer une GUA à partir des messages RA ICMPv6 du routeur local.
- Le préfixe est fourni par l'RA et le périphérique utilise soit la méthode EUI-64, soit la méthode de génération aléatoire pour créer un ID d'interface.

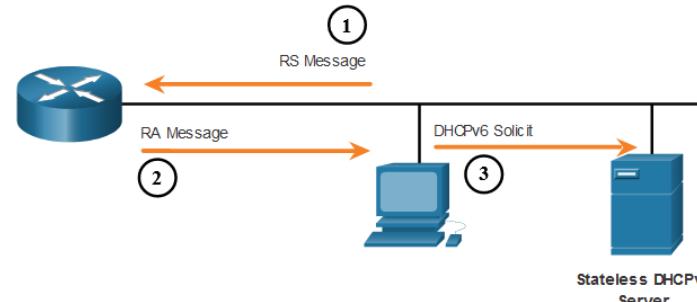


## Méthode 2: SLAAC et DHCP sans état

Un RA peut demander à un périphérique d'utiliser à la fois SLAAC et DHCPv6 sans état.

Le message RA suggère que les appareils utilisent les éléments suivants :

- SLAAC pour créer sa propre IPv6 GUA
- l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut.
- un serveur DHCPv6 sans état pour obtenir d'autres informations telles que l'adresse d'un serveur DNS et un nom de domaine.



# Adressage dynamique pour les IPv6 GUA

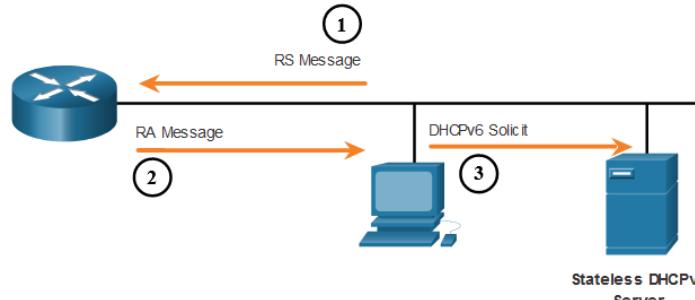
## Méthode 3: DHCPv6 avec état

Un RA peut demander à un périphérique d'utiliser uniquement DHCPv6 avec état.

DHCPv6 avec état est similaire à DHCP pour IPv4. Un périphérique peut recevoir automatiquement une GUA, une longueur de préfixe et les adresses des serveurs DNS à partir d'un serveur DHCPv6 avec état.

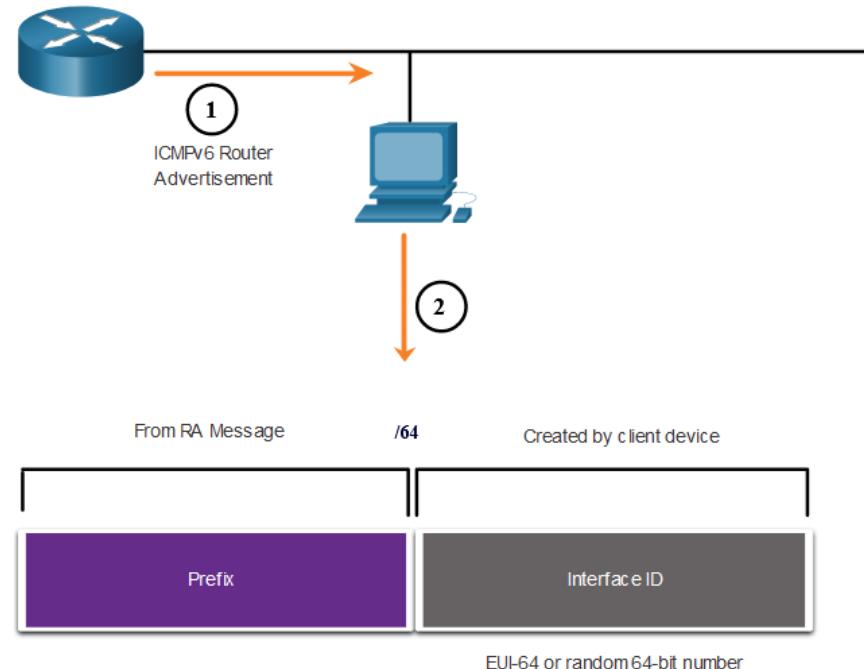
Le message RA suggère que les appareils utilisent les éléments suivants :

- l'adresse link-local du routeur, l'adresse IPv6 source du message d'annonce de routeur comme adresse de la passerelle par défaut.
- un serveur DHCPv6 avec état pour obtenir une adresse de diffusion globale, l'adresse d'un serveur DNS, un nom de domaine et toutes les autres informations.



# Processus EUI-64 contre génération aléatoire

- Lorsque le message d'annonce de routeur est la SLAAC seule ou la SLAAC avec DHCPv6 sans état, le client doit générer lui-même son ID d'interface.
- L'interface ID peut utiliser la méthode EUI-64 ou un nombre à 64 bits généré aléatoirement.



# Adressage dynamique pour les IPv6 GUA Processus EUI-64

L'IEEE a défini l'identifiant unique étendu (EUI), ou format EUI-64 modifié.

- Une valeur 16 bits de fffe (en hexadécimal) est insérée au milieu de l'adresse MAC Ethernet 48 bits du client.
- Le 7<sup>e</sup> bit de l'adresse MAC du client est inversé du binaire 0 à 1.
- Exemple :

MAC 48 bits	fc:99:47:75:ce:e0
ID d'interface EUI-64	fe:99:47: <b>ff:fe</b> :75:ce:e0

# Identifiants d'interface générés de manière aléatoire

Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface généré aléatoirement plutôt que l'adresse MAC et le processus EUI-64.

À partir de la version Windows Vista, Windows utilise un ID d'interface généré aléatoirement au lieu d'un ID créé avec le processus EUI-64.

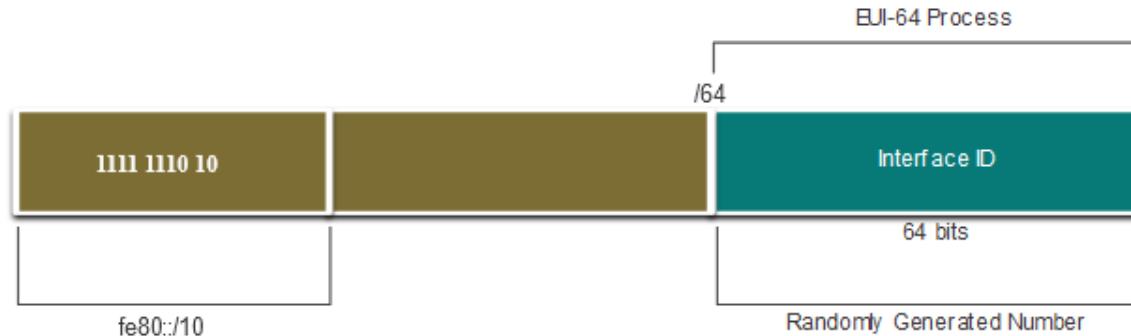
```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
  Suffixe DNS propre à la connexion . . .
  IPv6 Address . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
  Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
  Default Gateway . . . . . . . . . : fe80::1
C:\ >
```

**Remarque:** pour s'assurer que les adresses de monodiffusion IPv6 sont uniques, le client peut utiliser le processus de détection d'adresse dupliquée (DAD). Le principe est similaire à une requête ARP pour sa propre adresse. En l'absence de réponse, l'adresse est unique.

# 14.6 Adressage dynamique pour les LLA IPv6

# Adressage dynamique pour les IPv6 LLA LLA dynamiques

- Toutes les interfaces IPv6 doivent avoir un IPv6 LLA.
- Comme les IPv6 GUA, les LLA peuvent être configurés dynamiquement.
- La figure montre que l'adresse link-local est créée dynamiquement à partir du préfixe FE80::/10 et de l'ID d'interface à l'aide de la méthode EUI-64 ou d'un no



# Adressage dynamique pour les IPv6 LLA LLA dynamiques sur Windows

Les systèmes d'exploitation, tels que Windows, utiliseront généralement la même méthode pour une GUA créée par SLAAC et une LLA attribuée dynamiquement.

## ID d'interface généré par la méthode EUI-64

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . : fe80::1
C:\ >
```

## ID d'interface généré aléatoirement sur 64 bits :

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . : fe80::1
C:\ >
```

# Adressage dynamique pour les IPv6 LLA LLAs dynamiques sur les routeurs Cisco

Les routeurs Cisco créent automatiquement une adresse link-local IPv6 dès qu'une adresse de diffusion globale est attribuée à l'interface. Par défaut, les routeurs Cisco IOS utilisent la méthode EUI-64 pour générer l'ID d'interface de toutes les adresses link-local sur des interfaces IPv6.

Voici un exemple d'un LLA configuré dynamiquement sur l'interface G0/0/0 de R1:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

# Vérifier la configuration de l'adresse IPv6

Les routeurs Cisco créent automatiquement une adresse link-local IPv6 dès qu'une adresse de diffusion globale est attribuée à l'interface. Par défaut, les routeurs Cisco IOS utilisent la méthode EUI-64 pour générer l'ID d'interface de toutes les adresses link-local sur des interfaces IPv6.

Voici un exemple d'un LLA configuré dynamiquement sur l'interface G0/0/0 de R1 :

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)

R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

# Packet Tracer — Configurer l'adressage IPv6

Dans le cadre de ce Packet Tracer, vous ferez ce qui suit :

- Configurer l'adressage IPv6 sur le routeur
- Configurer l'adressage IPv6 sur les serveurs
- Configurer l'adressage IPv6 sur les clients
- Tester et vérifier la connectivité réseau
- **LAB14.1-IPV6**

# 14.7 Adresses de multidiffusion IPv6

# Adresses de multidiffusion IPv6 attribuées

Les adresses de multidiffusion IPv6 ont le préfixe FF00::/8. Il existe deux types d'adresses de multidiffusion IPv6 :

- Les adresses de multidiffusion bien connues
- Adresses de multidiffusion de nœud sollicité

**Remarque:** les adresses de multidiffusion ne peuvent être que des adresses de destination et non des adresses source.

# Adresses de multidiffusion IPv6 bien connues

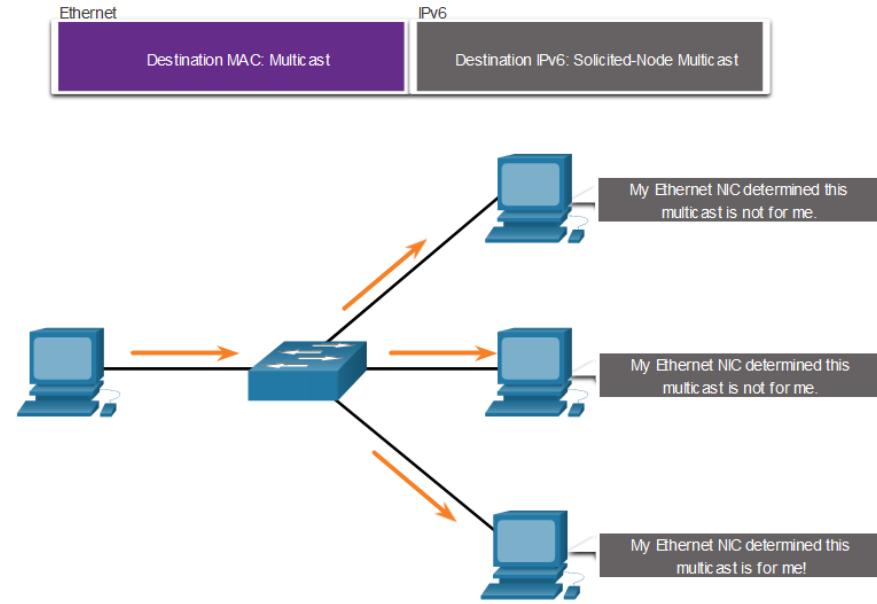
Des adresses de multidiffusion IPv6 bien connues sont attribuées et sont réservées à des groupes d'appareils prédéfinis.

Il existe deux groupes communs de multidiffusion assignés par IPv6 :

- **ff02::1 All-nodes multicast group** - Il s'agit d'un groupe de multidiffusion que tous les appareils compatibles IPv6 rejoignent. Un paquet envoyé à ce groupe est reçu et traité par toutes les interfaces IPv6 situées sur la liaison ou le réseau.
- **ff02::2 All-routers multicast group** - Il s'agit d'un groupe multicast que tous les routeurs IPv6 rejoignent. Un routeur devient un membre de ce groupe lorsqu'il est activé en tant que routeur IPv6 avec la commande de configuration globale **ipv6 unicast-routing** .

# Adresses de multidiffusion IPv6 Noeud sollicité IPv6 Multicast

- Une adresse de multidiffusion de noeud sollicité est comparable à une adresse de multidiffusion à tous les nœuds.
- Une adresse de multidiffusion à noeud sollicité est mise en correspondance avec une adresse de multidiffusion Ethernet spéciale.
- Cela permet à la carte réseau Ethernet de filtrer la trame en examinant l'adresse MAC de destination sans l'envoyer au processus IPv6 pour voir si le périphérique est la cible prévue du paquet IPV6.

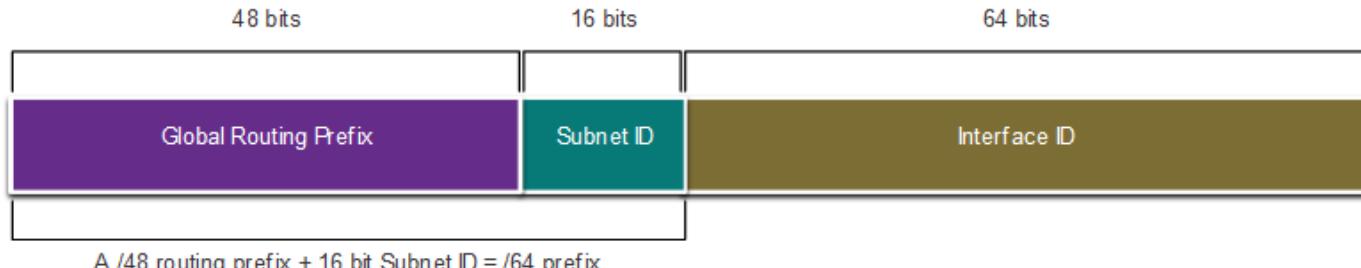


# 14.8 Sous-réseautage d'un réseau IPv6

# Sous-réseautage utilisant l'ID de sous-réseau

IPv6 a été conçu en pensant au sous-réseau.

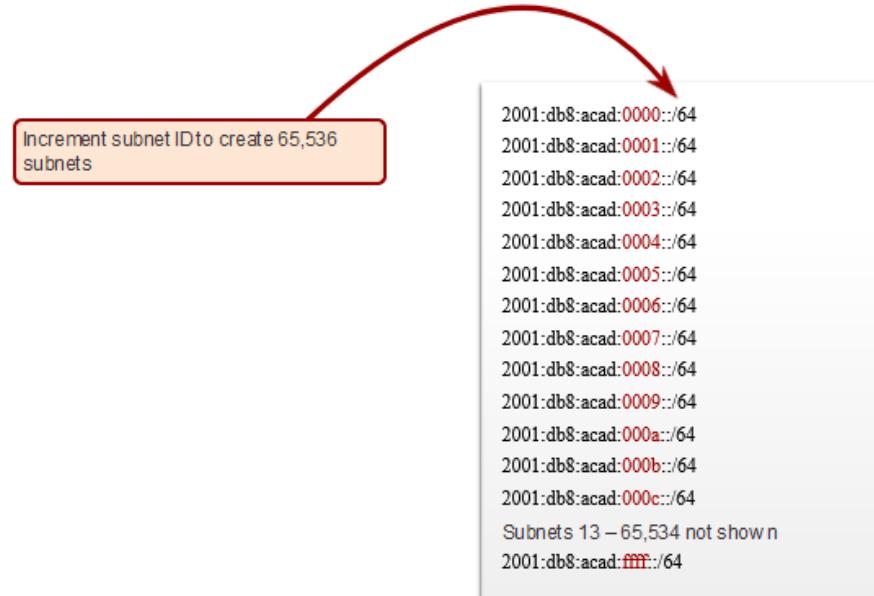
- Un champ d'ID de sous-réseau distinct dans la GUA IPv6 est utilisé pour créer des sous-réseaux.
- Le champ ID de sous-réseau est la zone située entre le préfixe de routage global et l'ID d'interface.



# Exemple de sous-réseautage IPv6

Étant donné le préfixe de routage global 2001:db8:acad::/48 avec un ID de sous-réseau de 16 bits.

- Permet 65 536 /64 sous-réseaux
- Le préfixe de routage global est le même pour tous les sous-réseaux.
- Seul l'hexagone d'identification du sous-réseau est incrémenté en hexadécimal pour chaque sous-réseau.

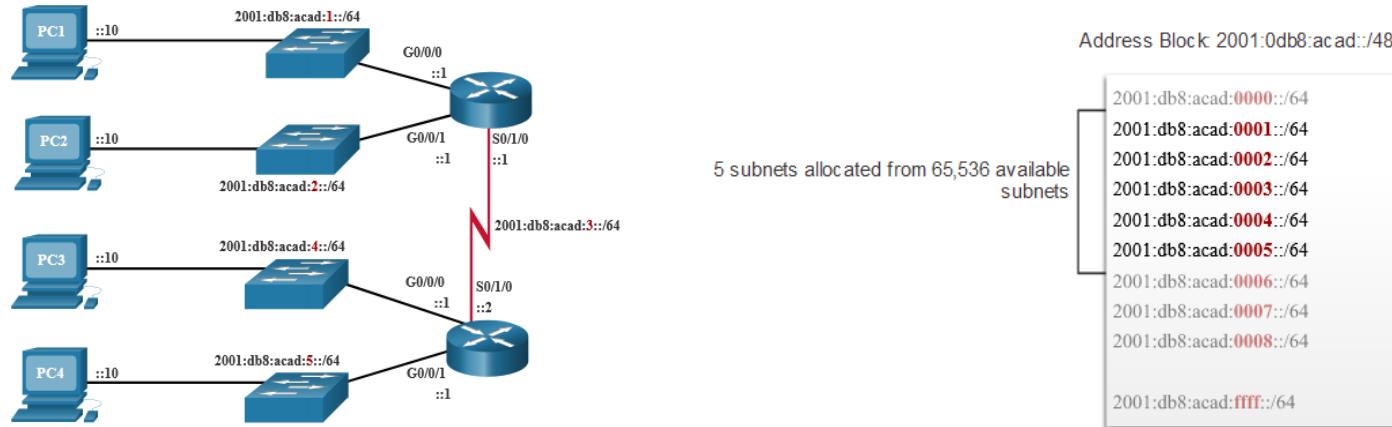


# Sous-réseautage un réseau IPv6

## Allocation de sous-réseau IPv6

La topologie de l'exemple nécessite cinq sous-réseaux, un pour chaque réseau local ainsi que pour la liaison série entre R1 et R2.

Les cinq sous-réseaux IPv6 ont été alloués, avec les champs d'ID de sous-réseau 0001 à 0005. Chaque sous-réseau /64 propose plus d'adresses qu'il ne sera jamais nécessaire.



# Routeur configuré avec des sous-réseaux IPv6

Comme pour la configuration IPv4, l'exemple indique que chacune des interfaces du routeur a été configurée pour utiliser un sous-réseau IPv6 différent.

```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

# Packet Tracer - Mise en œuvre d'un système d'adressage IPv6 divisé en sous-réseaux

Dans le cadre de ce Packet Tracer, vous ferez ce qui suit :

- Déterminez les sous-réseaux IPv6 et le système d'adressage
- Configurez l'adressage IPv6 sur les routeurs et les ordinateurs.
- Vérification de la connectivité IPv6
- **LAB14.2-IPV6**

# Travaux pratiques — Configurer les adresses IPv6 sur les périphériques réseau

Au cours de ce TP, vous aborderez les points suivants:

- Définir la topologie et configurer les paramètres de base du routeur et du commutateur
- Configurer manuellement les adresses IPv6
- Vérifier la connectivité de bout en bout
- **LAB14.3-IPV6**

# 14.9 Module pratique et questionnaire

# Qu'est-ce que j'ai appris dans ce module?

- Théoriquement, l'IPv4 est limité à 4,3 milliards d'adresses.
- L'IETF a créé divers protocoles et outils pour aider les administrateurs réseau à migrer leurs réseaux vers l'IPv6. Les techniques de migration peuvent être regroupées sous trois catégories: dual-stack, tunneling et traduction.
- Les adresses IPv6 ont une longueur de 128 bits et sont notées sous forme de chaînes de valeurs hexadécimales.
- Le format privilégié pour noter une adresse IPv6 est x:x:x:x:x:x:x, où chaque «x» est constitué de quatre valeurs hexadécimales.
- Il existe trois types d'adresses IPv6 : monodiffusion, multidiffusion et anycast (monodiffusion aléatoire).
- Une adresse de monodiffusion IPv6 identifie une interface sur un périphérique IPv6 de façon unique.
- Les adresses de diffusion globale (GUA) IPv6 sont uniques au monde et routables (Internet IPv6).
- Une adresse link-local IPv6 (LLA) permet à un appareil de communiquer avec d'autres appareils IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau).
- La commande pour configurer une GUA IPv6 sur une interface est **ipv6 adresse ipv6-adresse/prefix-length**.
- Un périphérique obtient une GUA dynamiquement via des messages ICMPv6. Les routeurs IPv6 envoient des messages d'annonce de routeur ICMPv6 toutes les 200 secondes à tous les périphériques IPv6 du réseau.

## Qu'est-ce que j'ai appris dans ce module? (Suite)

- Les messages RA ont trois méthodes : SLAAC, SLAAC avec un serveur DHCPv6 sans état et DHCPv6 avec état (pas de SLAAC).
- L'interface ID peut utiliser la méthode EUI-64 ou un nombre à 64 bits généré aléatoirement.
- Ce processus utilise l'adresse MAC Ethernet à 48 bits d'un client et insère 16 autres bits au milieu de cette adresse MAC pour créer un ID d'interface de 64 bits.
- Selon le système d'exploitation, un périphérique peut utiliser un ID d'interface.
- Tous les périphériques IPv6 doivent avoir un LLA IPv6. Un LLA peut être configuré manuellement ou créé dynamiquement.
- Les routeurs Cisco créent automatiquement une adresse link-local IPv6 dès qu'une adresse de diffusion globale est attribuée à l'interface.
- Il existe deux types d'adresses de multidiffusion IPv6 : les adresses de multidiffusion bien connues et les adresses de multidiffusion de nœuds sollicités.
- Deux groupes de multidiffusion assignés à CommonIPv6 sont : ff02 ::1 groupe de multidiffusion All-nœuds et ff02 ::2 groupe de multidiffusion All-routers.
- Une adresse de multidiffusion de nœud sollicité est comparable à une adresse de multidiffusion à tous les nœuds. Elle offre l'avantage d'être mappée à une adresse de multidiffusion Ethernet spéciale.
- IPv6 a été conçu en pensant au sous-réseau. Un champ d'ID de sous-réseau distinct dans la GUA IPv6 est utilisé pour créer des sous-réseaux.