Version expérimentale
En cours de validation

RÉSUMÉ THÉORIQUE – FILIÈRE SYSTÈMES ET RÉSEAUX

M201 – METTRE EN PLACE UNE INFRASTRUCTURE RÉSEAUX

42 heures

SOMMAIRE

MODALITÉS PÉDAGOGIQUES

1

LE GUIDE DE SOUTIEN

Il contient le résumé théorique et le manuel des travaux pratiques

2

LA VERSION PDF

Une version PDF est mise en ligne sur l'espace apprenant et formateur de la plateforme WebForce Life

3

DES CONTENUS TÉLÉCHARGEABLES

Les fiches de résumés ou des exercices sont téléchargeables sur WebForce Life

4

DU CONTENU INTERACTIF

Vous disposez de contenus interactifs sous forme d'exercices et de cours à utiliser sur WebForce Life

5

DES RESSOURCES EN LIGNES

Les ressources sont consultables en synchrone et en asynchrone pour s'adapter au rythme de l'apprentissage

PARTIE 1

Maîtriser les Concepts de commutation

Dans ce module, vous allez :

- Être en mesure de configurer les fonctionnalités avancées des routeurs et des commutateurs

5 heures

CHAPITRE 1

Configurer les périphériques réseaux

Ce que vous allez apprendre dans ce chapitre :

- Configurer les paramètres de base des périphériques réseaux

2 heures

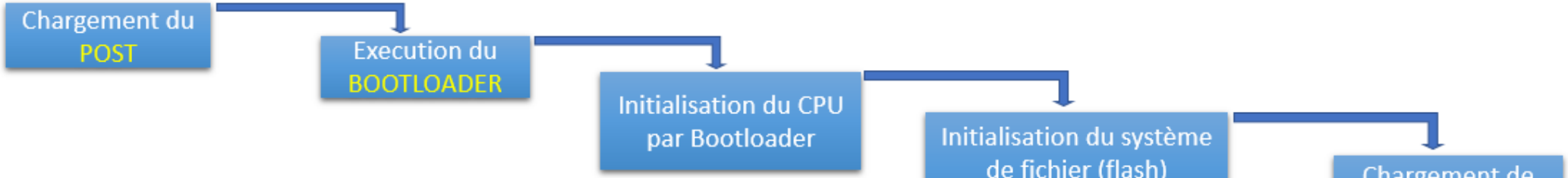
CHAPITRE 1

Configurer les périphériques réseaux

1. Configuration d’un commutateur
2. Les paramètres de base d'un routeur

La séquence de démarrage du commutateur

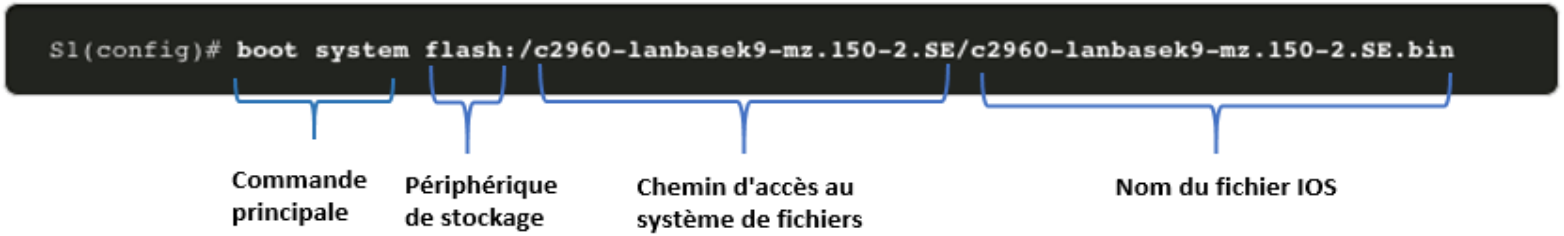
Une fois qu'un commutateur Cisco est mis sous tension, il passe par la séquence de démarrage suivante en cinq étapes:



POST : un programme auto-test de mise sous tension stocké dans la ROM, vérifie le sous-système CPU. Il teste le processeur, la DRAM et la partie du périphérique flash.
BOOTLOADER : (chargeur de démarrage) est un petit programme stocké dans la ROM qui est exécuté immédiatement après la fin de POST.

La commande boot system

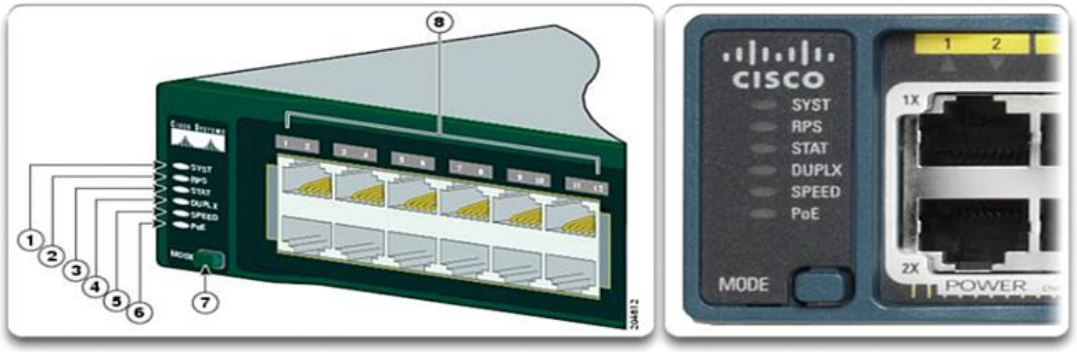
- Le commutateur tente de démarrer automatiquement en utilisant les informations de la variable d'environnement **BOOT**. Si cette variable n'est pas définie, le commutateur tente de charger et d'exécuter le premier fichier exécutable qu'il peut trouver.
- Le système d'exploitation IOS initialise ensuite les interfaces à l'aide des commandes Cisco IOS figurant dans le fichier de configuration initiale. Le fichier startup-config est appelé **config.text** et se trouve en flash.



PARTIE 1

PARTIE 1

LED du commutateur



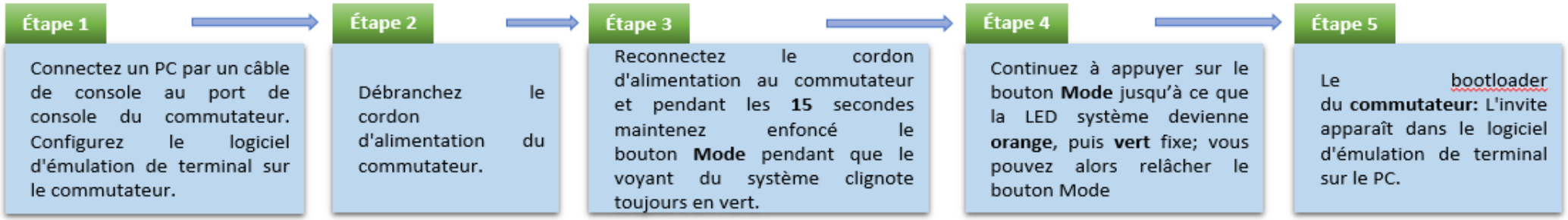
1	The system LED	5	The port speed LED
2	The RPS LED (if RPS is supported on the switch)	6	The PoE status LED (if PoE is supported on the switch)
3	The port status LED (This is the default mode.)	7	The Mode button
4	The port duplex mode LED	8	The port LEDs

	Lumière éteinte	Vert	Vert, clignotant	Orange	Orange, clignotant	Vert/Orange en alternance
RPS	RPS est éteinte/Pas de RPS	Prêt pour RPS	RPS est activé mais pas disponible	RPS secours ou défaut	l'alimentation interne a été défaillant, le relais de l'alimentation RPS	S/O
Fonctionnalités	Non sélectionné, aucun problème	Sélectionné	S. o.	S. o.	Non sélectionné, problèmes de port présents	S. o.
Lorsque le mode nommé est sélectionné, le LED associé à chaque port physique indique:						
STAT	Aucun lien ou arrêt	Liaison active	Activité	Port bloqué empêchant la boucle	Port bloqué empêchant la boucle	Liaison défectueuse
DUPLEX	Semi-duplex	Duplex intégral	S. o.	S. o.	S. o.	S. o.
SPEED (vitesse)	10 Mbits/s	100 Mbit/s	1000 Mb/s	S. o.	S. o.	S. o.
Fonctionnalités	PoE désactivé	PoE activé	S. o.	PoE désactivé	Le mode PoE est désactivé en raison d'une erreur.	PoE refusé (dépassement du budget)

Récupération après une panne de système

Le bootloader permet d'accéder au commutateur si le système d'exploitation ne peut être utilisé en raison de fichiers système manquants ou endommagés. Le chargeur de démarrage dispose d'une ligne de commande qui permet d'accéder aux fichiers stockés dans la mémoire flash.

Le chargeur de démarrage est accessible via une connexion à la console en suivant ces étapes :



La li t de récupérer un mot de passe perdu ou oublié. Par exemple, la commande **dir** peut être utilisée pour afficher la liste des fichiers dans un dossier spécifique.

```
switch: set
BOOT=flash:/c2960-lanbasek9-mz.122-55.SE7/c2960-lanbasek9-mz.122-55.SE7.bin
(output omitted)
switch: flash_init
Initializing Flash...
flashfs[0]: 2 files, 1 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 32514048
flashfs[0]: Bytes used: 11838464
flashfs[0]: Bytes available: 20675584
flashfs[0]: flashfs fsck took 10 seconds.
...done Initializing Flash.
```

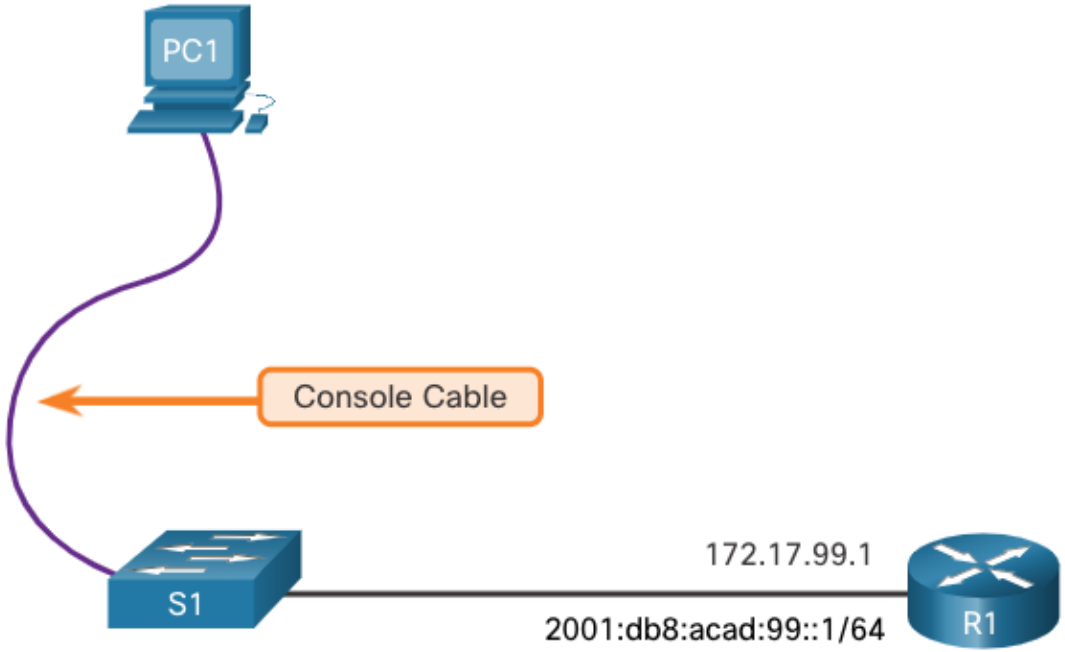
```
switch: dir flash:
Directory of flash:/
2 -rwx 11834846 c2960-lanbasek9-mz.150-2.SE8.bin
3 -rwx 2072 multiple-fs
```

```
switch: BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
switch: set
BOOT=flash:c2960-lanbasek9-mz.150-2.SE8.bin
(output omitted)
switch: boot
```

PARTIE 1

Accès à la gestion du commutateur

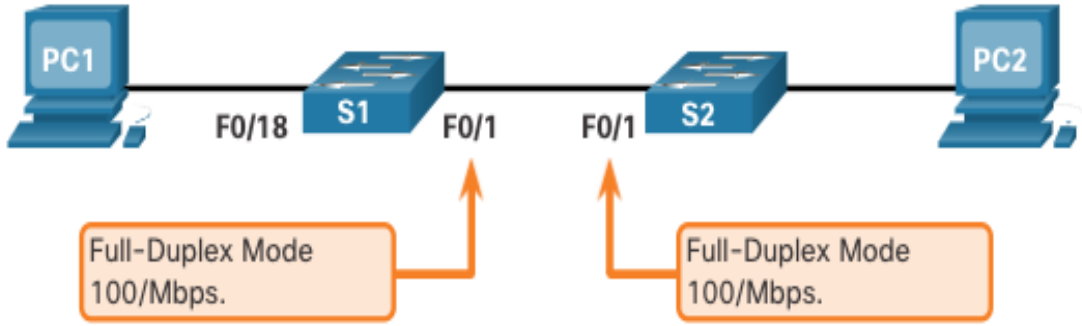
- Pour préparer un commutateur pour l'accès à la gestion à distance, l'interface virtuelle du commutateur (SVI) doit être configuré avec une adresse IP et un masque de sous-réseau .
- Pour gérer le commutateur à partir d'un réseau distant, le commutateur doit être configuré avec une passerelle par défaut.
- Un câble de console est utilisé pour se connecter à un PC afin que le commutateur puisse être configuré initialement.



La communication en mode duplex

- Les communications duplex intégrale simultanées augmentent la bande passante réelle, car les deux extrémités de la connexion transmettent et reçoivent simultanément des données.
- Contrairement à la communication Full-duplex, la communication Half-duplex est unidirectionnelle. La communication en Half-duplex pose des problèmes de performance car les données ne peuvent circuler que dans un seul sens à la fois, ce qui entraîne souvent des collisions.

Remarque: Des paramètres incorrects relatifs au mode duplex ou au débit peuvent entraîner des problèmes de connectivité.



Auto-MDIX

- Lorsque la fonction auto-MDIX (automatic medium-dependent interface crossover) est activée, l'interface du commutateur détecte automatiquement le type de connexion de câble requis (droit ou croisé) et configure la connexion de manière appropriée.
- Lorsque la fonction Auto-MDIX est utilisée sur une interface, la vitesse et le mode duplex de celle-ci doivent être réglés sur auto afin que le système fonctionne correctement.
- Pour examiner le paramètre Auto-MDIX pour une interface spécifique, utilisez la commande **show controllers ethernet-controller** avec le mot-clé **phy** .
- Pour limiter la sortie aux lignes référençant Auto-MDIX, utilisez le filtre **Inclut Auto-MDIX**

PARTIE 1

Commandes de vérification du commutateur

Tâche	Commandes IOS
Affichez l'état et la configuration des interfaces.	S# **show interfaces** [*interface-id*]
Affichez la configuration initiale actuelle.	S# **show startup-config**
Affichez la configuration courante.	S# **show running-config**
Affichez les informations sur le système de fichiers Flash.	S# **show flash**
Affichez l'état matériel et logiciel du système.	S# **show version**
Affichez l'historique des commandes exécutées.	S# **show history**
Affichez les informations IP d'une interface.	S# **show ip interface** [*interface-id*] OU S# **show ipv6 interface** [*interface-id*]
Affichez la table d'adresses MAC.	S# **show mac-address-table** OU S# **show mac address-table**

Les erreurs de la couche d'accès réseau

Certaines erreurs de support ne sont pas assez graves pour provoquer la défaillance du circuit, mais causent des problèmes de performances réseau. Le tableau explique certaines de ces erreurs courantes qui peuvent être détectées à l'aide de la commande **show**

Type d'erreur	Description
Erreurs en entrée	Nombre total d'erreurs. Elles comprennent les trames incomplètes, trames géantes, pas de mémoire tampon, CRC, trame, débordement et comptes ignorés.
Trames incomplètes	Paquets éliminés car ils sont inférieurs à la taille de paquet minimale définie pour le support. Par exemple, toute trame Ethernet inférieure à 64 octets est considérée comme incomplète.
Trames géantes	Paquets éliminés car ils sont supérieurs à la taille de paquet maximale définie pour le support. Par exemple, toute trame Ethernet supérieure à 1518 octets est considérée comme «géante».
CRC	Les erreurs CRC sont générées lorsque la somme de contrôle calculée ne correspond pas à la somme de contrôle reçue.
Erreurs en sortie	Somme de toutes les erreurs ayant empêché la transmission finale des datagrammes vers l'interface examinée.
Collisions	Nombre de messages retransmis à cause d'une collision Ethernet.
Collisions tardives	Collision se produisant après la transmission de 512 bits de la trame.

Accès à distance sécurisé

Affecter une IP à un VLAN

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

Affecter une IP à une interface

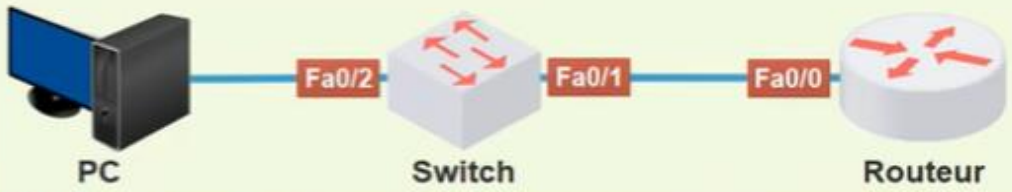
```
Routeur(config)#interface fastEthernet 0/0
Routeur(config-if)#ip address 192.168.1.2 255.255.255.0
```

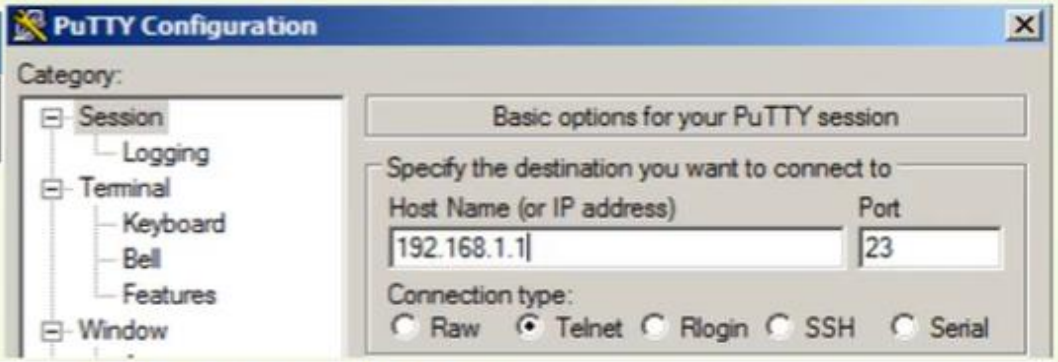
Configurer Telnet

```
Switch(config)#line vty 0 4
Switch(config-line)#password Carl
Switch(config-line)#login
```

Configurer SSH

```
Switch(config)#username Glenn password
Switch(config)#ip domain-name Formation
Switch(config)#ip ssh version 2
Switch(config)#line vty 0 4
Switch(config-line)#login local
Switch(config-line)#transport input ssh
```






```
Switch(config)#crypto key generate rsa
How many bits in the modulus [512]: 1024
Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Rick(config)#
Feb 20 23:22:11: %SSH-5-ENABLED: SSH version 1 has been enabled
```

PARTIE 1

CHAPITRE 1

Configurer les périphériques réseaux

1. Configuration d’un commutateur
2. Les paramètres de base d'un routeur

PARTIE 1

Configuration de base d'un routeur

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

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#
```

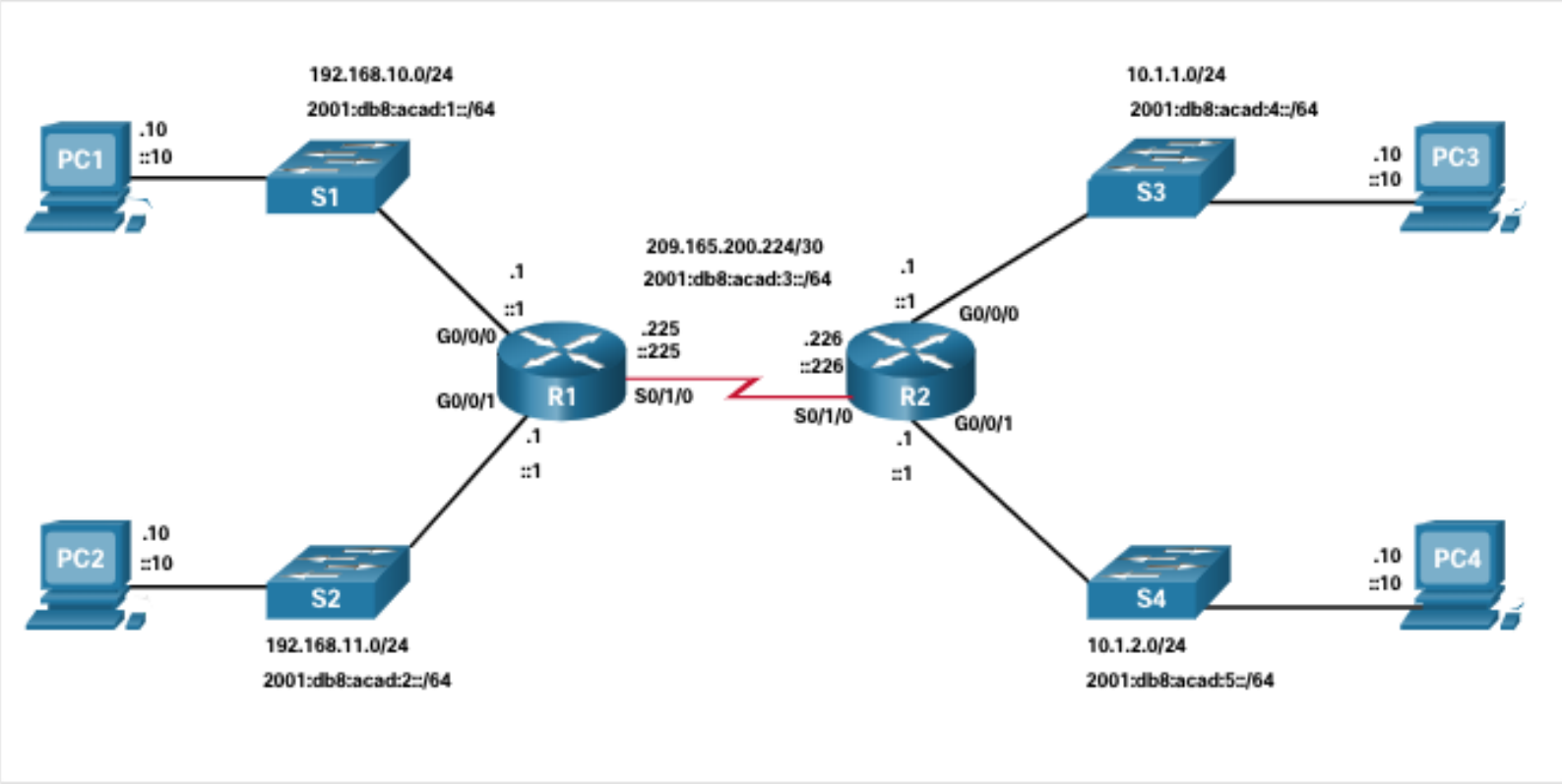
```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

PARTIE 1

Topologie à double pile

Une fonction de distinction entre les commutateurs et les routeurs est le type d'interface pris en charge par chacun. Par exemple, les commutateurs de la couche 2 prennent en charge les LAN ; ils disposent donc de plusieurs ports FastEthernet ou Gigabit Ethernet. La topologie à double pile de la figure est utilisée pour démontrer la configuration des interfaces IPv4 et IPv6 du routeur.



Configurer les interfaces du routeur

Les routeurs sont compatibles avec les LAN et les WAN et peuvent interconnecter différents types de réseaux; ils prennent donc en charge plusieurs types d'interfaces y compris les interfaces série, DSL et câblées.

Pour être disponible, une interface doit être:

- **Configurée avec au moins une adresse IP** - ----------→ **ip address** *ip-address subnet-mask* et **ipv6 address** *ipv6-address/prefix* .
- **Activée** - ----------→ **no shutdown** .
- **Description** - ----------→ **description** *description* (au maximum 240 caractères).

Interfaces de bouclage IPv4

- L'interface de bouclage est une interface logique interne au routeur. Elle n'est pas affectée à un port physique et ne peut jamais être connectée à un autre appareil. Elle est considérée comme une interface logicielle qui est automatiquement placée en état «up», tant que le routeur fonctionne.
- L'interface de bouclage est utile en cas de test et de gestion d'un périphérique Cisco IOS, car elle garantit qu'au moins une interface est toujours disponible. Par exemple, elle peut être utilisée à des fins de test des processus de routage internes, par exemple, en émulant les réseaux se trouvant derrière le routeur.

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

PARTIE 1

Commandes de vérification de l'interface

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

Tâche	Commandes IOS
affiche un résumé pour toutes les interfaces, y compris l'adresse IPv4 ou IPv6 de l'interface et l'état opérationnel actuel.	R# **show ip interface brief** OU R# **show ipv6 interface brief**
affiche l'état de l'interface et toutes les adresses IPv4/IPv6 appartenant à l'interface	R# **show ip interface** [*interface-id*] OU R# **show ipv6 interface** [*interface-id*]
Affiche les commandes appliquées à l'interface spécifiée.	R# **show running-config interface** [*interface-id*]
Affiche le contenu de la table de routage IPv4/IPv6 stocké dans la mémoire vive.	R# **show ip route** OU R# **show ipv6 route**

Filtrer les résultats des commandes show

- Les commandes qui génèrent plusieurs écrans de sortie sont, par défaut, mises en pause après 24 lignes. À la fin de cette interruption, le texte **--More--** s'affiche. Appuyez sur **Enter** pour afficher la ligne suivante et appuyez sur la touche Espace pour afficher la série de lignes suivante.
- Utilisez la commande **terminal length** pour indiquer le nombre de lignes à afficher. La valeur 0 (zéro) empêche le routeur de s'arrêter entre les écrans de résultat.
- Une autre fonctionnalité très utile qui améliore l'expérience de l'utilisateur dans le CLI est le filtrage des sorties de commandes **show** .
- Les commandes de filtrage permettent d'afficher des sections de résultat spécifiques.
- Pour activer la commande de filtrage, tapez le symbole (**|**) après la commande **show** , puis saisissez un paramètre de filtrage et une expression de filtrage:
  - **Section** - Affiche l'intégralité de la section commençant par l'expression de filtrage
  - **Include** - Inclut toutes les lignes de résultat correspondant à l'expression de filtrage.
  - **Exclude** - Exclut toutes les lignes de résultat correspondant à l'expression de filtrage.
  - **Begin** - Affiche toutes les lignes de résultat à partir d'un certain point, en commençant par la ligne qui correspond à l'expression de filtrage

CHAPITRE 2

Appliquer les Concepts de commutation

Ce que vous allez apprendre dans ce chapitre :

- Comprendre les concepts de commutation

1 heures

CHAPITRE 2

Appliquer les Concepts de commutation

1. Concepts de commutation

PARTIE 1

Transfert de trame

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 pour 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

La table d'adresses MAC du commutateur

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.

.

```
SW1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0012.a647.3d5a    DYNAMIC     Et0/0
   1    0015.795c.02b3    DYNAMIC     Et0/0
   1    001f.e429.5a05    DYNAMIC     Et0/0
   1    0020.013c.0786    DYNAMIC     Et0/0
   1    0020.8e6a.c20a    DYNAMIC     Et0/0
   1    0026.5218.10b6    DYNAMIC     Et0/0
   1    003d.3a69.b32a    DYNAMIC     Et0/0
   1    003e.a910.a51f    DYNAMIC     Et0/0
   1    0040.9d5c.9832    DYNAMIC     Et0/0
   1    0047.380f.b496    DYNAMIC     Et0/0
```

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 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**
- **Commutation par coupure (cut-through)**

PARTIE 1

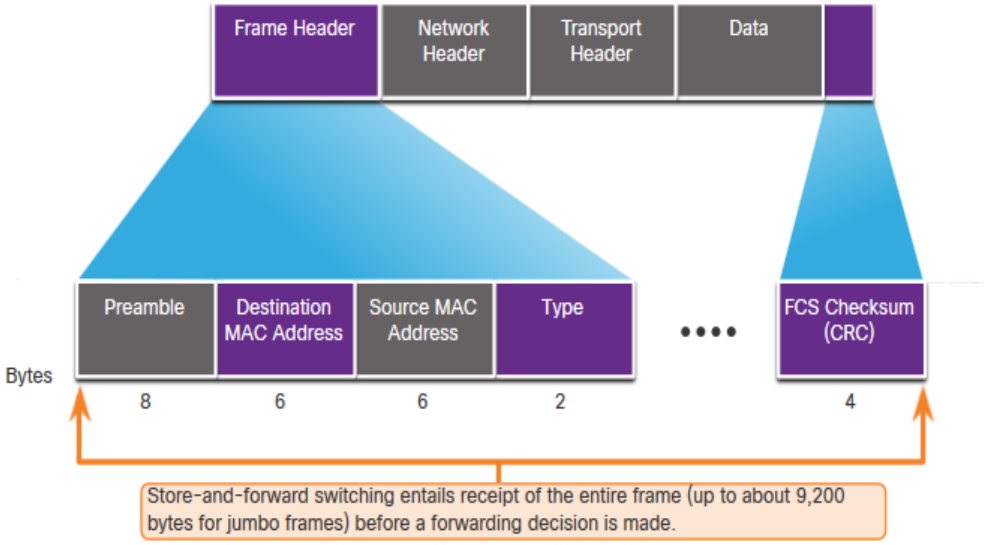
Commutation de trame

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

Le commutateur Reçoit la trame entière et assure la validité de la trame.

Le stockage et le transfert présentent deux caractéristiques principales :

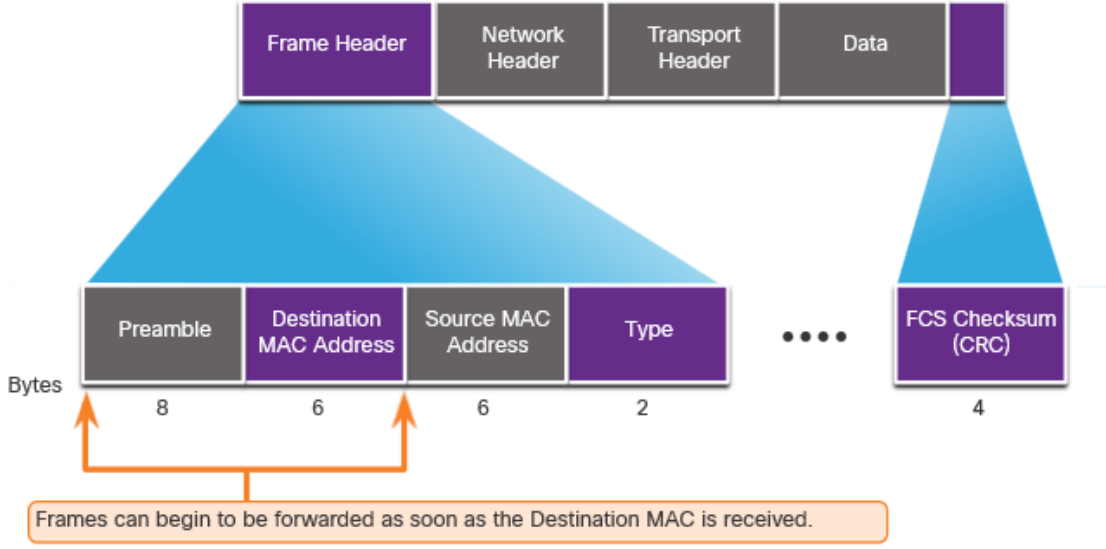
- Vérification des erreurs
- Mise en mémoire tampon



○ Commutation par coupure (Cut-Through)

Le commutateur 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.

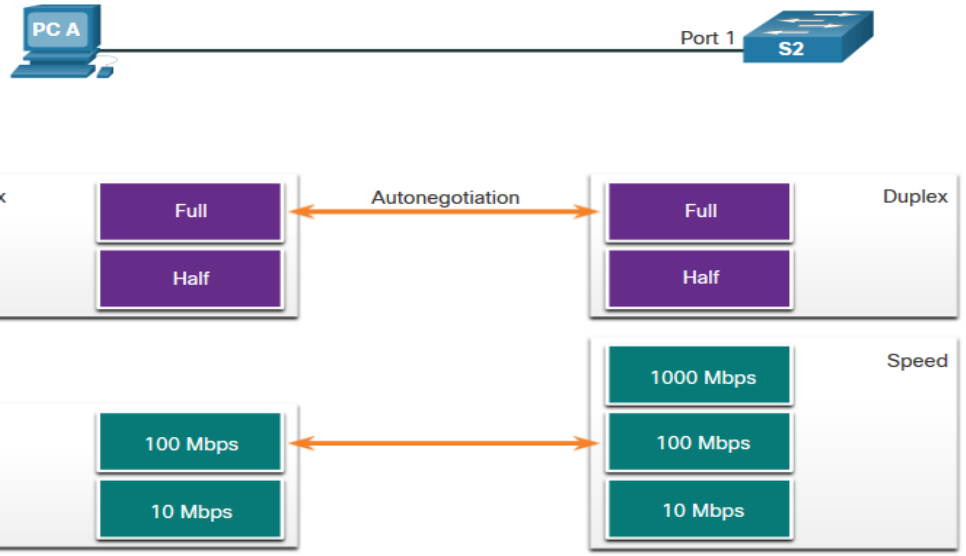


PARTIE 1

Domaines de collision

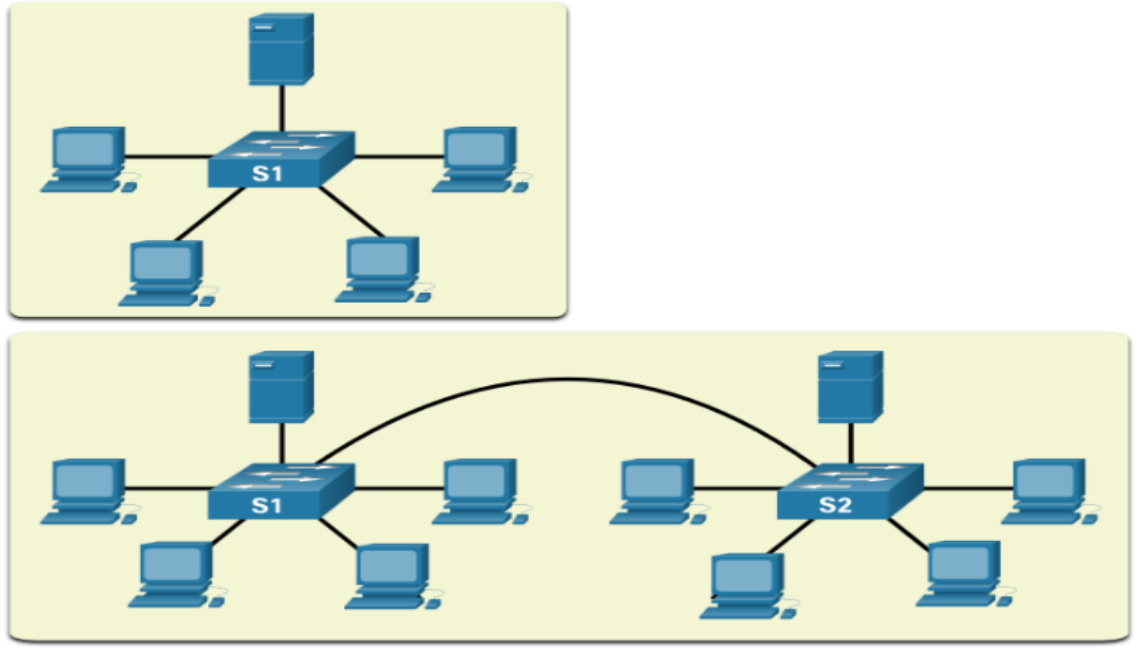
Les commutateurs éliminent les domaines de collision et réduisent la congestion.

- 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.
- Trop de diffusions peuvent causer de la congestion et des performances réseau médiocres.



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:

Caractéristiques	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.

CHAPITRE 3

Mettre en œuvre des VLAN

Ce que vous allez apprendre dans ce chapitre :

- Configurer les VLAN
- Configurer le routage inter-VLAN

2 heures

CHAPITRE 3

Mettre en œuvre des VLAN

1. Aperçu des réseaux locaux virtuels (VLAN)
2. Configuration des VLAN
3. Routage inter-VLAN
4. Le protocole DTP

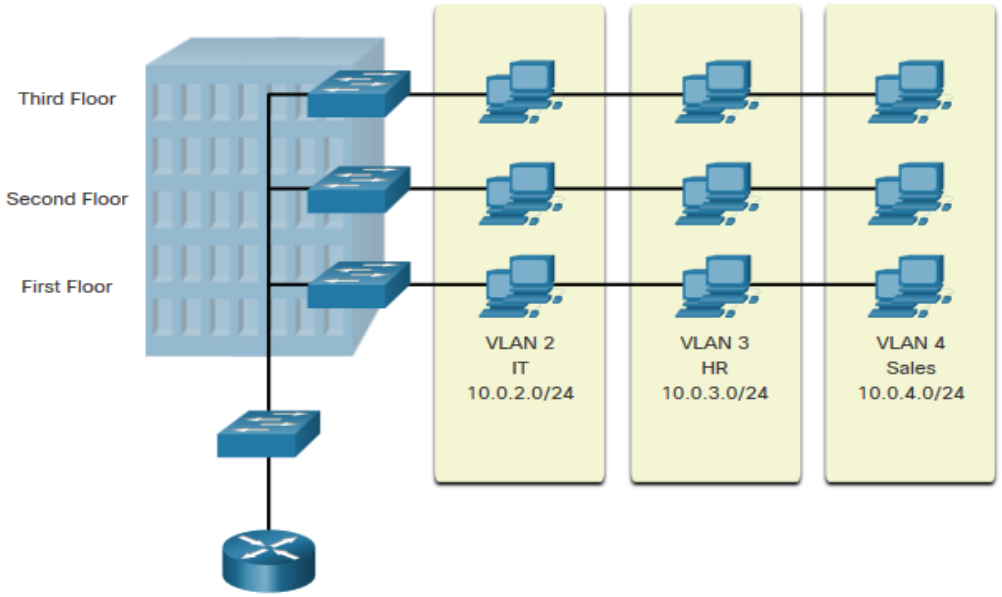
Aperçu des réseaux locaux virtuels (VLAN)

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

Aperçu des réseaux locaux virtuels (VLAN)

- **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, il est recommandé d'attribuer ces caractéristiques par défaut à d'autres VLAN

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

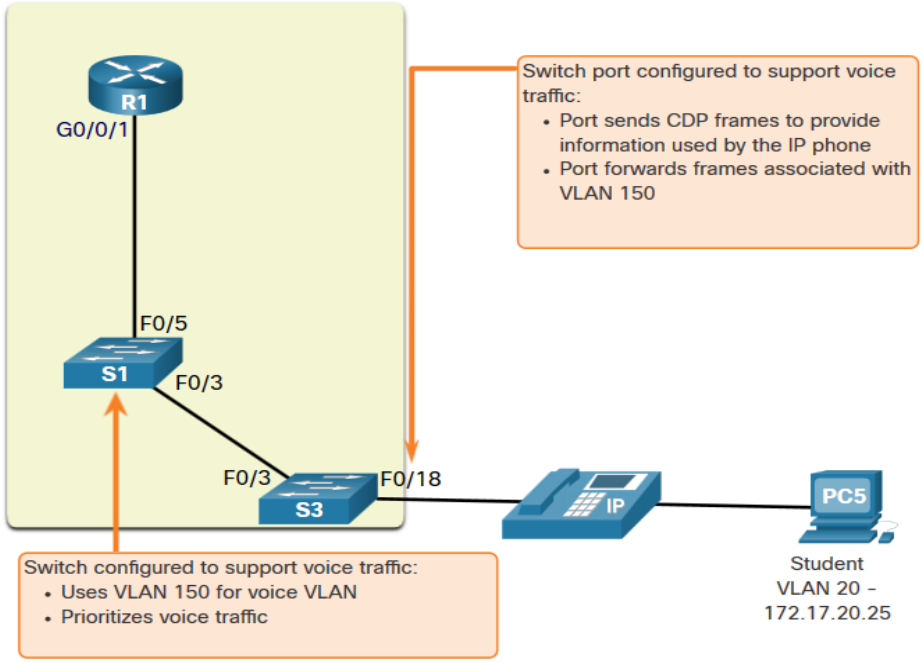
- Ceci est utilisé uniquement pour les liaisons de trunk.
- Toutes les trames sont marquées sur une liaison de trunk 802.1Q, à l'exception de celles sur le VLAN natif.

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.

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.



PARTIE 1

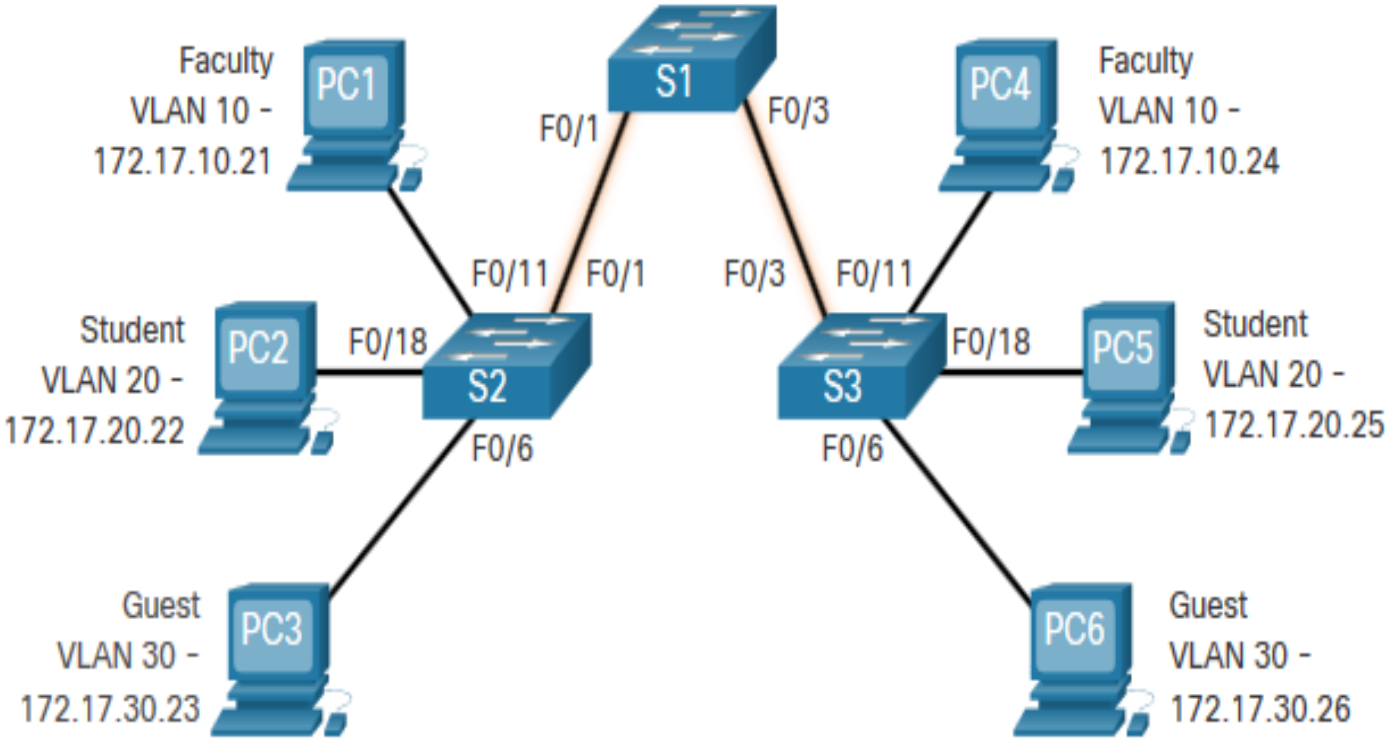
Les VLAN dans un environnement à plusieurs commutateurs

- **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



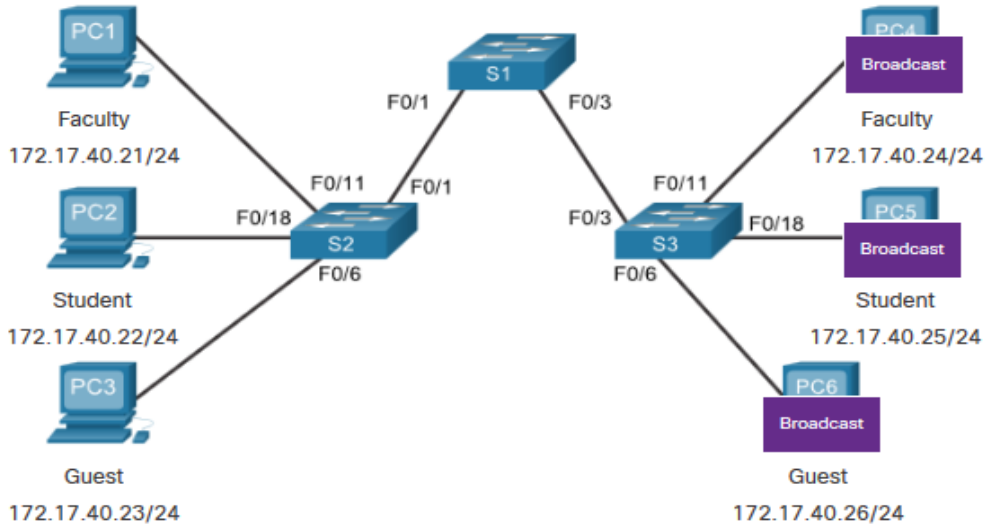
PARTIE 1

PARTIE 1

Les VLAN dans un environnement à plusieurs commutateurs

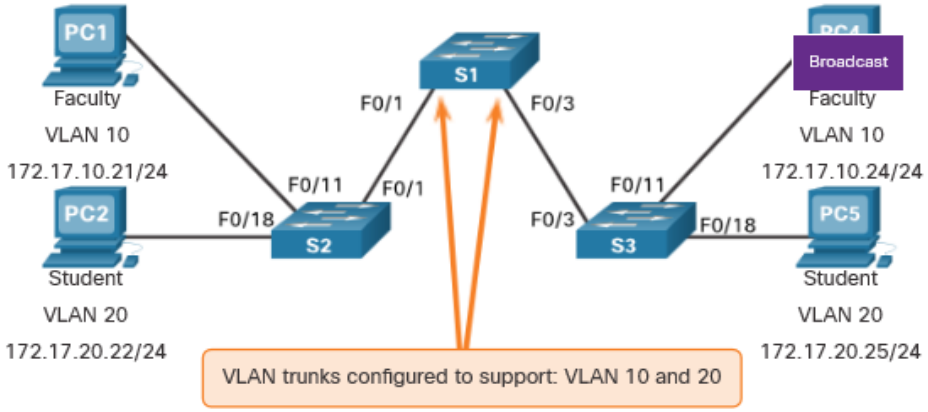
- **Réseau sans/avec VLAN**

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.

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



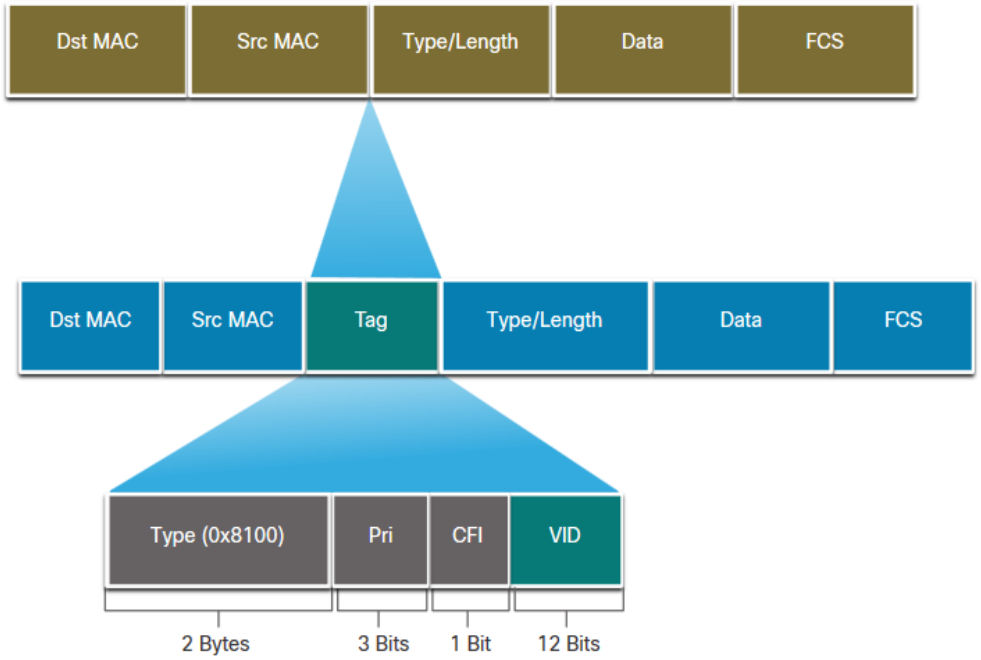
PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

Les 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	• Champ de 2 octets avec hexadécimal 0x8100 • Ceci est appelé TPID (Tag Protocol ID)
Priorité Utilisateur	• Valeur de 3 bits prenant en charge
CFI (Canonical Format Identifier)	• Identificateur de 1 bit qui prend en charge les trames Token Ring sur des liaisons Ethernet
ID de VLAN (VID)	• Numéro d'identification VLAN de 12 bits qui prend en charge jusqu'à 4096 ID de VLAN.



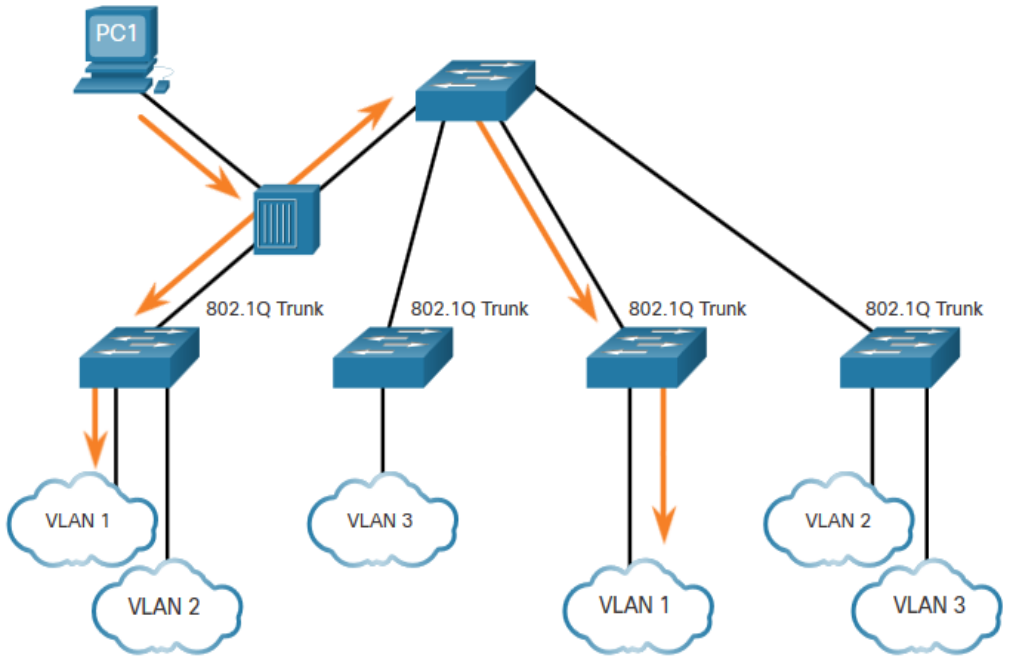
PARTIE 1

Les 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.



PARTIE 1

CHAPITRE 3

Mettre en œuvre des VLAN

1. Aperçu des réseaux locaux virtuels (VLAN)
2. Configuration des VLAN
3. Routage inter-VLAN
4. Le protocole DTP

Création et attribution 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# **configure terminal**
Créez un VLAN avec un numéro d'identité valide.	Switch(config)# **vlan** *vlan-id*
Indiquez un nom unique pour identifier le VLAN.	Switch(config-vlan)# **name** *vlan-name*
Repassez en mode d'exécution privilégié.	Switch(config-vlan) # **end**
Passez en mode de configuration globale.	Switch# **configure terminal**

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# **configure terminal**
Passez en mode de configuration d'interface.	Switch(config)# **interface** *interface-id*
Définissez le port en mode d'accès.	Switch(config-if)# **switchport mode access**
Affectez le port à un réseau local virtuel.	Switch(config-if)# **switchport access vlan** *vlan-id*
Repassez en mode d'exécution privilégié.	Switch(config-if)# **end**

Vérification de la configuration VLAN

- Utiliser la commande **show vlan** . La syntaxe complète est :
- **show vlan [brief** | **id** *vlan-id* | **name** *vlan-name* | **summary**]

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

Modification de la configuration 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.

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.

Commandes de configuration de trunk

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

Le protocole VTP

Le protocole VTP permet de diffuser la déclaration des VLANs pour les ports trunk sur l'ensemble du réseau en réalisant une administration centralisée de ceux-ci. Ce protocole est propriétaire CISCO. Il fonctionne avec une architecture client serveur.

Le serveur tient à jour une table de VLANs déclarés. Cette table est diffusée à l'ensemble des clients étant sur le même domaine VTP. De ce fait chaque modification de la table est répercutée à l'ensemble des clients. Ainsi tous les VLANs définis sur le serveur pourront transiter par l'ensemble des ports trunk des switchs clients (sauf configuration contraire sur les interfaces).

Les matériels peuvent être en mode :

- **Server** : Il est associé à un domaine VTP. La déclaration des VLANs s'effectue sur le serveur. Il tient à jour la liste des VLANs déclarés et la diffuse à l'ensemble des clients.

- **Client** : Il est associé à un domaine VTP. Il reçoit la liste des VLANs, il la propage aux autres clients auxquels il est connecté et met à jour sa propre liste.

- **Transparent** : Il est associé à aucun domaine VTP. Sa liste de VLAN est locale et n'est pas mis à jour lorsqu'il reçoit une trame VTP. Cependant il propage les listes de VLAN qu'il reçoit.

- **VTP password** : il est possible d'indiquer un mot de passe sur le serveur pour le domain VTP. Dans ce cas les clients ne peuvent se mettre à jour que s'ils ont le même mot de passe. Ceci permet de déjouer les attaques consistant pour un pirate à se faire passer pour le VTP serveur.

- **VTP prunning** : le VTP prunning permet d'optimiser le protocole VTP en ne déclarant les VLANs que sur les ports trunk ou cela est nécessaire et utile.

Configuration du serveur :

```
Switch1# vlan database
Switch1 (vlan)# vtp domain monDomain
Switch1 (vlan)# vtp passwd monMotDePasse
Switch1 (vlan)# vtp server
Switch1 (vlan)# vtp prunning
Switch1 (vlan)# exit
```

Configuration du client :

```
Switch1# vlan database
Switch1 (vlan)# vtp domain monDomain
Switch1 (vlan)# vtp passwd monMotDePasse
Switch1 (vlan)# vtp client
Switch1 (vlan)# vtp prunning
Switch1 (vlan)# exit
```

CHAPITRE 3

Mettre en œuvre des VLAN

1. Aperçu des réseaux locaux virtuels (VLAN)
2. Configuration des VLAN
3. Routage inter-VLAN
4. Le protocole DTP

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 (SVIS)** - Il s'agit de la solution la plus évolutive pour les moyennes et grandes entreprises.

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.

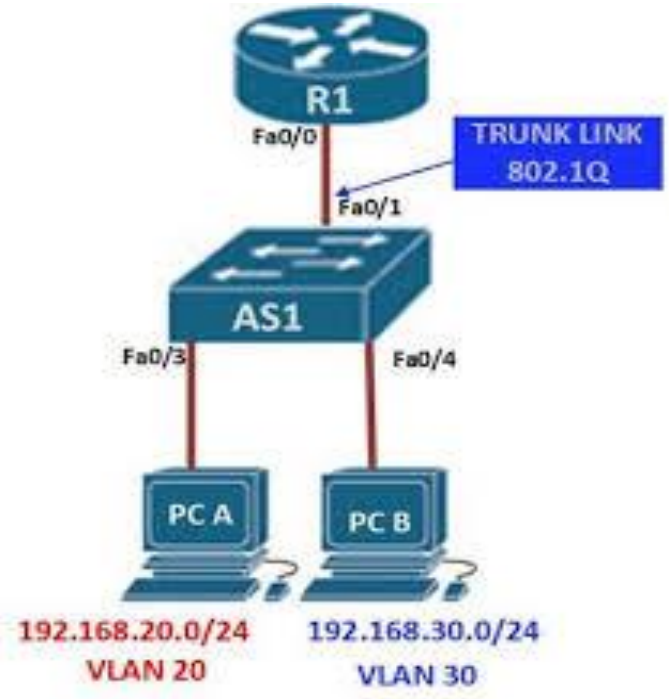
Remarque : Cette méthode de routage inter-VLAN n'est plus implémentée dans les réseaux commutés et est incluse à des fins d'explication uniquement.

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. 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 VLAN balisé 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 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.

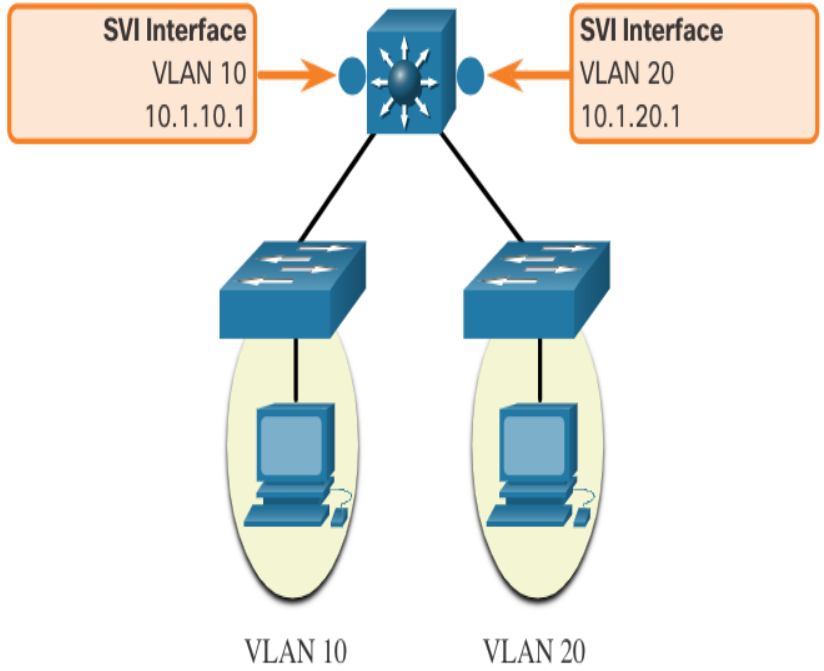


PARTIE 1

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.

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 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 on-a-stick 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.

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 échouer.

Type de problème	Comment réparer	Comment vérifier
VLAN manquants	• Créez (ou recréez) le VLAN s'il n'existe pas. • Assurez-vous que le port hôte est attribué au VLAN correct.	**show vlan [brief]** **show interfaces switchport** **ping**
Problèmes de port de trunk de commutateur	• Assurez-vous que les trunks sont correctement configurés. • Assurez-vous que le port est un port de trunk et activé.	**show interface trunk** **show running-config**
Problèmes liés aux ports de commutateur	• Attribuez le port au correct VLAN. • Assurez-vous que le port est un port d'accès et activé. • L'hôte n'est pas correctement configuré dans le mauvais sous-réseau.	**show interfaces switchport** **show running-config interface** **ipconfig**
Problèmes de configuration du routeur	• L'adresse IPv4 de la sous-interface du routeur est mal configurée. • La sous-interface du routeur est attribué à l'ID du VLAN.	**show ip interface brief** **show interfaces**

CHAPITRE 3

Mettre en œuvre des VLAN

1. Aperçu des réseaux locaux virtuels (VLAN)
2. Configuration des VLAN
3. Routage inter-VLAN
4. Le protocole DTP

Configuration de protocole DTP (Dynamic Trunking Protocol)

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

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**.

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

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

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

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	Trunc	Accès
Dynamique souhaitable	Trunc	Trunc	Trunc	Accès
Trunk	Trunc	Trunc	Trunc	Connectivité limitée
Accès	Accès	Accès	Connectivité limitée	Accès

Vérifier la configuration du 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

PARTIE 2

Etablir un réseau d'entreprise évolutif

Dans ce module, vous allez :

- Être en mesure de concevoir un réseau évolutif
- Etre en mesure de comprendre et configurer le protocole STP
- Etre capable de configurer l'agrégation des liaisons avec l'EtherChannel
- Etre en mesure de comprendre le fonctionnement du FHRP

6 heures

CHAPITRE 1

Etudier l’évolutivité du réseau

Ce que vous allez apprendre dans ce chapitre :

- Concevoir un réseau évolutif avec le bon choix des équipements

1.5 heures

CHAPITRE 1

Etudier l’évolutivité du réseau

1. Conception de réseau évolutif
2. Sélection des périphériques réseau

PARTIE 2

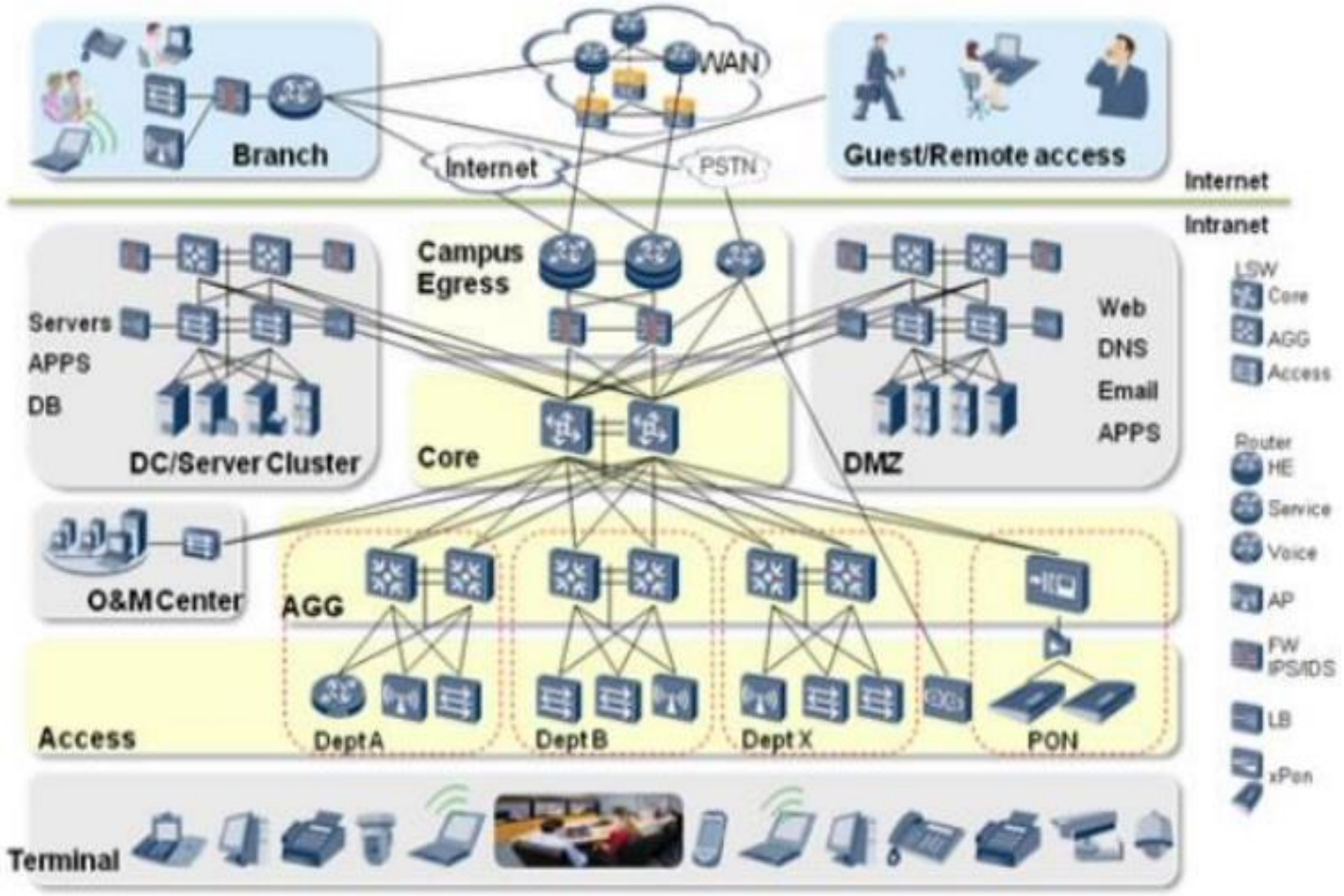
L'évolutivité de réseau

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:

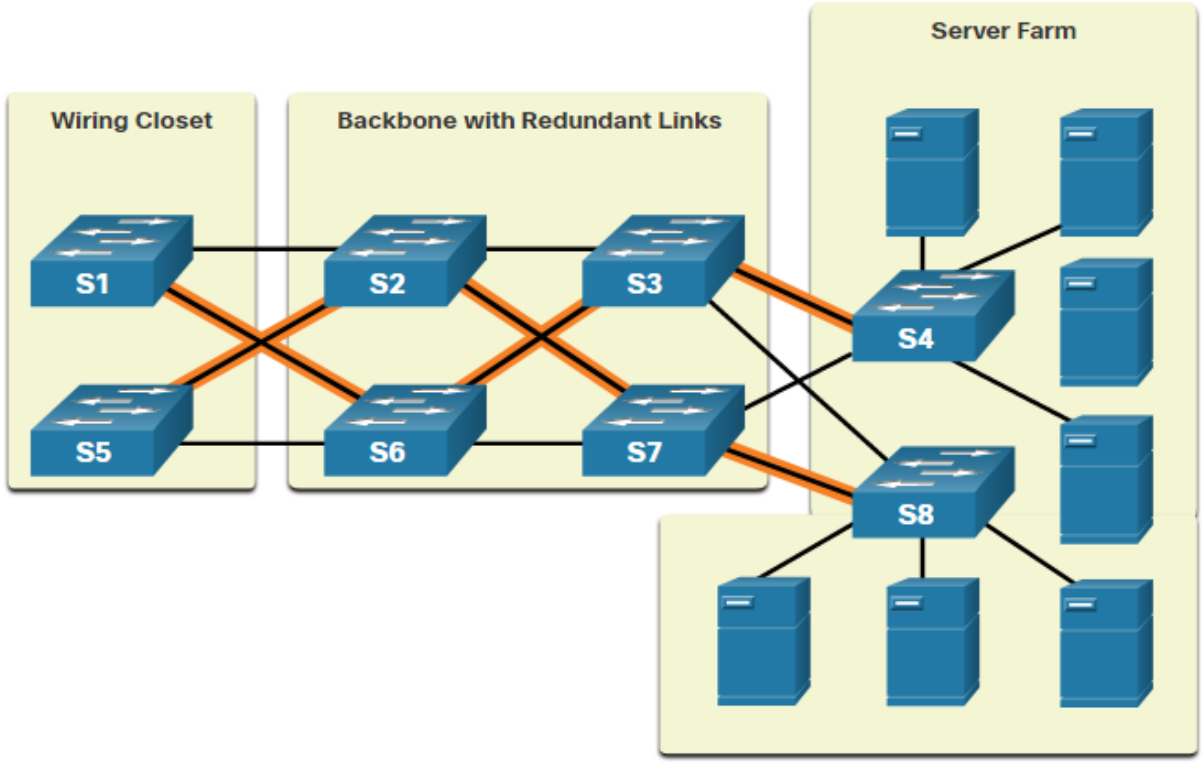
- **Redondance**
- **Liens multiples**
- **Protocole de routage évolutif**
- **Connectivité sans fil**



PARTIE 2

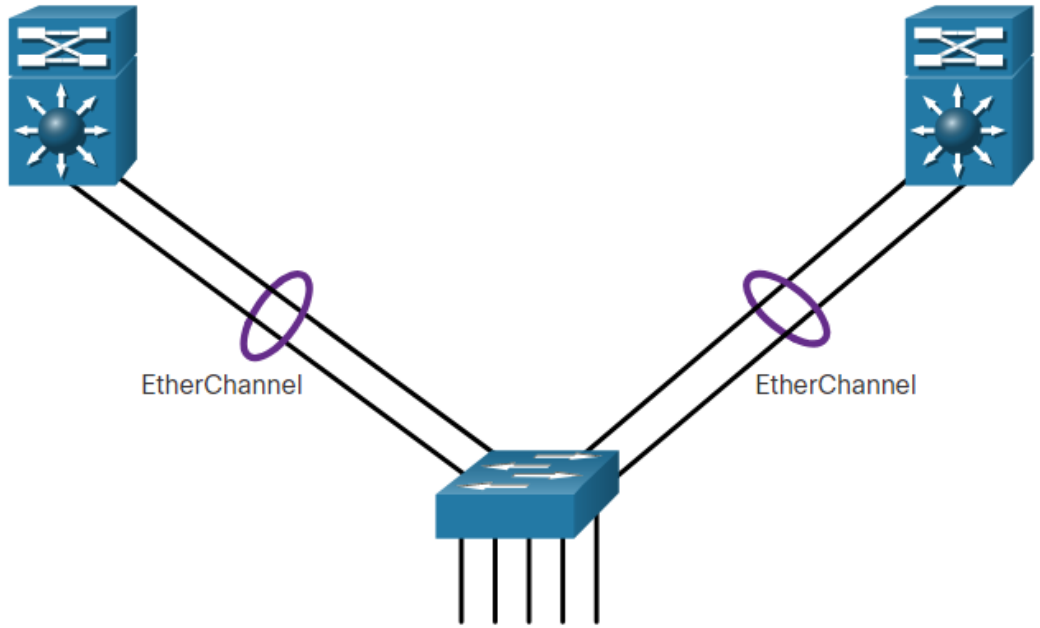
Planification pour la redondance

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



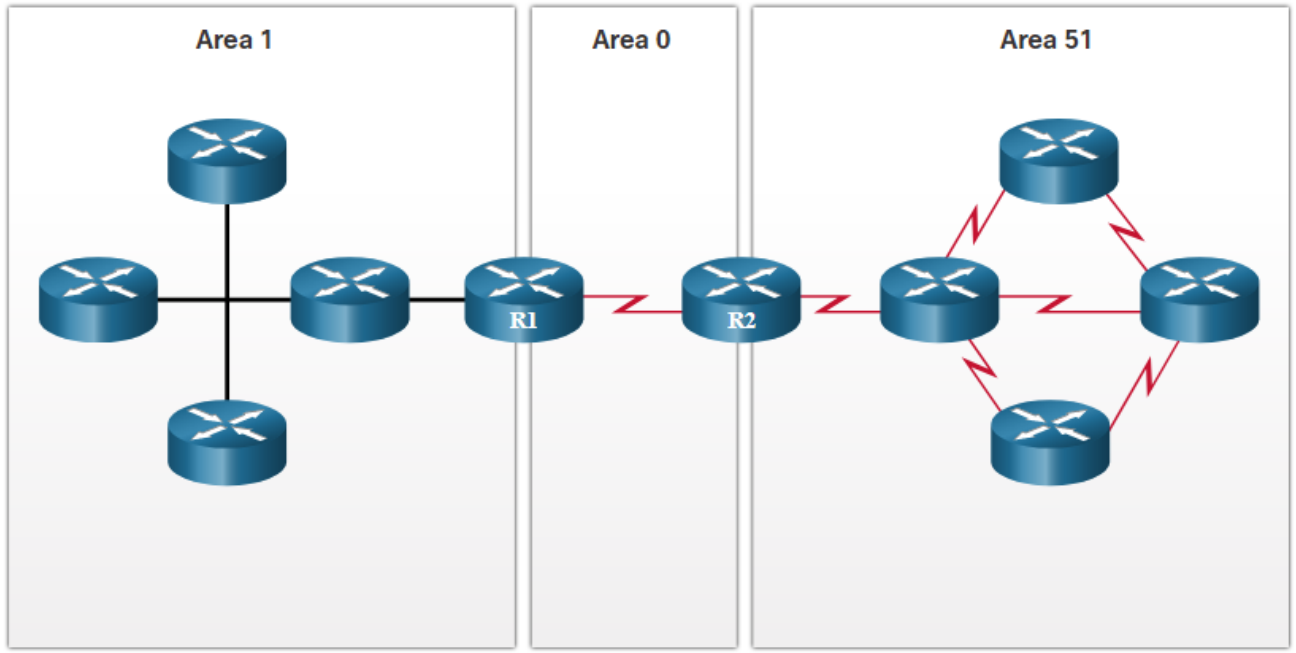
Liens multiples

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.



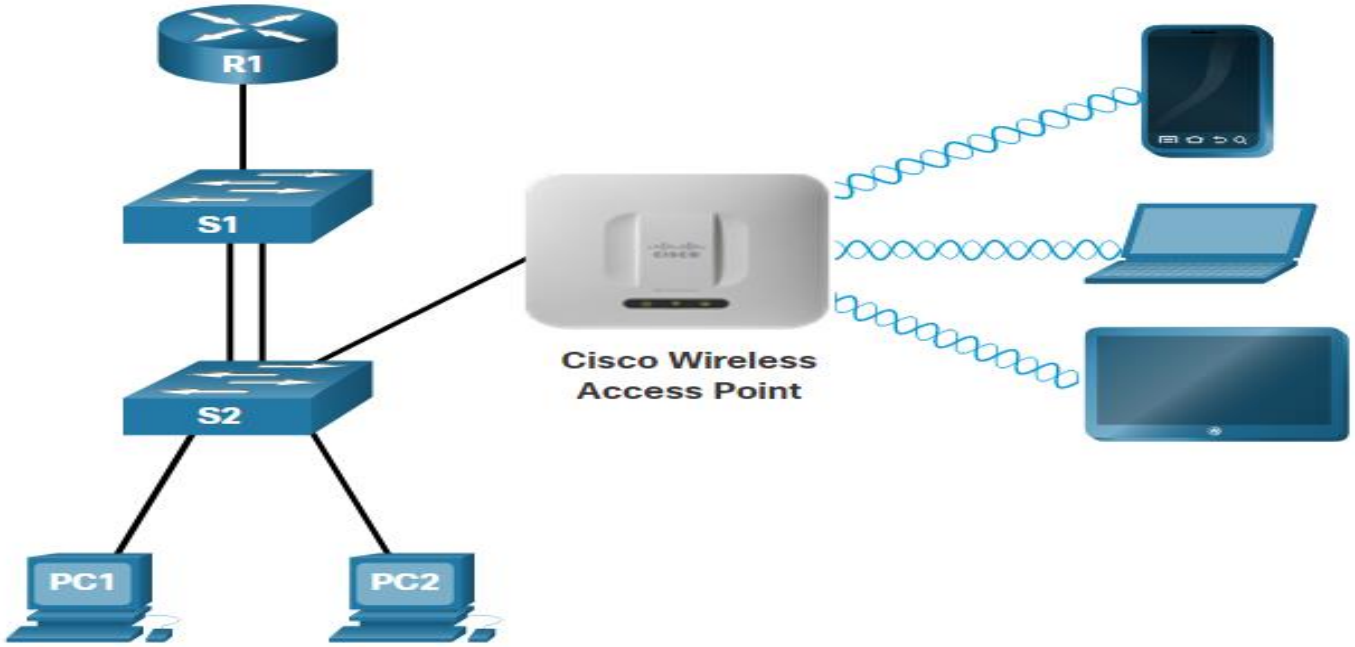
Protocoles de routage évolutif

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



Connectivite sans fil

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

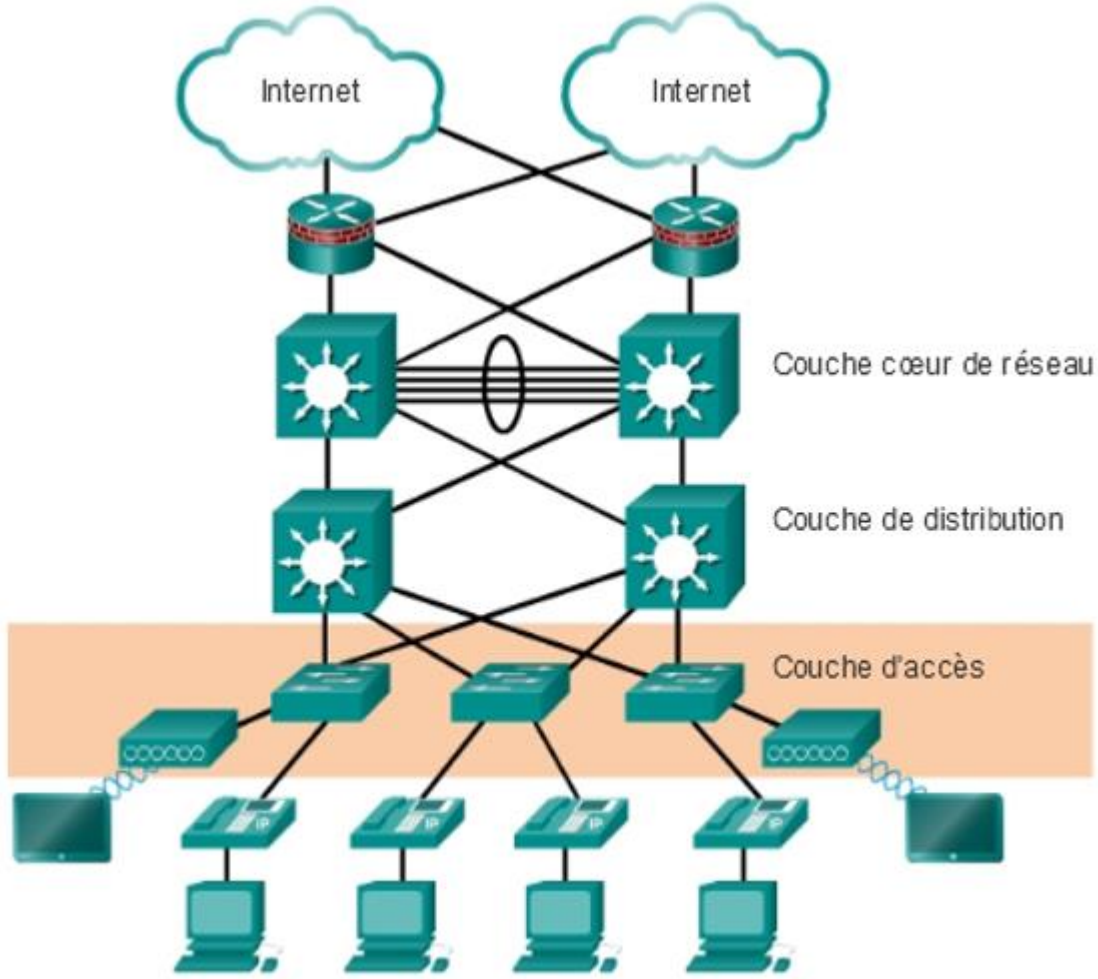


PARTIE 2

Conception hiérarchique

Un réseau bien conçu contrôle le trafic et limite la taille des domaines de défaillance.

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



CHAPITRE 1

Etudier l’évolutivité du réseau

1. Conception de réseau évolutif
2. Sélection des périphériques réseau

Sélection des Plates-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.

- **Commutateurs Cisco**

Les commutateurs LAN Campus (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.

Les commutateurs d'accès géré 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.

Sélection des Plates-formes de commutateur

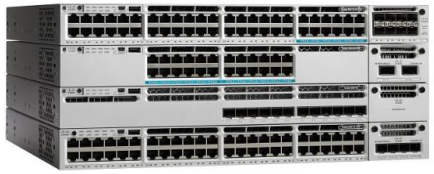
Les commutateurs d'accès Ethernet pour fournisseurs de services apportent surveillance des applications, services unifiés, virtualisation, sécurité intégrée et gestion simplifiée.

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**

Pour sélectionner 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.

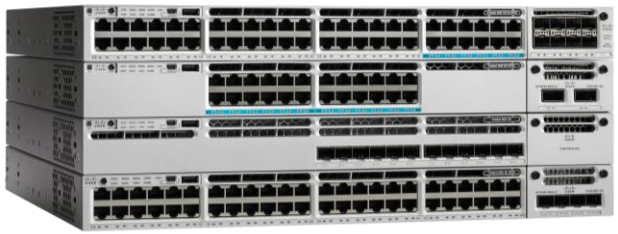
Sélection des Plates-formes de commutateur

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.

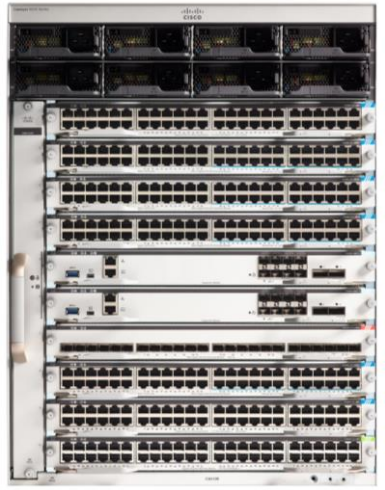
- **Densité du ports**

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.



Sélection des Plates-formes 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.

Sélection 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.

PARTIE 2

Sélection des routeurs

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.

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

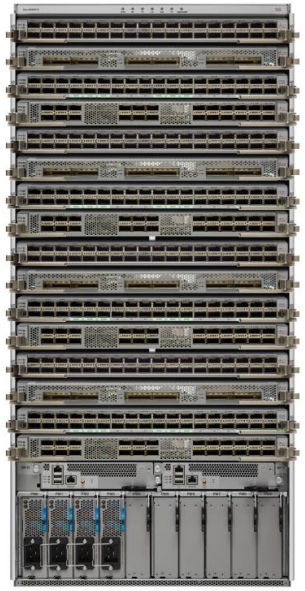
Les routeurs industriels, tels que ceux illustrés dans la figure, sont conçus pour fournir des fonctionnalités de classe entreprise dans des environnements robustes et difficiles. Les routeurs industriels à services intégrés de la série Cisco 1100 sont illustrés.

PARTIE 2

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.

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.



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

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

CHAPITRE 2

Implémenter la redondance dans les réseaux commutés sans boucle

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le fonctionnement du protocole STP
- Configurer le protocole PVST+

2.5 heures

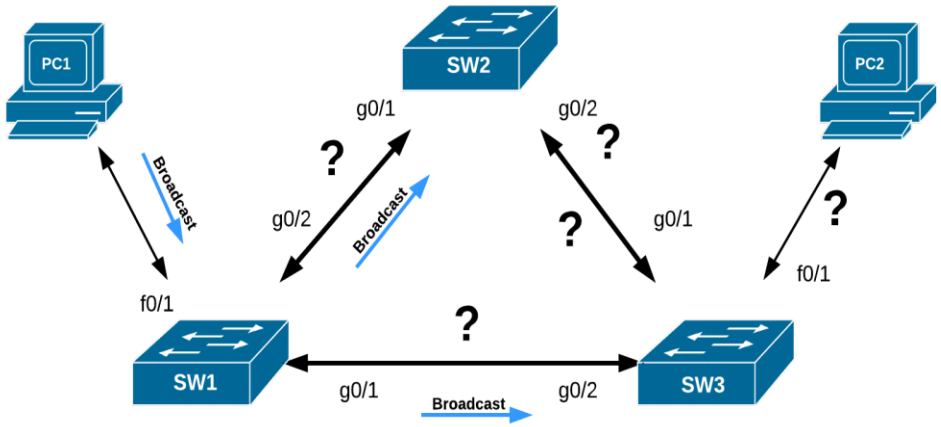
CHAPITRE 2

Implémenter la redondance dans les réseaux commutés sans boucle

1. Concepts du protocole Spanning Tree (STP)
2. Configuration du protocole STP

Redondance dans les réseaux commutés de couche 2

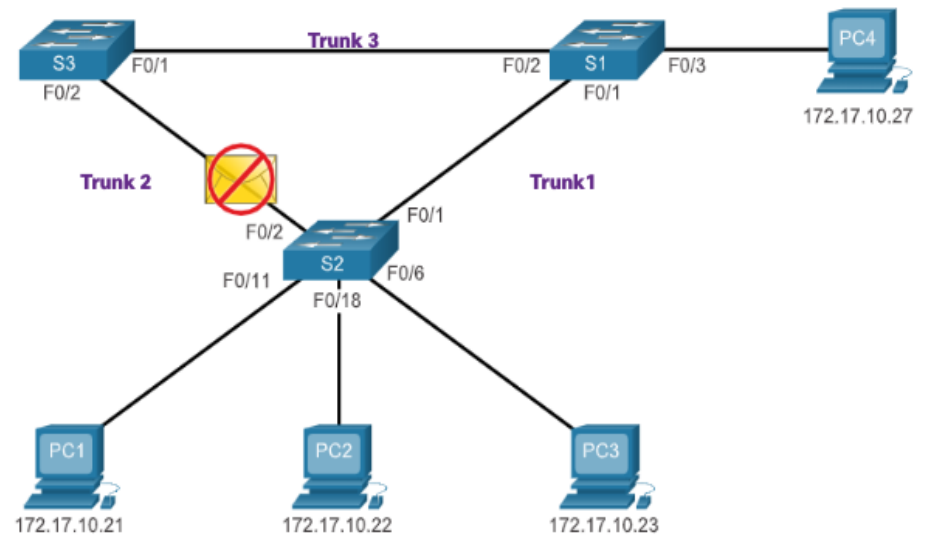
- La redondance est un élément indispensable de la conception hiérarchique pour éviter les points de défaillance uniques et prévenir l'interruption des services de réseau fournis aux utilisateurs.
- Si les réseaux redondants exigent l'ajout de chemins physiques, la redondance logique doit être également intégrée à la conception.
- 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.
- 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.



PARTIE 2

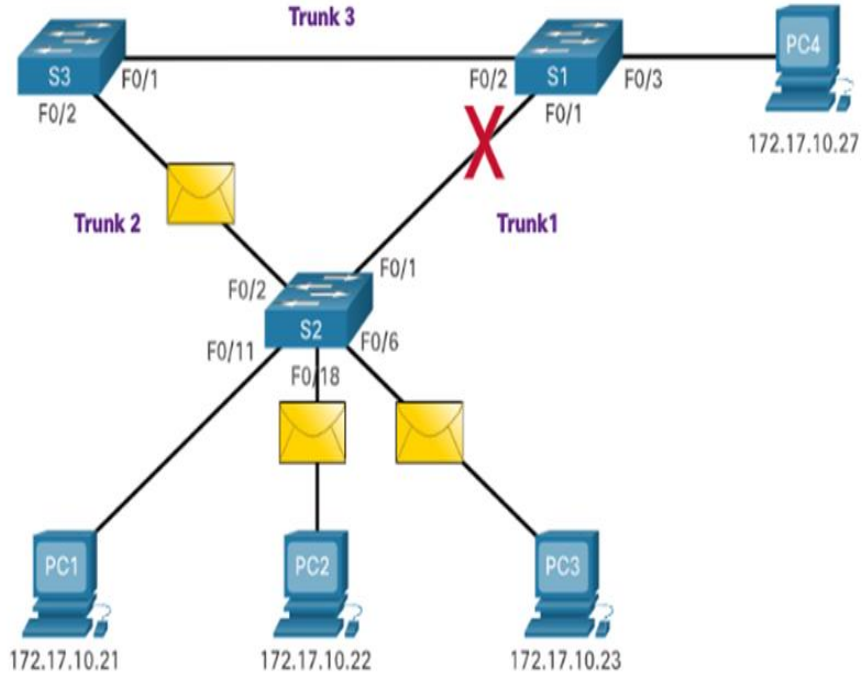
Concepts du protocole Spanning Tree (STP)

- 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.

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



Concepts du protocole Spanning Tree (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.
- Pour empêcher ces problèmes de survenir dans un réseau redondant, un certain type de Spanning Tree doit être activé aux commutateurs.

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.

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

- Sélection d'un pont racine
- Les chemins redondants bloqués
- Créer une topologie sans boucle
- Recalculer en cas de défaillance du

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:

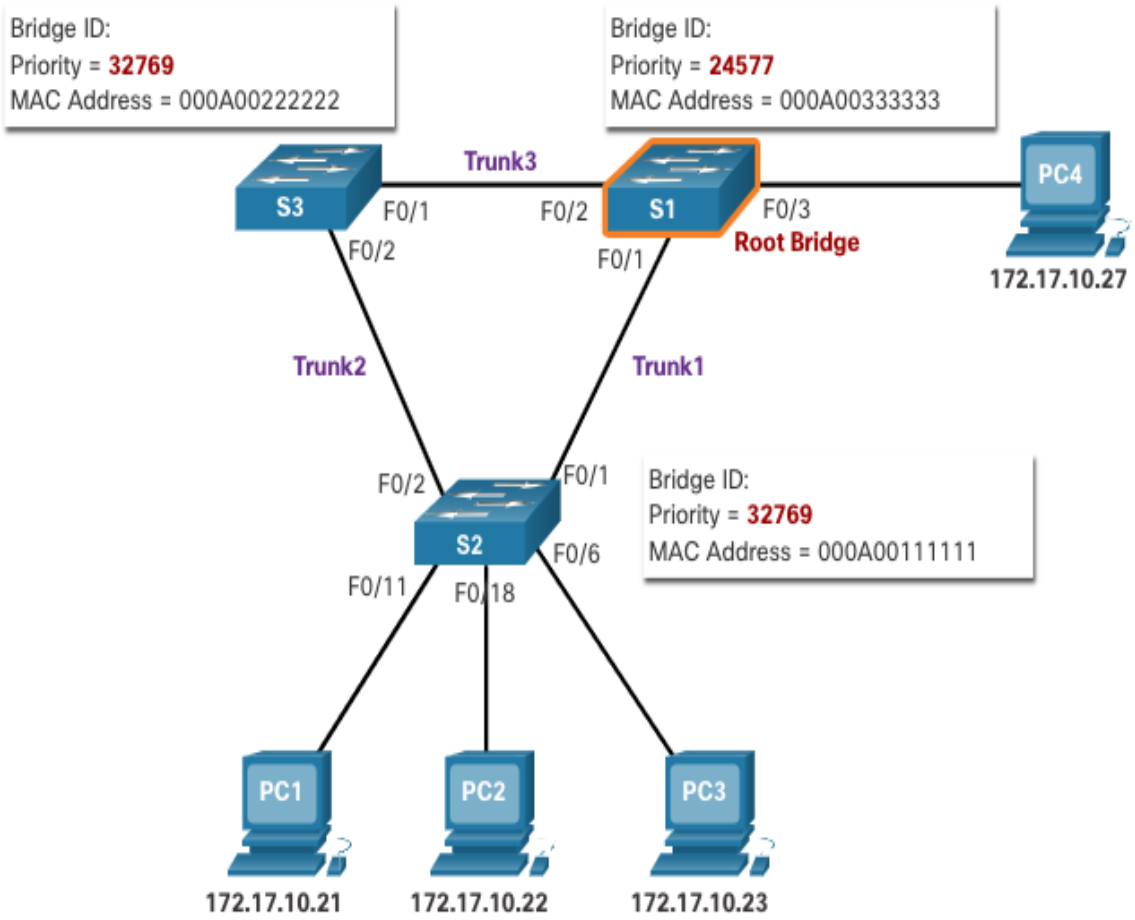
1. **Choisir le pont racine**
2. **Choisir les ports racine.**
3. **Choisir les ports désignés.**
4. **Choisir des ports alternatifs (bloqués).**

- 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.
- **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.

PARTIE 2

1. Choisir le pont 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.



Séquence du BID 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.

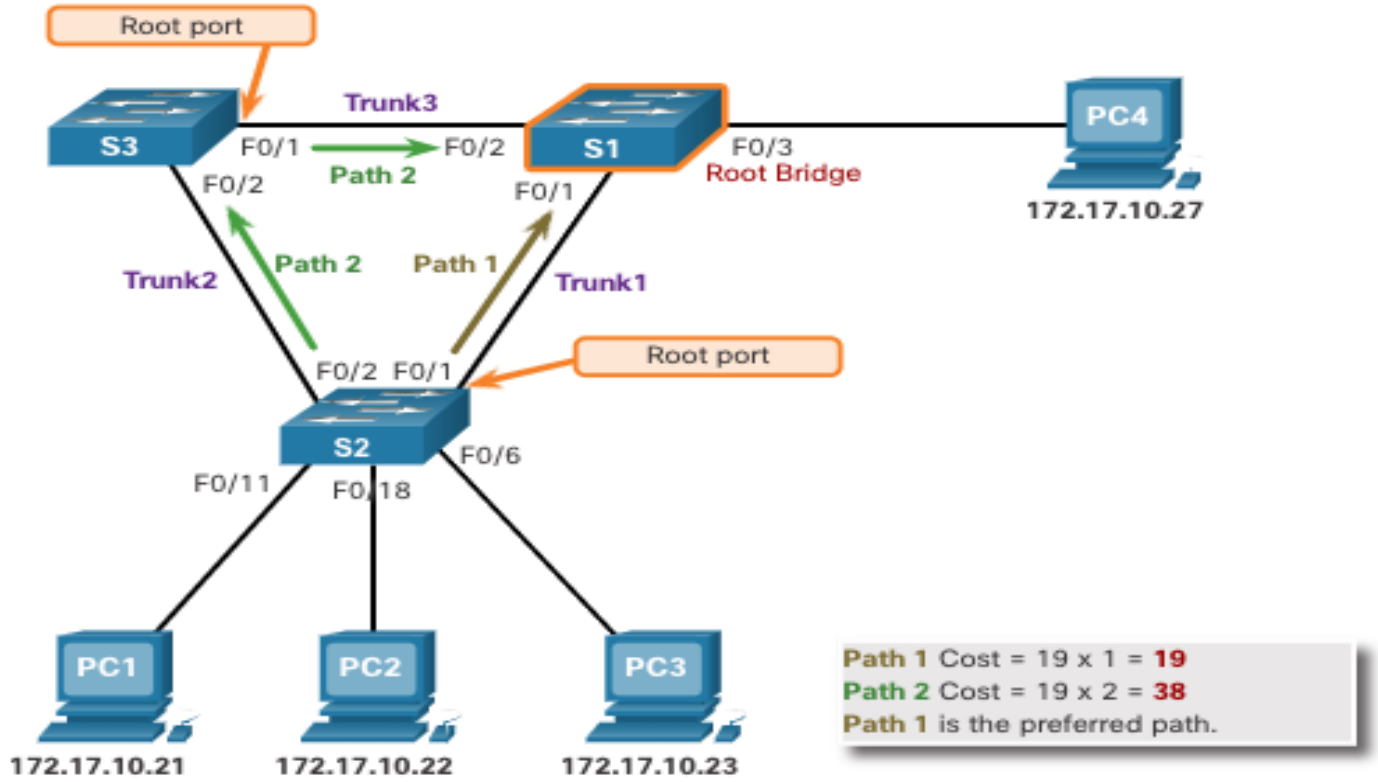
2. Choisir les ports racine

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.

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.

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

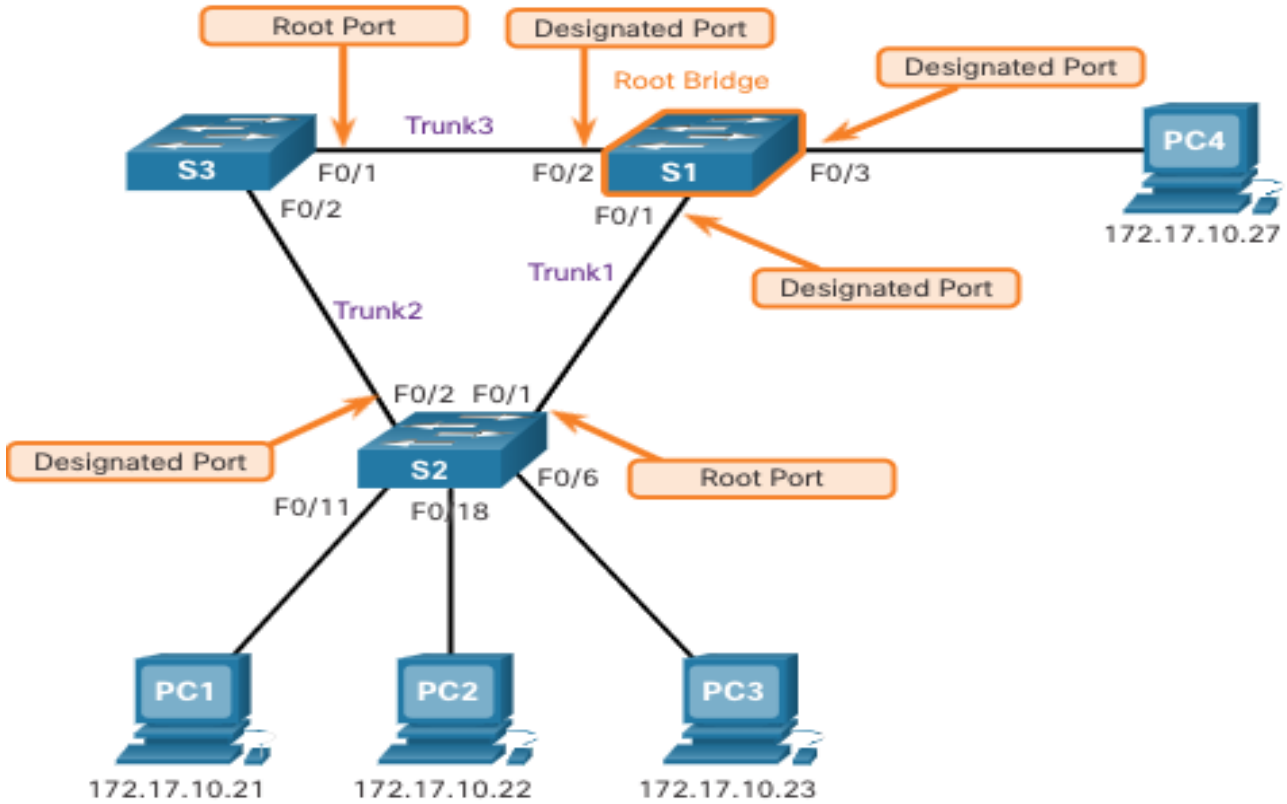


PARTIE 2

PARTIE 2

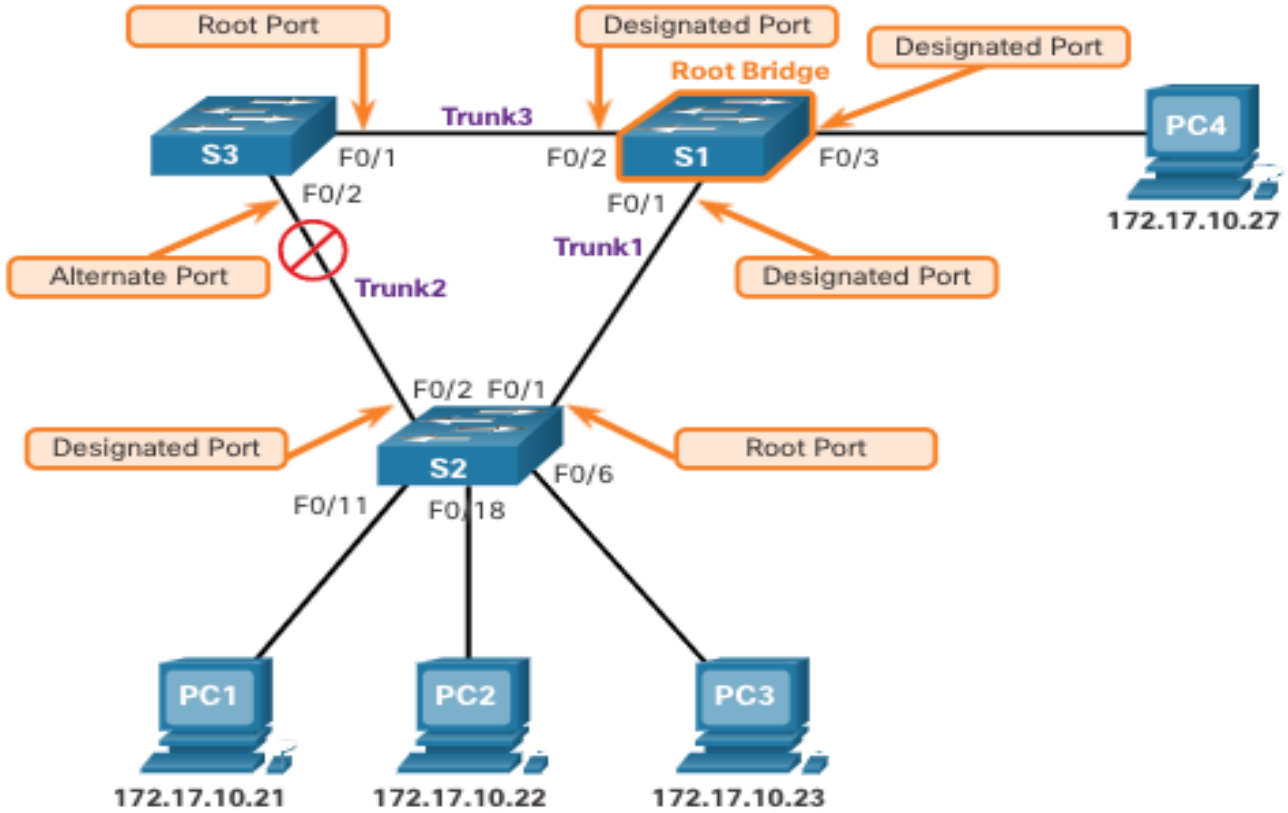
3. Choisir les ports désignés

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.



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.

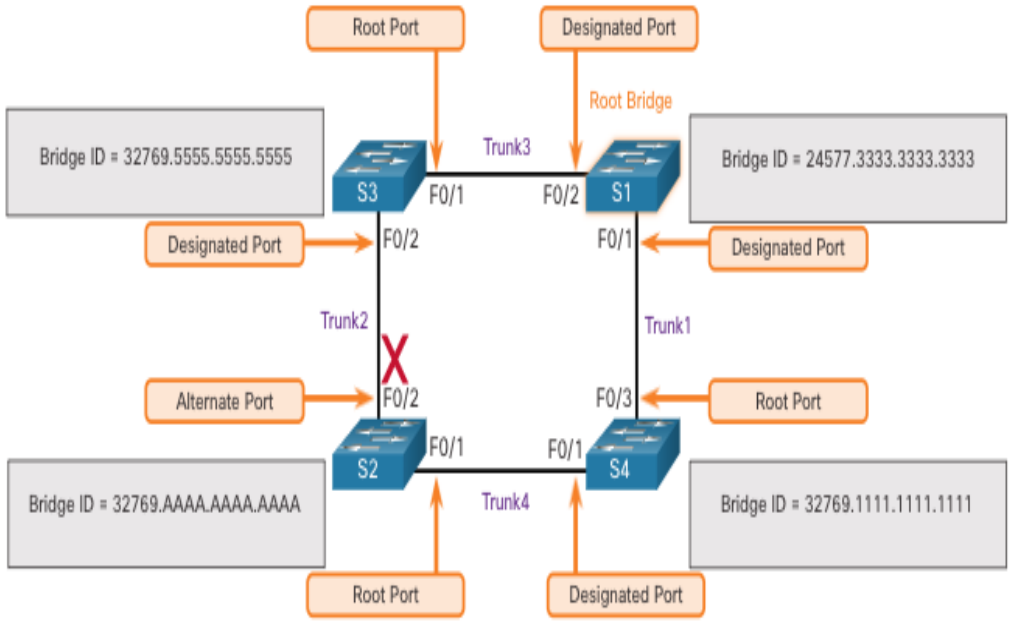


PARTIE 2

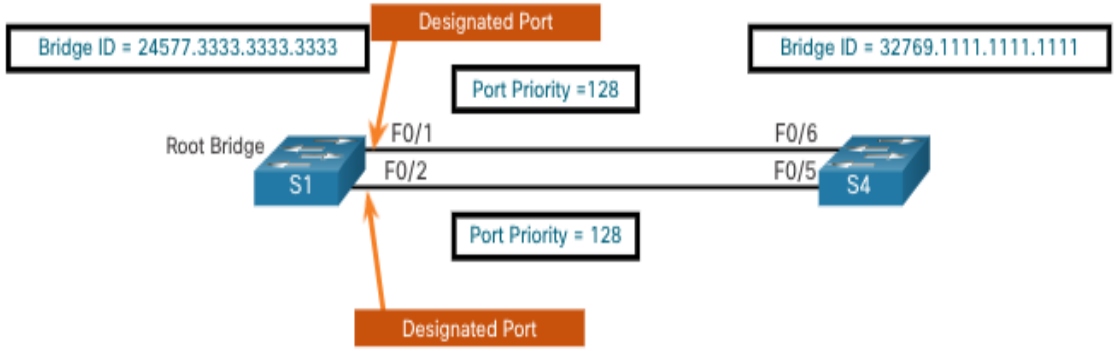
Choisir un port racine à partir de plusieurs chemins d'accès au même coût

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:

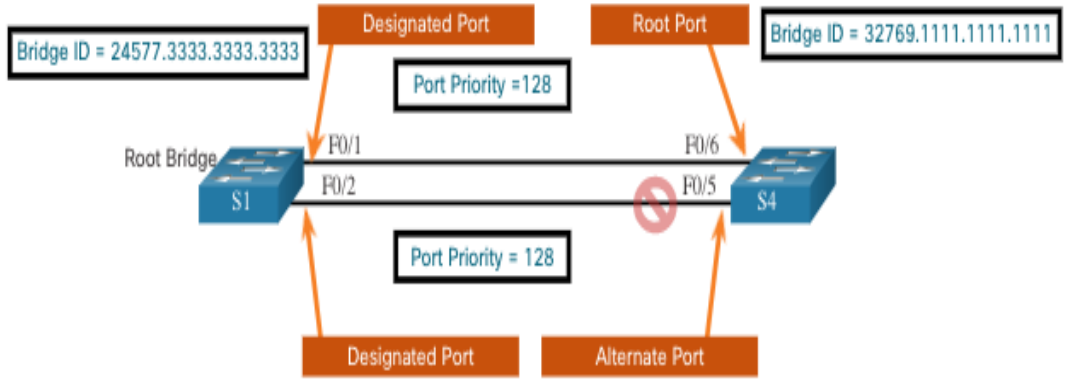
BID d'émetteur le plus faible:



Priorité de port d'émetteur le plus faible:



ID de port d'émetteur le plus faible:

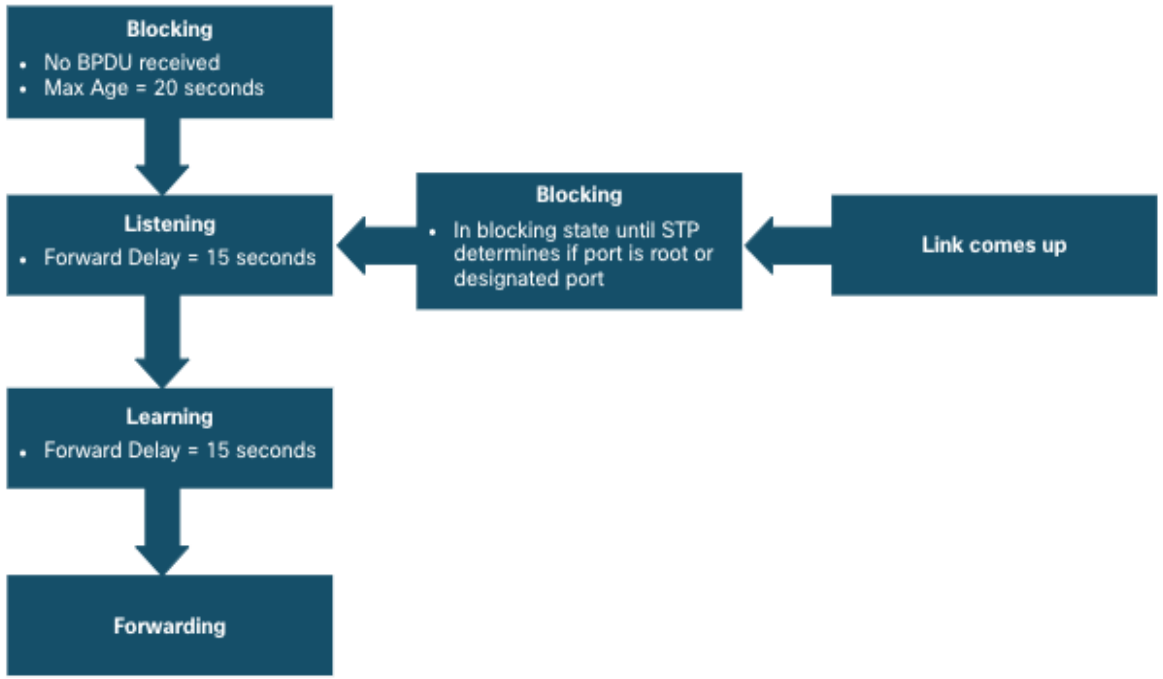


STP minuteurs et les états des ports

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 peut être modifier 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.

.



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

- **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.

Versions du protocole STP

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 inspiré de l'implémentation MISTP plus ancienne de Cisco (Multiple Instance STP). 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.

PARTIE 2

Concepts du protocole RSTP

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.

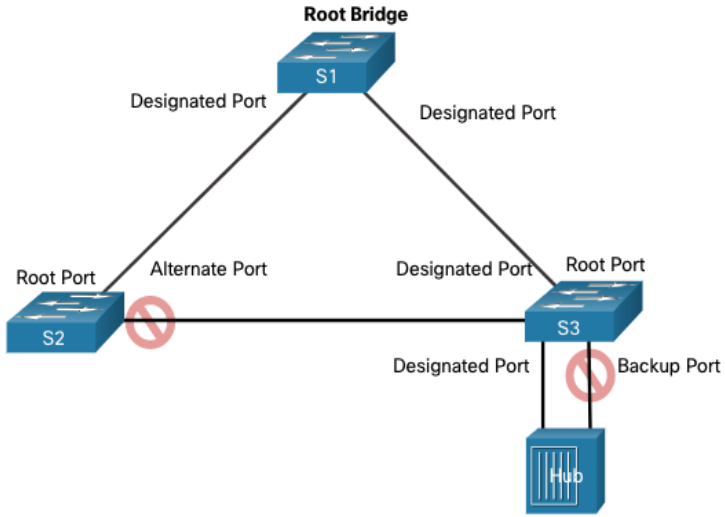
Remarque: Rapid PVST+ est l'implémentation de Cisco du protocole RSTP par VLAN. En utilisant le protocole Rapid PVST+ une instance indépendante s'exécute sur chaque VLAN.

États de port RSTP

STP	RSTP
Disabled	Discarding
Blocking	
Listening	
Learning	Learning
Forwarding	Forwarding

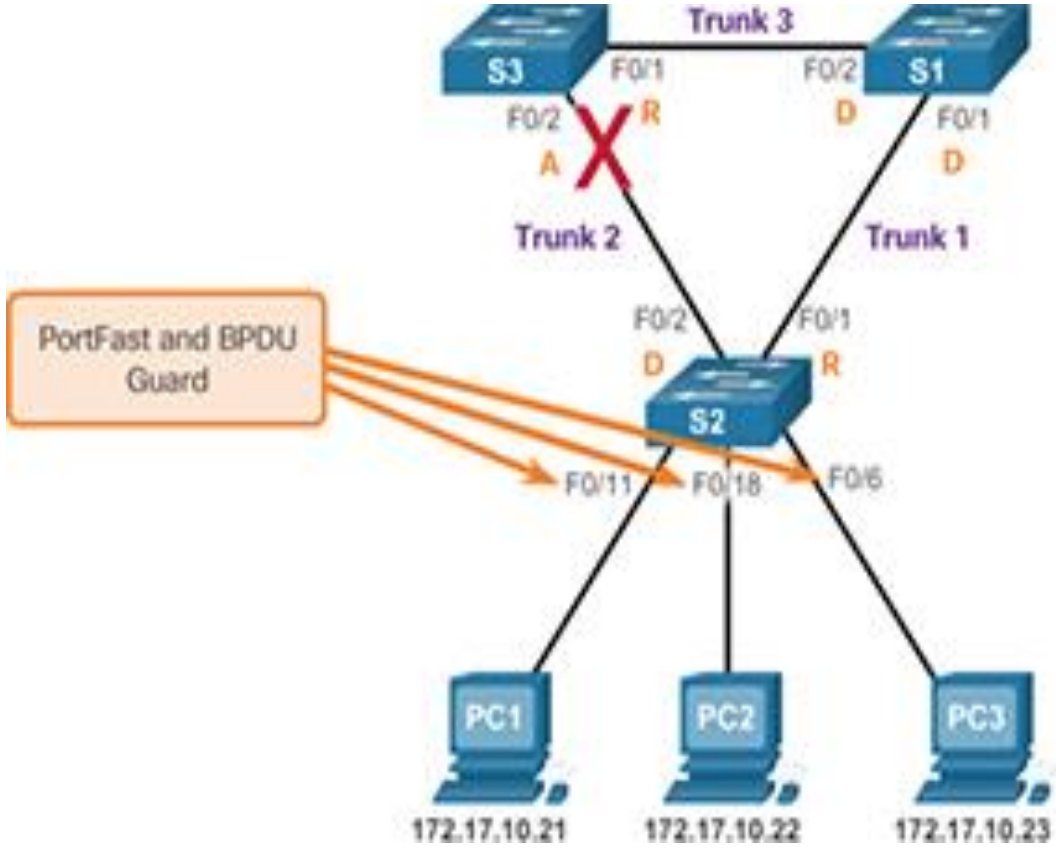
Rôles de port

STP	RSTP
Root Port	Root Port
Designated Port	Designated Port
Blocked Port (Non-Designated Port)	Backup Port
	Alternate Port



PortFast et protection BPDU

- Lorsqu'un port de commutateur est configuré avec **PortFast**, ce port passe immédiatement de l'état de blocage à l'état de transfert. 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.



PARTIE 2

CHAPITRE 2

Implémenter la redondance dans les réseaux commutés sans boucle

1. Concepts du protocole Spanning Tree (STP)
2. Configuration du protocole STP

Commandes de configuration de STP (pvst | mst |rapid-pvst)

Etapes		Description
Etape 1	**configure terminal**	Entrer en mode de configuration globale.
Etape 2	**spanning-tree mode {pvst | mst | rapid-pvst}**	Configurez un mode spanning-tree sur les ports STP du commutateur. • Sélectionnez pvst pour activer PVST+. • Sélectionnez mst pour activer MSTP (et RSTP). Pour plus d'étapes de configuration, reportez-vous au Chapitre 15 « Configuration de MSTP ». • Sélectionnez rapid-pvst pour activer rapid PVST+ (le paramètre par défaut).
Etape 3	**interface** *interface-id*	(Recommandé uniquement pour le mode PVST+ rapide) Spécifiez un port STP à configurer et entrez en mode de configuration de l'interface. Les interfaces valides incluent les ports physiques, les VLAN et les canaux de port. La plage d'ID VLAN est comprise entre 1 et 4094. La plage port-canal est comprise entre 1 et 26.
Etape 4	**spanning-tree link-type point-to-point**	(Recommandé uniquement pour le mode PVST+ rapide) Spécifiez que le type de lien pour ce port est point à point. Si vous connectez ce port à un port distant via une liaison point à point et que le port local devient un port désigné, le commutateur négocie avec le port distant et modifie rapidement le port local à l'état de transfert.
Etape 5	**end**	Repasser en mode d'exécution privilégié.
Etape 6	**clear spanning-tree detected-protocols**	(Recommandé uniquement pour le mode PVST+ rapide) Si un port du commutateur exécutant l'arborescence étendue est connecté à un port d'un commutateur IEEE 802.1D hérité, redémarrez le processus de migration de protocole sur l'ensemble du commutateur. Cette étape est facultative si le commutateur désigné détecte que ce commutateur exécute rapidement PVST+.
Etape 7	**show spanning-tree summary** and **show spanning-tree interface** *interface-id*	Vérifier les entrées
Etape 8	**copy running-config startup-config**	(Facultatif) Enregistrer les entrées dans le fichier de configuration.

Commandes de configuration de PVST+

Configurez et vérifiez le protocole rapid-PVST+ :

Tâche	Commande IOS
Passez en mode de configuration globale.	Switch# **configure terminal**
Configurer le mode d'arbre recouvrant du protocole rapid PVST+..	Switch(config)# **spanning-tree mode rapid-pvst**
Passez en mode de configuration d'interface.	Switch(config)# **interface** *interface-id*
Choisissez un VLAN natif autre que le VLAN 1.	Switch(config-if)# **spanning-tree link-type point-to-point**
Indiquez la liste des VLAN autorisés sur la liaison trunk.	Switch(config-if)# **switchport trunk allowed vlan** *vlan-list*
Repassez en mode d'exécution privilégié.	Switch(config-if)# **end**
Désactiver tous les protocoles STP détectés.	Switch# **clear spanning-tree detected-protocols**
Vérifier la configuration du protocole Rapid PVST+.	Switch# **show spanning-tree** *interface_id*

CHAPITRE 3

Configurer l'agrégation des liaisons

Ce que vous allez apprendre dans ce chapitre :

- Configurer l'agrégation des liaisons avec ETHERCHANNEL

1 heures

CHAPITRE 3

Configurer l'agrégation des liaisons

1. Fonctionnement d'EtherChannel
2. Configuration d’EtherChannel

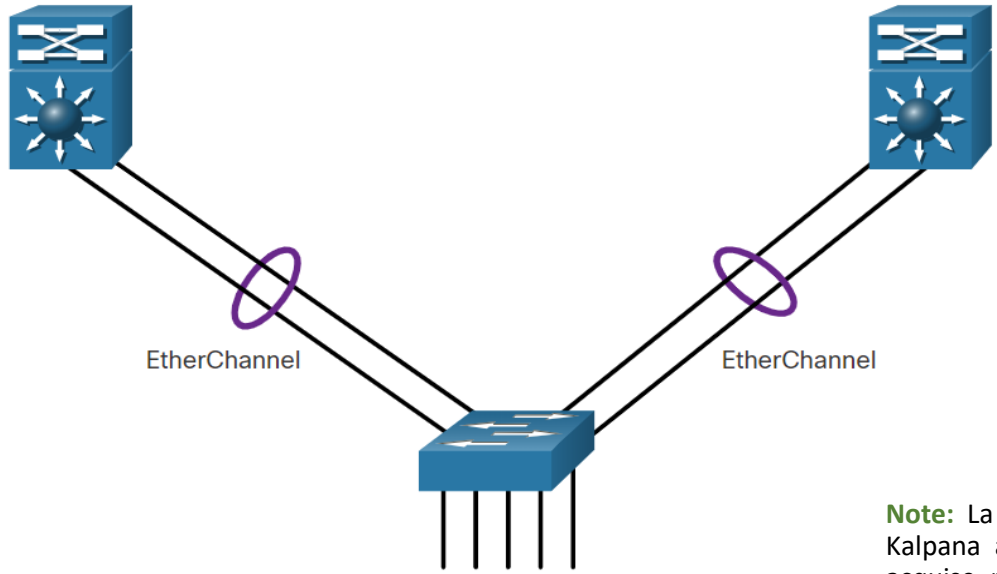
PARTIE 2

Technologie EtherChannel

EtherChannel est une technologie d'agrégation de liens qui permet d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique.

Le but est d'augmenter la vitesse et la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs. Elle permet de simplifier une topologie Spanning-Tree en diminuant le nombre de liens.

EtherChannel est principalement utilisé sur la dorsale du réseau local, dans le "switch block" entre la couche Access et Distribution, mais on peut aussi l'utiliser pour connecter des postes d'utilisateurs, des serveurs.



Note: La technologie EtherChannel a été inventée par la société Kalpana au début des années 1990. Cette société a ensuite été acquise par Cisco Systems en 1994. En 2000, l'IEEE a publié le standard 802.3ad, qui est une version ouverte de EtherChannel.

Technologie EtherChannel

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.
- 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.
- EtherChannel offre de la redondance car 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 différentes ne peuvent pas être associés.
- Actuellement, chaque EtherChannel peut être composé de huit ports Ethernet maximum, configurés pour être compatibles.
- 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.
- Une configuration appliquée à l'interface de canal de port affecte toutes les interfaces physiques attribuées à cette interface.

Protocole de négociation automatique

Des EtherChannels 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.

PAgP : (prononcé "Pag - P") est un protocole propriétaire de Cisco qui aide à la création automatique de liens EtherChannel.

LACP : fait partie d'une spécification IEEE (802.3ad) qui permet de regrouper plusieurs ports physiques pour former un seul canal logique. 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.

```
(config-if-range)#channel-group 1 mode ?
  active     Enable LACP unconditionally
  auto       Enable PAgP only if a PAgP device is detected
  desirable  Enable PAgP unconditionally
  on         Enable Etherchannel only
  passive    Enable LACP only if a LACP device is detected
```

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

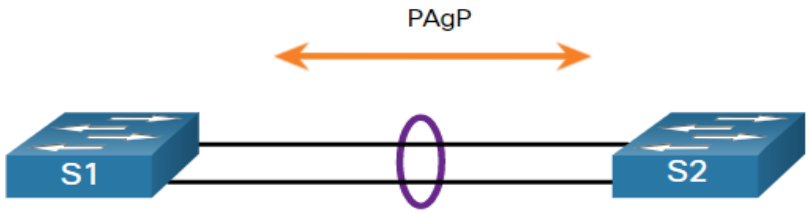
PARTIE 2

Fonctionnement de PAgP

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.

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.

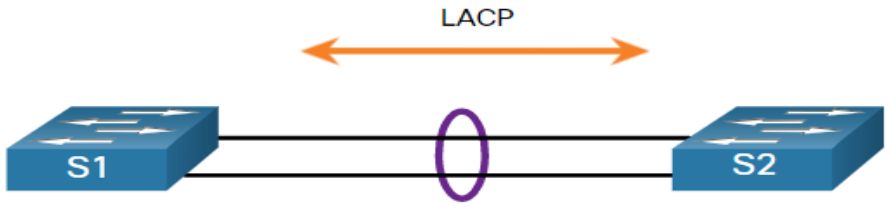
S1	S2	Établissement de canal
On (activé)	Allumé	Oui
On	Desirable/Auto	Non
Desirable	Desirable	Oui
Desirable	Auto	Oui
Auto	Desirable	Oui
Auto	Auto	Non

Fonctionnement de LACP

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

CHAPITRE 3

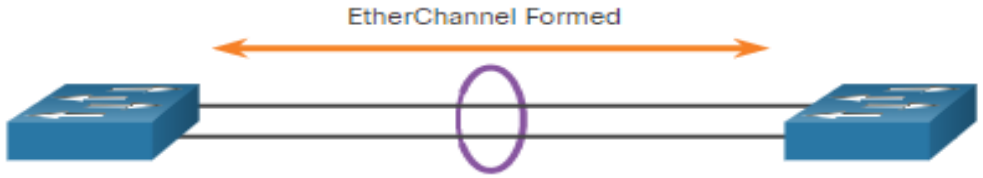
Configurer l'agrégation des liaisons

1. Fonctionnement d'EtherChannel
2. Configuration d’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'l'EtherChannel.
- **VLAN correspondant** - Toutes les interfaces d'une liaison EtherChannel doivent être attribuées au même VLAN, ou être configurées en tant que trunk.
- **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** .



S1 Port Configurations	
Speed	1 Gbps
Duplex	Full
VLAN	10

S2 Port Configurations	
Speed	1 Gbps
Duplex	Full
VLAN	10

PARTIE 2

Vérification et dépannage d'un EtherChannel

- **Configuration d'EtherChannel**

On configure l'EtherChannel sur une ou groupe d'interfaces avec la commande suivante : **channel-groupe** *number* **mode** *mode*

```
Switch(config)# interface range fa0/1 – 4 {we can use the range or single interface}
Switch(config-if-range)# channel-group [1 – 6] mode [auto | desirable | on | active | passive]
```

- **Vérification d'EtherChannel**

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.

```
Switch# show interface etherchannel
Switch# show etherchannel [summary | port | load-balance | port-channel | detail]
Switch# show [pagp | lacp ] neighbors
```

CHAPITRE 4

Comprendre le concept du FHRP

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le fonctionnement des protocoles FHRP
- Configurer le protocole HSRP

1 heures

CHAPITRE 4

Comprendre le concept du FHRP

1. Protocoles de redondance au premier saut
2. Fonctionnement et configuration du protocole HSRP

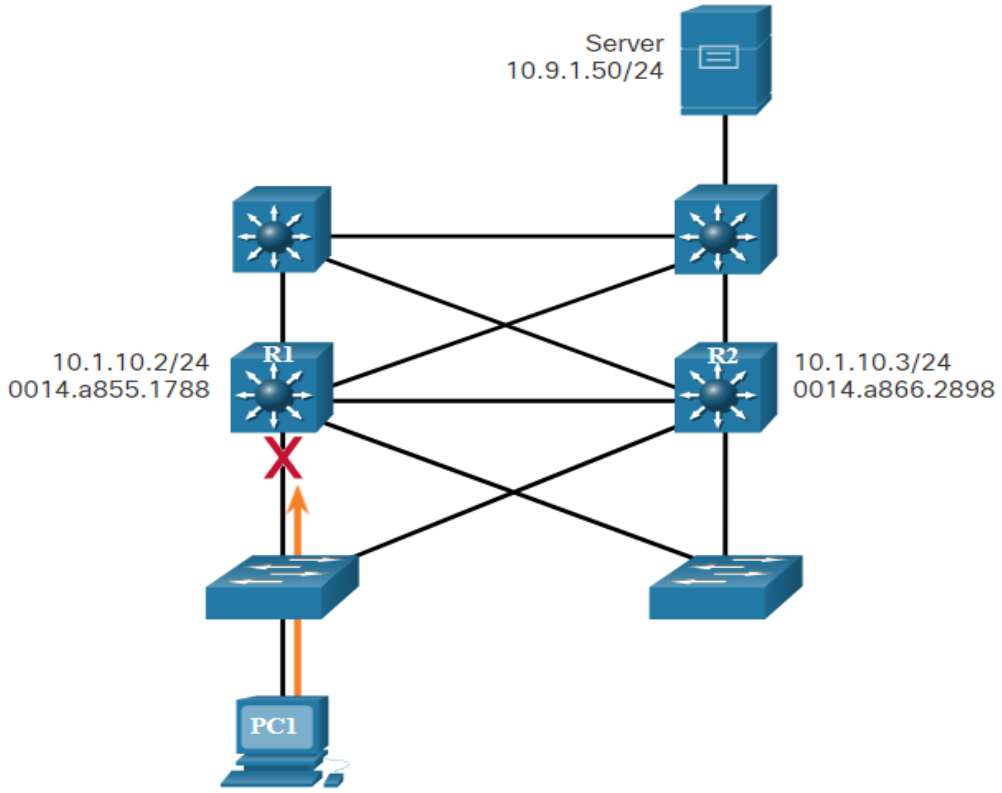
PARTIE 2

Limitations de la passerelle par défaut

Les périphériques finaux sont généralement configurés avec une adresse IPv4 unique pour une passerelle par défaut.

- Si l'interface passerelle-routeur par défaut tombe en panne, les hôtes du réseau local perdent leur connectivité à l'extérieur du réseau.
- Cela se produit même si un routeur redondant ou un commutateur de couche 3 qui pourrait servir de passerelle par défaut existe.

Les protocoles de redondance de premier saut **(FHRP)** sont des mécanismes qui fournissent des passerelles alternatives par défaut dans les réseaux commutés où deux ou plusieurs routeurs sont connectés aux mêmes VLANs.

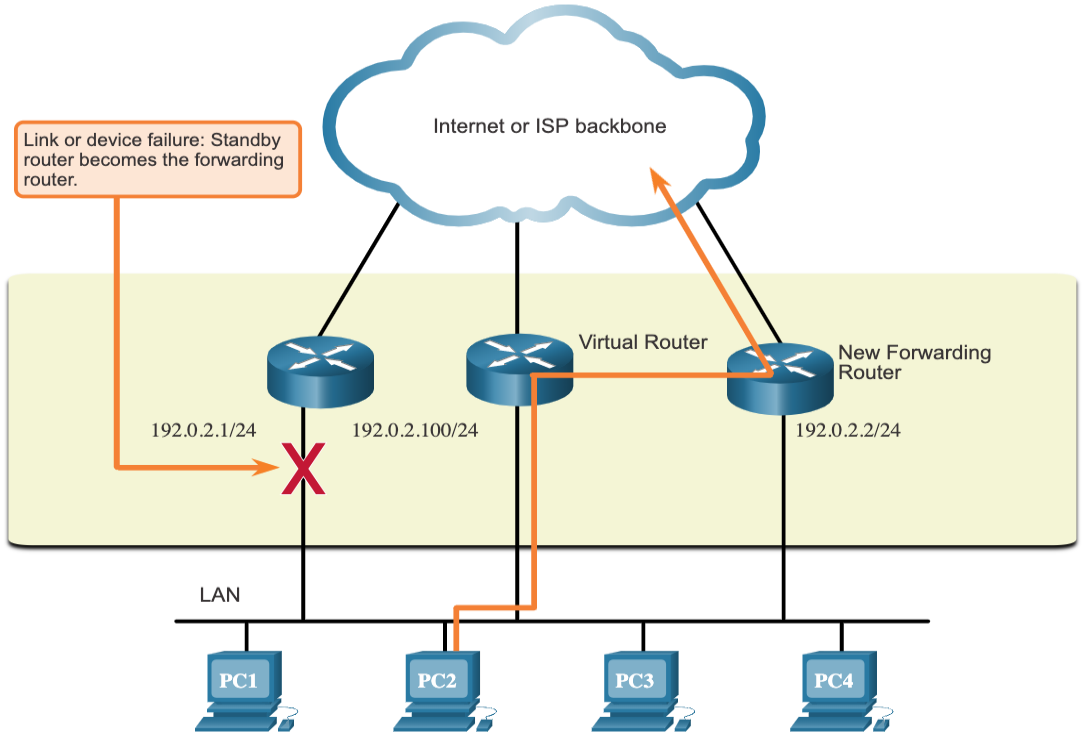


Étapes du basculement d'un routeur

Lorsque le routeur actif tombe en panne, le protocole de redondance fait passer le routeur de réserve au nouveau rôle de routeur actif, comme le montre la figure.

Voici la procédure en cas de défaillance du routeur actif:

1. Le routeur de secours cesse de voir les messages Hello du routeur de transfert.
2. Le routeur de secours assume le rôle du routeur de transfert.
3. Étant donné que le nouveau routeur de transfert assume à la fois le rôle de l'adresse IPv4 et celui de l'adresse MAC du routeur virtuel, aucune interruption de service n'est constatée au niveau des périphériques hôtes.



Options FHRP

Les protocoles de redondance du premier saut (passerelle par défaut) sont les suivants : **HSRP**, **VRRP** et **GLBP.**

Options FHRP	Description
Protocole HSRP (Hot Standby Router Protocol)	Le Protocole HSRP (Hot Standby Router Protocol) est un protocole FHRP propriétaire de Cisco, conçu pour permettre le basculement transparent d'un périphérique IPv4 au premier saut.
HSRP pour IPv6	Il s'agit d'un FHRP propriétaire de Cisco qui offre les mêmes fonctionnalités que le HSRP, mais dans un environnement IPv6.
Protocole de redondance des routeurs virtuels version 2 (VRRPv2)	Il s'agit d'un protocole d'élection non propriétaire qui attribue dynamiquement la responsabilité d'un ou plusieurs routeurs virtuels aux routeurs VRRP sur un réseau local IPv4.
Le protocole VRRPv3	Il s'agit d'un protocole qui offre la capacité de prendre en charge les adresses IPv4 et IPv6. Le VRRPv3 fonctionne dans des environnements multi-fournisseurs et est plus évolutif que le VRRPv2.
Protocole d'équilibrage de charge de la passerelle (GLBP)	Il s'agit d'un FHRP propriétaire de Cisco qui protège le trafic de données d'un routeur ou d'un circuit défaillant, comme le HSRP et le VRRP, tout en permettant l'équilibrage de la charge (également appelé partage de la charge) entre un groupe de routeurs redondants.
GLBP pour IPv6	Il s'agit d'un FHRP propriétaire de Cisco qui offre les mêmes fonctionnalités que le GLBP, mais dans un environnement IPv6.
Protocole IRDP (ICMP Router Discovery Protocol)	Spécifié dans la RFC 1256, IRDP est une solution FHRP héritée. Le protocole IRDP permet aux hôtes IPv4 de localiser les routeurs offrant une connectivité IPv4 à d'autres réseaux IP (non locaux).

PARTIE 2

Options FHRP

La comparaison entre les protocoles de redondance du premier saut (passerelle par défaut) suivants : **HSRPv1, HSRPv2**, **VRRP** et **GLBP.**

	HSRPv1	HSRPv2	VRRP	GLBP
Propriétaire	Cisco		IEEE	Cisco
Supporte	IPv4		IPv4/IPv6	
IP	224.0.0.2	224.0.0.102	224.0.0.18	224.0.0.102
Port UDP	1985	2029	112	3222
Mac Virtuelle	0000-0C07-AcXX	0000-0C9F-FXXX	0000-5E00-01XX	0007-b4XX-XXXX
Groupe	0-255	0-4095	0-254	0-1023
Rôles	Active/Passive		Master/Backup	AVG/AVF
Priorité	100			
Hello Timer	3s		1s	3s
Hold Timer	10s		3,6s	10s
Preempt	Disable		Actif	

CHAPITRE 4

Comprendre le concept du FHRP

1. Protocoles de redondance au premier saut
2. Fonctionnement et configuration du protocole HSRP

PARTIE 2

Fonctionnement du protocole HSRP

Aperçu du HSRP

Le HSRP assure une haute disponibilité du réseau en fournissant une redondance de routage de premier saut pour les hôtes IP sur les réseaux configurés avec une adresse de passerelle IP par défaut.

Il est utilisé dans un groupe de routeurs pour sélectionner un périphérique actif et un périphérique de secours.

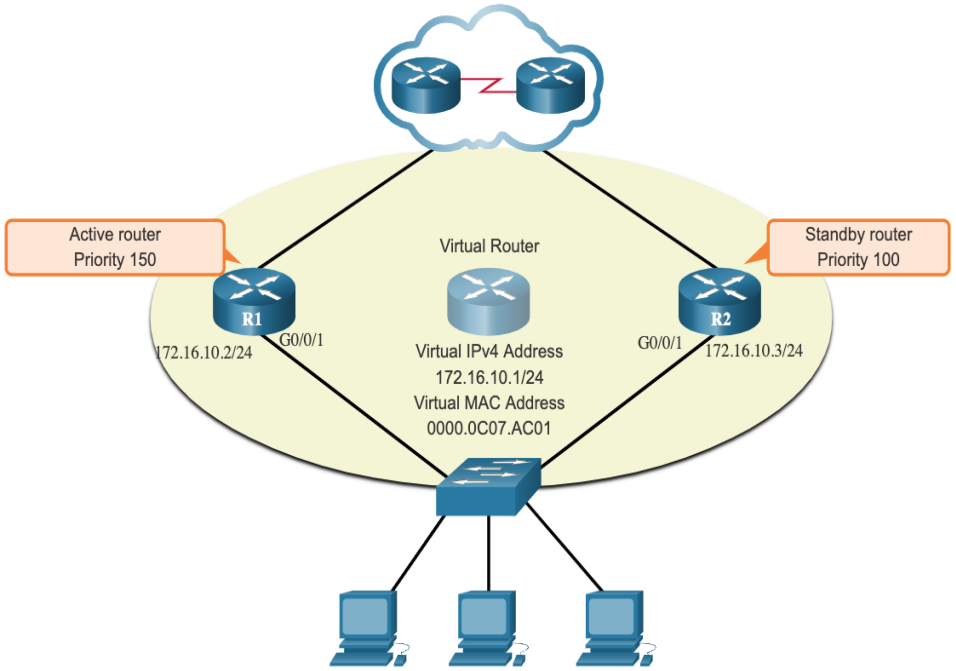
Le périphérique actif est celui qui est utilisé pour le routage des paquets ;

Le périphérique de secours est celui qui prend le relais en cas de défaillance du périphérique actif ou lorsque des conditions prédéfinies sont remplies.

Priorité et préemption HSRP

Le rôle des routeurs actifs et de secours est déterminé lors du processus de sélection de HSRP. Par défaut, le routeur avec l'adresse IPv4 la plus élevée devient le routeur actif.

- Il est possible d'utiliser la priorité HSRP pour déterminer le routeur actif.
- Le routeur associé à la priorité HSRP la plus élevée devient le routeur actif.
- La valeur par défaut de la priorité HSRP est 100.
- Si les priorités sont identiques, le routeur avec l'adresse IPv4 la plus élevée devient le routeur actif.
- Pour configurer un routeur comme étant le routeur actif, utilisez la commande **standby priority** . La plage de priorité HSRP va de 0 à 255.
- Pour forcer un nouveau processus d'élection du HSRP à avoir lieu lorsqu'un routeur de plus haute priorité est mis en ligne, la préemption doit être activée à l'aide de la commande de l'interface **standby preempt** .



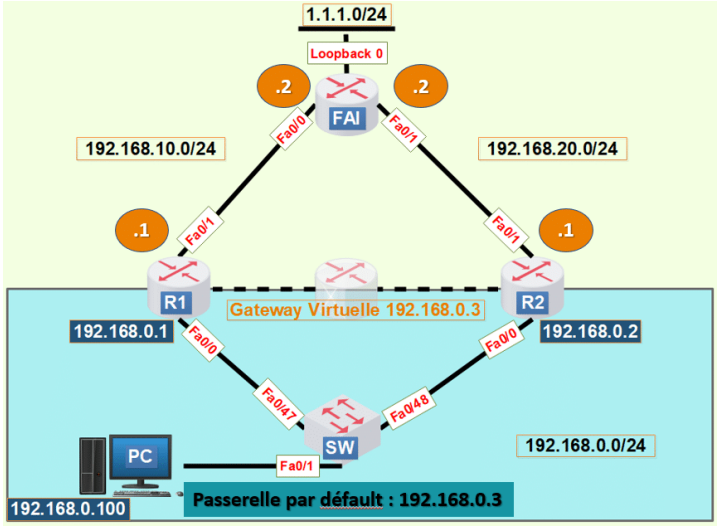
États et temps de la HSRP

- Par défaut, les routeurs actif et de secours envoient des paquets **Hello** à l'adresse de multidiffusion du groupe HSRP toutes les 3 secondes.
- Le routeur de secours (standby) prend la main s'il ne reçoit pas un **message Hello** du routeur actif après **10 secondes**.
- Vous pouvez diminuer ces délais pour accélérer le basculement ou la préemption.
- Pour éviter une utilisation accrue du CPU et des changements inutiles d'état de secours (standby), ne réglez pas la minuterie d'accueil en dessous de **1 seconde** ou la minuterie d'attente en dessous de **4 secondes**.

États HSRP	Description
Initial	État initial lorsqu'une interface devient disponible pour la première fois ou qu'un changement de configuration a lieu.
Apprendre	Le routeur n'a pas encore appris son adresse IP virtuelle, ni reçu de messages « hello » du routeur actif. Il est en attente d'un message du routeur actif.
Écouter	Le routeur connait son adresse IP virtuelle, mais n'est ni le routeur actif, ni le routeur de secours. Il attend un message de ceux-ci.
Parler	Le routeur envoie des messages « hello » périodiques et participe activement à la sélection du routeur actif et/ou du routeur de secours (standby).
En attente (secours)	Le routeur est candidat pour devenir le prochain routeur actif et envoie des messages « hello » périodiques.

PARTIE 2

Configuration du protocole HSRP/VRRP/GLBP



HSRP : Hot Standby Router Protocol	VRRP : Virtual Router Redundancy Protocol	GLBP : Gateway Load Balancing Protocol
R1(config)#interface fa0/0 R1(config-if)#standby 1 ip 192.168.1.3	R1(config)#interface fa0/0 R1(config-if)#vrrp 1 ip 192.168.1.3	R1(config)#interface fa0/0 R1(config-if)#glbp 1 ip 192.168.1.3
R2(config)#interface fa0/0 R2(config-if)#standby 1 ip 192.168.1.3	R2(config)#interface fa0/0 R2(config-if)#vrrp 1 ip 192.168.1.3	R2(config)#interface fa0/0 R2(config-if)#glbp 1 ip 192.168.1.3
R1(config-if)#standby 1 priority 150	R1(config-if)#vrrp 1 priority 150	R1(config-if)#glbp 1 priority 150
R1(config-if)#standby 1 preempt	R1(config-if)#vrrp 1 preempt	R1(config-if)#glbp 1 preempt

GLBP fait de **l'équilibrage de charge**, basé sur un **système de poids par membre.**

```
R1(config-if)#glbp 1 load-balancing round-robin | weighted | host-dependant
```

PARTIE 3

Mettre en œuvre les protocoles de configuration dynamique

Dans ce module, vous allez :

- Être capable de configurer les services d'attribution automatique des adresses IPv4 et IPv6

3 heures

CHAPITRE 1

Comprendre le fonctionnement de DHCPv4

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le fonctionnement de DHCPv4

1 heures

CHAPITRE 1

Comprendre le fonctionnement de DHCPv4

1. Fonctionnement de DHCPv4

Concepts 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.
- le protocole DHCPv4 offre un gain de temps extrêmement précieux aux administrateurs réseau.
- 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. 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

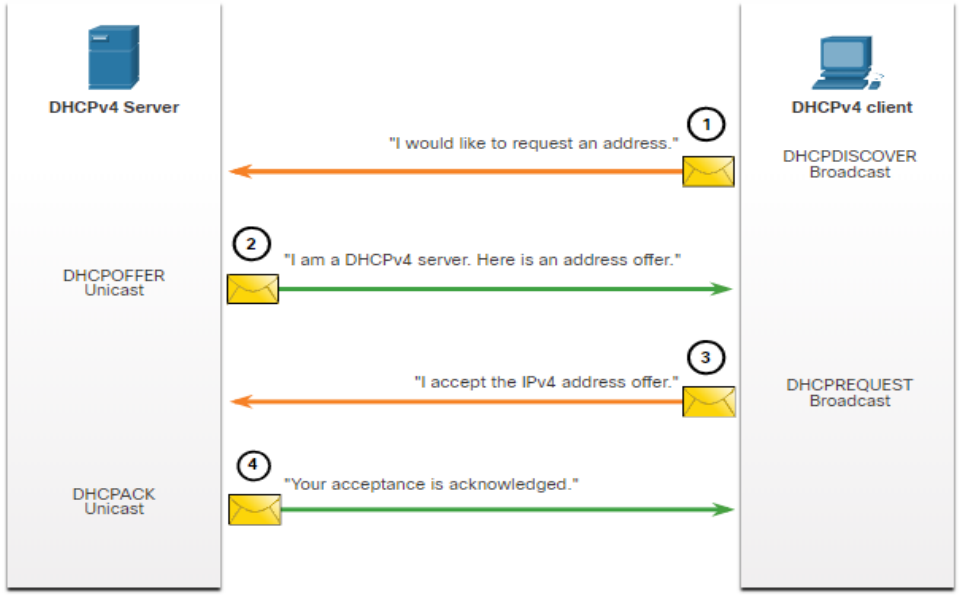
DHCPv4 fonctionne en mode client/serveur. Lorsqu'un client communique avec un serveur DHCPv4, le serveur attribue ou loue une adresse IPv4 à ce client.

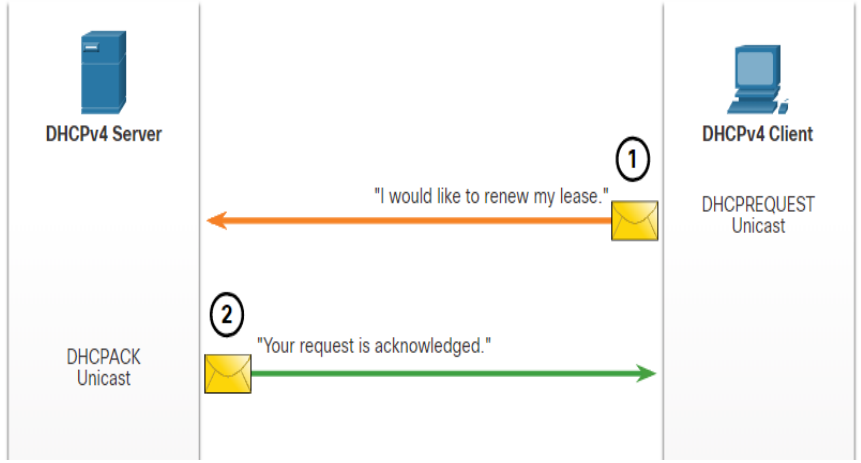
- Le client se connecte au réseau avec cette adresse IPv4 louée jusqu'à l'expiration du bail. Le client doit régulièrement contacter le serveur DHCP pour renouveler le bail.
- Ce mécanisme de bail permet de s'assurer que les clients qui sont déplacés ou qui sont mis hors tension ne conservent pas des 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.

Étapes 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)**





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.

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.

PARTIE 3

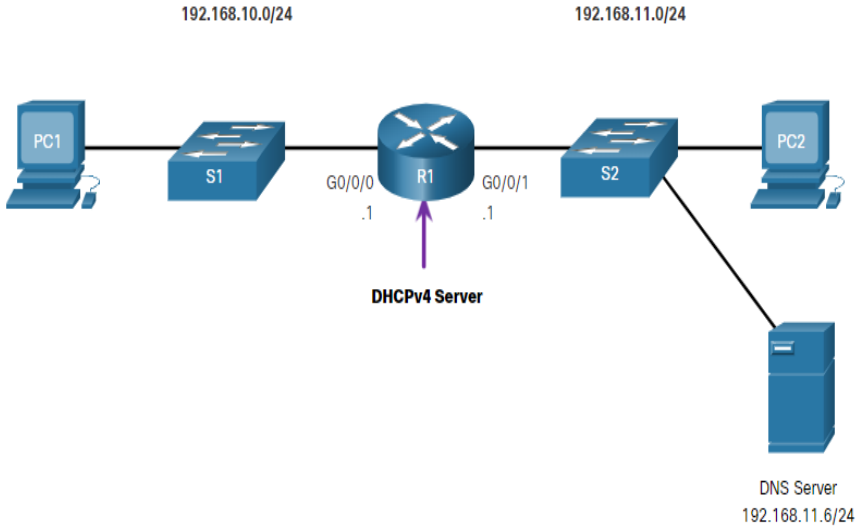
Configurer un serveur Cisco IOS DHCPv4

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.

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. La commande est **ip dhcp excluded-address *low-address [high address]***
- **Étape 2**. Définissez un nom de pool DHCPv4, avec La commande **ip dhcp pool *pool-name***
- **Étape 3**. Configurez le pool DHCPv4, avec l'instruction **network** pour définir la plage d'adresses disponibles, et la commande **default-router** pour définir le routeur servant de passerelle par défaut.

Tâche	Commande IOS
Exclusion d'adresses IPv4	**ip dhcp excluded-address** *[low-address] [high address]*
Définir un nom de pool DHCPv4	**ip dhcp pool** *pool-name*
Définir le pool d'adresses	**network** *network-number* [*mask* | / prefix-length]*prefix-length*]
Définir le routeur ou la passerelle par défaut	**default-router** address [*address2….address8*]
Définir un serveur DNS	**dns-server** *address* [*address2…address8*]
Définir le nom de domaine	**domain-name** *domain*
Définir la durée du bail DHCP	**lease** {*days* [*hours* [*minutes*]] | **infinite**}
Définir le serveur WINS NetBIOS	**netbios-name-server** *address* [*address2…address8*]



PARTIE 3

Configurer un serveur Cisco IOS DHCPv4

- **Vérification DHCPv4**

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

Commande	Description
show running-config | section dhcp	Affiche les commandes DHCPv4 configurées sur le routeur.
show ip dhcp binding	Affiche une liste de toutes les liaisons entre les adresses IPv4 et les adresses MAC fournies par le service DHCPv4.
show ip dhcp server statistics	Affiche les informations de comptage concernant le nombre de messages DHCPv4 qui ont été envoyés et reçus
ipconfig /all	affiche les paramètres TCP/IP sur un poste client

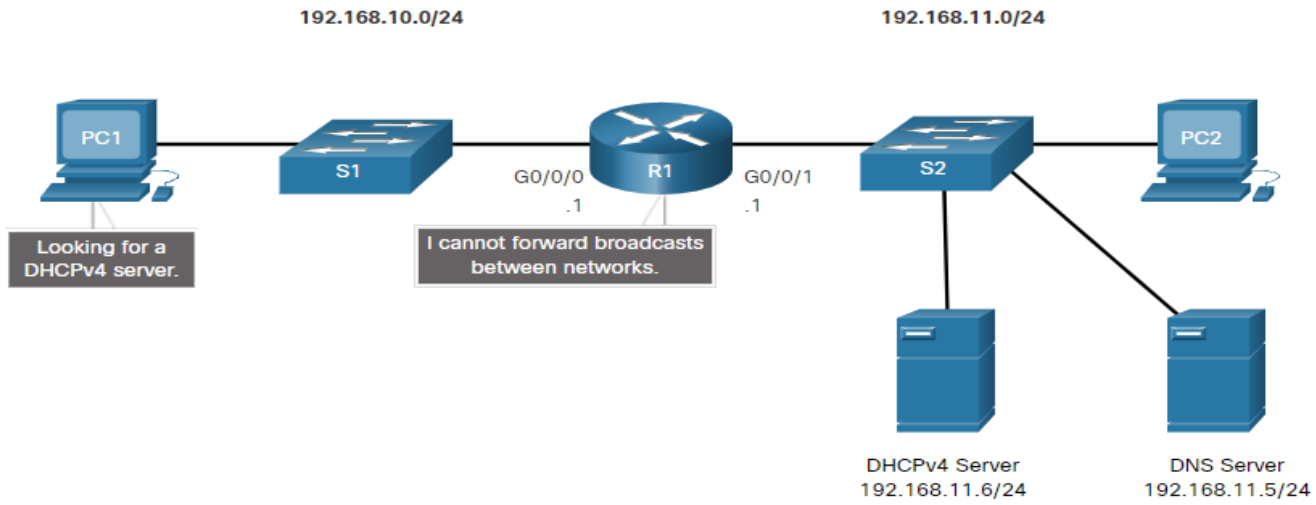
- **Désactiver le serveur Cisco IOS DHCPv4**

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. 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.

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.

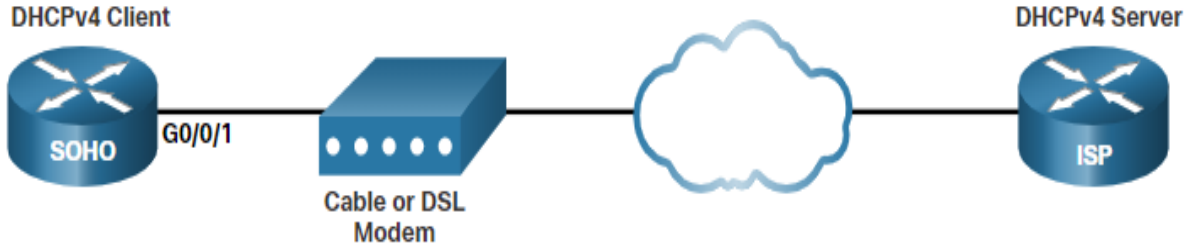


- Étant donné que le serveur DHCPv4 se trouve sur un autre réseau, PC1 ne peut pas recevoir d'adresse IP via DHCP. R1 doit être configuré pour relayer les messages DHCPv4 au serveur DHCPv4.
- Configurez R1 avec la commande de configuration de l'interface **ip helper-address** *address* . Cela entraînera R1 à relayer les diffusions DHCPv4 vers le serveur DHCPv4.
- 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.

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.

- 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** .



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.

PARTIE 3

CHAPITRE 2

Comprendre le fonctionnement de DHCPv6

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le fonctionnement de SLAAC et DHCPv6
- Configurer le service DHCPv6

2 heures

CHAPITRE 2

Comprendre le fonctionnement de DHCPv6

1. Attribution de GUA IPv6
2. Fonctionnement de SLAAC
3. Fonctionnement et configuration de DHCPv6

Configuration de l'hôte IPv6

Sur un routeur, une adresse de monodiffusion globale (GUA) IPv6 est configurée manuellement à l'aide de la commande de configuration de l'interface :

ipv6 address *ipv6-address/prefix-length* .

- Un hôte Windows peut également être configuré manuellement avec une configuration d'adresse GUA IPv6.
- Cependant, la saisie manuelle d'un GUA IPv6 peut prendre beaucoup de temps et est parfois susceptible de provoquer des erreurs.
- Par conséquent, la plupart des hôtes Windows sont activés pour acquérir dynamiquement une configuration GUA IPv6.

IPv6 Adresse de link-local

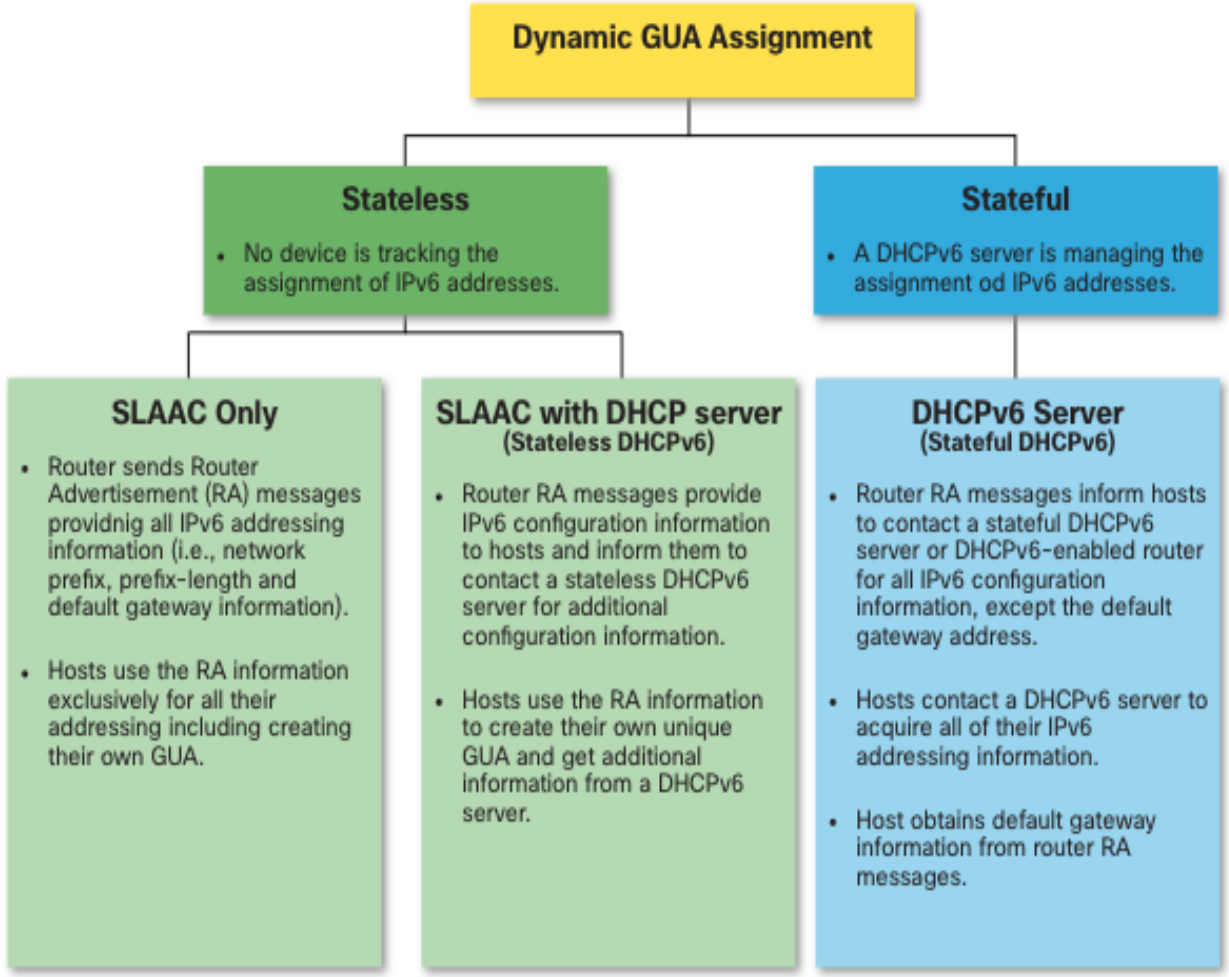
- L'adresse link-local IPv6 est automatiquement créée par l'hôte lorsqu'il démarre et que l'interface Ethernet est active.
- L'interface n'a pas créé de GUA IPv6 dans la sortie car le segment réseau n'avait pas de routeur pour fournir des instructions de configuration réseau pour l'hôte.

.

Attribution de GUA IPv6

Par défaut, un routeur compatible IPv6 envoie périodiquement des annonces de routeur ICMPv6, ce qui simplifie la façon dont un hôte peut créer ou acquérir dynamiquement sa configuration IPv6.

- Un hôte peut être attribué dynamiquement à une GUA en utilisant des services sans état et avec état.
- Toutes les méthodes sans état et avec état dans ce module utilisent des messages d'annonce de routeur (RA) ICMPv6 pour suggérer à l'hôte comment créer ou acquérir sa configuration IPv6.
- Bien que les systèmes d'exploitation hôtes suivent la suggestion de l'annonce de routeur (RA), la décision réelle revient finalement à l'hôte.



PARTIE 3

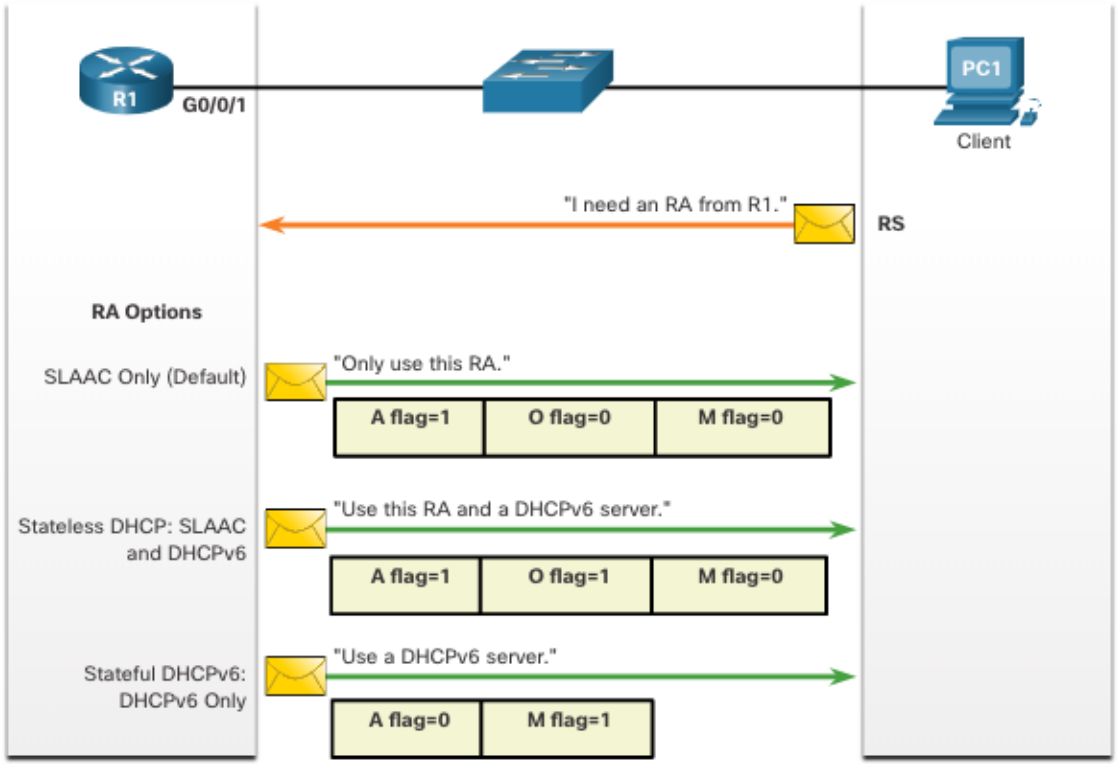
Trois indicateurs de message RA

La façon dont un client obtient une GUA IPv6 dépend des paramètres du message d'annonce de routeur (RA).

Un message d'AR ICMPv6 comprend les trois indicateurs suivants:

- **Indicateur A** - L'indicateur de configuration automatique d'adresse signifie d'utiliser SLAAC (Stateless Address Autoconfiguration) pour créer une GUA IPv6
- **Indicateur O** - Les autres indicateurs de configuration signifient que des informations supplémentaires sont disponibles auprès d'un serveur DHCPv6 sans état.
- **Indicateur M** - Un indicateur de configuration d'adresse gérée signifie qu'il faut utiliser un serveur DHCPv6 avec état pour obtenir un GUA IPv6.

En utilisant différentes combinaisons des indicateurs A, O et M, les messages RA informent l'hôte des options dynamiques disponibles.



PARTIE 3

CHAPITRE 2

Comprendre le fonctionnement de DHCPv6

1. Attribution de GUA IPv6
2. Fonctionnement de SLAAC
3. Fonctionnement et configuration de DHCPv6

Fonctionnement du SLAAC

Présentation du SLAAC

La méthode SLAAC permet aux hôtes de créer leur propre adresse de monodiffusion globale IPv6 unique sans les services d'un serveur DHCPv6.

- SLAAC est un service sans état, ce qui signifie qu'il n'y a pas de serveur qui conserve les informations d'adresse réseau pour savoir quelles adresses IPv6 sont utilisées et lesquelles sont disponibles.
- SLAAC envoie périodiquement des messages de RA ICMPv6 (c.-à-d. toutes les 200 secondes) fournissant des informations d'adressage et d'autres informations de configuration pour que les hôtes configurent automatiquement leur adresse IPv6 en fonction des informations contenues dans le message RA.
- Un hôte peut également envoyer un message de sollicitation de routeur (RS) demandant un message RA.
- SLAAC peut être déployé en tant que SLAAC uniquement, ou SLAAC avec DHCPv6.

Activation de SLAAC

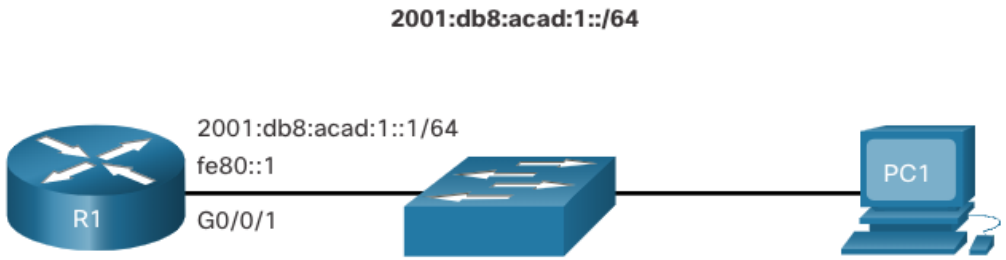
L'interface R1 G0/0/1 a été configuré avec les adresses GUA IPv6 et link-local indiquées.

Les adresses IPv6 de R1 G0/0/01 comprennent:

- **Adresse IPv6 link-local** - fe80::1
- **GUA / sous-réseau** - 2001:db8:acad:1::1, 2001:db8:acad:1::/64
- **Groupe tous les nœuds IPv6** - ff02::1

R1 est configuré pour rejoindre le groupe de multidiffusion IPv6 ff02::1 et commence à envoyer des messages RA contenant des informations de configuration d'adresse aux hôtes à l'aide de SLAAC.

Le groupe des routeurs IPv6 répond à l'adresse de multidiffusion IPv6 ff02::2.



PARTIE 3

Fonctionnement du SLAAC

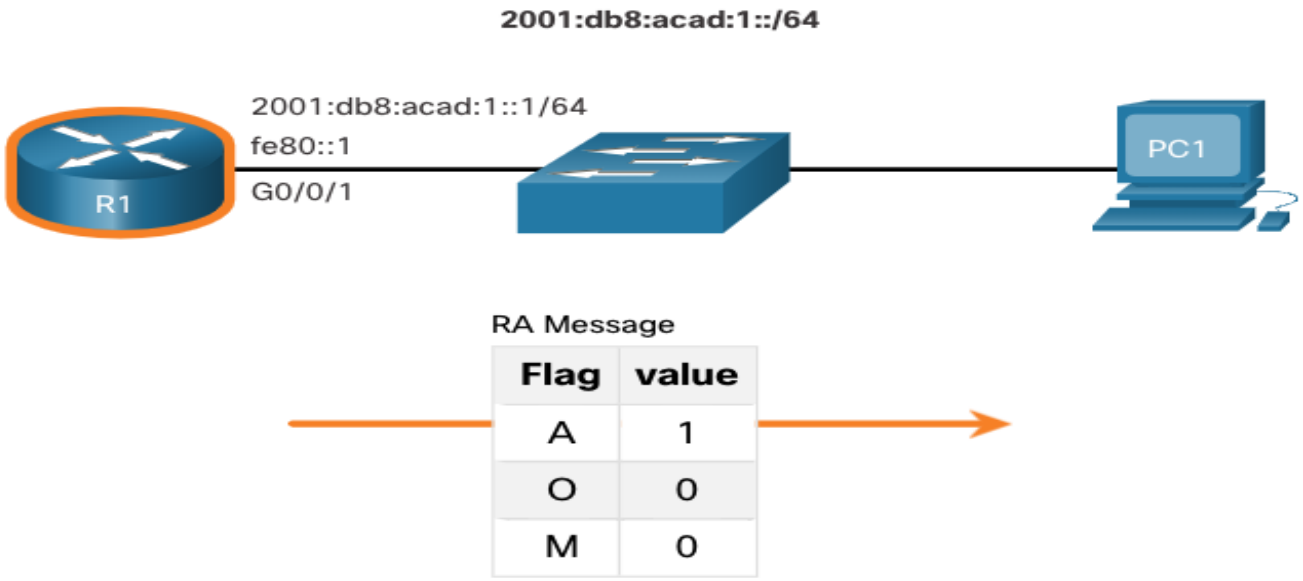
- **SLAAC seule méthode**

Les indicateurs suivants sont définis pour les messages RA de R1:

- **A = 1 -** Informe le client d'utiliser le préfixe GUA IPv6 dans le message RA et de créer dynamiquement son propre ID d'interface.
- **O = 0** et **M = 0** - Informe le client d'utiliser également les informations supplémentaires contenues dans le message RA (c'est-à-dire le serveur DNS, le MTU et les informations de passerelle par défaut).

La commande **ipconfig** de Windows confirme que PC1 a généré un GUA IPv6 à l'aide de la message RA de R1.

L'adresse de passerelle par défaut est Link Local Adresse de l'interface R1 G0/0/1.



PARTIE 3

Fonctionnement du SLAAC

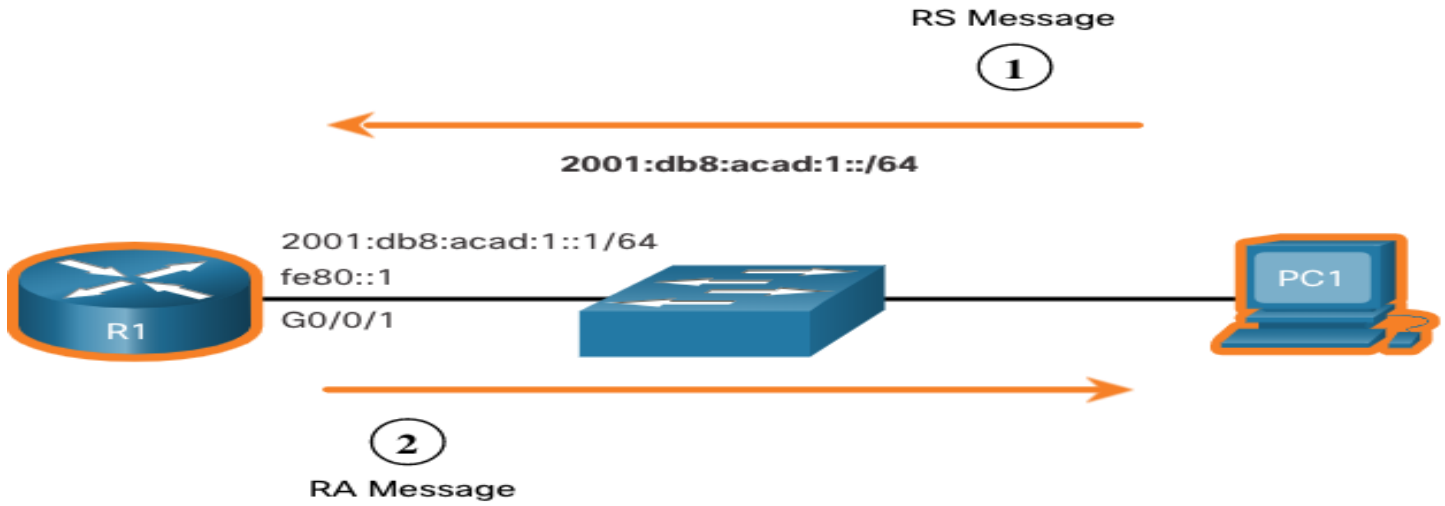
- **Messages RS ICMPv6**

Un routeur envoie des messages RA toutes les 200 secondes ou lorsqu'il reçoit un message RS d'un hôte.

- Les hôtes activés IPv6 souhaitant obtenir des informations d'adressage IPv6 envoient un message RS à l'adresse de multidiffusion IPv6 tout-routeurs ff02::2.

La figure illustre comment un hôte commence la méthode SLAAC.

1. PC1 vient de démarrer et envoie un message RS à l'adresse de multidiffusion des tout-routeurs IPv6 ff02::2 demandant un message RA.
2. R1 génère un message RA, puis envoie le message RA à l'adresse de multidiffusion tout-nœuds IPv6 ff02::1. PC1 utilise ces informations pour créer une GUA IPv6 unique.



PARTIE 3

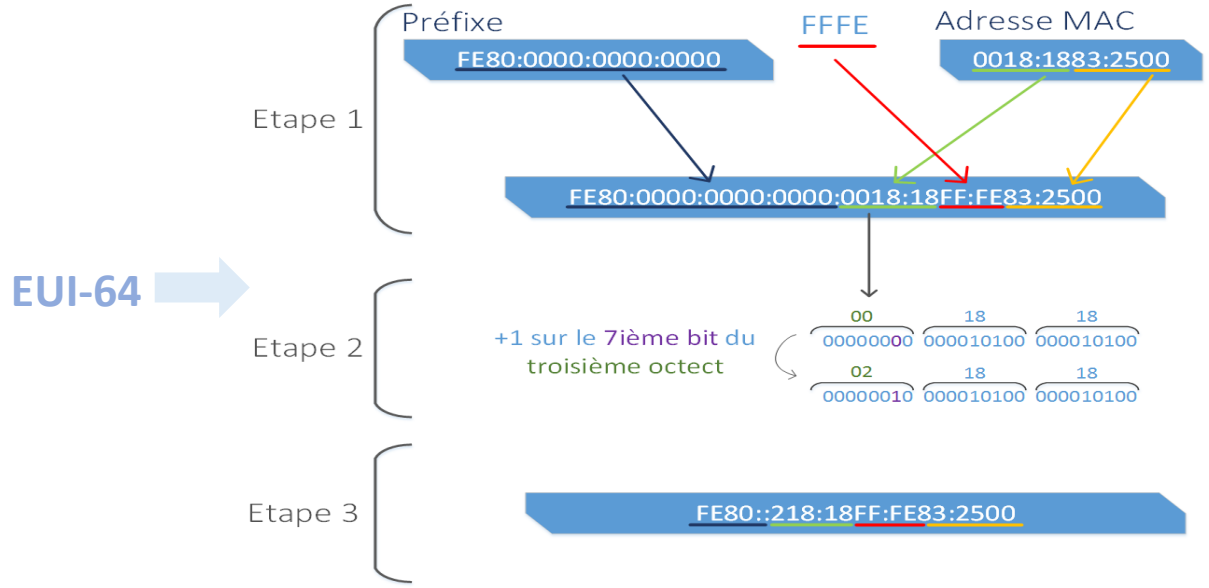
PARTIE 3

Processus d'hôte pour générer l'ID d'interface

À l'aide de SLAAC, un hôte acquiert ses informations de sous-réseau IPv6 64 bits de la RA du routeur et doit générer le reste de l'identificateur d'interface 64 bits à l'aide de l'un des éléments suivants :

- **Génération aléatoire** - L'ID de l'interface 64-bit est généré aléatoirement par le système d'exploitation du client. C'est la méthode maintenant utilisée par les hôtes Windows 10.
- **EUI-64** - L'hôte crée un ID d'interface en utilisant son adresse MAC 48 bits et insère la valeur hexadécimale de fffe au milieu de l'adresse. Certains systèmes d'exploitation utilisent par défaut l'ID d'interface généré aléatoirement plutôt que la méthode EUI-64, en raison de problèmes de confidentialité. En effet, l'adresse MAC Ethernet de l'hôte est utilisée par l'EUI-64 pour créer l'ID de l'interface.

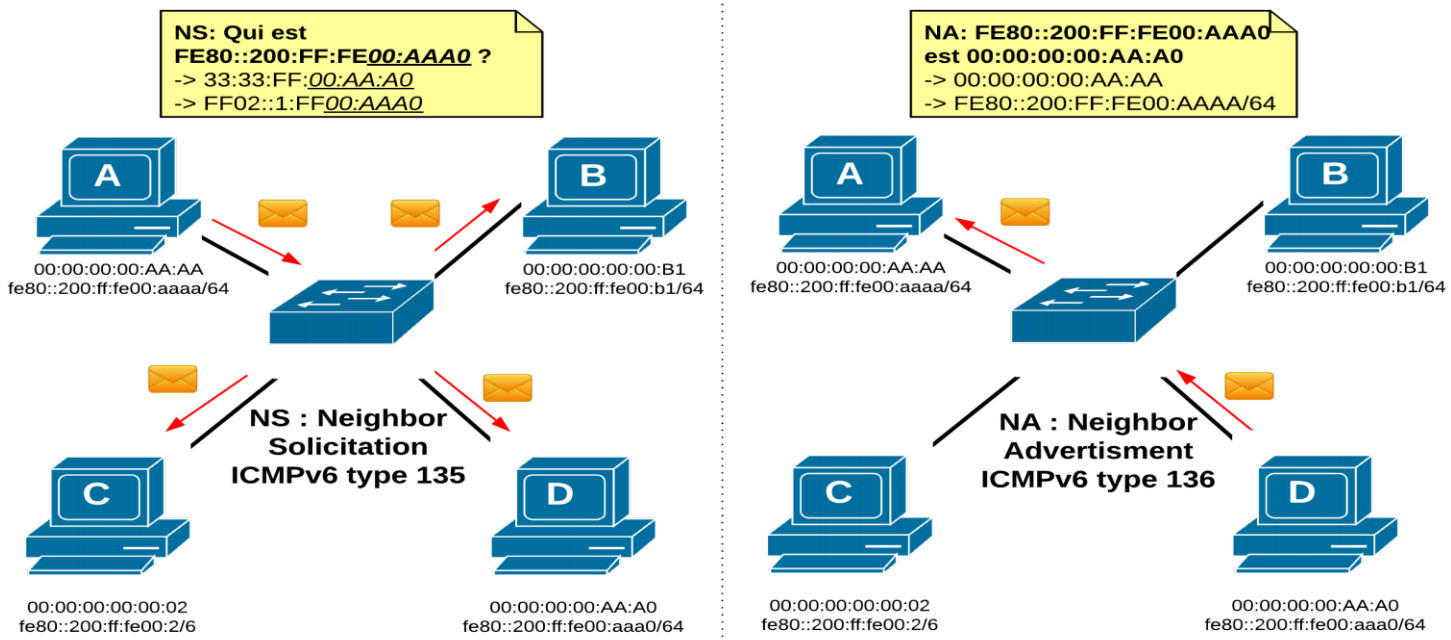
Remarque: Windows, Linux et Mac OS permettent à l'utilisateur de modifier la génération de l'ID d'interface pour être généré aléatoirement ou pour utiliser EUI-64.



Détection des adresses en double

Un hôte SLAAC peut utiliser le processus de détection des adresses en double (DAD) pour s'assurer que la GUA IPv6 est unique.

- L'hôte envoie un message de sollicitation de voisin ICMPv6 (NS) avec une adresse de multidiffusion de nœud sollicité spécialement construite contenant les 24 derniers bits de l'adresse IPv6 de l'hôte.
- Si aucun autre périphérique ne répond par un message d'annonce de voisin (NA), alors l'adresse est virtuellement garantie d'être unique et peut être utilisée par l'hôte.
- Si un NA est reçu par l'hôte, l'adresse n'est pas unique et l'hôte doit générer un nouvel ID d'interface à utiliser.

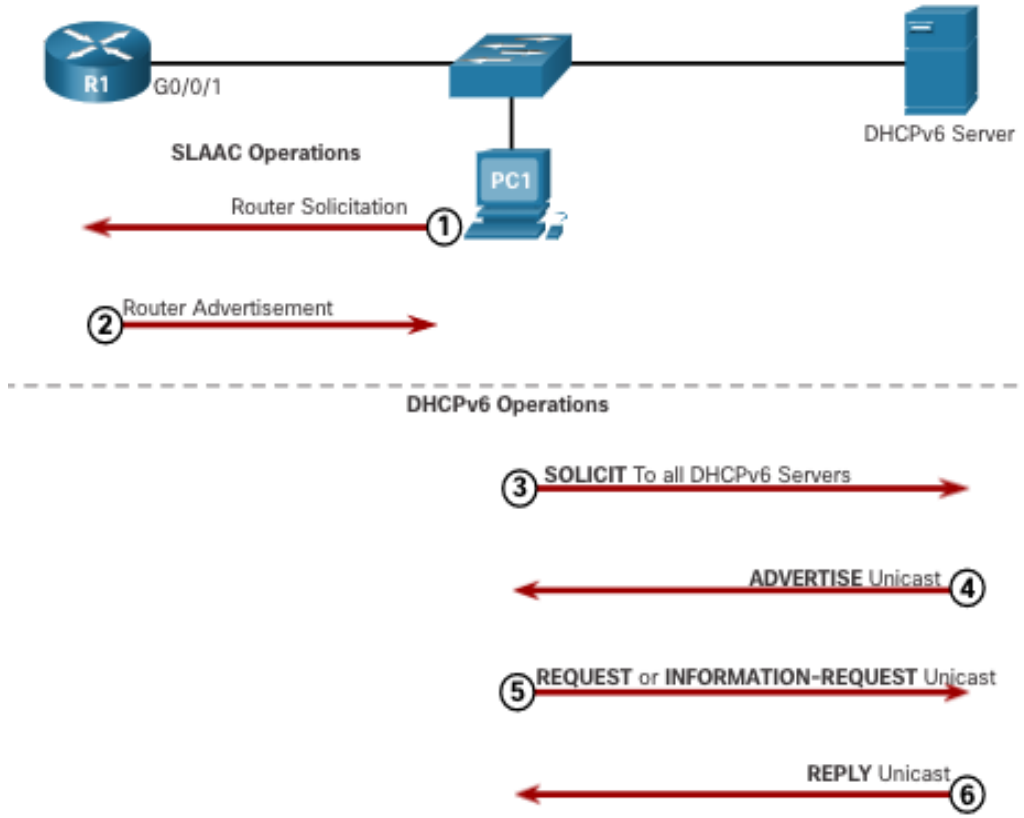


Étapes du fonctionnement de DHCPv6

Le DHCPv6 avec état n'exige pas le SLAAC, alors que le DHCPv6 sans état l'exige.

Quoi qu'il en soit, lorsqu'un RA indique d'utiliser DHCPv6 ou DHCPv6 avec état:

1. L'hôte envoie un message RS.
2. Le routeur répond avec un message RA.
3. L'hôte envoie un message DHCPv6 SOLICIT.
4. Le serveur DHCPv6 répond par un message ANNONCE.
5. L'hôte répond au serveur DHCPv6.
6. Le serveur DHCPv6 envoie un message REPONSE.



Remarque: Les messages DHCPv6 serveur à client utilisent le port de destination UDP 546 tandis que les messages DHCPv6 client à serveur utilisent le port de destination UDP 547.

PARTIE 3

CHAPITRE 2

Comprendre le fonctionnement de DHCPv6

1. Attribution de GUA IPv6
2. Fonctionnement de SLAAC
3. Fonctionnement et configuration de DHCPv6

Fonctionnement de DHCPv6 sans état

Si une RA indique la méthode DHCPv6 sans état, l'hôte utilise les informations contenues dans le message RA pour l'adressage et contacte un serveur DHCPv6 pour obtenir des informations supplémentaires.

Remarque: Le serveur DHCPv6 fournit uniquement des paramètres de configuration pour les clients et ne gère pas une liste de liaisons d'adresses IPv6 (c'est-à-dire sans état).

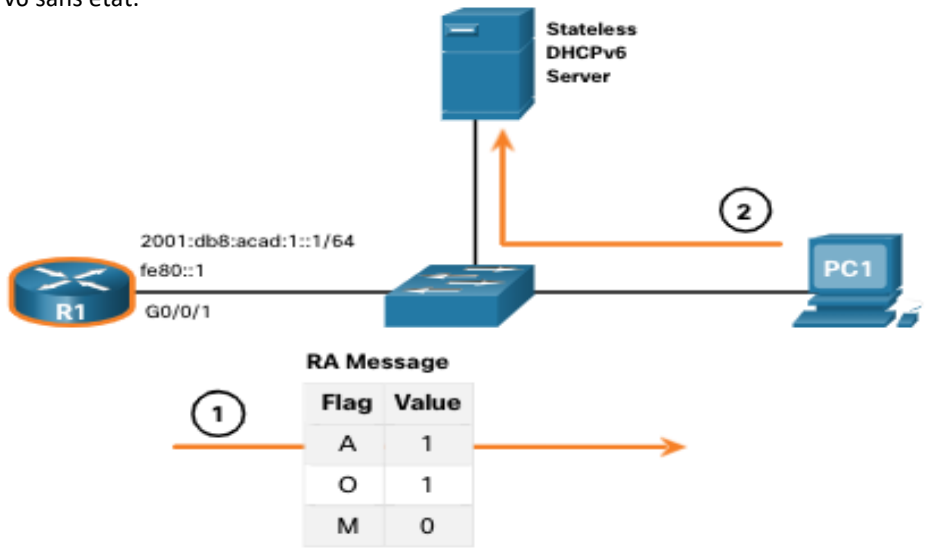
Par exemple, PC1 reçoit un message RA sans état contenant:

- Le préfixe de réseau IPv6 GUA et la longueur du préfixe.
- Indicateur défini sur 1 indiquant à l'hôte d'utiliser SLAAC.
- Indicateur O défini sur 1 pour informer l'hôte de rechercher ces informations de configuration supplémentaires auprès d'un serveur DHCPv6.
- Indicateur M défini sur la valeur par défaut 0.
- PC1 envoie un message DHCPv6 SOLICIT demandant des informations supplémentaires à partir d'un serveur DHCPv6 sans état.

Activer DHCPv6 sans état sur une interface

DHCPv6 sans état est activé à l'aide de la commande de configuration de l'interface **ipv6 nd other config-flag** définissant l'indicateur O sur 1.

Remarque: Vous pouvez utiliser la commande **no ipv6 nd other config-flag** pour réinitialiser l'interface à l'option SLAAC par défaut uniquement (O flag = 0).



PARTIE 3

PARTIE 3

Fonctionnement de DHCPv6 avec état

Si un message RA indique la méthode DHCPv6 avec état, l'hôte contacte un serveur DHCPv6 pour obtenir toutes les informations de configuration.

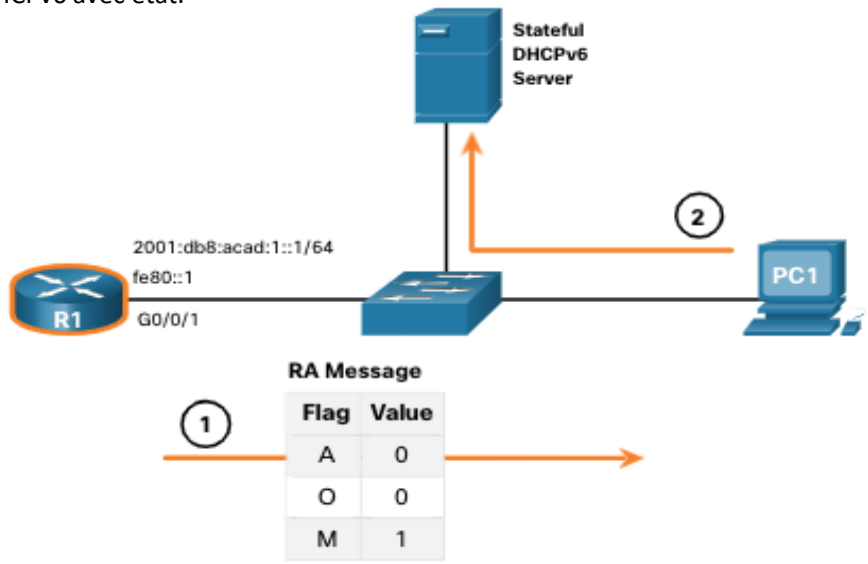
Remarque: le serveur DHCPv6 est doté avec état et gère une liste de liaisons d'adresses IPv6.

Par exemple, PC1 reçoit un message RA avec état contenant:

- Le préfixe de réseau IPv6 GUA et la longueur du préfixe.
- Indicateur défini sur 0 indiquant à l'hôte de contacter un serveur DHCPv6.
- Indicateur défini sur 0 indiquant à l'hôte de contacter un serveur DHCPv6.
- Indicateur M défini sur la valeur 1.
- PC1 envoie un message DHCPv6 SOLICIT demandant des informations supplémentaires à partir d'un serveur DHCPv6 avec état.

Activer DHCPv6 avec état sur une interface

DHCPv6 avec état est activé à l'aide de la commande de configuration de l'interface **ipv6 nd managed-config-flag** définissant l'indicateur M sur 1.



Rôles de routeur DHCPv6

Les routeurs Cisco IOS sont des appareils puissants. Dans les réseaux de petit taille, il n'est pas nécessaire d'avoir des appareils séparés pour avoir un serveur, un client ou un agent de relais DHCPv6. Un routeur Cisco IOS peut être configuré pour fournir des services de serveur DHCPv6.

Plus précisément, il peut être configuré pour être l'un des éléments suivants :

- **Serveur DHCPv6** - Un routeur fournit des services DHCPv6 sans état ou avec état.
- **Client DHCPv6** - L'interface du routeur acquiert une configuration IP IPv6 à partir d'un serveur DHCPv6.
- **Agent de relais DHCPv6** - Un routeur fournit des services de transfert DHCPv6 lorsque le client et le serveur sont situés sur différents réseaux.

Commandes de vérification du serveur DHCPv6

Utilisez les commandes du tableau pour vérifier que le serveur Cisco IOS DHCPv6 est opérationnel.

Commande	Description
show ipv6 dhcp pool	vérifie le nom du pool DHCPv6 et ses paramètres. La commande identifie également le nombre de clients actifs.
show ipv6 dhcp binding	pour afficher l'adresse link-local IPv6 du client et l'adresse de monodiffusion globale attribuée par le serveur.
show ipv6 dhcp interface *interface-id*	Vérifie que le routeur client a reçu d'autres informations DHCPv6 nécessaires.

PARTIE 3

Configurer de DHCPv6 sans état

Configurer un serveur DHCPv6 sans état

L'option de serveur DHCPv6 sans état nécessite que le routeur annonce les informations d'adressage réseau IPv6 dans les messages RA.

Il y a cinq étapes pour configurer et vérifier un routeur en tant que serveur DHCPv6 sans état:

1. Activez le routage IPv6 en utilisant la commande **ipv6 unicast-routing** .
2. Définissez un nom de pool DHCPv6 à l'aide de la commande de configuration globale **ipv6 dhcp pool** *POOL-NAME* .
3. Configurer le pool DHCPv6 avec des options. Les options courantes incluent **le serveur DNS X:X:X:X:X:X:X:X** et **le nom de domaine *nom***.
4. Liez l'interface au pool à l'aide de la commande de configuration de l'interface **ipv6 dhcp server** *POOL-NAME* .
   - Changez manuellement l'indicateur O de 0 à 1 en utilisant la commande d'interface **ipv6 nd other-config-flag**. Les messages RA envoyés sur cette interface indiquent que des informations supplémentaires sont disponibles auprès d'un serveur DHCPv6 sans état. L'indicateur A est 1 par défaut, indiquant aux clients d'utiliser SLAAC pour créer leur propre GUA.
5. Vérifiez que les hôtes ont reçu des informations d'adressage IPv6 à l'aide de la commande **ipconfig /all** .

Configurer un client DHCPv6 sans état

Un routeur peut également être un client DHCPv6 et obtient une configuration IPv6 à partir d'un serveur DHCPv6, tel qu'un routeur fonctionnant en tant que serveur DHCPv6.

1. Activez le routage IPv6 en utilisant la commande **ipv6 unicast-routing** .
2. Configurer le routeur client pour créer un LLA. Une adresse link-local IPv6 est créée sur une interface de routeur lorsqu'une adresse de monodiffusion globale est configurée, ou sans GUA à l'aide de la commande de configuration d'interface **ipv6 enable** . Cisco IOS utilise EUI-64 pour créer l'ID d'interface.
3. Configurez le routeur client pour qu'il utilise SLAAC à l'aide de la commande **ipv6 address autoconfig** .
4. Vérifiez que le routeur client reçoit une GUA à l'aide de la commande **show ipv6 interface brief** .
5. Vérifiez que le routeur client a reçu d'autres informations DHCPv6 nécessaires. La commande **show ipv6 dhcp interface g0/0/1** confirme que les informations relatives aux options DHCP, telles que le serveur DNS et le nom de domaine, ont été reçues par le client.

PARTIE 3

Configurer de DHCPv6 avec état

Configurer un serveur DHCPv6 avec état

L'option de serveur DHCP avec état exige que le routeur compatible IPv6 indique à l'hôte de contacter un serveur DHCPv6 pour obtenir toutes les informations d'adressage réseau IPv6 nécessaires.

Il y a cinq étapes pour configurer et vérifier un routeur en tant que serveur DHCPv6 avec état:

1. Activez le routage IPv6 en utilisant la commande **ipv6 unicast-routing** .
2. Définissez un nom de pool DHCPv6 à l'aide de la commande globale de configuration **ipv6 dhcp pool** *POOL-NAME* .
3. Configurer le pool DHCPv6 avec des options. Les options courantes incluent la commande de **address prefix** , le nom de domaine, l'adresse IP du serveur DNS, etc.
4. Liez l'interface au pool à l'aide de la commande de configuration de l'interface **ipv6 dhcp server** *POOL-NAME* .
   - Changez manuellement l'indicateur M de 0 à 1 en utilisant la commande **ipv6 nd managed-config-flag**.
   - Modifiez manuellement l'indicateur A de 1 à 0 à l'aide de la commande d'interface **ipv6 nd prefix default no-autoconfig** pour informer le client de ne pas utiliser SLAAC pour créer une GUA. Le routeur répondra ensuite aux requêtes DHCPv6 avec état par des informations contenues dans le pool.
5. Vérifiez que les hôtes ont reçu des informations d'adressage IPv6 à l'aide de la commande **ipconfig /all** .

Configurer un client DHCPv6 avec état

Un routeur peut également être un client DHCPv6. Le routeur client doit avoir l'option **ip unicast-routing** activé et une adresse link-local IPv6 pour envoyer et recevoir des messages IPv6.

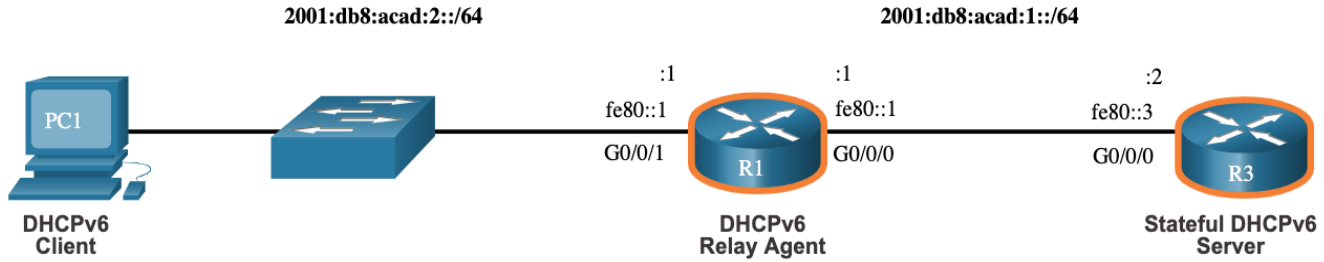
Il y a cinq étapes pour configurer et vérifier un routeur en tant que client DHCPv6 sans état.

1. Activez le routage IPv6 en utilisant la commande **ipv6 unicast-routing** .
2. Configurer le routeur client pour créer un LLA. Une adresse link-local IPv6 est créée sur une interface de routeur lorsqu'une adresse de monodiffusion globale est configurée, ou sans GUA à l'aide de la commande de configuration d'interface **ipv6 enable** . Cisco IOS utilise EUI-64 pour créer un ID d'interface.
3. Configurez le routeur client pour utiliser DHCPv6 à l'aide de la commande de configuration de l'interface **ipv6 address dhcp** .
4. Vérifiez que le routeur client reçoit une GUA à l'aide de la commande **show ipv6 interface brief** .
5. Vérifiez que le routeur client a reçu d'autres informations DHCPv6 nécessaires à l'aide de la commande **show ipv6 dhcp interface** *interface-id* .

Configurer un agent de relais DHCPv6

Si le serveur DHCPv6 se trouve sur un réseau différent de celui du client, alors le routeur IPv6 peut être configuré en tant qu'agent de relais DHCPv6.

- La configuration d'un agent de relais DHCPv6 est similaire à celle d'un routeur IPv4 en tant que relais DHCPv4.
- **Ipv6 dhcp relay destination** *address interface-id* . Cette commande est configurée sur l'interface située au niveau des clients DHCPv6 et spécifie l'adresse du serveur DHCPv6 et l'interface de sortie pour atteindre le serveur, comme indiqué dans la sortie. L'interface de sortie n'est requise que lorsque l'adresse de tronçon suivant est un LLA.



Vérifiez l'agent de relais DHCPv6

- Vérifiez que l'agent de relais DHCPv6 est opérationnel avec les commandes

  show ipv6 dhcp interface et **show ipv6 dhcp binding** .

- Vérifiez que les hôtes Windows ont reçu des informations d'adressage IPv6 à l'aide de la commande **ipconfig /all** .

PARTIE 3

PARTIE 4

Sécuriser un réseau local

Dans ce module, vous allez :

- Être en mesure d'assurer la sécurité de réseau LAN
- Être capable de concevoir et sécuriser un réseau sans fil (WLAN)

6 heures

CHAPITRE 1

Sécuriser la couche 2 du réseau LAN

Ce que vous allez apprendre dans ce chapitre :

- Comprendre les concepts de base de la sécurité de la couche 2 du réseau LAN
- Configurer la sécurité des ports d’un commutateur

2 heures

CHAPITRE 1

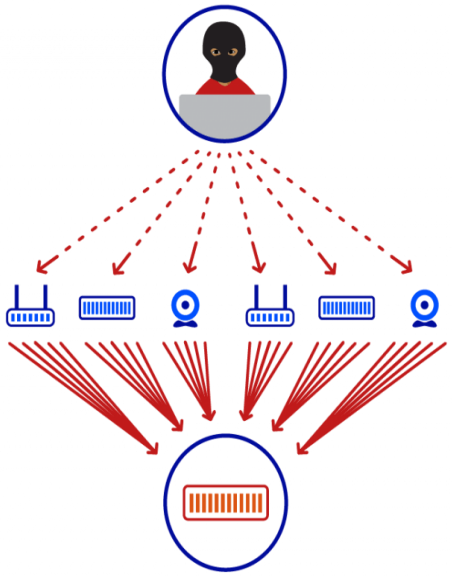
Sécuriser la couche 2 du réseau LAN

1. Concepts de sécurité LAN
2. Configuration de la sécurité du commutateur

Les attaques de réseau au quotidien

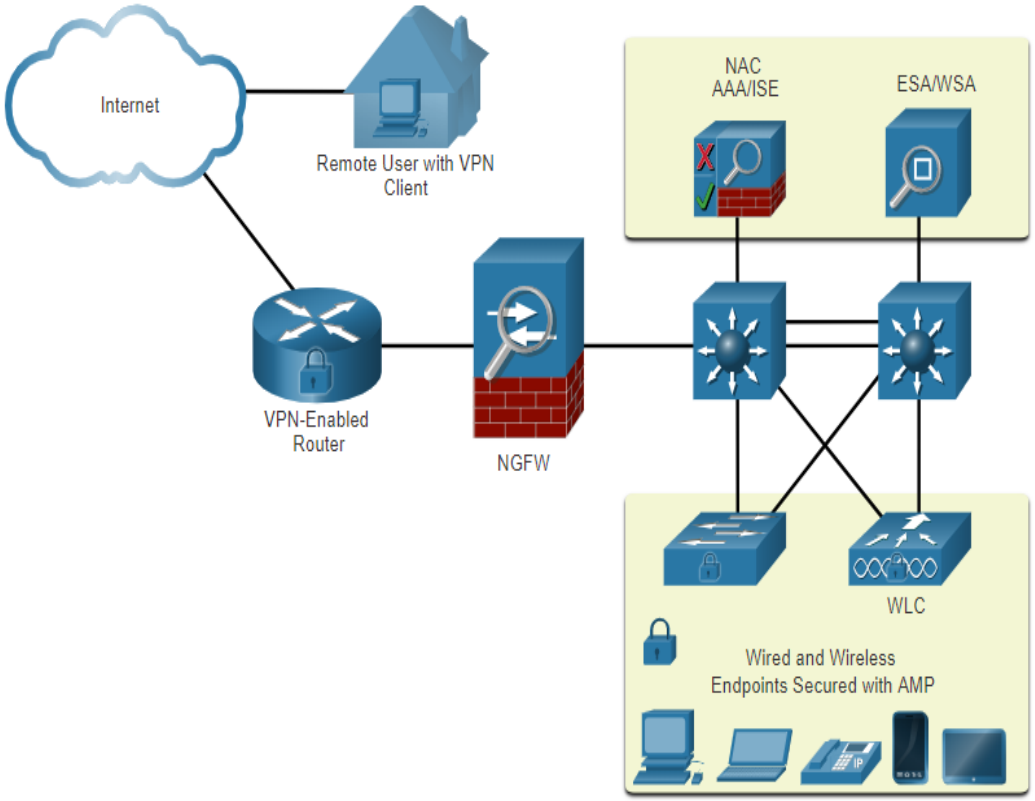
Les médias d'information couvrent généralement les attaques contre les réseaux d'entreprise. Ces attaques impliqueront un ou plusieurs les éléments suivants:

- **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.



Protection des terminaux

- 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 divers appareils de sécurité du réseau, qui 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.
- **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).



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 ofppt
R1(config-line)# login
```

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

Composants AAA

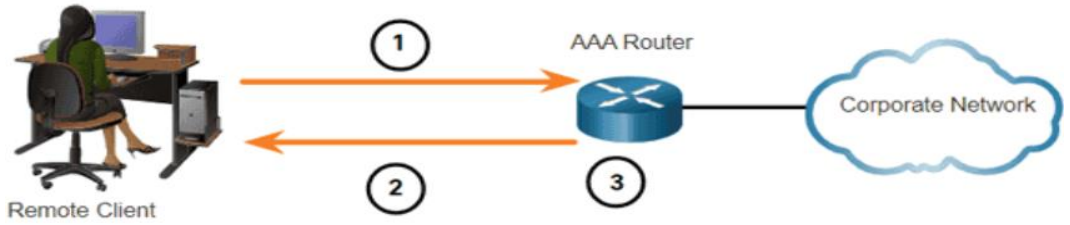
AAA signifie Authentification, Autorisation et Comptabilité et fournit le cadre principal pour configurer le contrôle d'accès sur un périphérique réseau.

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:



Remarque : L'authentification AAA locale est idéale pour les réseaux de petite taille.

L'authentification AAA basée sur le serveur :

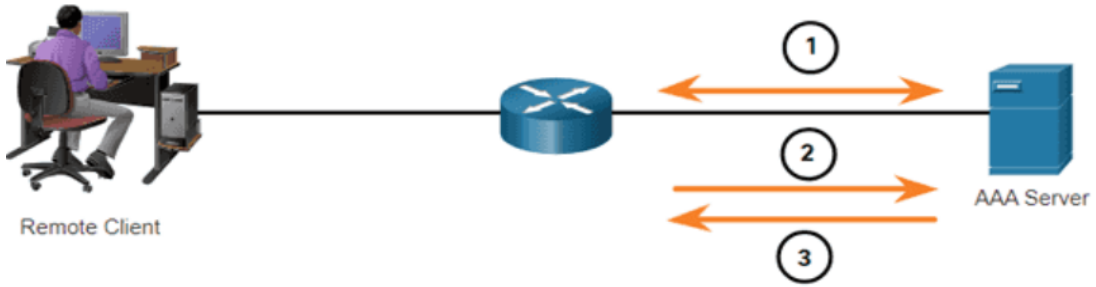
Remarque : Le routeur utilise les protocoles RADIUS ou TACACS+ pour communiquer avec le serveur AAA.

PARTIE 4

Composants AAA

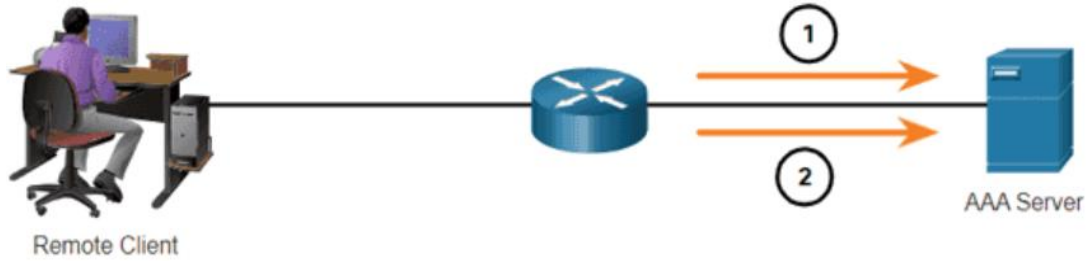
- **L'autorisation**

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 privilèges 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.



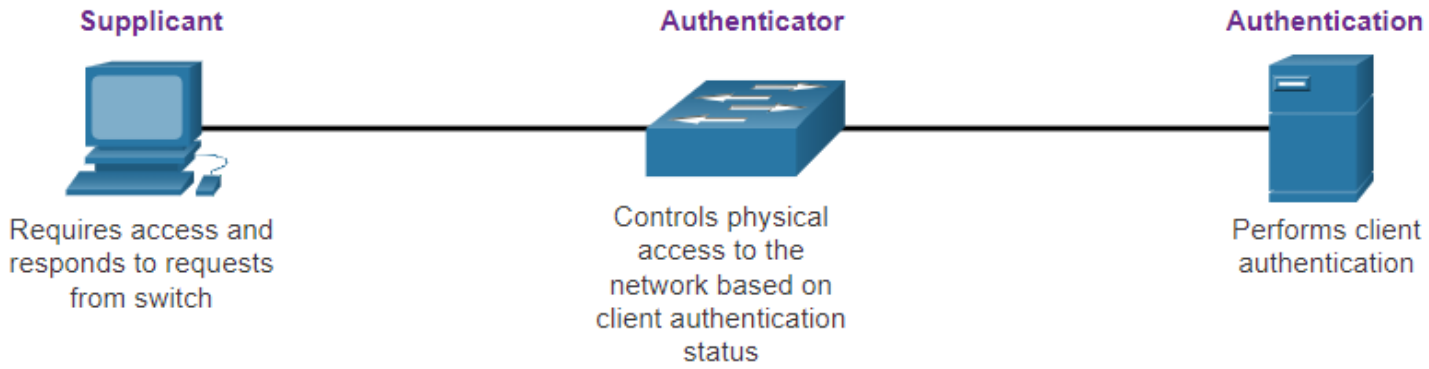
802.1x

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.

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 (ou point d'accès sans fil) 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.
- **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.

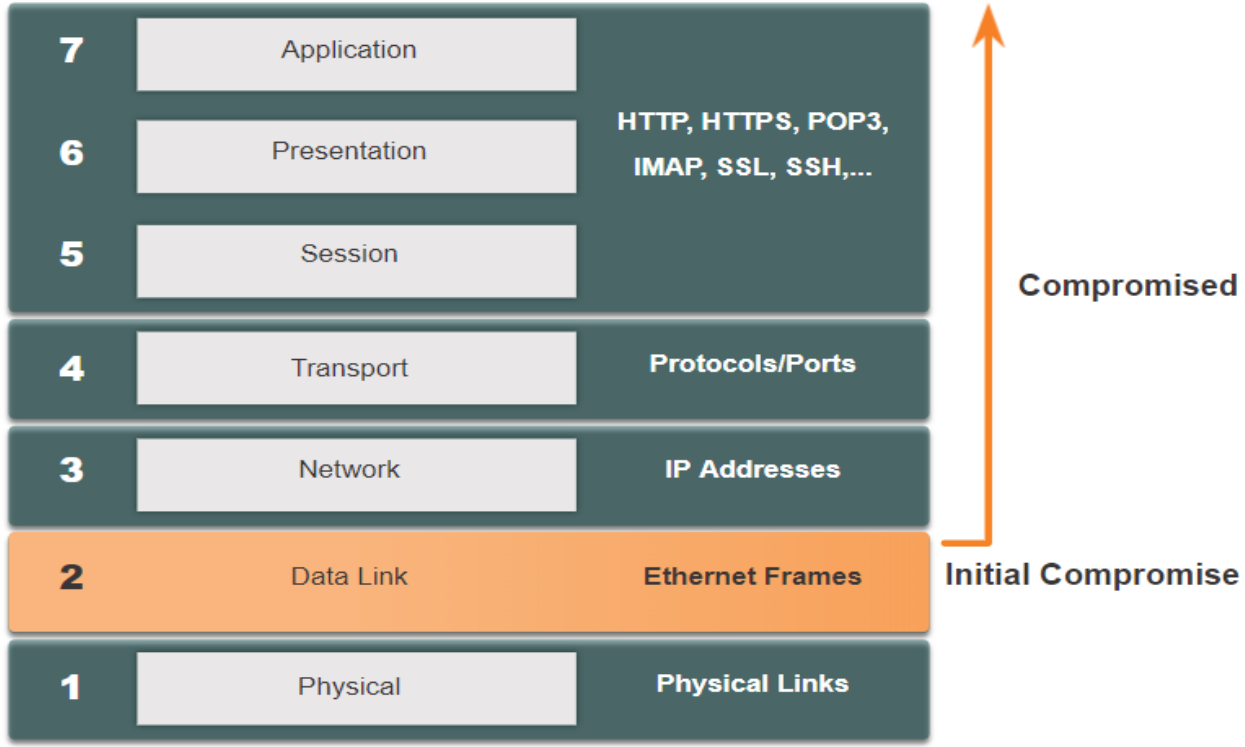


PARTIE 4

Vulnérabilités de couche 2

Aujourd'hui, avec le BYOD et des attaques plus sophistiquées, nos réseaux locaux sont devenus plus vulnérables à la pénétration

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.



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.

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 revérifier 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

Le tableau fournit un aperçu des solutions pour aider à atténuer les attaques de couche 2.

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.

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

CHAPITRE 1

Sécuriser la couche 2 du réseau LAN

1. Concepts de sécurité LAN
2. Configuration de la sécurité du commutateur

Mise en œuvre de la sécurité des ports

Ports inutilisés sécurisés

- 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. 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 source sécurisées qui ont été configurées manuellement ou apprises dynamiquement sur le port.
- En limitant le nombre d'adresses MAC autorisées sur un port à un, la sécurité du port peut être utilisée pour contrôler l'accès non autorisé au réseau.

Mise en œuvre de la sécurité des ports

- **Activer la sécurité de port**

- La sécurité des ports est activée avec la commande de configuration de l'interface **switchport port-security** .
- Utilisez la commande **show port-security interface** pour afficher les paramètres de sécurité de port actuels.

- **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
```

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
```

Mise en œuvre de la sécurité des ports

Obsolescence de la sécurité des ports

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 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}}
```

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}
```

Mode	Description
Shutdown (par défaut)	Le port passe immédiatement à l'état désactivé par erreur
restreindre	Le port supprime les paquets dont l'adresse source est inconnue. Un message syslog génèré.
protéger	Le port supprime les paquets avec des adresses source MAC inconnues. Aucun message Syslog n'est envoyé.

CHAPITRE 2

Concevoir et sécuriser un réseau local sans fil

Ce que vous allez apprendre dans ce chapitre :

- Concevoir et sécuriser un réseau local sans fil
- Configurer et dépanner les réseaux WLAN

4 heures

CHAPITRE 2

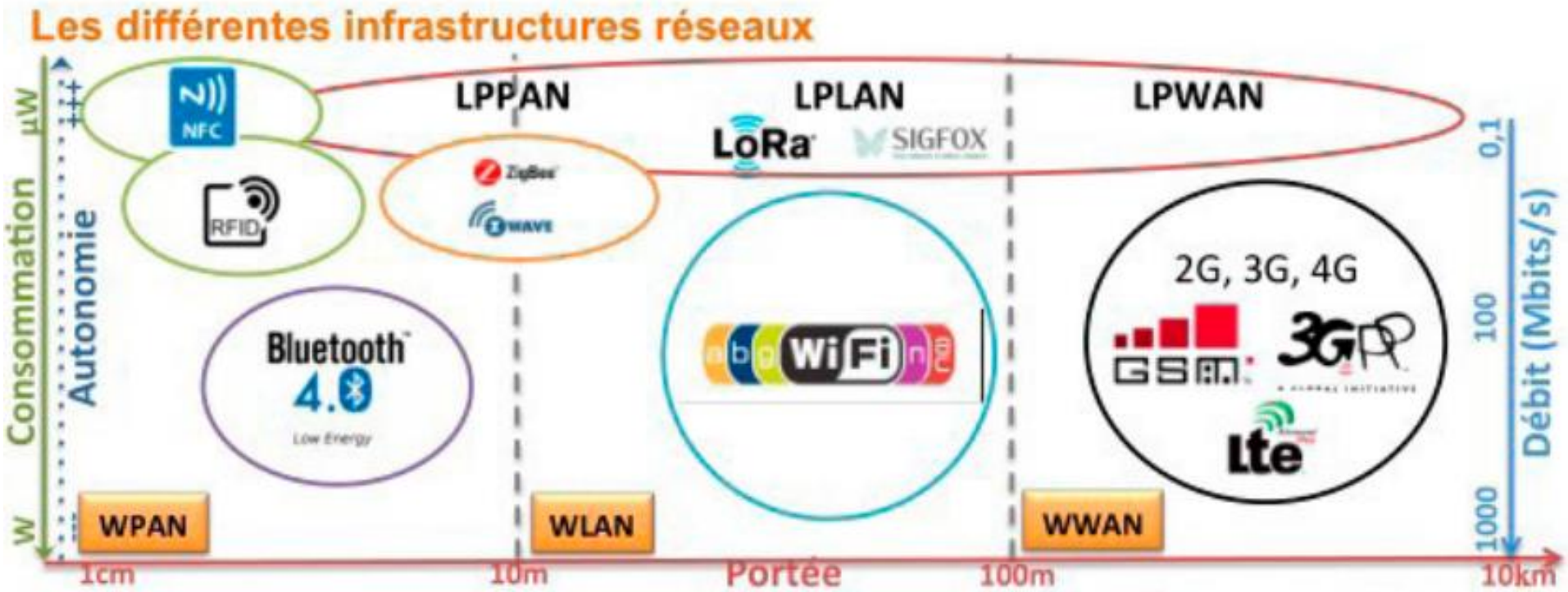
Concevoir et sécuriser un réseau local sans fil

1. Présentation de la technologie sans fil
2. Fonctionnement d'un réseau WLAN
3. Mécanismes de sécurité WLAN
4. Configuration de réseau WLAN

Réseau 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.
- Maniabilité et simplicité d’emploi

Technologies sans fil



Normes du 802.11

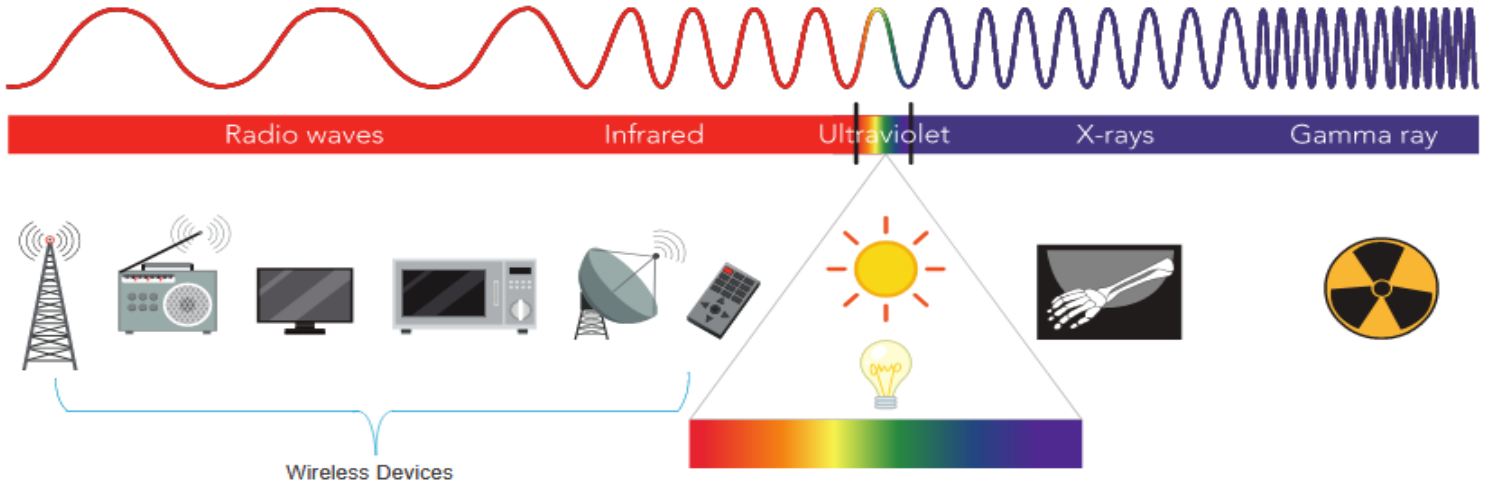
Les normes 802.11 WLAN définissent comment les fréquences radio sont utilisées pour les liaisons sans fil.

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

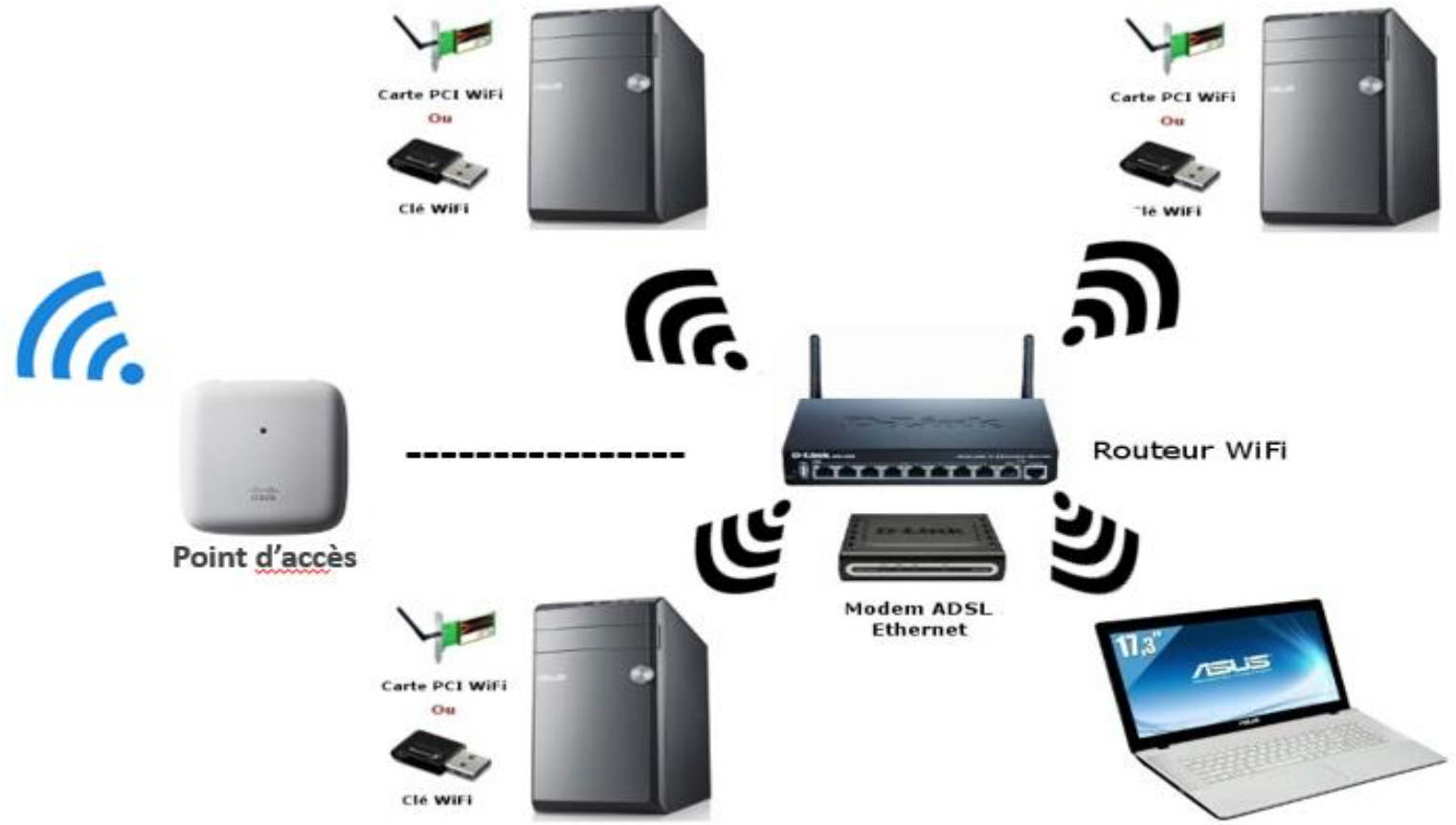
Fréquences Radio

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

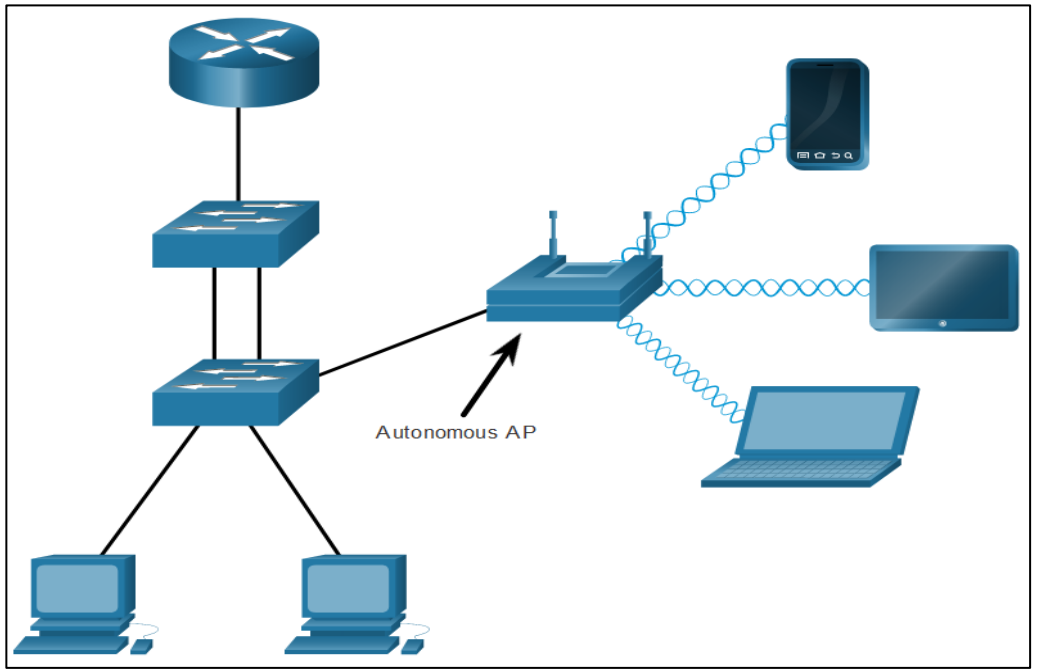


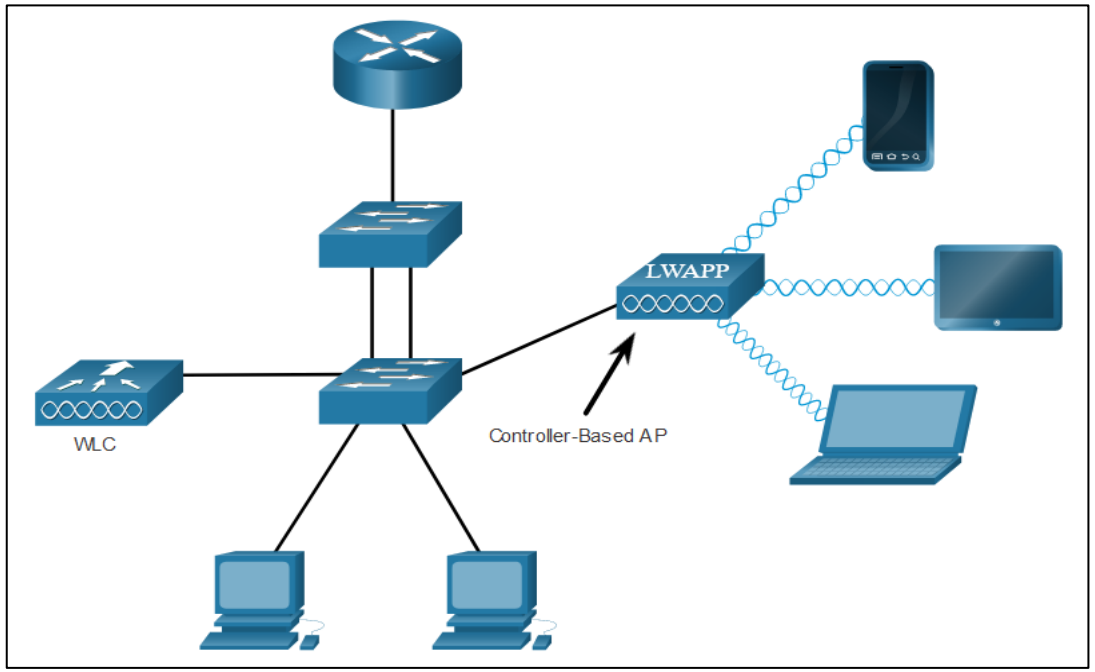
Composants WIFI



Catégories AP

Les points d'accès peuvent être classés comme des points d'accès autonomes ou des points d'accès basés sur un contrôleur.





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.

CHAPITRE 2

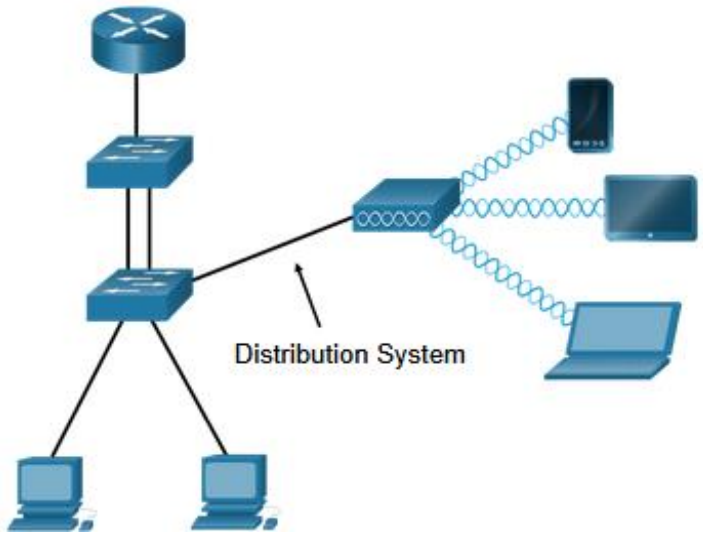
Concevoir et sécuriser un réseau local sans fil

1. Présentation de la technologie sans fil
2. Fonctionnement d'un réseau WLAN
3. Mécanismes de sécurité WLAN
4. Configuration de réseau WLAN

Modes de topologie sans fil 802.11

Mode ad hoc

Mode infrastructure



Partage de connexion

PARTIE 4

BSS et ESS

Le mode infrastructure définit deux blocs de topologie:

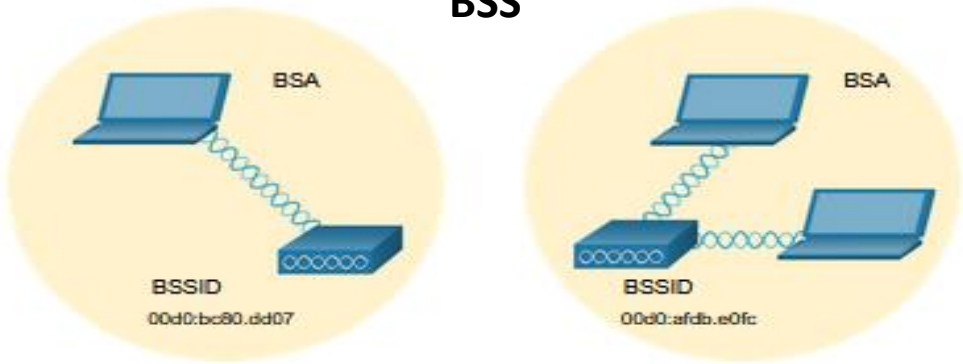
Ensemble de services de base (BSS)

- Un BSS consiste en un seul AP interconnectant tous les clients sans fil associés.
- Les clients de différents BSS ne peuvent pas communiquer.

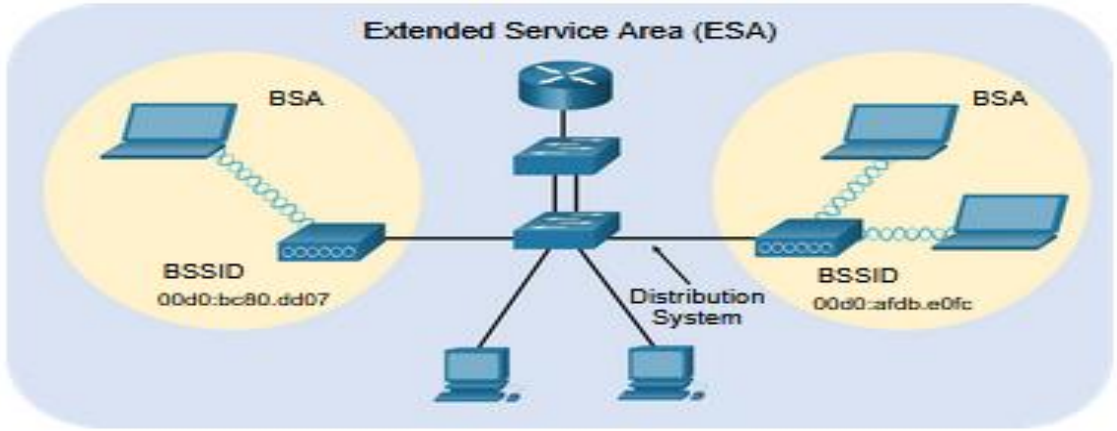
Ensemble de service étendu (ESS)

- Union de deux ou plusieurs BSS interconnectés par un système de distribution câblé.
- Les clients de chaque BSS peuvent communiquer via l'ESS.

BSS



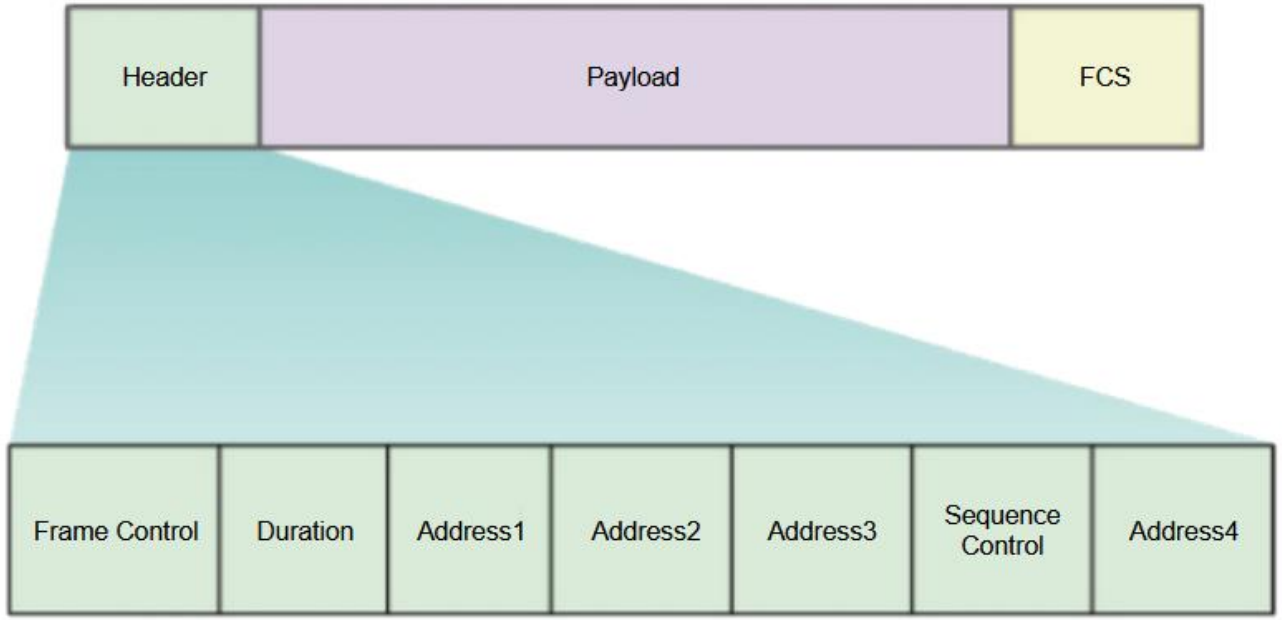
ESS



PARTIE 4

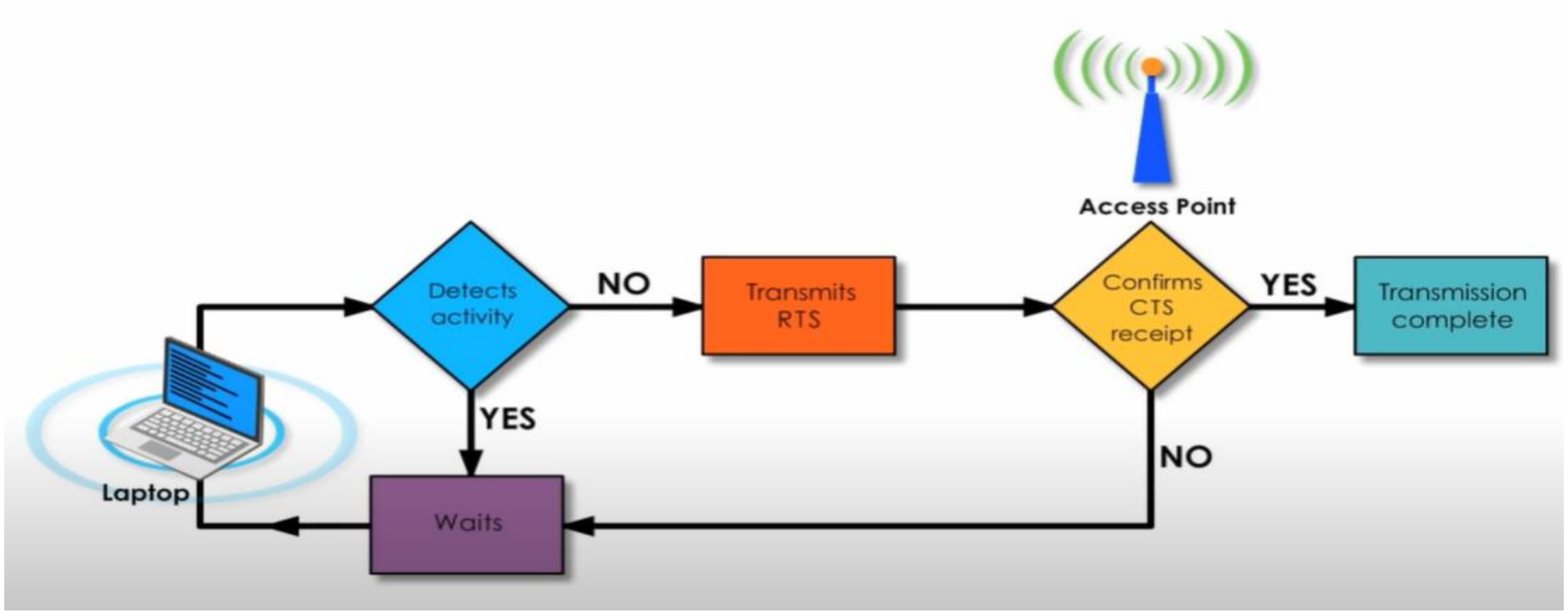
Structure de trame 802.11

Le format de trame 802.11 est similaire au format de trame Ethernet, sauf qu'il contient plus de champs.



CSMA/CA

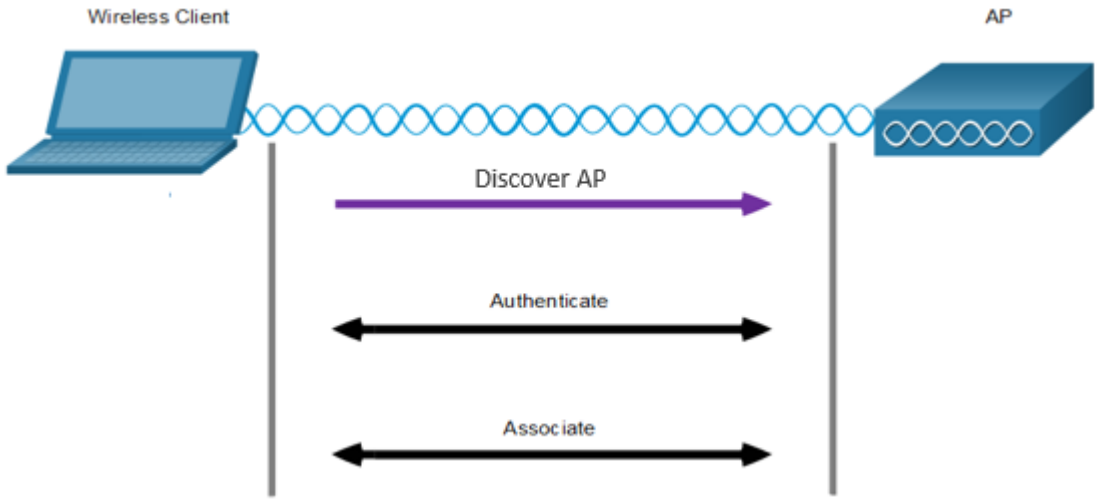
Les WLAN utilisent l'accès multiple par détection de porteuse avec évitement de collision (CSMA/CA) pour déterminer comment et quand envoyer des données. Un client sans fil effectue les opérations suivantes:



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:

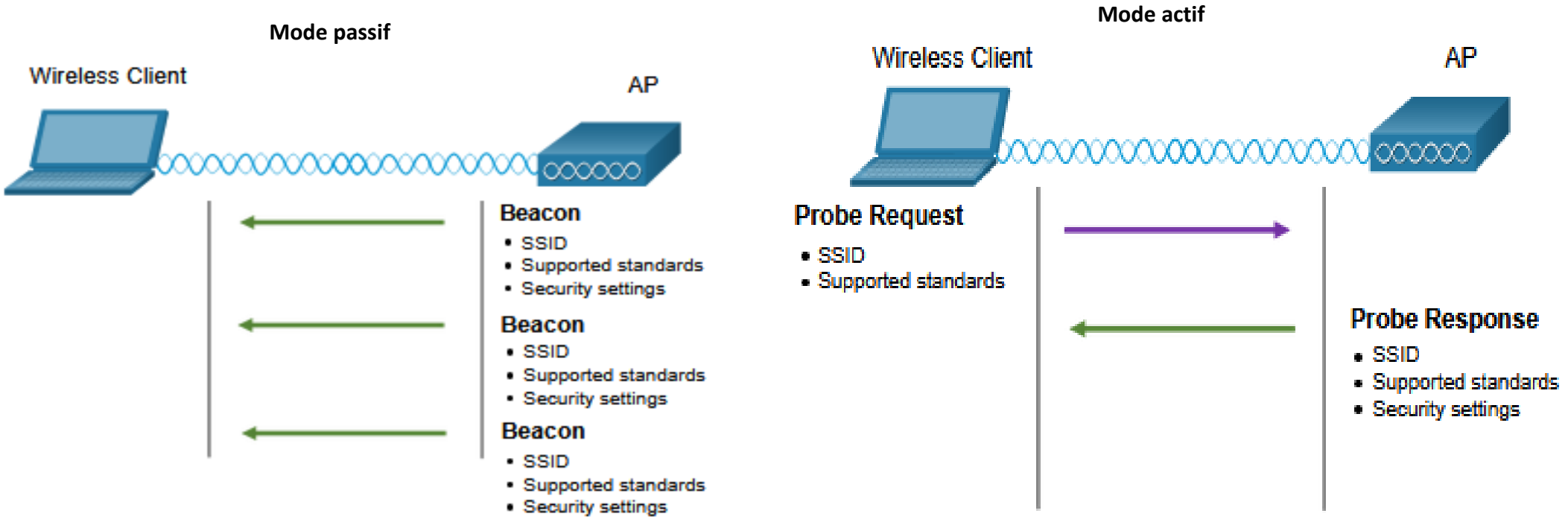


Afin d'avoir une association réussie, un client sans fil et un AP doivent se mettre d'accord sur des paramètres spécifiques.

- **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.

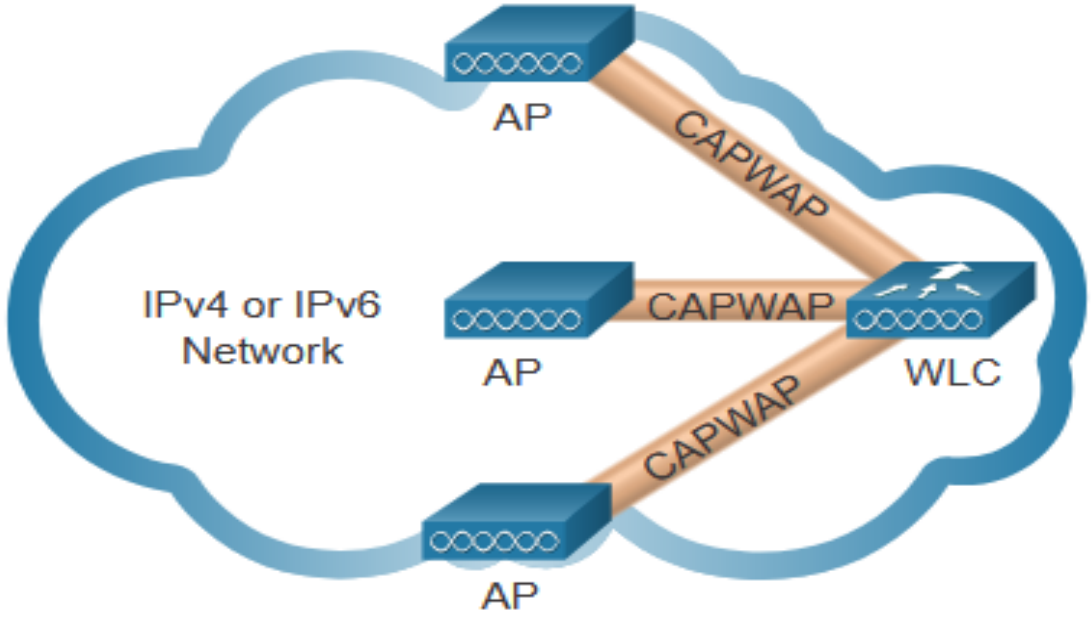
Mode découverte passif et actif

Les clients sans fil se connectent à l'AP à l'aide d'un processus de balayage (sondage) passif ou actif.



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.



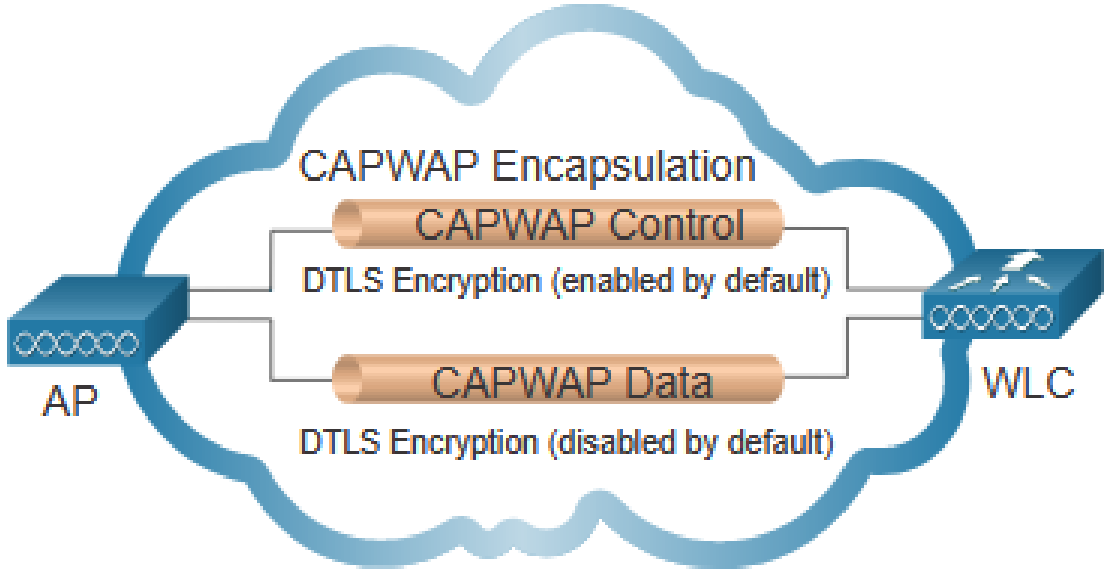
Architecture MAC divisée

Le concept de MAC divisé du CAPWAP remplit toutes les fonctions normalement remplies par les AP individuels et les répartit entre deux composantes fonctionnelles :

Fonctions MAC AP	Fonctions MAC WLC
Balises et réponses des sondes	Authentification
Accusé de réception et retransmissions de paquets	Association et réassociation de clients itinérants
Mise en file d'attente des trames et priorisation des paquets	Traduction de trame vers d'autres protocoles
Cryptage et décryptage des données de la couche MAC	Arrêt du trafic 802.11 sur une interface filaire

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.

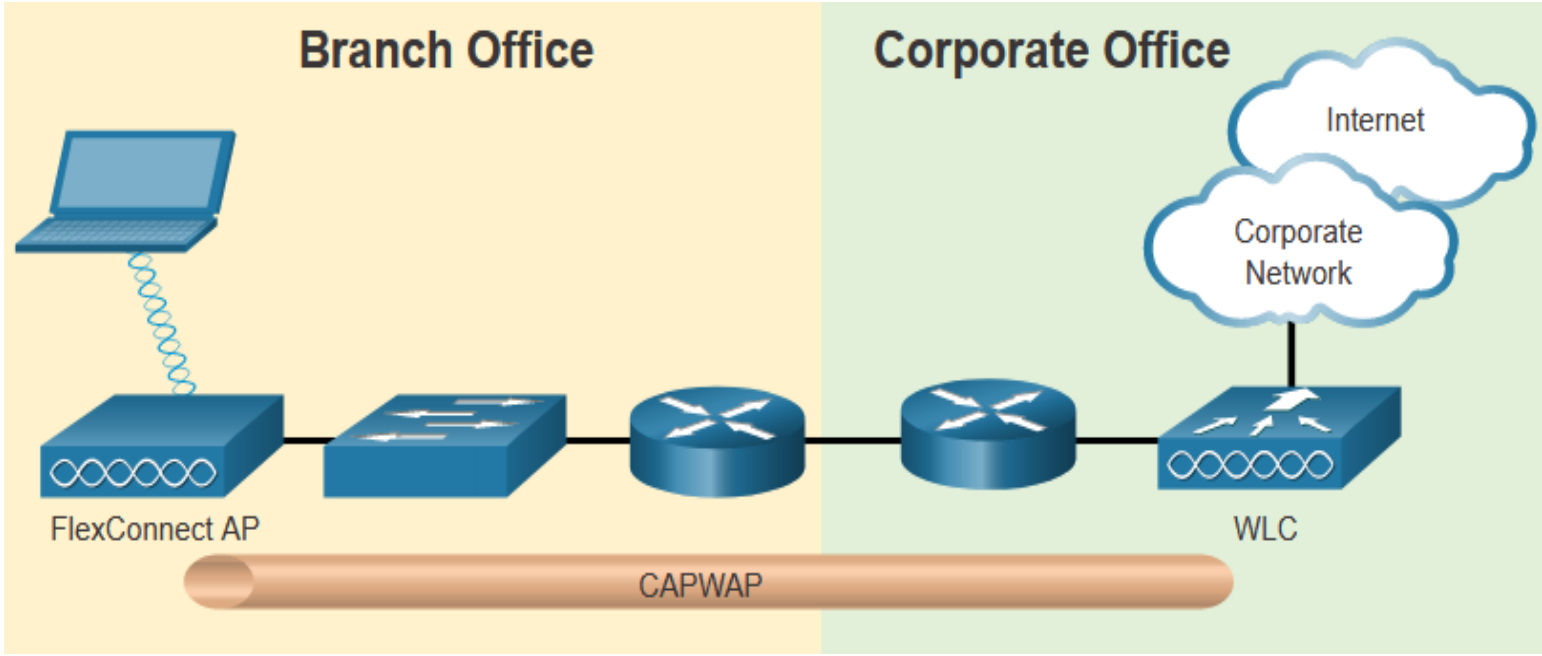


Flex Connect APs

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.

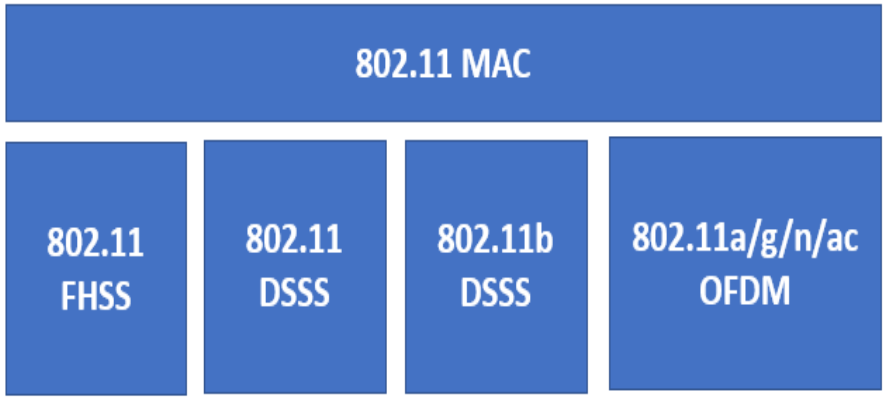


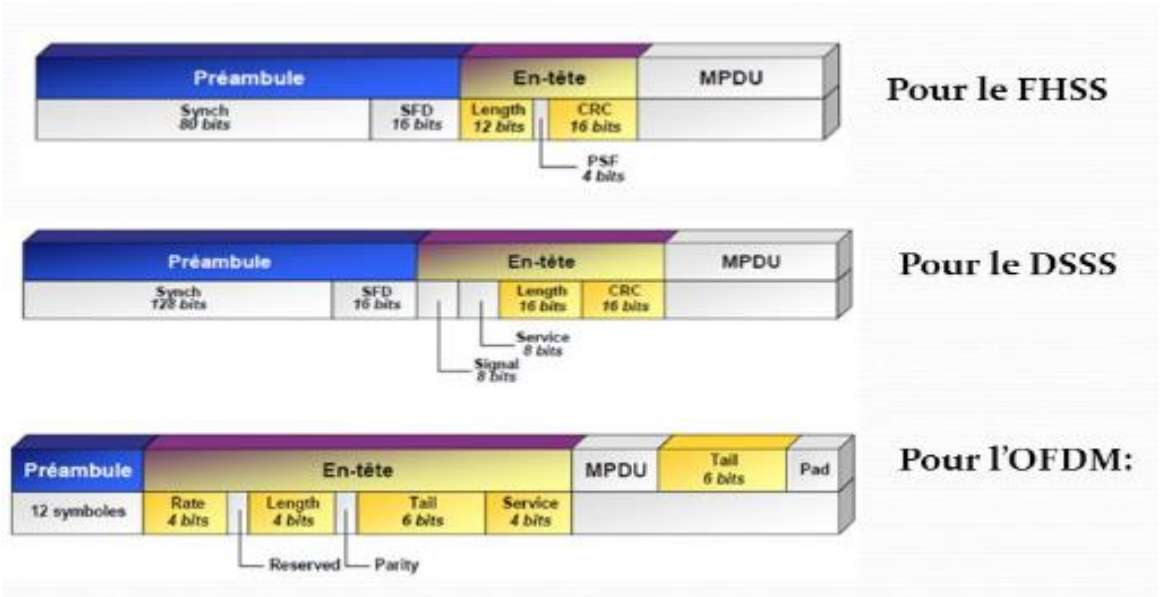
Saturation des canaux de fréquences

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 étalement de séquence directe (DSSS)** - Une technique de modulation conçue pour étaler un signal sur une bande de fréquences plus large.
- **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.
- **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.

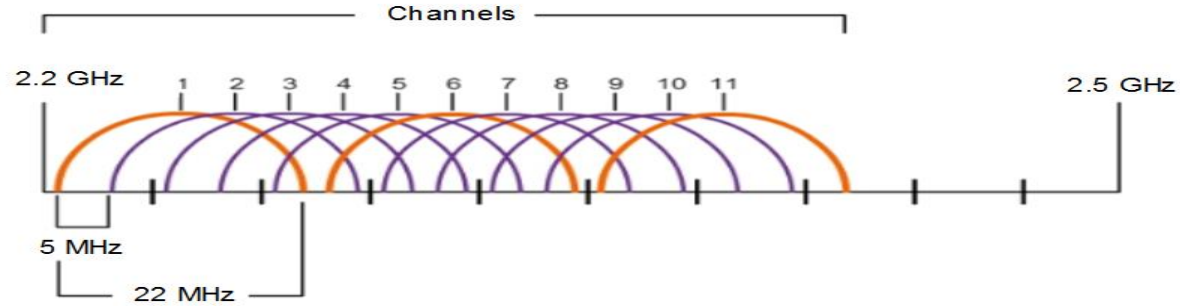




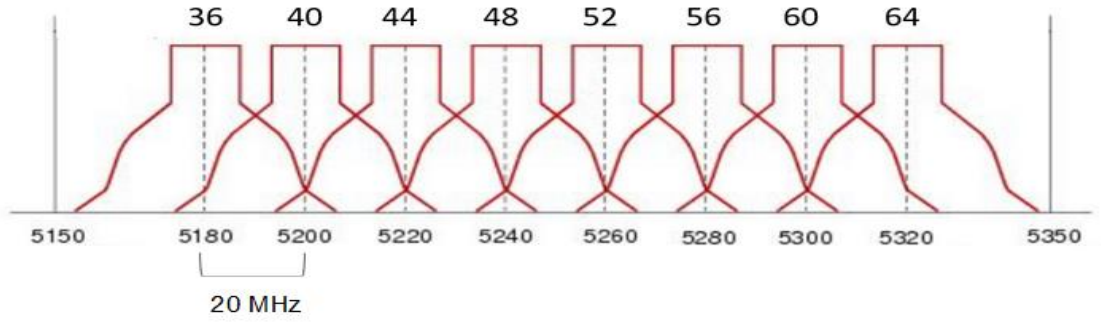
PARTIE 4

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.



- 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.



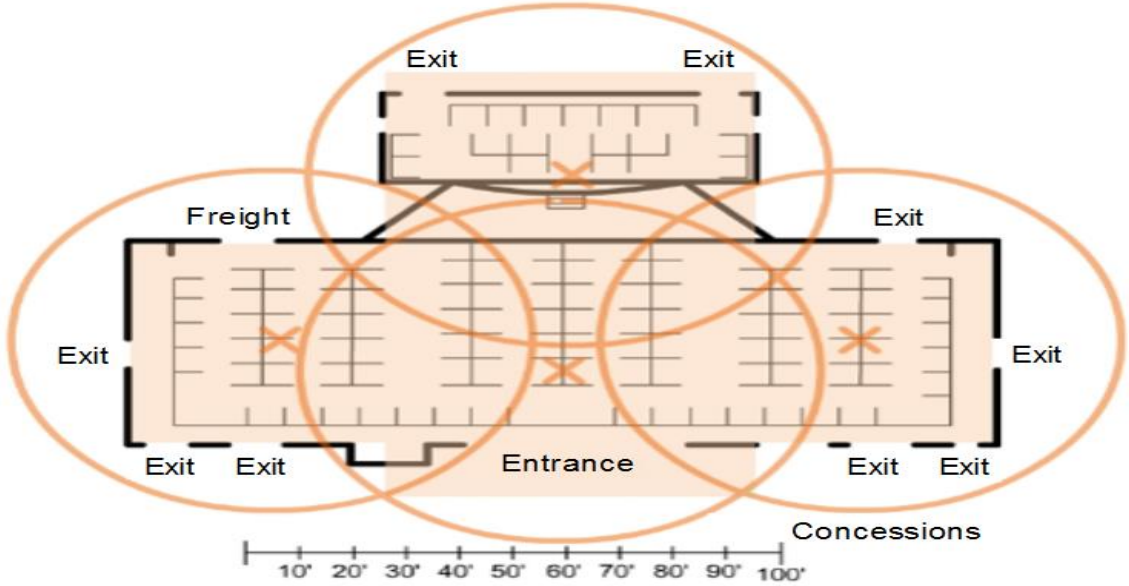
PARTIE 4

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.



CHAPITRE 2

Concevoir et sécuriser un réseau local sans fil

1. Présentation de la technologie sans fil
2. Fonctionnement d'un réseau WLAN
3. Mécanismes de sécurité WLAN
4. Configuration de 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 attaque visant le WLAN

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

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.

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

Mécanismes de sécurité WLAN

- **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

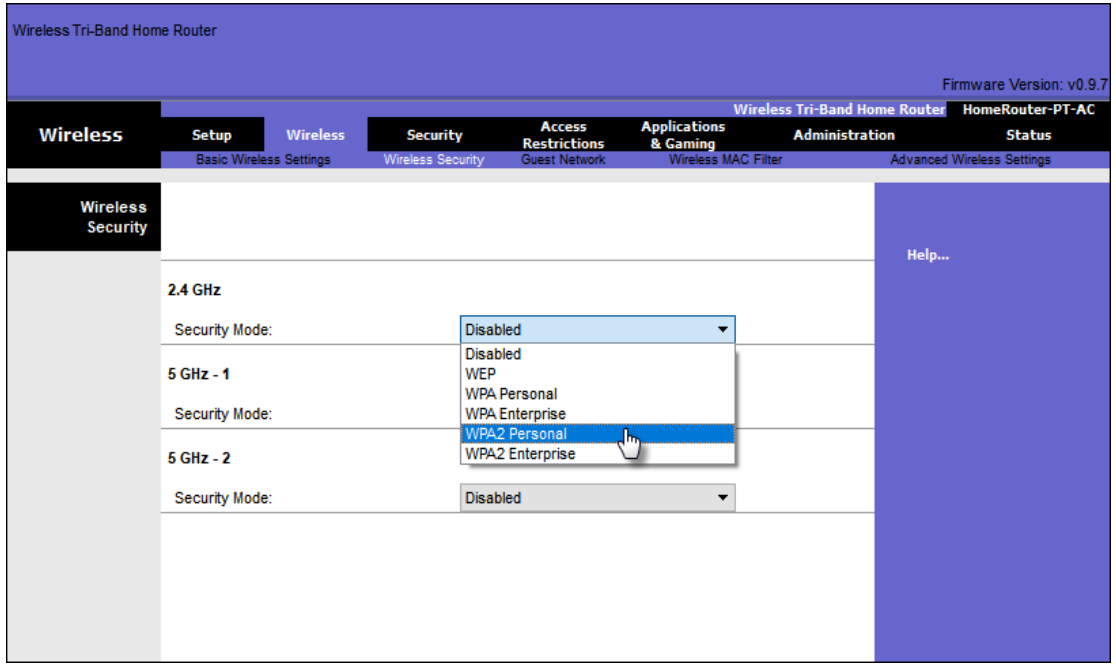
Il existe quatre techniques d'authentification par clé partagée, comme décrit dans le tableau.

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).
- **Entreprise** - Destiné aux réseaux d'entreprise. 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.

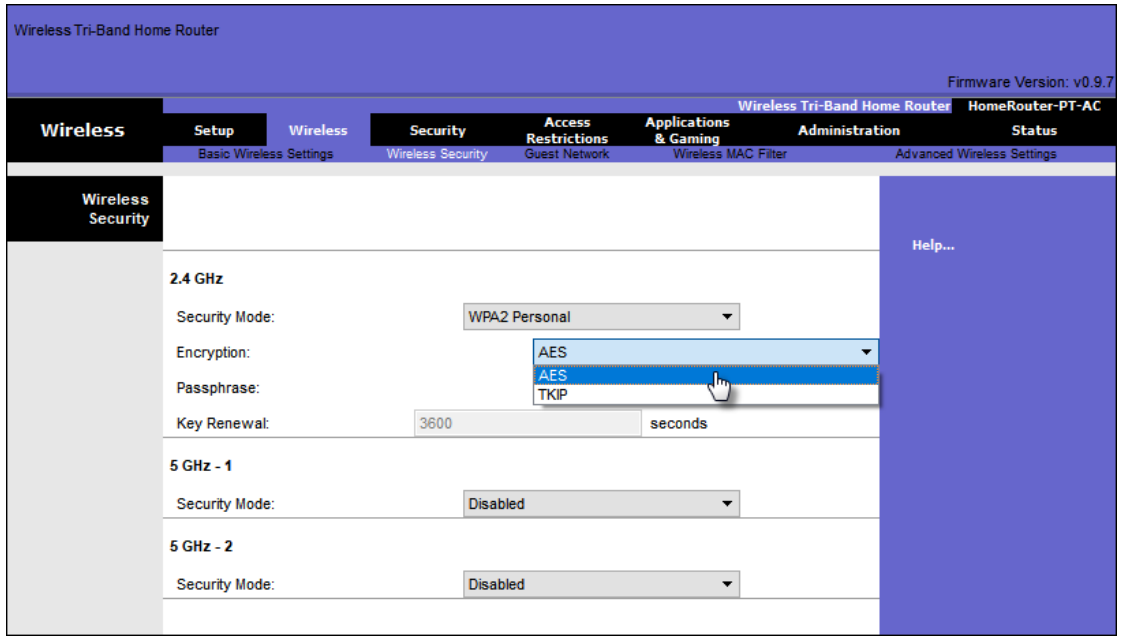


PARTIE 4

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.



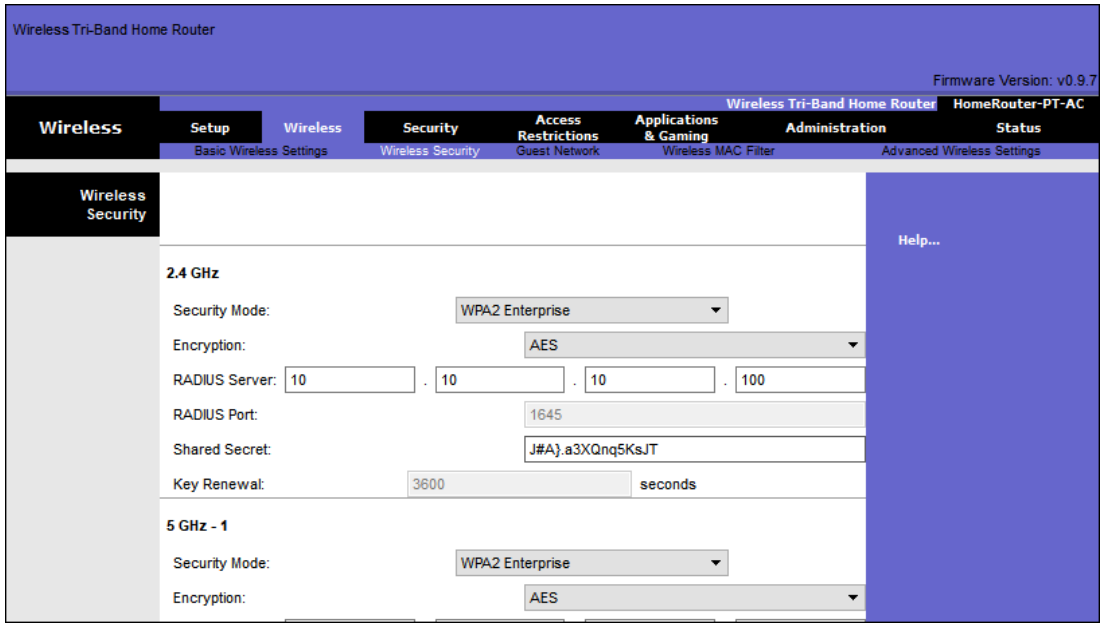
PARTIE 4

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.



PARTIE 4

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.

CHAPITRE 2

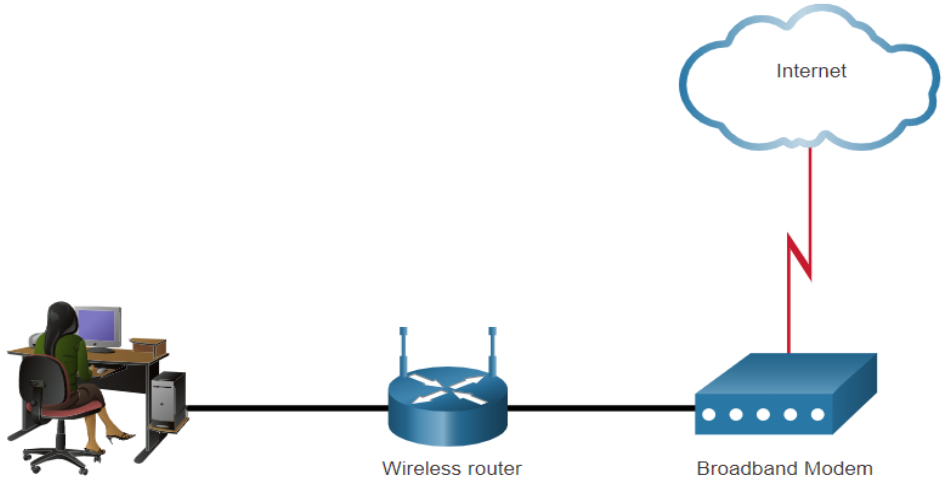
Concevoir et sécuriser un réseau local sans fil

1. Présentation de la technologie sans fil
2. Fonctionnement d'un réseau WLAN
3. Mécanismes de sécurité WLAN
4. Configuration de réseau WLAN

Configuration de base d'un réseau WLAN

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.
- Renouvelez l'adresse IP.
- Connectez-vous au routeur avec la nouvelle adresse IP.



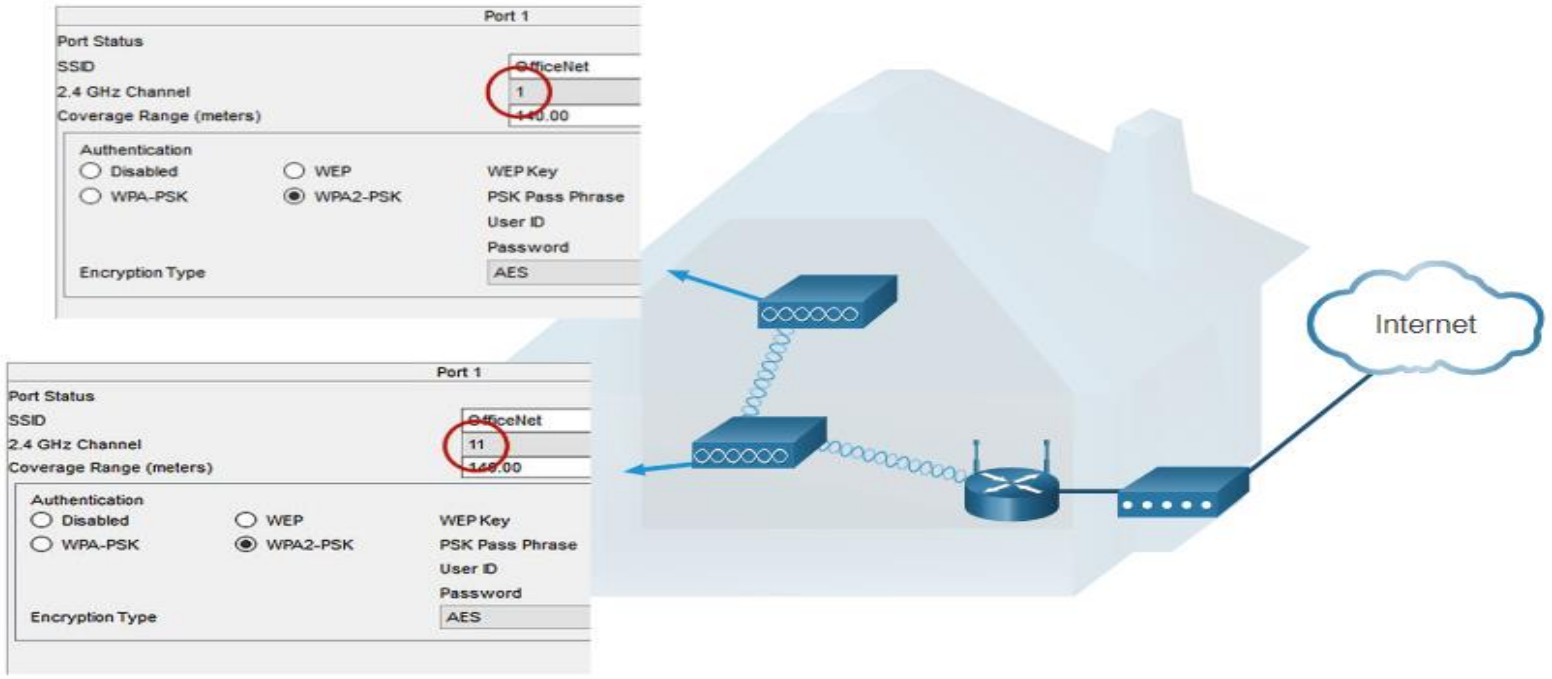
La configuration sans fil de base comprend les étapes suivantes:

- 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.
- Les fabricants ont développé des applications de smartphone qui permettent de créer rapidement un réseau sans fil maillé (WMN).



PARTIE 4

PARTIE 4

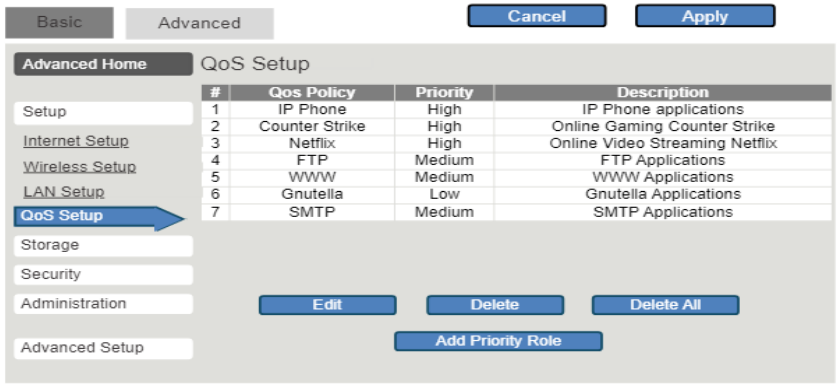
Configuration d'un WLAN

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.

Qualité de Service

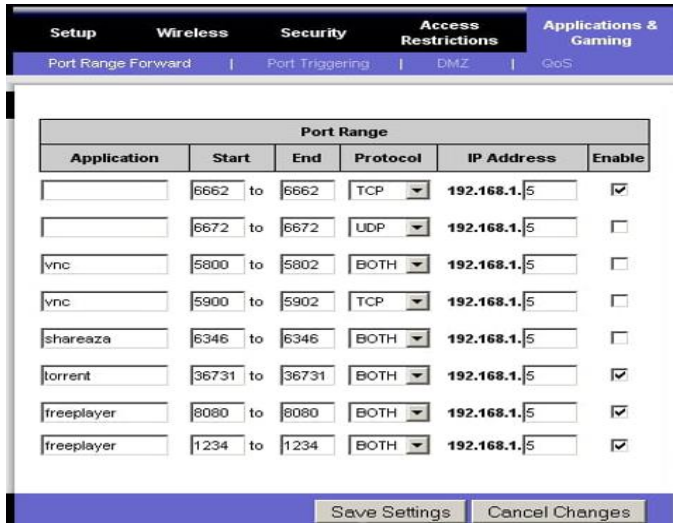
De nombreux routeurs sans fil ont une option de configuration de la qualité de service (QoS).



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.

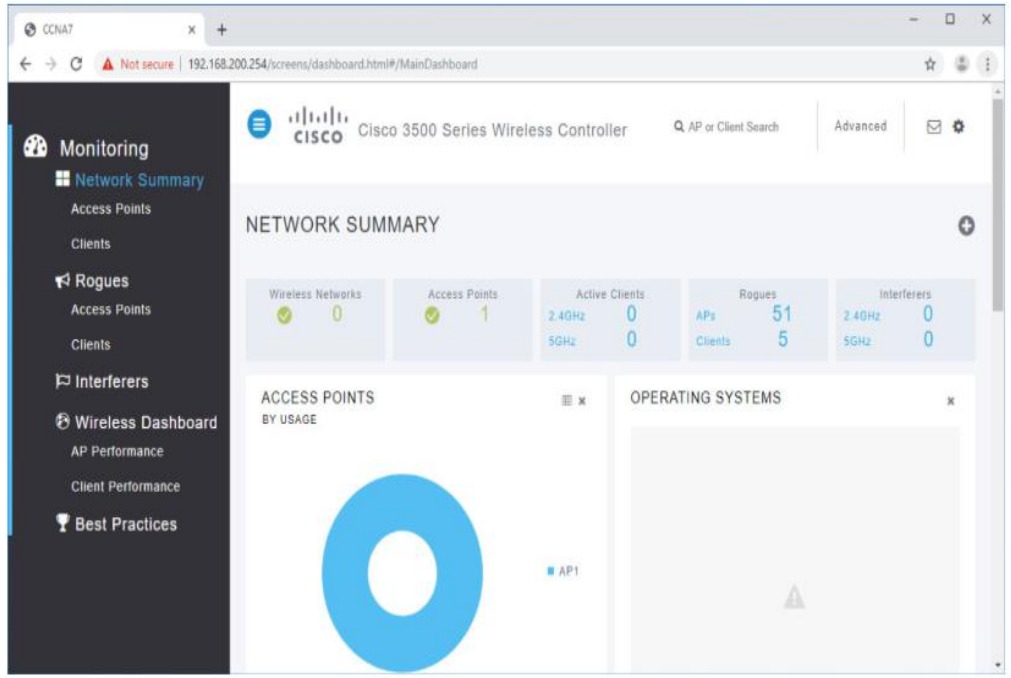


Accès au WLC

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.

- Pour vous **connecter et configurer** un contrôleur WLAN, vous devrez ouvrir un **navigateur Web** à **l'adresse IP** du contrôleur, avec HTTP ou bien HTTPS.
- Il faut bien sûr que le **contrôleur** ait déjà son **adresse IP de gestion** assignée à son interface.
- **L'interface Web** donne un moyen efficace de :
  - Surveiller
  - Configurer
  - Et de dépanner un réseau sans fil.
- Il est bien sûr possible, **si vous préférez les lignes de commandes**, de vous y connecter par une session Telnet ou SSH.

Que ce soit par l'interface Web ou l'interface CLI, les admin devront avoir un compte utilisateur de gestion.



PARTIE 4

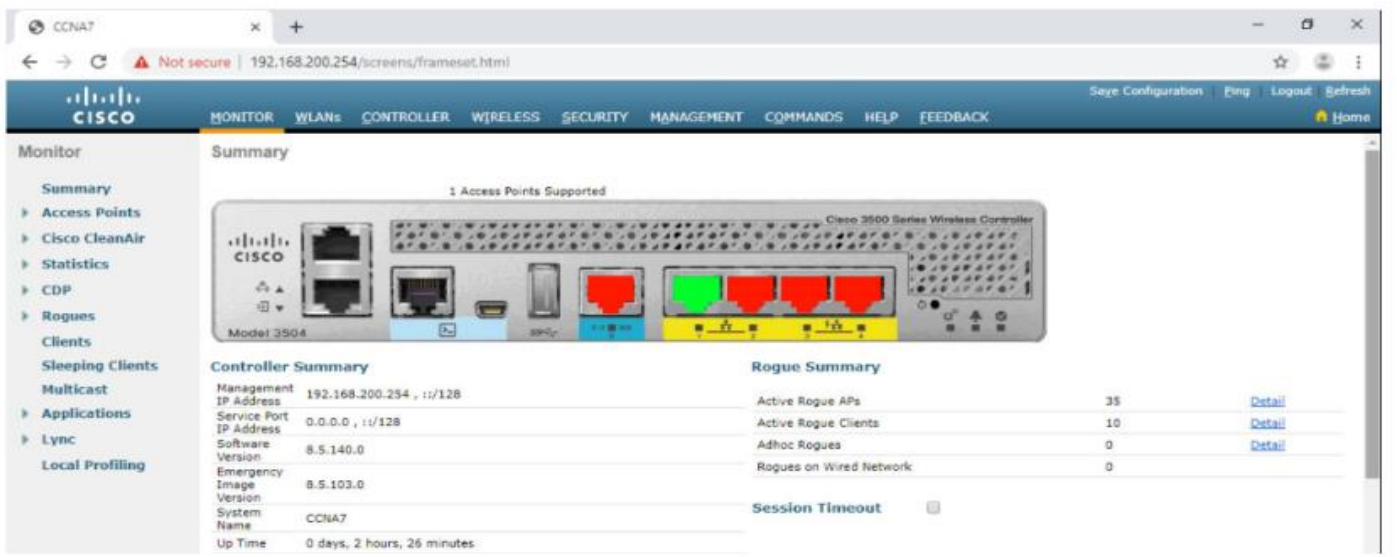
CONNEXION ÀU CONTRÔLEUR WLAN (WLC)

La connexion d'un **contrôleur LAN sans fil**, au **réseau**, n'est pas aussi simple, car il existe plusieurs types de connexions différents.

- Quand on travaille sur des routeurs ou des switches, les termes **« interfaces »** et **« port »,** sont identiques.
- Par exemple, **chez les commutateurs**, on peut les appeler **modèles 48 ports**, et on dira qu'on fait des modifs sur **des interfaces.**

Chez les contrôleurs sans fil, c'est un petit peu différent, **les ports et les interfaces** font référence à différents concepts:

- **Les ports du contrôleur** sont des **connexions physiques** à relier vers un réseau câblé ou commuté.
  Tandis que **les interfaces** sont des **connexions logiques** qui s'établissent en interne au sein même du contrôleur.



PARTIE 4

UTILISATION DES PORTS WLC

Il est possible de connecter plusieurs types différents de ports, du contrôleur au réseau.

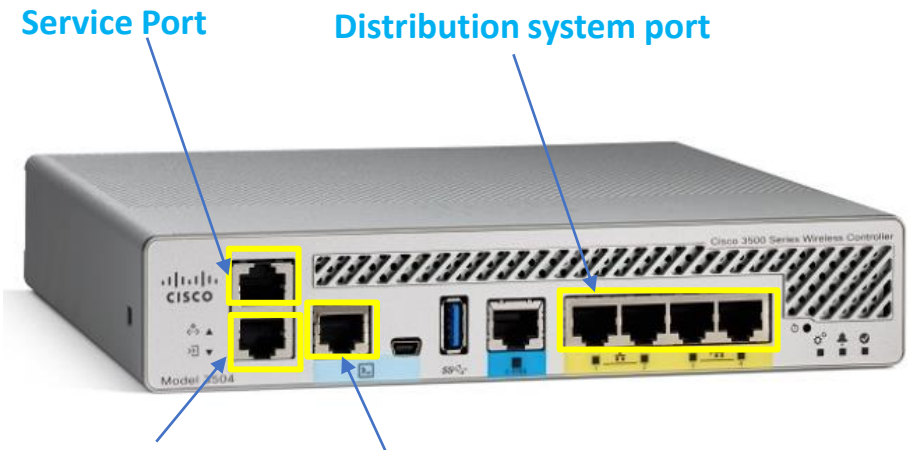
Sur le schéma, on peut voir :

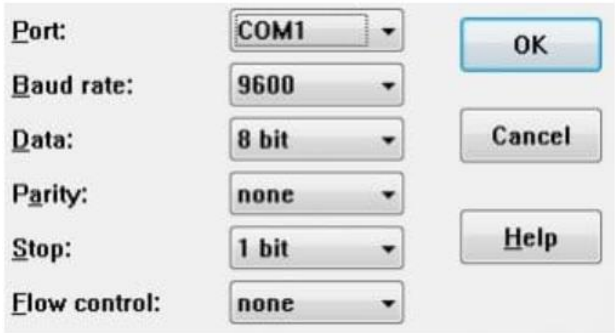
- **1 Port de service (Service Port):**
  qui est utilisé pour la gestion du système. C'est-à-dire pour **récupérer le système**, ou pour gérer les fonctions de **démarrage**. Ce port se connecte toujours à un port du switch en mode « Accès ».
  Chaque port de service, ne peut prendre en charge qu'un seul vlan.

- **Les ports de distribution du système (Distribution system port).**
  Ils sont utilisés pour le **trafic** des points d'accès et aussi pour de la **simple gestion.**
  Ce type de port se connecte généralement à un port du switch en mode « Trunk »
  Le symbole **« LAG »** représente les liens agrégés, qui permettent de regrouper plusieurs ports réseau.

- **Le Port console**:
  pour se connecter à l'aide d'un **terminal**, configurer avec les mêmes paramètres que pour la **CLI** sur les switchs et routeurs.
  C'est-à-dire :
  - Une vitesse de **9600 bauds**
  - **8 bits** de données,
  - Et **1 bit** d'arrêt

- **1 Port de redondance :**
  qui est utile pour connecter un autre contrôleur, afin de garantir un fonctionnement en haute dispo.





PARTIE 4

UTILISATION DES INTERFACES WLC

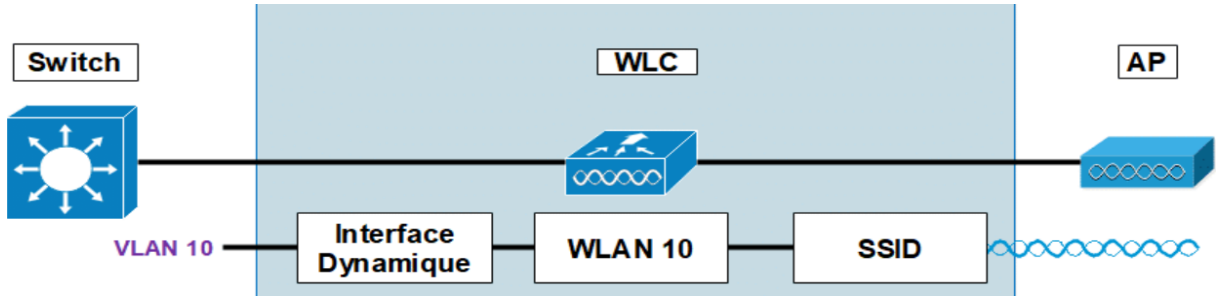
Comme pour les ports du contrôleur, on va maintenant détailler ces interfaces.

- **Interface de gestion:** qui est utilisée pour le trafic de gestion de base, c'est-à-dire pour :
  - **L'authentification** des utilisateurs RADIUS
  - La **communication** de contrôleur à contrôleur
  - Les **sessions** Web et SSH
  - **SNMP**, le protocole **NTP** (Network Time Protocol), syslog, etc.
- **Interface qui gère la redondance:** Le contrôleur actif utilisera **l'adresse de l'interface de gestion** et les contrôleurs de secours utiliseront **l'adresse qui gère la redondance**.
- **Interface virtuelle:** Le contrôleur a une **interface virtuelle** qu'il utilise pour la gestion de la mobilité.
  Ce qui inclut :
  - le relais **DHCP**
  - L'authentification **Web**
  - La terminaison **VPN**
  - D' autres fonctionnalités.

  L'adresse IP de l'interface virtuelle est utilisée uniquement dans la communication entre le contrôleur et les clients sans fil.
- **Interface du port de service:** Elle est utilisée pour communiquer avec le port de service.
- **Interface dynamique:** qui est utilisée pour connecter un **VLAN à un WLAN**. Ce qui permet d'établir des connexions logiques entre les réseaux sans fil et câblés.

La connectivitéé avec WLC

- A l'aide de ses **ports système de distribution**, un contrôleur pouvait se connecter à plusieurs VLAN sur le réseau commuté.
- Alors en interne, le contrôleur doit en quelque sorte **mapper ces VLAN câblés**, à des réseaux sans fil logiques équivalents.
- Par exemple, supposons que le **VLAN 10** soit réservé aux utilisateurs sans fil dans le service marketing d'une entreprise. Ce VLAN devra être connecté à un LAN sans fil, qui existe sur un contrôleur et sur ses points d'accès qui lui sont associés. Et le réseau sans fil doit ensuite être **étendu** à chaque client qui vient s'associer au **SSID** du service marketing.



- **Les contrôleurs sans fil** fournissent donc la connectivité par des **interfaces logiques en interne**, qui doivent être configuré avec :
  - une **adresse IP**
  - un **masque de sous-réseau**
  - une **passerelle par défaut**
  - un **serveur DHCP** (Dynamic Host Configuration Protocol).
- Chaque interface logique est ensuite affectée à un port physique et à un ID VLAN.
- On peut considérer une interface comme une terminaison de couche 3 sur un VLAN.

Approches de Dépannage

Une méthodologie de dépannage courante et efficace est basée sur la méthode scientifique et peut être divisée en six étapes principales indiquées dans le tableau.

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 implémentant 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.

PARTIE 5

Mettre en œuvre le routage d'un réseau d'entreprise

Dans ce module, vous allez :

- Etre en mesure de comprendre les mécanismes du routage
- Etre en mesure de comprendre les concepts des protocoles de routage
- Etre capable de Configurer les protocoles de routage OSPF et BGP

8 heures

CHAPITRE 1

Comprendre le Concepts de routage

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le Concepts du routage
- Configurer les routes statiques

2 heures

CHAPITRE 1

Comprendre le Concepts de routage

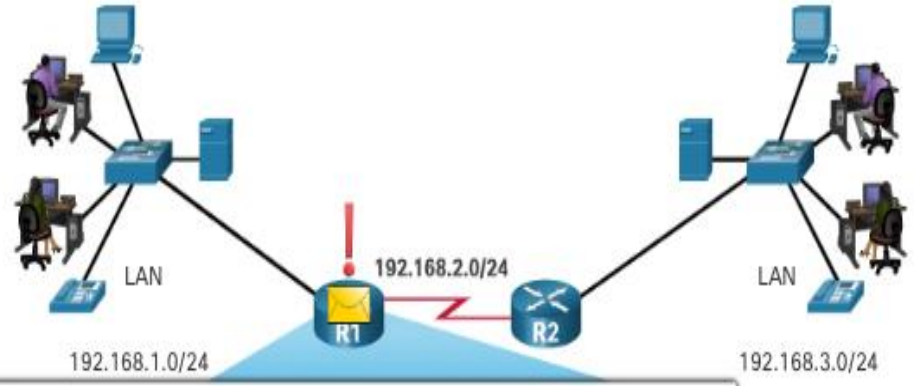
1. Concepts de routage
2. Dépanner les routes statiques et par défaut

Deux fonctions d'un routeur

Les principales fonctions d'un routeur consistent à **déterminer le meilleur chemin** d'acheminement des paquets en fonction des informations contenues dans sa table de routage, et à **transférer des paquets** vers leur destination.

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

R1 et R2 utiliseront leurs tables de routage IP respectives pour déterminer d'abord le meilleur chemin, puis transférer le paquet.




```
R1# show ip route
Codes:
C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default
U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, Serial0/0/0
S    192.168.3.0/24 [1/0] via 192.168.2.2
```

Routers use the routing table like a map to discover the best path for a given network.

PARTIE 5

Détermination du chemin

- **Le meilleur chemin équivaut à la plus longue correspondance**

- Le meilleur chemin dans la table de routage est également connu comme la correspondance la plus longue.
- La table de routage contient des entrées de routage composées d'un préfixe (adresse réseau) et d'une longueur de préfixe.
- La longueur du préfixe de l'itinéraire dans la table de routage est utilisée pour déterminer le nombre minimum de bits d'extrême gauche qui doivent correspondre.
- La correspondance la plus longue est celle qui, dans la table de routage, présente le plus grand nombre de bits de correspondance d'extrême gauche avec l'adresse IP de destination du paquet. La correspondance la plus longue est toujours l'itinéraire préféré.

Remarque: Le terme longueur du préfixe sera utilisé pour faire référence à la partie réseau des adresses IPv4 et IPv6.

Exemple de la plus longue correspondance IPv4

Un paquet IPv4 a l'adresse IPv4 de destination **172.16.0.10**. Le routeur a trois entrées de route dans sa table de routage IPv4 qui correspondent à ce paquet : **172.16.0.0/12**, **172.16.0.0/18** et **172.16.0.0/26**. Parmi les trois routes, **172.16.0.0/26** est celle qui présente la plus longue correspondance et doit être choisir pour transférer le paquet.

Exemple de la plus longue correspondance IPv6

Un paquet IPv6 a l'adresse IPv6 de destination **2001:db8:c000::99**. . Le routeur a trois entrées de route dans sa table de routage IPv6 qui correspondent à ce paquet : **2001:db8:c000::/40**, **2001:db8:c000::/48** et **2001:db8:c000:5555::/64**. la deuxième entrée d'itinéraire **/48** qui présente la plus longue correspondance. La troisième entrée d'itinéraire n'est pas une correspondance car son préfixe **/64** nécessite 64 bits correspondants.

Création de la table de routage

Réseaux directement connectés : Ajouté à la table de routage lorsqu'une interface locale est configurée avec une adresse IP et un masque de sous-réseau (longueur du préfixe) et qu'elle est active (up et up).

Réseaux distants :Réseaux qui ne sont pas directement connectés au routeur. Un routeur apprend des réseaux distants de deux manières différentes:

- **Routes statiques** - Ajoutés à la table de routage lorsqu'un itinéraire est configuré manuellement.
- **Protocoles de routage dynamique** - Ajoutés à la table de routage lorsque les protocoles de routage apprennent dynamiquement sur le réseau distant.

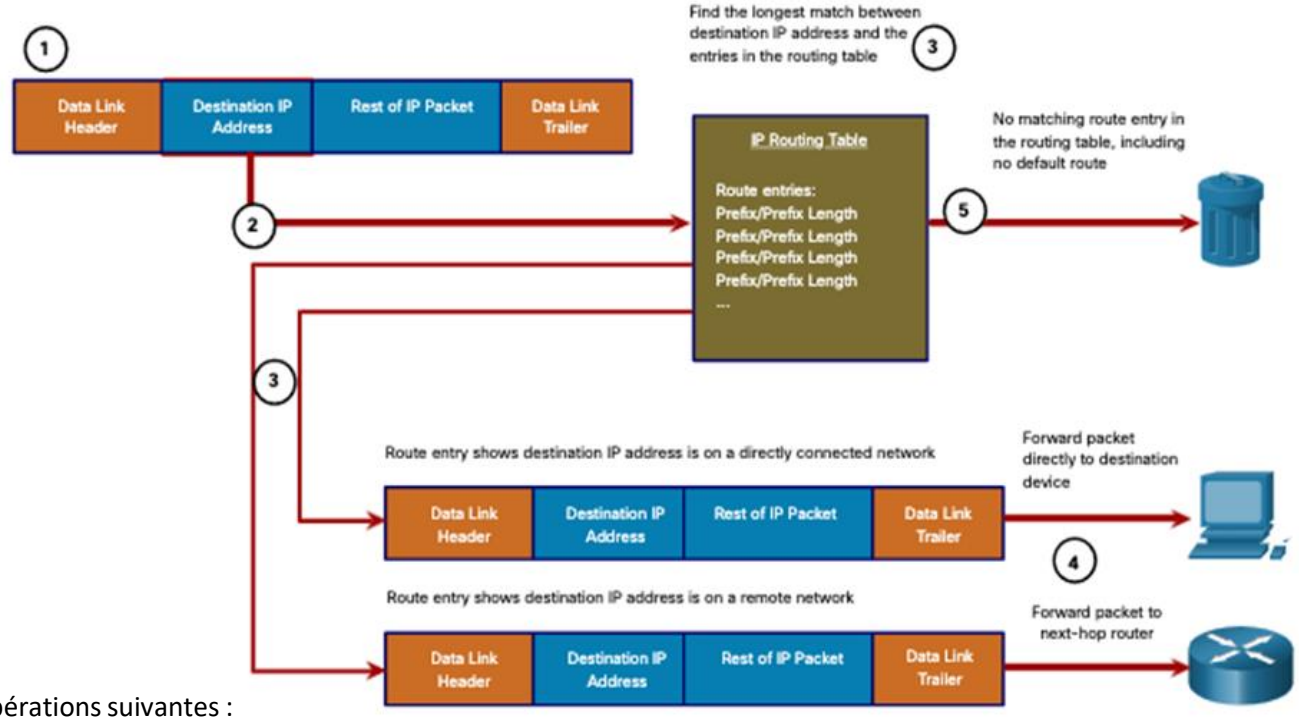
Route par défaut : spécifie un routeur de saut suivant à utiliser lorsque la table de routage ne contient pas d'itinéraire spécifique correspondant à l'adresse IP de destination. L'itinéraire par défaut peut être saisi manuellement sous forme d'itinéraire statique ou appris automatiquement à partir d'un protocole de routage dynamique.

- Une route par défaut a une longueur de préfixe /0. Cela signifie qu'aucun bit ne doit correspondre à l'adresse IP de destination pour que cette entrée d'itinéraire soit utilisée. S'il n'y a pas de routes avec une correspondance supérieure à 0 bits, l'itinéraire par défaut est utilisé pour transférer le paquet. L'itinéraire par défaut est parfois appelé passerelle de dernier recours.

Transmission de paquets

- **Processus de décision sur la transmission des paquets**

1. Le bloc de liaison de données avec un paquet IP encapsulé arrive sur l'interface d'entrée.
2. Le routeur examine l'adresse IP de destination dans l'en-tête du paquet et consulte sa table de routage IP.
3. Le routeur trouve le préfixe correspondant le plus long dans la table de routage.
4. Le routeur encapsule le paquet dans un cadre de liaison de données et le transmet à l'extérieur de l'interface de sortie. La destination peut être un périphérique connecté au réseau ou un routeur de saut suivant.
5. Toutefois, s'il n'y a pas d'entrée de route correspondante, le paquet est supprimé.



Une fois qu'un routeur a déterminé le meilleur chemin, il peut effectuer les opérations suivantes :

- **Transférer le paquet à un périphérique sur un réseau directement connecté**
- **Transférer le paquet à un routeur de saut suivant**
- **Déposer le paquet - Aucune correspondance dans la table de routage**

PARTIE 5

Transmission de paquets

Transmission de paquets de bout en bout

La responsabilité principale de la fonction de transfert de paquets est d'encapsuler les paquets au type de trame de liaison de données approprié pour l'interface de sortie. Par exemple, le format de trame de liaison de données pour une liaison série peut être le protocole PPP (Point-to-Point), le protocole HDLC (High-Level Data Link Control) ou un autre protocole de couche 2.

Mécanismes de transmission de paquets

La responsabilité principale de la fonction de transfert de paquets est d'encapsuler les paquets au type de trame de liaison de données approprié pour l'interface de sortie. Plus un routeur peut effectuer cette tâche efficacement, plus les paquets peuvent être transférés plus rapidement par le routeur.

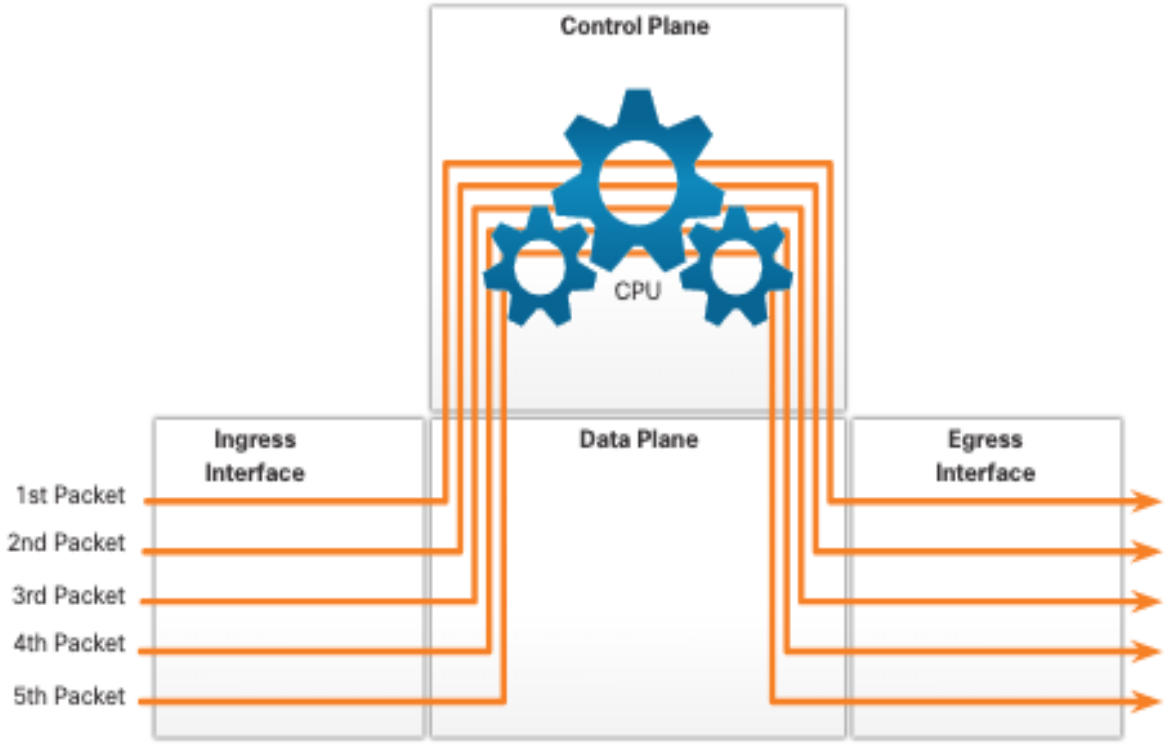
Les routeurs prennent en charge trois mécanismes de transfert des paquets:

- Commutation de processus
- Commutation rapide
- Protocole CEF (Cisco Express Forwarding)

Mécanismes de transmission de paquets

- **Processus de commutation :**

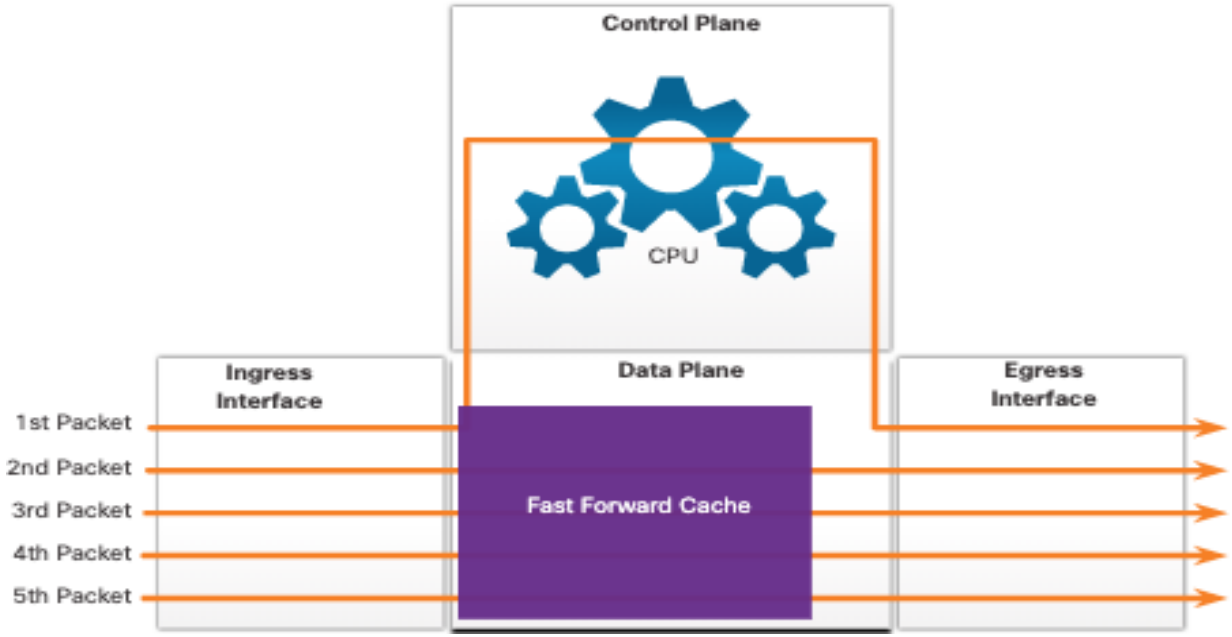
Un ancien mécanisme de transmission de paquets encore disponible pour les routeurs Cisco. Lorsqu'un paquet arrive sur une interface, il est transféré au plan de contrôle où le processeur fait correspondre l'adresse de destination avec une entrée de sa table de routage, puis détermine l'interface de sortie et transmet le paquet. Il est important de comprendre que le routeur effectue cette opération pour chaque paquet, même si la destination est identique pour une série de paquets.



Mécanismes de transmission de paquets

- **Commutation rapide :**

Un autre mécanisme de transfert de paquets plus ancien qui a succédé à la commutation de processus. Commutation rapide utilise un cache à commutation rapide pour stocker les informations du saut suivant. Lorsqu'un paquet arrive sur une interface, il est transféré au plan de contrôle où le processeur (CPU) recherche une correspondance dans le cache à commutation rapide. S'il ne trouve rien, le paquet est commuté par le processus et transféré à l'interface de sortie. Les informations relatives au flux du paquet sont ensuite stockées dans le cache à commutation rapide. Si un autre paquet ayant la même destination arrive sur une interface, les informations de tronçon suivant du cache sont réutilisées sans intervention du processeur.



Mécanismes de transmission de paquets

- **Cisco Express Forwarding (CEF) :**

Le mécanisme de transmission de paquets Cisco IOS le plus récent et par défaut. Le CEF construit une base d'informations sur les expéditions (FIB), et un tableau de contiguïté. Les entrées des tables ne sont pas déclenchées par des paquets comme dans le cas d'une commutation rapide, mais par des changements, par exemple lorsque quelque chose change dans la topologie du réseau. Lorsqu'un réseau a convergé, le FIB et les tables de contiguïté contiennent toutes les informations qu'un routeur doit prendre en compte pour acheminer un paquet.

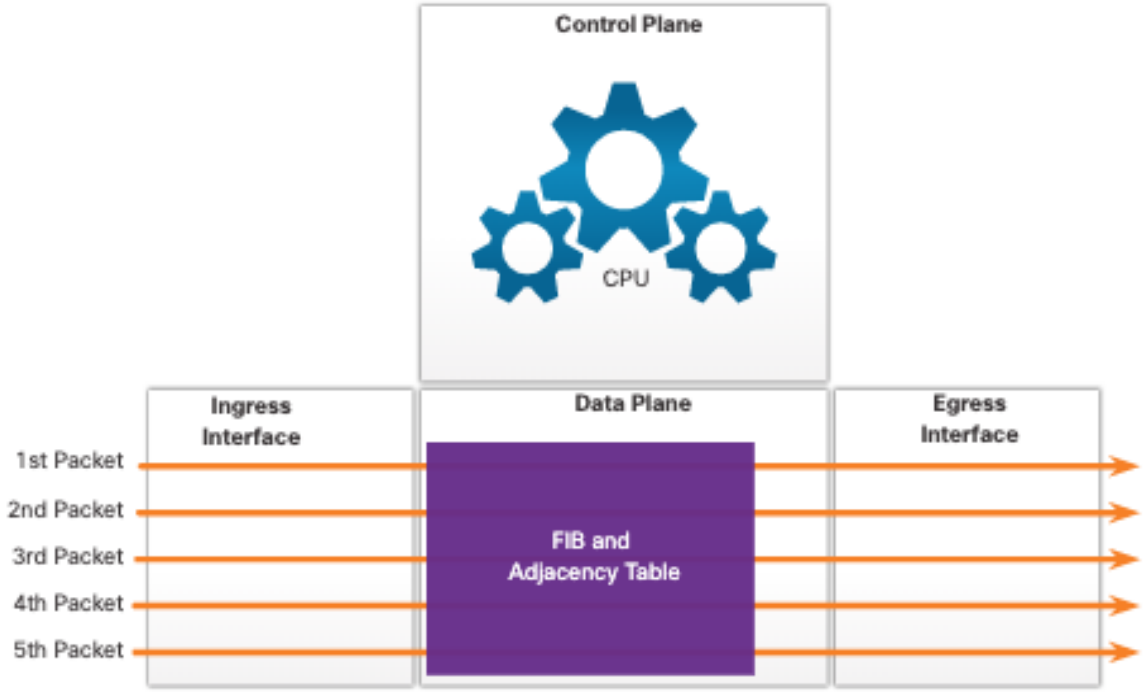


Table de routage IP

Une table de routage contient une liste d'itinéraires vers des réseaux connus (préfixes et longueurs de préfixes). La source de cette information est dérivée des éléments suivants :

- Réseaux connectés directement
- Routes statiques
- Protocoles de routage dynamiques.

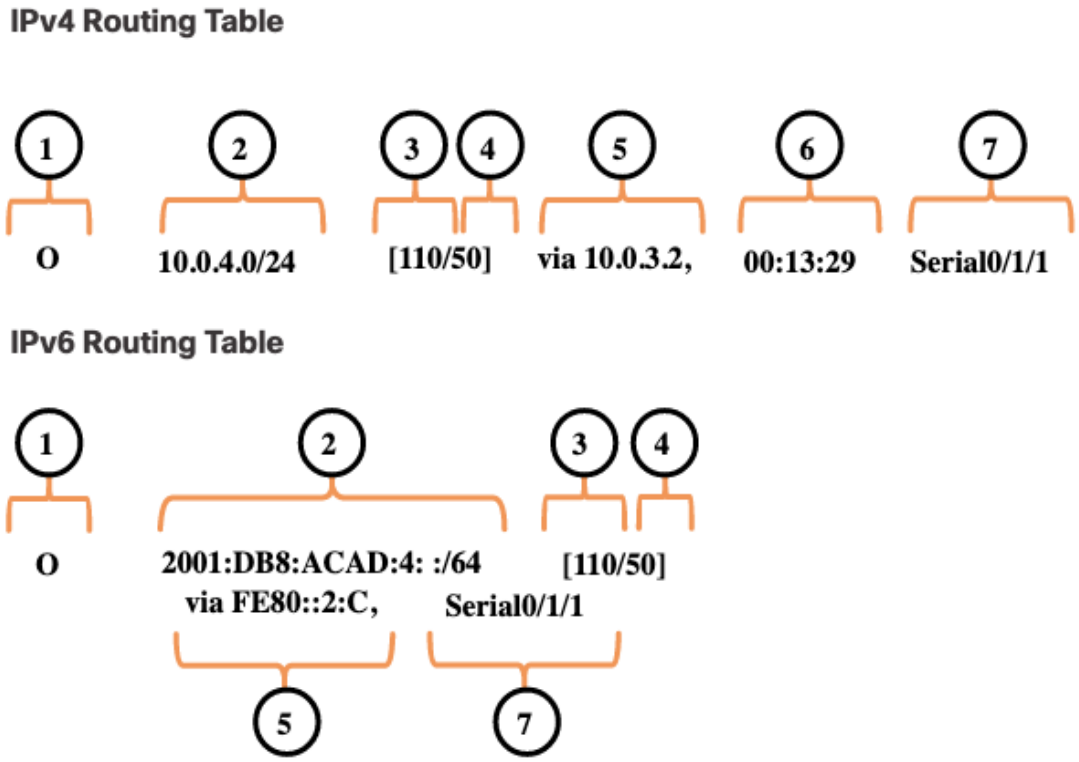
La source de chaque itinéraire dans la table de routage est identifiée par un code. Les codes communs comprennent les éléments suivants :

- **L** - Identifie l'adresse assignée à une interface de routeur.
- **C** - Identifie un réseau connecté directement.
- **S** - Identifie une route statique créée pour atteindre un réseau donné.
- **O** - Identifie un réseau découvert de manière dynamique depuis un autre routeur à l'aide du protocole de routage OSPF.
- ***** - Cette route peut convenir comme route par défaut.

Entrées de la table de routage

Dans la figure, les chiffres identifient les informations suivantes :

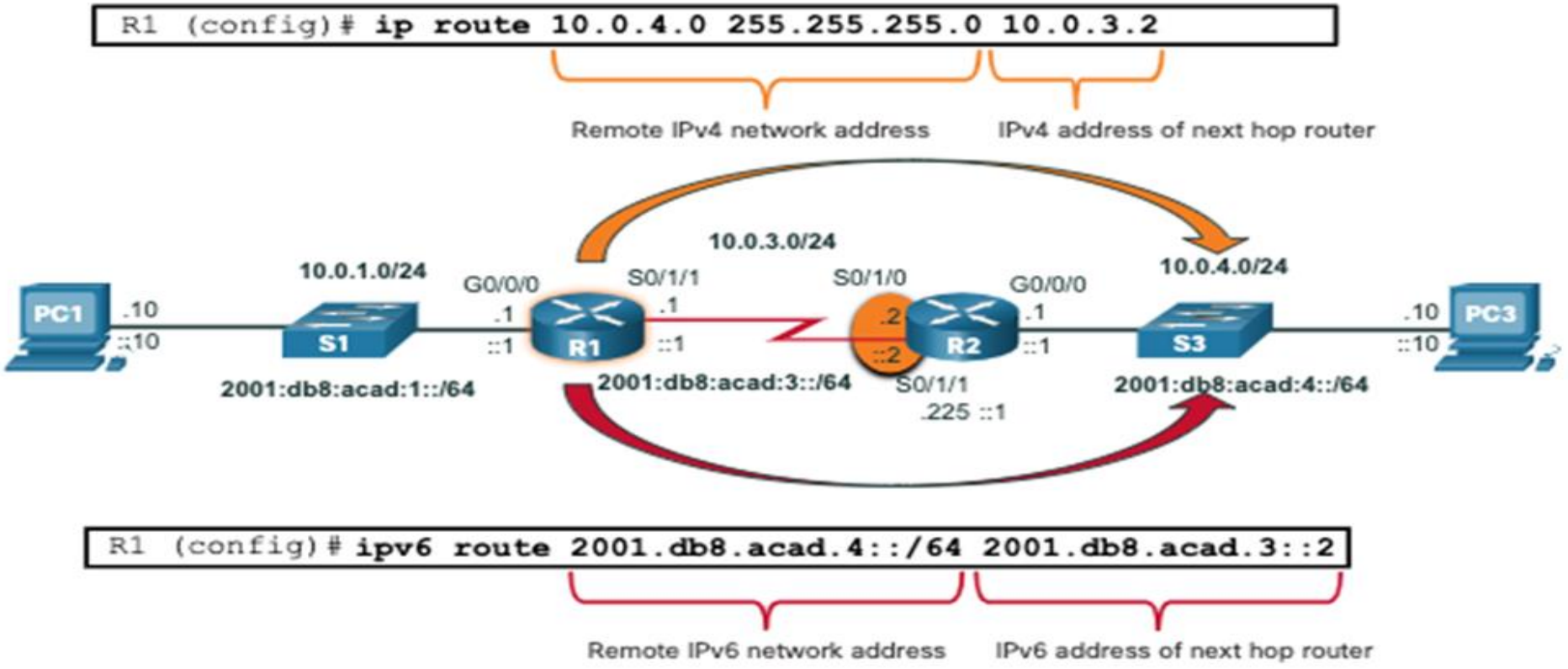
1. **Source de l'itinéraire (Route source)** - : indique comment l'itinéraire a été appris.
2. **Réseau de destination (préfixe et longueur du préfixe)** - : Identifie l'adresse du réseau distant.
3. **Distance administrative**- identifie la fiabilité de la source de la route. Des valeurs inférieures indiquent la route source préférée.
4. **Métrique** - : indique de la valeur attribuée pour atteindre le réseau distant. Les valeurs les plus faibles indiquent les routes préférées.
5. **Saut suivant** - : identifie l'adresse IP du prochain routeur vers lequel le paquet sera transféré.
6. **Horodatage de route** - : indique la durée écoulée depuis que la route a été découverte.
7. **Interface de sortie** - : Elle identifie l'interface de sortie à utiliser pour que les paquets sortants atteignent leur destination finale.



PARTIE 5

Routes statiques dans la table de routage IP

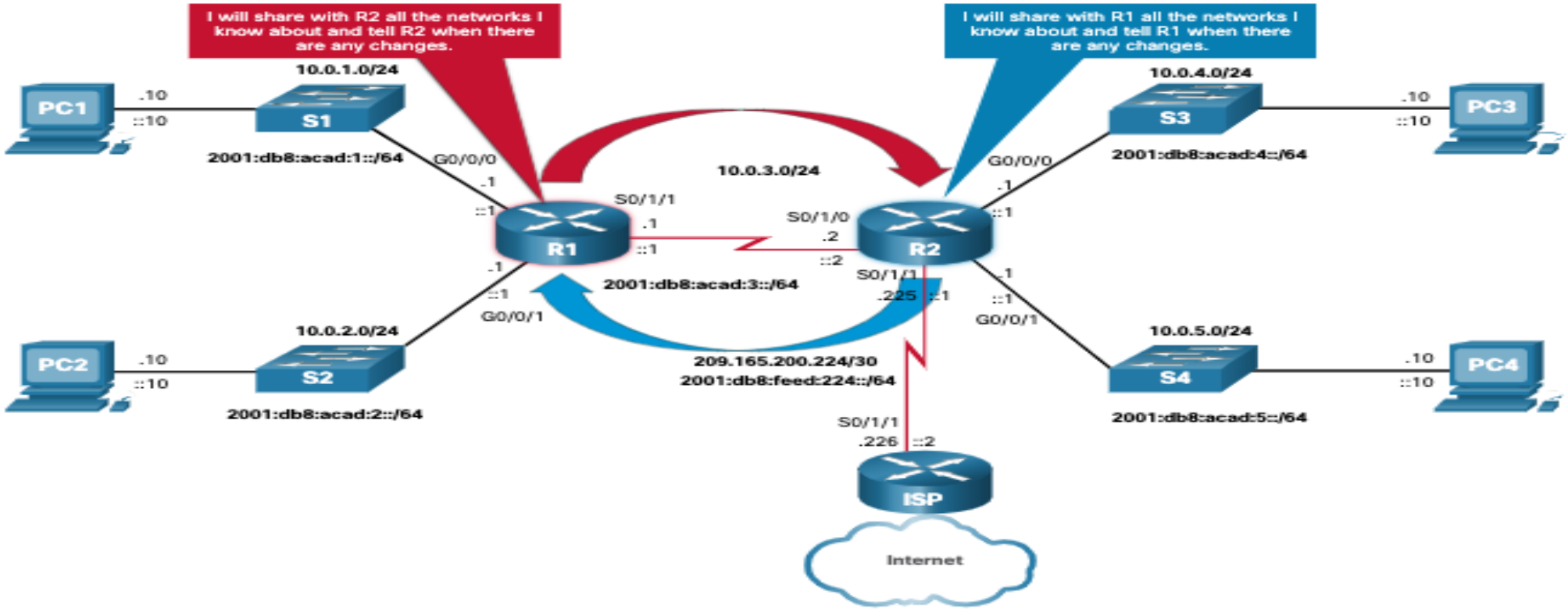
La topologie de la figure est simplifiée pour afficher un seul réseau local connecté à chaque routeur. La figure montre les routes statiques IPv4 et IPv6 configurées sur R1 pour atteindre les réseaux 10.0.4.0/24 et 2001:db8:acad:4::/64 sur R2.



PARTIE 5

Protocoles de routage dynamique

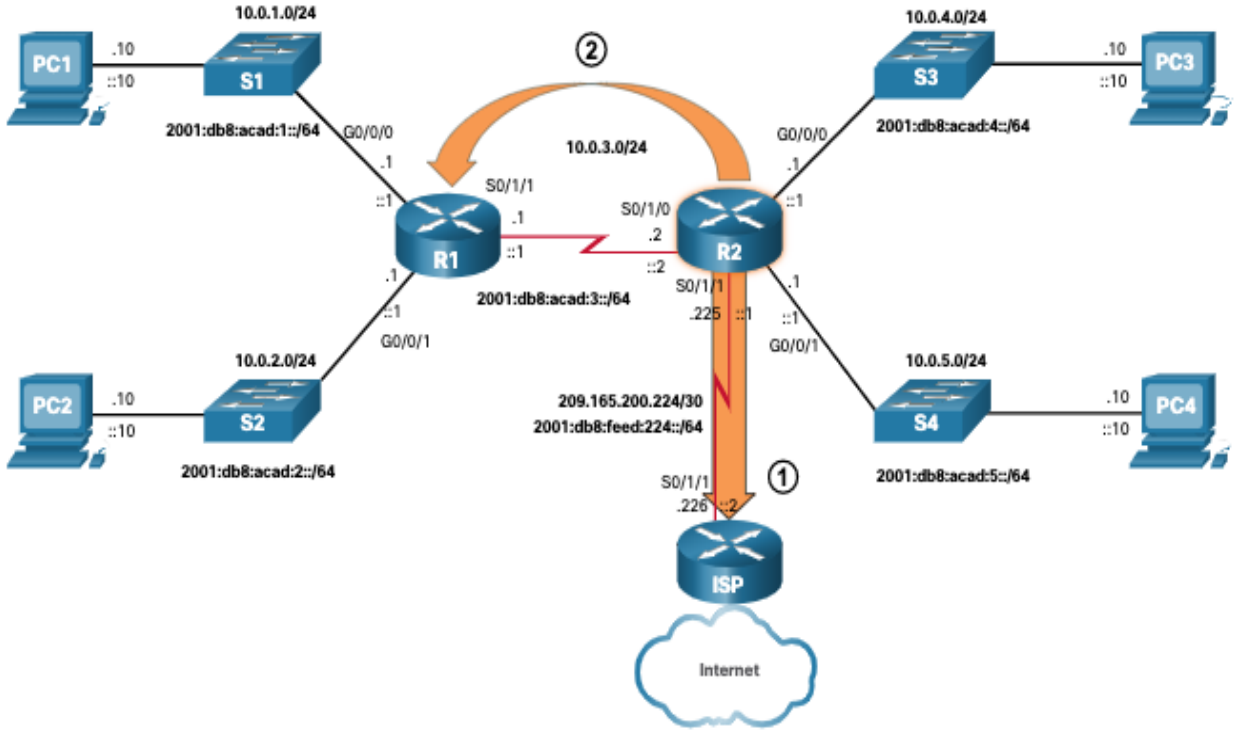
Les protocoles de routage dynamique sont utilisés par les routeurs pour partager automatiquement des informations sur l'accessibilité et l'état des réseaux distants. Les protocoles de routage dynamique effectuent plusieurs tâches, notamment la détection de réseaux et la gestion des tables de routage.



PARTIE 5

Route par défaut

La route par défaut spécifie un routeur de saut suivant à utiliser lorsque la table de routage ne contient pas de route spécifique correspondant à l'adresse IP de destination. Une route par défaut peut être soit une route statique, soit apprise automatiquement à partir d'un protocole de routage dynamique. Une route par défaut a une entrée d'itinéraire IPv4 0.0.0.0/0 ou une entrée d'itinéraire IPv6 de ::/0. Cela signifie que zéro ou aucun bit doit correspondre entre l'adresse IP de destination et l'itinéraire par défaut.



PARTIE 5

Structure d'une table de routage IPv4 et IPv6

```
Router# show ip route
(Output omitted)
   192.168.1.0/24 is variably..
C 192.168.1.0/24 is direct..
L 192.168.1.1/32 is direct..
O 192.168.2.0/24 [110/65]..
O 192.168.3.0/24 [110/65]..
   192.168.12.0/24 is variab..
C 192.168.12.0/30 is direct..
L 192.168.12.1/32 is direct..
   192.168.13.0/24 is variably..
C 192.168.13.0/30 is direct..
L 192.168.13.1/32 est direct..
   192.168.23.0/30 is subnette..
O 192.168.23.0/30 [110/128]..
Router#
```

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
   via FE80::2:C, Serial0/0/1
C 2001:DB8:ACAD:1::/64 [0/0]
   via GigabitEthernet0/0/0, directly connected
L 2001:DB8:ACAD:1::1/128 [0/0]
   via GigabitEthernet0/0/0, receive
C 2001:DB8:ACAD:2::/64 [0/0]
  via GigabitEthernet0/0/1, directly connected
L 2001:DB8:ACAD:2::1/128 [0/0]
   via GigabitEthernet0/0/1, receive
C 2001:DB8:ACAD:3::/64 [0/0]
   via Serial0/1/1, directly connected
L 2001:DB8:ACAD:3::1/128 [0/0]
   via Serial0/1/1, receive
O 2001:DB8:ACAD:4::/64 [110/50]
   via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
   via FE80::2:C, Serial0/1/1
L FF00::/8 [0/0]
   via Null0, receive
R1#
```

Distance administrative

Chaque protocole de routage peut décider d'un chemin différent pour atteindre la destination en fonction de la métrique de ce protocole de routage.

Cela soulève quelques questions, notamment les suivantes :

- Comment le routeur sait-il quelle source utiliser ?
- Quel itinéraire doit-il installer dans la table de routage ?

Le logiciel CISCO IOS utilise ce que l'on appelle la distance administrative (AD) pour déterminer la route à installer dans la table de routage IP. L'AD indique la «fiabilité» de la route. Plus la distance administrative est faible, plus la route est fiable.

Origine de la route	Distance administrative
Directement connecté	0
Route statique	1
Résumé du routage EIGRP	5
BGP externe	20
EIGRP interne	90
OSPF	110
IS-IS	115
RIP	120
EIGRP externe	170
BGP interne	200

La table répertorie divers protocoles de routage et leurs AD associés.

Routage statique et dynamique

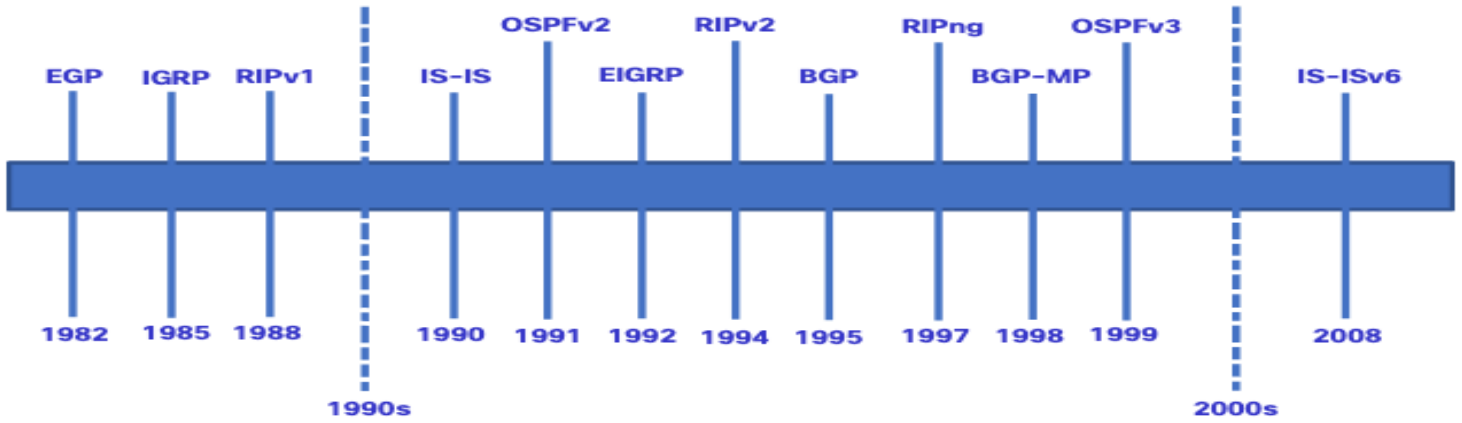
Le routage statique et le routage dynamique ne s'excluent pas mutuellement. En revanche, la plupart des réseaux utilisent une combinaison de protocoles de routage dynamique et de routes statiques.

Le tableau présente une comparaison de certaines différences entre le routage dynamique et statique.

Fonctionnalité	Routage dynamique	Routage statique
Complexité de la configuration	Généralement indépendant de la taille du réseau	Augmente avec la taille du réseau
Modifications de la topologie	S'adapte automatiquement aux modifications de la topologie	Intervention de l'administrateur requise
Extensibilité	Idéal pour les topologies de réseau simple et complexe	Idéal pour les topologies simples
Sécurité	La sécurité doit être configurée	La sécurité est inhérente
Utilisation des ressources	Utilise le CPU, la mémoire, la bande passante de la liaison	Aucune ressource supplémentaire n'est nécessaire
Prévisibilité du chemin	L'itinéraire dépend de la topologie et du protocole de routage utilisés	Définie explicitement par l'administrateur

Évolution du routage dynamique

Les protocoles de routage dynamique sont utilisés dans les réseaux depuis la fin des années quatre-vingt.



L

	IGP (Protocoles relatifs aux passerelles intérieures)				EGP (Protocoles relatifs aux passerelles extérieures)
	Vecteur de distance		État de liens		Protocole BGP
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	Protocole EIGRP pour IPv6	OSPFv3	IS-IS pour IPv6	BGP-MP

PARTIE 5

Concepts de protocole de routage dynamique

Un protocole de routage est un ensemble de processus, d'algorithmes et de messages qui sont utilisés pour échanger des informations de routage et construire la table de routage en y indiquant les meilleurs chemins. L'objectif des protocoles de routage dynamique est notamment le suivant :

- Découverte des réseaux distants ;
- Actualisation des informations de routage ;
- Choix du meilleur chemin vers des réseaux de destination ;
- Capacité à trouver un nouveau meilleur chemin si le chemin actuel n'est plus disponible.

Les protocoles de routage déterminent le meilleur chemin, ou la meilleure route, vers chaque réseau. Cette route est alors fournie à la table de routage. La route sera installée dans la table de routage s'il n'y a pas d'autre source de routage avec un AD inférieur.

Les protocoles de routage dynamique utilisent généralement leurs propres règles et métriques pour constituer et mettre à jour leur table de routage.

Protocole de routage	Métrique
Protocole RIP (Routing Information Protocol)	•La métrique est le nombre de sauts •Chaque routeur le long d'un chemin ajoute un saut au nombre de sauts. •Un maximum de 15 sauts autorisés.
Protocole OSPF (Open Shortest Path First)	•La métrique est le "coût" qui est basé sur la largeur de bande cumulative de la source à la destination. •Les liaisons plus rapides se voient attribuer des coûts plus faibles que les liaisons plus lentes (coût plus élevé).
Protocole EIGRP (Enhanced Interior Gateway Routing Protocol)	•Il calcule une mesure basée sur la bande passante et les valeurs de retard les plus lentes. •La fiabilité et la charge peuvent également être incluses dans le calcul de la métrique.

CHAPITRE 1

Comprendre le Concepts de routage

1. Concepts de routage
2. Dépanner les routes statiques et par défaut

Routes statiques

Types de routes statiques

Les routes statiques sont généralement implémentées sur un réseau. Cela est vrai même lorsqu'un protocole de routage dynamique est configuré.

Les routes statiques peuvent être configurées pour IPv4 et IPv6. Les deux protocoles prennent en charge les types de routes statiques sont:

- **Route statique standard**
- **Route statique par défaut**
- **Route statique flottante**
- **Route statique récapitulative**

Les routes statiques sont configurées en utilisant les commandes de configuration globale **ip route** et **ipv6 route** global configuration commands.

Options de tronçon suivant

En configurant une route statique, le tronçon suivant peut être identifié par une adresse IP, une interface de sortie, ou les deux. La manière dont la destination est spécifiée crée un des trois types de routes statiques sont :

- **Route de tronçon suivant** - Seule l'adresse IP du tronçon suivant est spécifiée.
- **Route statique connectée directement** - Seule l'interface de sortie du routeur est spécifiée
- **Route statique entièrement spécifiée** - l'adresse IP du tronçon suivant et l'interface de sortie sont spécifiées

Routes statiques

Commande de route statique IPv4

Les routes statiques IPv4 sont configurées à l'aide des commandes suivantes:

```
Router(config)# ip route network-address subnet-mask { ip-address | exit-intf [ip-address]} [distance]
```

Remarque : Les paramètres *ip-address* , *exit-intf* ou *ip-address* et *exit-intf* doivent être configurés.

Commande de route statique IPv6

Les routes statiques IPv6 sont configurées à l'aide des commandes suivantes:

```
Routeur (config) # ipv6 route ipv6-prefix/prefix-length { ipv6-address | exit-intf [ ipv6-address]} [ distance]
```

La plupart des paramètres sont identiques à la version IPv4 de la commande.

Vérifier une route statique

En utilisant **show ip route**, **show ipv6 route**, **ping** et **traceroute**, autres commandes utiles pour vérifier les routes statiques sont les suivantes:

- **show ip route static**
- **show ip route** *network*
- **show running-config | section ip route**

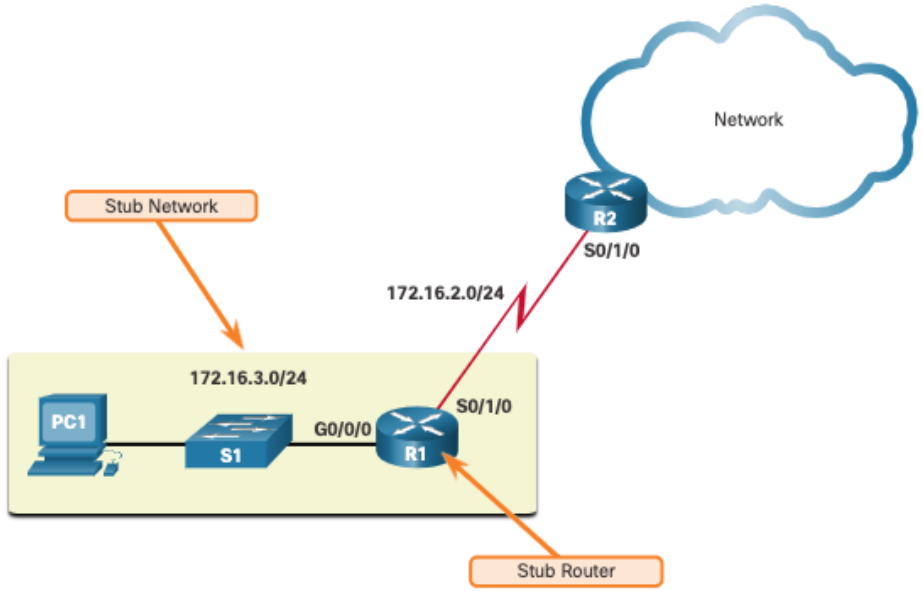
Remplacez **ip** par **ipv6** pour les versions IPv6 de la commande.

PARTIE 5

Configuration de Routes statiques par défaut IP

- **Routes statique par défaut**

- Une route par défaut est une route statique qui correspond à tous les paquets. Une route unique par défaut pour représenter un réseau qui ne figure pas dans la table de routage
- Les routes statiques par défaut sont couramment utilisées lors de la connexion d'un routeur périphérique à un réseau de fournisseur de services, ou d'un routeur d'extrémité. (un routeur avec un seul routeur voisin en amont).



- **Configuration de routes statiques par défaut IPv4 et IPv6**

La syntaxe de commande de base pour une route statique par défaut d'IPv4 est la suivante :

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

La syntaxe de commande de base pour une route statique par défaut d'IPv6 est la suivante :

```
Router(config)# ipv6 route ::/0 {ipv6-address | exit-intf}
```

PARTIE 5

Configuration de Routes statiques IP flottantes

Route statique flottante

- Un autre type de route statique est une route statique flottante. Les routes statiques flottantes sont des routes statiques utilisées pour fournir un chemin de secours à une route statique ou une route dynamique. La route statique flottante est utilisée uniquement lorsque la route principale n'est pas disponible.
- Pour cela, la route statique flottante est configurée avec une distance administrative plus élevée que la route principale. La distance administrative indique la fiabilité d'une route. Si plusieurs chemins vers la destination existent, le routeur choisira le chemin présentant la plus courte distance administrative.
- La distance administrative d'une route statique peut être augmentée pour rendre la route moins souhaitable que celle d'une autre route statique ou d'une route apprise via un protocole de routage dynamique. De cette manière, la route statique «flotte» et n'est pas utilisée lorsque la route dont la distance administrative est meilleure est active.

Configuration de routes statiques flottantes IPv4 et IPv6

Les commandes pour configurer les routes par défaut et flottante IP sont les suivantes:

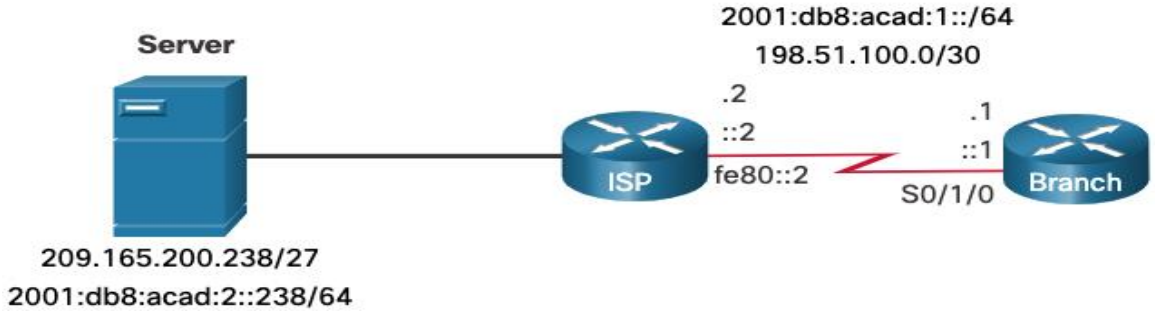
```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address} {distance}

Router(config)# ipv6 route ::/0 {ipv6-address} {distance}
```

Configuration de routes statiques de l'hôte

- **Routes statiques de l'hôte**

Une route d'hôte peut prendre la forme d'une route statique configurée manuellement pour diriger le trafic vers un périphérique de destination spécifique, tel que le serveur présenté dans la figure. La route statique utilise une adresse IP de destination et un masque 255.255.255.255 (/32) pour les routes d'hôte IPv4 et une longueur de préfixe /128 pour les routes IPv6 d'hôte.



- **Configuration de routes statiques de l'hôte**

L'exemple montre la configuration de route statique d'hôte IPv4 et IPv6 sur le routeur Branch pour accéder au serveur.

```
Branch(config)# ip route 209.165.200.238 255.255.255.255 198.51.100.2
Branch(config)# ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2
Branch(config)# exit
Branch#
```

PARTIE 5

Dépannage de la configuration des routes statiques et par défaut IPv4

Les réseaux échouent pour plusieurs raisons:

- Une interface est désactivée
- Un fournisseur de services perd une connexion
- Les liaisons sont sursaturées
- Un administrateur entre une configuration erronée

Pour trouver et résoudre efficacement ces problèmes, il est avantageux d'être intimement familier avec les outils qui permettent d'identifier rapidement les problèmes de routage.

Commande	Description
`ping`	• Vérifie la connectivité de couche 3 au destination. • Les pings étendus fournissent des options supplémentaires.
`traceroute`	• Vérifie le chemin d'accès au réseau de destination. • Il utilise des messages de réponse d'écho ICMP pour déterminer les sauts au destination.
`show ip route`	• Affiche la table de routage. • Permet de vérifier les entrées du route pour les adresses IP de destination.
`show ip interface brief`	• Affiche l'état des interfaces de périphériques. • Permet de vérifier l'état opérationnel et l'adresse IP d'une interface.
`show cdp neighbors`	• Affiche une liste des périphériques Cisco connectés directement. • Également utilisé pour valider la connectivité des couches 1 et 2.

CHAPITRE 2

Implémenter le protocole OSPF

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le fonctionnement et Configurer le protocole OSPF

4 heures

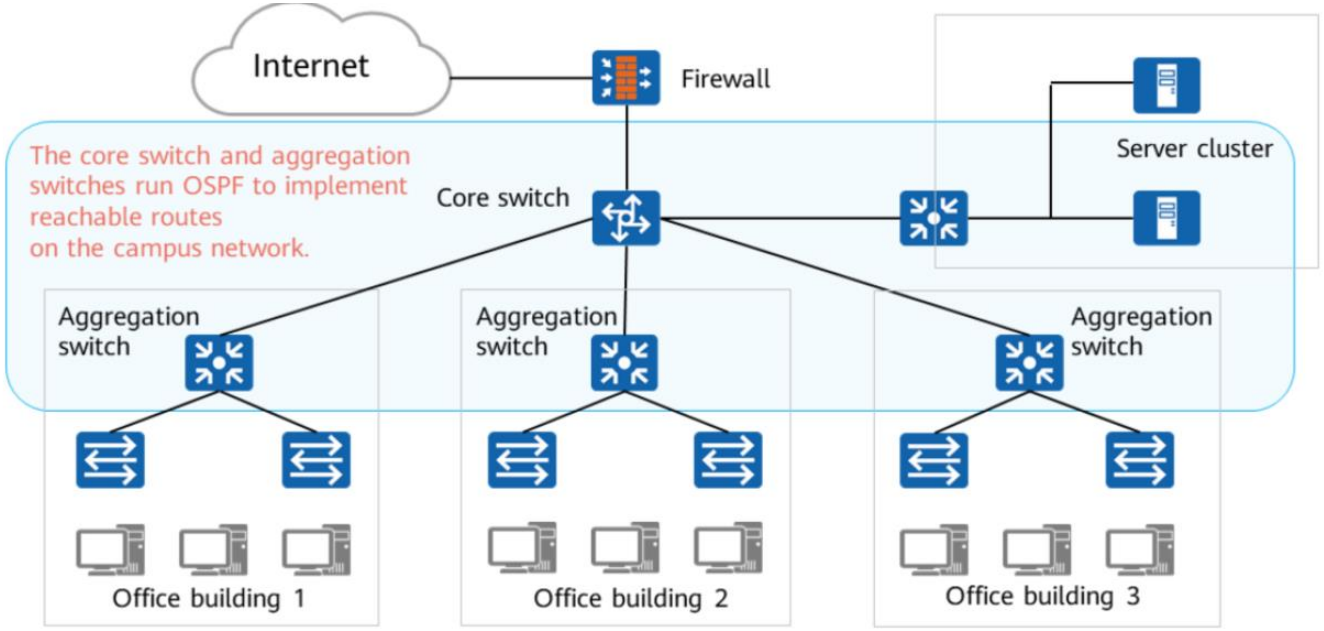
CHAPITRE 2

Implémenter le protocole OSPF

1. Concepts OSPF
2. Configuration OSPFv2 à zone unique
3. Configuration OSPFv3 à zone unique
4. Configuration OSPF à zone multiple

Présentation du protocole OSPF

- OSPF (Open Shortest Path First) est un protocole de routage à état de liens qui a été développé comme alternative au protocole de routage à vecteur de distance, ou RIP.
- Le protocole OSPF présente des avantages considérables par rapport au protocole RIP car il offre une convergence plus rapide et s'adapte mieux aux réseaux de plus grande taille.
- Le protocole OSPF prend en charge le concept de zones pour assurer l'évolutivité.
- Une liaison est une interface sur un routeur, un segment de réseau qui connecte deux routeurs, ou un réseau stub tel qu'un LAN Ethernet connecté à un seul routeur.
- Les informations relatives à l'état de ces liens sont appelées état de liens. Toutes les informations relatives à l'état de liaison incluent le préfixe réseau, la longueur du préfixe et le coût.



Types de paquets OSPF

Le tableau récapitule les cinq types différents de paquets d'état de liens (LSP) utilisés par OSPFv2. OSPFv3 utilise des types de paquets similaires.

Type	Nom du paquet	Description
1	Hello	Découvre les voisins et crée des contiguïtés entre eux
2	DBD (Database Description)	Vérifie la synchronisation de la base de données entre les routeurs
3	LSR (Link-State Request)	Demande des enregistrements d'état de liens spécifiques d'un routeur à un autre
4	LSU (Link-State Update)	Envoie les enregistrements d'état de liens spécifiquement demandés
5	LSAck (Link-State Acknowledgment)	Reconnaît les autres types de paquet

Ces paquets servent à détecter les routeurs voisins et à échanger des informations de routage pour garantir l'exactitude des informations relatives au réseau.

Bases de données OSPF

Les messages OSPF sont utilisés pour créer et gérer trois bases de données OSPF, comme suit:

Base de données	Tableau	Description
Base de données de contiguïté	Table de voisinage	•Répertorie tous les routeurs voisins avec lesquels un routeur a établi une communication bidirectionnelle. •Cette table est unique pour chaque routeur •Accessible via la commande **`show ip ospf neighbor`** .
Base de données d'états de liens (LSDB)	Table topologique	•Liste des informations relatives à tous les autres routeurs du réseau •La base de données représente le réseau LSDB. •Tous les routeurs au sein d'une zone possèdent des LSDB identiques •Accessible via la commande **`show ip ospf database`** .
Base de données de réacheminement	Table de routage	•Liste de routes générée lors de l'exécution d'un algorithme sur la base de données d'états de liens. •La table de routage de chaque routeur est unique et contient des informations sur les modalités (la façon et l'endroit) d'envoi des paquets aux autres routeurs •Accessible via la commande **`show ip route`** .

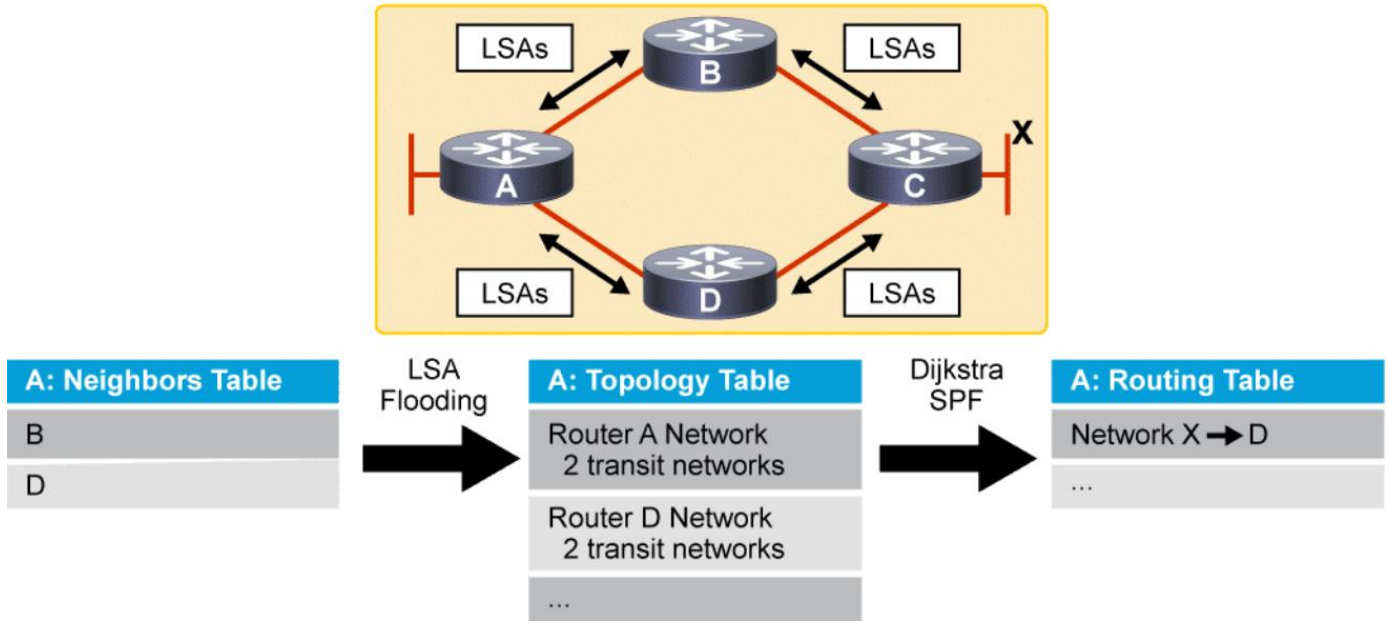
Le routeur crée la table topologique à l'aide des résultats des calculs basés sur l'algorithme SPF de Dijkstra. L'algorithme SPF est basé sur le coût cumulé permettant d'atteindre une destination.

PARTIE 5

Fonctionnement de l'état de liens

Pour mettre à jour les informations de routage, les routeurs OSPF effectuent le processus de routage à état de liens générique qui suit afin d'atteindre un état de convergence: Voici les étapes de routage d'état de lien qui sont effectuées par un routeur:

1. Établissement des contiguïtés de voisinage
2. Échange d'annonces à état de liens
3. Créer la base de données de l'état des liens
4. Exécution de l'algorithme SPF
5. Choisissez la meilleure route

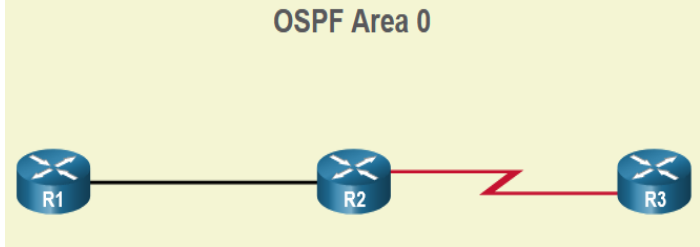


OSPF à zone unique et multiple

Pour une efficacité et une évolutivité supérieures, le protocole OSPF prend en charge le routage hiérarchique à l'aide de zones. Une zone OSPF est un groupe de routeurs qui partagent les mêmes informations d'état de liens dans leurs LSDB. Le protocole OSPF peut être implémenté de deux manières différentes:

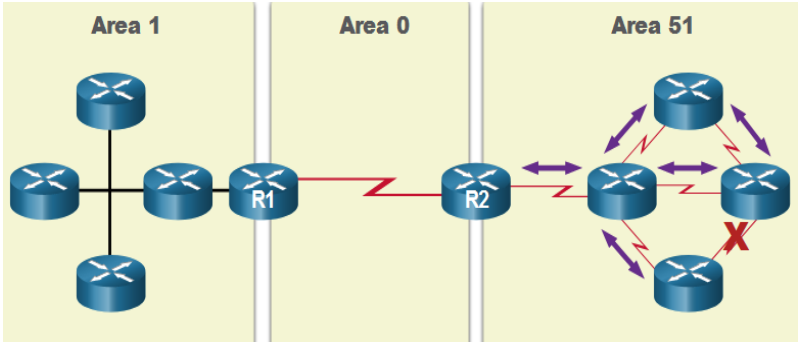
○ OSPF à zone unique

Tous les routeurs sont dans une zone. La meilleure pratique consiste à utiliser la zone 0.



○ OSPF à zone multiple

- le protocole OSPF est mis en œuvre à l'aide de plusieurs zones, de façon hiérarchique. Toutes les zones doivent se connecter à la zone de réseau fédérateur (zone 0). Les routeurs qui relient les zones entre elles sont des routeurs ABR (Area Border Router).
- Les options de conception d'une topologie hiérarchique avec le protocole OSPF à zones multiples présentent les avantages suivants:
  - **Tables de routage plus petites**
  - **Réduction de la charge de mise à jour des états de liens**
  - **Réduction de la fréquence des calculs SPF**



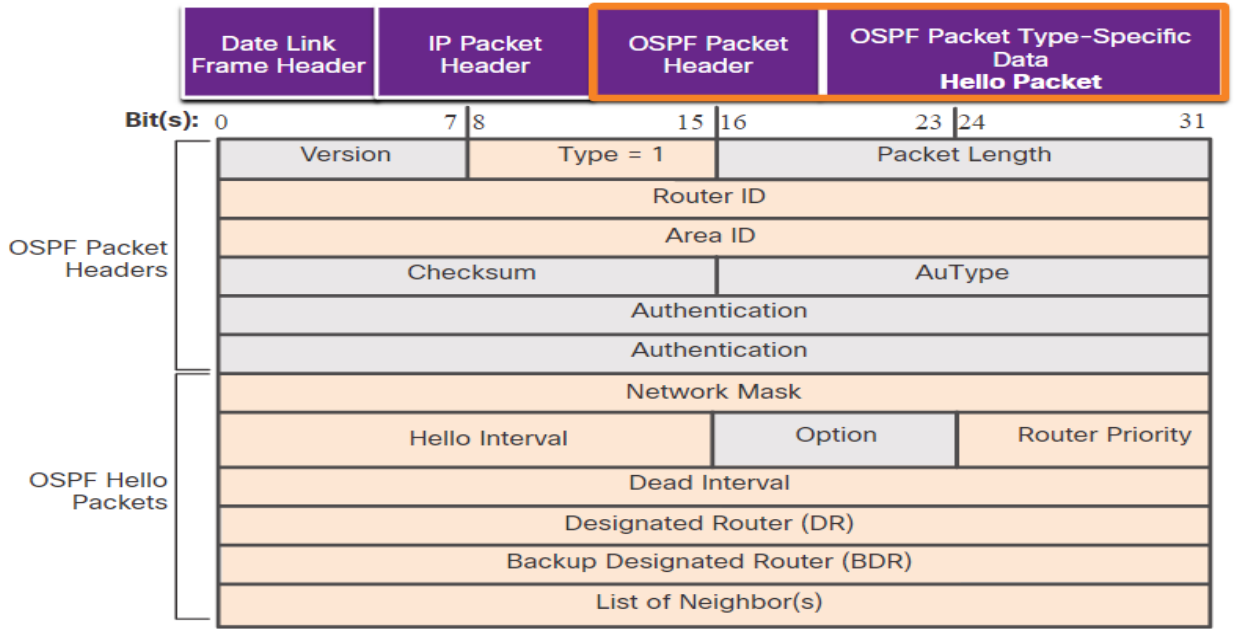
Remarque : Ce module se concentre sur l'OSPF à zone unique.

PARTIE 5

Paquet Hello

Le paquet de type 1 du protocole OSPF correspond au paquet Hello. Les paquets Hello sont utilisés pour effectuer les opérations suivantes:

- Découvrir des voisins OSPF et établir des contiguïtés.
- Annoncer les paramètres sur lesquels les deux routeurs doivent s'accorder pour devenir voisins.
- Choisir le routeur désigné (DR) et le routeur désigné de secours (BDR) sur les réseaux à accès multiple, de type Ethernet. Les liens point-à-point ne nécessitent pas de routeur DR ou BDR.



Mise à jour d'état de liens

- Les paquets LSU sont également utilisés pour transmettre des mises à jour de routage OSPF. Un paquet LSU peut contenir 11 types différents de paquets LSA OSPFv2 OSPFv3 a renommé plusieurs de ces paquets LSA et comporte également deux paquets LSA supplémentaires.
- Les paquets LSU et LSA sont souvent utilisés de manière interchangeable, mais la hiérarchie correcte est que les paquets LSU contiennent des messages LSA.

LSUs

Type	Packet Name	Description
1	Hello	Discovers neighbors and builds adjacencies between them
2	DBD	Checks for database synchronization between routers
3	LSR	Requests specific link-state records from router to router
4	LSU	Sends specifically requested link-state records
5	LSAck	Acknowledges the other packet types

LSAs

LSA Type	Description
1	Router LSAs
2	Checks for database synchronization between routers
3 or 4	Summary LSAs
5	Autonomous System External LSAs
6	Multicast OSPF LSAs
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Patrol (BGPs)

États opérationnels OSPF

État	Description
État Down	• Aucun paquet Hello reçu = Down. • Le routeur envoie des paquets Hello. • Transition vers l'état Init.
État Init	• Les paquets Hello sont reçus du voisin. • Ils contiennent des ID de routeur du routeur expéditeur. • Transition vers l'état Two-Way.
État Two-Way	• Dans cet état, la communication entre les deux routeurs est bidirectionnelle. • Sur les liens à accès multiple, les routeurs choisissent un DR et un BDR. • Transition vers l'état ExStart.
État ExStart	• Sur les réseaux point à point, les deux routeurs décident quel routeur initiera l'échange de paquets DBD et décident du numéro de séquence de paquets DBD initial.
État Exchange	• Les routeurs échangent des paquets DBD. • Si d'autres informations de routeur sont nécessaires, passez à l'état Loading. Sinon, passez à l'état Full.
État Loading	• Les paquets LSR et LSU permettent d'obtenir des informations supplémentaires sur les routes. • Les routes sont traitées à l'aide de l'algorithme SPF. • Transition vers l'état Full.
État Full	• La base de données d'état de liaison du routeur est entièrement synchronisée.

Établissement des contiguïtés de voisin

Pour déterminer s'il y a un voisin OSPF sur le lien, le routeur envoie un paquet Hello contenant son ID de routeur sur toutes les interfaces compatibles OSPF. Le paquet Hello est envoyé à l'adresse de multidiffusion réservée. Tous les routeurs OSPF IPv4 224.0.0.5. Seuls les routeurs OSPFv2 traitent ces paquets.

1	État Down vers état Init	Lorsque OSPFv2 est activé sur l'interface, R1 passe de Down à Init et commence à envoyer des paquets Hello OSPFv2 hors de l'interface pour tenter de découvrir des voisins.
2	État Init	Lorsqu'un R2 reçoit un paquet Hello du routeur R1 précédemment inconnu, il ajoute l'ID du routeur de R1 à la liste des voisins et répond avec un paquet Hello contenant son propre ID de routeur.
3	État Two-Way	R1 reçoit le paquet Hello de R2 et remarque que le message contient l'ID du routeur R1 dans la liste des voisins de R2. R1 ajoute l'ID de routeur de R2 à la liste des voisins et effectue des transitions vers l'état bidirectionnel. Si R1 et R2 sont connectés à une liaison point à point, ils passent à l'état ExStart Si R1 et R2 sont connectés sur un réseau Ethernet commun, l'option DR/BDR se produit.
4	Choisir le routeur désigné (DR) et le routeur désigné de secours (BDR)	L'option DR et BDR se produit, où le routeur ayant l'ID de routeur le plus élevé ou la priorité la plus élevée est élu comme DR, et le deuxième plus élevé est le BDR

Synchronisation des bases de données OSPF

Après l'état de communication bidirectionnelle (Two-way), les routeurs passent progressivement à des états de synchronisation des bases de données. Il s'agit d'un processus en trois étapes, comme suit:

- Décider du premier routeur: Le routeur avec l'ID de routeur le plus élevé envoie son DBD en premier.
- DBD Exchange: Autant que nécessaire pour transmettre la base de données L'autre routeur doit reconnaître chaque DBD avec un paquet LSack.
- Envoyer un LSR: Chaque routeur compare les informations DBD avec le LSDB local. Si le DBD contient des informations de liaison plus récentes, le routeur passe à l'état de Loading.

Une fois que tous les LSR ont été échangés et satisfaits, les routeurs sont considérés comme synchronisés et dans un état Full. Les mises à jour (LSU) sont envoyées:

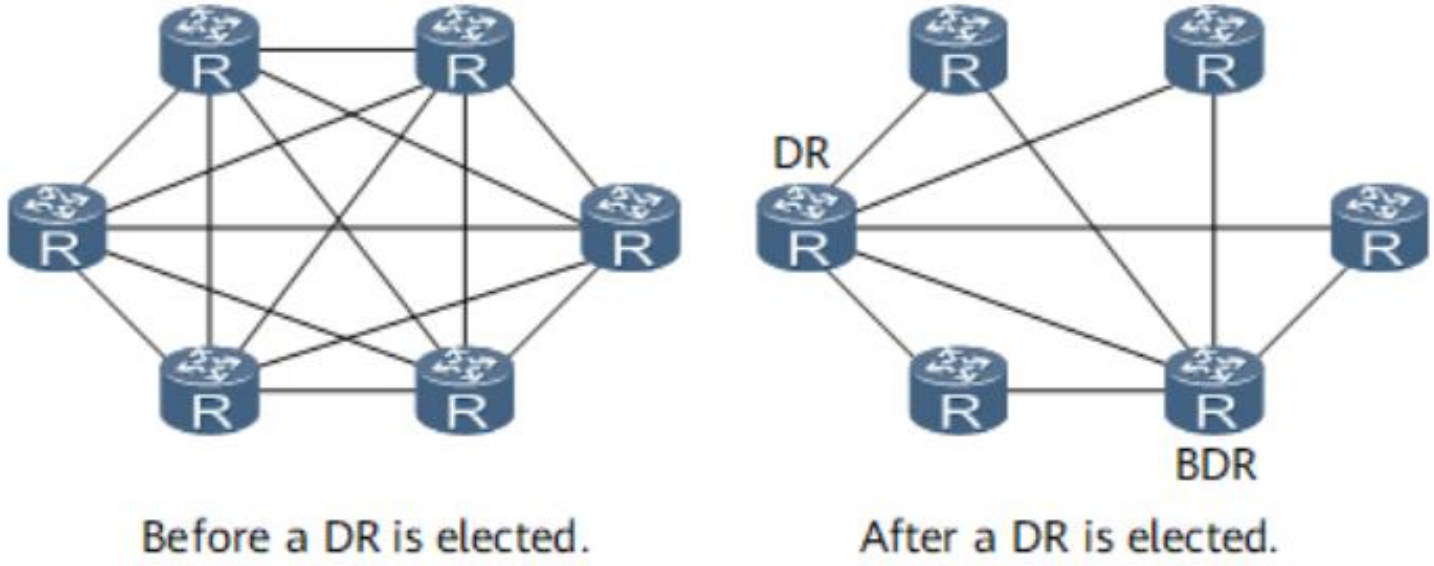
- En cas de détection d'une modification (mises à jour incrémentielles)
- Toutes les 30 minutes

La nécessité d'un DR

Les réseaux à accès multiple peuvent présenter deux problématiques pour le protocole OSPF concernant l'inondation des LSA, comme suivant:

- **Création de plusieurs contiguïtés**
- **Diffusion massive de paquets LSA**

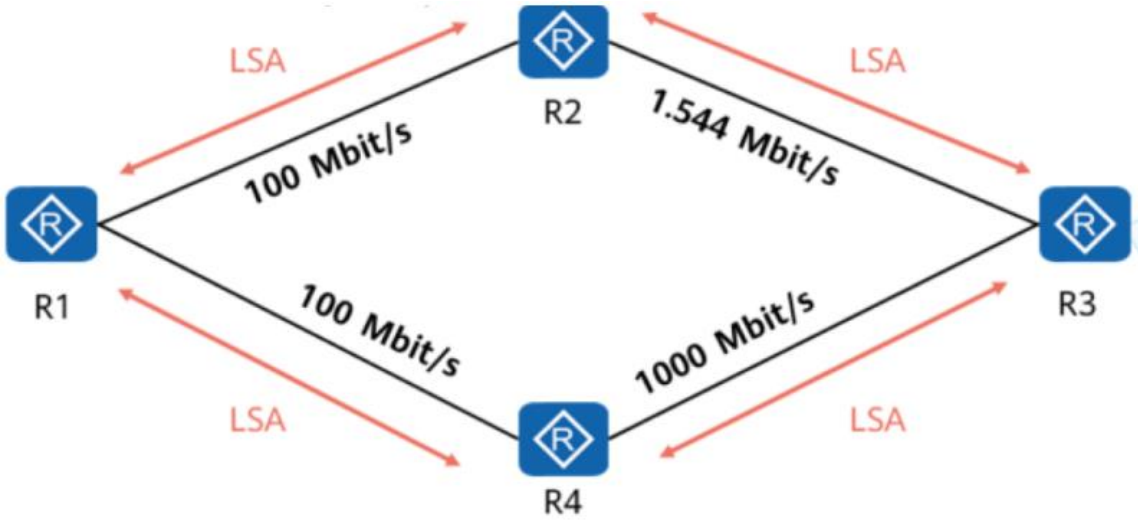
- Sur les réseaux à accès multiple, le protocole OSPF choisit un DR, qui sera le point de collecte et de distribution pour les LSA envoyées et reçues. Un BDR est également sélectionné en cas de panne du routeur DR. Tous les autres routeurs deviennent des DROTHERS. Un DROTHER est un routeur qui n'est ni le routeur DR ni le routeur BDR.



Before a DR is elected. After a DR is elected.

Inondation de la LSA

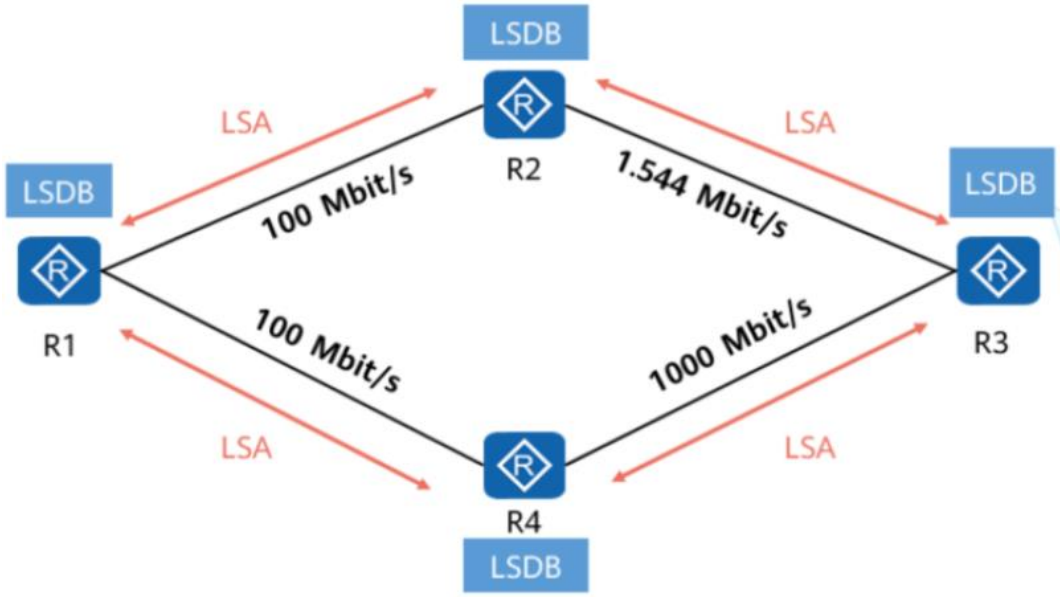
- Les routeurs qui exécutent un protocole d'état de lien établissent une relation de voisinage, puis échangent des annonces d'état de lien (LSA).
- Chaque routeur génère un LSA qui décrit les informations d'état sur son interface directement connectée.
- Le LSA contient le coût de l'interface et la relation entre le routeur et ses routeurs voisins.



- LSAs, instead of routes, are advertised.
- An LSA describes a router interface's status information, such as the cost of the interface and a connected interface name.

Création de LSDB

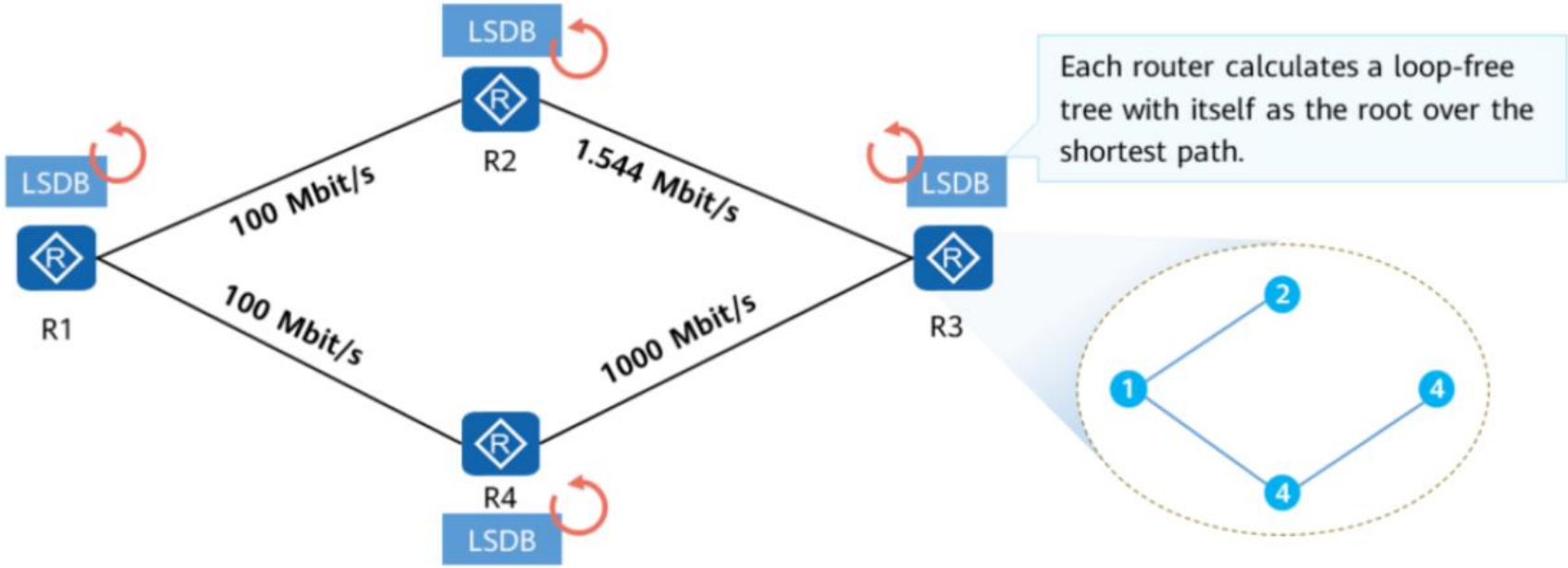
- Chaque routeur génère des LSA et ajoute les LSA reçus à sa propre base de données d'état des liens (LSDB).
- Les routeurs apprennent toute la topologie du réseau via le LSDB.



- The router stores LSAs in the LSDB.
- The LSDB contains the description of all router interfaces on the network.
- The LSDB contains the description of the entire network topology.

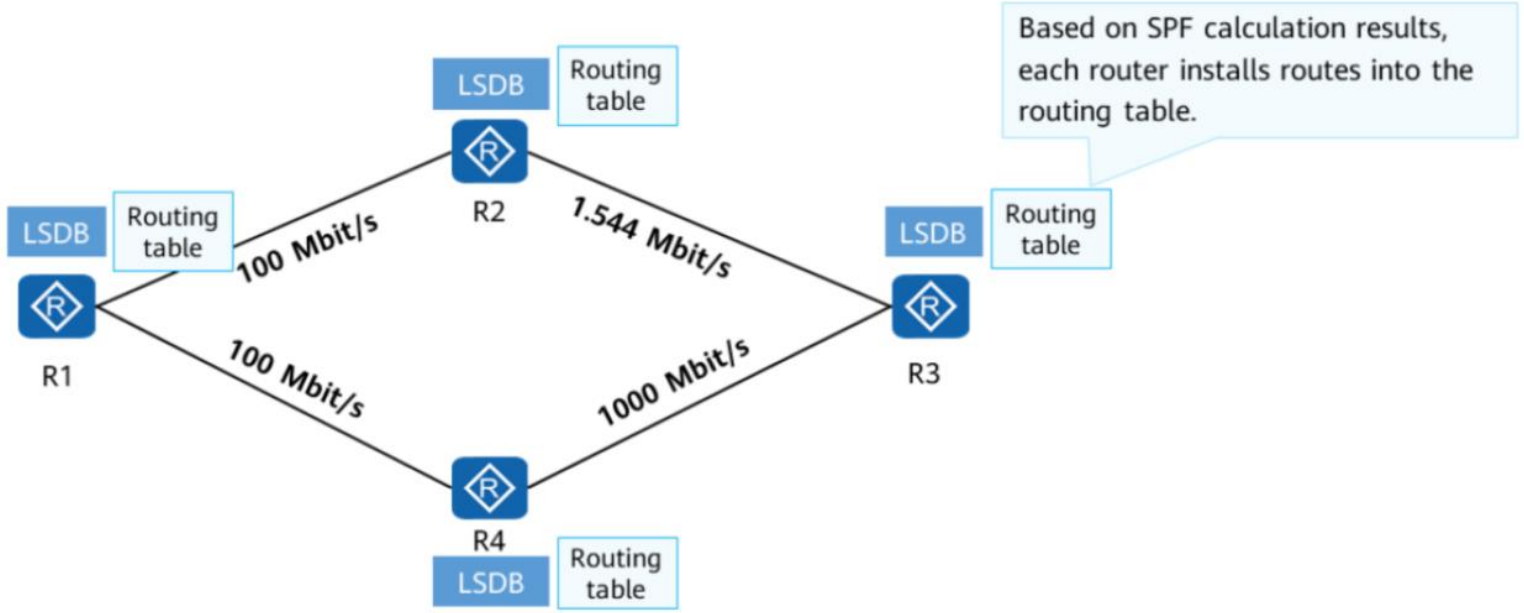
Calcul du FPS

- Chaque routeur utilise l'algorithme Shortest Path First (SPF) et les informations LSDB pour calculer les routes.
- Chaque routeur calcule un arbre sans boucle avec lui-même comme racine et chemin le plus court.
- Avec cet arbre, un routeur détermine le chemin optimal vers chaque coin d'un réseau.



Génération de table de routage

- Le routeur installe des routes pour les chemins préférés calculés dans sa table de routage.



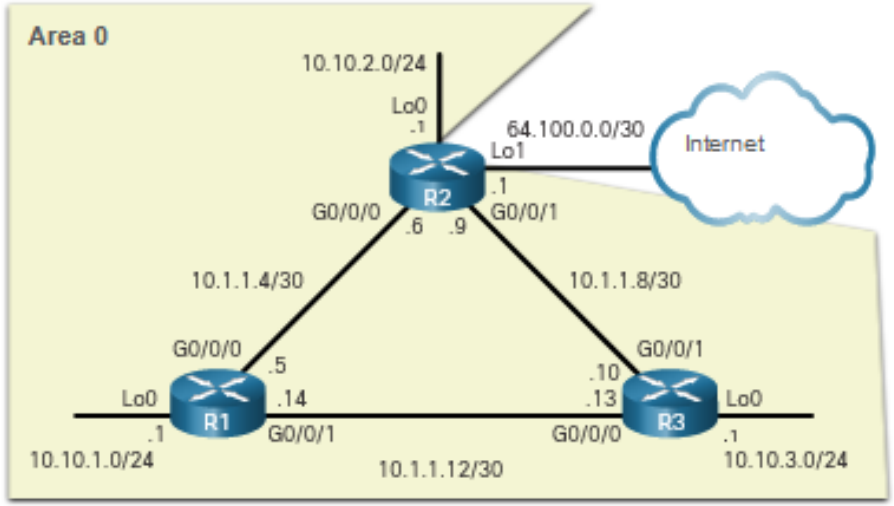
CHAPITRE 2

Implémenter le protocole OSPF

1. Concepts OSPF
2. Configuration OSPFv2 à zone unique
3. Configuration OSPFv3 à zone unique
4. Configuration OSPF à zone multiple

Mode de configuration du routeur pour OSPF

- **Topologie de référence OSPF**



- **Mode de configuration du routeur pour OSPF**

Vous pouvez activer OSPFv2 à l'aide de la commande **router ospf** *process-id* en mode de configuration globale.

- La valeur *process-id* représente un nombre compris entre 1 et 65535 et est sélectionnée par l'administrateur du réseau.
- La valeur *process-id* est localement significative. Il est recommandé d'utiliser le même *process-id* sur tous les routeurs OSPF.

```
R1(config)# router ospf 10
```

PARTIE 5

PARTIE 5

ID de routeur OSPF

- **ID de routeur**

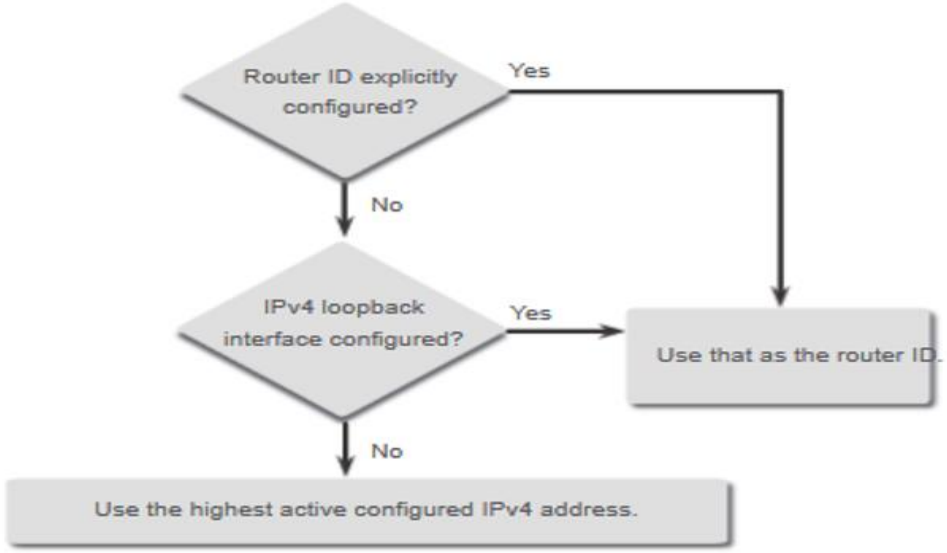
Un ID de routeur OSPF est une valeur 32 bits, représentée par une adresse IPv4. Il est utilisé pour identifier de manière unique un routeur OSPF, et tous les paquets OSPF incluent l'ID du routeur d'origine.

L'ID du routeur est utilisé par un routeur compatible OSPF pour faire ce qui suit :

- **Participer à la synchronisation des bases de données OSPF**
- **Participer à l'élection du routeur désigné (DR)**

L'ID du routeur est explicitement configuré à l'aide de la commande de mode de configuration **router-id** *rid* du routeur OSPF.

- **Ordre de priorité de l'ID de routeur**



Configuration d'ID de routeur OSPF

- **Configurer une interface de bouclage comme ID de routeur**

```
R1(config-if)# interface Loopback 1
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

- **Configurer explicitement un ID de routeur**

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

- **Modifier un ID de Routeur**

```
R1# show ip protocols | include Router ID
  Router ID 10.10.1.1
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
R1# clear ip ospf process
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux point à point

La syntaxe de commande network et ip ospf

Vous pouvez spécifier les interfaces appartenant à un réseau point à point en configurant la commande **network** .

- La syntaxe de base de la commande **network** est la suivante:

```
Router(config-router)# network network-address wildcard-mask area area-id
```

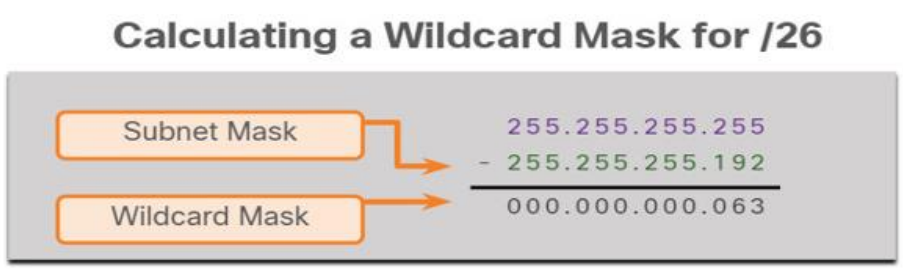
Pour configurer OSPF directement sur l'interface, utilisez la commande de mode de configuration **ip ospf** de l'interface

- La syntaxe de base de la commande **ip ospf** est la suivante:

```
Router(config-if)# ip ospf process-id area area-id
```

Le masque générique

- Le masque générique est généralement l'inverse du masque de sous-réseau configuré sur cette interface.



PARTIE 5

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux point à point

- **Configurer OSPF à l'aide de la commande network**

```
R1(config)# router ospf 10
R1 (config-router) # network 10.10.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.4 0.0.0.3 area 0
R1 (config-router) # network 10.1.1.12 0.0.0.3 area 0
R1(config-router)#
```

- **Configurer OSPF à l'aide de la commande ip ospf**

```
R1(config)# interface GigabitEthernet 0/0/0
R1 (config-if) # ip ospf 10 area 0
R1(config)# interface GigabitEthernet 0/0/1
R1 (config-if) # ip ospf 10 area 0
R1(config)# interface Loopback 0
R1 (config-if) # ip ospf 10 area 0
R1 (config-if) #
```

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux point à point

- **Interface passive**

Par défaut, les messages OSPF sont acheminés à partir de toutes les interfaces compatibles OSPF. Cependant, ces messages ne doivent être envoyés que par des interfaces qui se connectent à d'autres routeurs compatibles OSPF.

L'envoi de messages inutiles sur un réseau local affecte le réseau de trois façons :

- **Utilisation inefficace de la bande passante**
- **Utilisation inefficace des ressources**
- **Risque de sécurité accru**

Utilisez la commande du mode de configuration du routeur **passive-interface** pour empêcher la transmission de messages de routage via une interface de routeur, mais permettre que le réseau soit annoncé aux autres routeurs.

- **Configurer les interfaces passives**

```
R1(config)# router ospf 10
R1 (config-router) # passive-interface Loopback 0
R1 (config-router) # end
R1#
```

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux point à point

- **Réseaux point à point OSPF**

Par défaut, les routeurs Cisco choisissent une DR et une BDR sur les interfaces Ethernet, même s'il n'y a qu'un autre périphérique sur la liaison. Vous pouvez vérifier cela avec la commande **show ip ospf interface**.

Pour passer à un réseau point à point, utilisez la commande de configuration de l'interface **ip ospf network point-to-point** sur toutes les interfaces sur lesquelles vous souhaitez désactiver le processus d'élection DR/BDR.

- **Configurer le réseau point à point sur l'interface**

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf network point-to-point
R1(config-if)# end
R1# show ip ospf interface GigabitEthernet 0/0/0
.........
Process ID 10, Router ID 1.1.1.1, Network Type
POINT_TO_POINT, Cost: 1
  .......
```

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux point à point

Configurer le réseau point à point sur l'interface Loopback

Pour simuler un vrai réseau local, l'interface de bouclage peut être configurée comme un réseau point à point pour annoncer le réseau complet.

- Ce que R2 voit lorsque R1 annonce l'interface de bouclage tel quel:

```
R2# show ip route | include 10.10.1
O 10.10.1.1/32 [110/2] via 10.1.1.5, 00:03:05,
GigabiteThernet0/0/0
```

La configuration est modifiée à R1 :

```
R1(config-if)# interface Loopback 0
R1(config-if)# ip ospf network point-to-point
```

Résultat à R2:

```
R2# show ip route | include 10.10.1
O 10.10.1.0/24 [110/2] via 10.1.1.5, 00:03:05,
GigabiteThernet0/0/0
```

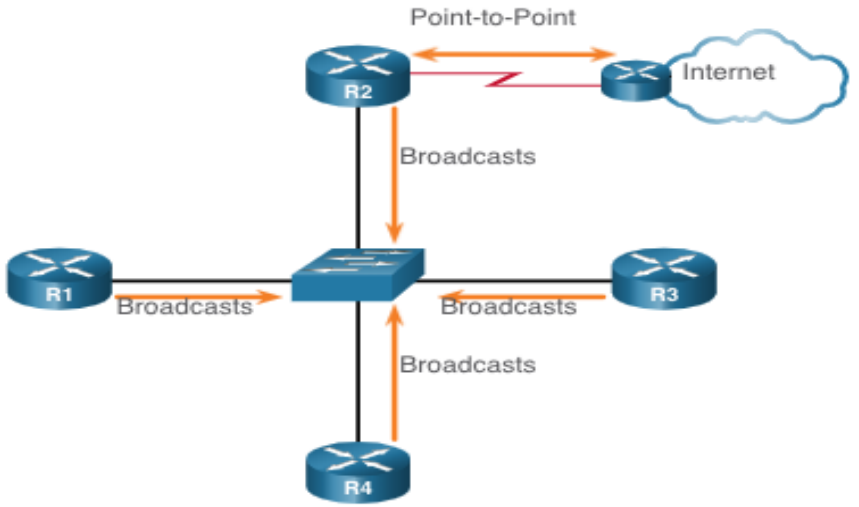
PARTIE 5

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux multi-accès

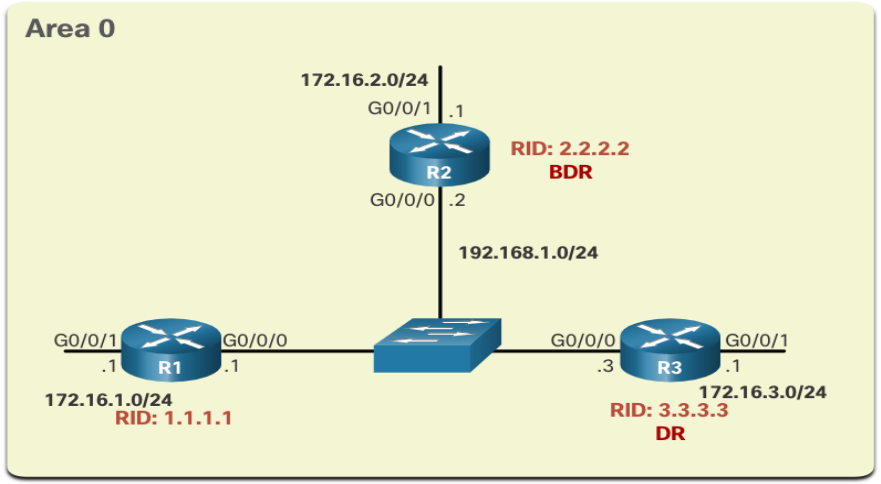
- **Le réseau OSPF multi-accès**

Les réseaux OSPF à accès multiple sont uniques en ce sens qu'un seul routeur contrôle la distribution des LSAs.

- Le routeur qui est élu pour ce rôle est un Routeur désigné OSPF (DR).



- **Topologie de référence OSPF à accès multiple**



Remarque :
Le DR utilise l'adresse IPv4 multicast 224.0.0.5
Les BDR utilisent l'adresse à accès multiple 224.0.0.6

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux multiaccès

- **Vérifier les contiguïtés DR/BDR**

Pour vérifier les contiguïtés OSPFv2, utilisez la commande **show ip ospf neighbor** . L'état des voisins dans les réseaux multi-accès peut être le suivant :

- **FULL/DROTHER**- Il s'agit d'un routeur DR ou BDR qui est entièrement contigu avec un routeur non DR ou BDR. Ces deux voisins peuvent échanger des paquets Hello, des mises à jour, des demandes, des réponses et des accusés de réception.
- **FULL/DR** - le routeur est entièrement contigu avec le DR voisin indiqué. Ces deux voisins peuvent échanger des paquets Hello, des mises à jour, des demandes, des réponses et des accusés de réception.
- **FULL/BDR** - Le routeur est entièrement contigu avec le BDR voisin indiqué. Ces deux voisins peuvent échanger des paquets Hello, des mises à jour, des demandes, des réponses et des accusés de réception.
- **2-WAY/DROTHER** - Le routeur non-DR ou BDR a une relation de voisin avec un autre routeur non-DR ou BDR. Ces deux voisins échangent des paquets Hello.

L'état normal d'un routeur OSPF est généralement FULL. Si un routeur reste bloqué dans un autre état, cela indique des problèmes dans l'établissement des contiguïtés. La seule exception est l'état 2-WAY, qui est normal sur un réseau de diffusion à accès multiple.

```
R2# show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
1.1.1.1 1 FULL/BROTHER 00:00:31 192.168.1.1 GigabiteThernet0/0/0
3.3.3.3 1 FULL/DR  00:00:34 192.168.1.3 GigabitEthernet0/0/0 R2#
```

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux multiaccès

Processus d'élection DR/BDR par défaut

La sélection du DR et du BDR OSPF est basée sur les critères suivants, dans l'ordre indiqué:

1. Les routeurs du réseau choisissent le routeur ayant la priorité d'interface la plus élevée comme étant le DR. Le routeur ayant la deuxième priorité d'interface la plus élevée est choisi comme BDR.
   - La priorité peut être tout nombre compris entre 0 et 255.
   - Si la valeur de priorité de l'interface est définie sur 0, cette interface ne peut pas être sélectionnée comme DR ou BDR.
   - La priorité par défaut des interfaces de diffusion à accès multiple est de 1.
2. Si les priorités d'interface sont égales, c'est le routeur dont l'ID est le plus élevé qui est choisi comme DR. Le routeur ayant le deuxième ID le plus élevé est choisi comme BDR.

- Le processus de sélection a lieu dès que le premier routeur avec une interface OSPF devient actif sur le réseau actif. Si certains routeurs du réseau n'ont pas fini de démarrer, il est possible qu'un routeur avec un ID de routeur plus bas devienne le DR.
- L'ajout d'un nouveau routeur ne déclenche pas un nouveau choix.

Défaillance et récupération du DR

En cas de panne du DR :

- Le BDR devient automatiquement le DR, même si un DROTHER de priorité ou d'ID de routeur plus élevés a été ajouté au réseau après la sélection initiale du DR et du BDR.
- Une fois qu'un BDR est promu en DR, une nouvelle élection de BDR a lieu et le DROTHER ayant la plus haute priorité ou l'ID de routeur est élu comme nouveau BDR.

Mettre en œuvre le protocole OSPFv2 à zone unique sur des réseaux multiaccès

La commande ip ospf priority

- Si les priorités des interfaces sont identiques sur tous les routeurs, le routeur dont l'ID est le plus élevé est sélectionné comme DR.
- Au lieu de se baser sur l'ID de routeur, il vaut mieux contrôler la sélection au moyen des priorités d'interfaces. Cela permet également à un routeur d'être DR dans un réseau et DROTHER dans un autre.
- Pour définir la priorité d'une interface, utilisez la commande **ip ospf priority** *value* , où la valeur est 0 à 255.
  - Une valeur de 0 ne devient pas une DR ou une BDR.
  - Une valeur de 1 à 255 sur l'interface rend plus probable que le routeur devienne le DR ou le BDR.

Configurer la priorité OSPF

L'exemple montre les commandes utilisées pour modifier la priorité de l'interface R1 G0/0/0 de 1 à 255, puis réinitialiser le processus OSPF.

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
R1#  clear ip ospf process
Reset ALL OSPF processes? [no]: y
R1# *Jun 5 03:47:41.563: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on
GigabitEthernet0/0/0 from FULL to DOWN, Neighbor Down: Interface down or detached
```

PARTIE 5

Mesure de coût Cisco OSPF

- Les protocoles de routage utilise une métrique pour déterminer le meilleur chemin d'un paquet sur un réseau. Le protocole OSPF utilise le coût comme métrique. Un coût plus faible indique un meilleur chemin.
- Le coût d'une interface Cisco est inversement proportionnel à la largeur de bande de l'interface. Par conséquent, une bande passante plus élevée indique un coût plus faible. La formule utilisée pour calculer le coût OSPF est la suivante:

Coût=bande passante de référence/ bande passante de l'interface

- La bande passante de référence par défaut correspond à 10^8 (100,000,000); par conséquent, la formule est la suivante:

Coût = 100,000,000 bps/bande passante de l'interface en bps

- Comme la valeur du coût OSPF doit être un nombre entier, les interfaces FastEthernet, Gigabit Ethernet et 10 GigE partagent le même coût. Pour corriger cette situation, vous pouvez:
  - Réglez la bande passante de référence avec la commande **auto-cost reference-bandwidth** sur chaque routeur OSPF.
  - Définissez manuellement la valeur de coût OSPF avec la commande **ip ospf cost** sur les interfaces nécessaires.

Réglage de la bande passante de référence

- La valeur de coût doit être un entier. Si un élément inférieur à un entier est calculé, OSPF arrondit à l'entier le plus proche. Par conséquent, le coût OSPF affecté à une interface Gigabit Ethernet avec la bande passante de référence par défaut de 100,000,000 bit/s serait égal à 1, car l'entier le plus proche pour 0,1 est 0 au lieu de 1.

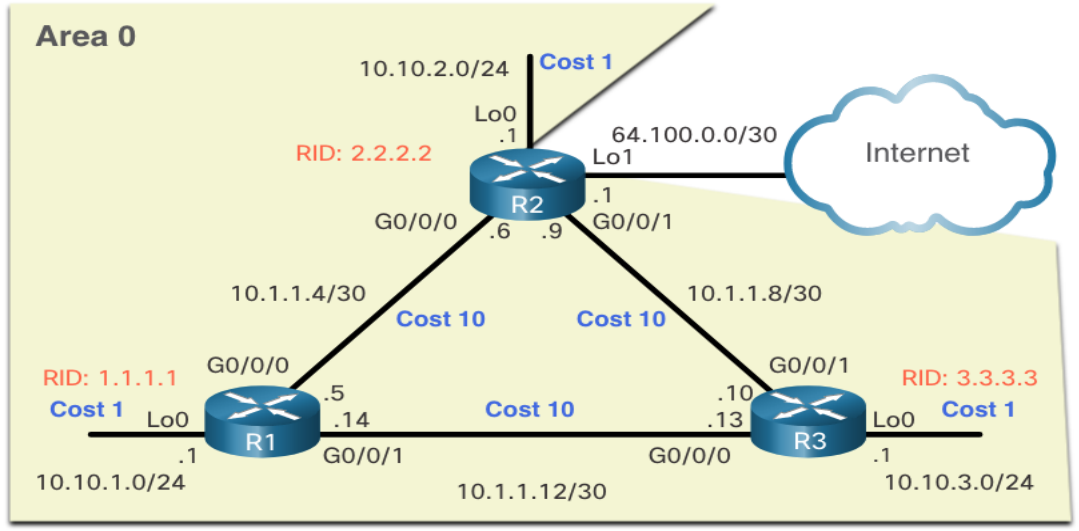
Coût = 100000000 bps /1000000000 = 1

- Pour cette raison, toutes les interfaces plus rapides que Fast Ethernet auront la même valeur de coût de 1 qu'une interface Fast Ethernet.
- Pour aider le protocole OSPF à déterminer le chemin exact, la bande passante de référence doit être remplacée par une valeur supérieure pour prendre en compte les réseaux disposant de liens plus rapides que 100 Mbit/s.
- Pour ajuster la bande passante de référence, utilisez la command **auto-cost reference-bandwidth** *Mbps* en mode de configuration de routeur.
  - Cette commande doit être configurée sur chaque routeur du domaine OSPF.
  - Notez dans la commande que la valeur est exprimée en Mbps; par conséquent, pour ajuster les coûts pour Gigabit Ethernet, utilisez la commande **auto-cost reference-bandwidth 1000.** Pour 10 Gigabit Ethernet, utilisez la commande **auto-cost reference-bandwidth 10000.**
  - Pour revenir à la bande passante de référence par défaut, utilisez la commande **auto-cost reference-bandwidth 100** .
- Une autre option consiste à modifier le coût sur une interface spécifique à l'aide de la commande **ip ospf cost** *cost* .
- Utilisez la commande **show ip ospf interface** pour vérifier le coût OSPFv2 assigné à l'interface 0/0/0 de R1.

PARTIE 5

OSPF accumule le coût

- Le coût d'une route OSPF est la valeur cumulée depuis un routeur jusqu'au réseau de destination.
- En supposant que la commande **auto-cost reference-bandwidth 10000** ait été configurée sur les trois routeurs, le coût des liaisons entre chaque routeur est maintenant de 10. Les interfaces de bouclage ont un coût par défaut de 1.
- Vous pouvez calculer le coût pour chaque routeur pour atteindre chaque réseau.
- Par exemple, le coût total pour R1 pour atteindre le réseau 10.10.2.0/24 est de 11. En effet, le lien vers le coût R2 = 10 et le coût par défaut de bouclage = 1. 10 + 1 = 11.
- Vous pouvez vérifier cela à l'aide de la commande **show ip route** .



Définir manuellement la valeur de coût OSPF

Les raisons de définir manuellement la valeur de coût sont les suivantes:

- L'administrateur peut vouloir influencer la sélection des chemins au sein d'OSPF, ce qui entraîne la sélection de chemins différents de ceux normalement attribués aux coûts par défaut et à l'accumulation des coûts.
- Connexions à l'équipement d'autres fournisseurs qui utilisent une formule différente pour calculer le coût OSPF.

Pour modifier la valeur de coût déclarée par le routeur OSPF local à d'autres routeurs OSPF, utilisez la commande de configuration de l'interface **ip ospf cost** *value* .

- **Configuration**

```
R1(config)# interface g0/0/1
R1(config-if)# ip ospf cost 30
R1(config-if)# interface lo0
R1(config-if)# ip ospf cost 10
R1(config-if)# end
R1#
```

Modifier les intervalles Hello/Dead OSPFv2

- Les paquets OSPFv2 Hello sont transmis à l'adresse de multidiffusion 224.0.0.5 (tous les routeurs OSPF) toutes les 10 secondes. Il s'agit de la valeur du minuteur par défaut sur les réseaux à accès multiple et point à point.

  Remarque: Les paquets Hello ne sont pas envoyés sur les interfaces définies sur passive par la commande **passive-interface** .

- L'intervalle Dead est la période pendant laquelle le routeur attend de recevoir un paquet Hello avant de déclarer le voisin en panne. Ce délai est de 40 secondes sur les réseaux multi-accès et point à point.
- Il peut être souhaitable de modifier les minuteurs OSPF afin que les routeurs détectent plus rapidement les défaillances du réseau. Cela augmente le trafic, mais le besoin d'une convergence rapide est parfois plus important que les inconvénients du trafic supplémentaire produit.
- Les intervalles Hello et Dead OSPFv2 peuvent être modifiés manuellement au moyen des commandes suivantes de mode de configuration d'interface :\

```
Router(config-if)# ip ospf hello-interval seconds
Router(config-if)# ip ospf dead-interval seconds
```

- utilisez les commandes **no ip ospf hello-interval** et **no ip ospf dead-interval** pour rétablir les valeurs par défaut des intervalles

  - **Configuration**

```
R1 (config) # interface g0/0/1
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)#
```

PARTIE 5

Propager une route statique par défaut dans OSPFv2

Pour propager une route par défaut, le routeur périphérie doit être configuré avec:

- Une route statique par défaut en utilisant la commande **ip route 0.0.0.0 0.0.0.0** [*next-hop-address* | *exit-intf*] .
- La commande de configuration de routeur **default-information originate** . R2 devient donc la source des informations de la route par défaut et la route statique par défaut est propagée dans les mises à jour OSPF.

Configuration

Dans l'exemple, R2 est configuré avec un bouclage pour simuler une connexion à l'internet. Une route par défaut est configurée et propagée à tous les autres routeurs OSPF du domaine de routage.

```
R2 (config) # interface lo1
R2 (config-if) # ip address 64.100.0.1 255.255.255.252
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point
interface, may impact performance
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

PARTIE 5

Vérifier le protocole OSPFv2 à zone unique

- **Vérifiez les paramètres de protocole OSPF**

Avec la commande **show ip protocols :**

```
R1# show ip protocols
*** IP Routing is NSF aware ***
(output omitted)
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routage sur les interfaces configurées explicitement (zone 0):
            Loopback0
            GigabitEthernet0/0/1
            GigabitEthernet0/0/0
  Routing Information Sources:
            Gateway Distance Last Update
            3.3.3.3 110 00:09:30
            2.2.2.2 110 00:09:58
  Distance: (default is 110)
R1#
```

- **Vérifier les informations du processus OSPF**

Avec la commande **show ip ospf :**

```
R1# show ip ospf
Routing Process "ospf 10" with ID 1.1.1.1
Start time: 00:01:47.390, Time elapsed: 00:12:32.320
 (output omitted)
Cisco NSF helper support enabled
Reference bandwidth unit is 10000 mbps
            Area BACKBONE(0)
                        Number of interfaces in this area is 3
                        Area has no authentication
                        SPF algorithm last executed 00:11:31.231 ago
                        Algorithme SPF exécuté 4 fois
                        Area ranges are
                        Number of LSA 3. Checksum Sum 0x00E77E
                        Number of opaque link LSA 0. Checksum Sum
0x000000
                        Nombre de DCbitless LSA 0 Nombre
d'indication LSA 0
                        Number of DoNotAge LSA 0 Flood list length 0
R1#
```

PARTIE 5

Vérifier le protocole OSPFv2 à zone unique

- **Vérifier les paramètres d'interface OSPF**

Avec la commande **show ip ospf interface :**

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via
Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type
POINT_TO_POINT, Cost: 10

<output omitted>

  Neighbor Count is 1, Adjacent neighbor count is 1
            Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R1#
```

Vérifier les interfaces compatibles OSPF

Avec la commande **show ip ospf interface brief**

```
R1# show ip ospf interface brief
Interface PID Area IP Address/Mask Cost State Nbrs F/C
Lo0 10 0 10.10.1.1/24 10 P2P 0/0
Gi0/0/1 10 0 10.1.1.14/30 30 P2P 1/1
Gi0/0/0 10 0 10.1.1.5/30 10 P2P 1/1
R1#
```

- **Vérifier les voisins OSPF**

Avec la commande **show ip ospf neighbor :**

```
R1# show ip ospf neighbor
Neighbor ID Pri State Dead Time  Address Interface
3.3.3.3 0 FULL/ - 00:00:35 10.1.1.13 GigabiteThernet0/0/1
2.2.2.2 0 FULL/ - 00:00:31 10.1.1.6 GigabitEthernet0/0/0
R1#
```

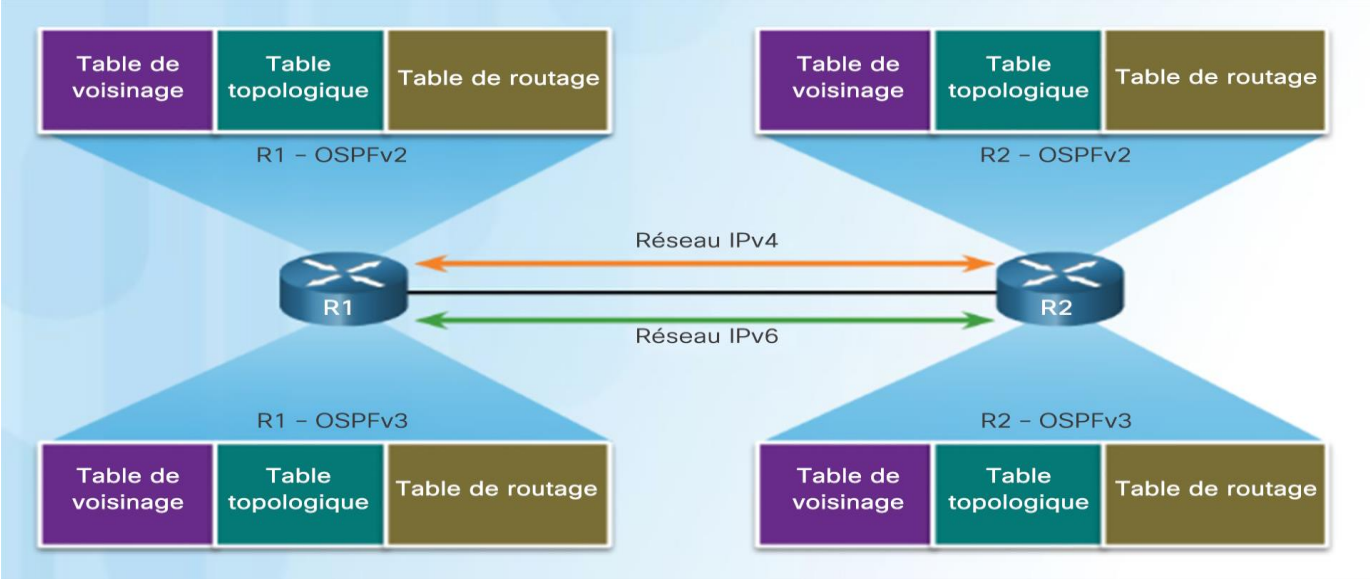
CHAPITRE 2

Implémenter le protocole OSPFv2 à zone unique

1. Configuration OSPFv2 à zone unique
2. Configuration OSPFv3 a zone unique
3. Configuration OSPF à zone multiple

OSPFv3

- OSPFv3 est l'équivalent OSPFv2 pour l'échange de préfixes IPv6. L'OSPFv3 échange des informations de routage pour renseigner la table de routage IPv6 avec des préfixes distants.
- OSPFv3 dispose des mêmes fonctionnalités qu'OSPFv2, à la différence près qu'il utilise IPv6 comme transport de couche réseau, en communiquant avec les homologues OSPFv3 et en annonçant les routes IPv6.
- OSPFv3 utilise également l'algorithme SPF comme moteur de calcul pour déterminer les meilleurs chemins dans l'ensemble du domaine de routage.
- OSPFv3 a des processus distincts par rapport à son homologue IPv4. Les processus et les opérations sont fondamentalement les mêmes que dans le protocole de routage IPv4, mais ils fonctionnent indépendamment.

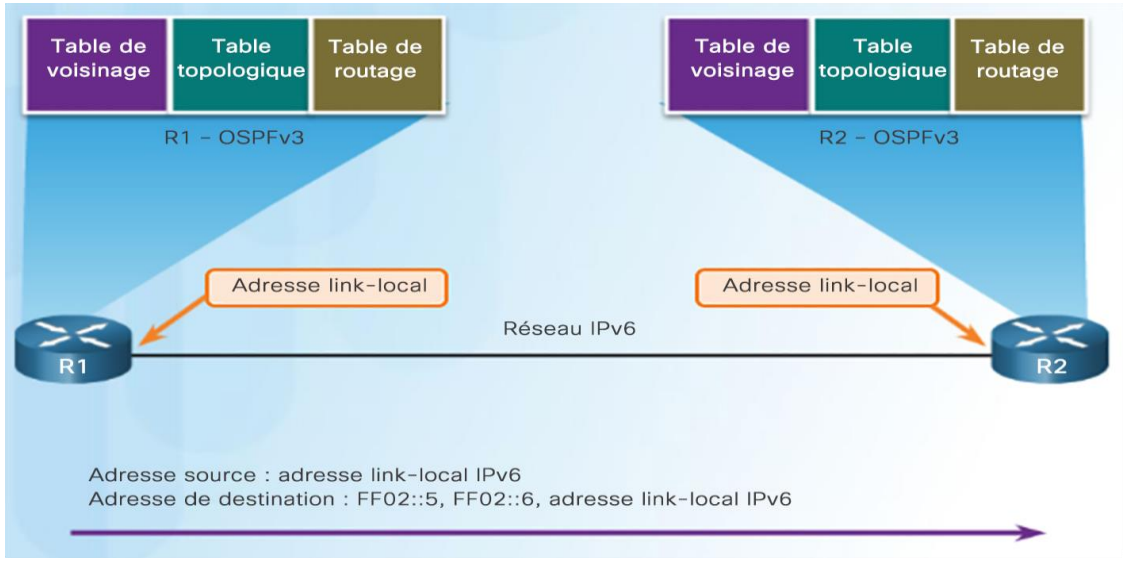


OSPFv3 vs OSPFv2

Caractéristique	OSPFv2	OSPFv3
Annonces	Réseaux IPv4	Préfixes IPv6
Adresse source	Adresse IPv4 source	Adresse link-local IPv6
Adresse de destination	Options possibles : • Adresse de multidiffusion IPv4 voisine • Adresse de multidiffusion tous les routeurs OSPF 224.0.0.5 • Adresse de multidiffusion 224.0.0.6 DR/BDR	Options possibles : • Adresse link-local IPv6 voisine • Adresse de multidiffusion FF02::5 pour tous les routeurs OSPF • Adresse de multidiffusion FF02::6 DR/BDR
annonce des réseaux	Configuration au moyen de la commande de configuration de routeur **network**	Configuration au moyen de la commande de configuration d'interface **ipv6 ospf** *id-processus* **area** *id-zone*
Routage de monodiffusion IP	Le routage de monodiffusion IPv4 n'est pas activé par défaut	Le transfert de monodiffusion IPv6 n'est pas activé par défaut. Utilisez la commande de configuration globale **ipv6 unicast-routing** pour l'activation.
Authentication	Texte clair et MD5	Authentification IPv6 (IPsec)

Adresses link-local

- Une adresse link-local IPv6 permet à un appareil de communiquer avec d'autres appareils IPv6 sur la même liaison et uniquement sur cette liaison (sous-réseau).
- Les paquets associés à une adresse source ou de destination link-local ne peuvent pas être acheminés au-delà de leur liaison d'origine.
- Les adresses link-local IPv6 sont utilisées pour échanger les messages OSPFv3.

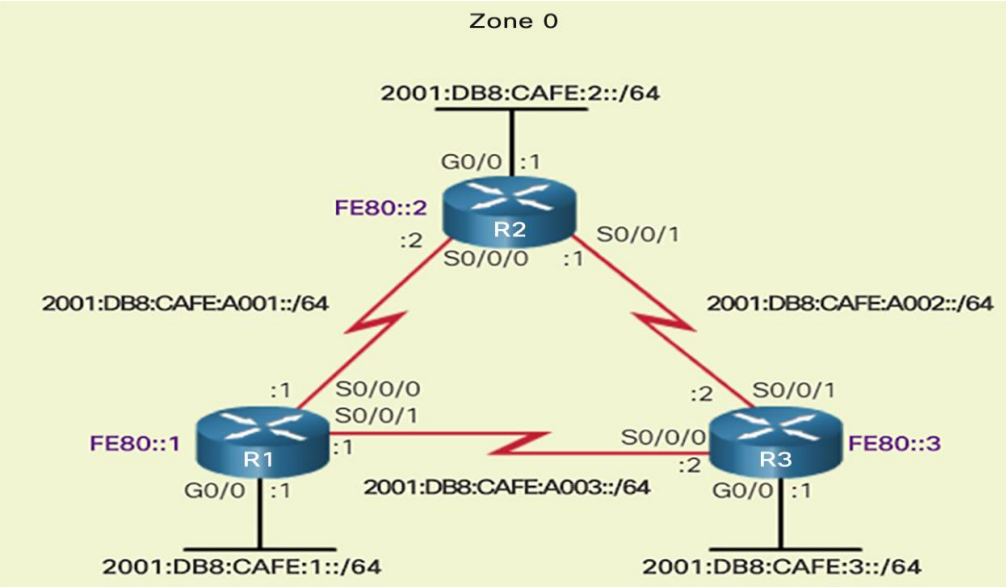


Configuration OSPFv3 à zone unique

Étapes de configuration du protocole OSPFv3 a zone unique

1. Activez le routage de monodiffusion IPv6 en mode de configuration globale : **ipv6 unicast-routing**.
2. (Facultatif) Configurez les adresses link-local.
3. Configurez un ID de routeur 32 bits dans de mode de configuration de routeur OSPFv3 – **router-id** *rid*.
4. Configurez les informations facultatives de routage, telles que l'ajustement de la bande passante de référence.
5. (Facultatif, mais recommandé) Configurez les paramètres d'interface OSPFv3 spécifiques tels que la configuration de la bande passante sur les liaisons série.
6. Activez le routage OSPFv3 routage en mode de configuration d'interface : **ipv6 ospf area**.

- **Topologie réseau OSPFv3**



PARTIE 5

PARTIE 5

Configuration de l'ID de routeur OSPFv3

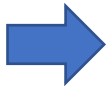
- Utilisez la commande de configuration globale **ipv6 router ospf** *id-processus* pour passer en mode de configuration du routeur.
- Utilisez la commande de mode de configuration de routeur **router-id** *rid* pour attribuer un ID de routeur et exécutez la commande **show ipv6 protocols** pour la vérification.

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)#
*Mar 29 11:21:53.739: %OSPFv3-4-NORTRID: Process OSPFv3-1-
IPv6 could not pick a router-id, please configure manually
R1(config-rtr)#
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)#
R1(config-rtr)# auto-cost reference-bandwidth 1000
% OSPFv3-1-IPv6:  Reference bandwidth is changed. Please
ensure reference bandwidth is consistent across all routers.
R1(config-rtr)#
R1(config-rtr)# end
R1#
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
    None
```

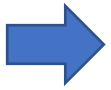
Modification d'un ID de routeur OSPFv3

Utilisez la commande de mode d'exécution privilégié **clear ipv6 ospf process** après avoir modifié l'ID de routeur pour valider la modification de l'ID de routeur et forcer un routeur à renégocier les contiguïtés de voisinage en utilisant le nouvel ID de routeur.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 10.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
   None
```



```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# end
R1#
```



```
R1# clear ipv6 ospf process
Reset selected OSPFv3 processes? [no]: y
R1#
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Number of areas: 0 normal, 0 stub, 0 nssa
  Redistribution:
    None
```

Activation du protocole OSPFv3 a zone unique sur des interfaces

- Utilisez la commande de mode de configuration d'interface **ipv6 ospf area** pour activer OSPFv3 sur une interface spécifique. Assurez-vous que l'interface se trouve dans une zone OSPF.
- Utilisez la commande **show ipv6 ospf interfaces brief** pour la vérification.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# interface Serial0/0/1
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)#
R1(config-if)# end
R1#
R1# show ipv6 ospf interfaces brief
Interface  PID   Area     Intf ID  Cost   State  Nbrs F/C
Se0/0/1    10     0         7      15625  P2P    0/0
Se0/0/0    10     0         6      647    P2P    0/0
Gi0/0      10     0         3       1     WAIT   0/0
R1#
```

Vérification des voisins OSPFv3 a zone unique

- Utilisez la commande **show ipv6 ospf neighbor** pour vérifier la connectivité de voisinage avec les routeurs connectés directement.

```
R1# show ipv6 ospf neighbor

OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

Neighbor ID     Pri   State           Dead Time   Interface ID  Interface
3.3.3.3           0   FULL/  -        00:00:39    6             Serial0/0/1
2.2.2.2           0   FULL/  -        00:00:36    6             Serial0/0/0
```

Sortie	Description
Neighbor ID	L'ID de routeur du routeur voisin
Pri	Le niveau de priorité OSPFv3 de l'interface utilisé dans le processus de sélection DR/BDR
État	L'état OSPFv3 – Full signifie que l'algorithme a été exécuté pour la base de données d'état des liaisons et que le routeur voisin et R1 disposent de LSDB identiques. Les interfaces Ethernet à accès multiple peuvent apparaître comme 2WAY. Un tiret indique qu'aucun DR/BDR n'est nécessaire.
Dead Time	Durée restante avant de déclarer un voisin comme hors service en cas de non-réception d'un paquet Hello OSPFv3. Cette valeur est réinitialisée lorsqu'un paquet Hello est reçu.
Adresse	L'adresse de l'interface en connexion directe du voisin
Interface	L'interface sur R1 utilisée pour former une contiguïté avec le routeur voisin

Vérification des paramètres et les interfaces du protocole OSPFv3 a zone unique

- Exécutez la commande **show ipv6 protocols** pour vérifier des informations clés sur la configuration OSPFv3.

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
 Router ID 1.1.1.1
 Number of areas: 1 normal, 0 stub, 0 nssa
 Interfaces (Area 0):
   Serial0/0/1
   Serial0/0/0
   GigabitEthernet0/0
```

- Exécutez la commande **show ipv6 ospf interface** pour afficher une liste détaillée de chaque interface compatible OSPFv3.
- La commande **show ipv6 ospf interface brief** est un résultat plus facile pour vérifier que les interfaces sont utilisées pour OSPFv3.

```
R1# show ipv6 ospf interface brief
Interface    PID   Area            Intf ID    Cost  State Nbrs F/C
Se0/0/1      10    0               7          15625 P2P   1/1
Se0/0/0      10    0               6          647   P2P   1/1
Gi0/0        10    0               3          1     DR    0/0
```

Vérification de la table de routage IPv6

- Utilisez la commande **show ipv6 route** pour voir la table de routage IPv6.
- Utilisez la commande **show ipv6 route ospf** pour afficher uniquement les routes OSPFv3.

```
R1# show ipv6 route ospf
IPv6 Routing Table - default - 10 entries
Codes:C - Connected, L - Local, S - Static, U - Per-user Static route
      B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
      I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
      EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
      NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
     OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
 O   2001:DB8:CAFE:2::/64 [110/657]
     via FE80::2, Serial0/0/0
 O   2001:DB8:CAFE:3::/64 [110/1304]
     via FE80::2, Serial0/0/0
 O   2001:DB8:CAFE:A002::/64 [110/1294]
     via FE80::2, Serial0/0/0
```

CHAPITRE 2

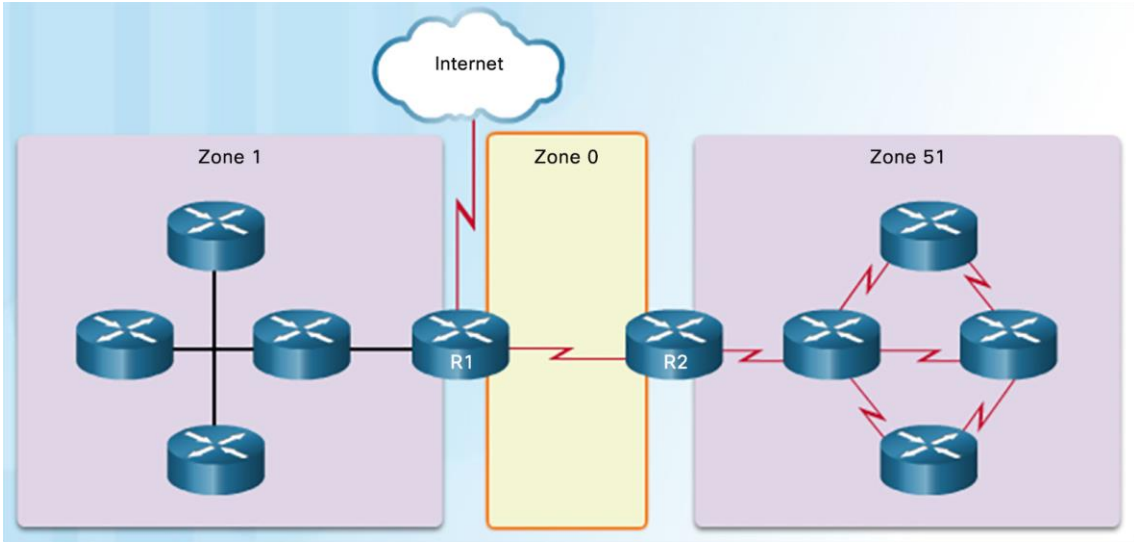
Implémenter le protocole OSPFv2 à zone unique

1. Configuration OSPFv2 à zone unique
2. Configuration OSPFv3 a zone unique
3. Configuration OSPF à zone multiple

Étapes d'implémentation du protocole OSPF a zone multiple

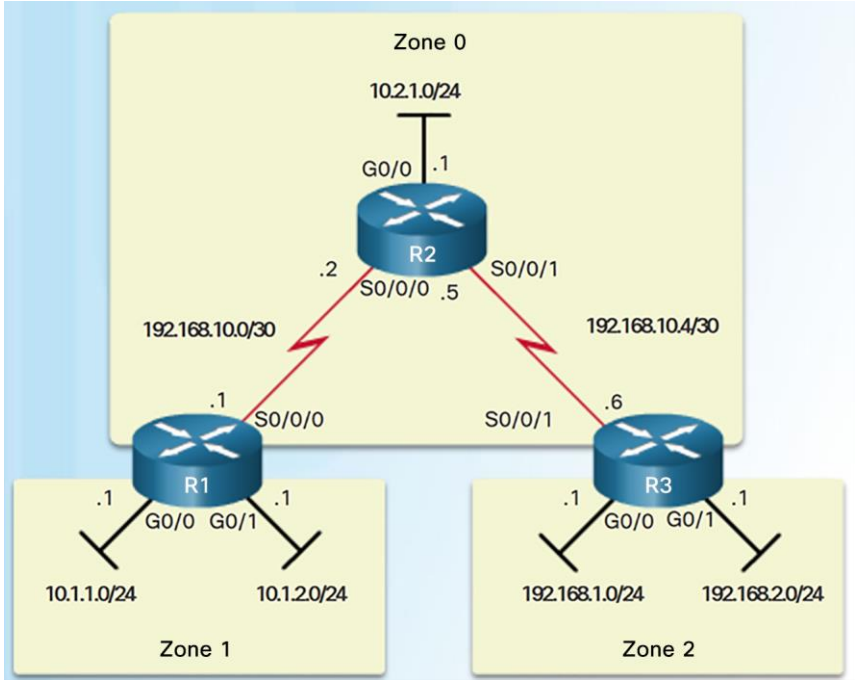
Il existe quatre étapes d'implémentation du protocole OSPF à zones multiples :

- **Étape 1**. Regroupez les paramètres et exigences de réseau
- **Étape 2**. Définissez les paramètres OSPF
  - Protocole OSPF à zone unique ou à zones multiples ?
  - Plan d'adressage IP
  - Zones OSPF
  - Topologie du réseau
- **Étape 3**. Configurez l'implémentation OSPF à zones multiples sur la base des paramètres définis précédemment.
- **Étape 4**. Vérifiez l'implémentation du protocole OSPF à zones multiples.



Configuration du protocole OSPFv2 à zones multiples

Topologie réseau OSPFv2 a zone multiple :



Configuration :

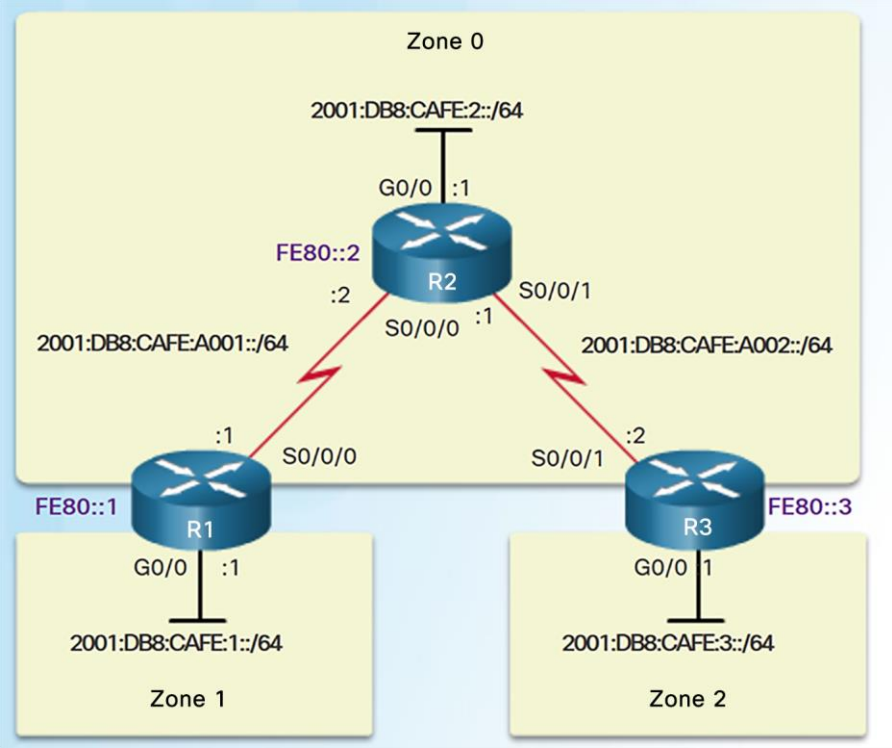
```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# network 10.1.1.1 0.0.0.0 area 1
R1(config-router)# network 10.1.2.1 0.0.0.0 area 1
R1(config-router)# network 192.168.10.1 0.0.0.0 area 0
R1(config-router)# end
R1#
```

- Aucune commande spéciale n'est requise pour implémenter un protocole OSPFv2 à zones multiples.
- Un routeur devient un routeur ABR lorsqu'il possède deux instructions network dans différentes zones.
- R1 est un routeur ABR. Il dispose de plusieurs interfaces dans la zone 1 et d'une dans la zone 0.

PARTIE 5

Configuration du protocole OSPFv3 à zones multiples

Topologie réseau OSPFv3 a zone multiple :



Configuration :

```
R1(config)# ipv6 router ospf 10
R1(config-rtr)# router-id 1.1.1.1
R1(config-rtr)# exit
R1(config)#
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ipv6 ospf 10 area 1
R1(config-if)#
R1(config-if)# interface Serial0/0/0
R1(config-if)# ipv6 ospf 10 area 0
R1(config-if)# end
R1#
```

- Aucune commande spéciale n'est requise pour implémenter un protocole OSPFv3 à zones multiples.
- Un routeur devient un ABR lorsqu'il a deux interfaces dans différentes zones.

PARTIE 5

PARTIE 5

Vérification du protocole OSPF à zones multiples

- Commandes pour vérifier le protocole OSPFv2 à zones multiples
  - **show ip ospf neighbor**
  - **show ip ospf**
  - **show ip ospf interface**
  - **Show ip protocols**
  - **show ip ospf interface brief**
  - **show ip route ospf**
  - **show ip ospf database**

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  It is an area border router
  Number of areas in this router is 2. 2 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    10.1.1.1 0.0.0.0 area 1
    10.1.2.1 0.0.0.0 area 1
    192.168.10.1 0.0.0.0 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      02:20:36
    2.2.2.2              110      02:20:39
  Distance: (default is 110)
```

- Commandes pour vérifier le protocole OSPFv2 à zones multiples
  - **show ipv6 ospf neighbor**
  - **show ipv6 ospf**
  - **show ipv6 ospf interface**
  - **Show ipv6 protocols**
  - **show ipv6 ospf interface brief**
  - **show ipv6 route ospf**
  - **show ipv6 ospf database**

```
R1# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "ospf 10"
  Router ID 1.1.1.1
  Area border router
  Number of areas: 2 normal, 0 stub, 0 nssa
  Interfaces (Area 0):
    Serial0/0/0
  Interfaces (Area 1):
    GigabitEthernet0/0
  Redistribution:
    None
R1#
```

CHAPITRE 3

Implémenter le protocole BGP

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le concept et implémenter le protocole BGP

1,5 heures

CHAPITRE 2

Implémenter le protocole BGP

1. Concepts du protocole BGP
2. Configuration du protocole BGP

Système Autonome (AS)

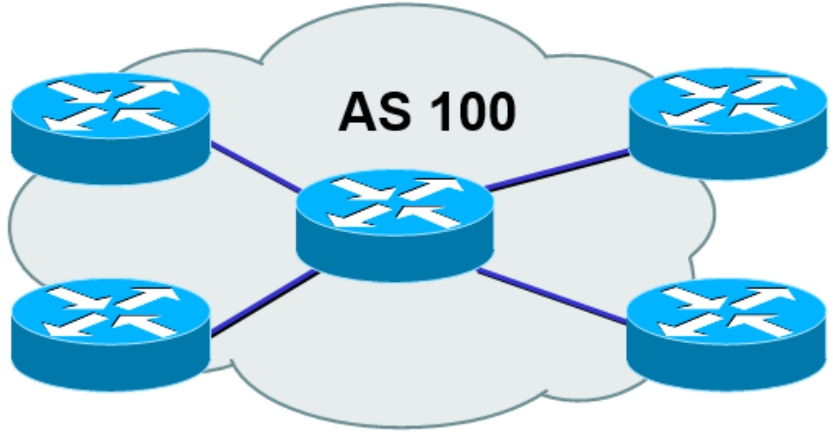
- Ensemble de réseaux partageant la même politique de routage
- Utilisation d'un même protocole de routage
- Généralement sous une gestion administration unique
- Utilisation d'un IGP au sein d'un même AS
- Caractérisé par un numéro d'AS :

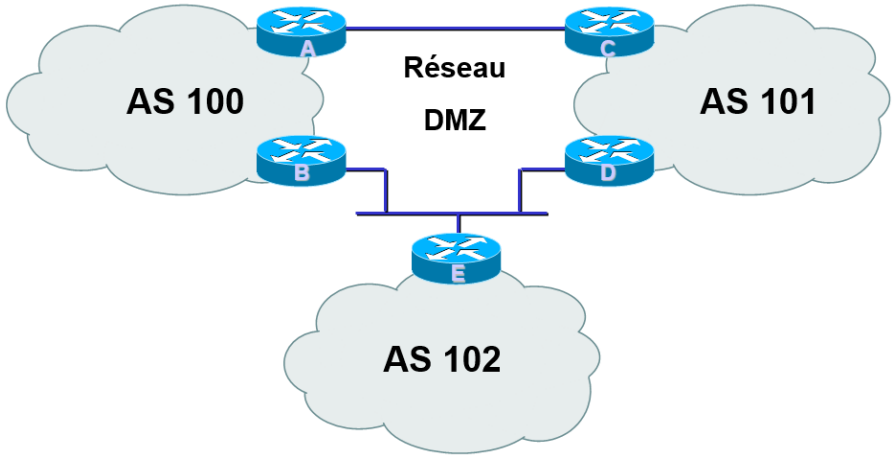
  Défini par la RFC1771 sur 16bits soit 65535 possibilities, Gere par l'IANA et ses délégations

- Il existe des numéros d'AS privés et publics

  AS 0 : reserve
  De AS 1 a AS 64496 : reserve par l'IANA pour un usage public
  De AS 64496 a AS 64511 : reserve pour de la documentation
  De AS 64512 a AS 65534 : usage privée
  AS 65535 : reserve

- Le réseau démilitarisé est partagé entre plusieurs AS



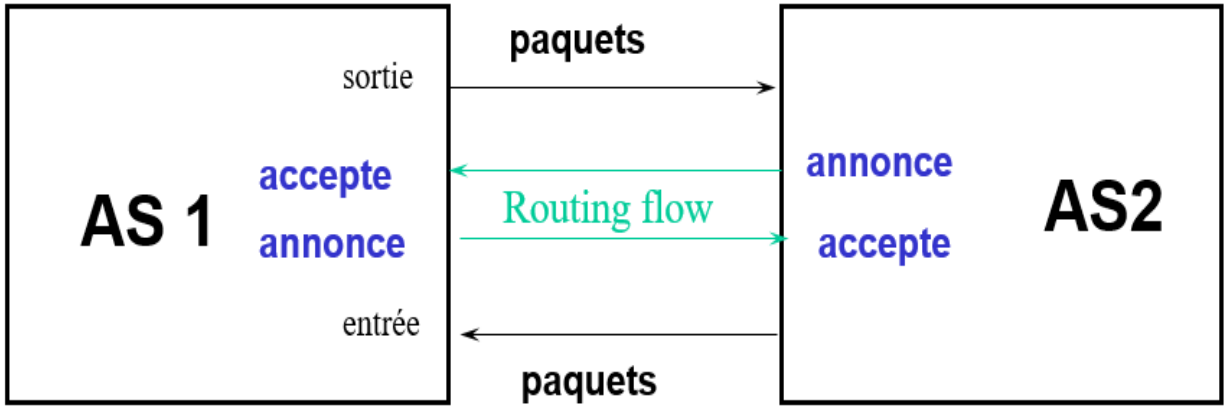


Pourquoi a-t-on besoin d'un EGP ?

- S'adapter à un réseau de grande taille
  - Hiérarchie
  - limiter la portée des pannes
- Définir des limites administratives
- Routage politique
  - contrôler l'accessibilité des préfixes (routes)

Politique de routage

- Définition de ce que vous acceptez ou envoyez aux autes
  - connexion économique, partage de charge, etc...
- Accepter des routes de certains FAI et pas d'autres
- Envoyer des routes à certains FAI et pas à d'autres
- Préferrer les routes d'un FAI plutôt que d'un autre

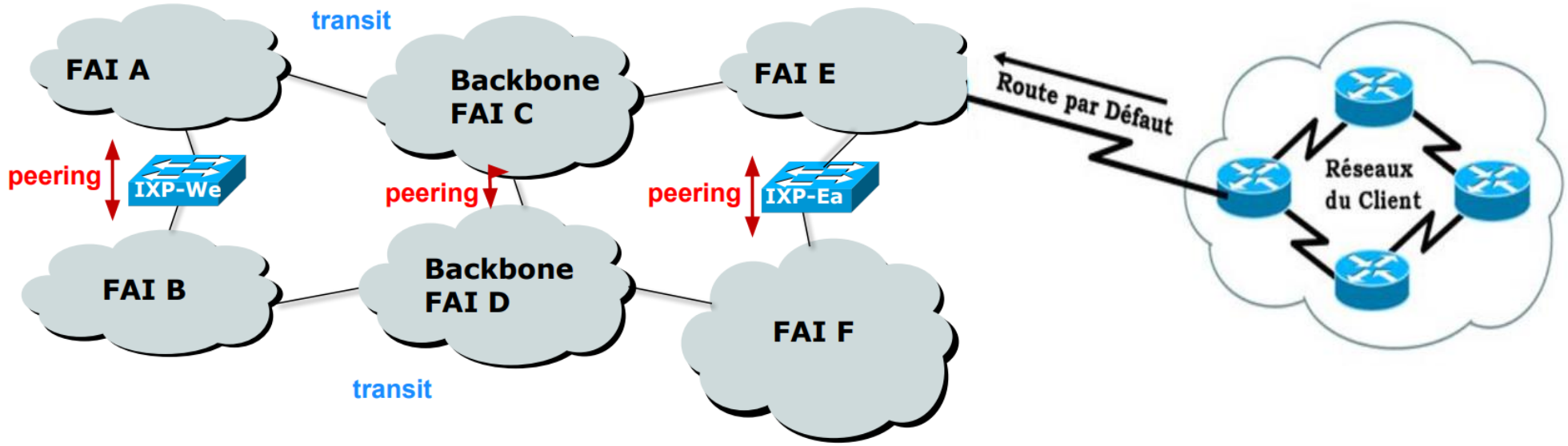


Pour que **AS 1** et **AS 2** puissent communiquer :
AS1 annonce des routes à AS2
AS2 accepte des routes de AS1
AS2 annonce des routes à AS1
AS1 accepte des routes de AS2

PARTIE 5

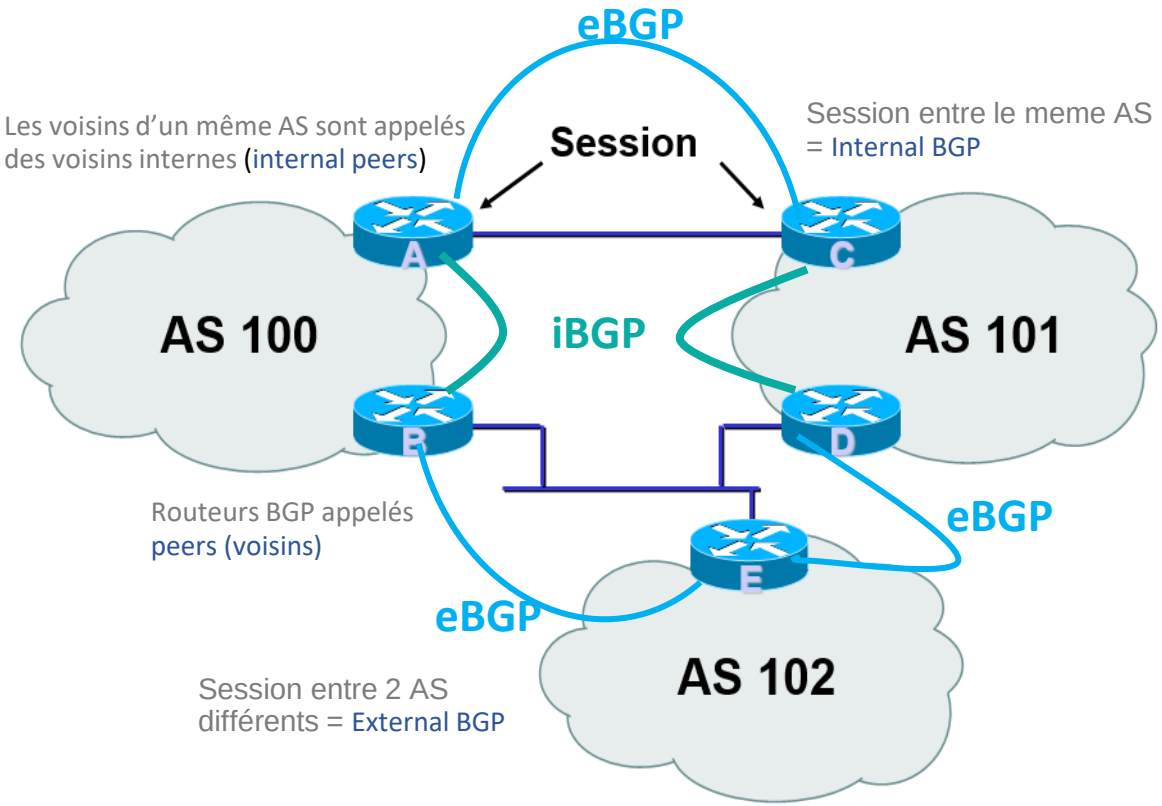
Peering et transit

- **Transit** – Transporter du traffic à travers le réseau d'un opérateur.
- **Peering** – échange d'information de routage et de trafic.
- **Default** – Destination par défaut lorsqu'il n'y a pas de routes spécifiques dans la table de routage



Le protocole BGP

- **BGP** (Path Vector Protocol) est un protocole EGP utilisé entre AS
- BGP est un protocole de routage basé sur les vecteurs de chemin (path vector) (voir RFC 1322)
- BGP est transporté par le protocole TCP
- Les mises à jours sont incrémentielles
- BGP conserve le chemin d'AS pour atteindre un réseau cible
- De nombreuses options permettent d'appliquer une politique de routage
- Chaque AS est le point de départ d'un ensemble de préfixes (NLRI)
- Les préfixes sont échangés dans les sessions BGP
- Plusieurs chemins possibles pour un préfixe
- Choix du meilleur chemin pour le routage
- Les attributs et la configuration "politique" permettent d'influencer ce choix du meilleur chemin
- Chaque routeur iBGP doit établir une session avec tous les autres routeurs iBGP du même AS



Le protocole BGP

Quand utiliser BGP?

BGP est le plus approprié quand au moins une des conditions suivantes existe:

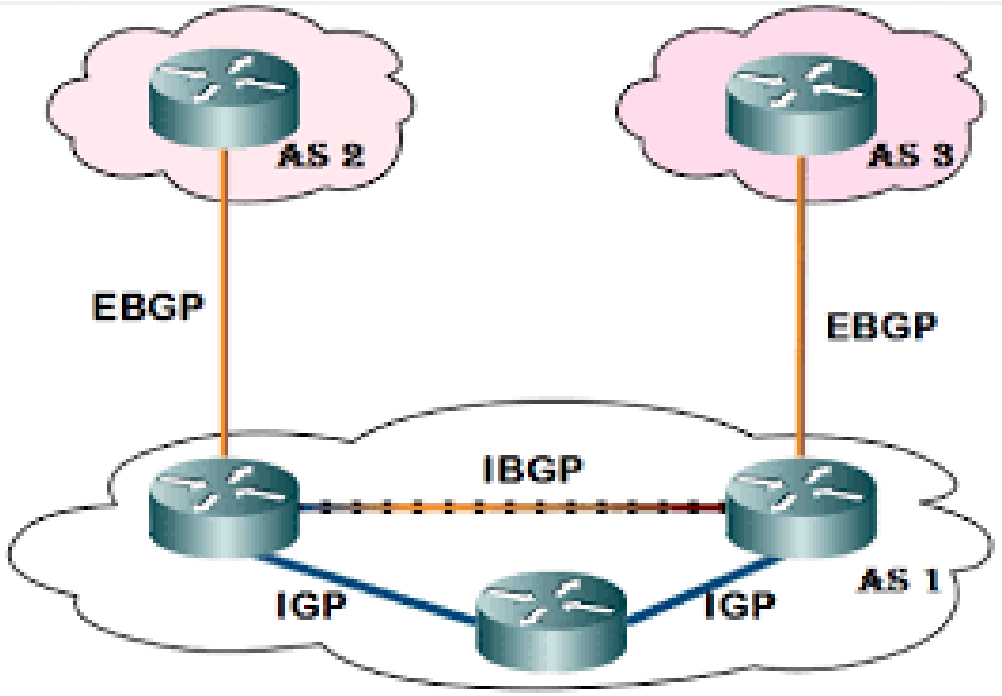
- Un AS a des connexions multiples avec d'autres AS-
- Un AS autorise les paquets à transiter pour joindre d'autres systèmes autonomes
- Le trafic entrant et sortant de votre AS doit être manipulé
- Les effets de BGP sont très bien compris et maîtrisés.

Quand ne pas utiliser BGP?

BGP n'est pas toujours très approprié. Ne pas utiliser BGP si vous avez une des conditions suivantes :

- Une seule connexion à Internet ou à un autre AS-
- La politique de routage et la sélection de route ne concernent pas votre AS
- Manque de mémoire ou de puissance CPU sur les routeurs BGP pour gérer les mises à jour
- Maîtrise insuffisante du processus de sélection de chemin BGP et du filtrage de route
- Faible bande passante entre systèmes autonomes

→Utilisez des routes Statiques à la place de BGP.



iBGP pour le transport
- Quelques/Tous les préfixes Internet à travers le backbone de l'ISP
- Préfixe des clients des ISP

eBGP utilisé
- Exchanger les préfixes avec les autres AS
- Implémente la politique de routage

PARTIE 5

Création de la table de Forwarding

- BGP "**in**" fonctionnement

  Recois les informations chemin du "peers"

  Résultat de la sélection des chemins est inséré dans la table BGP.

  "best path" est taggué

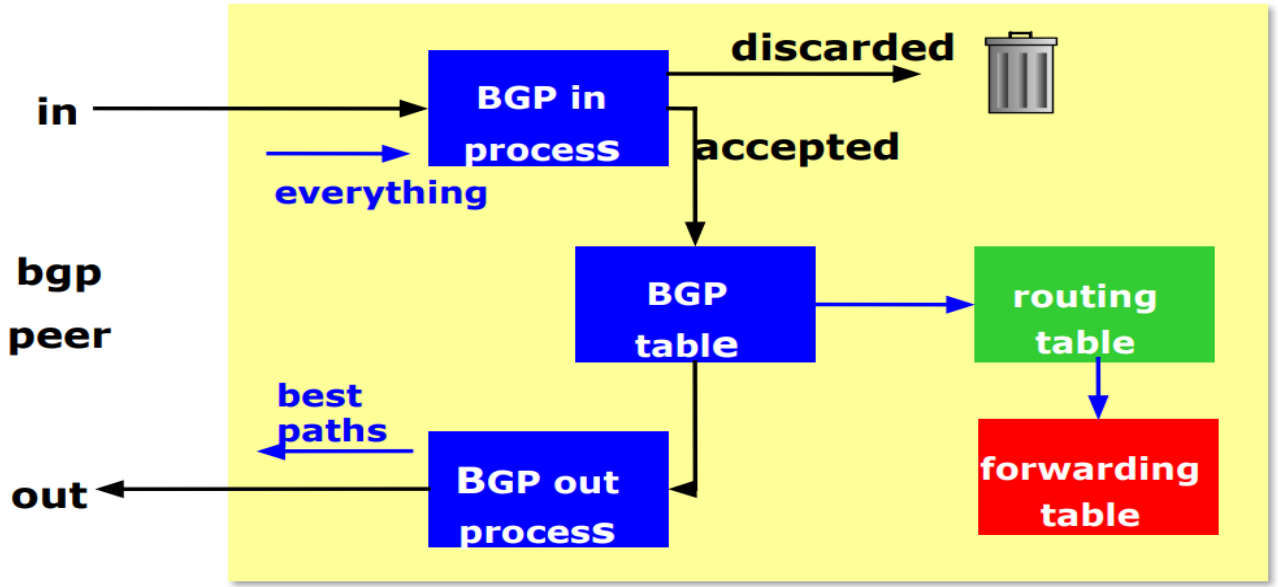
- BGP "**out**" fonctionnement

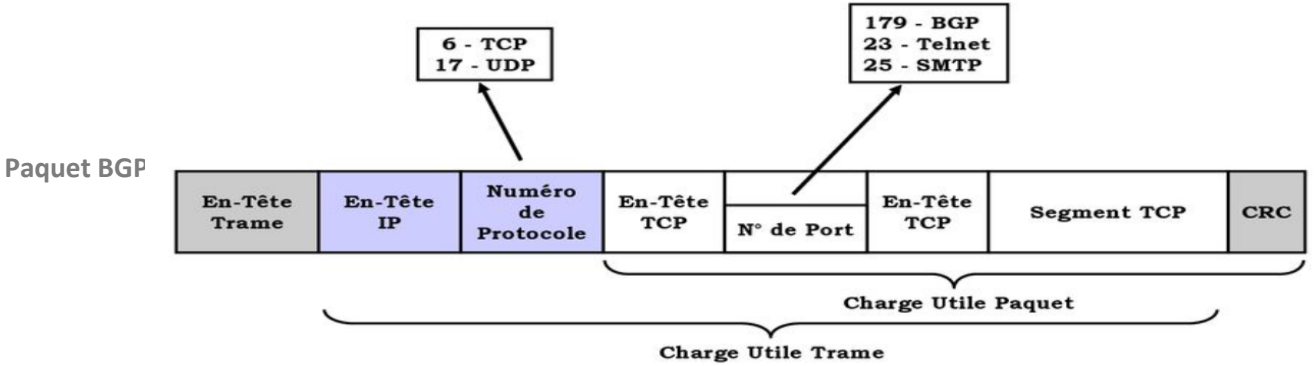
  announce les informations des "meilleurs routes" aux peers

- Les meilleures routes sont installées dans la table de routage (**RIB**)
- Les meilleurs routes sont installées dans la table de forwarding (**FIB**):

  Les préfixes et longueur de préfixe sont uniques

  Plus petite "Distance administrative"





PARTIE 5

Types de messages BGP

- Différents types de messages sont utilisés pour le fonctionnement de BGP
- Chaque message (Min 19 Octets, Max 4096 Octets) comprend un en-tête constitué de trois champs:
  - **Marker (16 octets)** : Authentifie les messages BGP entrants ou détecte une perte de synchronisation
  - **Length (2 octets)** : Longueur du message BGP, en-tête inclus
  - **Type (1 Octet)** : Type de message (4 valeurs)

Les messages BGP :

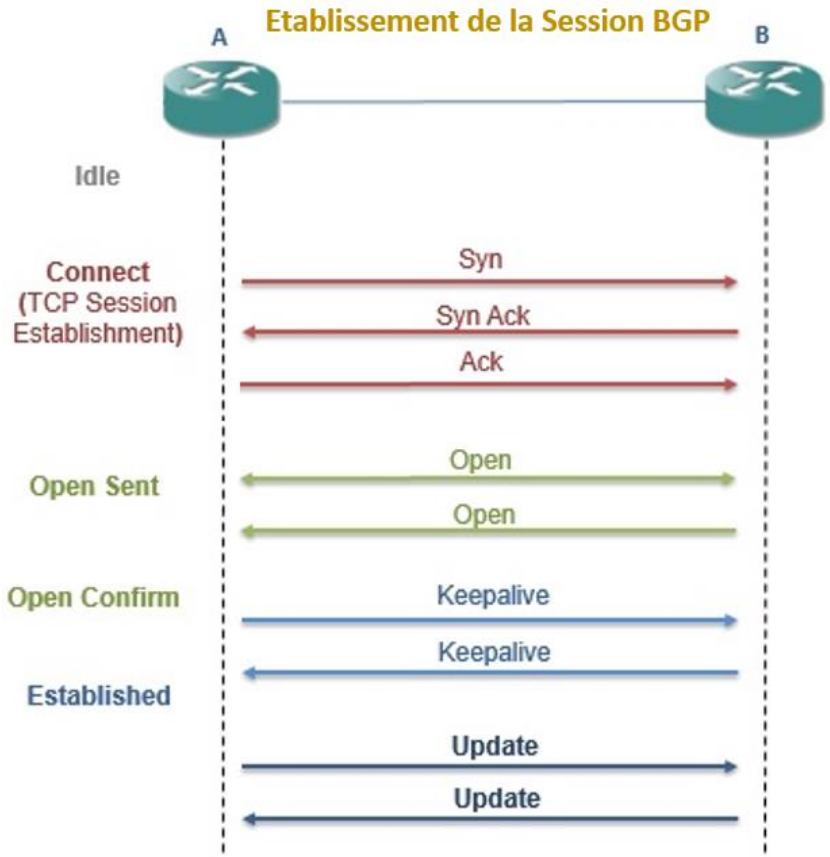
- **Open :** Etablissement d'une connexion BGP. Contient : version BGP, N°AS, Hold time, Router ID
- **Keepalive :**

  Transmis périodiquement entre voisins pour maintenir les connexions

  Hold time = 3 périodes de Keepalive
- **Notification :**

  Informe le routeur récepteur de la présence d'erreurs La connexion est fermée après l'envoi de ce message
- **Update :**

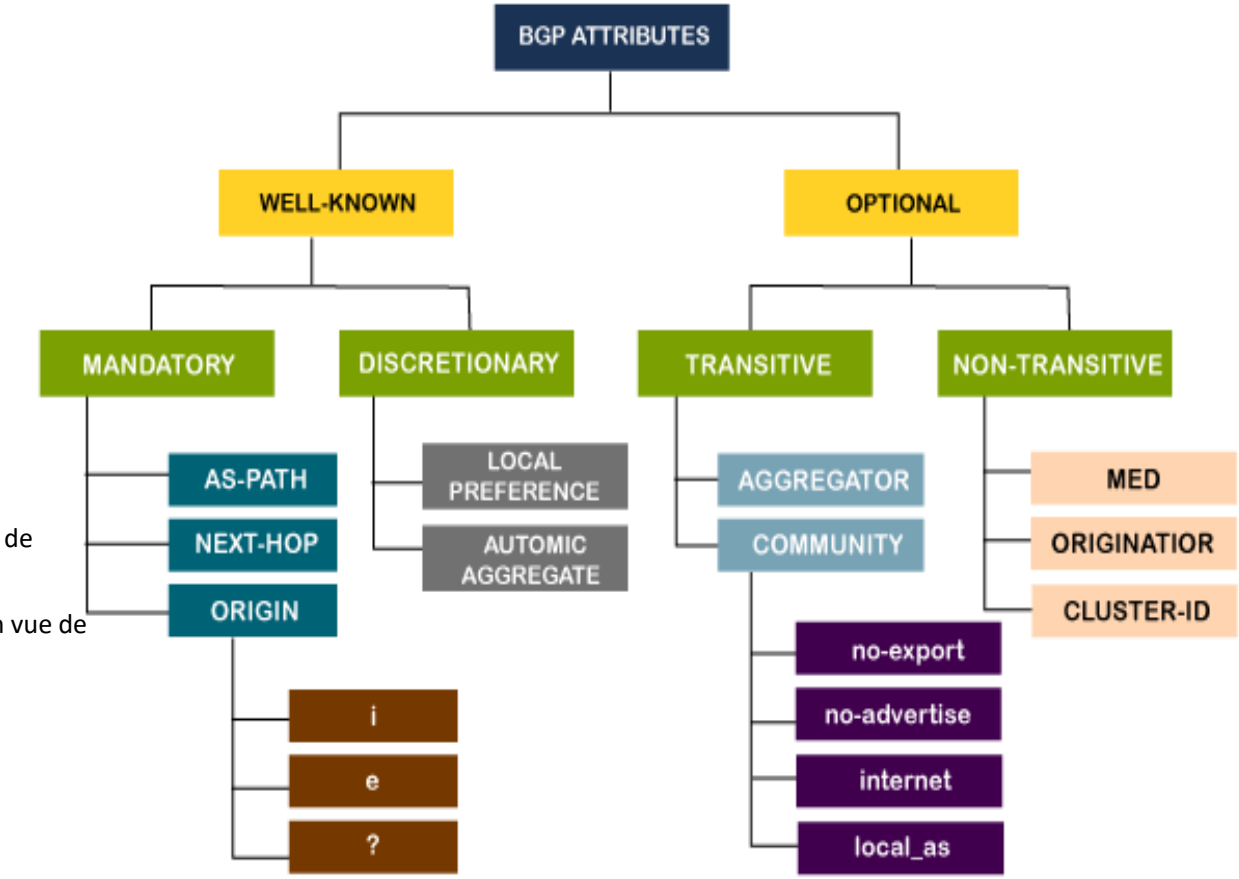
  Contient toutes les informations que BGP utilise Informations concernant un chemin Constitués de trois composantes: NLRI (Network Layer Reachability Information) Attributs de chemins Routes retirée.



PARTIE 5

Les attributs de chemins BGP

- Encodés sous la forme d'un triplet Type, Longueur & Valeur (TLV)
- Attributs Transitifs ou non transitif
- Certains attributs sont obligatoires
- Ils sont utilisés pour choisir le meilleur chemin
- Ils permettent d'appliquer des règles d'ingéniérie du trafic (routage politique)
- Liste des attributs de chemins BGP
  - **Origin :** Origine de la route (IGP, EGP ou Incomplete)
  - **AS-path (chemin d'AS) :** Liste ordonnée des systèmes autonomes traversés
  - **Next-hop (prochain routeur) :** Adresse IP du voisin eBGP
  - **Multi-Exit Discriminator (MED) :** Métrique destinée aux routeurs externes en vue de préférer certaines routes internes
  - **Local preference (préférence locale) :** Métrique destinée aux routeurs internes en vue de préférer certaines routes externes
  - **BGP Community (communauté BGP) :** Marquage de route
  - **Atomic Aggregate :** Liste des AS supprimés après une agrégation
  - **Aggregator :** Identificateur et AS du routeur qui a réalisé l'agrégation
  - **Cluster ID :** Cluster d'origine
  - **Originator ID** : Identificateur du route reflector

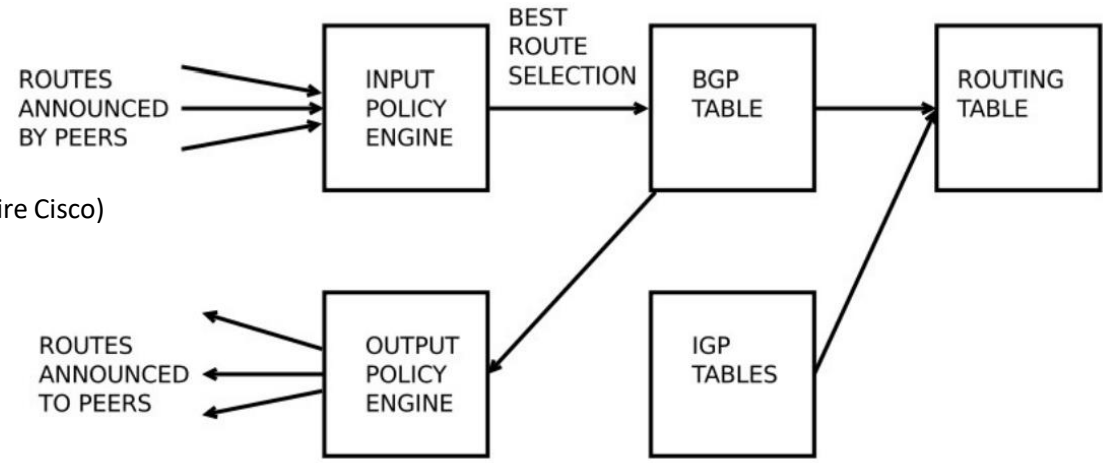


PARTIE 5

Le processus de décision de BGP

Les étapes du processus de décision

Prend en compte uniquement les routes sans boucles et avec un prochain saut valide

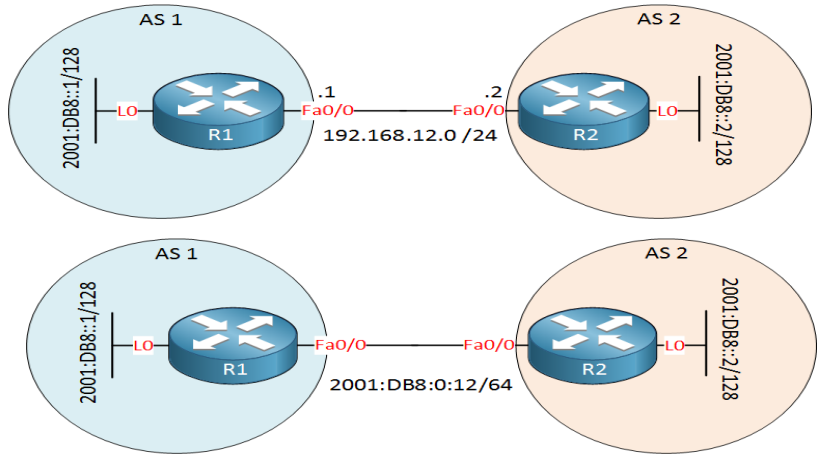


1. Si le prochain saut est inaccessible, la route est ignorée
2. Si attribut **Weight** utilisé alors choix de la valeur la plus élevée (Local au routeur - Propriétaire Cisco)
3. Attribut **Local preference** - Choix de la valeur la plus élevée (Global dans l'AS)
4. Route dont ce routeur est l'**origine**
5. Attribut **AS-Path** - chemin le plus court
6. Attribut **Origin** - Valeur la plus faible (IGP< EGP < Incomplete)
7. Attribut **MED** - Valeur la plus faible (Venant d'autres AS)
8. Chemin **eBGP** préféré par rapport au chemin iBGP
9. Chemin via le voisin IGP le plus proche (Chemin interne)
10. **Router ID BGP** le plus faible (Adresse IP la plus élevée sur le routeur ou adresse IP d'une interface Loopback)

PARTIE 2

Multi-Protocol BGP pour IPv6 – RFC2545

- La version normale de BGP ne prenait en charge que les préfixes de monodiffusion IPv4. Aujourd'hui nous utilisons MP-BGP (Multiprotocol BGP) qui supporte différentes adresses : **IPv4 unicast, IPv4 multicast, IPv6 unicast, IPv6 multicast**
- MP-BGP est également utilisé pour MPLS VPN où nous utilisons MP-BGP pour échanger les étiquettes VPN. Pour chaque type "d'adresse" différent, MP-BGP utilise une famille d'adresses différente.
- Pour autoriser ces nouvelles adresses, MBGP a quelques nouvelles fonctionnalités que l'ancien BGP n'a pas :
  - **Identifiant de famille d'adresses (AFI) :** spécifie la famille d'adresses.
  - **Identifiant de famille d'adresses ultérieures (SAFI) :** Contient des informations supplémentaires pour certaines familles d'adresses.
  - **Informations d'accessibilité de la couche réseau multiprotocole inaccessible (MP_UNREACH_NLRI) :** il s'agit d'un attribut utilisé pour transporter les réseaux inaccessibles.
  - **Annonce des capacités BGP :** Ceci est utilisé par un routeur BGP pour annoncer à l'autre routeur BGP quelles capacités il prend en charge. MP-BGP et BGP-4 sont compatibles, le routeur BGP-4 peut ignorer les messages qu'il ne comprend pas.
- Étant donné que MP-BGP prend en charge IPv4 et IPv6, nous avons plusieurs options. Les routeurs MP-BGP peuvent devenir voisins en utilisant des adresses IPv4 et échanger des préfixes IPv6 ou inversement. Voyons quelques exemples de configuration…



NLRI = Network Layer Reachability Information = Préfixes

CHAPITRE 2

Implémenter le protocole BGP

1. Concept du protocole BGP
2. Configuration du protocole BGP

Étapes de la configuration BGP

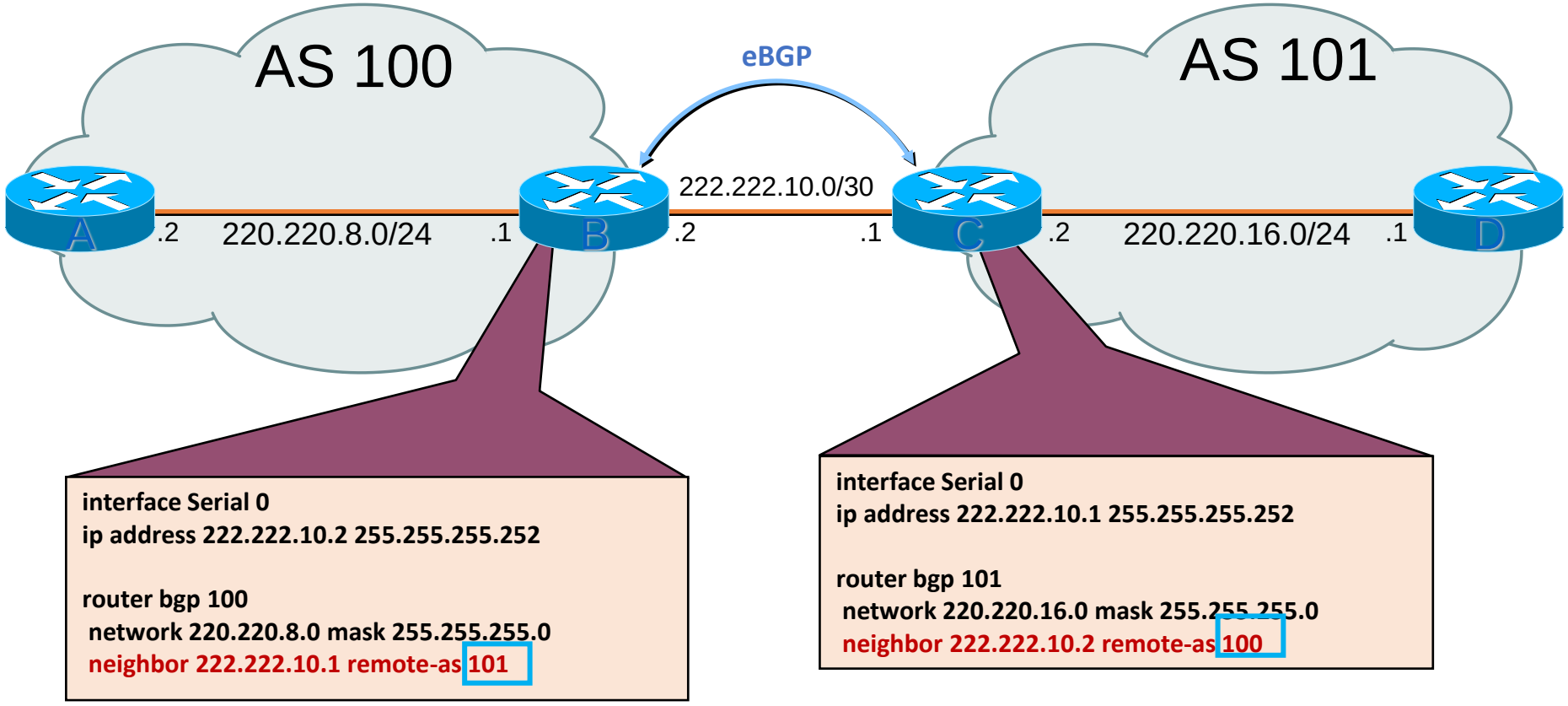
Pour mettre en œuvre eBGP :

- Activez le routage BGP.
- Configurez les voisins (homologues) BGP.
- Annoncez les réseaux provenant de ce système autonome (AS).

Commande	Description
`Router(config)# router bgp as-number`	Active un processus de routage BGP et place le routeur en mode de configuration.
`Router(config-router)# neighbor ip-address remote-as as-number`	Spécifie un voisin BGP. Le numéro AS est le numéro AS du voisin.
`Router(config-router)# network network-address [mask network-mask]`	Annonce une adresse réseau à un voisin eBGP en indiquant qu'elle provient de cet AS. Le masque de réseau est le masque de sous-réseau du réseau.

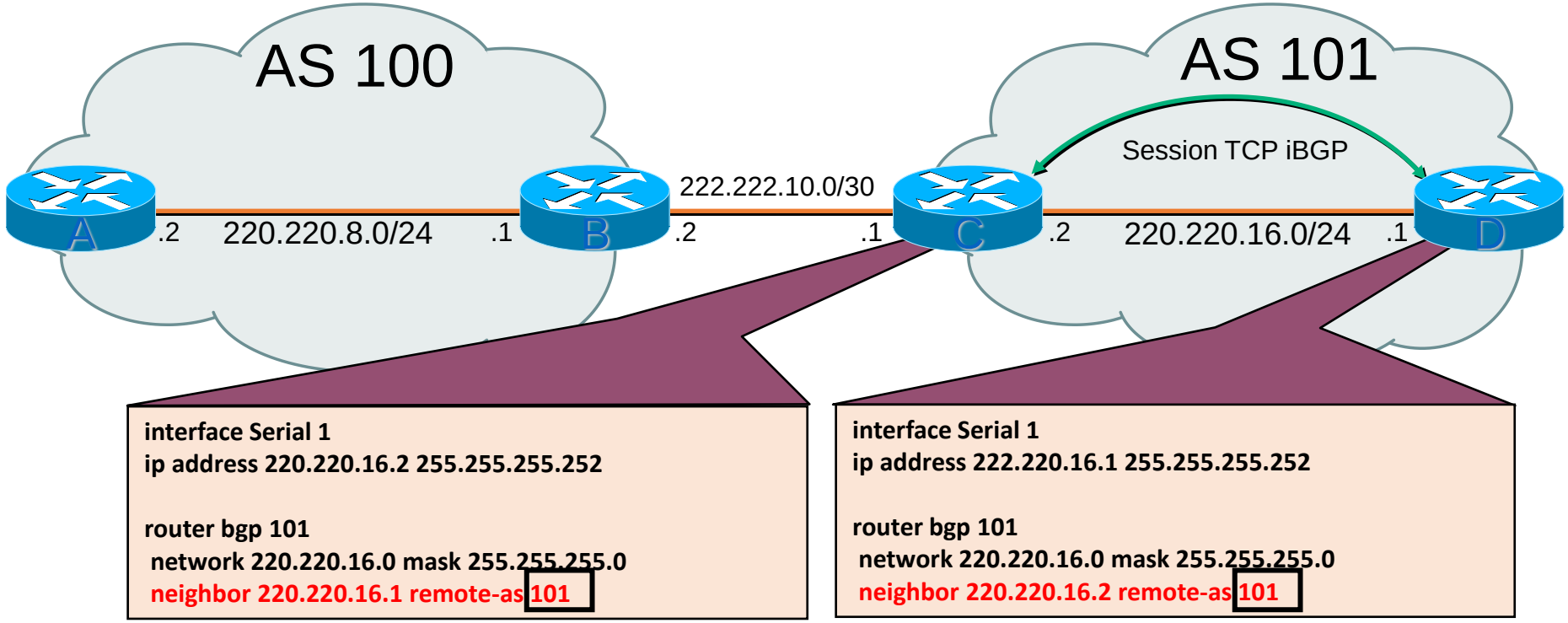
Exemple de configuration du protocole eBGP

- à zone unique



Exemple de configuration du protocole iBGP

- à zone unique



Vérification de la configuration BGP

- Ces commandes permettent de vérifier la configuration BGP :

Commande	Description
show ip bgp	Affiche les entrées de la table de routage BGP. Vous pouvez spécifier un numéro de réseau pour avoir des informations plus spécifiques sur un préfixe ou utiliser le mot -clé subnets pour avoir des informations plus spécifiques sur un préfixe et tous ses sous-réseaux.
show ip bgp summary	Affiche un résumé des connexions BGP
show ip bgp neighbors	Affiche des informations détaillées sur chaque connexion BGP
show ip bgp paths	Affiche tous les chemins BGP de la base de données

show ip bgp neighbors [address] [**received-routes**|**routes**|**advertised-routes**| {**paths** regular-expression}|**dampened-routes**]

Paramètres	Description
address	Adresse du voisin duquel vous avez appris les routes. Sans cet argument tous les voisins sont affichés.
received-routes	Affiche toutes les routes reçues du voisin (celles acceptées et celles refusées).
routes	Affiche toutes les routes acceptées et refusées. C'est un sous-ensemble du mot-clé received-routes.
advertised-routes	Affiche toutes les routes annoncées vers le voisin.
paths regular-expression	Spécifie une expression régulière utilisée pour établir une correspondance avec les chemins reçus.
dampened-routes	Affiche toutes les routes momentanément indisponibles avec le voisin à l'adresse spécifiée.

PARTIE 6

Gérer la connectivité des réseaux d'entreprise

Dans ce module, vous allez :

- Etre en mesure de comprendre les technologies de réseau WAN
- Etre capable de sécuriser l'accès au réseau informatique
- Etre en mesure de mettre en place un système de gestion, de surveillance et de dépannage des réseaux informatiques

9.5 heures

CHAPITRE 1

Étudier les réseaux étendus

Ce que vous allez apprendre dans ce chapitre :

- Étudier les différents technologies des réseaux étendus

2.5 heures

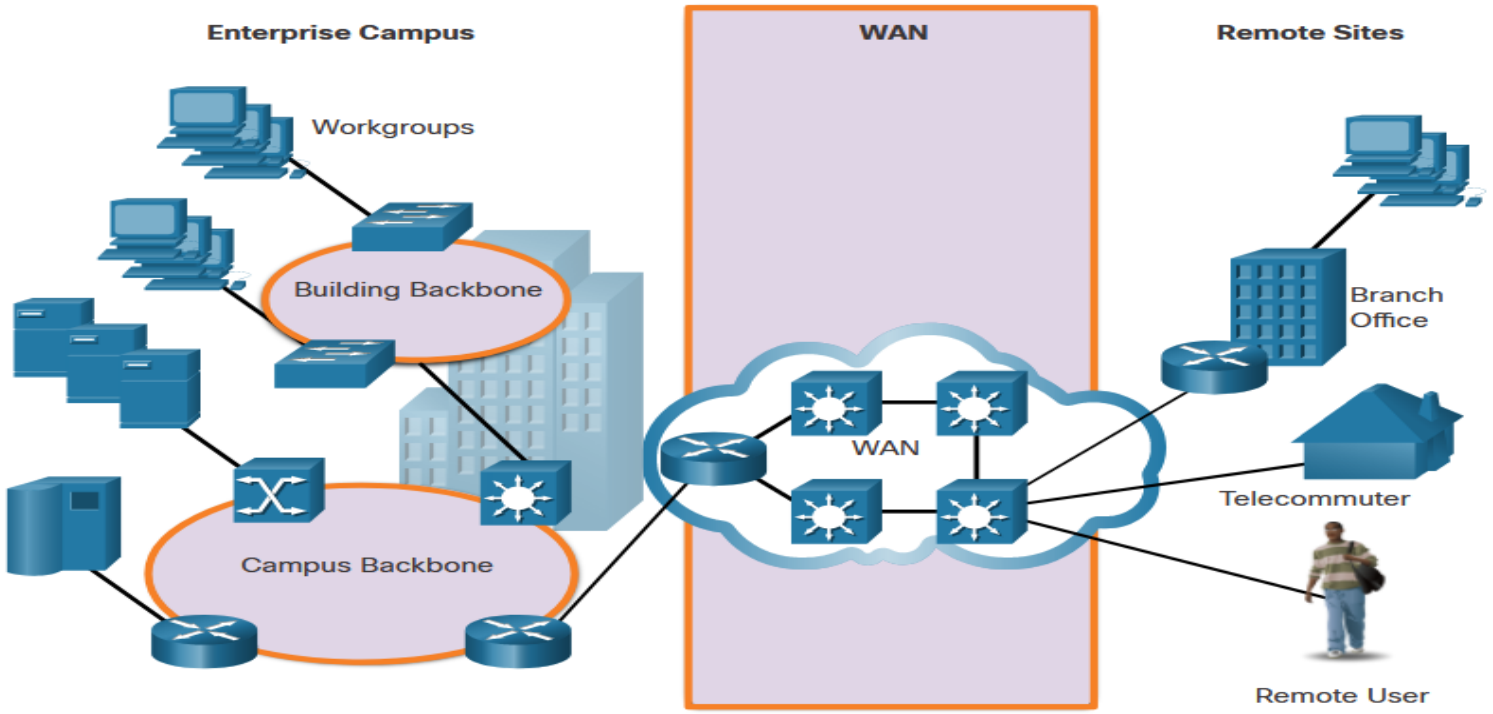
CHAPITRE 1

Étudier les réseaux étendus

1. Concepts WAN
2. Connectivite WAN traditionnelle
3. Connectivite WAN moderne
4. Options de connectivité Internet

LAN et WAN

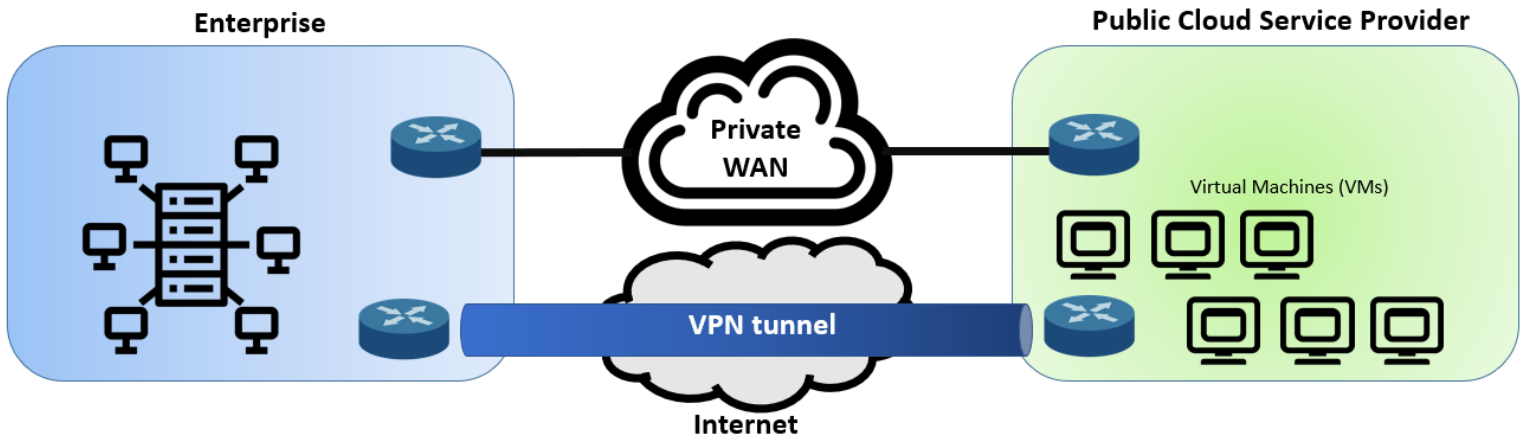
Un réseau étendu est un réseau de télécommunications qui s'étend sur une zone géographique relativement vaste et qui doit se connecter au-delà des limites du réseau local.



Les WAN privés et publics

- Un WAN privé est une connexion dédiée à un seul client.
- Les réseaux WAN privés fournissent les éléments suivants :
  - Niveau de service garanti
  - Bande passante cohérente
  - Sécurité

- Une connexion WAN publique est généralement fournie par un FAI ou un fournisseur de services de télécommunication utilisant l'internet. Dans ce cas, les niveaux de service et la bande passante peuvent varier et les connexions partagées ne garantissent pas la sécurité.



Topologies WAN

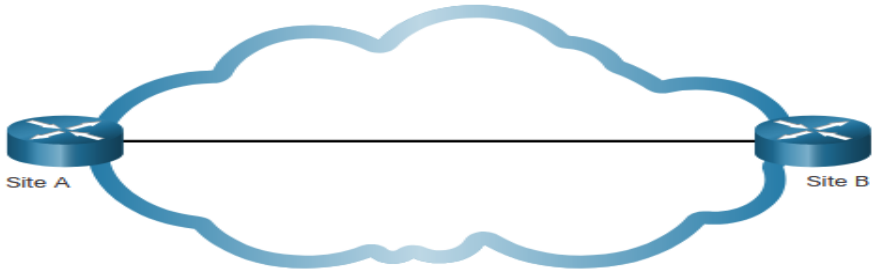
Les WAN sont implémentés à l'aide des conceptions de topologie logiques suivantes:

- **Topologie point à point**
- **Topologie en étoile**
- **Topologie à double résidence**
- **Topologie à maillage global**
- **Topologie partiellement maillée**

Remarque : Les grands réseaux déploient généralement une combinaison de ces topologies.

Topologie point à point

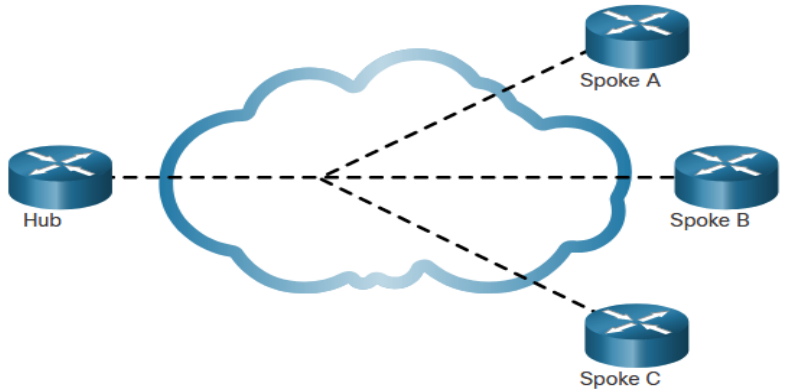
- Utilise un circuit point à point pour relier deux terminaux.



.

Topologie en étoile

- Permet de partager une interface unique sur le routeur du concentrateur avec tous les circuits en étoile.



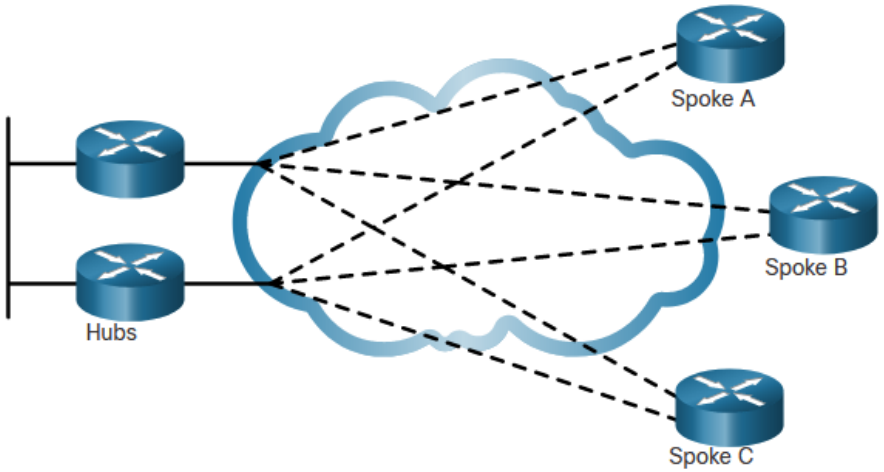
- **Remarque:** Le routeur concentrateur représente un point de défaillance unique. Si elle échoue, la communication entre les rayons échoue également.

PARTIE 5

Topologies WAN

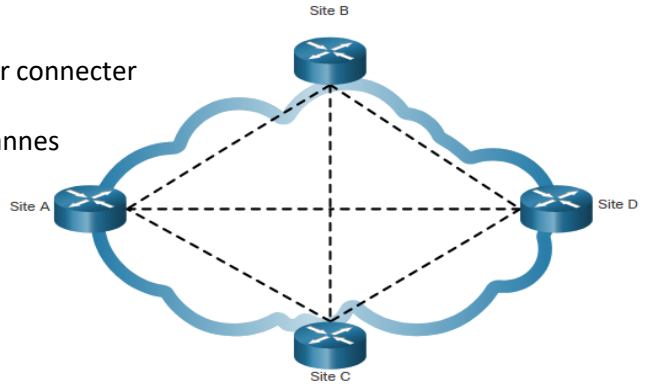
Topologie à double résidence

- Elle offre une meilleure redondance du réseau, un équilibrage des charges, un calcul et un traitement distribués, et la possibilité de mettre en place des connexions de fournisseurs de services de secours.



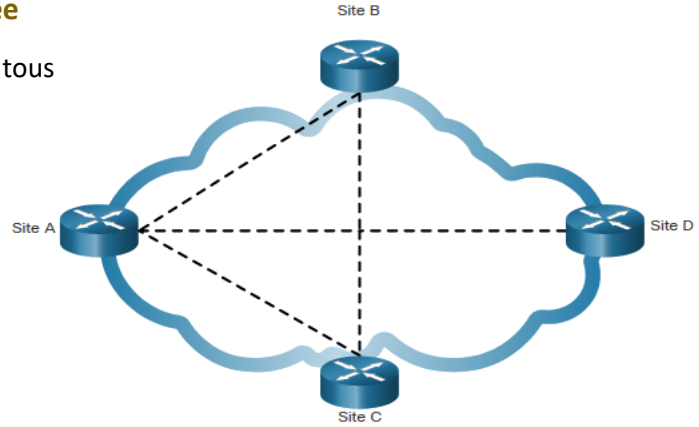
Topologie à maillage global

- Utilise plusieurs circuits virtuels pour connecter tous les sites
- La topologie la plus tolérante aux pannes



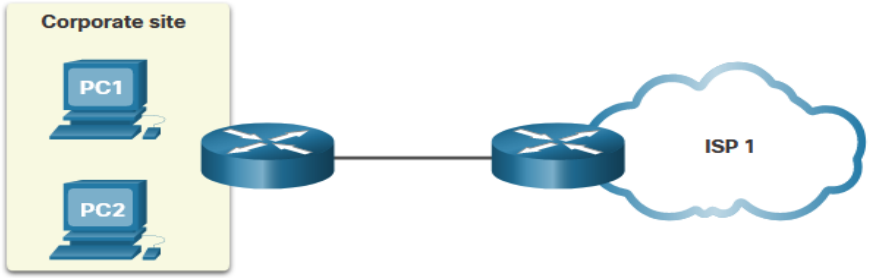
Topologie partiellement maillée

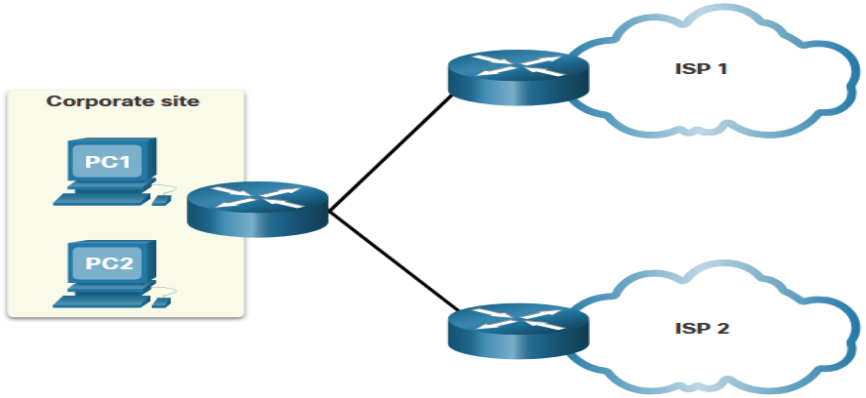
Connecte de nombreux sites mais pas tous



Connexions de transporteur

Le fournisseur de services peut ou non être le transporteur réel. Un transporteur possède et entretient la connexion physique et l'équipement entre le fournisseur et le client. En règle générale, une organisation choisit une connexion WAN à une seule ou à deux entreprises.

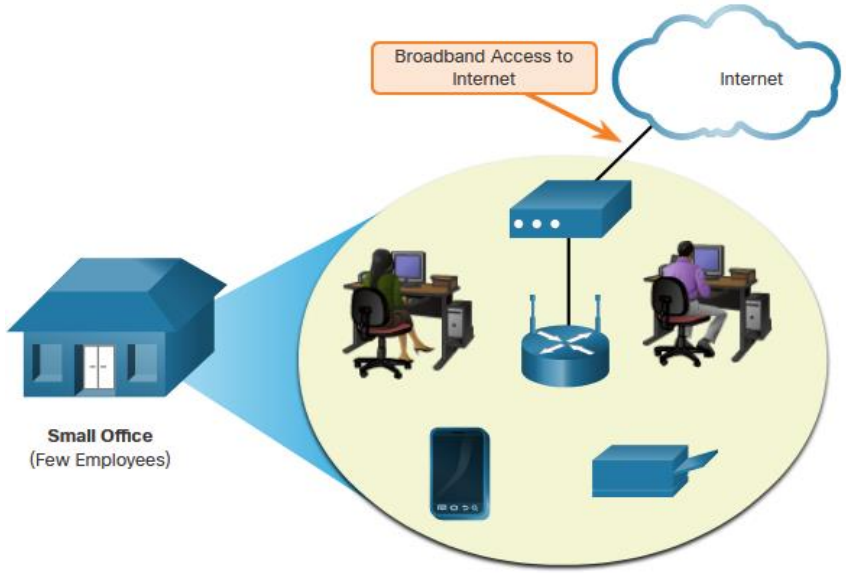




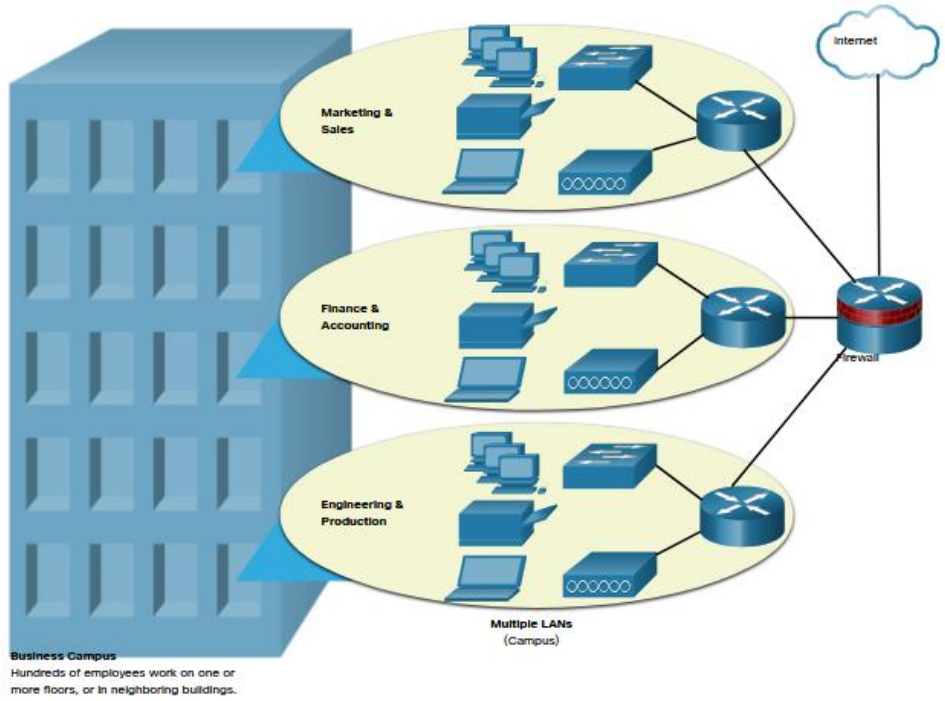
Évolution des réseaux

Le réseau doit répondre aux besoins de fonctionnement quotidien de l'entreprise, et il doit aussi être en mesure de s'adapter et de suivre l'évolution de l'entreprise.

- **Petit réseau domestique**



- **Réseau local**

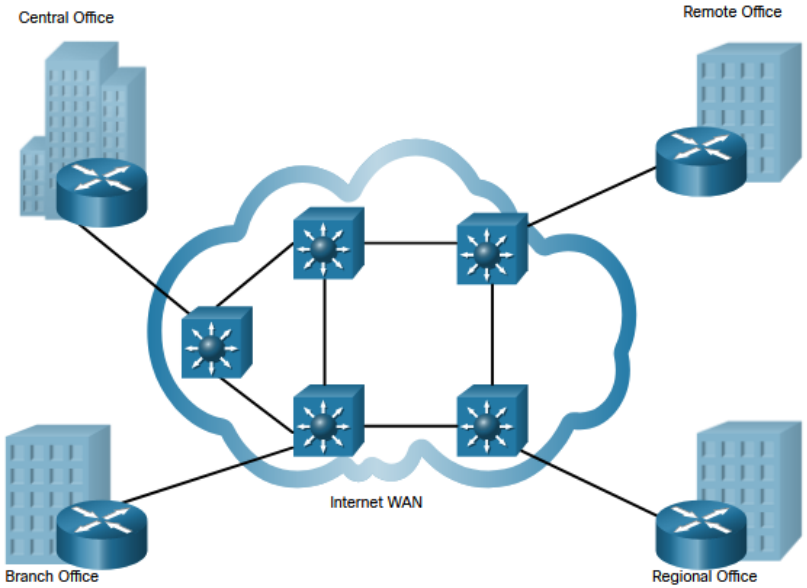


PARTIE 6

PARTIE 6

Évolution des réseaux

- **Réseau de filiale**



- **Réseau distribué**

WAN dans le modèle OSI

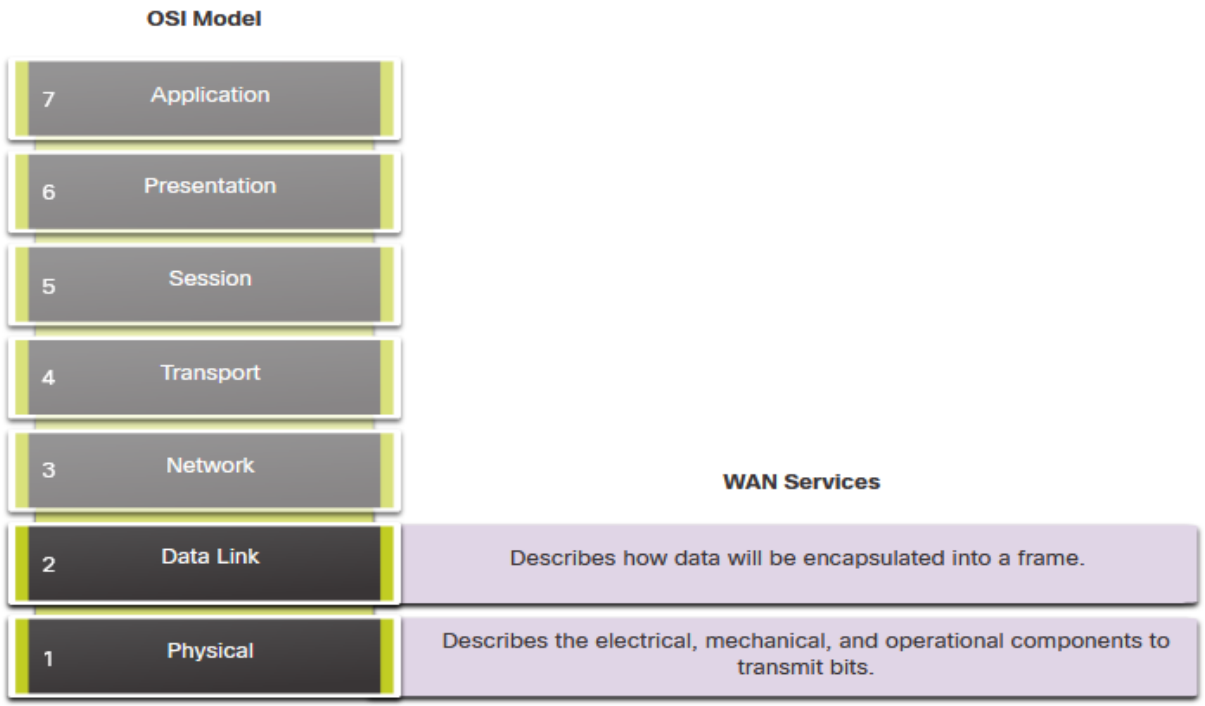
La plupart des normes WAN se concentrent sur la couche physique et la couche de liaison de données.

Protocoles de couche 1

- Synchronous Digital Hierarchy (SDH)
- Synchronous Optical Networking (SONET)
- Multiplexage en longueur d'onde dense (DWDM)

Protocoles de couche 2

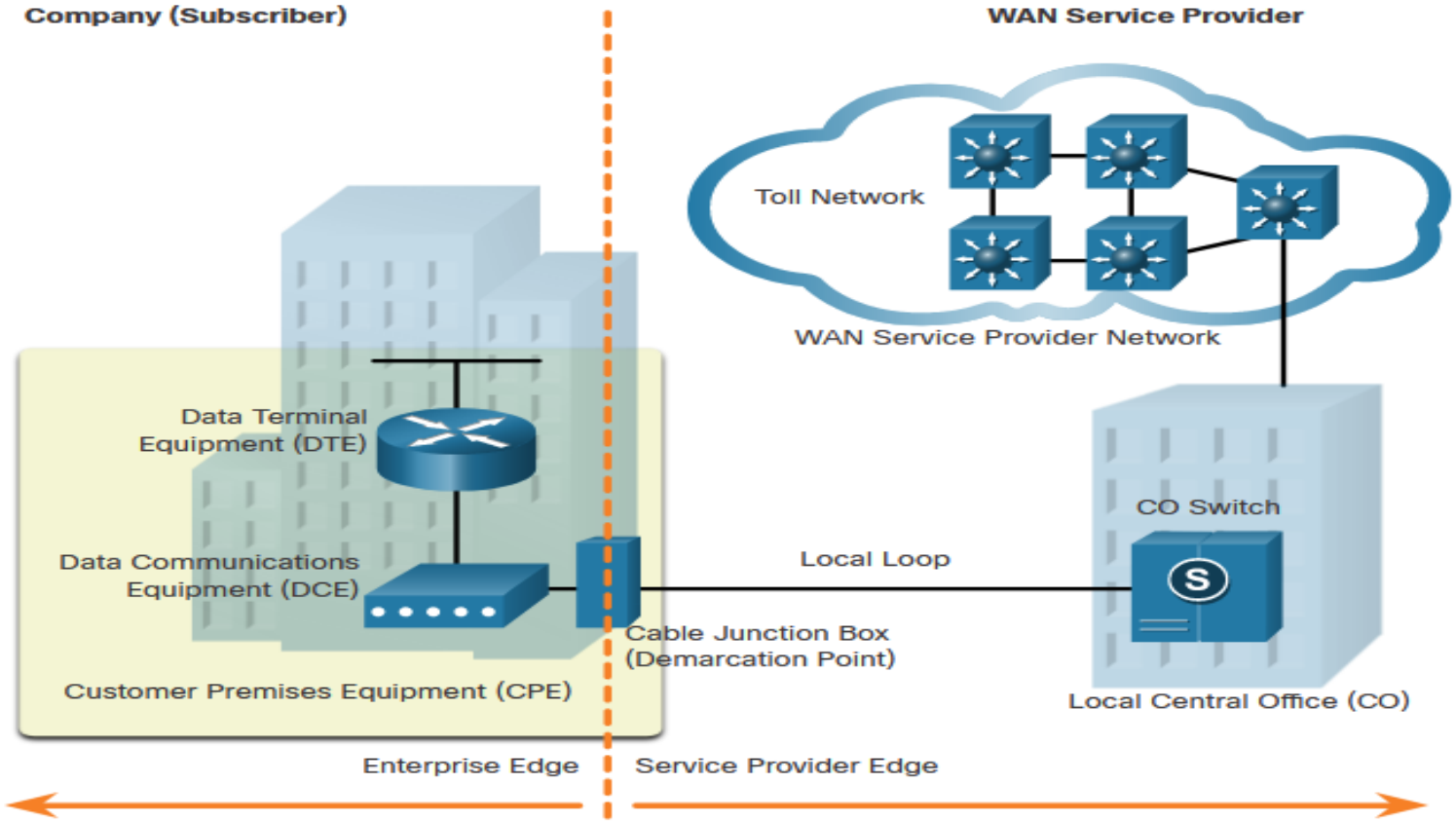
- Large bande (c.-à-d. DSL et câble)
- Sans-fil
- WAN Ethernet (Metro Ethernet)
- Commutation multiprotocole par étiquette (MPLS)
- PPP (Point-to-Point Protocol)
- HDLC (High Level Data Link Control)
- Relais de trame (Frame relay)
- Mode de transfert asynchrone (ATM)



PARTIE 6

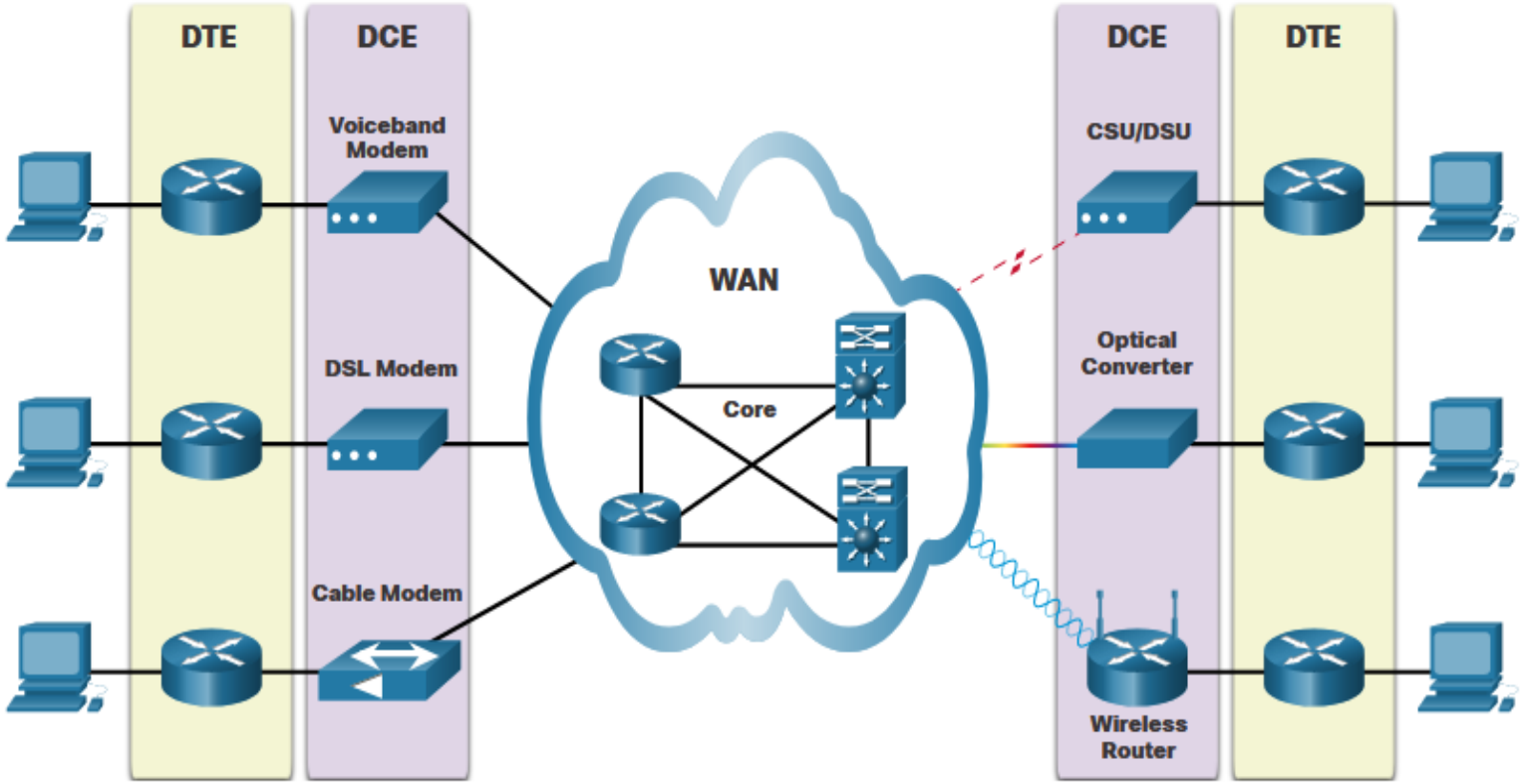
Terminologie WAN courante

Il y a des termes spécifiques utilisés pour décrire les connexions RE entre l'abonné (c.-à-d. l'entreprise/le client) et le fournisseur de services RE.



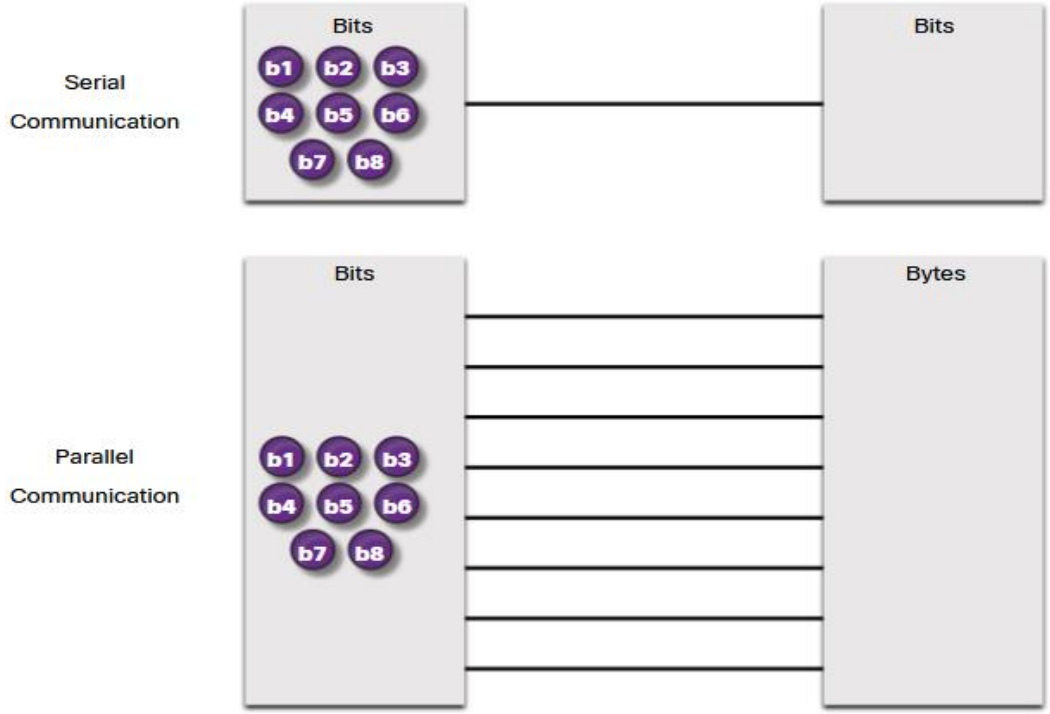
Périphériques WAN

Il existe de nombreux types d'appareils spécifiques aux environnements WAN :



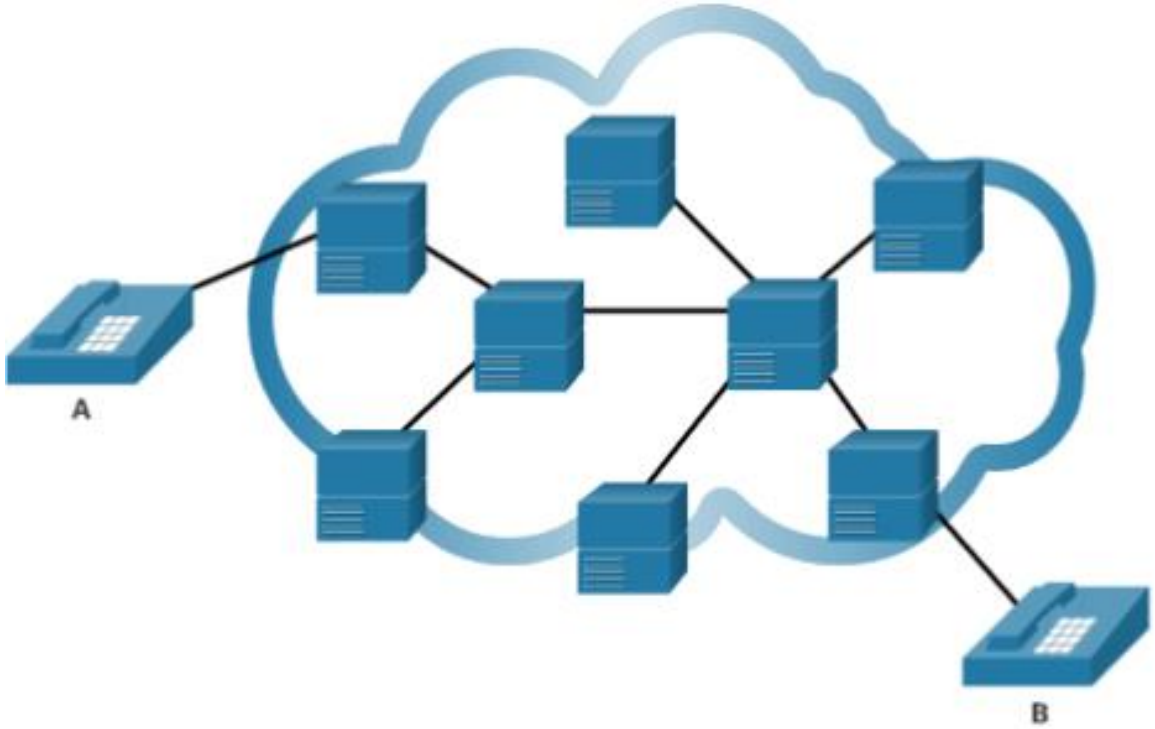
Communication série / Parallele

- Presque toutes les communications réseau se font à l'aide d'une distribution de communication série.
- À mesure que la longueur du câble augmente, la synchronisation entre plusieurs canaux devient plus sensible à la distance. Pour cette raison, la communication parallèle est limitée à de très courtes distances



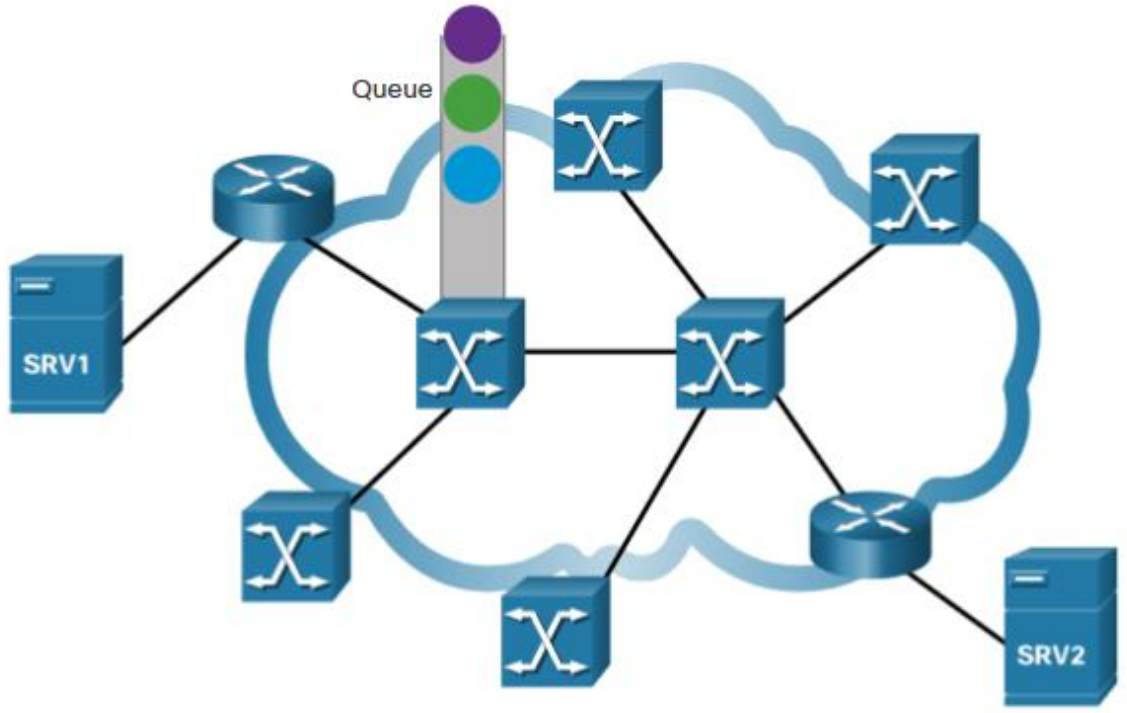
Communication commutée par circuits

Un réseau à commutation de circuits établit un circuit (ou canal) dédié entre les points d'extrémité avant que les utilisateurs puissent communiquer.



Communication commutée par paquets

La communication réseau est le plus souvent implémentée à l'aide de la communication commutée par paquets.



SDH, SONET et DWDM

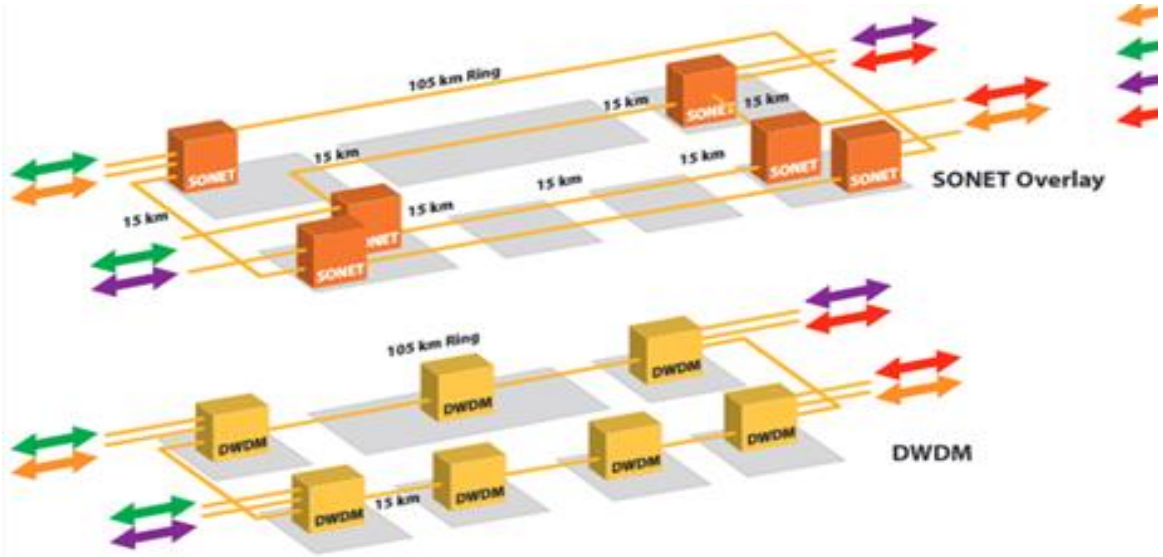
Les réseaux de fournisseurs de services utilisent des infrastructures à fibre optique pour transporter les données des utilisateurs entre les destinations. Le câble à fibre optique est de loin supérieur au câble en cuivre pour les transmissions à longue distance en raison de son atténuation et des interférences beaucoup plus faibles.

Deux normes OSI de fibre optique de couche 1 sont disponibles pour les fournisseurs de services:

- **SDH** - Synchronous Digital Hierarchy (SDH) est une norme mondiale pour le transport de données sur un câble à fibre optique.
- **SONET** - Synchronous Optical Networking (SONET) est la norme nord-américaine qui fournit les mêmes services que SDH.

SDH/SONET définissent comment transférer un trafic multiple de données, de voix et de vidéo sur fibre optique sans laser ou LED sur de grandes distances.

Dense Wavelength Division Multiplexing (DWDM) est une technologie plus récente qui augmente la capacité de charge des données de SDH et SONET en envoyant simultanément plusieurs flux de données (multiplexage) en utilisant différentes longueurs d'onde de lumière.



PARTIE 6

CHAPITRE 1

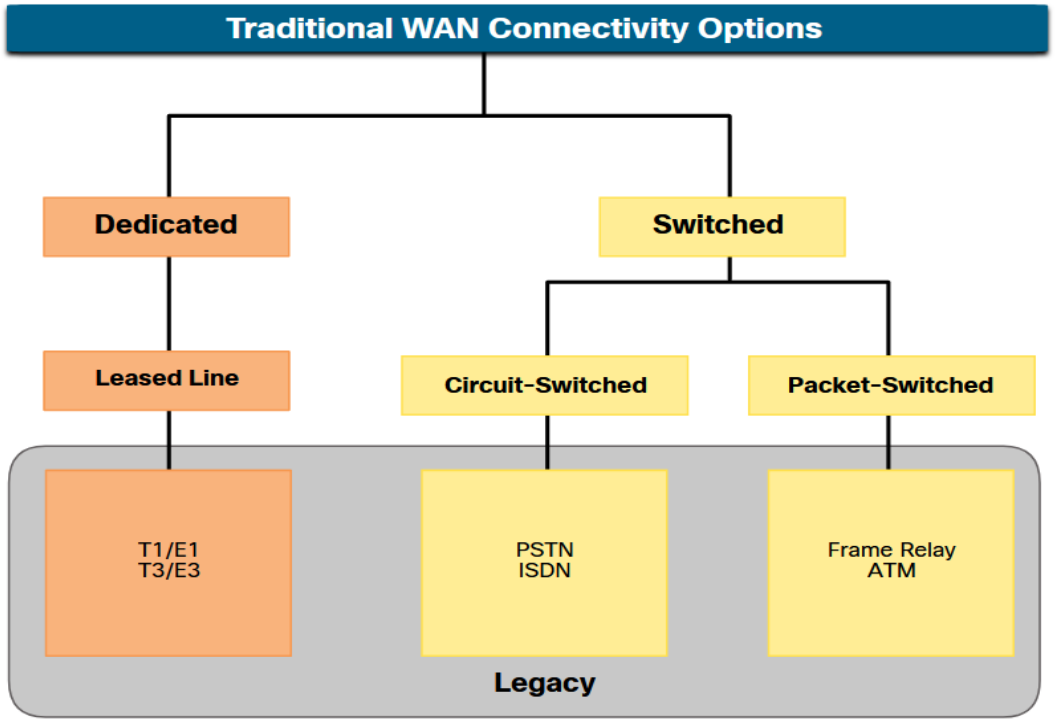
Étudier les réseaux étendus

1. Concepts WAN
2. Connectivite WAN traditionnelle
3. Connectivite WAN moderne
4. Options de connectivité Internet

Options de connectivité WAN traditionnelles

Pour comprendre les WAN d'aujourd'hui, il est utile de savoir où ils ont commencé.

- Lorsque les réseaux locaux sont apparus dans les années 1980, les organisations ont commencé à constater la nécessité de s'interconnecter avec d'autres endroits.
- Pour ce faire, ils avaient besoin de leurs réseaux pour se connecter à la boucle locale d'un fournisseur de services.
- Cela a été réalisé en utilisant des lignes spécialisées ou en utilisant des services commutés d'un fournisseur de services.



Ligne louée

Le terme ligne louée fait référence au fait que l'organisation paie tous les mois un certain montant à un fournisseur de services pour utiliser la ligne.

- Les lignes louées sont disponibles dans différentes capacités fixes et leur prix est généralement basé sur la largeur de bande requise et la distance entre les deux points connectés.
- Deux systèmes sont utilisés pour définir la capacité numérique d'une liaison série média cuivre:
  - **T-carrier** - Utilisé en Amérique du Nord, T-carrier fournit des liaisons T1 prenant en charge la bande passante jusqu'à 1,544 Mbps et des liaisons T3 prenant en charge la bande passante jusqu'à 43,7 Mbps.
  - **E-carrier** - Utilisé en Europe, e-carrier fournit des liaisons E1 prenant en charge la bande passante jusqu'à 2,048 Mbps et des liaisons E3 prenant en charge la bande passante jusqu'à 34,368 Mbps.

Avantages	
Simplicité	Les liaisons de communication point à point ne nécessitent que peu d'expertise pour leur installation et leur maintenance.
Qualité	Les liaisons de communication point à point offrent habituellement une grande qualité de service, si la bande passante est adaptée.
Disponibilité	Une disponibilité constante est essentielle pour certaines applications, telles que commerce électronique. Les liaisons de communication point à point offrent une capacité permanente dédiée, nécessaire pour la voix ou la vidéo sur IP.

Inconvénients	
Coût	Les liaisons point à point sont généralement le type d'accès WAN le plus coûteux. Le coût des liaisons louées peut être important lorsqu'elles servent à connecter plusieurs sites répartis sur des grandes distances.
Flexibilité limitée	Le trafic WAN est souvent variable et les lignes louées possèdent une capacité fixe, de telle sorte que la bande passante de la ligne correspond rarement de manière exacte à ce qui est nécessaire.

PARTIE 6

Les connexions à commutation de circuits

Les connexions à commutation de circuits sont fournies par les entreprises de réseau téléphonique de service public (PSTN). La boucle locale reliant le CPE au CO est un support cuivre.

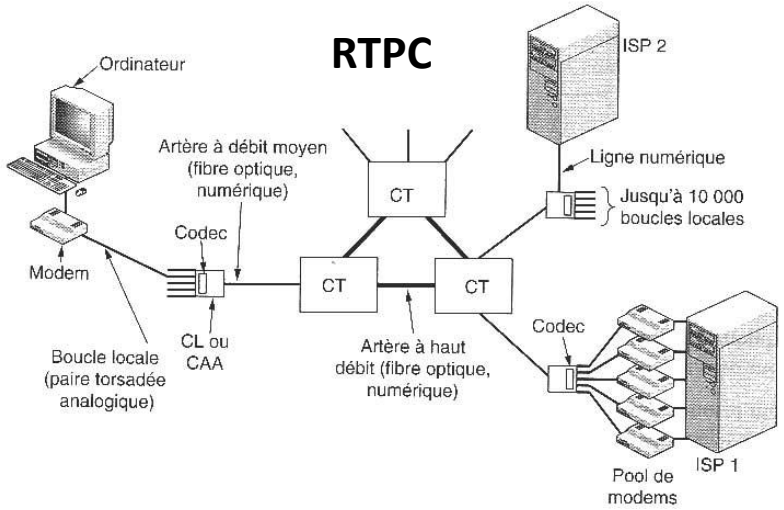
Il existe deux options traditionnelles de commutation de circuits :

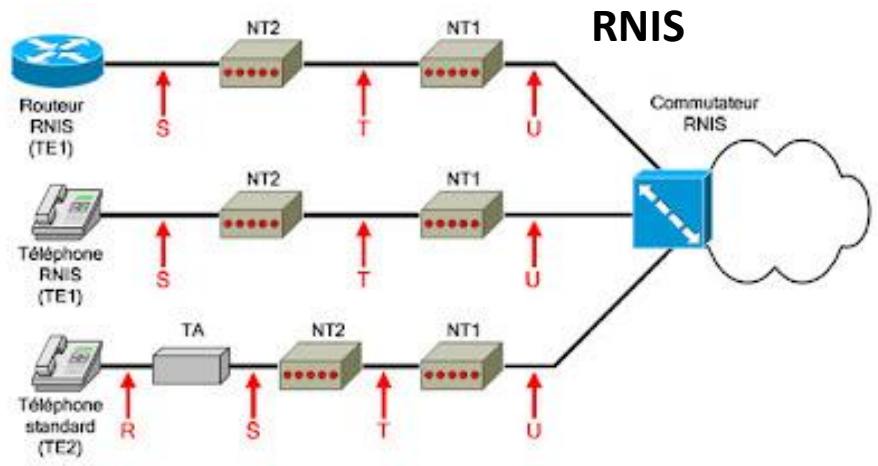
Réseau téléphonique public commuté (RTPC)

- L'accès WAN à distance utilise le RTPC comme connexion WAN. Les boucles locales classiques peuvent transporter des données informatiques binaires sur le réseau téléphonique à l'aide d'un modem.
- Les caractéristiques physiques de la boucle locale et sa connexion au réseau téléphonique public commuté (RTPC) limitent le débit du signal à moins de 56 kbit/s.

RNIS (Réseau Numérique à Intégration de Services)

- Le ISDN est une technologie de commutation de circuit qui permet à la boucle locale du RTPC de transporter des signaux numériques. Cela a permis d'obtenir des connexions commutées de plus grande capacité que l'accès par ligne commutée. ISDN fournit des débits de données de 45 Kbit/s à 2,048 Mbit/s.





PARTIE 6

Les connexions à commutation de paquet

La commutation de paquets fractionne le trafic en paquets qui sont acheminés sur un réseau partagé. Il permet à plusieurs paires de nœuds de communiquer sur le même canal.

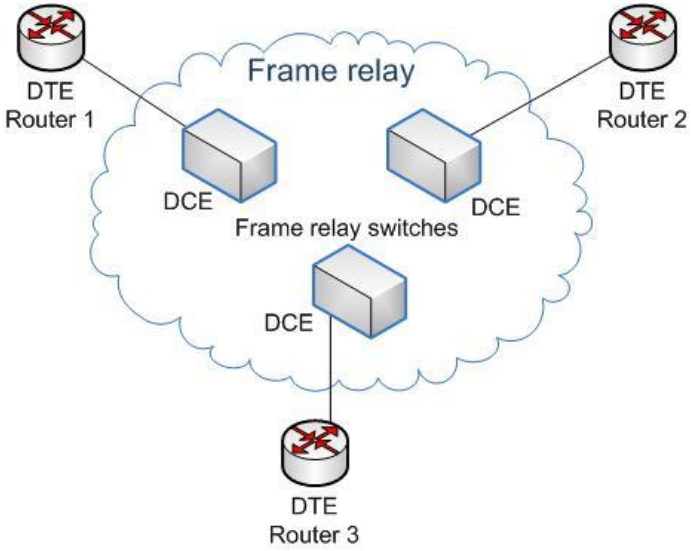
Il existe deux options traditionnelles (anciennes) de commutation de paquet:

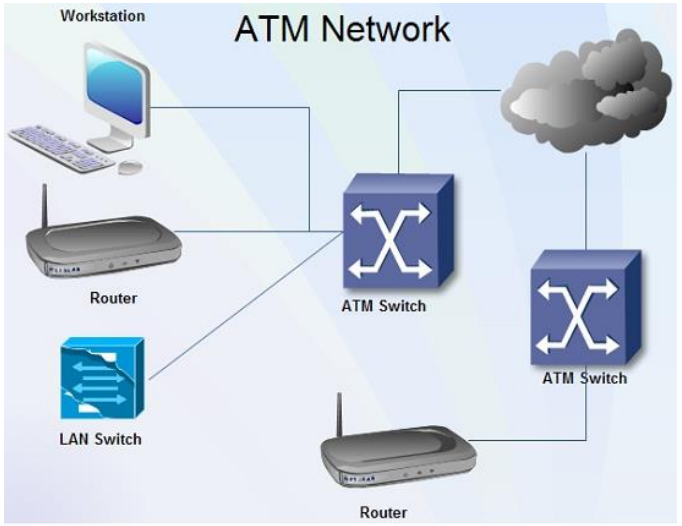
Relais de Trame (Frame Relay)

- Frame Relay est une technologie WAN simple de couche 2 NBMA (non-broadcast multi-access) utilisée pour connecter des LAN d'entreprises entre eux.
- Frame Relay crée des circuits virtuels permanents identifiés grâce à un identifiant de connexion de liaison de données (DLCI).

mode de transfert asynchrone (ATM)

- La technologie ATM (Asynchronous Transfer Mode) peut transférer de la voix, de la vidéo et des données sur des réseaux privés et publics.
- La technologie ATM repose sur une architecture à cellules et non sur une architecture à trames. Les cellules ATM présentent toujours une longueur fixe de 53 octets.





CHAPITRE 1

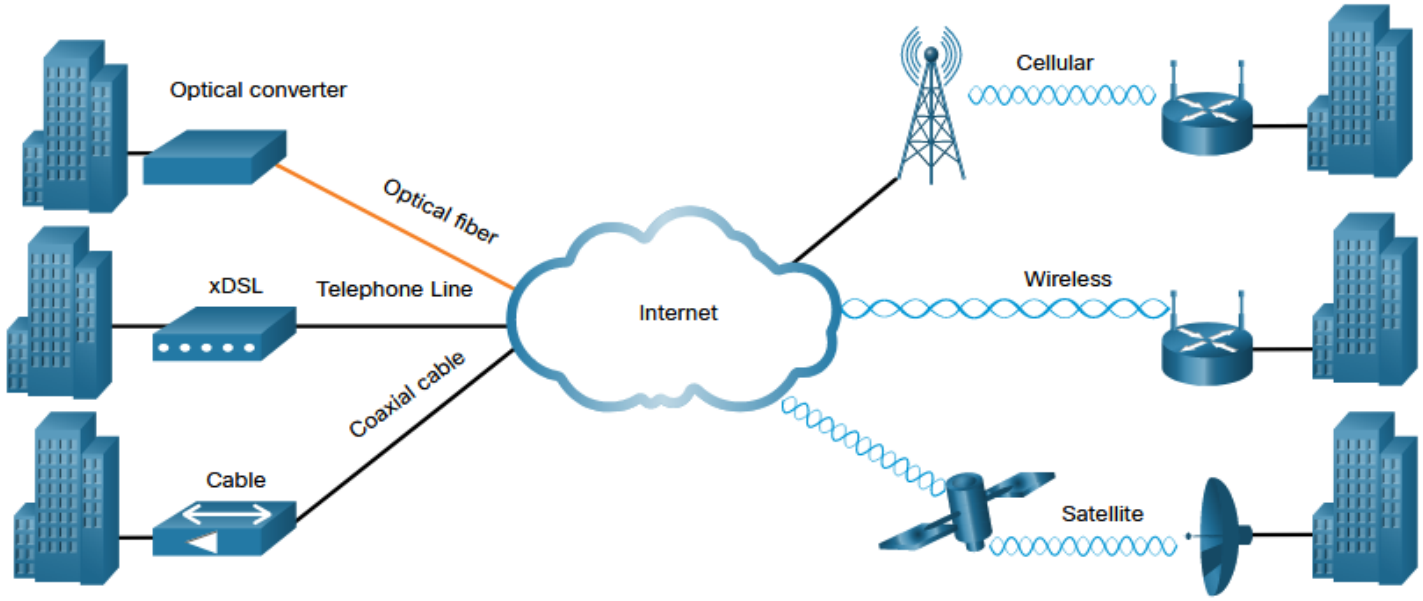
Étudier les réseaux étendus

1. Concepts WAN
2. Connectivite WAN traditionnelle
3. Connectivite WAN moderne
4. Options de connectivité Internet

WAN modernes

Les WAN modernes ont plus d'options de connectivité que les WAN traditionnels.

- Les entreprises ont désormais besoin d'options de connectivité WAN plus rapides et plus flexibles.
- Les options de connectivité WAN traditionnelles ont rapidement diminué parce qu'elles ne sont plus disponibles, trop coûteuses ou ont une bande passante limitée.



Options de connectivité WAN moderne

De nouvelles technologies ne cessent d'émerger. La figure résume les options de connectivité WAN modernes.

Haut débit dédié

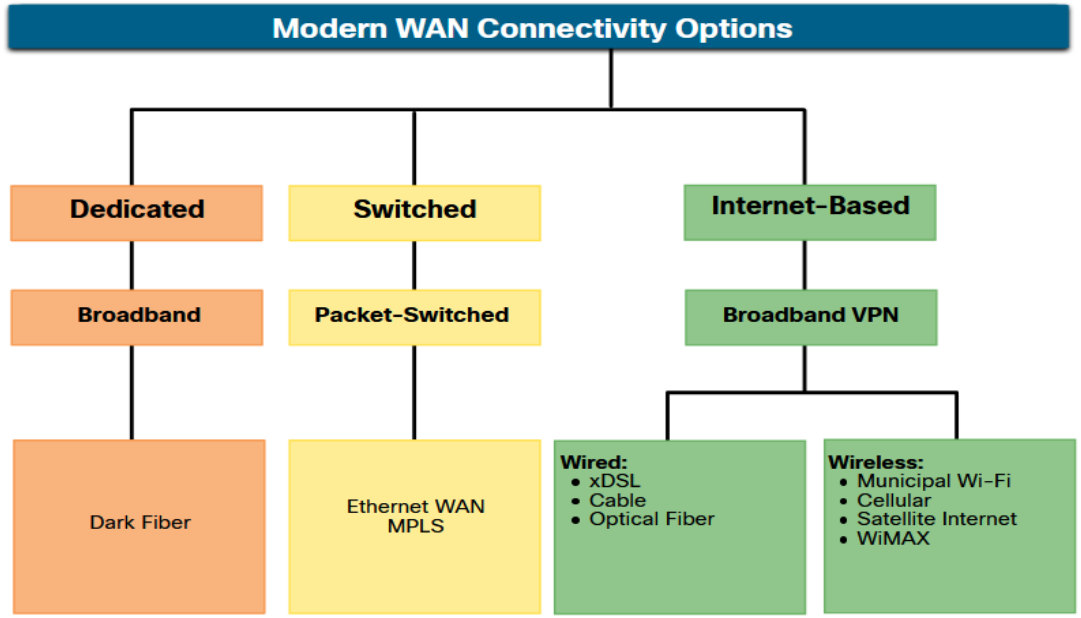
- La fibre optique peut être installée indépendamment par une organisation pour connecter des emplacements distants directement entre eux.
- La fibre noire peut être louée ou achetée auprès d'un fournisseur.

Commutation de paquets

- Ethernet métropolitain (Metro E) - Remplacement de nombreuses options WAN traditionnelles.
- MPLS - Permet aux sites de se connecter au fournisseur, quelles que soient ses technologies d'accès.

Haut débit sur l'internet

- Les entreprises utilisent désormais couramment l'infrastructure Internet mondiale pour la connectivité WAN.



WAN Ethernet

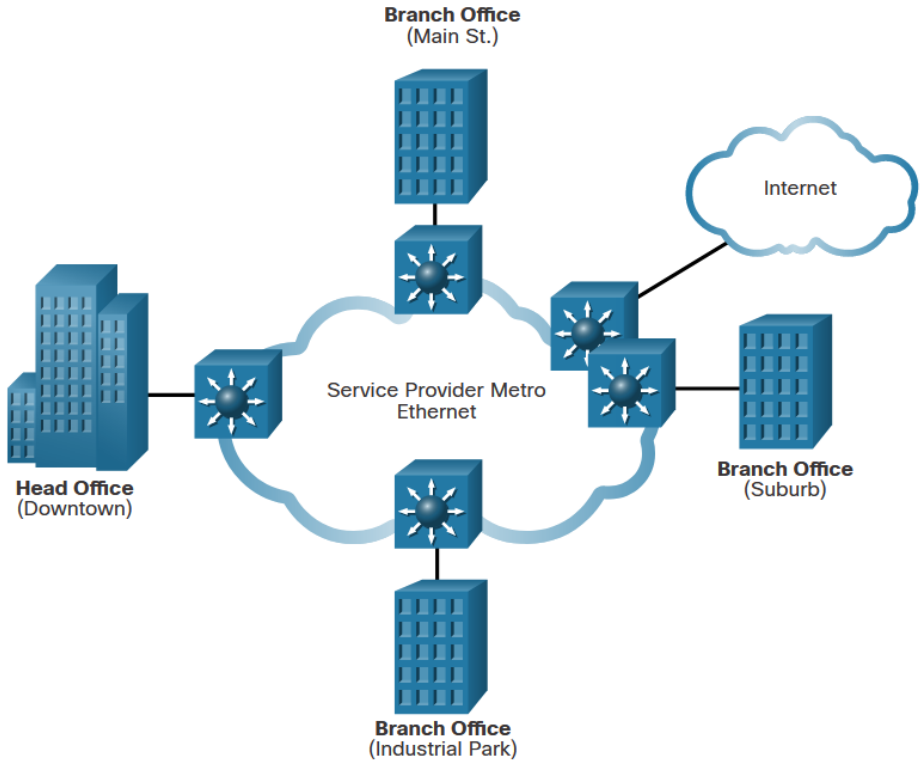
Les fournisseurs de services proposent maintenant un service WAN Ethernet basé sur un câblage à fibre optique.
Le service WAN Ethernet peut prendre de nombreux noms, notamment les suivants:

- **Ethernet métropolitain (Metro E)**
- **EoMPLS (Ethernet over MPLS)**
- **Service LAN privé virtuel (VPLS)**

Un port Ethernet WAN présente de nombreux bénéfices:

- **Frais généraux et administratifs réduits**
- **Intégration facile avec les réseaux existants**
- **Productivité de l'entreprise accrue**

Remarque: les WAN Ethernet ont gagné du terrain et ils sont de plus en plus utilisés pour remplacer les liaisons point-à-point, WAN ATM et Frame Relay.

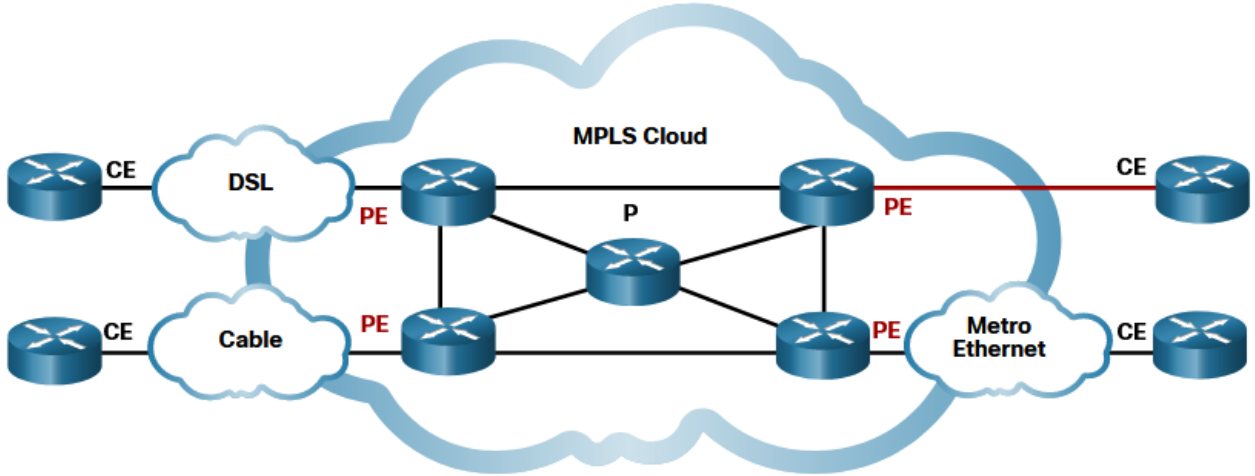


PARTIE 6

MPLS

Multiprotocol Label Switching (MPLS) est une technologie de routage WAN de fournisseur de services haute performance pour interconnecter les clients sans tenir compte de la méthode d'accès ou de la charge utile.

- MPLS prend en charge diverses méthodes d'accès client (par exemple, Ethernet, DSL, câble, relais de trame).
- MPLS peut encapsuler tous les types de protocoles, y compris le trafic IPv4 et IPv6.
- Un routeur MPLS peut être un routeur Edge client (CE), un routeur Edge fournisseur (PE) ou un routeur Fournisseur interne (P).
- Les routeurs MPLS sont des routeurs à changement d'étiquette (LSR). Ils attachent des étiquettes aux paquets qui sont ensuite utilisés par d'autres routeurs MPLS pour transférer le trafic.
- MPLS fournit également des services pour la prise en charge de la QoS, l'ingénierie du trafic, la redondance et les VPN.



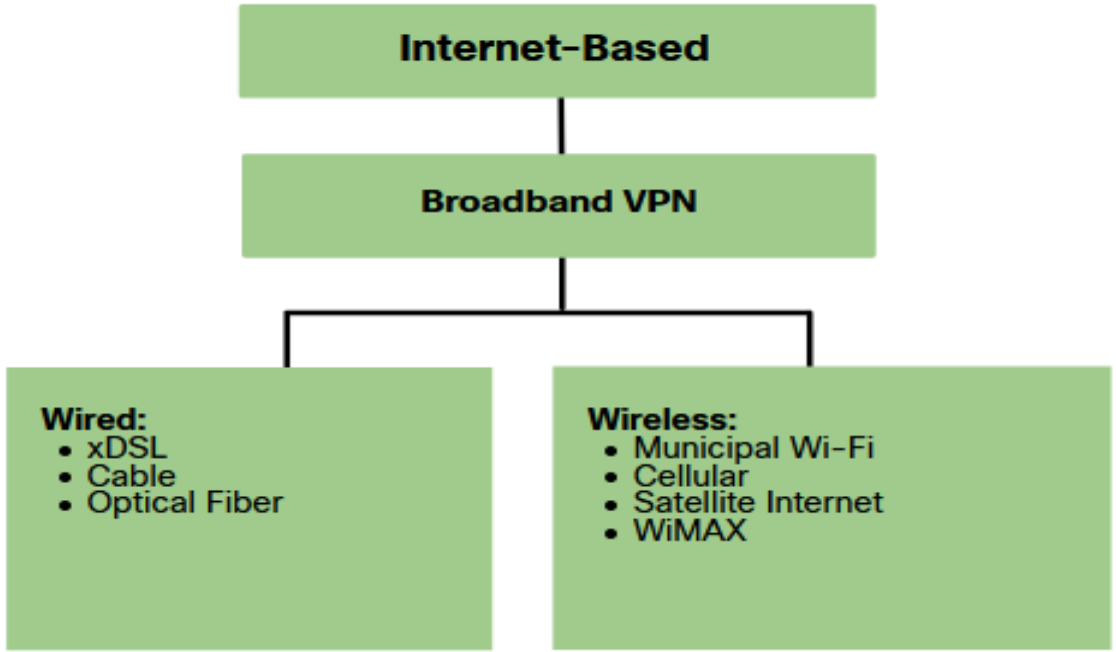
CHAPITRE 1

Étudier les réseaux étendus

1. Concepts WAN
2. Connectivite WAN traditionnelle
3. Connectivite WAN moderne
4. Options de connectivité Internet

Options de connectivité basée sur l'internet

- La connectivité à large bande basée sur l'internet est une alternative à l'utilisation d'options WAN dédiées.
- La connectivité Internet peut être divisée en options filaires et sans fil.



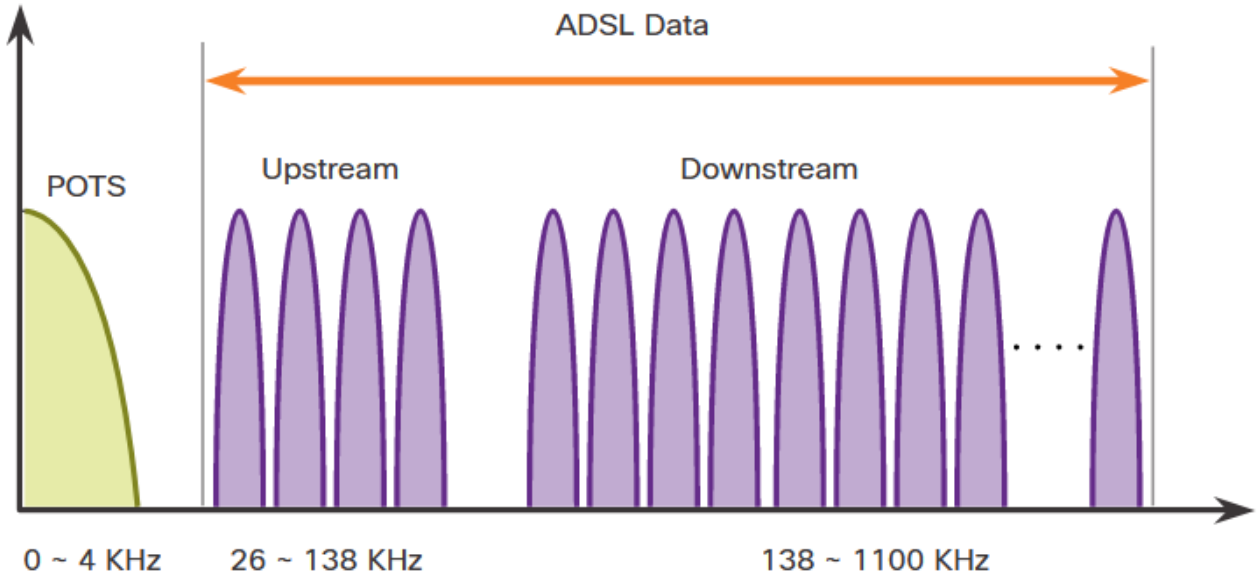
Technologie DSL

La technologie DSL est une technologie de connexion permanente qui utilise les lignes téléphoniques à paire torsadée existantes pour transmettre les données à large bande passante et offre des services IP à ses abonnés.

Les DSL sont classés comme ADSL asymétrique (ADSL) ou DSL symétrique (SDSL).

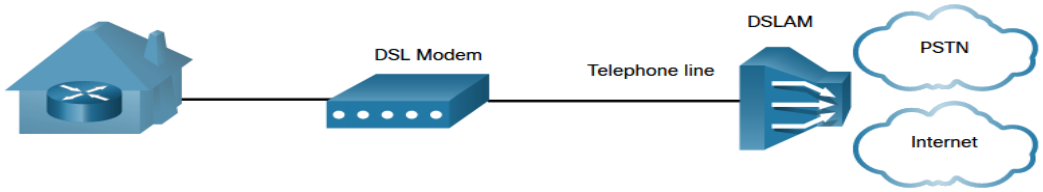
- Le service ADSL+2 offre à l'utilisateur une bande passante pour le téléchargement vers l'utilisateur supérieure à celle du transfert d'informations dans la direction opposée.
- Le service SDSL fournit la même capacité dans les deux sens.

Le service DSL taux de transfert varient en fonction de la longueur réelle de la boucle locale, ainsi que du type et de la condition du câblage.



Connexions DSL

Les opérateurs télécoms déploient des connexions DSL dans la boucle locale. La connexion est configurée entre le modem DSL et le multiplexeur d'accès DSL (DSLAM).

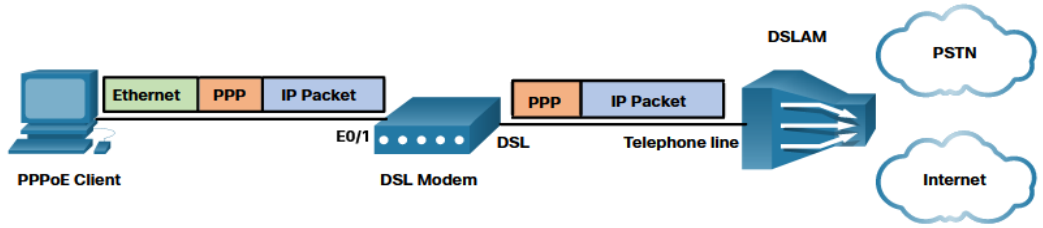


DSL et PPP

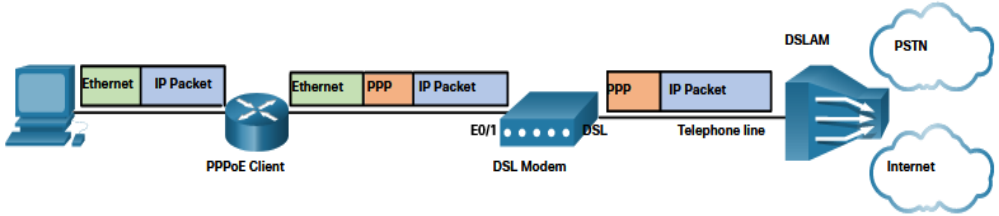
Les ISP utilisent toujours PPP comme protocole de couche 2 pour les connexions DSL à large bande.

Il existe deux façons de déployer PPP over Ethernet (PPPoE):

- **Hôte avec client PPoE**



- **Routeur PPPoE Client**

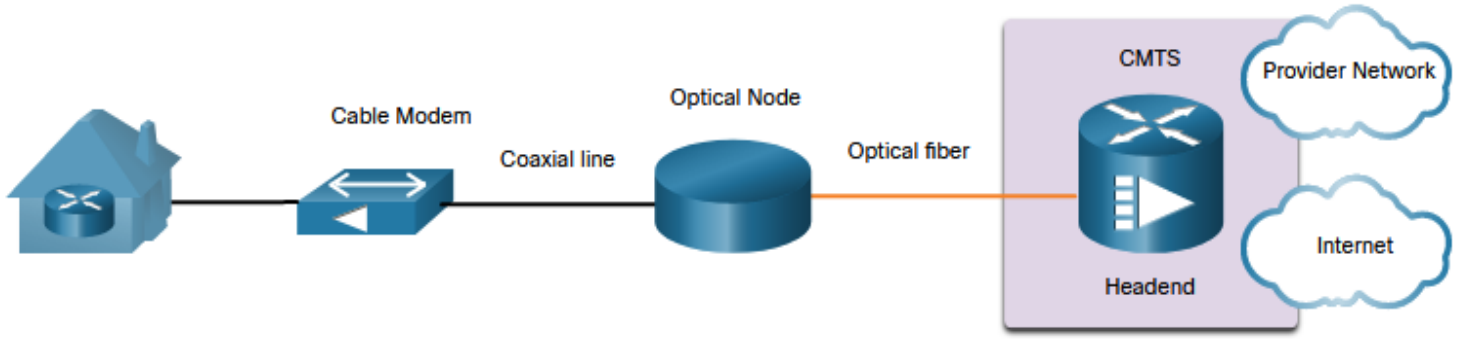


PARTIE 6

Technologie de câble

La technologie de câble est une technologie de connexion permanente à haute vitesse qui utilise un câble coaxial de l'entreprise de distribution pour fournir des services IP aux utilisateurs.

La norme internationale DOCSIS (Data over Cable Service Interface Specification) permet d'ajouter les données haut-débit à un système de câblage existant.



Remarque: Tous les abonnés locaux partagent la même bande passante. Si un grand nombre d'utilisateurs rejoignent le service, il est possible que le niveau de bande passante disponible soit inférieur au niveau prévu.

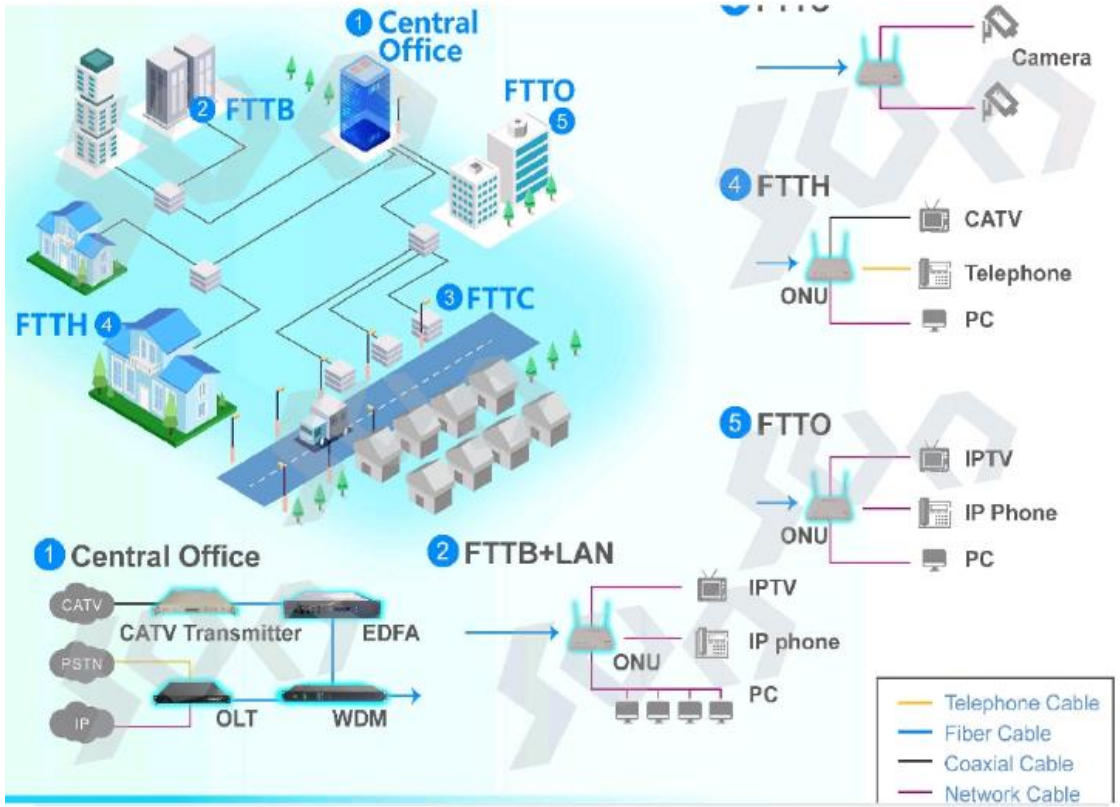
PARTIE 6

Fibre optique

De nombreuses municipalités, villes et fournisseurs installent un câble à fibre optique à l'emplacement de l'utilisateur. Ceci est communément appelé Fibre to the x (FTTx) et comprend ce qui suit:

- **FTTH (Fibre to the Home)** - Fibre atteint la limite de la résidence.
- **FTTB (Fiber to the Building)** - La fibre atteint la limite du bâtiment avec la connexion finale à l'espace de vie individuel étant faite par des moyens alternatifs.
- **FTTN (Fibre to the Node/Neighborhood)** - Le câblage optique atteint un nœud optique qui convertit les signaux optiques dans un format acceptable pour la paire torsadée ou le câble coaxial vers le local.

Remarque : FTTx peut fournir la bande passante la plus élevée de toutes les options haut débit.



Haut débit basé sur Internet sans fil

La technologie sans fil utilise le spectre radio disponible pour envoyer et recevoir des données.

- **Wi-Fi Municipal** - fournissent un accès à l'internet à haut débit gratuitement ou à un prix nettement inférieur à celui des autres services à large bande.
- **Cellulaire** -3G/4G/5G et Long-Term Evolution (LTE) sont des technologies cellulaires.
- **Internet par satellite** - Généralement utilisé par les utilisateurs ruraux ou dans les régions éloignées où le câble et l'ADSL ne sont pas disponibles.
- **WiMAX** - La technologie WiMAX est décrite dans la norme IEEE 802.16 qui fournit un service à haut-débit avec accès sans fil et offre une couverture étendue.

Technologie VPN

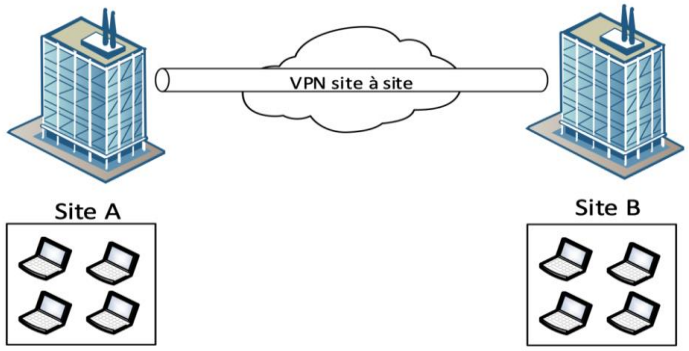
Un VPN est une connexion chiffrée entre réseaux privés sur un réseau public. Les tunnels VPN sont acheminés via l'internet à partir du réseau privé de l'entreprise vers le site distant ou l'hôte de l'employé.

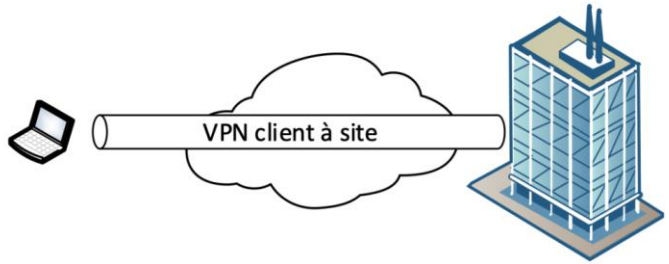
L'utilisation du VPN présente de nombreux bénéfices:

- **Réduction des coûts** - Élimine les liaisons WAN et les banques de modems dédiées coûteuses et spécialisées.
- **Sécurité** - Des protocoles avancés de cryptage et d'authentification protègent les données contre les accès non autorisés.
- **Évolutivité** - Les grandes entreprises peuvent ajouter des volumes importants de capacité sans ajouter d'infrastructure importante.
- **Compatibilité avec la technologie haut-débit** - Prise en charge par les fournisseurs d'accès haut-débit tels que la DSL et le câble DSL.

Les VPN sont généralement implémentés comme suit:

- **VPN site à site**- Les paramètres VPN sont configurés sur les routeurs. Les clients ne savent pas que leurs données sont cryptées.
- **Accès à distance**- L'utilisateur est conscient et initie une connexion d'accès à distance.

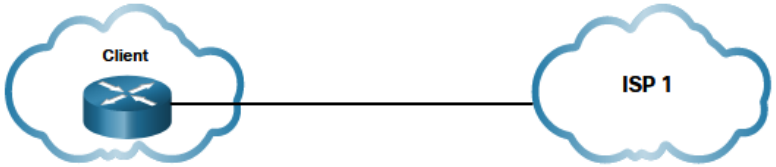




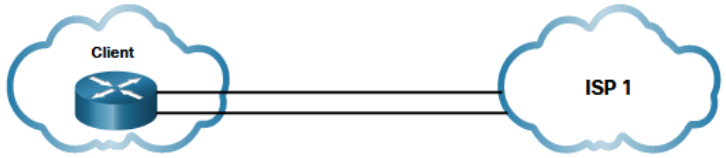
Options de connectivité de FAI

Une organisation peut se connecter à un fournisseur de services Internet de différentes manières. Le choix dépend des besoins et du budget de l'organisation.

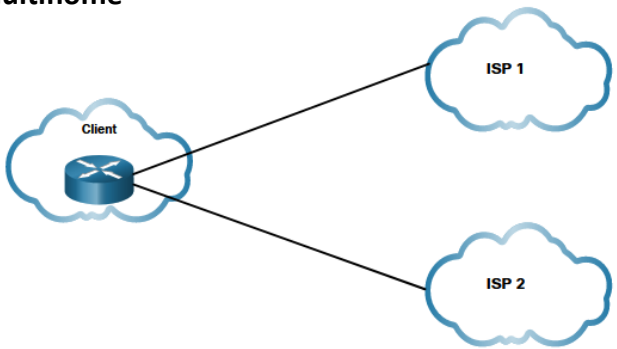
- **Single-home**



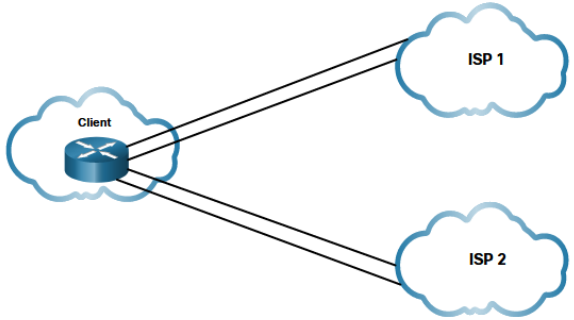
- **Double home**



- **Multihome**



- **Double-multihome**



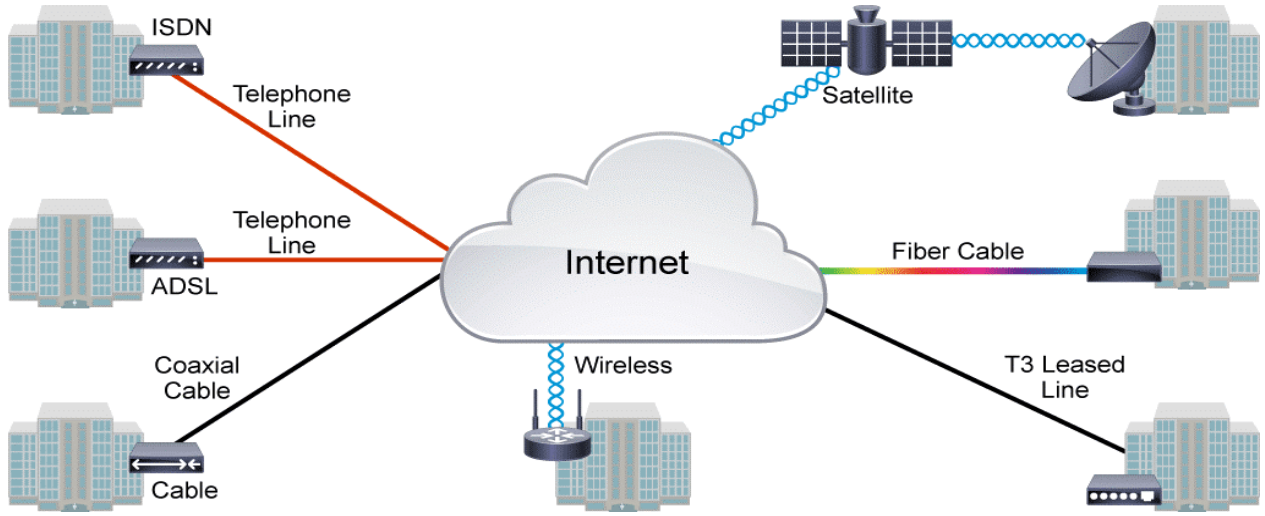
PARTIE 6

Comparaison des solutions haut débit

Chaque solution haut débit présente des avantages et des inconvénients. Si plusieurs solutions haut-débit sont disponibles, une analyse coûts/avantages doit être effectuée en vue de déterminer la meilleure solution.

Parmi les facteurs à prendre en compte, mentionnons les suivants:

- **Câble** - La bande passante est partagée par de nombreux utilisateurs. Par conséquent, les débits de données en amont sont souvent lents pendant les heures de forte utilisation dans les zones où il y a sur abonnement.
- **DSL** - Largeur de bande limitée et sensible à la distance (par rapport au bureau central du FAI). Le taux de téléchargement (Upload) est proportionnellement inférieur par rapport au taux de téléchargement (Download) .
- **Fiber-to-the-Home** - Cette option nécessite l'installation de la fibre directement à la maison.
- **Cellulaire/Mobile** - Avec cette option, la couverture est souvent un problème, même dans un petit bureau ou un bureau à domicile où la largeur de bande est relativement limitée.
- **Wi-Fi municipal** - La plupart des municipalités ne disposent pas d'un réseau Wi-Fi maillé déployé. Si elle est disponible et accessible, c'est une option viable.
- **Satellite** - Cette option est coûteuse et offre une capacité limitée par abonné. Généralement utilisé lors qu'aucune autre option n'est disponible.



CHAPITRE 2

Sécuriser l’accès aux réseaux

Ce que vous allez apprendre dans ce chapitre :

- Sécuriser l’accès aux réseaux avec les ACLs
- Configurer l’accès au réseau public avec NAT pour IPv4
- Sécuriser l’accès à distance avec la technologie VPN

3.5 heures

CHAPITRE 2

Sécuriser l’accès aux réseaux

1. Concepts de sécurité réseau
2. Les ACLs
3. NAT pour IPv4
4. Concept VPN

Attaques réseau courantes

Les réseaux sont sensibles aux types d'attaques suivants:

- **Attaques de reconnaissance**
- **Attaques par accès**
- **Attaques DoS**

Attaques de reconnaissance

Technique	Description
Exécuter une requête d'information sur une cible	L'acteur de menace recherche les premières informations sur une cible. Divers outils peuvent être utilisés, notamment la recherche Google, le site Web des organisations, le whois, etc.
Lancer un balayage ping du réseau cible	La requête d'informations révèle généralement l'adresse réseau de la cible. L'acteur de menace peut désormais lancer un balayage ping pour déterminer quelles adresses IP sont actives.
Lancer l'analyse des ports des adresses IP actives	Ceci est utilisé pour déterminer quels ports ou services sont disponibles. Exemples d'analyseurs de ports: Nmap, SuperScan, Angry IP Scanner et NetScanTools.
Exécuter des scanners de vulnérabilité	Il s'agit d'interroger les ports identifiés pour déterminer le type et la version de l'application et du système d'exploitation qui s'exécutent sur l'hôte. Des exemples d'outils incluent Nipper, Core Impact, Nessus, SAINT et Open VAS.
Exécuter des outils d'exploitation	L'acteur de menace tente maintenant de découvrir des services vulnérables qui peuvent être exploités. Des exemples d'outils d'exploitation de vulnérabilité comprennent Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit et Netsparker.

Attaques réseau courantes

- **Attaques d'accès**

Les acteurs de menace utilisent des attaques d'accès sur les périphériques réseau et les ordinateurs pour récupérer des données, y accéder ou pour augmenter les privilèges d'accès au statut d'administrateur.

- **Attaques par mot de passe**
- **Attaques d'usurpation d'identité**

Les autres attaques d'accès incluent:

- **Exploiter la confiance**
- **Redirection de port**
- **Attaques de l'homme-au-milieu**
- **Attaques par débordement de la mémoire tampon**

Techniques d'attaque IP

Techniques d'attaque IP	Description
Attaques ICMP	Les acteurs de menace utilisent des paquets d'écho (ping) ICMP (Internet Control Message Protocol) pour découvrir les sous-réseaux et les hôtes sur un réseau protégé, pour générer des attaques par inondation DoS et pour modifier les tables de routage des hôtes.
Amplification et attaques par réflexion	Les acteurs de menace tentent d'empêcher les utilisateurs légitimes d'accéder aux informations ou aux services à l'aide d'attaques DoS et DDoS.
Attaques par usurpation d'adresse	Les acteurs de menace usurpent l'adresse IP source dans un paquet IP pour effectuer une usurpation aveugle ou une usurpation non aveugle.
Attaques de l'homme-au-milieu (MITM)	Les acteurs de menace se positionnent entre une source et une destination pour surveiller, capturer et contrôler de manière transparente la communication. Ils pourraient espionner en inspectant les paquets capturés, ou modifier les paquets et les transmettre à leur destination d'origine.
Détournement de session	Les acteurs de menace accèdent au réseau physique, puis utilisent une attaque MITM pour détourner une session

Attaques ICMP

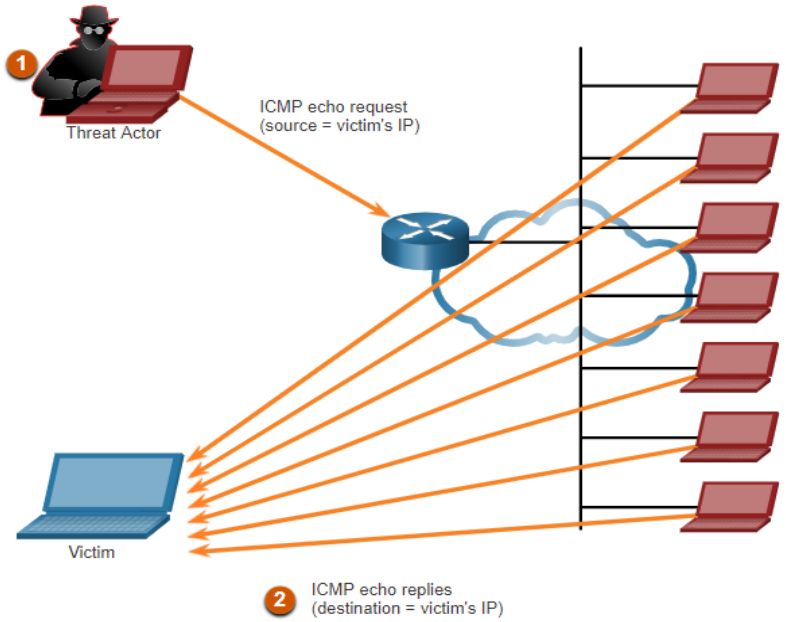
Messages ICMP utilisés par les pirates	Description
Demande d'écho ICMP et réponse d'écho	Ceci est utilisé pour effectuer une vérification de l'hôte et des attaques DoS.
ICMP inaccessible	Il est utilisé pour effectuer des attaques de reconnaissance et de balayage de réseau.
Réponse de masque ICMP	Ceci est utilisé pour mapper un réseau IP interne.
Redirection ICMP	Ceci est utilisé pour attirer un hôte cible dans l'envoi de tout le trafic via un appareil compromis et créer une attaque MITM.
Découverte du routeur ICMP	Ceci est utilisé pour injecter des entrées de route fausses dans la table de routage d'un hôte cible.

Attaques par amplification et réflexion

- Les cyberpirates utilisent souvent des techniques d'amplification et de réflexion pour créer des attaques DoS.
- L'exemple de la figure illustre une attaque Smurf utilisée pour submerger un hôte cible.

Remarque: De nouvelles formes d'attaques d'amplification et de réflexion telles que les attaques de réflexion et d'amplification basées sur DNS et les attaques d'amplification NTP (Network Time Protocol) sont désormais utilisées.

- Les acteurs de menace utilisent également des attaques d'épuisement des ressources pour planter un hôte cible ou pour consommer les ressources d'un réseau.



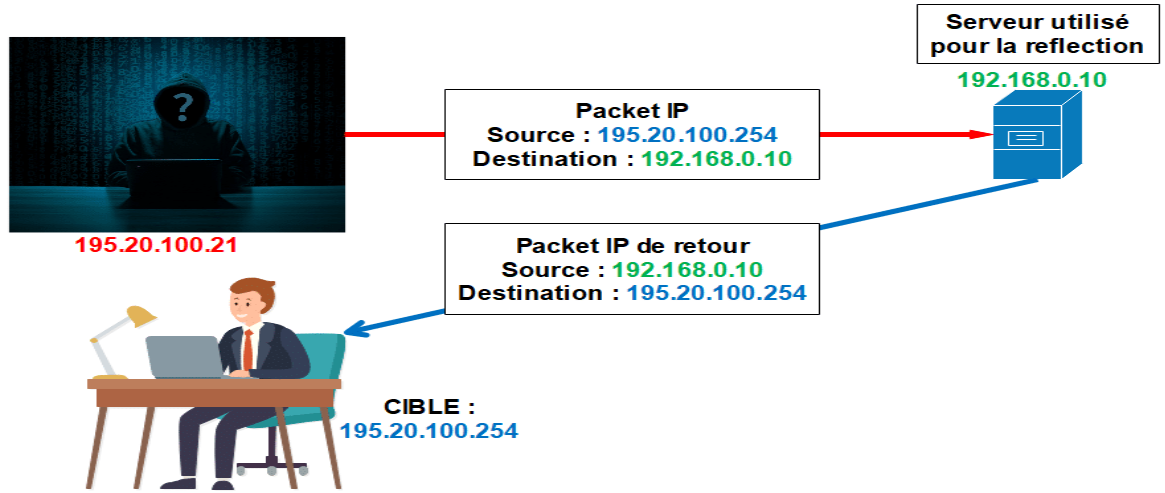
Attaques par usurpation d'adresse

Les attaques d'usurpation d'adresse IP se produisent lorsqu'un acteur de menace crée des paquets contenant de fausses informations d'adresse IP source pour masquer l'identité de l'expéditeur ou pour se faire passer pour un autre utilisateur légitime. L'usurpation d'identité est généralement intégrée à une autre attaque telle qu'une attaque de Smurf.

Les attaques d'usurpation d'identité peuvent être non aveugles ou aveugles:

- **Usurpation d'identité non aveugle** - L'acteur de menace peut voir le trafic qui est envoyé entre l'hôte et la cible. L'usurpation non aveugle détermine l'état d'un pare-feu et la prédiction du numéro de séquence. Il peut également détourner une session autorisée.
- **Usurpation aveugle** - L'acteur de menace ne peut pas voir le trafic envoyé entre l'hôte et la cible. L'usurpation aveugle est utilisée dans les attaques DoS.

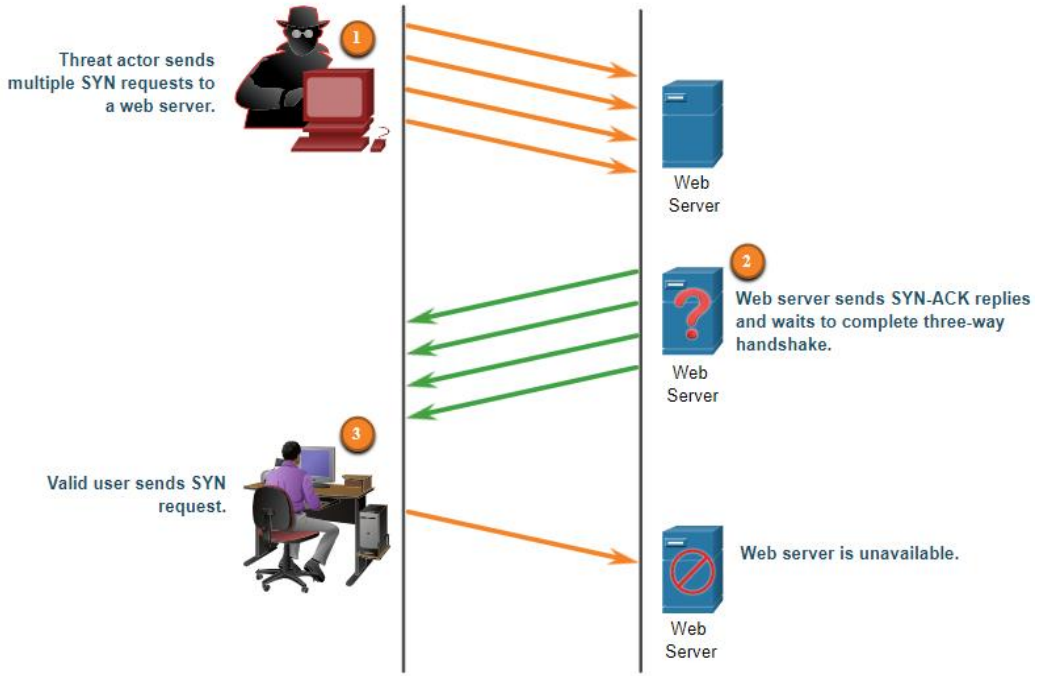
Les attaques par usurpation d'adresse MAC sont utilisées lorsque les cyberpirates ont accès au réseau interne. Les acteurs de menace modifient l'adresse MAC de leur hôte pour correspondre à une autre adresse MAC connue d'un hôte cible.



Attaques TCP

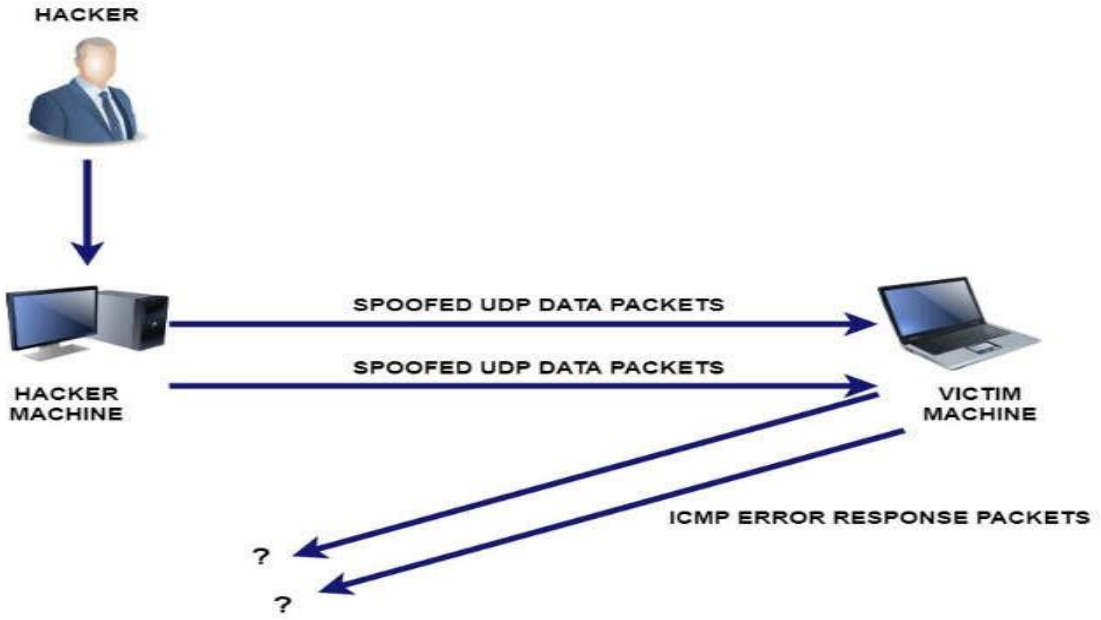
TCP SYN Attaque par inondation

1. L'acteur de menace envoie plusieurs demandes SYN à un serveur Web.
2. Le serveur Web répond avec des SYN-ACK pour chaque demande SYN et attend de terminer la négociation à poignée de main à trois voies. L'acteur de menace ne répond pas aux SYN-ACK.
3. Un utilisateur valide ne peut pas accéder au serveur Web car le serveur Web possède trop de connexions TCP semi-ouvertes.



Attaques UDP

- UDP n'est protégé par aucun cryptage. Vous pouvez ajouter un chiffrement à UDP, mais il n'est pas disponible par défaut. L'absence de cryptage signifie que n'importe qui peut voir le trafic, le modifier et l'envoyer à sa destination.
- **UDP Flood Attacks:** L'acteur de menace utilise un outil comme UDP Unicorn ou Low Orbit Ion Cannon. Ces outils envoient un flot de paquets UDP, souvent à partir d'un hôte usurpé, vers un serveur du sous-réseau. Le programme balaye tous les ports connus afin de trouver les ports fermés. Cela entraînera le serveur de répondre avec un message inaccessible du port ICMP. Étant donné qu'il existe de nombreux ports fermés sur le serveur, cela crée beaucoup de trafic sur le segment, qui utilise la majeure partie de la bande passante. Le résultat est très similaire à une attaque DoS.

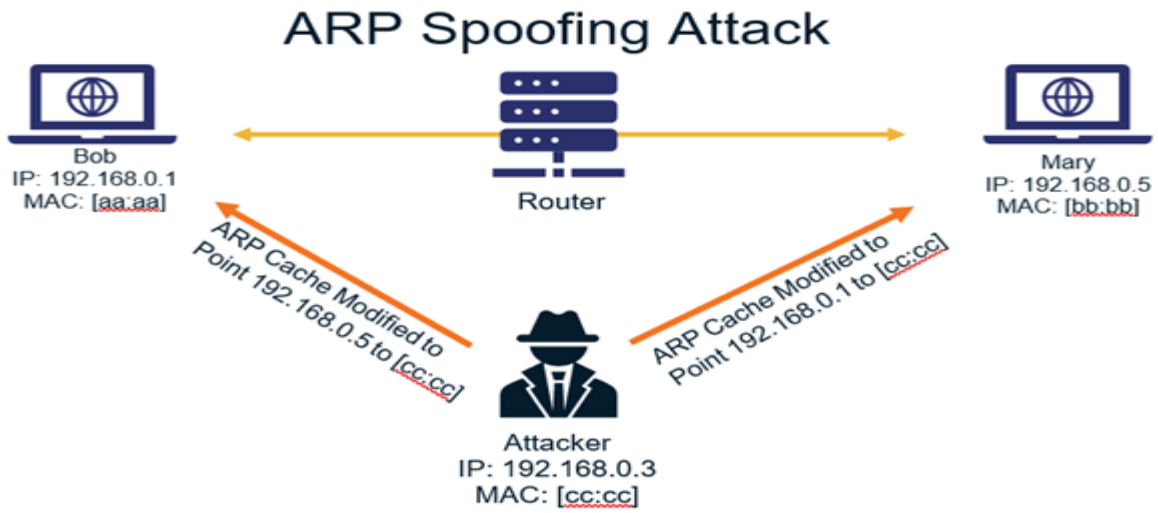


Attaque ARP

Empoisonnement du cache ARP

L'empoisonnement du cache ARP peut être utilisé pour lancer diverses attaques de l'homme-au-milieu.

1. PC-A requiert l'adresse MAC de sa passerelle par défaut (R1); par conséquent, il envoie une demande ARP pour l'adresse MAC de 192.168.10.1.
2. R1 met à jour son cache ARP avec les adresses IP et MAC de PC-A. R1 envoie une réponse ARP à PC-A, qui met ensuite à jour son cache ARP avec les adresses IP et MAC de R1.
3. L'acteur de menace envoie deux réponses ARP usurpées gratuitement en utilisant sa propre adresse MAC pour les adresses IP de destination indiquées. PC-A met à jour son cache ARP avec sa passerelle par défaut qui pointe maintenant vers l'adresse MAC hôte de l'acteur de menace. R1 met également à jour son cache ARP avec l'adresse IP de PC-A pointant vers l'adresse MAC de l'acteur de menace.



Attaques DNS

Les attaques DNS sont les suivantes:

Attaques du résolveur ouvert DNS: un résolveur ouvert DNS répond aux requêtes des clients en dehors de son domaine administratif. Les résolveurs ouverts DNS sont vulnérables à plusieurs activités malveillantes :

- Attaques d'empoisonnement du cache DNS
- Attaques par amplification et réflexion du DNS
- Attaques d'utilisation des ressources DNS

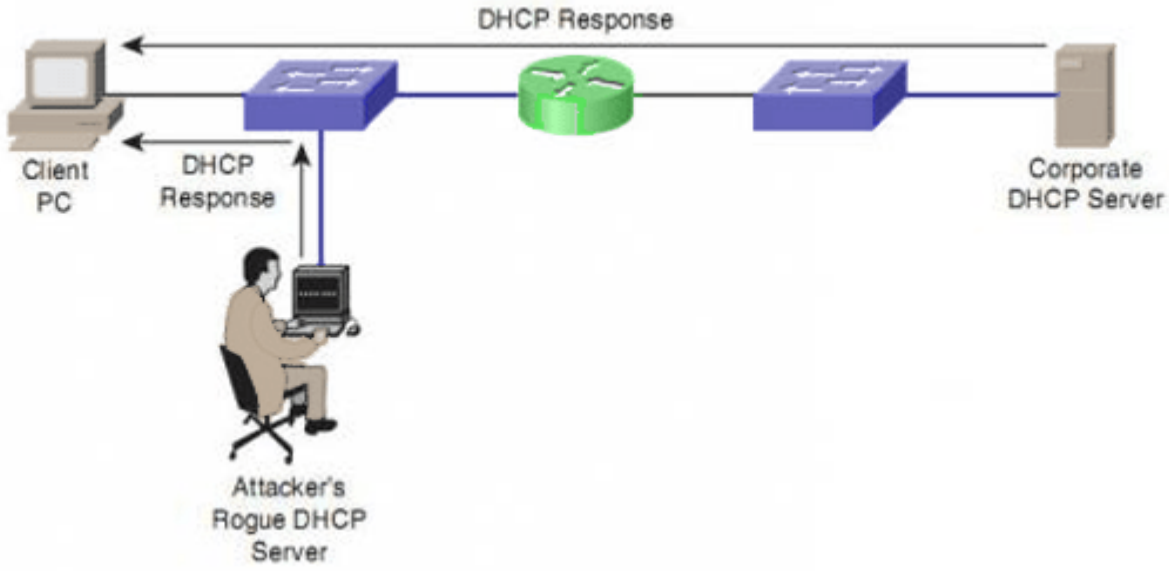
Attaques furtives DNS: pour masquer leur identité, les acteurs de menace utilisent également les techniques de furtivité DNS : Flux rapide, Double flux IP, Algorithmes de génération de domaine.

Attaques d'ombrage (shadowing) de domaine DNS : La surveillance de domaine implique que l'acteur de menace recueille des informations sur le compte du domaine afin de créer silencieusement plusieurs sous-domaines à utiliser lors des attaques. Ces sous-domaines pointent généralement vers des serveurs malveillants sans alerter le propriétaire réel du domaine parent.

Tunnellisation (tunneling) DNS : Les cyberpirates qui utilisent une attaque DNS par tunnellisation introduisent un trafic non DNS dans le trafic DNS.

Attaques DHCP

- Une **attaque d'usurpation DHCP** se produit lorsqu'un serveur DHCP non autorisé est connecté au réseau et fournit de faux paramètres de configuration IP aux clients légitimes. Un serveur non autorisé peut fournir de nombreuses informations erronées :
  - **Passerelle par défaut incorrecte** - L'acteur de menace fournit une passerelle non valide ou l'adresse IP de son hôte pour créer une attaque MITM. Cela peut ne pas être détecté car l'intrus intercepte le flux de données à travers le réseau.
  - **Serveur DNS incorrect** - L'acteur de menace fournit une adresse de serveur DNS incorrecte orientant l'utilisateur vers un site Web malveillant.
  - **Adresse IP incorrecte** - L'acteur de menace fournit une adresse IP non valide, une adresse IP de passerelle par défaut non valide, ou les deux. L'acteur de la menace crée ensuite une attaque DoS sur le client DHCP.



Meilleures pratiques de sécurité réseau

Confidentialité, disponibilité et intégrité

- La plupart des organisations suivent la triade de sécurité de l'information de la CIA:
  - **Confidentialité** - Seuls les individus, entités ou processus autorisés peuvent accéder aux informations sensibles. Cela peut nécessiter l'utilisation d'algorithmes de cryptage cryptographiques tels que AES pour crypter et décrypter les données.
  - **Intégrité** -Désigne la protection des données contre toute altération non autorisée. Il nécessite l'utilisation d'algorithmes de hachage cryptographiques tels que SHA.
  - **Disponibilité** - Les utilisateurs autorisés doivent avoir un accès interrompu aux ressources et données importantes. Cela nécessite la mise en œuvre de services, de passerelles et de liaisons redondants.

L'approche de défense en profondeur

- La plupart des organisations utilisent une approche de défense en profondeur de la sécurité. Cela nécessite une combinaison de périphériques réseau et de services fonctionnant ensemble.
- Plusieurs dispositifs et services de sécurité sont mis en œuvre.
  - **VPN**
  - **Pare-feu**
  - **IPS**
  - **ESA/WSA**
  - **Serveur AAA**



- Tous les périphériques réseau, y compris le routeur et les commutateurs, sont renforcés.

Pare-feu

Un pare-feu est un système ou un groupe de systèmes qui applique une stratégie de contrôle d'accès entre les réseaux.

Allow traffic from any external address to the web server.

Allow traffic to FTP server.

Allow traffic to SMTP server.

Allow traffic to internal IMAP server.

Deny all inbound traffic with network addresses matching internal-registered IP addresses.

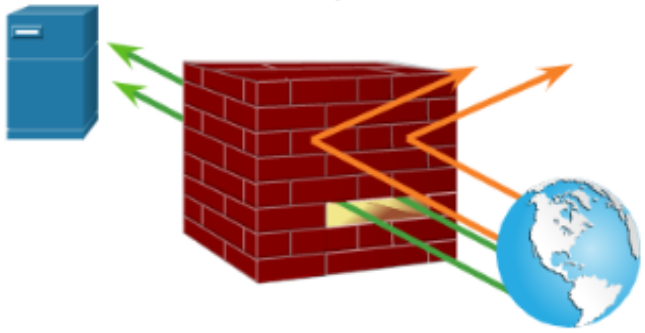
Deny all inbound traffic to server from external addresses.

Deny all inbound ICMP echo request traffic.

Deny all inbound MS Active Directory queries.

Deny all inbound traffic to MS SQL server queries.

Deny all MS Domain Local Broadcasts.

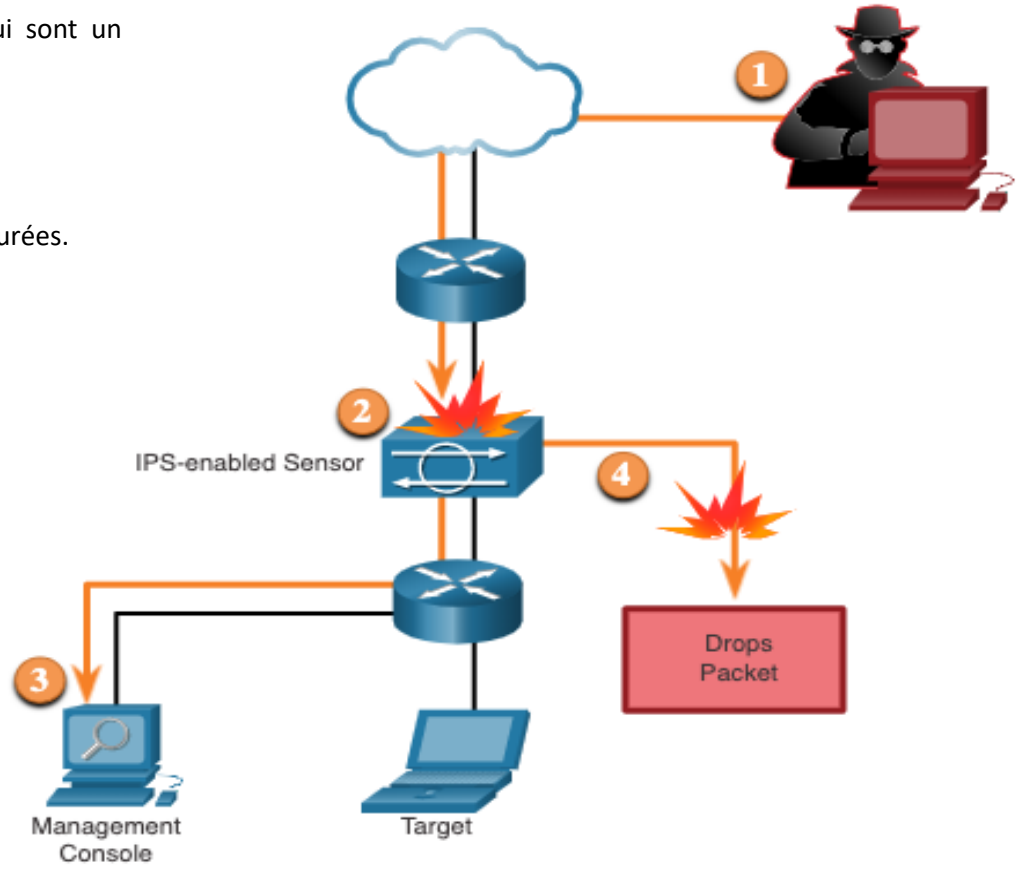


IPS

Les technologies IDS et IPS détectent les modèles de trafic réseau à l'aide de signatures, qui sont un ensemble de règles utilisées pour détecter les activités malveillantes.

La figure montre comment un IPS gère le trafic refusé.

1. L'acteur de menace envoie un paquet destiné à l'ordinateur portable cible.
2. L'IPS intercepte le trafic et l'évalue par rapport aux menaces connues et aux stratégies configurées.
3. L'IPS envoie un message de journal à la console de gestion.
4. L'IPS abandonne le paquet.



CHAPITRE 2

Sécuriser l’accès aux réseaux

1. Concepts de sécurité réseau
2. Les ACLs
3. NAT pour IPv4
4. Concept VPN

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

Une ACL (Access Control List) est une liste d'instructions destinées à autoriser ou à refuser le mouvement des données depuis la couche réseau et au-dessus. Ils sont utilisés pour filtrer le trafic sur nos réseaux comme l'exige la politique de sécurité.

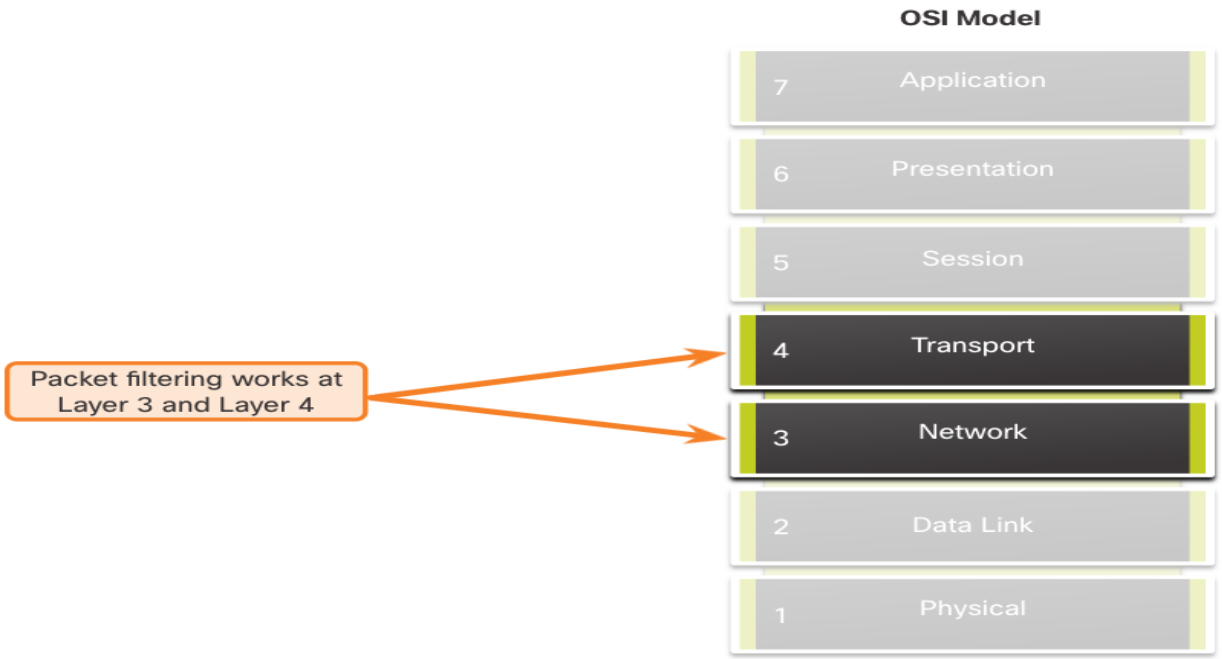
L'utilisation des ACL est cruciale pour la sécurité du réseau et dans ce chapitre, nous verrons comment nous pouvons les mettre en œuvre afin d'améliorer la sécurité du réseau.

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

Filtrage des paquets

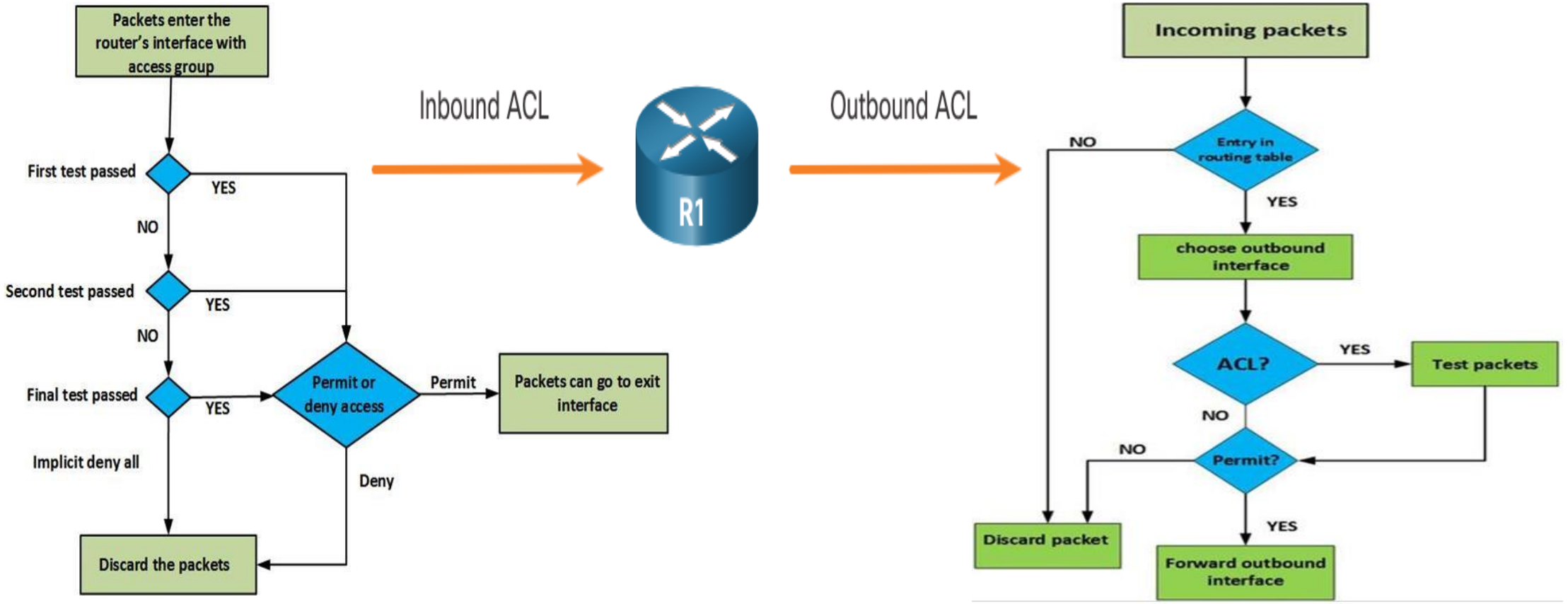
- Le filtrage de paquets contrôle l'accès à un réseau en analysant les paquets entrants et/ou sortants et en les transmettant ou en les abandonnant en fonction de critères donnés.
- Le filtrage des paquets peut être effectué au niveau de la couche 3 ou de la couche 4.
  - **ACL standard** - Les ACL filtrent 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.



PARTIE 6

Le fonctionnement des listes de contrôle d'accès

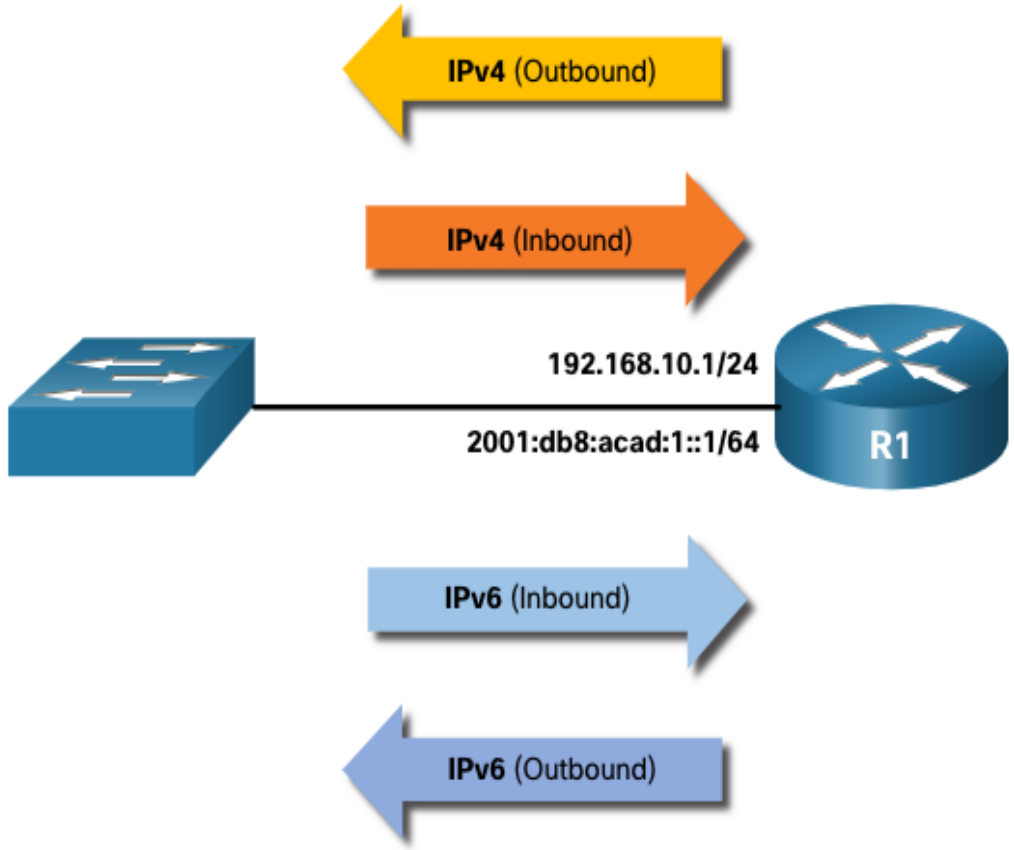
Les listes de contrôle d'accès peuvent être configurées pour s'appliquer au trafic entrant et au trafic sortant :



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.

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.



Directives pour la création d'ACL

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 **remark** .	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.

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**

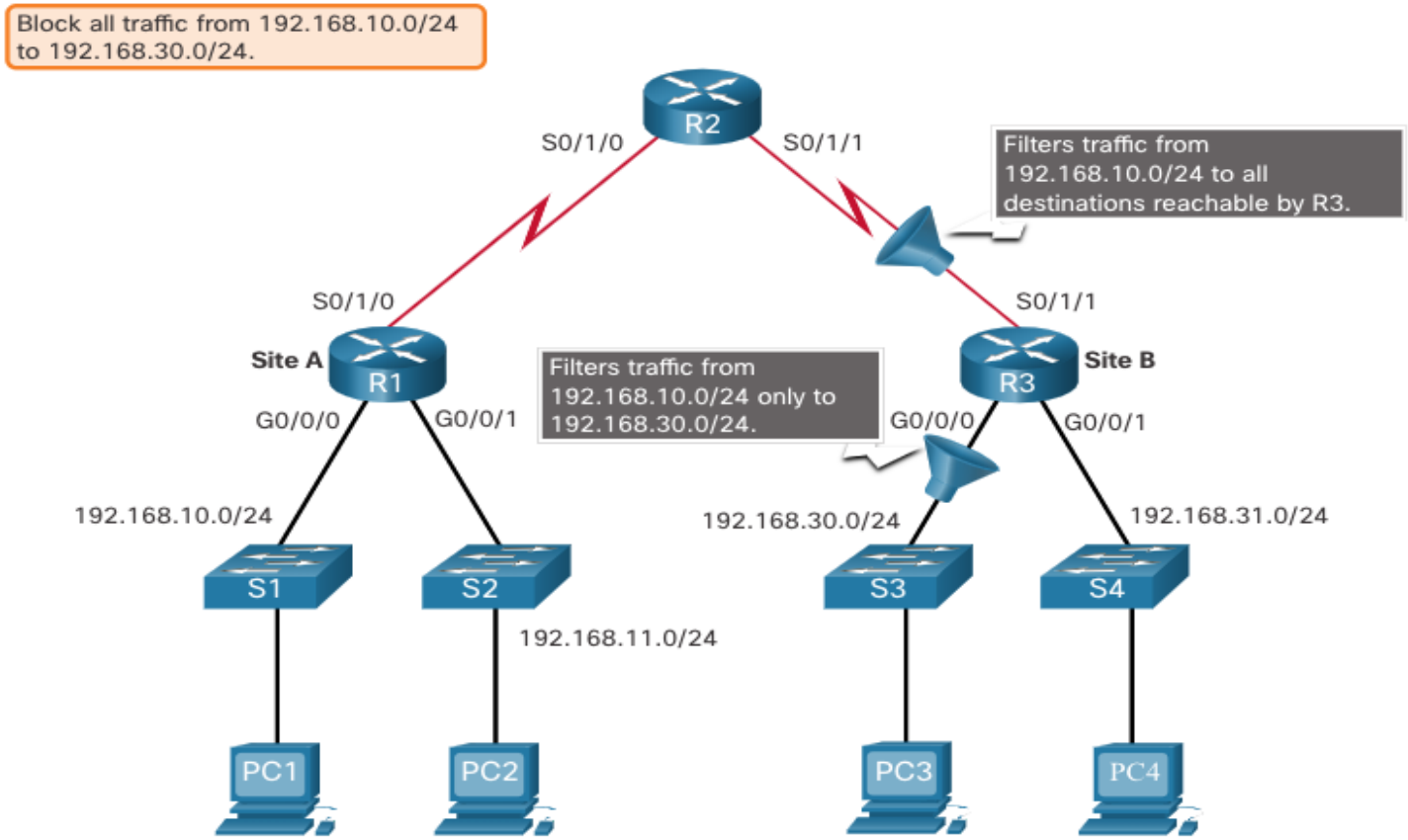
  - **Listes de contrôle d'accès numérotées**

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.

  - **Listes de contrôle d'accès nommées**

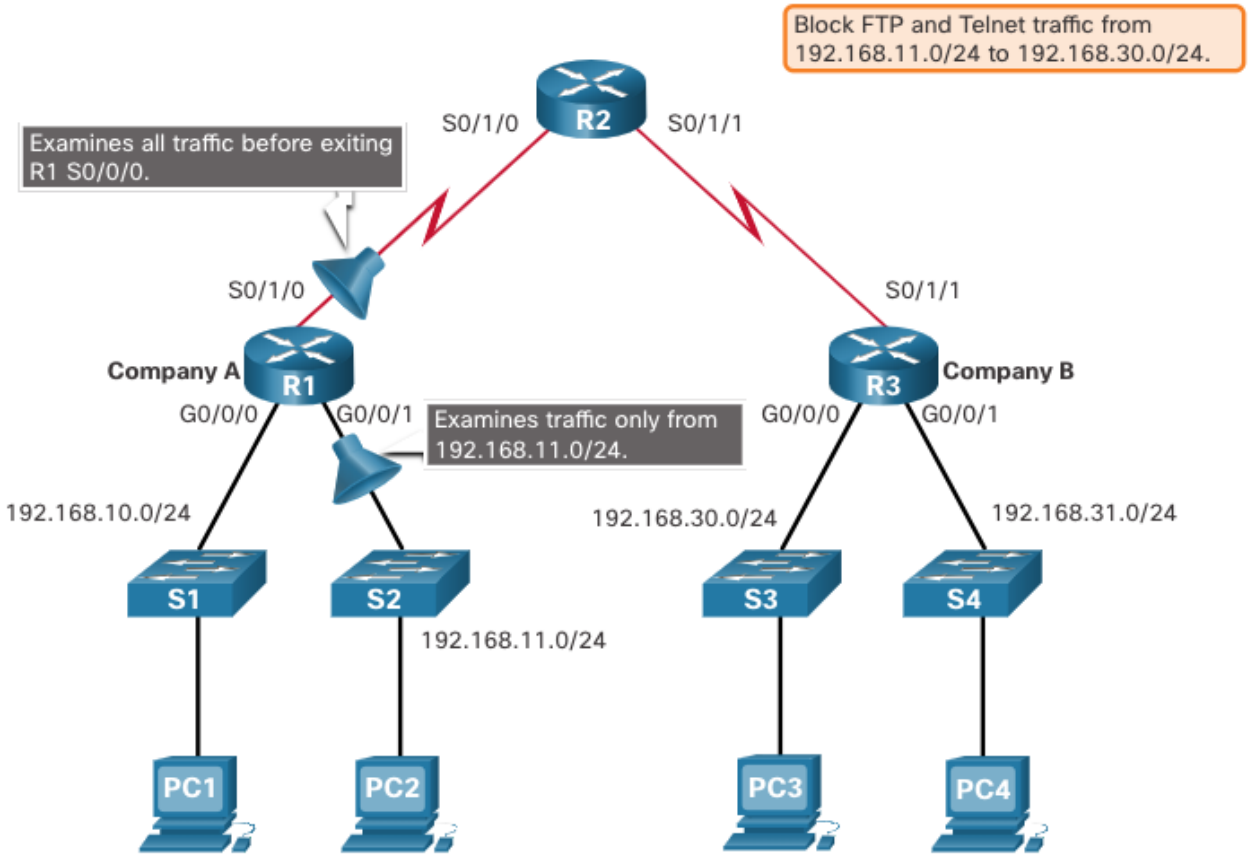
Les ACL nommées sont la méthode préférée à utiliser lors de la configuration des ACL. Plus précisément, les listes ACL standard et étendues peuvent être nommées pour fournir des informations sur l'objet de la liste ACL.

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



PARTIE 6

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



Créer une ACL

Toutes les listes de contrôle d'accès (ACL) doivent être planifiées.

- **Syntaxe des listes de contrôle d'accès IPv4 standard numérotées**

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

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

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

- **Syntaxe des listes de contrôle d'accès IPv4 standard nommées**

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

```
Router(config) # ip access-list standard {liste_name}
Router(config-ext-nacl) # {permit | deny |remark text} source  [source-wildcard]
```

- Les noms des listes de contrôle d'accès doivent contenir uniquement des caractères alphanumériques, sont sensibles à la casse et doivent être uniques.

- Pour supprimer une ACL standard numérotée, utilisez la commande de configuration globale **no access-list** *access-list-number.*
- Pour supprimer une ACL standard nommée, utilisez la commande de configuration globale **no access-list standard** *access-list-name.*

PARTIE 6

Appliquer une ACL 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.

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

Modifier les listes de contrôle d'accès IPv4

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

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.

Utiliser les numéros de séquence

- 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.
- l'instruction actuelle doit être supprimée d'abord avec la commande ***no*** *{sequence_number }*. Ensuite, le bon ACE peut être ajouté en utilisant le numéro de séquence.

Sécuriser les ports VTY à l'aide d'une ACL IPv4 standard

- **Appliquer une ACL sur les lignes VTY**

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 }
```

Configuration des ACL pour IPv4 : Modifier les listes de contrôle d'accès IPv4

- **Verifier une ACL**

Pour vérifier la configuration d' ACL on utilise la commande **show access-lists** .

- **Statistiques des listes de contrôle d'accès**

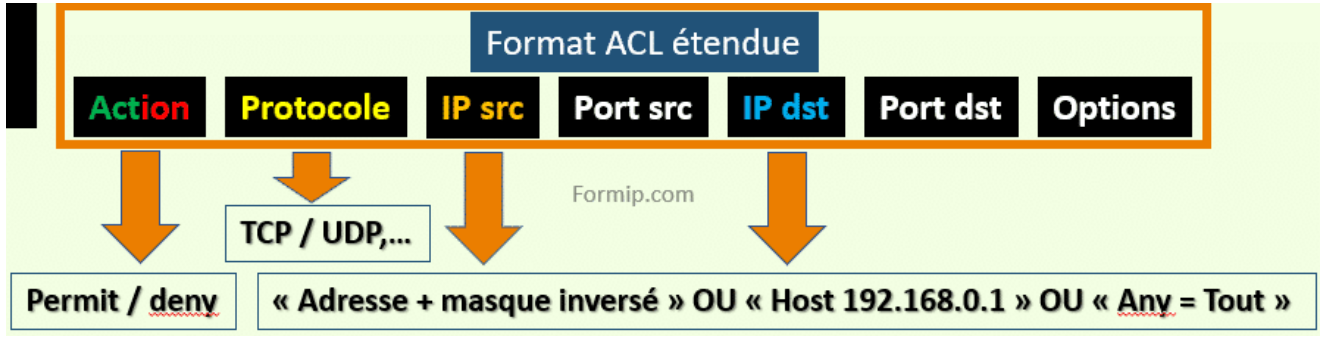
La commande **show access-lists** affiche des statistiques pour chaque instruction qui a été mise en correspondance.

- 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#
```

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** - Créé à l'aide de la commande de configuration globale **access-list** *access-list-number* .
- **ACL étendu nommée** - Créé à l'aide de la commande **ip access-list extended** *access-list-name* .

Utiliser le **?** pour obtenir de l'aide lors de la saisie d'un ACE complexe.

ACL numérique étendue

```
R1(config)#access-list 100 permit tcp any host 192.168.1.2 eq 80
R1(config)#access-list 100 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.2
```

ACL nommée étendue

deny any any

```
R1(config)#ip access-list extended monACLetendue
R1(config-ext-nacl)#permit tcp any host 192.168.1.2 eq 80
R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.2
```

PARTIE 6

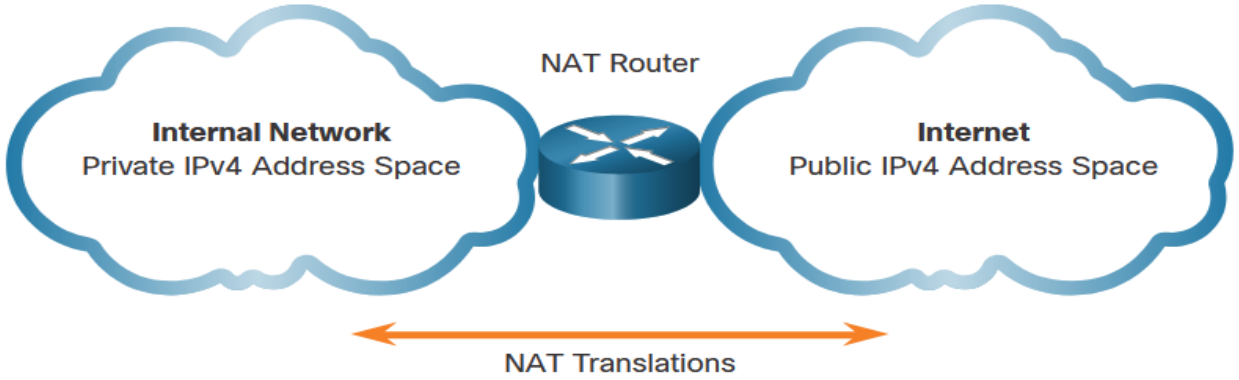
CHAPITRE 2

Sécuriser l’accès aux réseaux

1. Concepts de sécurité réseau
2. Les ACLs
3. NAT pour IPv4
4. Concept VPN

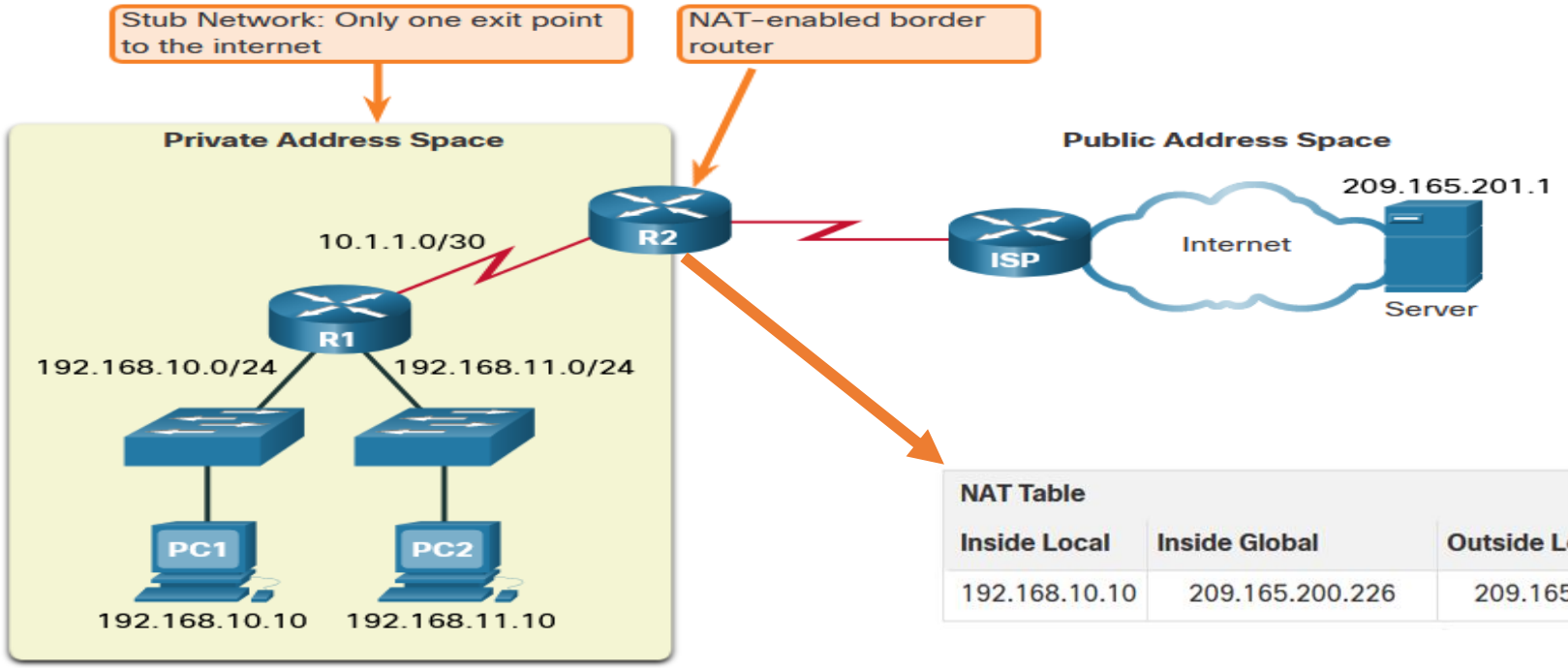
Comment fonctionne la NAT

- L'utilisation principale de NAT consiste à limiter la consommation des adresses IPv4 publiques.
- La NAT permet aux réseaux d'utiliser des adresses IPv4 privées en interne, et traduit ces adresses en une adresse publique lorsque nécessaire.
- Un routeur NAT fonctionne généralement à la périphérie d'un réseau d'extrémité.
- Lorsqu'un périphérique à l'intérieur du réseau stub veut communiquer avec un périphérique en dehors de son réseau, le paquet est transmis au routeur périphérique qui effectue le processus NAT, traduisant l'adresse privée interne du périphérique en une adresse publique, externe et routable.



Comment fonctionne la NAT

PC1 souhaite communiquer avec un serveur Web externe dont l'adresse publique est 209.165.201.1.



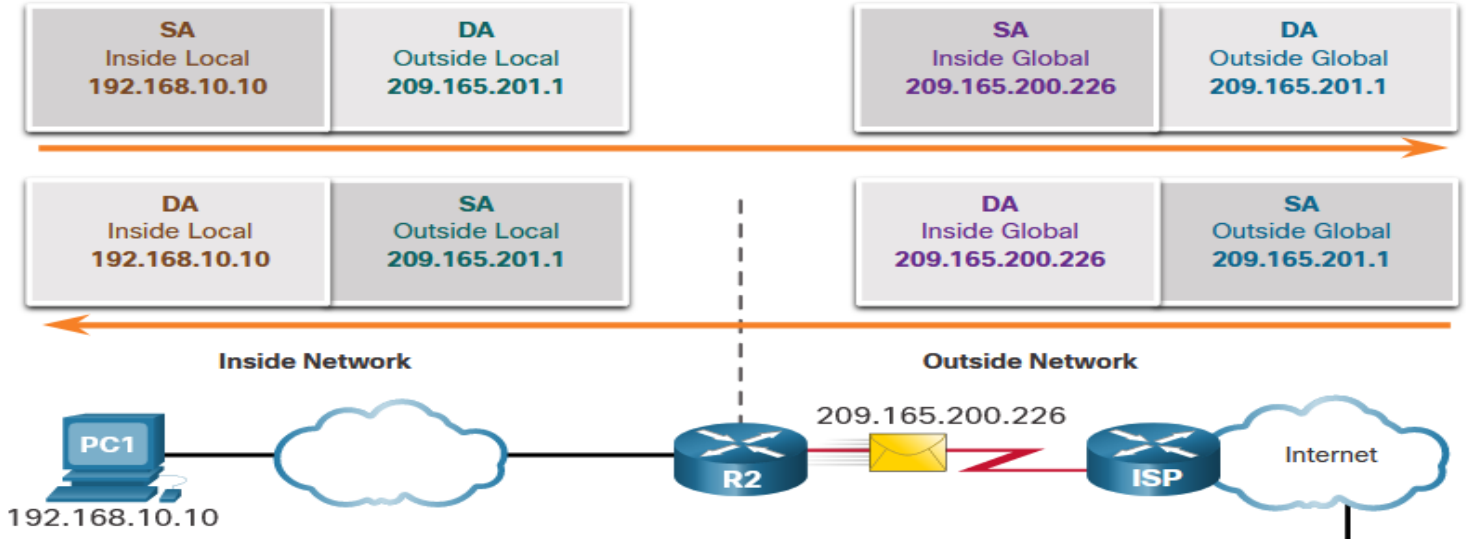
NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

PARTIE 6

Terminologie NAT

La fonction NAT comprend quatre types d'adresses : **Adresse locale interne - Adresse globale interne - Adresse locale externe - Adresse globale externe**



R2 NAT Table			
PC1		**Web Server**	
Inside Global Address	**Inside Local Address**	**Outside Local Address**	**Outside Global Address**
209.165.200.226	**192.168.10.10**	**209.165.201.1**	**209.165.201.1**

PARTIE 6

Caractéristiques de NAT

Bénéfices de la NAT

La NAT offre de nombreux avantages:

- La fonction NAT ménage le schéma d’adressage enregistré légalement en autorisant la privatisation des intranets.
- Elle économise les adresses au moyen d’un multiplexage au niveau du port de l’application.
- La fonction NAT augmente la souplesse des connexions au réseau public.
- La fonction NAT assure la cohérence des schémas d’adressage du réseau interne.
- La NAT permet de conserver le schéma des adresses IPv4 privées existant et de passer facilement à un nouveau schéma d'adressage public.
- La NAT cache les adresses IPv4 des utilisateurs et autres périphériques.

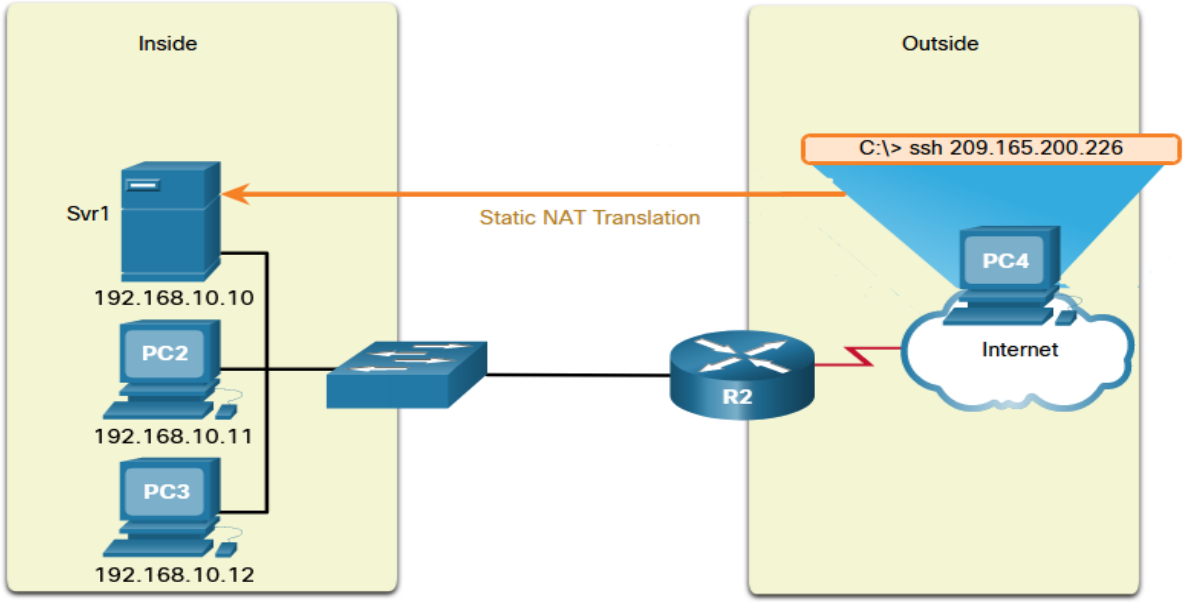
Inconvénients de la NAT

La NAT présente également des inconvénients:

- La NAT augmente les délais de transfert.
- L'adressage de bout en bout est perdu.
- Perte de la traçabilité IP de bout en bout
- NAT complique l'utilisation de protocoles de tunneling, tels que IPSec.
- Les services nécessitant l'établissement de connexions TCP depuis le réseau externe ou les protocoles sans état tels que ceux utilisant UDP peuvent être perturbés.

NAT statique

La NAT statique utilise un mappage un à un des adresses locales et globales configurées par l'administrateur réseau qui restent constantes.

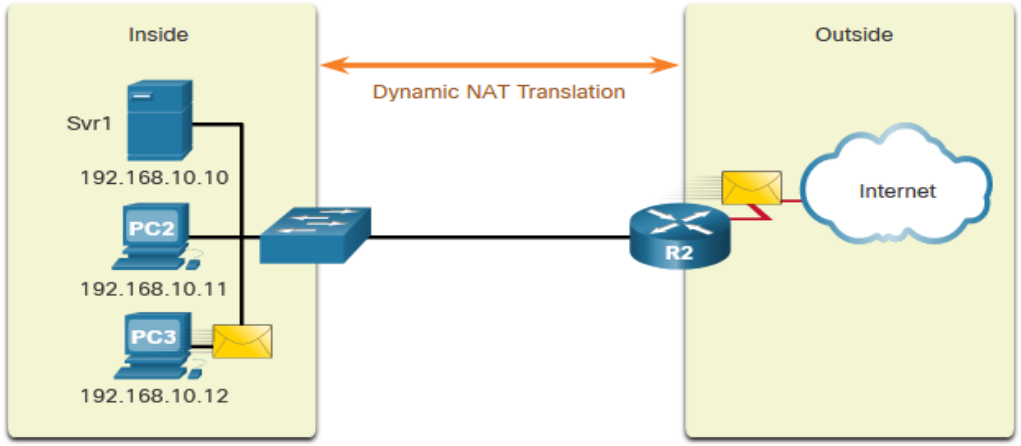


Static NAT Table	
Inside Local Address	**Inside Global Address – Addresses reachable via R2**
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Remarque: La NAT statique nécessite qu'il existe suffisamment d'adresses publiques disponibles pour satisfaire le nombre total de sessions utilisateur simultanées.

NAT dynamique

La NAT dynamique utilise un pool d'adresses publiques et les attribue selon la méthode du premier arrivé, premier servi.

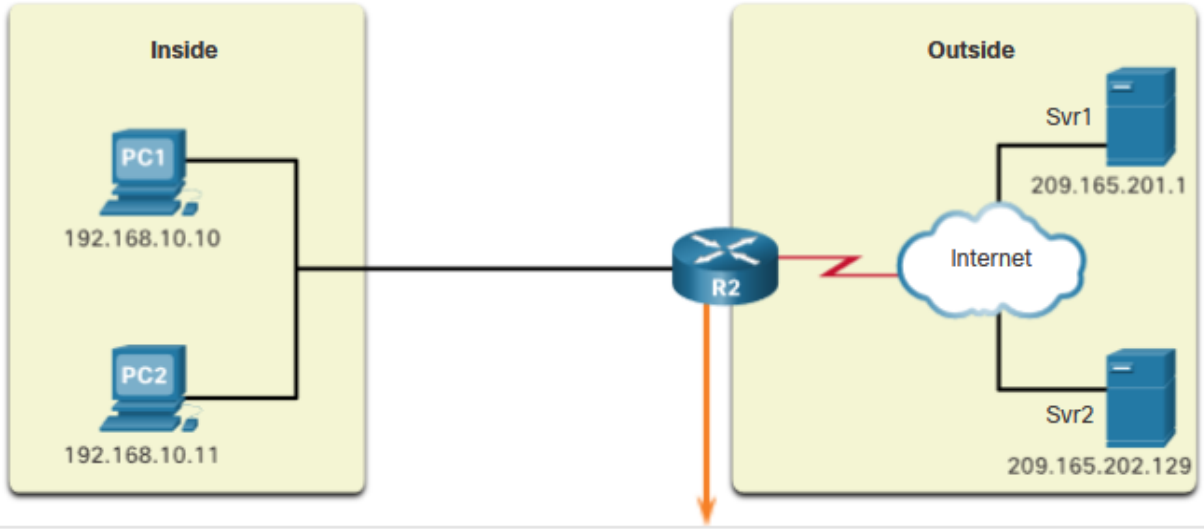


IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool – Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Remarque: La NAT dynamique nécessite qu'il existe suffisamment d'adresses publiques disponibles pour satisfaire le nombre total de sessions utilisateur simultanées.

Traduction d'adresses de port (PAT)

La traduction d'adresses de port (PAT), également appelée surcharge NAT, mappe plusieurs adresses IPv4 privées à une seule adresse IPv4 publique unique ou à quelques adresses.

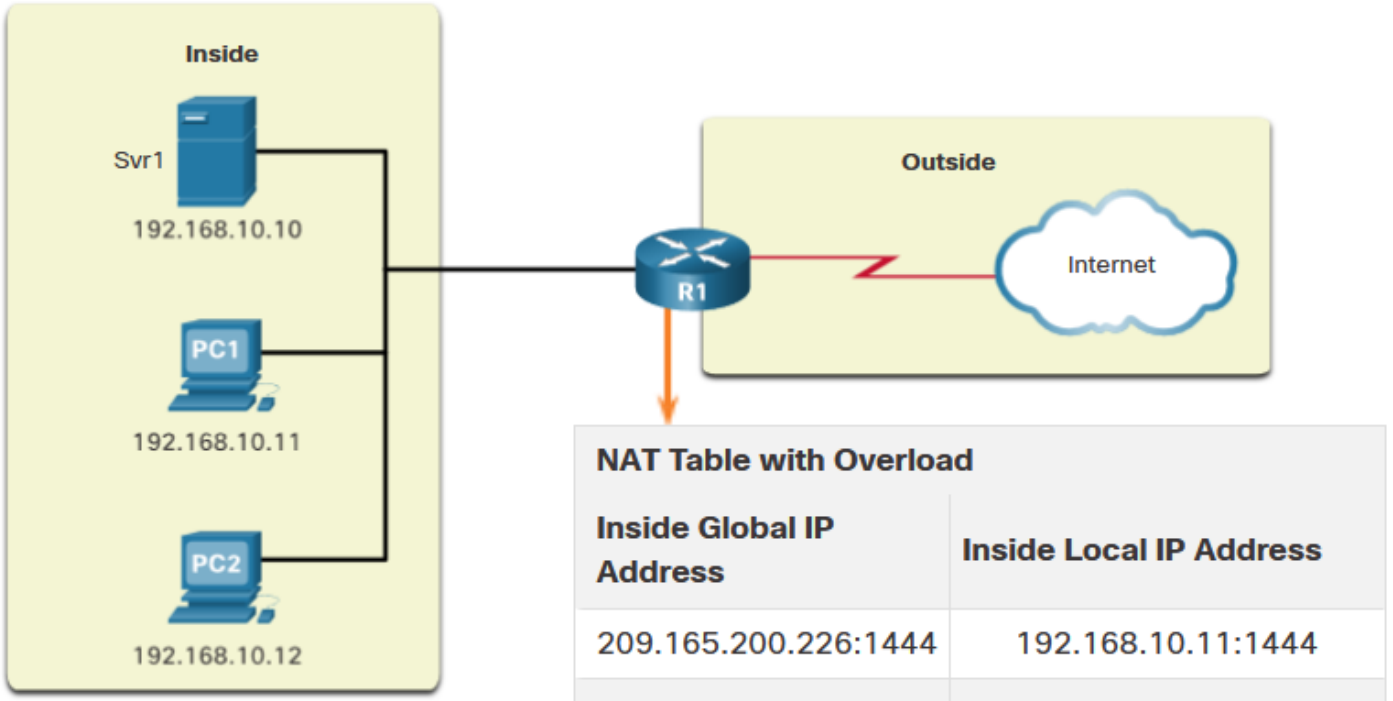


NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

PAT avec Port disponible suivant

La fonction PAT tente de conserver le port source d'origine. Si le port source d'origine est déjà utilisé, la PAT attribue le premier numéro de port disponible en commençant au début du groupe de ports approprié 0 à 511, 512 à 1023 ou 1024 à 65535.



NAT Table with Overload

Inside Global IP Address	Inside Local IP Address
209.165.200.226:1444	192.168.10.11:1444
209.165.200.226:1445	192.168.10.12:1444

Comparaison entre la NAT et la PAT

Récapitulation des différences entre NAT et PAT.

NAT	PAT
Un mappage un-à-un entre une adresse locale interne et une adresse globale interne.	Une adresse globale interne peut être mappée à de nombreuses adresses locale interne.
Utilise uniquement les adresses IPv4 dans le processus de traduction.	Utilise les adresses IPv4 et les numéros de port source TCP ou UDP dans le processus de traduction.
Une adresse globale interne unique est requise pour chaque hôte interne accédant au réseau externe.	Une seule adresse globale interne unique peut être partagée par plusieurs hôtes internes accédant au réseau externe.

- **Paquets sans segment de couche 4**

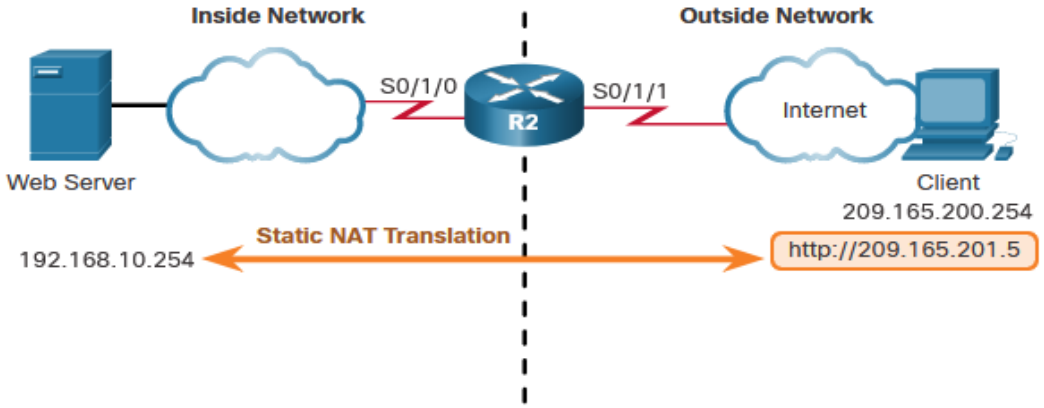
Certains paquets ne contiennent pas de numéro de port de couche 4, tels que les messages ICMPv4. Chacun de ces types de protocole est pris en charge différemment par la PAT.

Remarque: Ces messages et d'autres protocoles qui n'utilisent pas les numéros de port TCP ou UDP peuvent varier et sortent du cadre de ce programme.

Configurer la NAT statique

La configuration des traductions NAT statiques comporte deux étapes fondamentales:

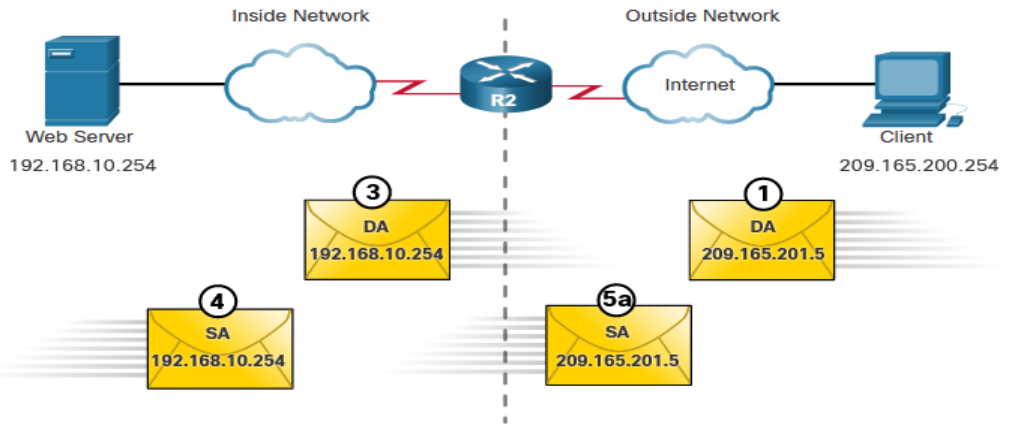
- **Étape 1** - Créer un mappage entre l'adresse locale interne et les adresses globales internes en utilisant la commande **ip nat inside source static** .
- **Étape 2** - Les interfaces participant à la traduction sont configurées comme à l'intérieur ou à l'extérieur par rapport à NAT avec les commandes **ip nat inside** et **ip nat outside** .




```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Analyser la NAT statique

Processus de traduction NAT statique entre le client et le serveur Web:



	Inside Local Address	Inside Global Address	Outside Local Address	Outside Global Address
2 5b	192.168.10.254	209.165.201.5	209.165.200.254	209.165.200.254

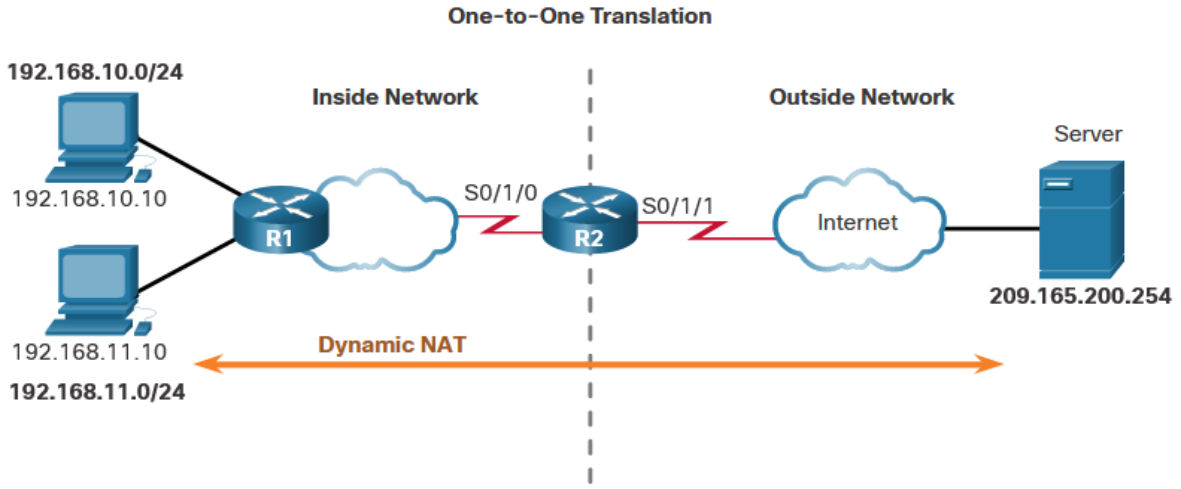
Vérifier NAT statique

- Pour vérifier le fonctionnement NAT, exécutez la commande **show ip nat translations** .
- Une autre commande utile est **show ip nat statistics.**
- Pour vérifier que la traduction NAT fonctionne, il est préférable d'effacer les statistiques des traductions passées à l'aide de la commande **clear ip nat statistics** avant d'effectuer le test.

Configurer la NAT dynamique

La configuration des traductions NAT dynamiques comporte cinq tâches :

- **Étape 1** - Définissez le pool d'adresses à utiliser pour la traduction en utilisant la commande **ip nat pool** .
- **Étape 2** - Configurez une liste de contrôle d'accès (ACL) standard pour identifier (autoriser) uniquement les adresses qui doivent être traduites.
- **Étape 3** - Liez l'ACL au pool, en utilisant la commande **ip nat inside source list** .
- **Étape 4** - Identifiez quelles interfaces sont à l'intérieur.
- **Étape 5** - Identifiez quelles interfaces sont à l'extérieur.




```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

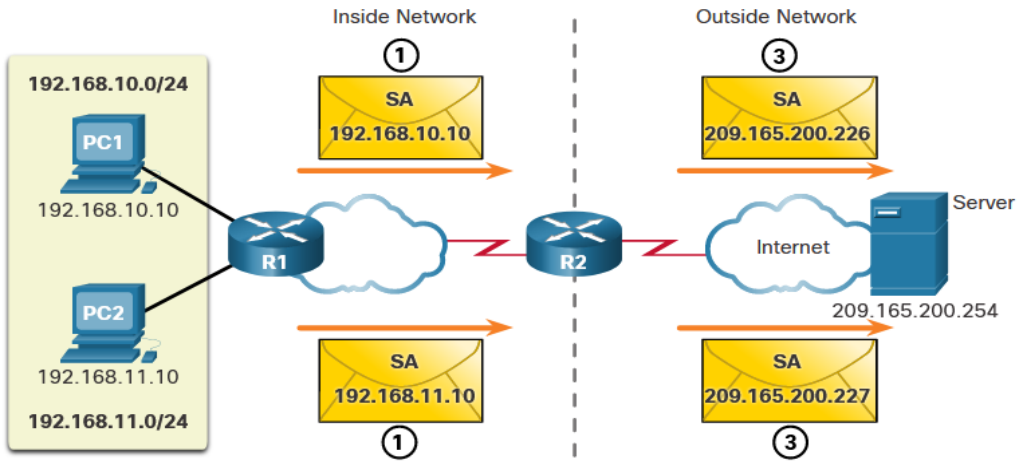
PARTIE 6

PARTIE 6

Analyser la NAT dynamique

Analyser la NAT dynamique - de l'intérieur à l'extérieur

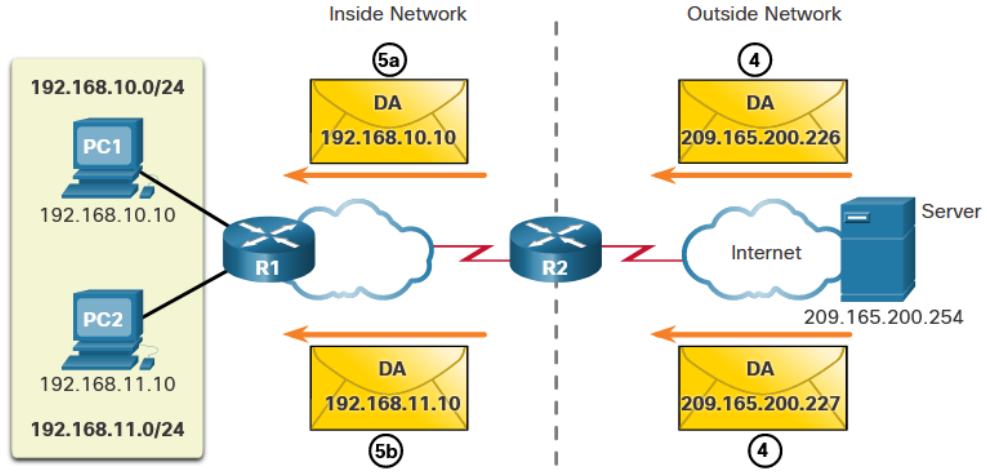
Processus de traduction NAT dynamique :



	IPv4 NAT Pool	
	Inside Local Address Pool	Inside Global Address
②	192.168.10.10	209.165.200.226
②	192.168.11.10	209.165.200.227

Analyser la NAT dynamique - de l'extérieur à l'intérieur

Processus de traduction NAT dynamique :



	IPv4 NAT Pool	
	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

Vérifier la NAT dynamique

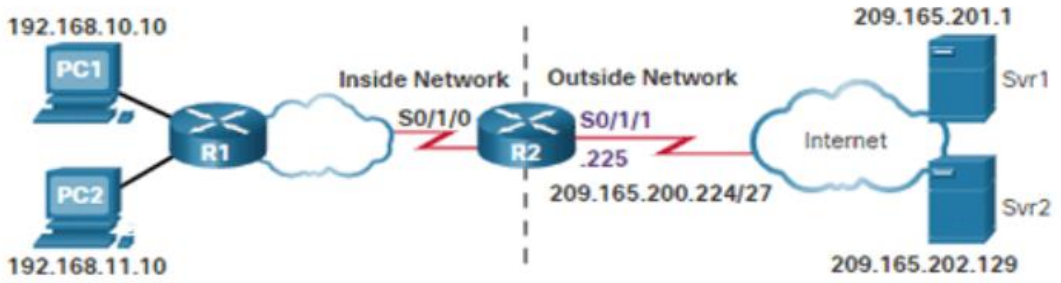
- La sortie de la commande **show ip nat translations** montre toutes les traductions statiques qui ont été configurées ainsi que les éventuelles traductions dynamiques créées par le trafic.
- Si vous ajoutez le mot-clé **verbose**, vous obtiendrez des informations supplémentaires sur chaque traduction, notamment la date de création et la durée d'utilisation d'une entrée.
- Par défaut, les entrées de traduction expirent au bout de 24 heures, sauf si les compteurs ont été configurés à l'aide de la commande du mode de configuration globale **ip nat translation timeout** *timeout-seconds* .
- Pour effacer les entrées dynamiques avant l'expiration du délai, utilisez la commande du mode d'exécution privilégié **clear ip nat translation** .

Commande	Description
clear ip nat translation *	Efface toutes les entrées de traduction dynamique d'adresses de la table de traduction NAT.
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Efface une entrée de traduction dynamique simple contenant une traduction interne ou une traduction à la fois interne et externe.
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Efface une entrée de traduction dynamique étendue.

- La commande **show ip nat statistics** affiche des informations sur le nombre total de traductions actives, les paramètres de configuration NAT, le nombre d'adresses dans le pool et le nombre d'adresses allouées.

Configuration PAT pour utiliser un seule adresse

Pour configurer PAT pour utiliser une seule adresse IPv4, ajoutez le mot-clé **overload** à la commande **ip nat inside source** .



NAT Table

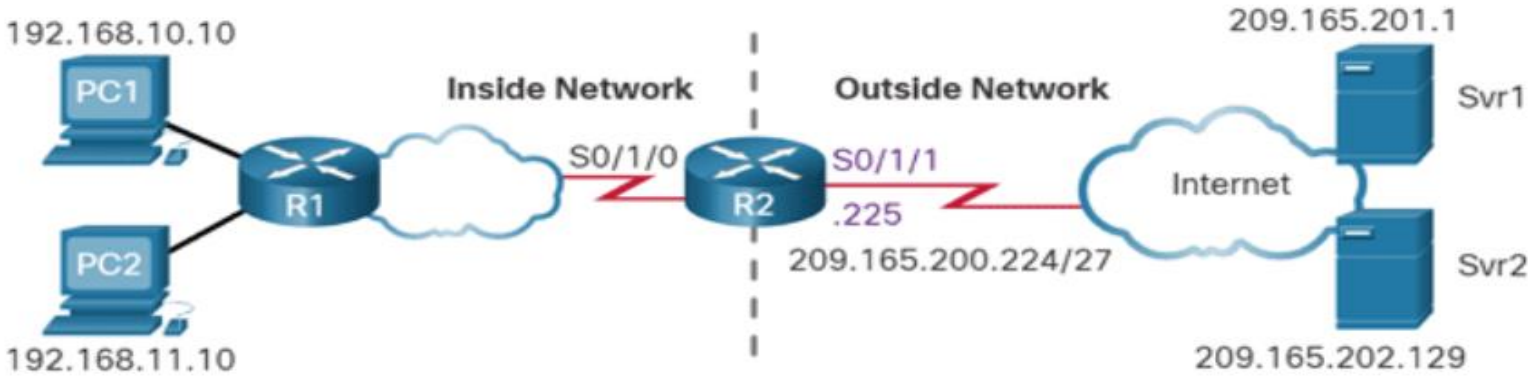
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.11.10:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

```
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2 (config) # interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2 (config) # interface Serial0/1/1
R2(config-if)# ip nat outside
```

PARTIE 6

Configurer PAT pour utiliser un pool d'adresses

Pour configurer PAT pour un pool d'adresses NAT dynamique, ajoutez simplement le mot-clé **overload** à la commande **ip nat inside source** .



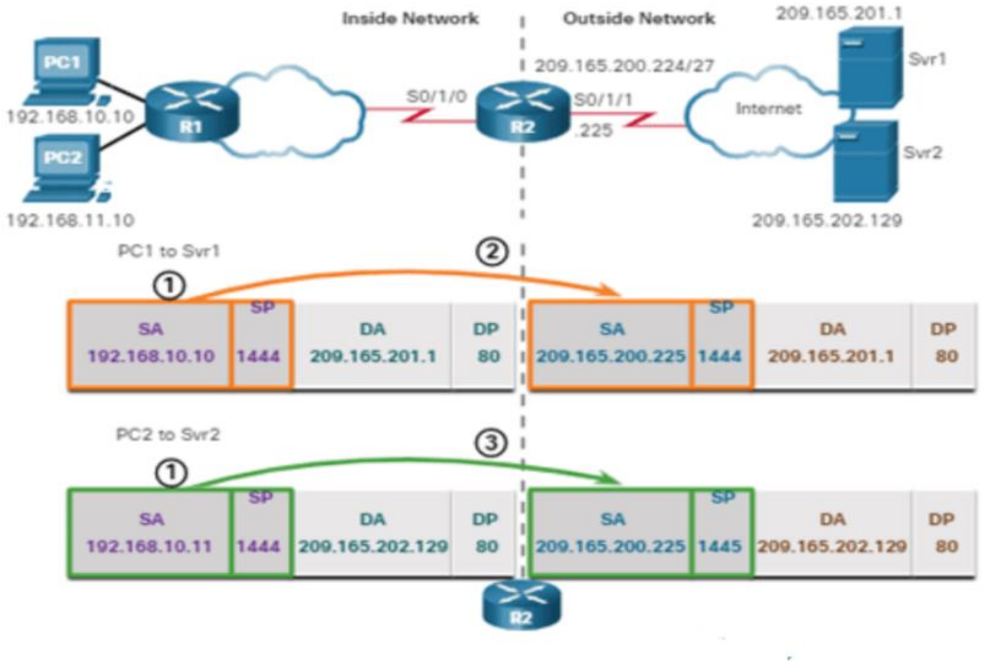

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2 (config) # interface serial0/1/0
R2(config-if)# ip nat inside
R2 (config-if) # interface serial0/1/0
R2(config-if)# ip nat outside
```

PARTIE 6

PARTIE 6

Analyser PAT

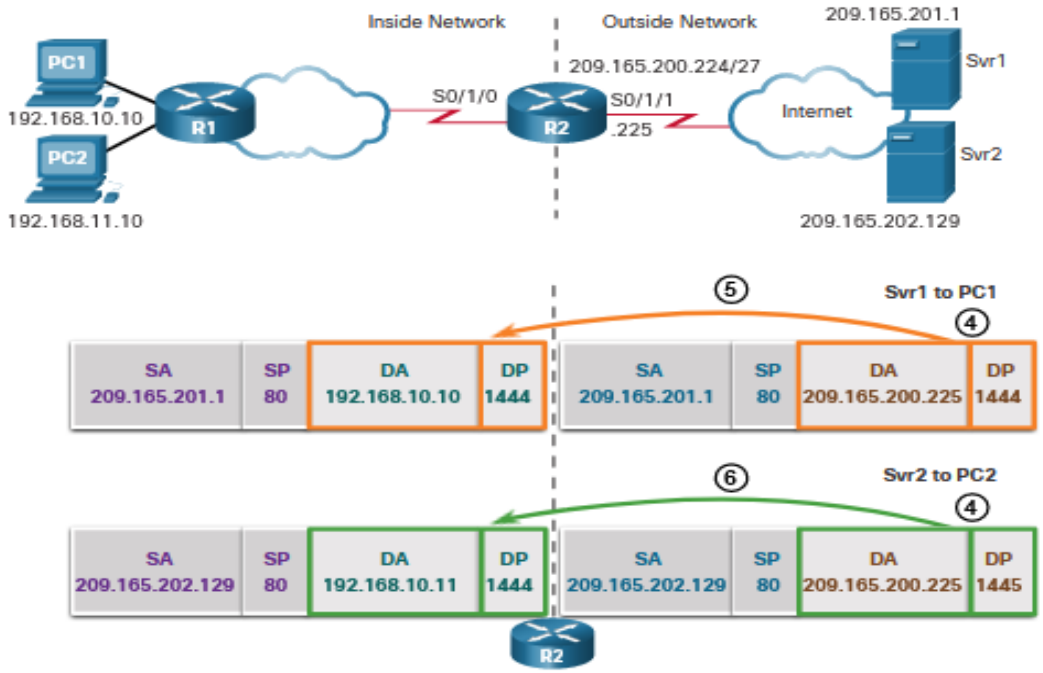
- **Analyser PAT - Serveur à PC**



NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.10:1444	209.165.200.225:1445	209.165.201.129:80	209.165.201.129:80

- **Analyser PAT - PC à Serveur**



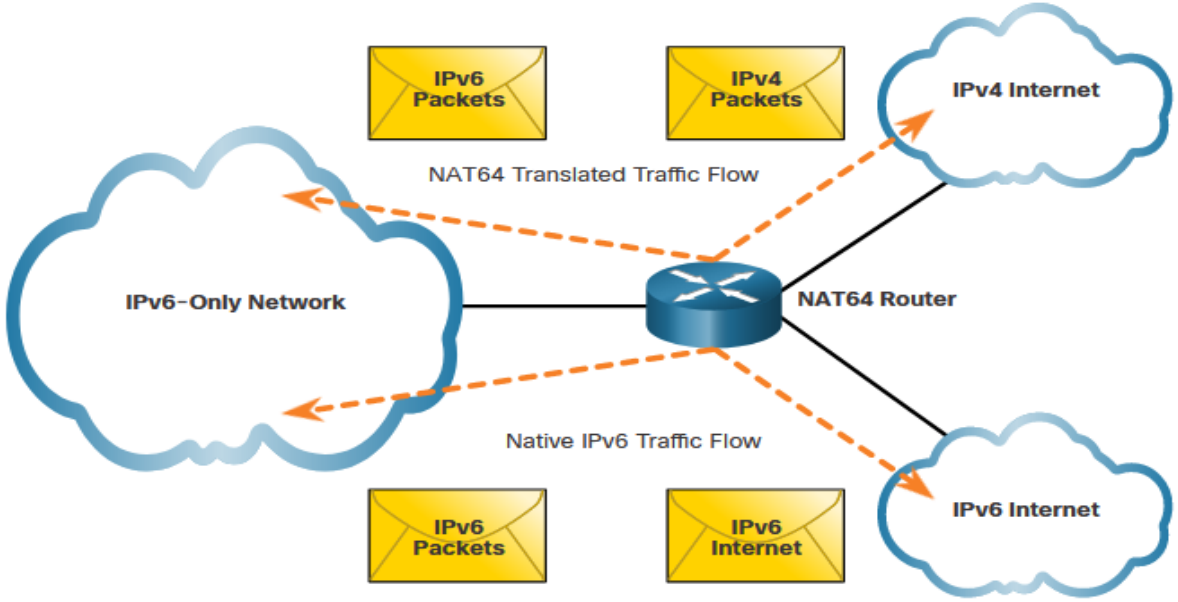
NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

NAT64

- **NAT pour IPv6?**

- La NAT pour IPv6 est utilisée dans un contexte très différent de la NAT pour IPv4. Elles ne servent pas à traduire des adresses IPv6 privées en adresses IPv6 globales.
- Les différentes NAT pour IPv6 servent à fournir de façon transparente un accès entre les réseaux IPv6-unique et les réseaux ipv4-unique.
- IPv6 permet la traduction de protocole entre IPv4 et IPv6 connu sous le nom de NAT64.
- La NAT pour IPv6 ne doit pas être utilisée en tant que stratégie à long terme, mais comme un mécanisme temporaire permettant d'aider à la migration d'IPv4 vers IPv6.



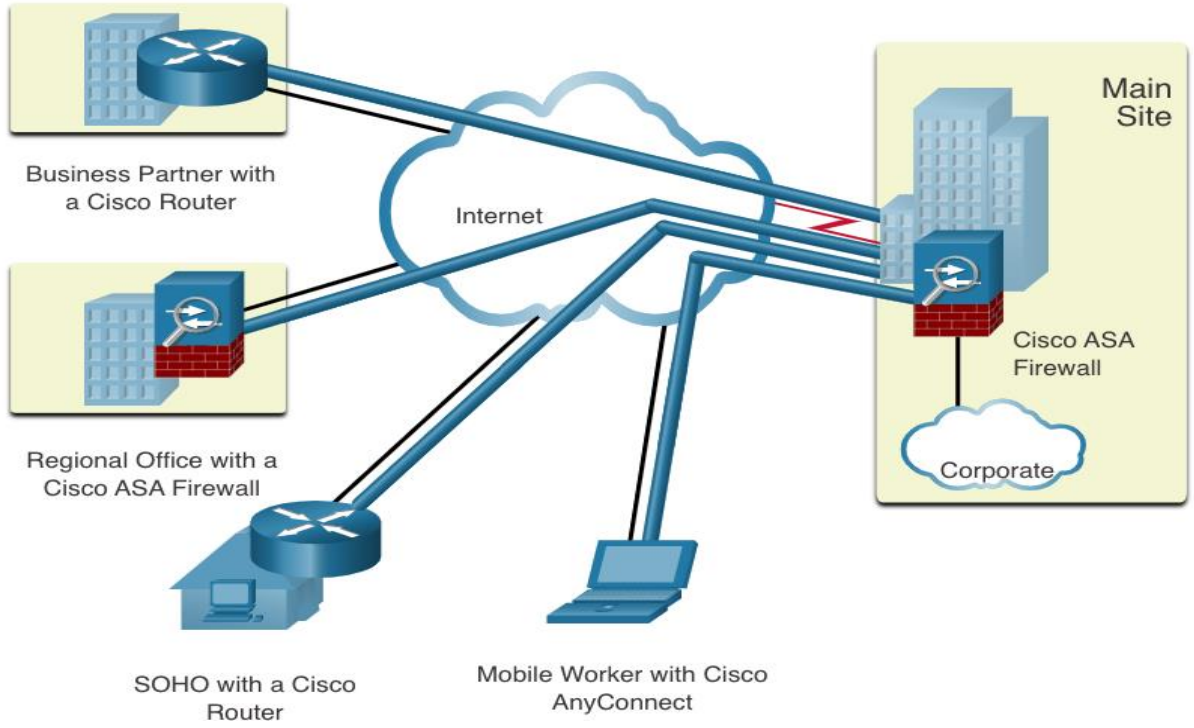
CHAPITRE 2

Sécuriser l’accès aux réseaux

1. Concepts de sécurité réseau
2. Les ACLs
3. NAT pour IPv4
4. Concept VPN

Technologies VPN

- **Réseau privé virtuel**
- Réseaux privés virtuels (VPN) pour créer des connexions de réseau privé de bout en bout.
- Un VPN est virtuel en ce sens qu'il transporte des informations au sein d'un réseau privé, mais que ces informations sont effectivement transférées via un réseau public.
- Un VPN est privé, dans le sens où le trafic est chiffré pour assurer la confidentialité des données pendant qu'il est transporté à travers le réseau public.



Technologies VPN

- **Les Bénéfices de VPN**

Les VPN modernes prennent en charge les fonctionnalités de chiffrement, telles que les protocoles IPsec (Internet Protocol Security) et SSL (Secure Sockets Layer) pour sécuriser le trafic réseau entre sites.

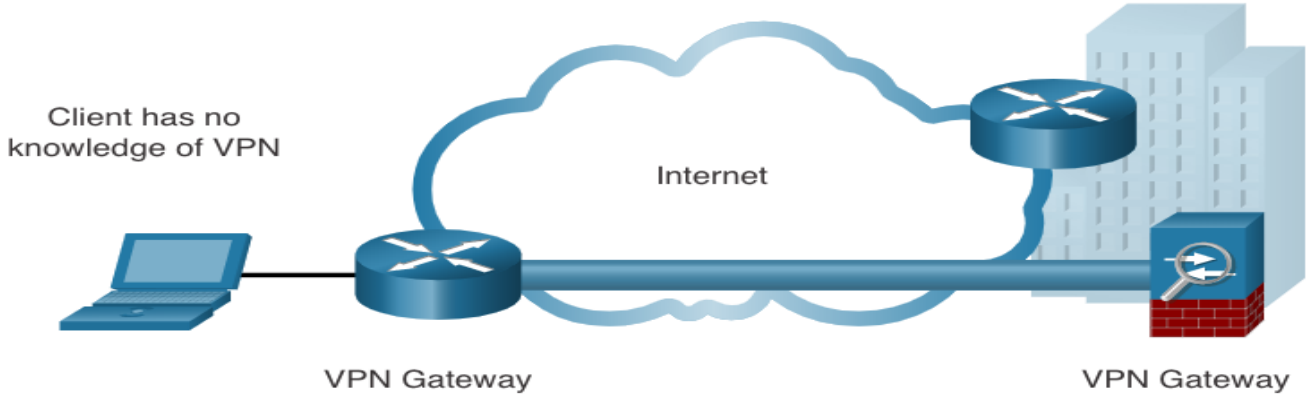
- Les principaux avantages des VPN sont présentés dans le tableau:

Bénéfice	Description
Réductions des coûts	Les organisations peuvent utiliser des VPN pour réduire leurs coûts de connectivité tout en augmentant simultanément la bande passante de connexion à distance.
Sécurité	Les protocoles de chiffrement et d'authentification protègent les données contre les accès non autorisé.
Extensibilité	Les VPN permettent aux organisations d'utiliser Internet, ce qui facilite l'ajout de nouveaux utilisateurs sans ajouter d'infrastructure importante.
Compatibilité	Les VPN peuvent être mis en œuvre sur une grande variété d'options de liaison WAN, y compris les technologies à large bande. Les travailleurs distants peuvent utiliser ces connexions à haut débit pour accéder en toute sécurité aux réseaux d'entreprise.

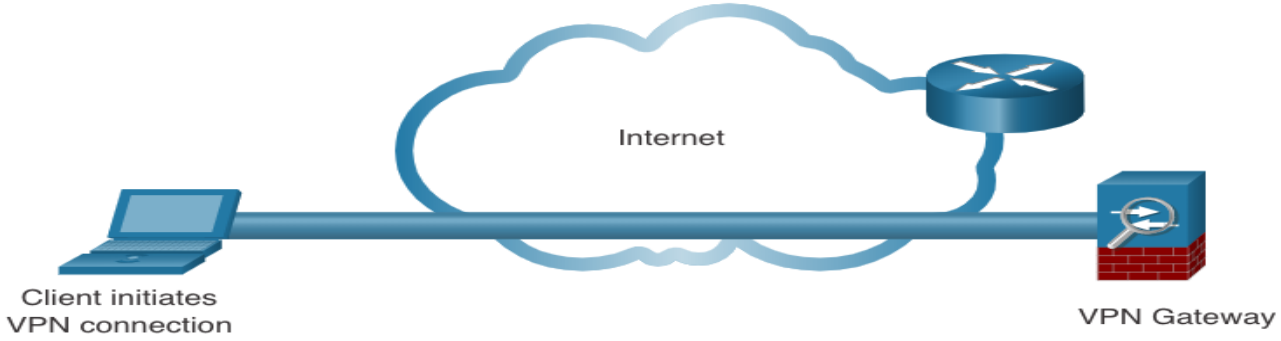
Technologies VPN

- **VPN de site à site et d'accès distant**

Un VPN de site à site se termine sur les passerelles VPN. Le trafic VPN n'est crypté qu'entre les passerelles. Les hôtes internes ne savent pas qu'un VPN est utilisé.



VPN d'accès à distance est créé dynamiquement lorsque cela est nécessaire pour établir une connexion sécurisée entre un client et un périphérique de terminaison VPN.

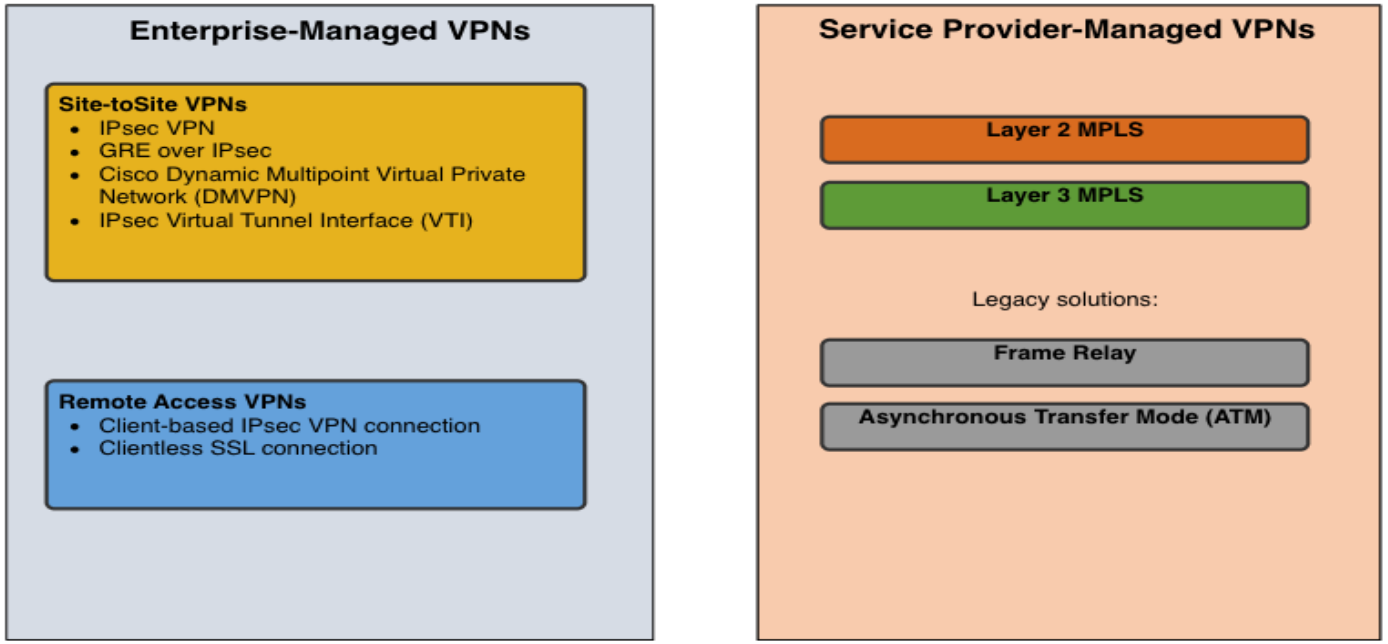


Technologies VPN

- **VPN d'entreprise et de prestataire de service**

Les VPN peuvent être gérés et déployés comme:

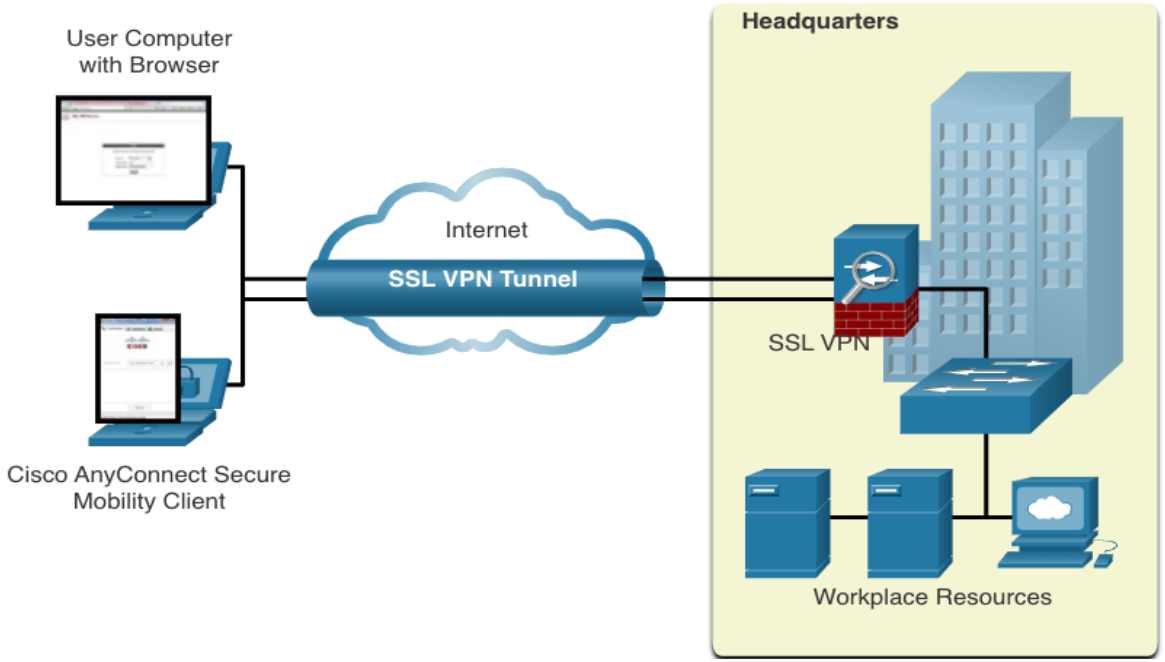
- **VPN d'entreprise** - des solutions similaires pour sécuriser le trafic d'entreprise sur l'internet. Les VPN de site à site et d'accès distant sont créés et gérés par l'entreprise à l'aide de VPN IPsec et SSL.
- **VPN des prestataires de services** – sont créés et gérés sur le réseau du fournisseur. Le fournisseur utilise la commutation d'étiquette multiprotocole (MPLS) au niveau de la couche 2 ou de la couche 3 pour créer des canaux sécurisés entre les sites d'une entreprise, séparant efficacement le trafic des autres clients.



Types de VPN

- **VPN d'accès à distance**

- Les VPN d'accès à distance permettent aux utilisateurs distants et mobiles de se connecter en toute sécurité à l'entreprise.
- Les VPN d'accès à distance sont généralement activés dynamiquement par l'utilisateur lorsque cela est nécessaire et peuvent être créés à l'aide d'IPsec ou de SSL.
  - **La Connexion VPN sans client** - La connexion est sécurisée à l'aide d'une connexion SSL par navigateur Web.
  - **La Connexion VPN basée sur le client** - Le logiciel client VPN tel que Cisco AnyConnect Secure Mobility Client doit être installé sur le terminal de l'utilisateur distant.



Remarque : Le type de méthode VPN mis en œuvre est basé sur les exigences d'accès des utilisateurs et les processus informatiques de l'organisation.

Types de VPN

- **SSL VPNs**

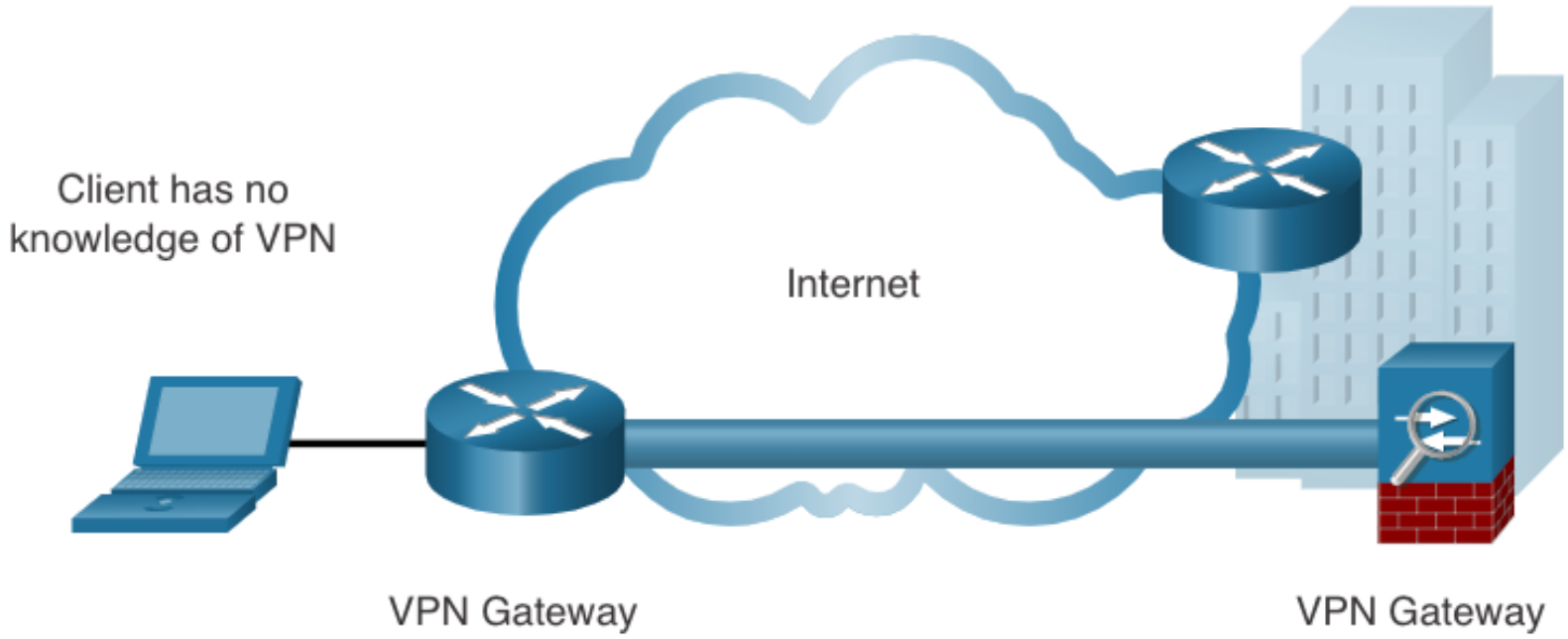
SSL utilise l'infrastructure du clé publique et les certificats numériques pour authentifier les pairs.

Le tableau compare les déploiements d'accès à distance IPsec et SSL.

Fonctionnalité	IPsec	SSL
Application prise en charge	**Vaste** – Toutes les applications basées sur IP	**Limité** – Uniquement les applications Web et le partage de fichiers
Force d'authentification	**Fort** – Authentification bidirectionnelle avec clés partagées ou certificats numériques	**Modéré** - authentification unidirectionnelle ou bidirectionnelle
Force de chiffrement	**Fort** – Longueurs de clé 56-256 bits	**Modéré à fort** - Longueur des clés 40 - 256 bits
Complexité de la connexion	**Moyen** – Nécessite un client VPN installé sur un hôte	**Faible** – Nécessite un navigateur Web sur un hôte
Option de connexion	**Limité** – Seuls les appareils spécifiques avec des configurations spécifiques peuvent se connecter	**Vaste** – Tout appareil peut se connecter avec un navigateur Web

VPN IPSec site à site

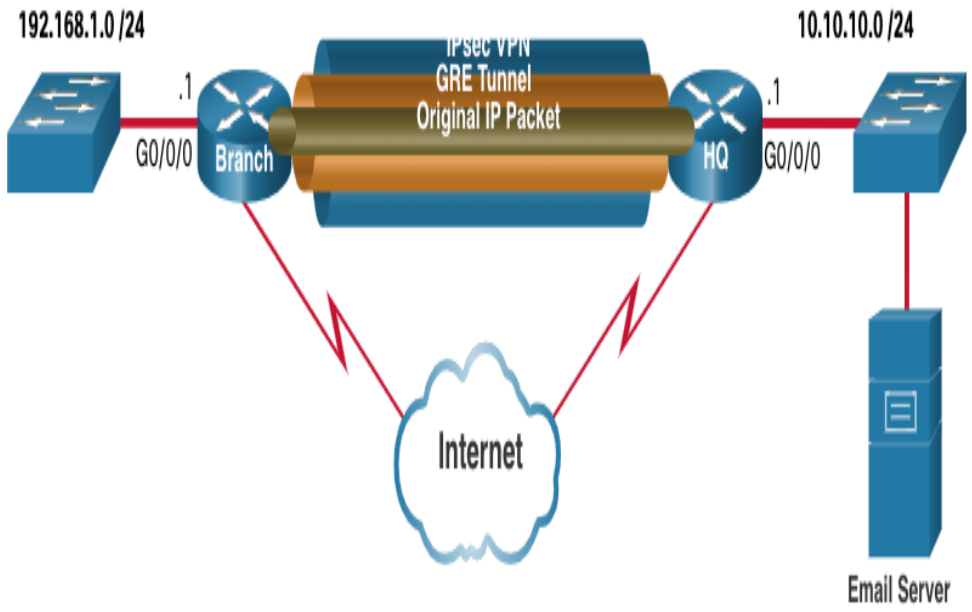
- Les VPN de site à site connectent des réseaux sur un réseau non fiable tel qu'Internet.
- Les hôtes finaux envoient et reçoivent du trafic TCP / IP non chiffré normal via une passerelle VPN.
- La passerelle VPN encapsule et crypte le trafic sortant d'un site et envoie le trafic via le tunnel VPN à la passerelle VPN sur le site cible. La réception de la passerelle VPN élimine les en-têtes, déchiffre le contenu et relaie le paquet vers l'hôte cible au sein de son réseau privé.



Types de VPN

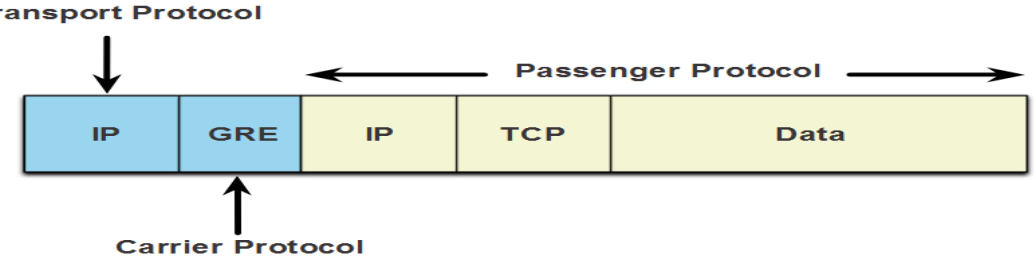
- **GRE sur Ipsec**

- Le protocole GRE (Generic Routing Encapsulation) est un protocole de tunneling VPN de site à site non sécurisé.
- Un tunnel GRE peut encapsuler divers protocoles de couche réseau ainsi que le trafic de multidiffusion et de diffusion.
- GRE ne prend pas en charge le cryptage par défaut; et par conséquent, il ne fournit pas de tunnel VPN sécurisé.
- Un paquet GRE peut être encapsulé dans un paquet IPsec pour le transmettre en toute sécurité à la passerelle VPN de destination.



Les termes utilisés pour décrire l'encapsulation du tunnel GRE sur Ipsec :

- **Protocole passager** - Il est un paquet d'origine qui doit être encapsulé par GRE. Il peut être un paquet IPv4 ou IPv6, d'une mise à jour de routage, etc.
- **Protocole de transporteur** - GRE est le protocole de transporteur qui encapsule le paquet passager d'origine.
- **Protocole de transport** - Il est un protocole qui sera réellement utilisé pour transmettre le paquet. Cela peut être IPv4 ou IPv6.



PARTIE 6

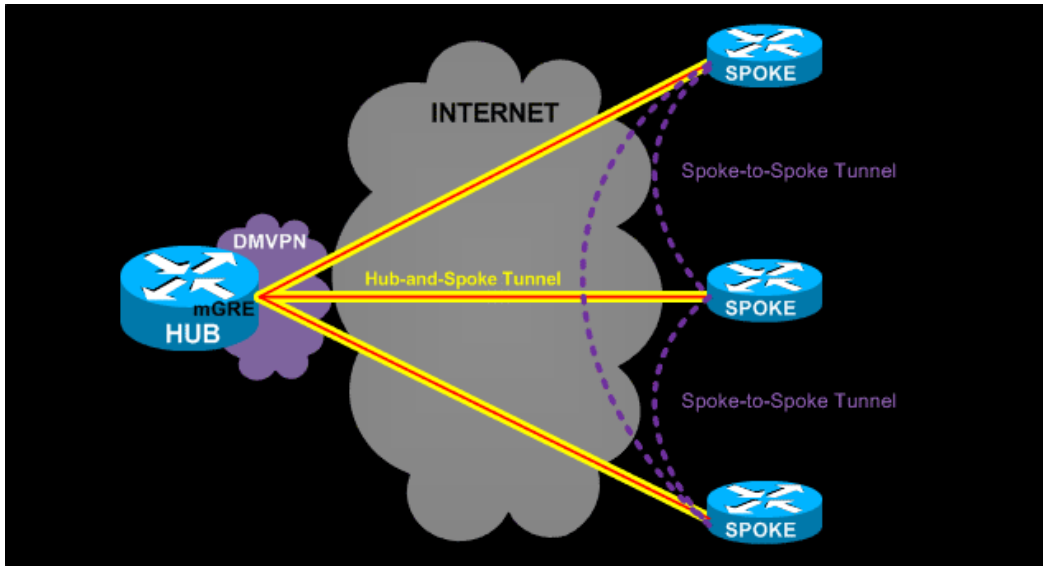
VPN multipoints dynamiques

Les VPN IPsec de site à site et GRE sur IPsec ne sont pas suffisants lorsque l'entreprise ajoute de nombreux autres sites.

DMVPN (Dynamic Multipoint VPN) est une solution logicielle de Cisco qui permet de créer plusieurs VPN de façon simple, dynamique et évolutive.

- DMVPN simplifie la configuration du tunnel VPN et fournit une option flexible pour connecter un site central avec les sites distant.
- Il utilise une configuration concentrateur et rayon pour établir une topologie maillée complète.
- Les sites à rayons établissent des tunnels VPN sécurisés avec le site concentrateur.
- Chaque site est configuré en utilisant Encapsulation de routage générique multipoints (mGRE). L'interface de tunnel GRE permet à une interface GRE unique de prendre en charge dynamiquement plusieurs tunnels IPsec.
- Les sites à rayons peuvent aussi obtenir des informations les uns sur les autres et construire des tunnels directs entre eux (tunnels à rayons).

- DMVPN est un réseau maillé complet de tunnel IPSEC à la demande avec le HUB via un tunnel statique basé sur le protocole de routage (OSPF, EIGRP, RIP, …)
  - MGRE (GRE Multipoint) : Créer les tunnels
  - NHRP (Next Hop Resolution Protocol) : Recherche dynamique de la prochaine IP HUB/SPOKE
  - IPSEC (IP Security) : Chiffrement des données
  - Routage :
    - Underlay : pour la connectivité des adresses IP publiques et le montage des tunnels GRE
    - Overlay : Pour échanger les routes privées une fois le tunnel de montage

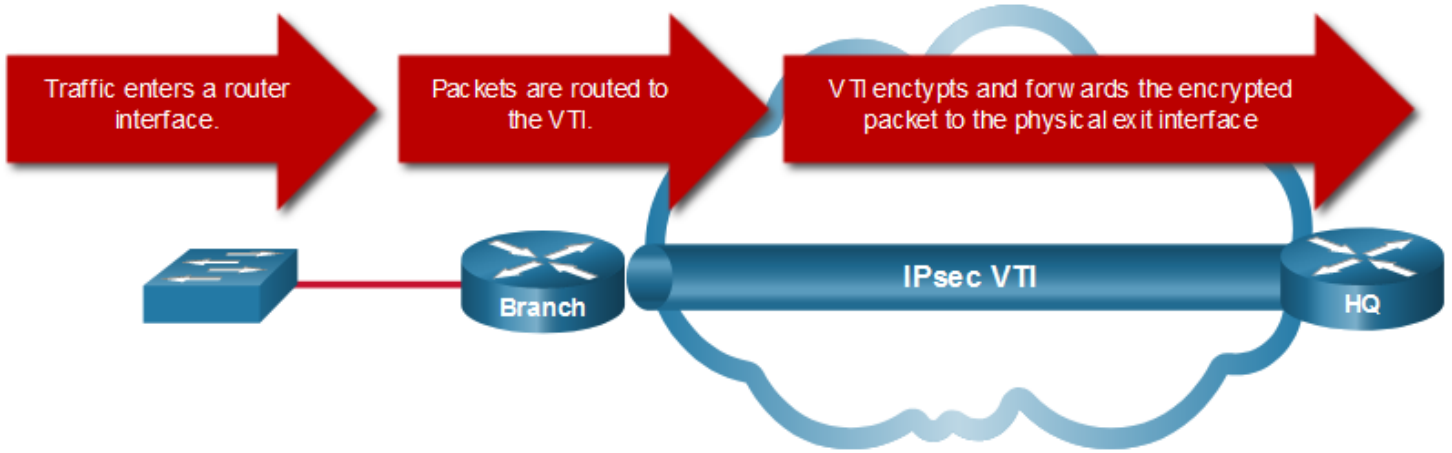


PARTIE 6

L'interface de tunnel virtuel Ipsec

L'interface de tunnel virtuel IPsec (VTI) simplifie le processus de configuration requis pour prendre en charge plusieurs sites et l'accès à distance.

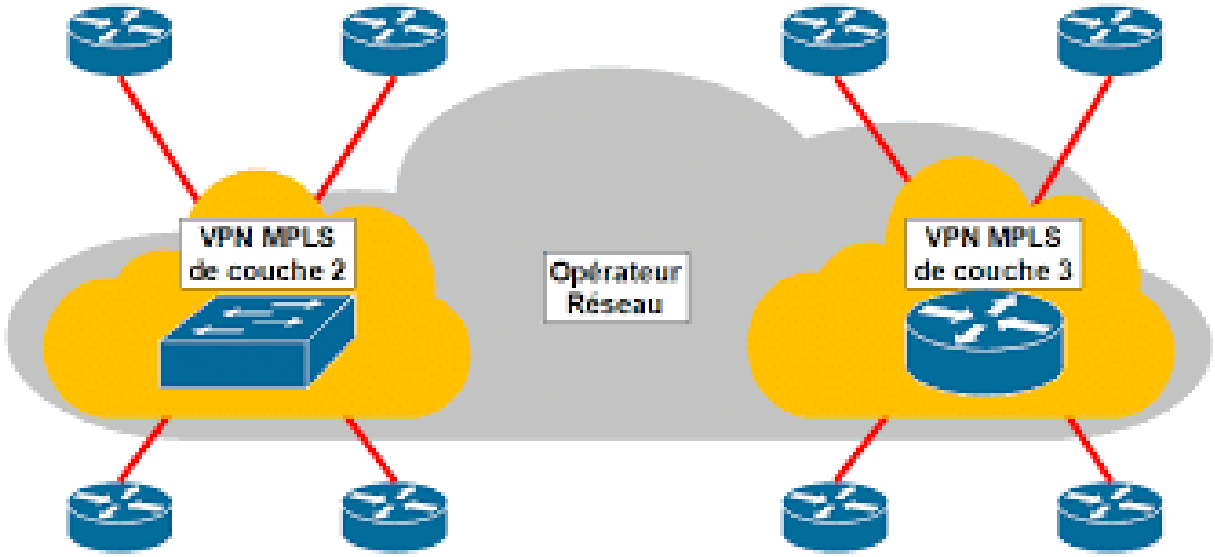
- Les configurations IPsec VTI sont appliquées à une interface virtuelle au lieu du mappage statique des sessions IPsec à une interface physique.
- IPsec VTI est capable d'envoyer et de recevoir le trafic crypté IP unicast et multicast. Par conséquent, les protocoles de routage sont automatiquement pris en charge sans ayant configurer de tunnels GRE.
- IPsec VTI peut être configuré entre les sites ou dans une topologie en étoile (hub-to-spoke).



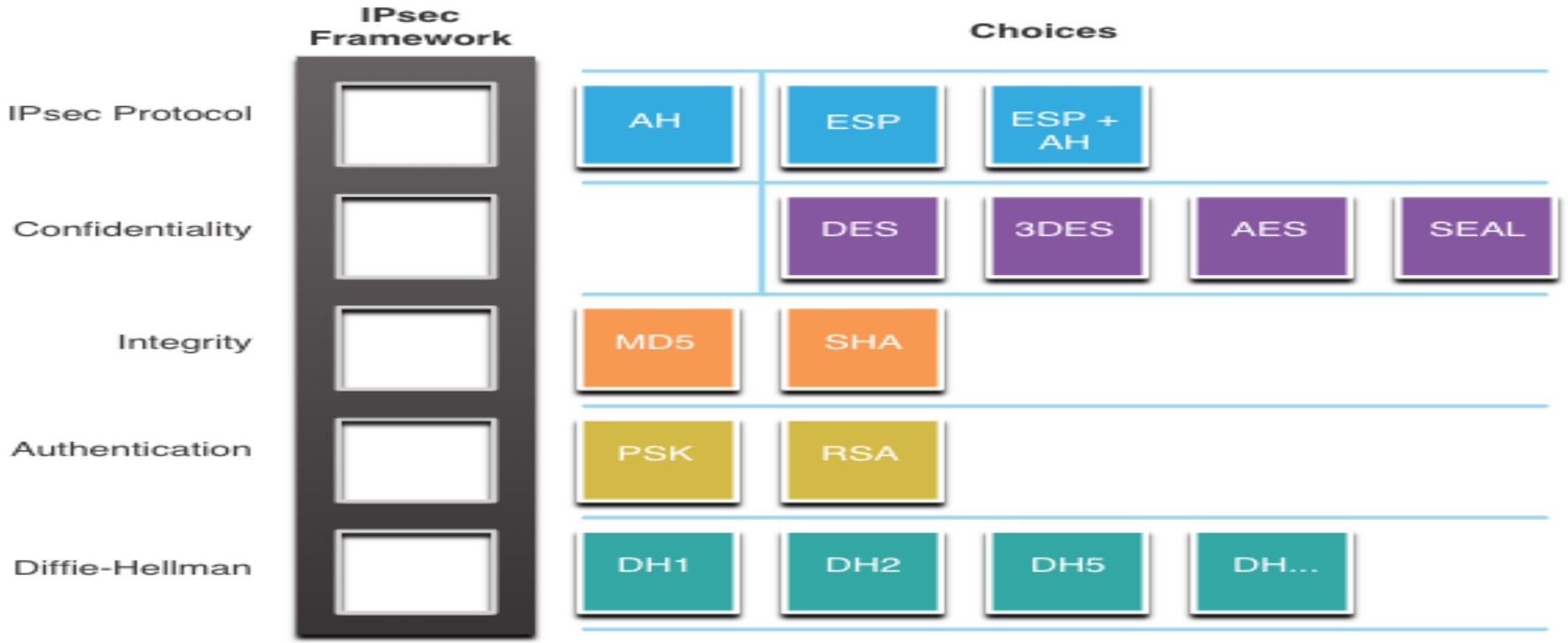
VPN MPLS prestataires de service

Aujourd'hui, les prestataires de services utilisent MPLS dans leur réseau principal. Le trafic est transmis via le réseau principal MPLS à l'aide d'étiquettes. Le trafic est sécurisé car les clients des fournisseurs de services ne peuvent pas voir le trafic de l'autre.

- MPLS peut fournir aux clients des solutions VPN gérées; par conséquent, la sécurisation du trafic entre les sites clients est la responsabilité du prestataire de services.
- Il existe deux types de solutions VPN MPLS prises en charge par les prestataires de services :
  - **VPN MPLS de couche 3** - Le prestataire de services participe au routage client en établissant trunking entre les routeurs du client et les routeurs du prestataire.
  - **VPN MPLS de couche 2**- Le prestataire de services n'est pas impliqué dans le routage du client. Au lieu de cela, le prestataire déploie un service LAN privé virtuel (VPLS) pour émuler un segment LAN multi-accès Ethernet sur le réseau MPLS. Aucun routage n'est impliqué. Les routeurs du client appartiennent effectivement au même réseau à accès multiple.

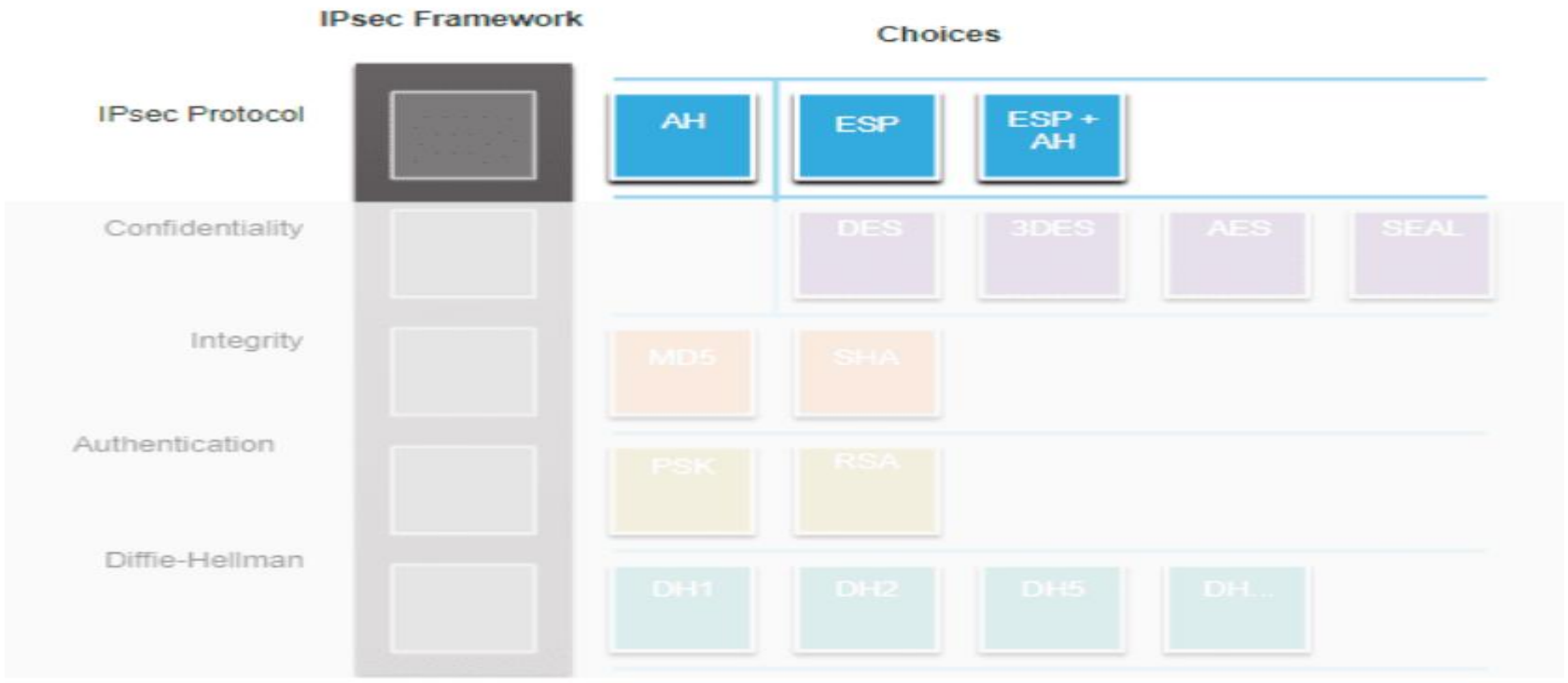


Les Technologies IPSec



Encapsulation du protocole Ipsec

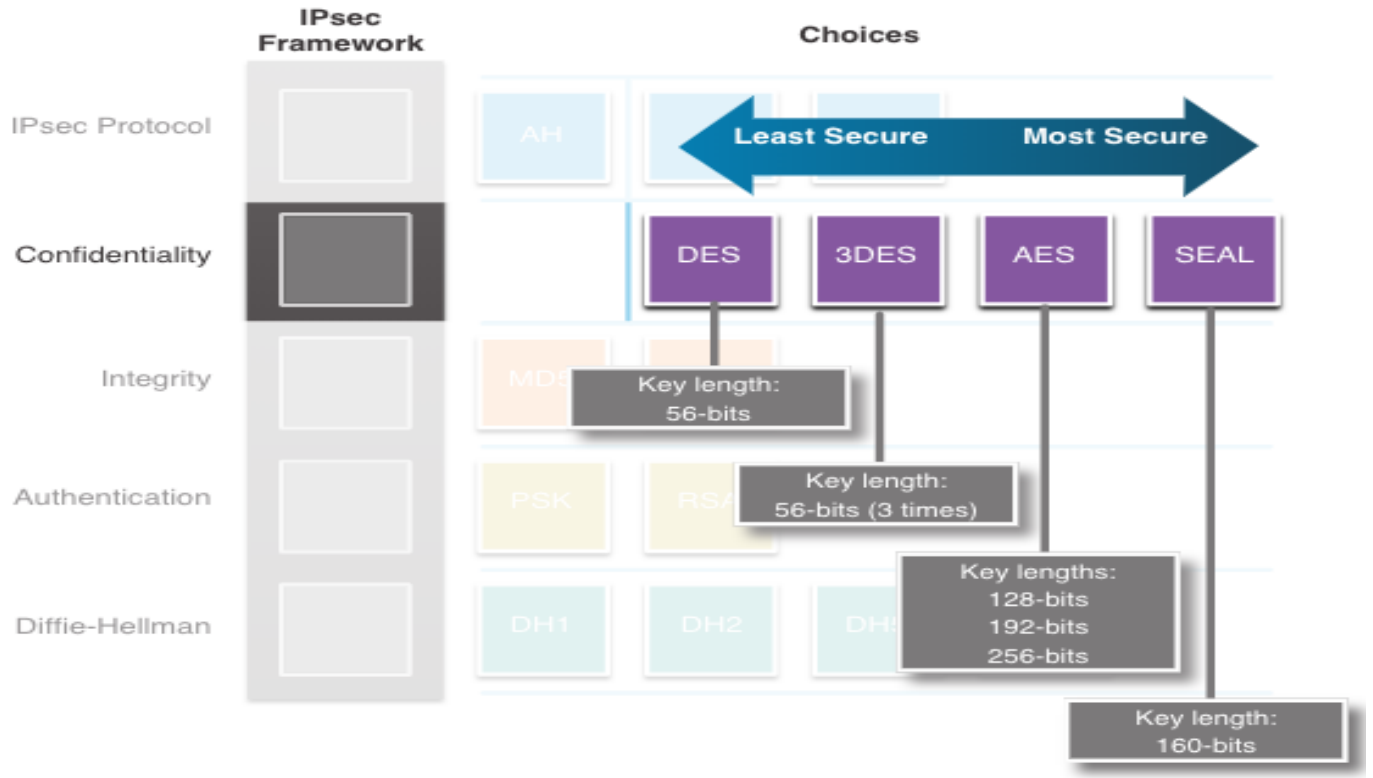
Le choix de l'encapsulation du protocole IPsec est le premier élément principale du structure.



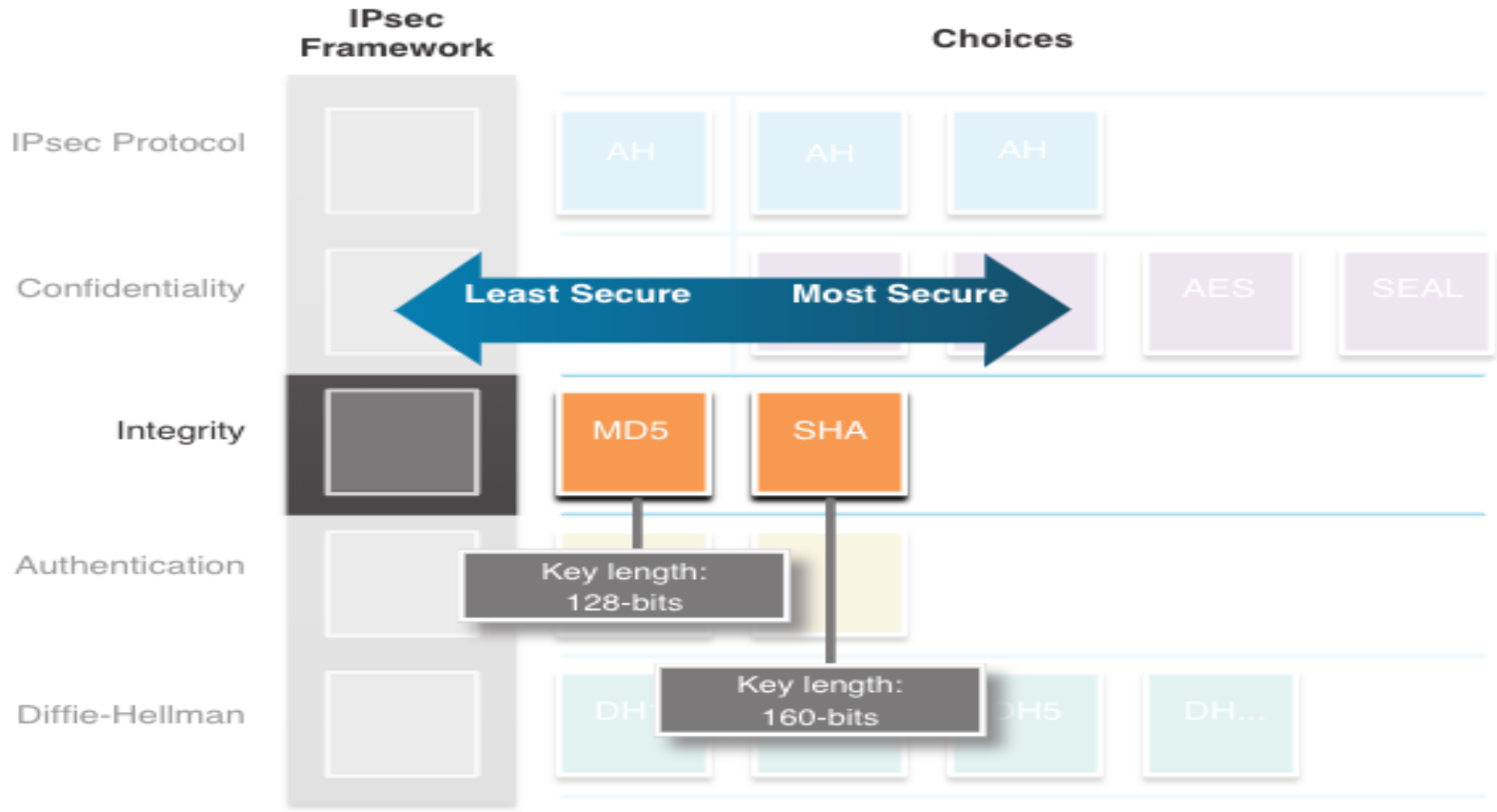
Confidentialité IPSec

Le degré de confidentialité dépend de l'algorithme de cryptage et de la longueur de la clé utilisée dans l'algorithme de cryptage.

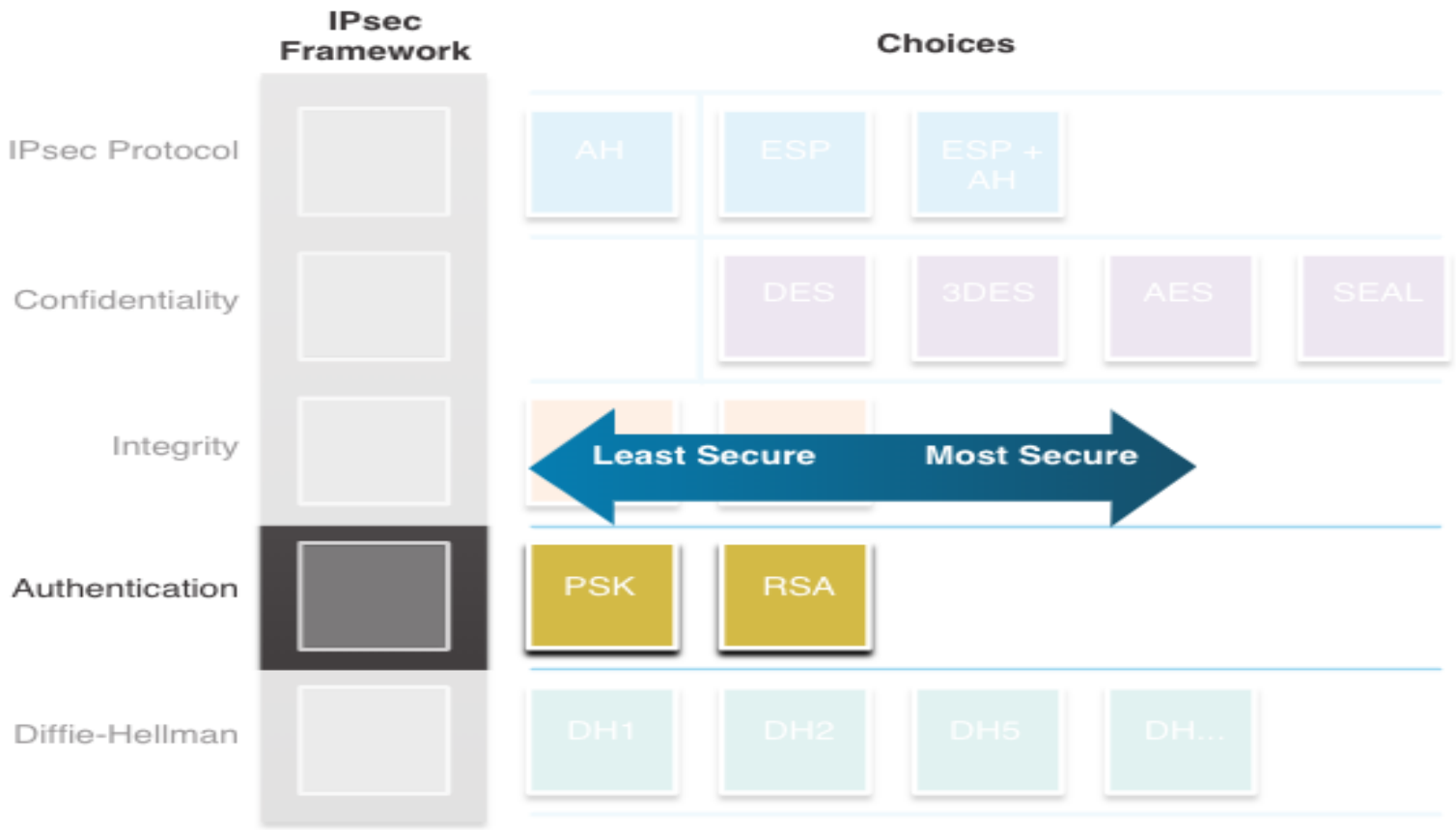
Le nombre de possibilités d'essayer de pirater la clé est fonction de la longueur de la clé - plus la clé est courte, plus il est facile de la casser.



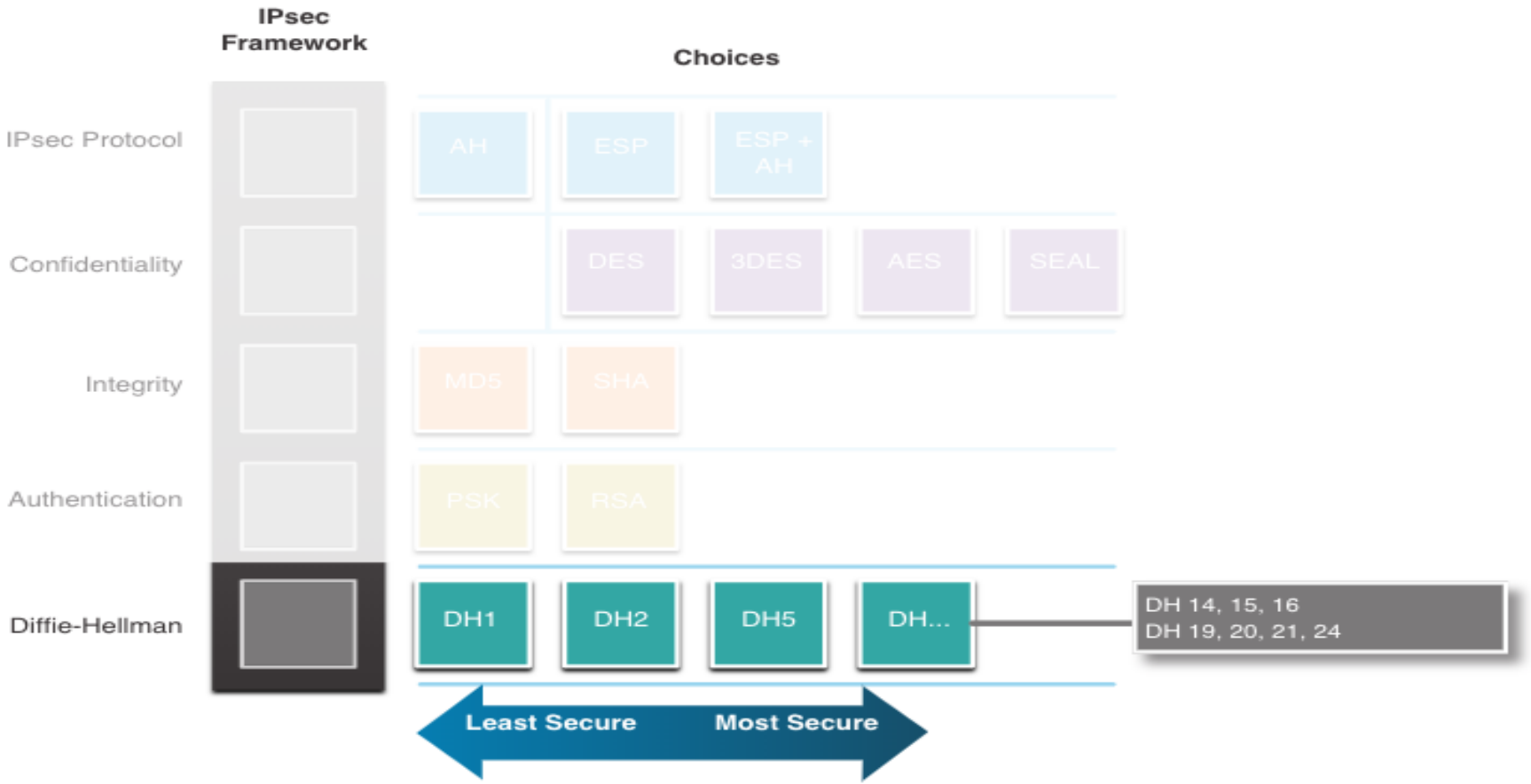
Intégrité IPSec



Authentification Ipsec



Échange de clé sécurisé avec Diffie – Hellman



Procédure de Configuration VPN IPSec site to site

La procédure de configuration comporte six étapes :

1. **Créer une ACL qui identifie le trafic du tunnel.**
2. **Créer une ISAKMP policy pour la IKE SA.**
3. **Configurer une clé partagée pour l'authentification ISAKMP.**
4. **Créer un Transform Set qui indique le mode et les protocoles AH et ESP.**
5. **Créer un Crypto-map qui indique l' ACL, l'adresse du pair et le Transform Set à utiliser.**
6. **On applique le Crypto-map sur l'interafce externe.**

ISAKMP : Internet Security Association Key And Management Protocol (Encryption Key Management)

IKE policy :

- encryption algorithm: **AES 256**
- hash algorithm: **sha1**
- authentication method: **Pre-Shared Key**
- Diffie-Hellman group: **#5**
- SA lifetime : **86400 seconds**

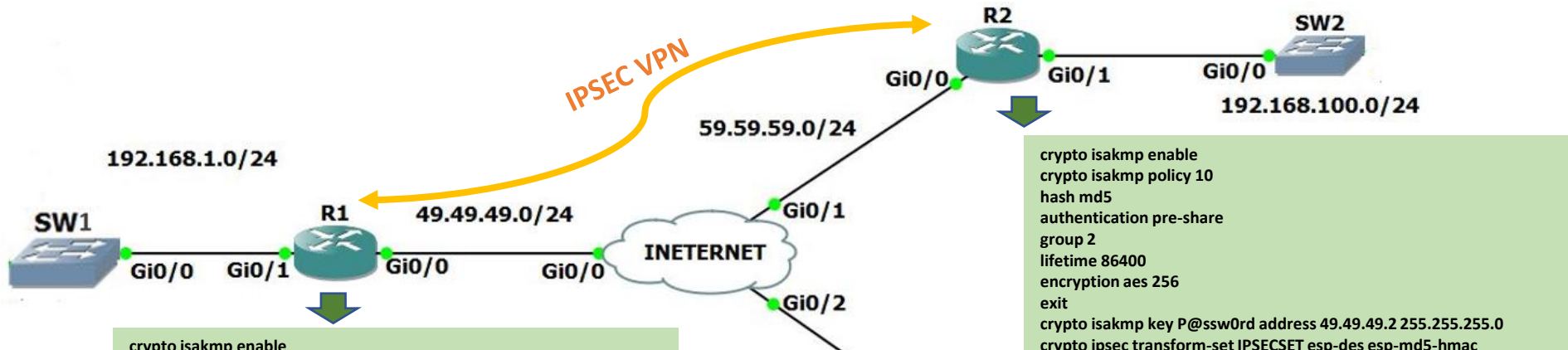
Les valeurs par défault

- encryption algorithm : **DES (56 bits)**
- hash algorithm : **SHA1**
- authentication method : **RSA Signature**
- Diffie-Hellman group : **#1**
- SA lifetime : **86400 seconds**

IPSEC :

- un seul transform-set : **esp-256-aes** et **esp-sha-hmac**

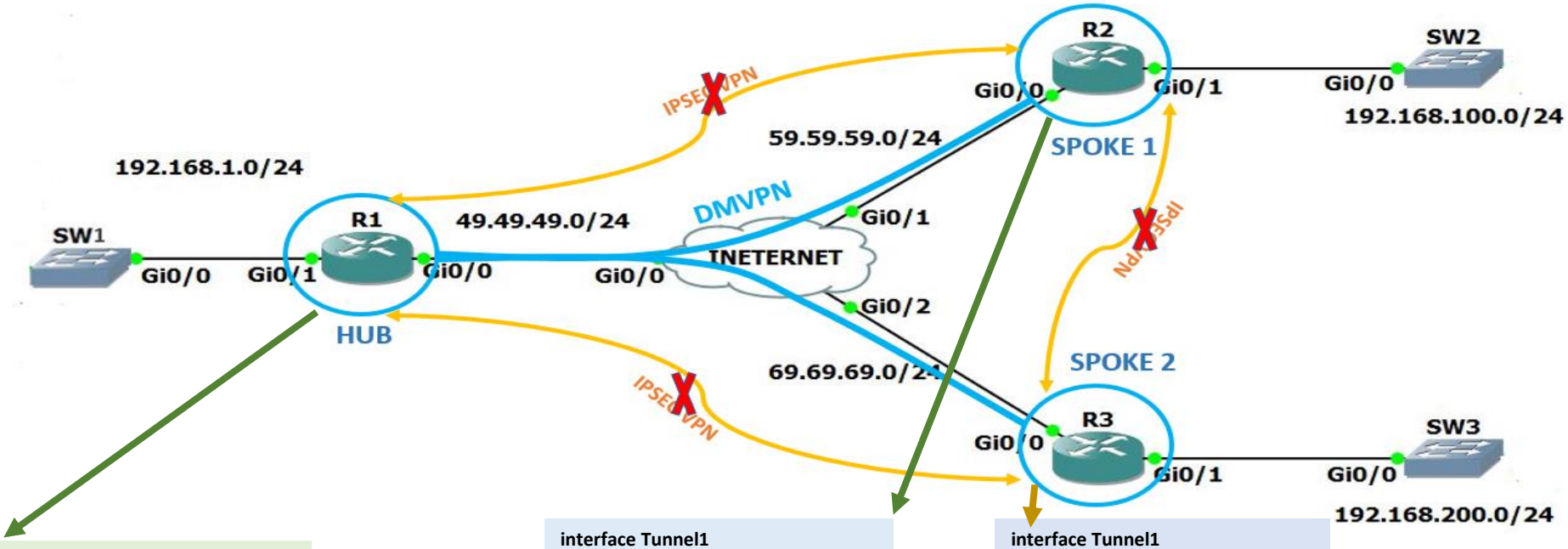
Exemple de Configuration VPN IPSec site to site




```
crypto isakmp enable
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
lifetime 86400
encryption aes 256
exit
crypto isakmp key P@ssw0rd address 59.59.59.2 255.255.255.0
crypto ipsec transform-set IPSECSET esp-des esp-md5-hmac
exit
access-list 101 permit ip 192.168.1.0 0.0.0.255 192.168.100.0 0.0.0.255
crypto map IPSECMAP 10 ipsec-isakmp
set peer 59.59.59.2
set transform-set IPSECSET
match address 101
exit
interface GigabitEthernet0/0
crypto map IPSECMAP
exit
```

```
crypto isakmp enable
crypto isakmp policy 10
hash md5
authentication pre-share
group 2
lifetime 86400
encryption aes 256
exit
crypto isakmp key P@ssw0rd address 49.49.49.2 255.255.255.0
crypto ipsec transform-set IPSECSET esp-des esp-md5-hmac
exit
access-list 101 permit ip 192.168.100.0 0.0.0.255 192.168.1.0 0.0.0.255
crypto map IPSECMAP 10 ipsec-isakmp
set peer 49.49.49.2
set transform-set IPSECSET
match address 101
exit
interface GigabitEthernet0/0
crypto map IPSECMAP
exit
```

Exemple de Configuration DMVPN




```
interface Tunnel1
 no sh
 ip address 12.0.0.1 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp authentication P@ssw0rd
 ip nhrp map multicast dynamic
 ip nhrp network-id 100
 tunnel source 49.49.49.2
 tunnel mode gre multipoint
 exit
```

```
interface Tunnel1
 ip address 12.0.0.3 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp authentication P@ssw0rd
 ip nhrp map 12.0.0.1 49.49.49.2
 ip nhrp map multicast 49.49.49.2
 ip nhrp network-id 100
 ip nhrp nhs 12.0.0.1
 tunnel source 69.69.69.2
 tunnel mode gre multipoint
 exit
```

```
interface Tunnel1
 ip address 12.0.0.2 255.255.255.0
 no ip redirects
 ip mtu 1416
 ip nhrp authentication P@ssw0rd
 ip nhrp map 12.0.0.1 49.49.49.2
 ip nhrp map multicast 49.49.49.2
 ip nhrp network-id 100
 ip nhrp nhs 12.0.0.1
 tunnel source 59.59.59.2
 tunnel mode gre multipoint
 exit
```

CHAPITRE 3

Mettre en place un système de gestion et de supervision des réseaux

Ce que vous allez apprendre dans ce chapitre :

- Adopter des techniques d’optimisation, surveillance et dépannage des réseaux informatiques

3.5 heures

CHAPITRE 3

Mettre en place un système de gestion et de supervision des réseaux

1. Gestion réseau
2. Supervision réseau
3. Dépannage réseau (Network Troubleshooting)

Aperçu du CDP

Le CDP est un protocole de couche 2 propriétaire de Cisco qui est utilisé pour recueillir des informations sur les appareils Cisco qui partagent la même liaison de données. CDP fonctionne indépendamment des supports et protocoles et s'exécute sur tous les périphériques Cisco, tels que routeurs, commutateurs et serveurs d'accès.

Le périphérique envoie des annonces CDP périodiques aux périphériques connectés. Ces annonces partagent des informations sur le type de périphérique détecté, le nom des périphériques, ainsi que le nombre et le type d'interfaces.

Configurer et vérifier le CDP

- Pour les périphériques Cisco, le protocole CDP est activé par défaut. Pour vérifier le statut du CDP et afficher des informations sur la CDP, entrez la commande **show cdp** .
- Pour désactiver le CDP sur une interface spécifique, saisissez **no cdp enable** dans le mode de configuration de l'interface. Le protocole CDP est toujours activé sur le périphérique; cependant, il n'envoie aucune annonce CDP via cette interface. Pour réactiver le CDP sur l'interface spécifique, saisissez **cdp enable.**
- Pour activer CDP globalement pour toutes les interfaces prises en charge sur le périphérique, saisissez **cdp run** comme mode de configuration globale. Le CDP peut être désactivé pour toutes les interfaces de l'appareil avec la commande **no cdp run** en mode de configuration globale.
- Utilisez la commande **show cdp interface** pour afficher les interfaces compatibles CDP d'un périphérique. L'état de chaque interface est également affiché.

Découvrir des appareils en utilisant le CDP

- Lorsque la CDP est activée sur le réseau, la commande **show cdp neighbors** peut être utilisée pour déterminer la configuration du réseau.
- On utilise la commande **show cdp neighbors detail** pour découvrir l'adresse IP du périphériques voisins.

Aperçu du LLDP

Le protocole LLDP (Link Layer Discovery Protocol) est un protocole de détection voisin ouvert semblable au protocole CDP. LLDP fonctionne avec des périphériques réseau, tels que des routeurs, des commutateurs et des points d'accès LAN sans fil. Ce protocole fait connaître son identité et ses capacités à d'autres appareils et reçoit les informations d'un appareil de couche 2 physiquement connecté.

Configurer et vérifier le LLDP

- Le LLDP peut être activé par défaut. Pour activer LLDP globalement sur un appareil réseau Cisco, saisissez la commande **lldp run** en mode de configuration globale. Pour désactiver le protocole LLDP, entrez la commande **no lldp run** en mode de configuration globale.
- LLDP peut être configuré sur des interfaces spécifiques. Cependant, le LLDP doit être configuré séparément pour transmettre et recevoir des paquets LLDP.
- Pour vérifier si le protocole LLDP a été activé sur le périphérique, entrez la commande **show lldp** en mode d'exécution privilégié.

Découvrir des périphériques en utilisant le LLDP

- Lorsque le protocole LLDP est activé, les voisins de l'appareil peuvent être détectés à l'aide de la commande **show lldp neighbors**.
- Pour plus d'informations sur les voisins, utilisez la commande **show lldp neighbors detail** qui permet d'obtenir la version IOS et l'adresse IP des voisins ainsi que la capacité de l'appareil.

Services de temps et de calendrier

- En règle générale, les paramètres de la date et de l'heure sur un routeur ou un commutateur peuvent être définis en utilisant l'une des deux méthodes suivantes :

- **Configurer manuellement la date et l'heure**

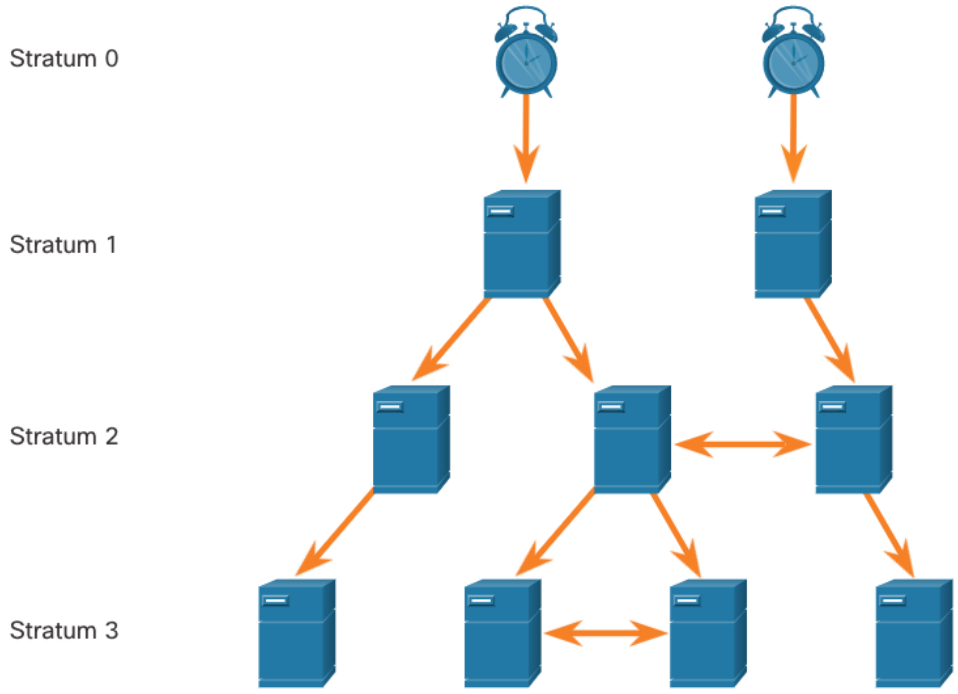
```
R1# clock set 20:36:00 nov 15 2019
R1#
*Nov 15 20:36:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 21:32:31
UTC Fri Nov 15 2019 to 20:36:00 UTC Fri Nov 15 2019, configured from console by console.
```

- **Configurer le Network Time Protocol (NTP)**

- À mesure qu'un réseau se développe, il devient difficile de s'assurer que tous les appareils de l'infrastructure fonctionnent avec un temps synchronisé en utilisant la méthode manuelle.
- La meilleure solution consiste à configurer le protocole NTP sur le réseau.
- Ce protocole permet aux routeurs du réseau de synchroniser leurs paramètres de temps avec un serveur NTP, qui fournit des paramètres de temps plus cohérents.
- Le NTP peut être configuré pour se synchroniser avec une horloge maîtresse privée, ou il peut se synchroniser avec un serveur NTP accessible au public sur l'internet.
- Le protocole NTP utilise le port UDP 123 et est décrit dans le document RFC 1305.

Opération NTP

- Les réseaux NTP utilisent un système de sources temporelles hiérarchique.
- Chaque niveau de ce système hiérarchique est appelé strate.
- Le niveau de strate correspond au nombre de sauts à partir de la source faisant autorité.
- Le temps synchronisé est distribué à travers le réseau en utilisant NTP.
- Le nombre de sauts maximal est de 15. La strate 16, le niveau de strate le plus bas, indique qu'un périphérique n'est pas synchronisé.
- **Strate 0:** Ces sources de temps faisant autorité sont des dispositifs de chronométrage de haute précision supposés être précis et associés à peu ou pas de retard.
- **Strate 1:** Dispositifs directement connectés aux sources de temps faisant autorité. Ils représentent la principale référence temporelle du réseau.
- **Strate 2 et inférieure:** les serveurs de la strate 2 sont connectés aux appareils de la strate 1 par des connexions réseau. Les périphériques de strate 2, tels que les clients NTP, synchronisent leur horloge à l'aide des paquets NTP des serveurs de la strate 1. Ils peuvent également servir de serveurs pour les périphériques de la strate 3.
- Les serveurs temporels de même niveau de strate peuvent être configurés de manière à agir en tant qu'homologues avec d'autres serveurs temporels de la même strate en vue de la sauvegarde ou de la vérification de l'heure.



PARTIE 6

PARTIE 6

Configurer et vérifier le NTP

- Avant que NTP ne soit configuré sur le réseau, la commande **show clock** affiche l'heure actuelle sur l'horloge du logiciel.
- La commande **ntp server** *ip-address* est émise en mode de configuration globale pour configurer le *ip-address* comme serveur NTP pour ce Routeur.
- Pour vérifier si la source temporelle est définie sur NTP, utilisez à nouveau la commande **show clock detail**.
- Les commandes **show ntp associations** and **show ntp status** sont utilisées pour vérifier que le Routeur est synchronisé avec le serveur NTP.

```
R1# show clock detail
20:55:10 .207 UTC ven jun. 15 2022
Time source is user configuration
R1# config t
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34 .563 UTC ven. jun. 15 2022
Time source is NTP
R1# show ntp associations
address ref clock st when poll each delay offset disp
*~209.165.200.225 .GPS.                    1 61 64 377 0.481 7.480 4.261
• sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**22(output omitted)
```

PARTIE 6

Systèmes de fichiers de routeurs

```
Router# show file systems
File Systems:
      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw   system:
            -             -    opaque     rw   tmpsys:
*   7194652672    6294822912      disk     rw   bootflash: flash:
    256589824     256573440      disk     rw   usb0:
   1804468224    1723789312      disk     ro   webui:
            -             -    opaque     rw   null:
            -             -    opaque     ro   tar:
            -             -   network     rw   tftp:
            -             -    opaque     wo   syslog:
     33554432      33539983     nvram     rw   nvram:
            -             -   network     rw   rcp:
            -             -   network     rw   ftp:
            -             -   network     rw   http:
            -             -   network     rw   scp:
            -             -   network     rw   sftp:
            -             -   network     rw   https:
            -             -    opaque     ro   cns:
Router#
```

```
Router# dir
Directory of bootflash:/
   11  drwx           16384   Aug 2 2019 04:15:13 +00:00  lost+found
370945  drwx            4096   Oct 3 2019 15:12:10 +00:00  .installer
338689  drwx            4096   Aug 2 2019 04:15:55 +00:00  .ssh
217729  drwx            4096   Aug 2 2019 04:17:59 +00:00  core
379009  drwx            4096  Sep 26 2019 15:54:10 +00:00  .prst_sync
80641  drwx             4096   Aug 2 2019 04:16:09 +00:00  .rollback_timer
161281  drwx            4096   Aug 2 2019 04:16:11 +00:00  gs_script
112897  drwx          102400   Oct 3 2019 15:23:07 +00:00  tracelogs
362881  drwx            4096  Aug 23 2019 17:19:54 +00:00  .dbpersist
298369  drwx            4096   Aug 2 2019 04:16:41 +00:00  virtual-instance
   12  -rw-               30   Oct 3 2019 15:14:11 +00:00  throughput_monitor_params
 8065  drwx            4096   Aug 2 2019 04:17:55 +00:00  onep
   13  -rw-               34   Oct 3 2019 15:19:30 +00:00  pnp-tech-time
249985  drwx            4096  Aug 20 2019 17:40:11 +00:00  Archives
   14  -rw-            65037   Oct 3 2019 15:19:42 +00:00  pnp-tech-discovery-summary
   17  -rw-          5032908  Sep 19 2019 14:16:23 +00:00
isr4200_4300_rommon_1612_1r_SPA.pkg
   18  -rw-        517153193  Sep 21 2019 04:24:04 +00:00  isr4200-
universalk9_ias.16.09.04.SPA.bin
7194652672 bytes total (6294822912 bytes free)
Router#
```

```
Router#
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/
32769  -rw-            1024                    startup-config
32770  ----              61                    private-config
32771  -rw-            1024                    underlying-config
    1  ----               4                    private-KS1
    2  -rw-            2945                    cwmp_inventory
    5  ----             447                    persistent-data
    6  -rw-            1237                    ISR4221-2x1GE_0_0_0
    8  -rw-              17                    ecfm_ieee_mib
    9  -rw-               0                    ifIndex-table
   10  -rw-            1431                    NIM-2T_0_1_0
   12  -rw-             820                    IOS-Self-Sig#1.cer
   13  -rw-             820                    IOS-Self-Sig#2.cer
33554432 bytes total (33539983 bytes free)
Router#
```

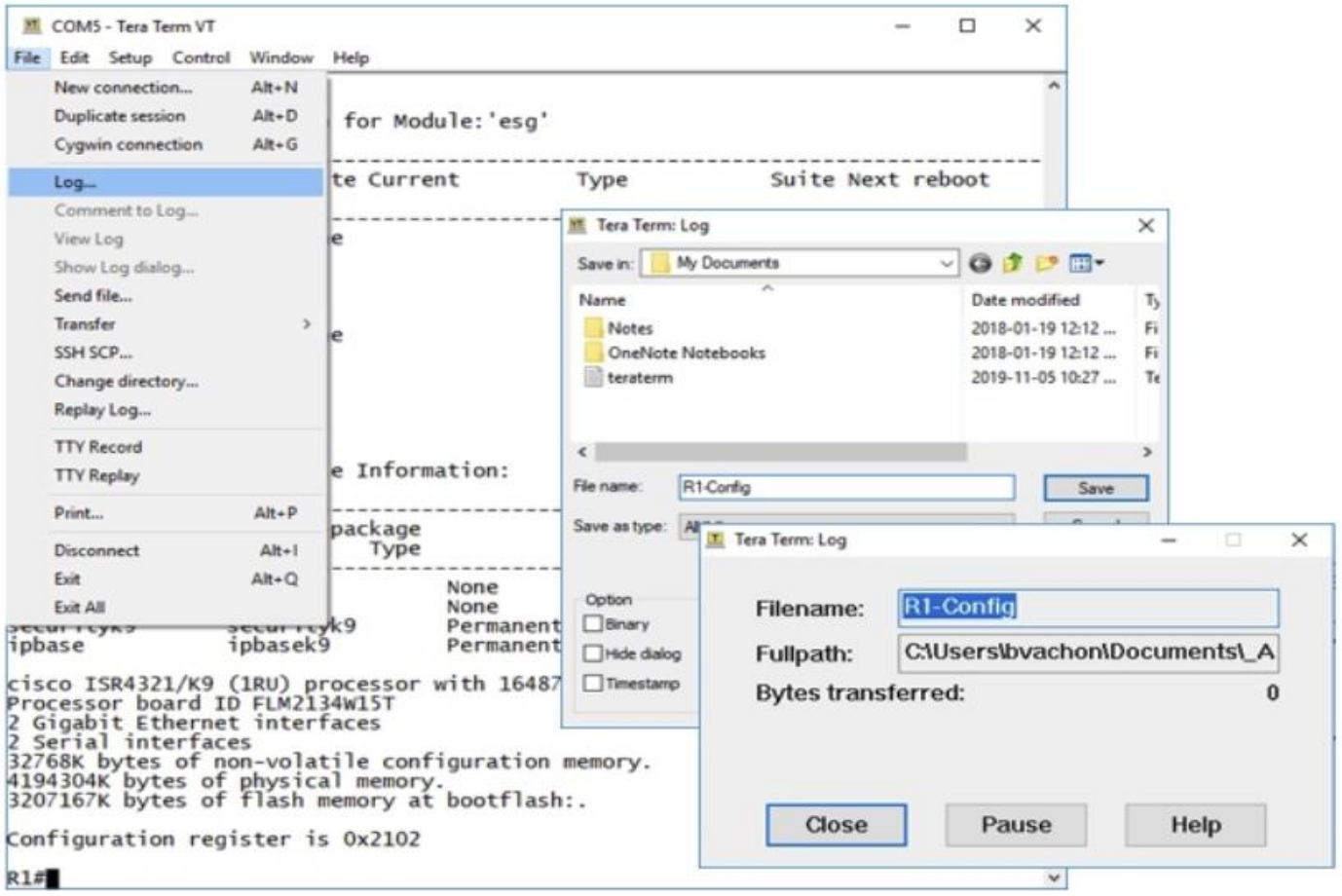
Systèmes de fichiers de commutateur

```
Switch# show file systems
File Systems:
       Size(b)     Free(b)      Type  Flags  Prefixes
*     32514048    20887552     flash     rw    flash:
           -           -      opaque     rw       vb:
           -           -      opaque     ro       bs:
           -           -      opaque     rw   system:
           -           -      opaque     rw   tmpsys:
       65536       48897       nvram     rw    nvram:
           -           -      opaque     ro   xmodem:
           -           -      opaque     ro   ymodem:
           -           -      opaque     rw     null:
           -           -      opaque     ro      tar:
           -           -     network     rw     tftp:
           -           -     network     rw      rcp:
           -           -     network     rw     http:
           -           -     network     rw      ftp:
           -           -     network     rw      scp:
           -           -     network     rw    https:
           -           -      opaque     ro      cns:
Switch#
```

PARTIE 6

Utiliser un fichier texte pour sauvegarder une configuration

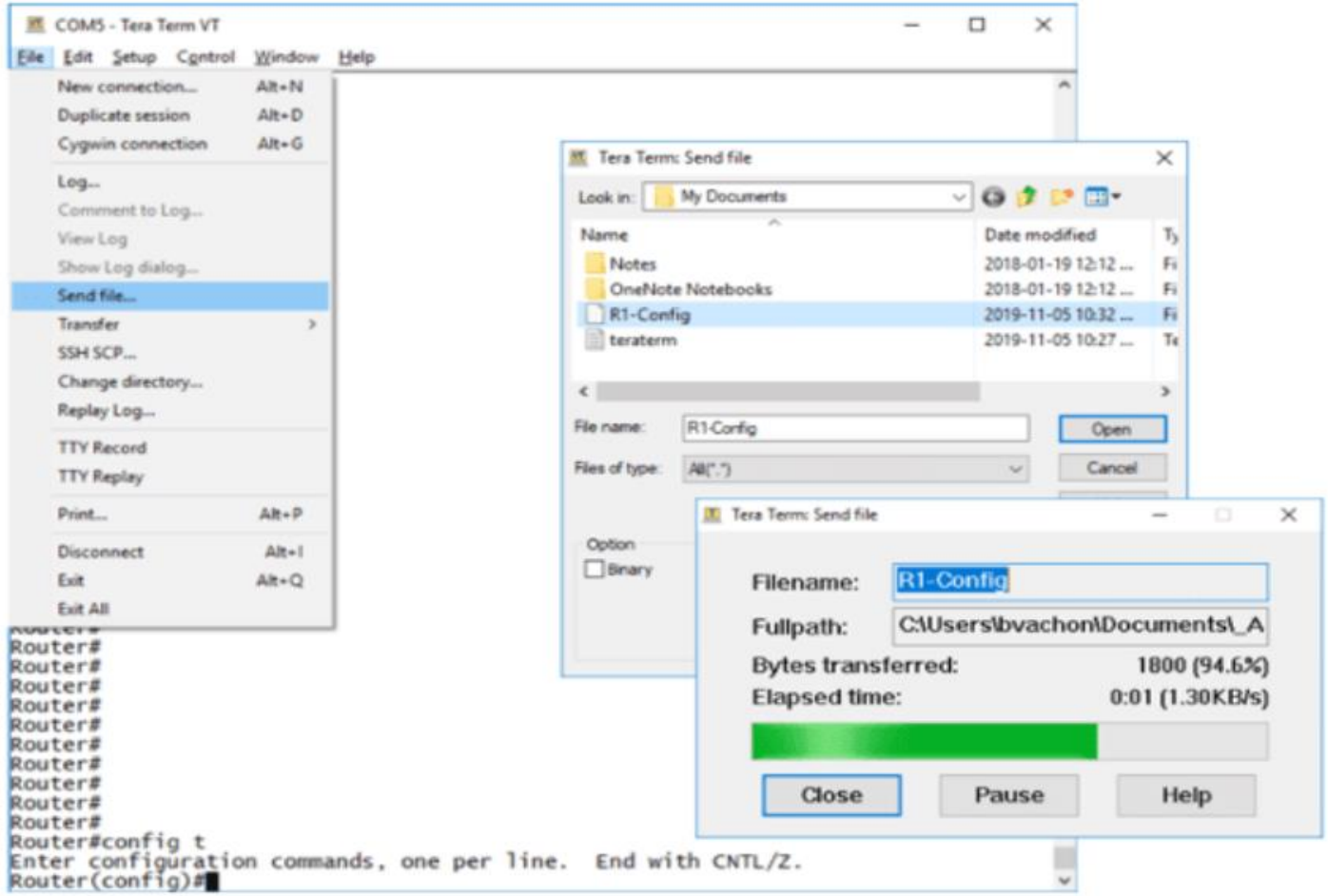
Les fichiers de configuration peuvent être enregistrés dans un fichier texte en utilisant Tera Term :



PARTIE 6

Utiliser un fichier texte pour restaurer une configuration

Au lieu de copier et coller, une configuration peut être restaurée à partir d'un fichier texte à l'aide de Tera Term.



Utilisation de serveur TFTP pour sauvegarder et restaurer une configuration

Procédez comme suit pour sauvegarder la configuration en cours sur un serveur TFTP:

Étape 1. Saisissez la commande **copy running-config tftp** .

Étape 2. Entrez l'adresse IP de l'hôte sur lequel le fichier de configuration sera stocké.

Étape 3. Entrez le nom à attribuer au fichier de configuration.

Étape 4. Appuyez sur Entrée pour confirmer chaque choix.

```
R1# copy running-config tftp
Remote host []?192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jun-2022
Write file R1-Jun-2022 to 192.168.10.254? [confirm]
Writing R1-Jun-2022 !!!!!! [OK]
```

Procédez comme suit pour restaurer la configuration en cours à partir d'un serveur TFTP:

Étape 1. Saisissez la commande **copy tftp running-config** .

Étape 2. Saisissez l'adresse IP de l'hôte sur lequel le fichier de configuration est stocké.

Étape 3. Entrez le nom à attribuer au fichier de configuration.

Étape 4. Appuyez sur **Enter** pour confirmer chaque choix.

```
R1# copy tftp: startup-config
Remote host []?192.168.10.254
Source filename []? R1-Jun-2022
Destination filename [startup-config]?

Accessing tftp://192.168.10.254/R1-Jun-2022…
Loading R1-Jun-2022 from 192.168.10.254 : !
[OK - 745 bytes]

745 bytes copied in 0 secs
```

Utilisation de l'USB pour sauvegarder et restaurer une configuration

- La fonction Flash USB fournit une capacité de stockage secondaire en option et un périphérique d'amorçage supplémentaire.

- Exécutez la commande **show file systems** pour vérifier que le lecteur USB est là et confirmer son nom.
- Utilisez la commande **copy run usb_name/** pour copier le fichier de configuration vers la clé USB.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Avertissement : Il existe déjà un fichier portant ce nom
Vous voulez sur-écrire ? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
R1#
```

- Pour restaurer les configurations avec une clé USB, il sera nécessaire de modifier le fichier USB R1-Config avec un éditeur de texte. En partant du principe que le nom de fichier est **R1-Config**, utilisez la commande **copy usbflash0:/R1-Config *running-config*** pour rétablir une configuration en cours.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
R1#
```

PARTIE 6

PARTIE 6

Procédures de récupération des mots de passe

- Les mots de passe des périphériques permettent d'empêcher les accès non autorisés. Les mots de passe chiffrés, tels que les mots de passe secrets chiffrés, doivent être remplacés après la récupération. Selon l'appareil, la procédure détaillée de récupération de mot de passe varie.
- Cependant, toutes les procédures de récupération des mots de passe pour les périphériques Cisco suivent le même principe:

Étape 1. Activez le mode ROMMON.

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

Étape 2. Modifiez le registre de configuration.

```
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

Étape 3. Copiez la configuration de démarrage dans la configuration d'exécution.

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#
```

Étape 4. changer le mot de passe.

```
R1# configure terminal
Entrez les commandes de configuration, une par ligne. End with
CNTL/Z.
R1(config)# enable secret cisco
```

Étape 5. Enregistrez le running-config comme nouveau startup-config.

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]? Building
configuration... [OK]
R1#
```

Sauvegarde d'une image IOS sur un serveur TFTP

Pour gérer les opérations réseau avec un temps d'indisponibilité minimum, il est nécessaire de mettre en place des procédures de sauvegarde des images Cisco IOS. Ainsi, l'administrateur réseau peut rapidement copier une image sur un routeur en cas d'image corrompue ou effacée.

Procédez comme suit :

Étape 1. Envoyez une requête ping au serveur TFTP. Ping sur le serveur TFTP pour tester la connectivité.

Étape 2. Vérifiez la taille de l'image en flash. Vérifiez que le serveur TFTP possède un espace disque suffisant pour accueillir l'image du logiciel Cisco IOS. Utilisez la commande **show flash0:** sur le routeur pour déterminer la taille du fichier image Cisco IOS.

Étape 3. Copiez l'image sur le serveur TFTP Copiez l'image sur le serveur TFTP en utilisant la commande **copy** *source-url destination-url* . Une fois la commande exécutée à l'aide des URL source et de destination spécifiées, l'utilisateur est invité à indiquer le nom du fichier source, l'adresse IP de l'hôte distant et le nom du fichier de destination. Le transfert commence.

```
R1# copy tftp: flash:
Address or name of remote host []? 2001:DB8:CAFE:100::99
Source filename []? isr4200-universalk9_ias.16.09.04.SPA.bin
Destination filename [isr4200-universalk9_ias.16.09.04.SPA.bin]?
Accessing tftp://2001:DB8:CAFE:100::99/ isr4200- universalk9_ias.16.09.04.SPA.bin... Loading isr4200-
universalk9_ias.16.09.04.SPA.bin from 2001:DB8:CAFE:100::99 (via GigabitEthernet0/0/0): !!!!!!!!!!!!!!!!!!!
[OK - 517153193 bytes]
517153193 bytes copied in 868.128 secs (265652 bytes/sec)
```

Copie d'une image de l'IOS sur un appareil

- **Étape 1. Envoyez une requête ping au serveur TFTP.** Ping sur le serveur TFTP pour tester la connectivité.
- **Étape 2. Vérifiez la quantité de flash libre.** Assurez-vous qu'il y a suffisamment d'espace de flash sur l'appareil mis à niveau en utilisant la commande **show flash:** Comparez l'espace de mémoire Flash disponible avec la nouvelle taille du fichier d'image.
- **Étape 3.** Copiez le fichier image IOS du serveur TFTP vers le routeur en utilisant la commande **copy tftp: flash:** Une fois la commande exécutée à l'aide des URL source et de destination spécifiées, l'utilisateur est invité à indiquer l'adresse IP de l'hôte distant, le nom du fichier source et le nom du fichier de destination.

```
R1# copy tftp: flash:
Address or name of remote host []?2001:DB8:CAFE:100::99
Source filename []? isr4200-universalk9_ias.16.09.04.SPA.bin
Destination filename [isr4200-universalk9_ias.16.09.04.SPA.bin]?
Accessing tftp://2001:DB8:CAFE:100::99/ isr4200- universalk9_ias.16.09.04.SPA.bin... Loading isr4200-
universalk9_ias.16.09.04.SPA.bin from 2001:DB8:CAFE:100::99 (via GigabitEthernet0/0/0) !!!!!!!!!!!!!!!!!!!
[OK - 517153193 bytes]
517153193 bytes copied in 868.128 secs (265652 bytes/sec)
```

La commande boot system

- Au démarrage, le code d'amorçage analyse le fichier de configuration de démarrage dans la NVRAM pour les commandes **boot system** qui spécifient le nom et l'emplacement de l'image du logiciel Cisco IOS à charger. Plusieurs commandes **boot system** peuvent être saisies successivement pour créer un plan d'amorçage à tolérance de panne.
- En l'absence de commandes **boot system** dans la configuration, le routeur charge par défaut la première image Cisco IOS valide dans la mémoire Flash et l'exécute.
- Pour passer à l'image IOS copiée après que cette image ait été enregistrée sur la mémoire flash du routeur, configurez le routeur pour qu'il charge la nouvelle image au démarrage en utilisant la commande **boot system** Enregistrez la configuration. Redémarrez le routeur pour qu'il démarre avec la nouvelle image.

```
R1# configure terminal
R1(config)# boot system flash0:isr4200-universalk9_ias.16.09.04.SPA.bin
R1(config)# exit
R1# copy running-config startup-config
R1# reload
```

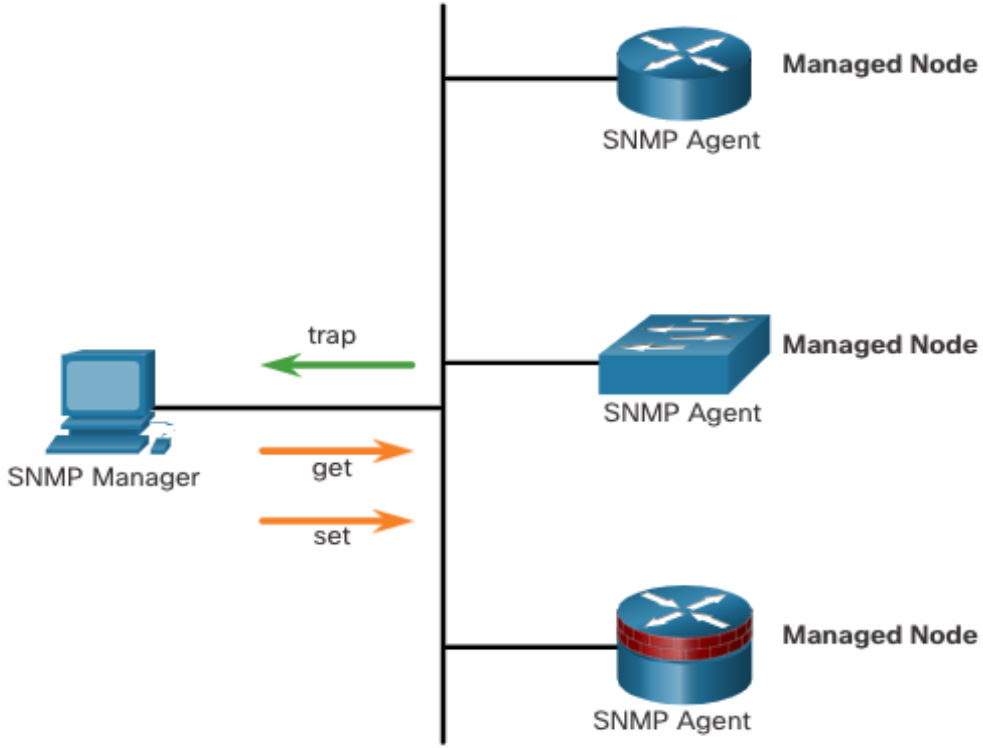
CHAPITRE 3

Mettre en place un système de gestion et de supervision des réseaux

1. Gestion réseau
2. Supervision réseau
3. Dépannage réseau (Network Troubleshooting)

Introduction au SNMP

- Le protocole SNMP permet aux administrateurs de gérer les périphériques sur un réseau IP. Ces derniers peuvent ainsi contrôler et gérer les performances du réseau, identifier et résoudre les problèmes et anticiper la croissance du réseau.
- SNMP est un protocole de couche Application qui procure un format pour les messages de communication entre les gestionnaires et les agents. Le système SNMP se compose de trois éléments :
  - Gestionnaire SNMP
  - Agents SNMP (nœud géré)
  - Base d'informations de gestion (MIB)
- Le gestionnaire SNMP interroge les agents et envoie des requêtes à la base de données MIB des agents sur le port UDP 161. Les agents SNMP envoient les déroutements SNMP au gestionnaire SNMP sur le port UDP 162.
- L'agent SNMP et la base de données MIB sont présents sur tous les périphériques client SNMP.
- Les MIB contiennent les données relatives aux périphériques et à leur fonctionnement. Elles peuvent être consultées par tout utilisateur distant authentifié. C'est l'agent SNMP qui est chargé de fournir l'accès à la MIB locale.

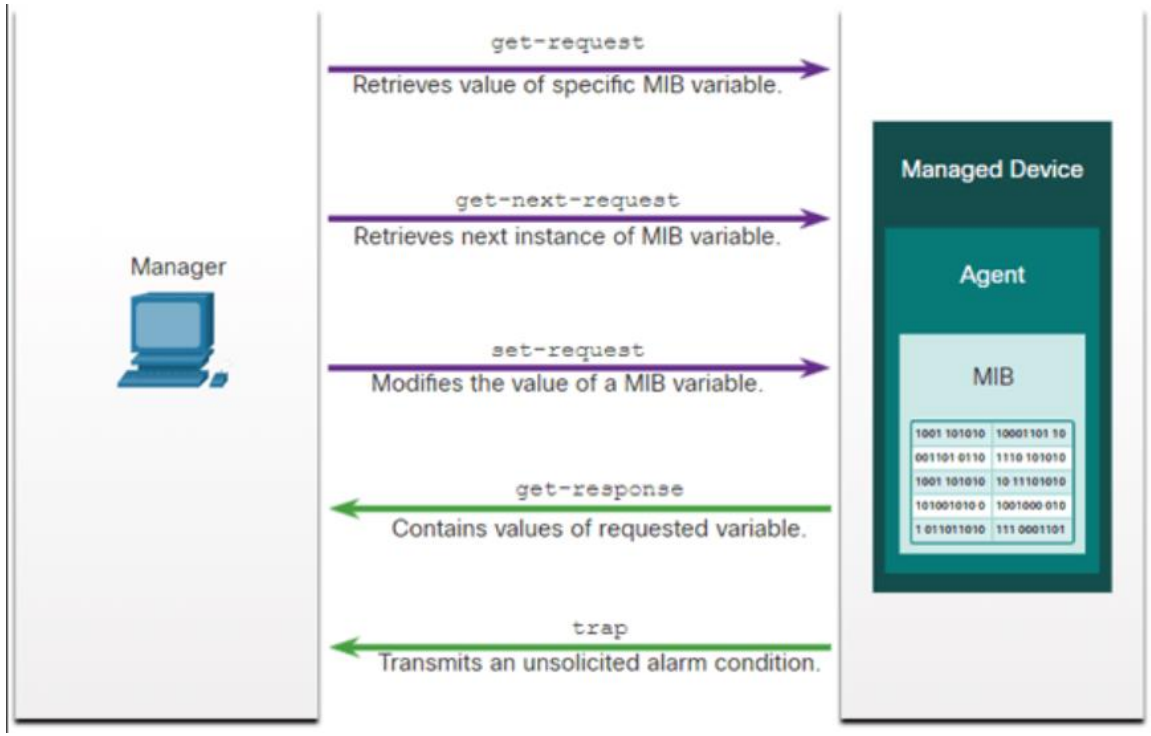


PARTIE 6

Opération SNMP

- Les agents SNMP qui résident sur les appareils gérés collectent et stockent des informations sur l'appareil et son fonctionnement localement dans le MIB. Le gestionnaire SNMP utilise ensuite l'agent SNMP pour accéder aux informations contenues dans la base de données MIB.
- Il existe deux types principaux de requêtes de gestionnaire SNMP, à savoir get et set. En plus de la configuration, un ensemble peut provoquer une action, comme le redémarrage d'un routeur.

Operation	Description
get-request	Récupère une valeur à partir d'une variable spécifique.
get-next-request	Récupère une valeur à partir d'une variable dans une table; le gestionnaire SNMP ne doit pas connaître le nom exact de la variable. Une recherche séquentielle est effectuée afin de trouver la variable requise dans une table.
get-bulk-request	Récupère des blocs importants de données, comme plusieurs lignes dans une table, qui autrement nécessiteraient la transmission de nombreux petits blocs de données. (Fonctionne uniquement avec SNMPv2 ou version ultérieure.)
get-response	Réponses aux **get-request, get-next-request,** and **set-request** par un NMS.
set-request	Stocke une valeur dans une variable spécifique.



PARTIE 6

Versions SNMP

- **SNMPv1** - Standard hérité défini dans la RFC 1157. Utilise une méthode d'authentification basée sur une chaîne de communauté simple. Ne doit pas être utilisé en raison de risques de sécurité.
- **SNMPv2c** - Défini dans les RFCs 1901-1908. Utilise une méthode d'authentification basée sur une chaîne de communauté simple. Fournit des options de récupération en bloc, ainsi que des messages d'erreur plus détaillés.
- **SNMPv3** - Défini dans les RFCs 3410-3415. Utilise l'authentification par nom d'utilisateur, assure la protection des données à l'aide de HMAC-MD5 ou HMAC-SHA et le chiffrement à l'aide du chiffrement DES, 3DES ou AES.

Cordes communautaires

Les protocoles **SNMPv1** et **SNMPv2c** utilisent des identifiants de communauté qui contrôlent l'accès à la base de données MIB. Les identifiants de communauté sont des mots de passe qui circulent en clair (plain text). Les identifiants de communauté SNMP authentifient l'accès aux objets MIB.

Il existe deux types d'identifiants de communauté:

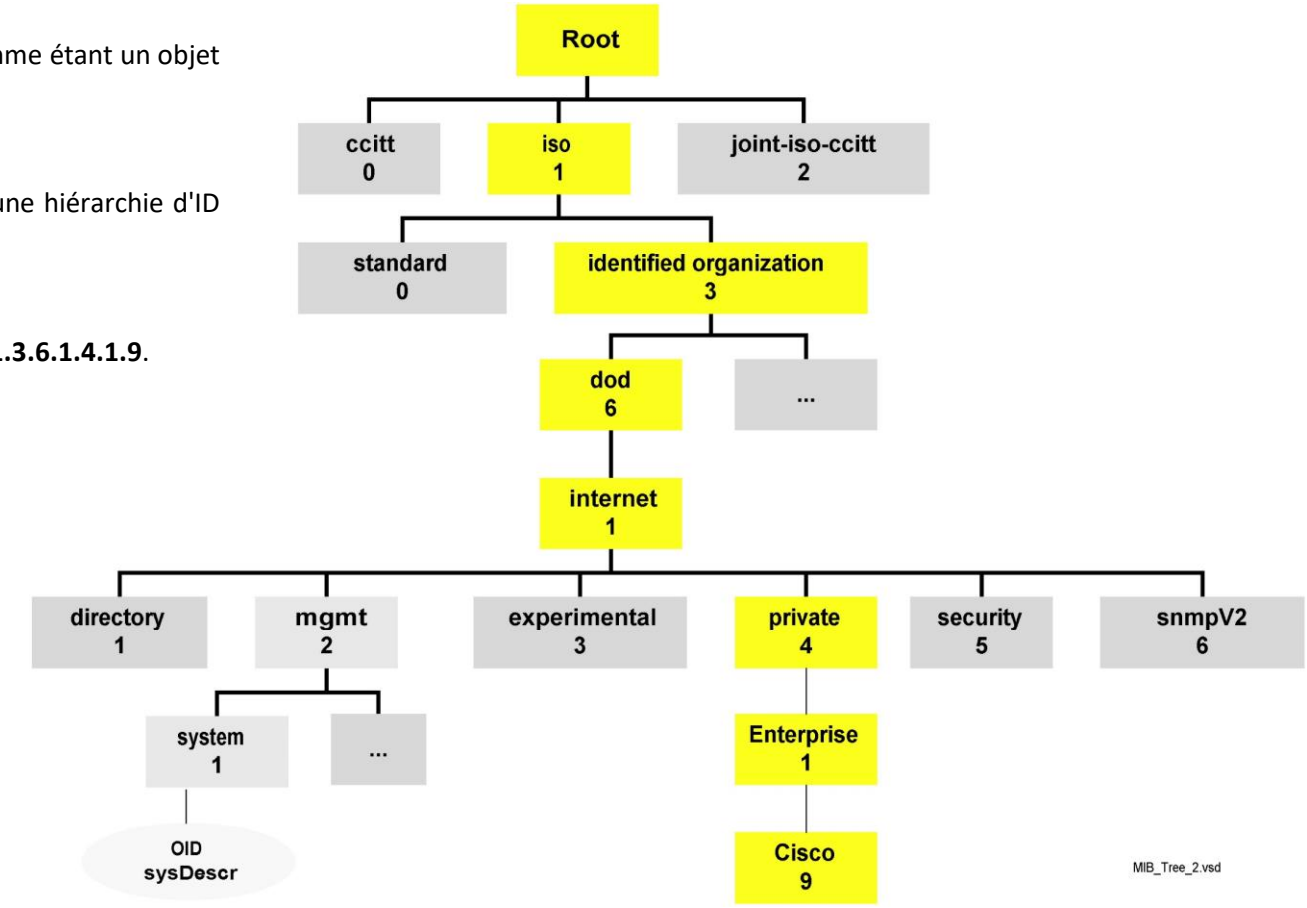
- **Lecture seule (ro)** - Ce type donne accès aux variables MIB, mais ne permet pas de modifier ces variables, seulement de les lire. La sécurité étant minimale dans la version 2c, de nombreuses entreprises utilisent le protocole SNMPv2c en mode lecture seule.
- **Lecture/écriture (rw)** - Ce type fournit un accès en lecture et en écriture à l'ensemble des objets de la base de données MIB.

Pour afficher ou définir des variables MIB, l'utilisateur doit spécifier l'identifiant de communauté approprié pour l'accès en lecture ou en écriture.

ID d'objet MIB

- La base de données MIB organise les variables de manière hiérarchique.
- De manière formelle, la base de données MIB définit chaque variable comme étant un objet avec un identifiant (OID).
- Les ID d'objet identifient de manière unique les objets gérés.
- La base de données MIB organise les OID sur la base des RFC au sein d'une hiérarchie d'ID d'objet, généralement affichée sous la forme d'une arborescence.

L'OID d'objet Cisco est **1.3.6.1.4.1.9**.

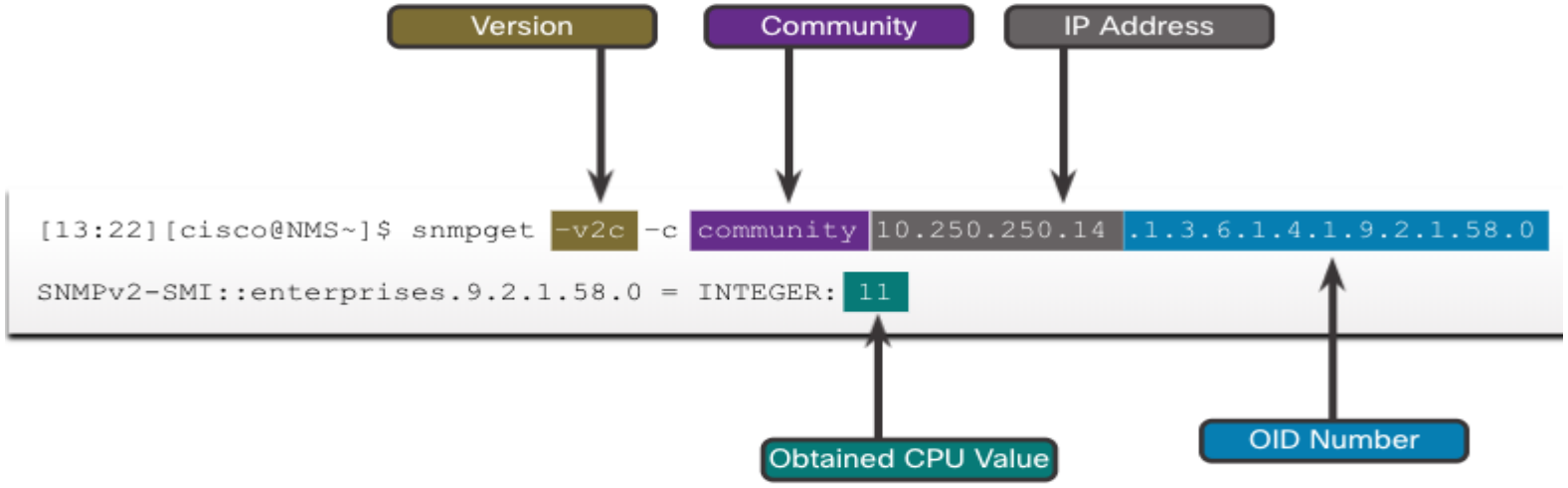


Remarque : Notez comment l'OID peut être décrit en mots ou en chiffres pour aider à localiser une variable particulière dans l'arbre.

PARTIE 6

Scénario d'interrogation SNMP

- SNMP peut être utilisé est d'observer l'utilisation du CPU sur une période de temps par des périphériques d'interrogation. Les statistiques du processeur doivent être compilées sur le système de gestion de réseau (NMS) et affichées graphiquement. Cela crée une ligne de base pour l'administrateur réseau.
- Les données sont récupérées par l'intermédiaire de l'utilitaire **snmpget**, exécuté sur le système de gestion de réseau (NMS). À l'aide de l'utilitaire snmpget, vous pouvez récupérer manuellement des données en temps réel ou demander au NMS d'exécuter un rapport. Ce rapport vous donnerait une période de temps pendant laquelle vous pourriez utiliser les données pour obtenir la moyenne.



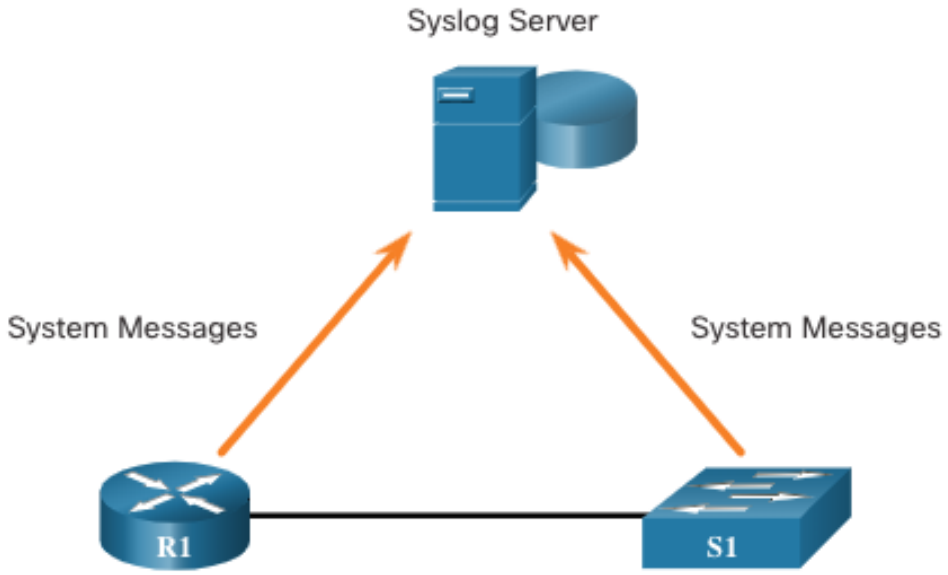
Remarque : Le navigateur SNMP de Cisco (SNMP Object Navigator) sur le site http://www.cisco.com permet à un administrateur réseau de rechercher des détails sur un **OID** particulier.

Introduction à Syslog

Syslog utilise le port UDP 514 pour envoyer des messages de notification d'événements sur les réseaux IP aux collecteurs de messages d'événements, comme le montre la figure.

Le service de consignation syslog assure trois fonctions principales, comme suit :

- La capacité à collecter les informations de journalisation pour la surveillance et le dépannage
- La capacité de sélectionner le type d'information de journalisation capturée
- La capacité à spécifier les destinations des messages Syslog capturés



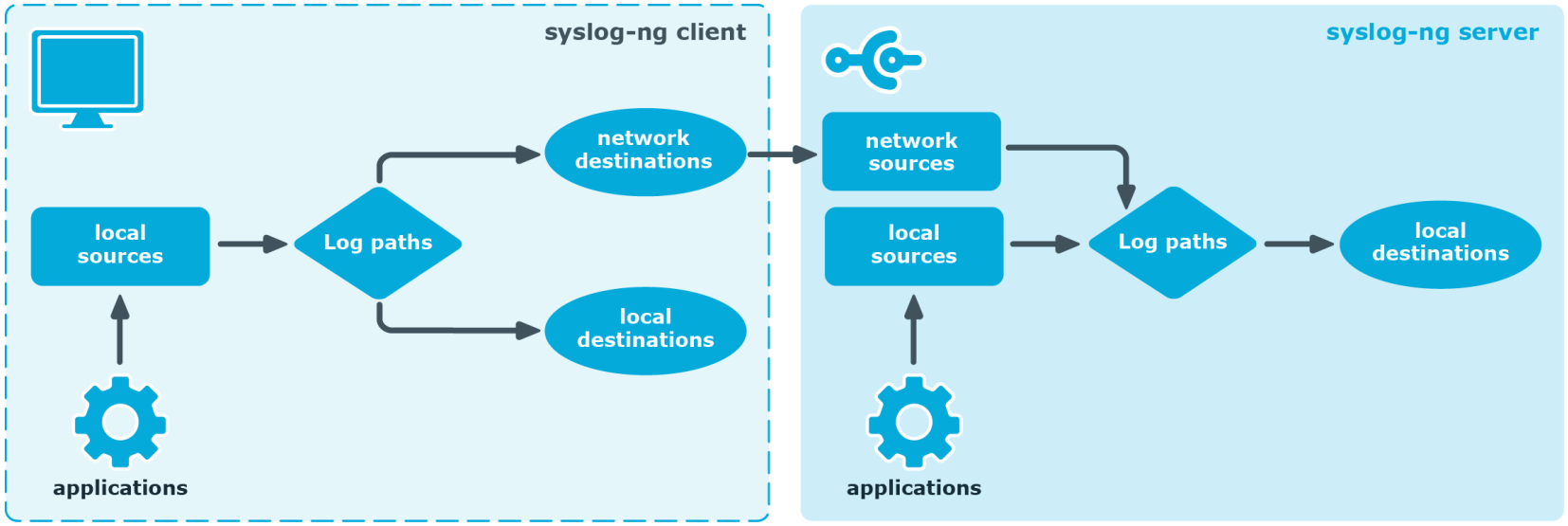
Opération Syslog

Le protocole syslog commence par envoyer des messages système et une sortie de debug à un processus d'enregistrement local. La configuration Syslog peut envoyer ces messages sur le réseau à un serveur syslog externe, où ils peuvent être récupérés sans avoir besoin d'accéder au périphérique réel.

De même, des messages Syslog peuvent également être envoyés vers un tampon interne. Les messages envoyés vers le tampon interne ne peuvent être affichés que par l'intermédiaire de l'interface en ligne de commande du périphérique.

Enfin, l'administrateur réseau peut spécifier que seuls certains types de messages sont envoyés à différentes destinations. Les destinations populaires des messages Syslog sont les suivantes:

- Tampon de consignation (RAM à l'intérieur d'un routeur ou d'un commutateur)
- Ligne de console
- Ligne de terminal
- Serveur Syslog



Format de message Syslog

Les périphériques Cisco génèrent des messages Syslog à la suite des événements réseau. Chaque message Syslog contient un niveau de gravité et une capacité.

Plus les numéros des niveaux sont petits, plus les alarmes Syslog sont critiques. Il est possible de définir le niveau de gravité des messages de manière à contrôler l'emplacement d'affichage de chaque type de message (par exemple sur la console ou d'autres destinations). La liste complète des niveaux Syslog est illustrée au tableau.

Gravité	Niveau de gravité	Explication
Urgence	Niveau 0	Système inutilisable
Alerte	Niveau 1	Action immédiate requise
Essentiel	Niveau 2	Condition critique
Erreur	Niveau 3	Condition d'erreur
Avertissement	Niveau 4	Condition d'avertissement
Notification	Niveau 5	Événement normal mais important
Informatif	Niveau 6	Message informatif
Débogage	Niveau 7	Message de débogage

Configurer l'horodatage Syslog

- Par défaut, les messages de journal ne sont pas horodatés.
- Les messages de journal doivent être horodatés de sorte que lorsqu'ils sont envoyés à une autre destination, comme un serveur Syslog, il reste une trace du moment où le message a été généré.
- Utilisez la commande **service timestamps log datetime** pour forcer les événements journalisés à afficher la date et l'heure.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1 (config) # interface g0/0/1
R1(config-if)# no shutdown
*Mar 1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up
R1(config-if)#
```

CHAPITRE 3

Mettre en place un système de gestion et de supervision des réseaux

1. Gestion réseau
2. Supervision réseau
3. Dépannage réseau (Network Troubleshooting)

PARTIE 6

Aperçu de la documentation réseau

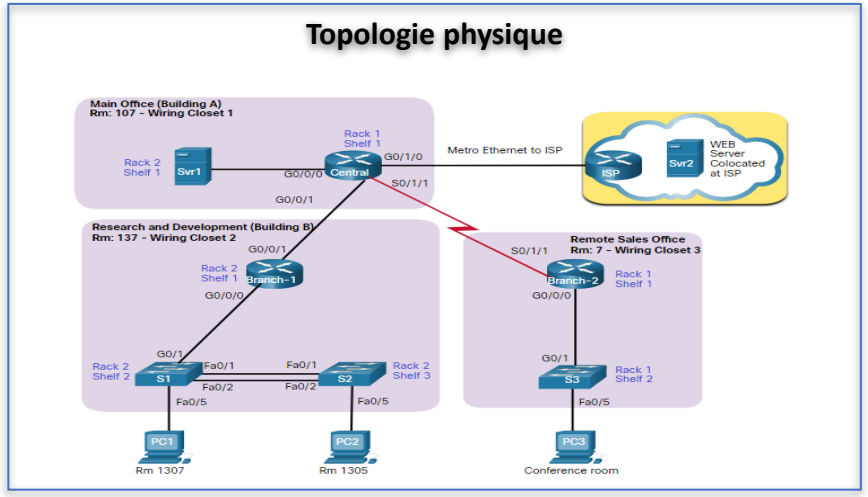
Une documentation réseau précise et complète est nécessaire pour surveiller et dépanner efficacement les réseaux.

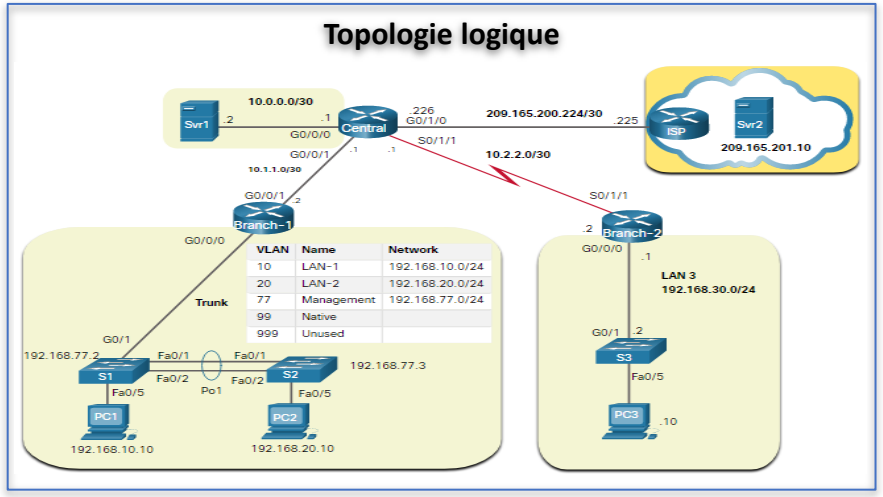
La documentation réseau commune comprend les éléments suivants :

- Diagrammes de topologie du réseau physique et du réseau logique
- Documentation sur les périphériques réseau qui enregistre toutes les informations pertinentes sur les périphériques
- Documentation de référence sur les performances réseau

Diagrammes de la topologie du réseau

Il existe deux types de diagrammes topologiques, physiques et logiques.





PARTIE 6

Documentation du périphérique réseau

La documentation relative aux dispositifs de réseau doit contenir des enregistrements précis et actualisés du matériel et des logiciels de réseau.

La documentation doit inclure toutes les informations pertinentes sur les périphériques réseau.

Dispositif de routage Documentation

Device	Model	Description	Location	IOS	License
Central	ISR 4321	Central Edge Router	Building A Rm: 137	Cisco IOS XE Software, Version 16.09.04 flash:isr4300-universalk9_ias.16.09.04.SPA.bin	ipbasek9 securityk9

Interface	Description	IPv4 Address	IPv6 Address	MAC Address	Routing
G0/0/0	Connects to SVR-1	10.0.0.1/30	2001:db8:acad:1::1/64	a03d.6fe1.e180	OSPF
G0/0/1	Connects to Branch-1	10.1.1.1/30	2001:db8:acad:a001::1/64	a03d.6fe1.e181	OSPFv3
G0/1/0	Connects to ISP	209.165.200.226/30	2001:db8:feed:1::2/64	a03d.6fc3.a132	Default
S0/1/1	Connects to Branch-2	10.1.1.2/24	2001:db8:acad:2::1/64	n/a	OSPFv3

Dispositif de commutation Documentation

Device	Model	Description	Mgt. IP Address	IOS	VTP
S1	Cisco Catalyst WS-C2960-24TC-L	Branch-1 LAN1 switch	192.168.77.2/24	IOS: 15.0(2)SE7 Image: C2960-LANBASEK9-M	Domain: CCNA Mode: Server

Port	Description	Access	VLAN	Trunk	EtherChannel	Native	Enabled
Fa0/1	Port Channel 1 trunk to S2 Fa0/1	-	-	Yes	Port-Channel 1	99	Yes
Fa0/2	Port Channel 1 trunk to S2 Fa0/2	-	-	Yes	Port-Channel 1	99	Yes
Fa0/3	*** Not in use ***	Yes	999	-	-		Shut
Fa0/4	*** Not in use ***	Yes	999	-	-		Shut
Fa0/5	Access port to user	Yes	10	-	-		Yes

Système final Documentation

Device	OS	Services	MAC Address	IPv4 / IPv6 Addresses	Default Gateway	DNS
SRV1	MS Server 2016	SMTP, POP3, File services, DHCP	5475.d08e.9ad8	10.0.0.2/30	10.0.0.1	10.0.0.1
				2001:db8:acad:1::2/64	2001:db8:acad:1::1	2001:db8:acad:1::1
SRV2	MS Server 2016	HTTP, HTTPS	5475.d07a.5312	209.165.201.10	209.165.201.1	209.165.201.1
				2001:db8:feed:1::10/64	2001:db8:feed:1::1	2001:db8:feed:1::1
PC1	MS Windows 10	HTTP, HTTPS	5475.d017.3133	192.168.10.10/24	192.168.10.1	192.168.10.1
				2001:db8:acad:1::251/64	2001:db8:acad:1::1	2001:db8:acad:1::1

Mesure de données

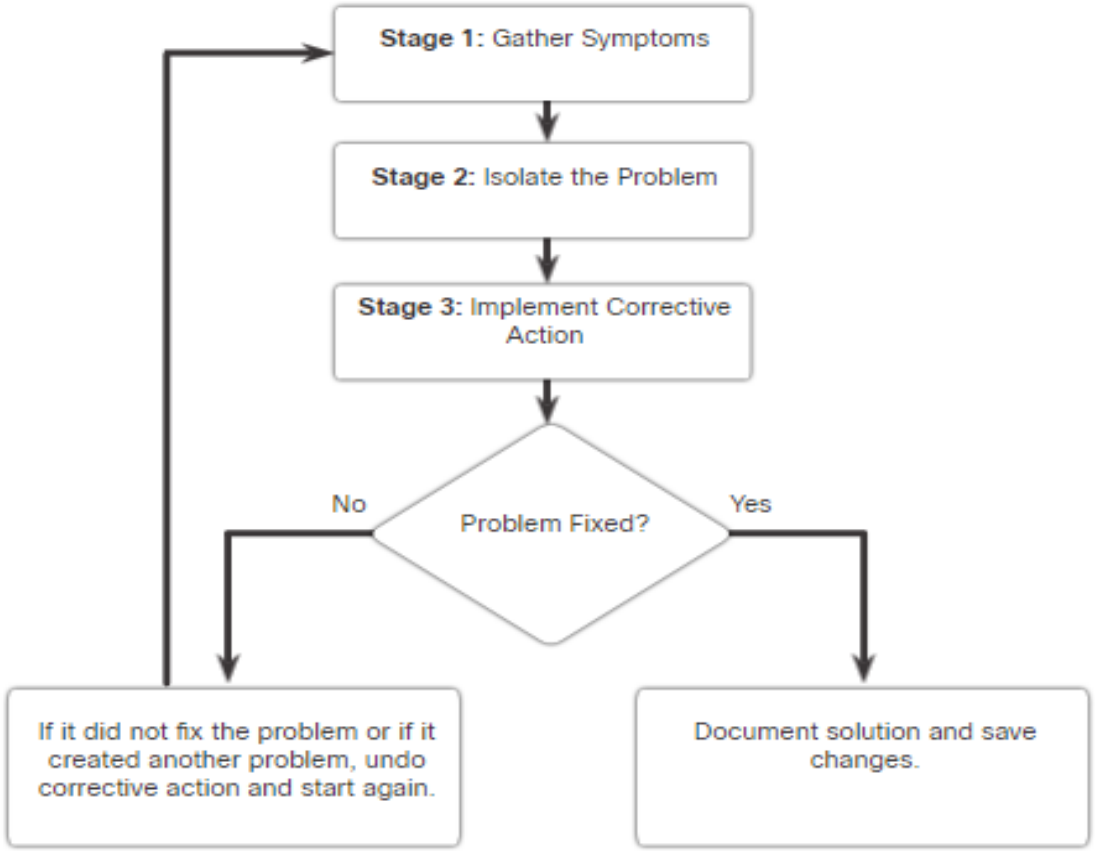
La figure répertorie certaines des commandes Cisco IOS les plus fréquemment utilisées pour la collecte des données.

Commande	Description
`show version`	• Affiche le temps de fonctionnement, les informations sur la version des logiciels et du matériel
`show ip interface [brief]` `show ipv6 interface [brief]`	• Affiche toutes les options de configuration définies sur une interface.
`show interfaces`	• Affiche les résultats détaillés pour chaque interface.
`show ip route [static | eigrp | ospf | bgp]` `show ipv6 route [static | eigrp | ospf | bgp]`	• La table de routage comprend des réseaux connectés directement et des réseaux distants.
`show cdp neighbors detail`	• Affiche des informations détaillées sur les appareils Cisco directement connectés.
`show arp` `show ipv6 neighbors`	• Affiche le contenu de la table ARP (IPv4) et de la table voisine (IPv6).
`show running-config`	• Affichez la configuration en cours.
`show vlan`	• Affiche l'état des VLAN sur un commutateur.
`show port`	• Affiche l'état des ports sur un commutateur.
`show tech-support`	• Utilisé pour collecter une grande quantité d'informations à l'aide de plusieurs commandes **show** à des fins de compte rendu de l'assistance technique.

Procédures générales de dépannage

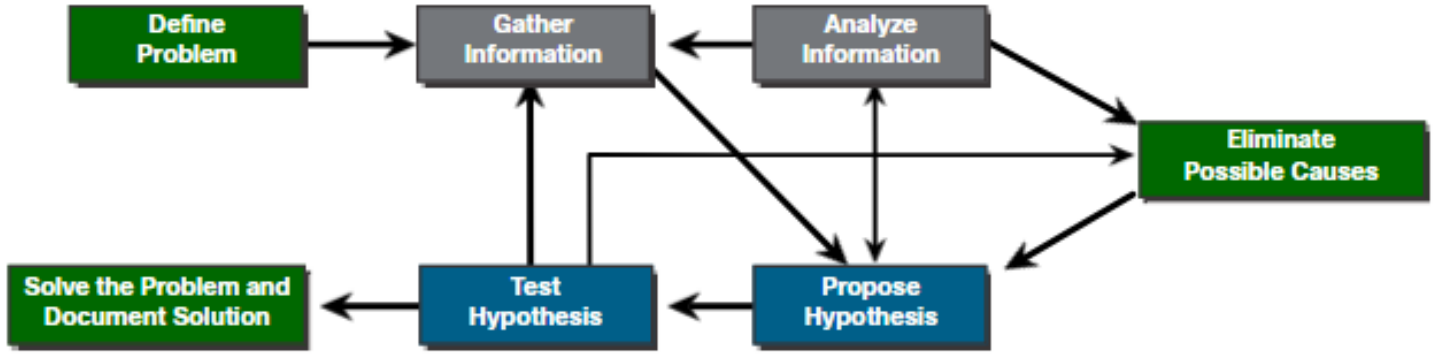
Le dépannage peut prendre du temps car les réseaux diffèrent, les problèmes diffèrent et l'expérience de dépannage varie.

- L'utilisation d'une méthode de dépannage structurée raccourcit le temps global de dépannage.
- Plusieurs processus de dépannage peuvent être utilisés pour résoudre un problème.



Procédures générales de dépannage

La figure montre un processus de dépannage plus détaillé en sept étapes.



Étapes	Description
Définir le problème	• Vérifiez qu'il y a un problème, puis définissez correctement le problème.
Rassembler des informations	• Les cibles (c'est-à-dire les hôtes, les appareils) sont identifiées, consultées et l'information recueillie.
Analyser les informations	• Identifiez les causes possibles à l'aide de la documentation réseau, des lignes de base réseau, des bases de connaissances et des homologues.
Éliminer les causes possibles	• Éliminer progressivement les causes possibles pour finalement identifier la cause la plus probable.
Proposer une hypothèse	• Lorsque la cause la plus probable a été identifiée, une solution doit être formulée.
Tester cette hypothèse	• Évaluez l'urgence du problème, créez un plan de restauration, implémentez la solution et vérifiez les résultats.
Résoudre le problème	• Une fois résolu, informez toutes les parties concernées et documentez la cause et la solution pour aider à résoudre les problèmes futurs.

Collecter des informations

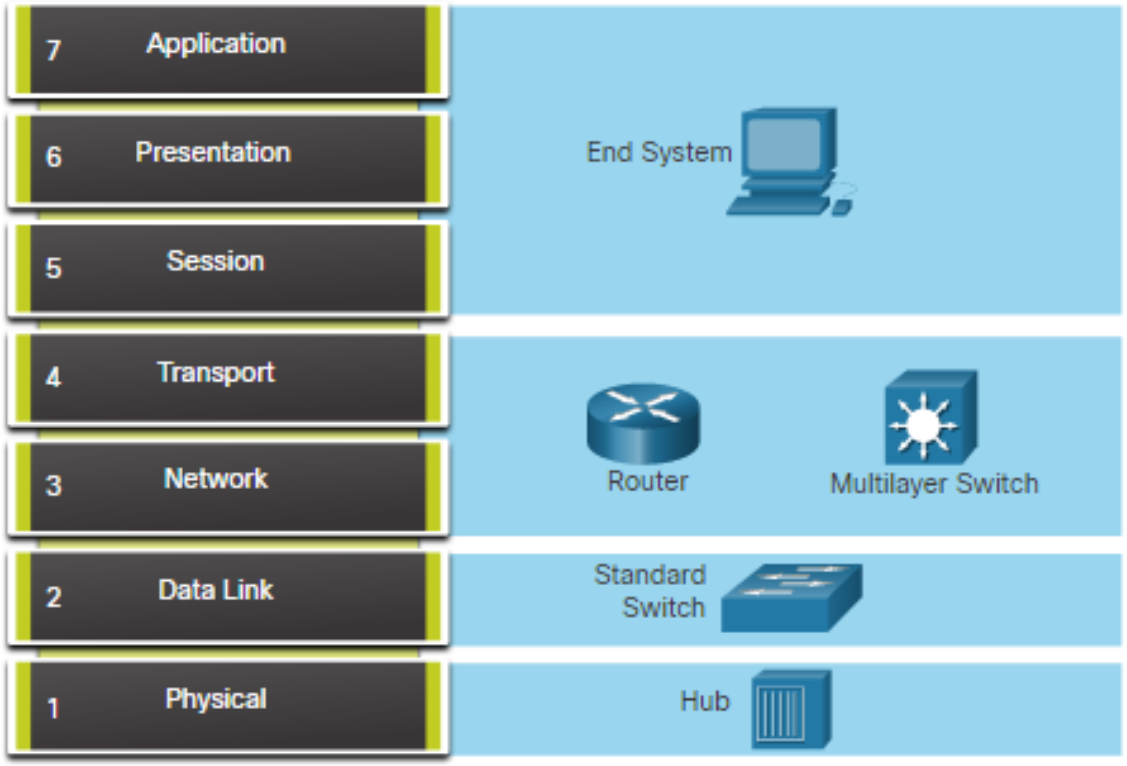
Commandes IOS Cisco courantes utilisées pour recueillir les symptômes des problèmes de réseau.

Commande	Description
ping {*host* | *ip-address*}	• Envoie un paquet de requête d'écho à une adresse, puis attend une réponse.
traceroute *destination*	• Identifie le chemin que suit un paquet via les réseaux.
telnet {*host* **|** *ip-address***}**	• Se connecte à une adresse IP en utilisant l'application Telnet (Remarque : utilisez SSH lorsque c'est possible).
ssh -l *user-id ip-address*	• Permet la connexion à une adresse IP à l'aide de SSH.
show ip interface brief **show ipv6 interface brief**	• Affiche un résumé de l'état de toutes les interfaces sur un périphérique.
show ip route **show ipv6 route**	• Affiche les tables de routage IPv4 et IPv6 actuelles.
show protocols	• Affiche l'état global et spécifique à l'interface de tout protocole de couche 3 configuré.
debug	• Affiche la liste des options pour activer ou désactiver les événements de débogage.

Dépannage avec les modèles en couches

Les modèles OSI et TCP/IP peuvent être appliqués pour isoler les problèmes de réseau lors du dépannage.

La figure montre quelques dispositifs courants et les couches OSI qui doivent être examinées au cours du processus de dépannage pour ce dispositif.



Méthodes de dépannage structurées

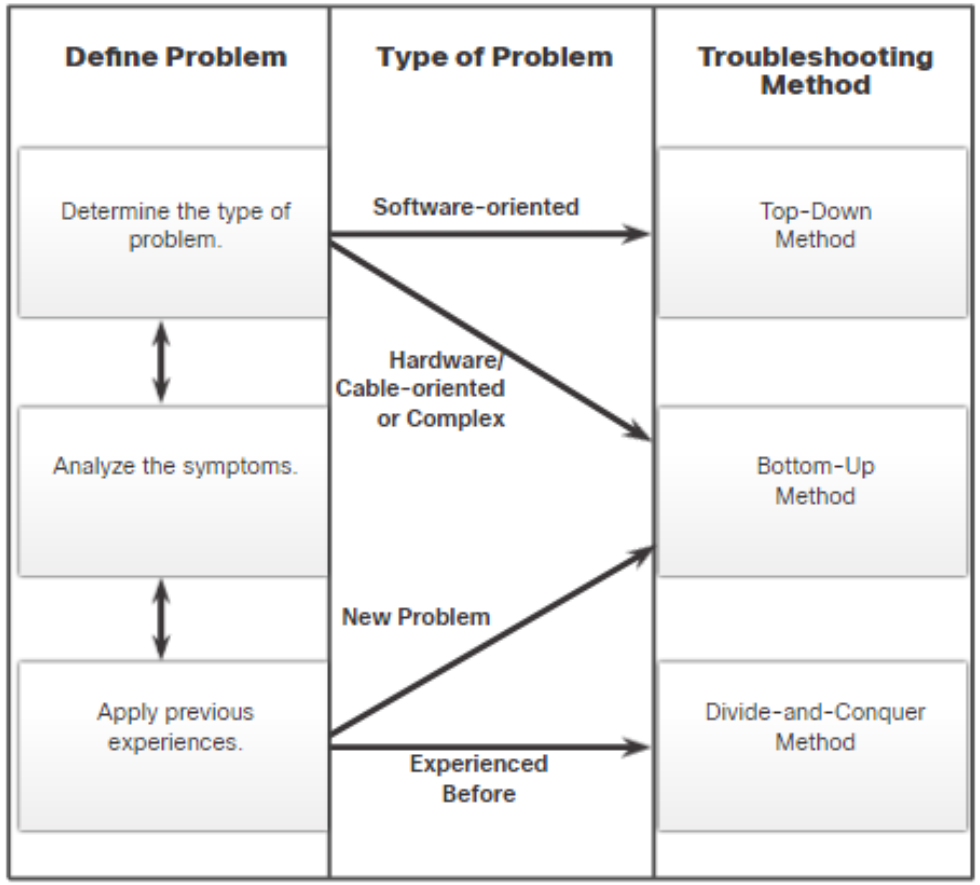
Les différentes approches de dépannage qui peuvent être utilisées sont les suivantes.

Approche de dépannage	Description
Méthode ascendante	• Bonne approche à utiliser lorsque l'on soupçonne que le problème est d'ordre physique.
Méthode descendante	• Utilisez cette approche pour les problèmes simples ou lorsque vous pensez que le problème concerne un élément logiciel.
Diviser et conquérir	• Commencez par une couche intermédiaire (c. -à-d., couche 3) et teste dans les deux sens à partir de cette couche.
Suivre le chemin	• Permet de découvrir le chemin de trafic réel de la source à la destination afin de réduire la portée du dépannage.
Substitution	• Vous échangez physiquement un appareil potentiellement problématique avec un appareil connu et fonctionnel.
Comparaison	• Tente de résoudre le problème en comparant un élément non opérationnel avec celui de travail.
Devinette instruite	• Le succès de cette méthode varie en fonction de votre expérience de dépannage et de votre capacité.

Lignes directrices pour le choix d'une méthode de dépannage

Afin de résoudre rapidement les problèmes réseau, prenez le temps de sélectionner la méthode de dépannage réseau la plus efficace.

- La figure illustre la méthode qui pourrait être utilisée lorsqu'un certain type de problème est découvert.
- Le dépannage est une compétence qui est développée en le faisant.
- Chaque problème réseau que vous identifiez et résolvez est ajouté à votre jeu de compétences.



Outils logiciels de dépannage

Voici quelques outils logiciels de dépannage courants :

Outil logiciel	Description
Outils de système d'administration de réseaux (NMS)	• Les logiciels de réseau comprennent des outils de surveillance, de configuration et de gestion des pannes au niveau des appareils. • Ces outils peuvent être utilisés pour étudier et corriger les problèmes de réseau.
Bases de connaissances	• Les bases de connaissances des vendeurs d'appareils réseau en ligne sont devenues des sources d'information indispensables. • En associant ces bases de connaissances aux moteurs de recherche sur Internet, un administrateur réseau a accès à de nombreuses informations basées sur l'expérience.
Outils de création d'une ligne de base	• De nombreux outils d'automatisation du processus de documentation réseau et de planification initiale sont disponibles. • Les outils de basculement permettent d'effectuer des tâches de documentation courantes telles que les diagrammes de réseau, de mettre à jour la documentation des logiciels et du matériel du réseau, et de mesurer de manière rentable l'utilisation de la bande passante du réseau de base.
Analyseurs de protocole	• Un analyseur de protocole peut capturer et afficher la couche physique dans les informations de couche d'application contenues dans un paquet. • Des analyseurs de protocoles tels que Wireshark peuvent aider à dépanner des problèmes de performances réseau.

Outils matériels de dépannage

Il existe plusieurs types d'outils de dépannage du matériel.

Outils matériels	Description
Multimètres numériques	Les appareils mesurent les valeurs électriques de la tension, du courant et de la résistance.
Testeurs de câble	Les appareils portatifs sont conçus pour tester les différents types de câblage de communication de données.
Analyseur de câble	Appareils portatifs multifonctionnels utilisés pour tester et certifier les câbles en cuivre et en fibre optique.
Analyseurs de réseau portables	Dispositif spécialisé utilisé pour dépanner les réseaux commutés et les VLAN.
Cisco Prime NAM	Interface basée sur un navigateur qui affiche l'analyse des performances des périphériques dans un environnement commuté et routé.

Syslog Server comme outil de dépannage

Syslog est utilisé par les clients syslog pour envoyer des messages de journal textuels à un serveur syslog.

- Les messages de journal peuvent être envoyés à la console, aux lignes VTY, au tampon mémoire ou au serveur syslog.
- Les messages du journal de bord de l'IOS de Cisco tombent dans l'un des huit niveaux.
- Plus le numéro de niveau est faible, plus le niveau de gravité est important.
- Par défaut, la console affiche les messages de niveau 6 (débogage).
- Dans la sortie de commande, les niveaux 0 (urgences) à 5 (notifications) sont envoyés au serveur syslog au 209.165.200.225.

```
R1(config)# logging host 209.165.200.225
R1(config)# logging trap notifications
R1(config)# logging on
R1(config)#
```

Niveau	Mot-clé
0	Urgences
1	Alertes
2	Essentiel
3	Erreurs
4	Avertissements
5	Notifications
6	Information
7	Débogage

Dépannage de la couche physique

Le tableau répertorie les symptômes courants des problèmes de réseau de couche physique.

Symptôme	Description
Performance inférieure à la ligne de base	• Les raisons les plus courantes sont la surcharge ou la sous-alimentation des serveurs, la configuration inadéquate des commutateurs ou des routeurs, l'encombrement du trafic sur une liaison à faible capacité et la perte chronique de trames.
Perte de connectivité	• La perte de connectivité peut être due à un câble défectueux ou déconnecté.
Goulots d'étranglement sur le réseau ou encombrement	• Si un itinéraire échoue, les protocoles de routage pourraient rediriger le trafic vers des itinéraires sous-optimaux.
Utilisation élevée de l'unité centrale (UC)	• Des taux d'utilisation élevés du processeur indiquent qu'un périphérique fonctionne à ou dépasse ses limites de conception.
Messages d'erreur de la console	• Les messages d'erreur signalés sur la console de l'appareil peuvent indiquer un problème de couche physique.

Le tableau répertorie les causes des problèmes réseau relatifs à la couche physique les plus fréquents sont les suivants :

Cause du problème	Description
Problèmes d'alimentation	Vérifiez le fonctionnement des ventilateurs et assurez-vous que les orifices d'admission et d'évacuation du châssis sont dégagés.
Défaillances matérielles	Des fichiers de pilote NIC défectueux ou corrompus, un mauvais câblage
Câbles défectueux	Recherchez les câbles endommagés, les câbles inadaptés et les connecteurs mal sertis. Les câbles suspects doivent être testés ou remplacés par des câbles qui fonctionnent.
Atténuation	L'atténuation peut être causée si une longueur de câble dépasse la limite de conception du support, ou lorsqu'il y a une mauvaise connexion résultant.
Bruit	Les interférences électromagnétiques locales (EMI)
Erreurs de configuration d'interface	Les causes peuvent inclure une fréquence d'horloge incorrecte, une source d'horloge incorrecte et une interface non activée.
Dépassement des limites de conception	Un composant pourrait fonctionner de manière sous-optimale s'il est utilisé au-delà des spécifications.
Surcharge du processeur	Les symptômes comprennent des processus avec des pourcentages élevés d'utilisation du CPU, des pertes de file d'attente d'entrée, des performances lentes, des dépassements de délais SNMP, l'absence d'accès à distance, l'absence de services DHCP, Telnet, et des pings lents ou sans réponse.

Dépannage de la couche de liaison des données

Le tableau répertorie les symptômes courants des problèmes de réseau de couche de liaison de données.

Symptôme	Description
Erreur de fonctionnement ou de connectivité au niveau de la couche réseau ou au-dessus	Certains problèmes de couche 2 peuvent empêcher l'échange de trames sur un lien, tandis que d'autres ne font que dégrader les performances du réseau.
Performances réseau inférieures au point de référence	• Les trames peuvent emprunter un chemin sous-optimal vers leur destination, mais elles arrivent, ce qui entraîne une utilisation inattendue de la bande passante élevée sur les liens. • Dans un environnement Ethernet, une requête ping étendue ou continue indique également si des trames sont abandonnées.
Nombre excessif de diffusions	• Les systèmes d'exploitation utilisent largement les diffusions et les multidiffusions.
Messages de console	• Les routeurs envoient des messages lorsqu'ils détectent un problème d'interprétation des trames entrantes (problèmes d'encapsulation ou de cadrage) ou lorsque des keepalives sont attendus mais n'arrivent pas.

Le tableau répertorie les causes des problèmes de réseau au niveau de la couche de liaison de données.

Cause du problème	Description
Erreurs d'encapsulation	Se produit lorsque les bits placés dans un champ par l'expéditeur ne sont pas ce que le destinataire attend de voir.
Erreurs de mappage d'adresses	Se produit lorsque la couche 2 et l'adressage de couche ne sont pas disponibles.
Erreurs de trames	Les erreurs de trame peuvent être provoquées par des parasites sur une ligne série, un câble mal conçu (trop long ou mal blindé), une carte réseau défaillante, une incohérence du duplex ou une mauvaise configuration de l'horloge de ligne (line clock) de la CSU (Channel Service Unit).
Défaillance ou boucles STP	La plupart des problèmes liés au protocole STP sont dus à la présence de boucles de redirection qui se produisent lors de l'absence de ports bloqués dans une topologie redondante et de l'acheminement en cercles du trafic de manière infinie, ou de la diffusion excessive de paquets en raison d'un taux élevé de modifications de la topologie STP.

Dépannage de la couche réseau

Le tableau répertorie les symptômes courants des problèmes de réseau de couche de liaison de données.

Symptôme	Description
Panne réseau	• Se produit lorsque le réseau est presque ou totalement non fonctionnel, ce qui affecte tous les utilisateurs et applications du réseau. • Ces pannes sont généralement constatées rapidement par les utilisateurs et les administrateurs réseau ; elles ont un impact énorme sur la productivité de l'entreprise.
Performances non optimales	• Il s'agit d'un sous-ensemble d'utilisateurs, d'applications, de destinations ou d'un type de trafic. • Les problèmes d'optimisation peuvent être difficiles à détecter et encore plus difficiles à isoler et à diagnostiquer. • Cela est dû au fait qu'elles impliquent généralement plusieurs couches, voire un seul ordinateur hôte. • Le fait de déterminer qu'un problème est un problème de couche réseau peut prendre du temps.

Le tableau répertorie les causes courants des problèmes de réseau de couche de liaison de données.

Cause du problème	Description
Problèmes généraux de réseau	• Souvent, une modification de la topologie peut sans le savoir avoir des effets sur d'autres zones du réseau. • Déterminez si une modification récente a été apportée au réseau et si quelqu'un a récemment travaillé à l'infrastructure du réseau.
Problèmes de connectivité	Vérifiez les problèmes d'équipement et de connectivité, y compris les problèmes d'alimentation, d'environnement et de couche 1, tels que les problèmes de câblage, de ports défectueux et de l'ISP.
Table de routage	Vérifiez le tableau de routage pour tout ce qui est imprévu, comme les itinéraires manquants ou les itinéraires inattendus.
Problèmes de voisinage	Vérifiez s'il y a des problèmes avec les routeurs formant des adjacences voisines.
Base de données topologique	Vérifiez le tableau pour tout ce qui est inattendu, comme les entrées manquantes ou les entrées inattendues.

Dépannage de la couche transport – ACLs

Des erreurs de configuration fréquentes peuvent avoir lieu dans les divers domaines suivants :

Mauvaises configurations	Description
Sélection du flux de trafic	Un ACL doit être appliqué à la bonne interface dans le bon sens de circulation.
Ordre incorrect des entrées de contrôle d'accès	Les entrées dans une ACL doivent être de spécifiques à générales.
Énoncé "deny any implicite"	L'ACE implicite peut être la cause d'une erreur de configuration ACL.
Masques génériques d'adresses et IPv4	Les masques génériques IPv4 complexes sont plus efficaces, mais sont plus sujets à des erreurs de configuration.
Sélection de protocole de couche transport	Il est important que seul le protocole de couche de transport correct soit spécifié dans un ACE.
Ports source et de destination	S'assurer que les ports entrants et sortants corrects sont spécifiés dans un ACE
Utilisation du mot-clé established	Le mot clé **established** appliqué de manière incorrecte peut fournir des résultats inattendus.
Protocoles non courants	Les ACL mal configurés causent souvent des problèmes pour les protocoles autres que TCP et UDP.

Dépannage de la couche d'application

Le tableau fournit une brève description de ces protocoles de couche d'application.

Applications	Description
SSH/TelNet	Permet aux utilisateurs d'établir des connexions de session de terminal avec des hôtes distants.
HTTP	Permet l'échange de textes, d'images graphiques, de sons, de vidéos et d'autres fichiers multimédia sur le web.
FTP	Effectue des transferts de fichiers interactifs entre les hôtes.
TFTP	Effectue des transferts de fichiers interactifs de base, généralement entre des hôtes et des dispositifs de réseau.
SMTP	Prend en charge les services de base de transmission de messages.
POP	Se connecte aux serveurs de messagerie et télécharge le courrier électronique.
SNMP	Collecte des informations de gestion à partir des périphériques réseau.
DNS	Fait correspondre les adresses IP aux noms attribués aux appareils du réseau.
NFS	Le système de fichiers réseau (NFS) permet aux ordinateurs de monter et d'utiliser des lecteurs sur des hôtes distants.

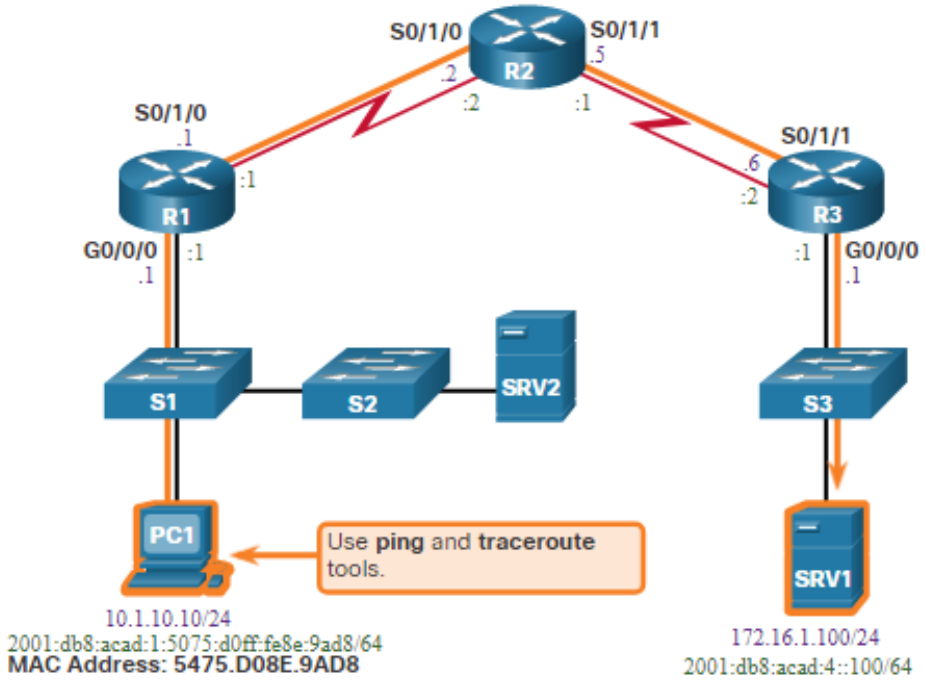
PARTIE 6

Composantes de dépannage de la connectivité de bout en bout

Les étapes de l'approche ascendante lorsqu'il n'y a pas de connectivité de bout en bout sont les suivantes :

1. Vérifiez la connectivité physique à l'endroit où la communication réseau s'arrête.
2. Vérifiez les incohérences de duplex.
3. Vérifiez l'adressage des couches de liaison de données et réseau sur le réseau local.
4. Vérifiez que la passerelle par défaut est correcte.
5. Assurez-vous que les appareils déterminent le chemin correct entre la source et la destination.
6. Vérifiez que la couche transport fonctionne correctement.
7. Vérifiez qu'il n'y a pas de listes de contrôle d'accès qui bloquent le trafic.
8. Vérifiez que les paramètres DNS sont corrects.

- D'une manière générale, c'est la découverte d'un problème de connectivité de bout en bout qui initie un dépannage.
- Deux des utilitaires les plus couramment utilisés pour vérifier un problème de connectivité de bout en bout sont **ping** et **traceroute**.



PARTIE 7

Mettre en place une solution VOIP

Dans ce module, vous allez :

- Etre en mesure de comprendre les perspectives de la VOIP
- Etre capable de Configurer et mettre en œuvre d'une solution VOIP

5 heures

CHAPITRE 1

Etudier la téléphonie classique

Ce que vous allez apprendre dans ce chapitre :

- Comprendre le fonctionnement de la téléphonie classique

0.5 heures

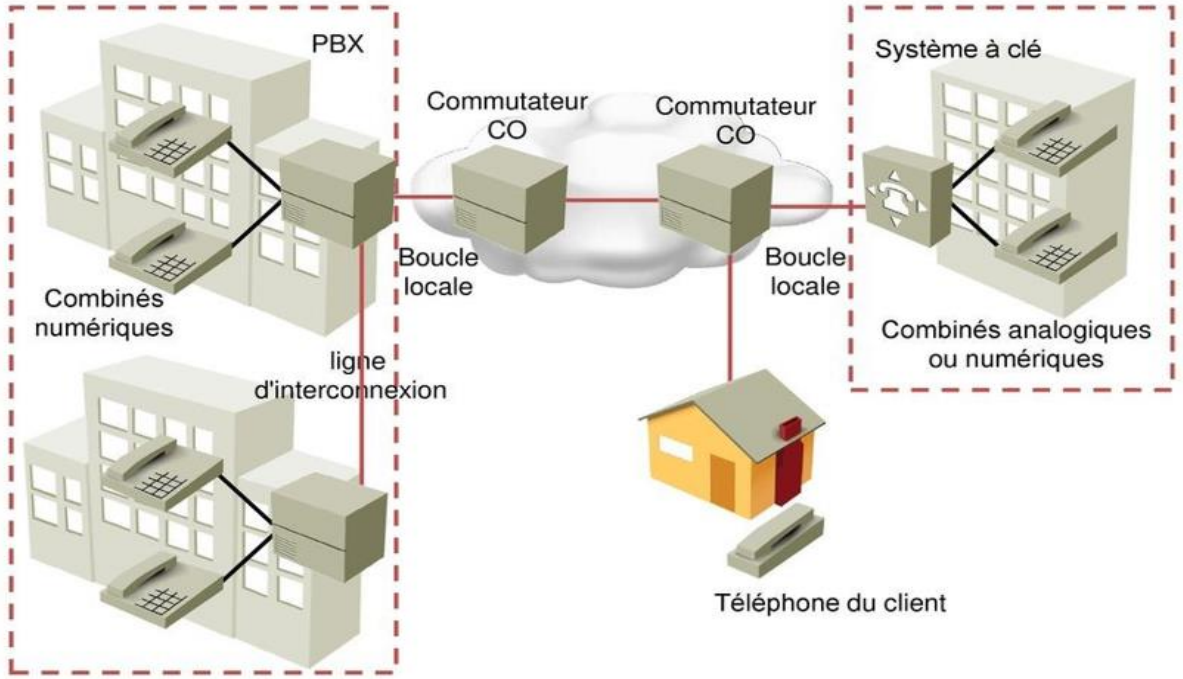
CHAPITRE 1

Etudier la téléphonie classique

1. Système téléphonique traditionnel
2. Circuits analogiques et numériques

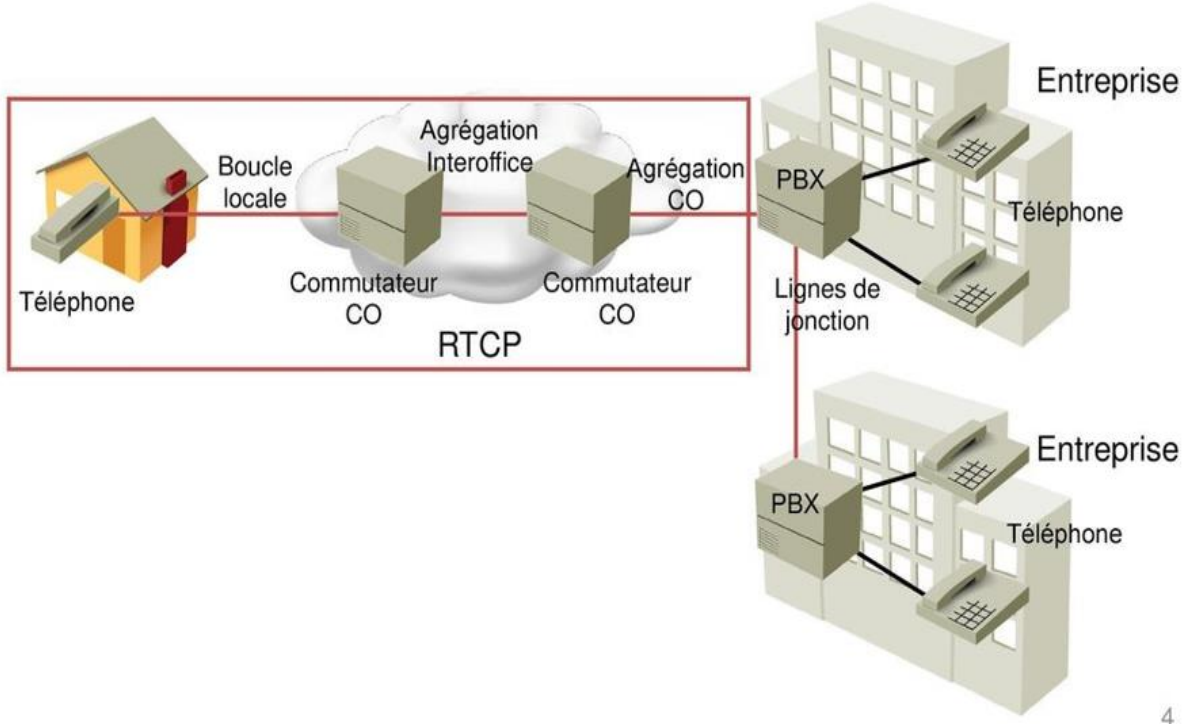
Système téléphonique traditionnel

- Le réseau de téléphonie traditionnelle est composé de RTPC, PBX, interrupteur, signalisation, établissement d'appel, et des plans de numérotation.
- Mettre un appel à travers le RTPC peut impliquer des circuits analogiques, des circuits numériques, des commutateurs CO, et agrégation Interoffice .Un PBX est utilisé dans des installations plus grandes et est similaire à un commutateur CO.
- Les principaux systèmes sont utilisés aux sites plus petits, ont moins de fonctionnalités que d'un PBX, dont les utilisateurs ont partagé les apparences de ligne sur tous les téléphones.
- La signalisation de surveillance communique les changements d'état dans un téléphone analogique ou combiné numérique; la signalisation d'adresse communique les chiffres composés en utilisant des DTMF ou des impulsions, et la signalisation d'information communique avec l'appelant ou l'appelé.



Etablissement d'appel RTCP

1. Le téléphone du client décroche en créant un circuit fermé.
2. Le commutateur CO de l'abonné détecte que le courant passe et génère une tonalité au téléphone du client.
3. Soit des DTMF ou des chiffres d'impulsions sont composés par le client.
4. Le commutateur CO collecte les chiffres et effectue une recherche SS7 pour déterminer le commutateur CO de destination.
5. La signalisation de surveillance indique à l'agrégation analogique distante ou numérique (trunk) qu'un appel entrant est arrivé.
6. Le PBX détermine à quel poste interne l'appel devrait aller et provoque le combiné cible, avec ce poste, à faire sonner.
7. Un rappel est généré au téléphone du client par leur commutateur CO locale.
8. Le combiné cible est décroché et un circuit est construit de bout en bout.

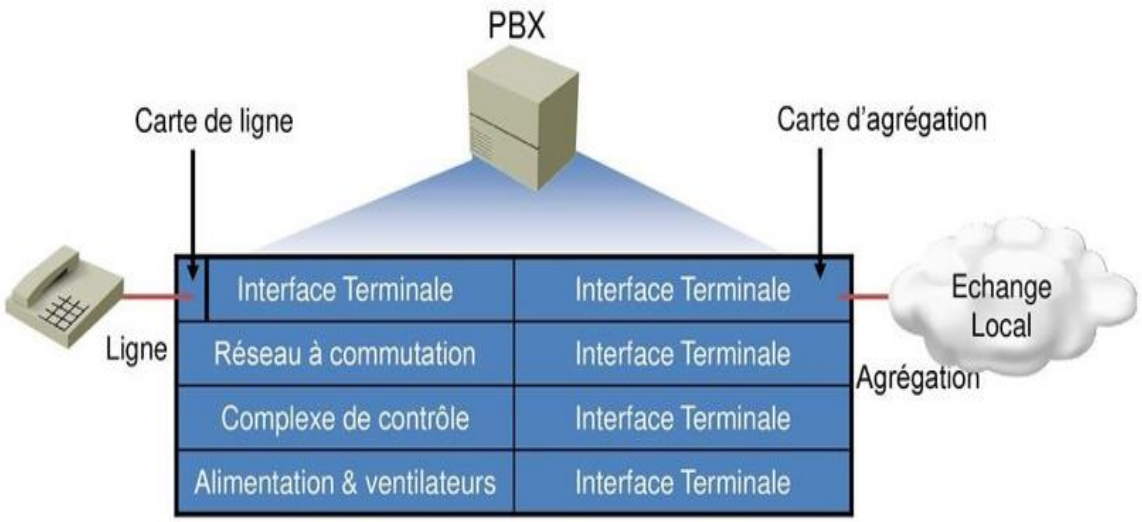


01 -Etudier la téléphonie classique

Système téléphonique traditionnel

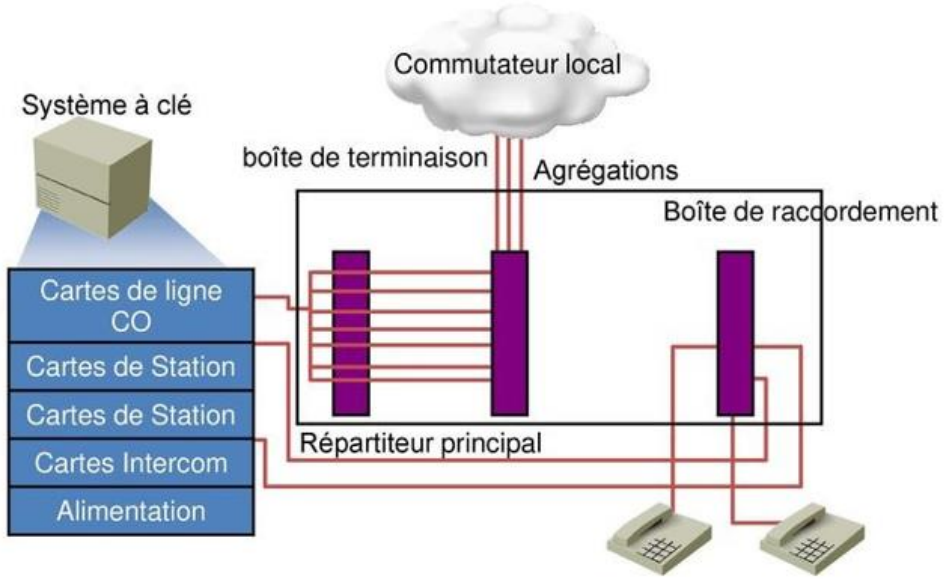
PBX vs Système à clé

PBX



- **Principalement numérique**
- **Similaire au commutateur CO**
- **Grand site d'entreprise (généralement plus de 50 utilisateurs)**
- **Composez 9 ou autre numéro d'accès pour accéder à la ligne extérieure**

Système à clé

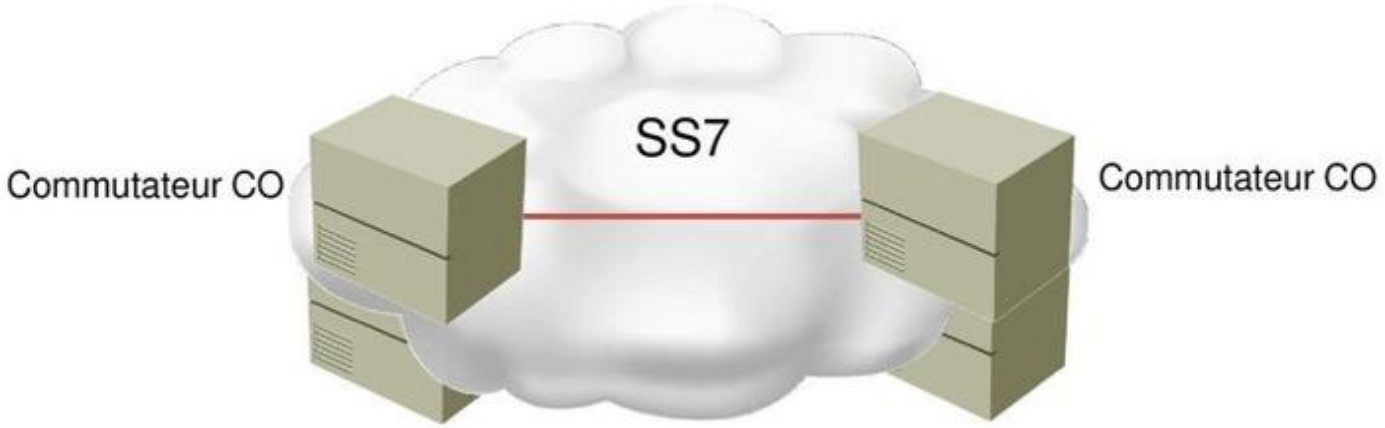


- **Analogique ou numérique**
- **Pas un commutateur**
- **Petite entreprise ou une succursale (généralement 50 utilisateurs ou moins)**
- **Appuyez sur un bouton pour accéder à la ligne extérieure**

PARTIE 7

Types de signalisation

- Il existe trois types de signalisation utilisés dans un réseau de téléphonie:
- La signalisation de surveillance communique l'état d'un dispositif de téléphonie.
- La signalisation d'adresse envoie des informations sur les chiffres composés.
- La signalisation d'information communique l'état actuel de l'appel.
- La signalisation peut être envoyé soit en bande ou hors-bande
- La signalisation en bande envoie la signalisation dans le même canal de communication que la voix.
- La signalisation hors bande envoie la signalisation dans un canal de communication distinct de la voix.



- **SS7** (Signaling System 7) est utilisé entre les compagnies de téléphone
- Fonctions SS7:
  - Signalisation d'information
  - Configuration d'appelRoutage d'appel
  - Facturation d'appel
  - Résolution des ligne sans frais
  - Utilise la signalisation hors-bande

CHAPITRE 3

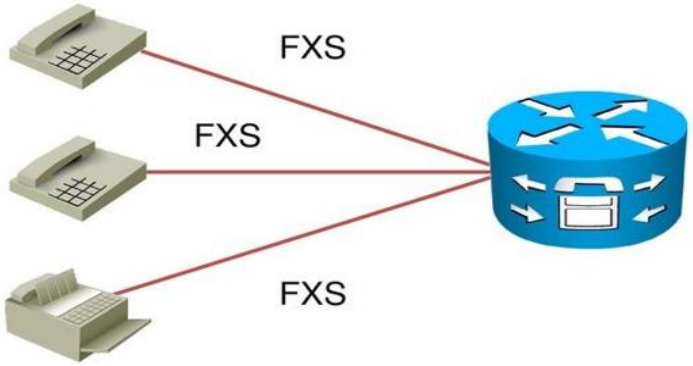
Etudier la téléphonie classique

1. Système téléphonique traditionnel
2. Circuits analogiques et numériques

Circuits analogiques

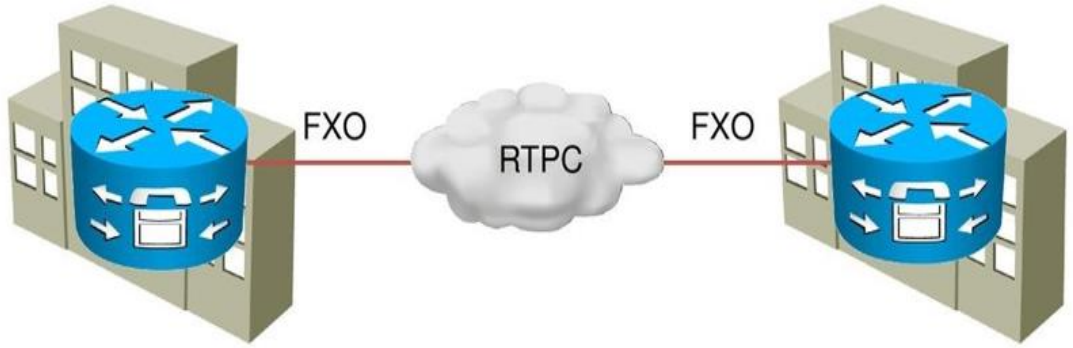
- Les téléphones analogiques ont un récepteur, un émetteur, deux-fils/quatre-fils hybrides, un composeur, un crochet commutateur, et un sonneur.
- Les ports FXS simulent un CO à un téléphone analogique ou fax qui est attaché au port.
- Les ports FXO connectent une passerelle voix Cisco à un commutateur CO ou à un port analogique d'un PBX.
- Les circuits analogiques comprennent FXS, FXO, et des circuits E&M.

Interface FXS



- Se connecte directement à des téléphones analogiques ou fax
- Offre un service local
- Émule le CO pour les périphériques connectés
- Fournit l'alimentation, les tonalités de progression de l'appel, et la tonalité d'appel

Interface FXO

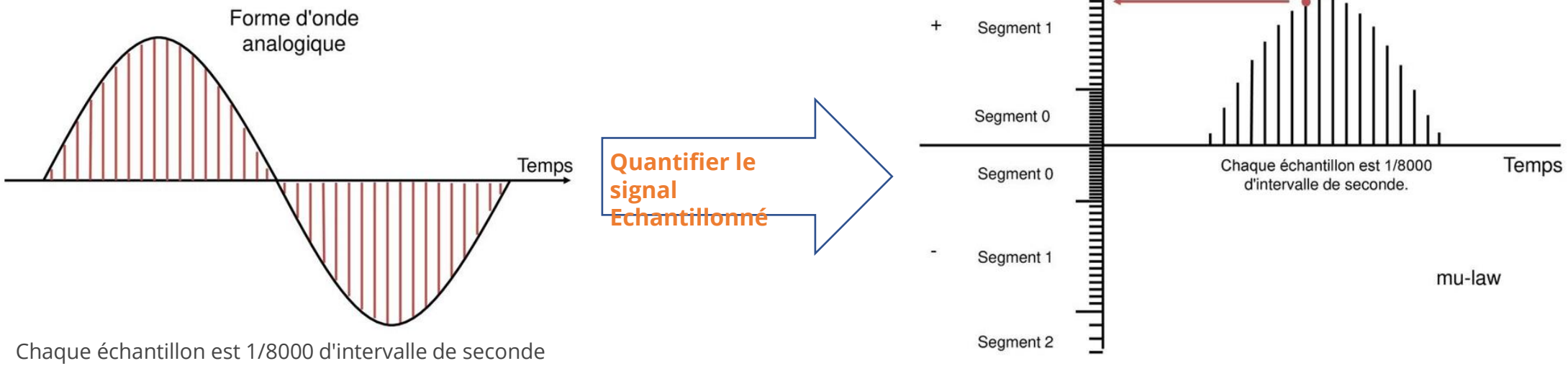


- Se connecte directement aux équipements de bureau
- Utilisé pour faire et recevoir des appels RTPC
- Peut être utilisé pour se connecter via le réseau RTPC vers un autre site
- Répond aux appels entrants

PARTIE 7

Concept de Cloud Computing

- Pour numériser un signal analogique, les échantillons doivent être pris régulièrement, quantifiés à une valeur binaire, et peuvent éventuellement être compressés.
- Les circuits T1 et E1 sont les circuits numériques les plus courantes.
- La numérisation des signaux analogiques
  - Échantillonner le signal analogique régulièrement.
  - Quantifier l'échantillon.
  - Coder la valeur dans une expression binaire.
  - Compresser les échantillons afin de réduire la bande passante (optionnel).



Chaque échantillon est 1/8000 d'intervalle de seconde

CHAPITRE 2

Décrire l'architecture VOIP

Ce que vous allez apprendre dans ce chapitre :

- Découvrir la téléphonie IP
- Comprendre les mécanismes de la Qualité de Services IP

3 heures

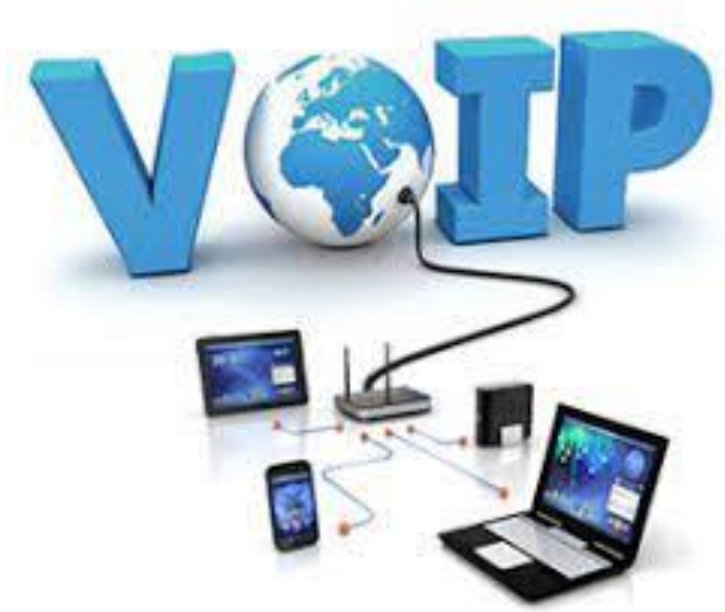
CHAPITRE 2

Décrire l'architecture VOIP

1. Voix sur IP (VoIP)
2. Protocoles de signalisation VOIP
3. Qualité de Services IP
4. Préparer le réseau pour la prise en charge de la voix

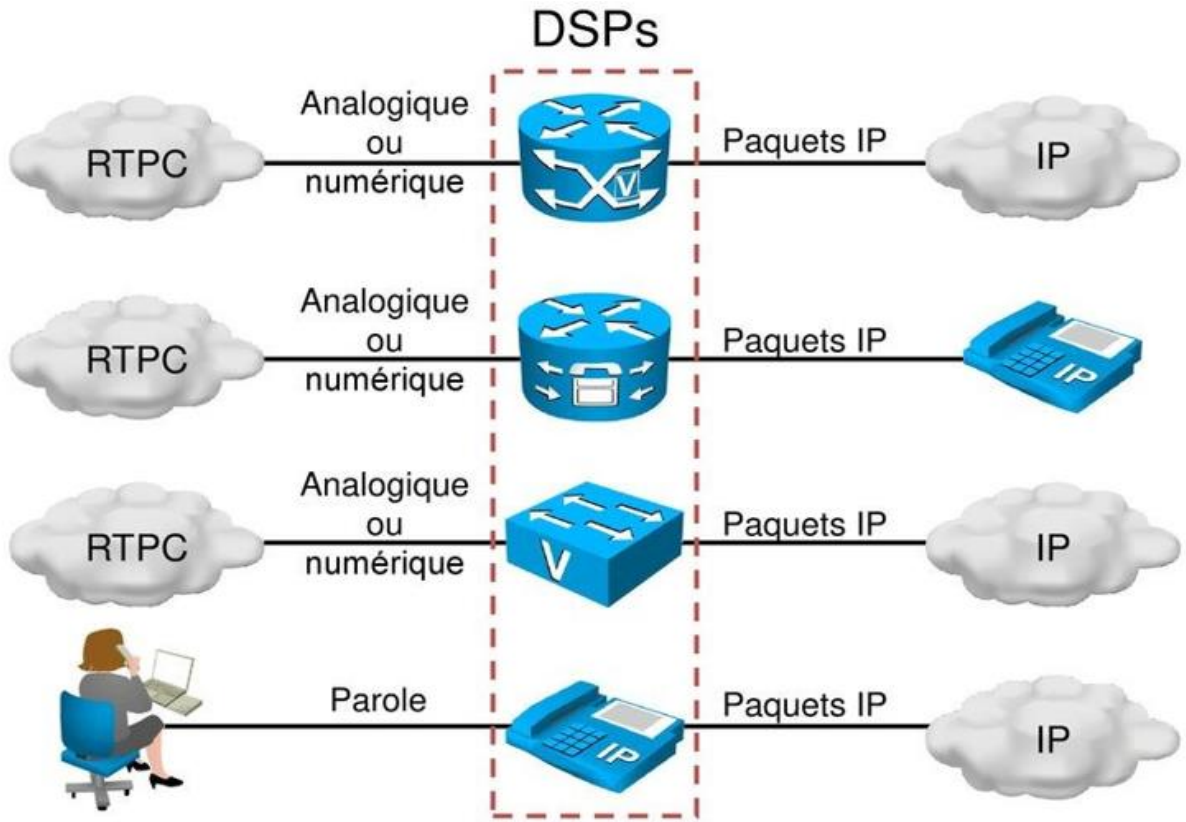
VoIP

- La Voix sur IP consiste à :
  - Utiliser les réseaux IP pour faire passer des communications téléphonique (de la voix ou de la vidéo) en plus des données.
  - Pouvoir connecter un central téléphonique d'entreprise (PABX) à un réseau informatique.
  - Disposer d'un téléphone "classique", mais au lieu d'être relié au PABX, être reliée à un réseau IP (un switch).
  - Disposer de passerelle entre le réseau VOIP et le réseau RTC (Réseau Téléphonique Commuté)



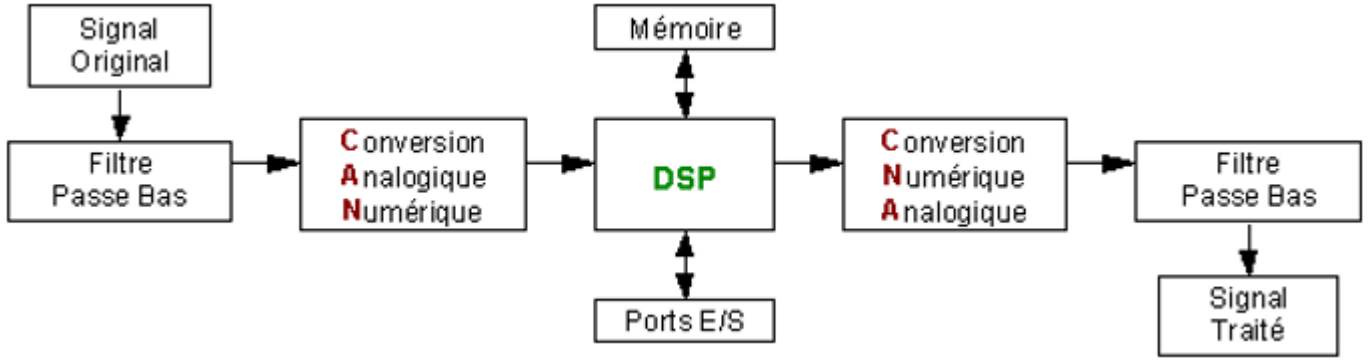
La mise en paquet

- La Voix est emballé dans des segments RTP; les segments RTP sont encapsulés dans des segments UDP; les segments UDP sont encapsulés dans des paquets IP et les paquets IP sont encapsulés dans un format spécifique de couche 2 qu'ils vont traverser.
- Les ressources DSP sont essentielles pour un système de Communications unifiées Cisco et traduit les données vocales traditionnelles en paquets IP et inversement.
- RTP est utilisé pour transporter des données vocales et vidéo à travers le réseau IP.
- RTCP est utilisé pour fournir les informations (feedback) sur le flux RTP.
- Les codecs les plus utilisés sont G.711, G.729, et iLBC.
- Les ressources DSP peuvent également fournir l'annulation d'écho et appeler des fonctions telles que les téléconférence et le transcodage.



Processeurs de signal numérique

- La puce DSP effectue l'échantillonnage, la quantification, le codage, et l'étape de compression optionnelle de numérisation.
- Il est utilisé dans les deux sens pour convertir un signal vocal analogique traditionnel ou numérique en VoIP, ou de VoIP en un signal vocal analogique traditionnel ou numérique
- Le nombre d'appels simultanés d'une puce qu'on peut traiter dépend du type de DSP et du codec utilisé.

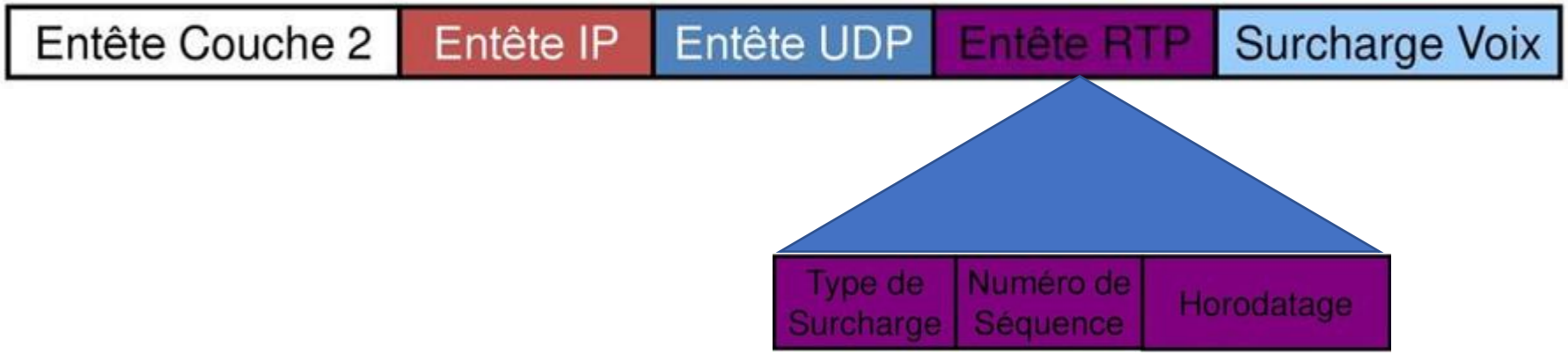


Protocole de contrôle RTP

- Fournit des fonctions réseau de bout en bout et des services de livraison de données sensibles au retard en temps réel, telles que la voix et la vidéo
- Choisit au hasard, même des ports de la plage de ports UDP
- Il peut être utilisé pour surveiller la qualité de la distribution de données et fournir des informations de contrôle
- Fournit des informations (feedback) sur les conditions actuelles du réseau
- Permet aux hôtes qui sont impliqués dans une session RTP d'échanger des informations sur la surveillance et le contrôle de la session:
    - Comptage de paquets
    - Retard des paquets
    - Nombre d'OctetLa perte des paquets
    - Gigue (variation du délai)
- Fournit un flux séparé de RTP pour l'utilisation du transport UDP
- Est joigné avec son flux RTP et utilise le même port que le flux RTP plus 1 (port impair)
- Comprend les services suivants:

Paquétisation de la voix

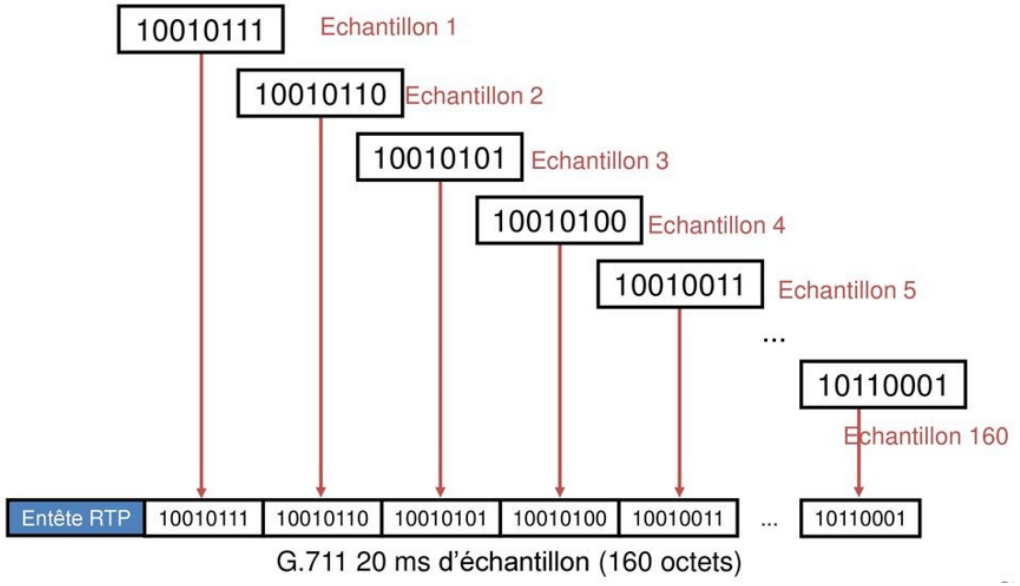
- La paquétisation de la voix est effectuée par les ressources DSP.
- DSP met en paquet la voix, échantillonne et compresse la voix en paquets.
- Les données vocales sont collectées jusqu'à ce que la surcharge de paquet soit pleine.
- Les données vocales sont mises dans la surcharge des segments RTP.
- RTP est encapsulé dans un segment UDP qui est encapsulé dans un paquet IP.
- Le paquet IP est encapsulé dans un format de couche 2.



Paquétisation de la voix

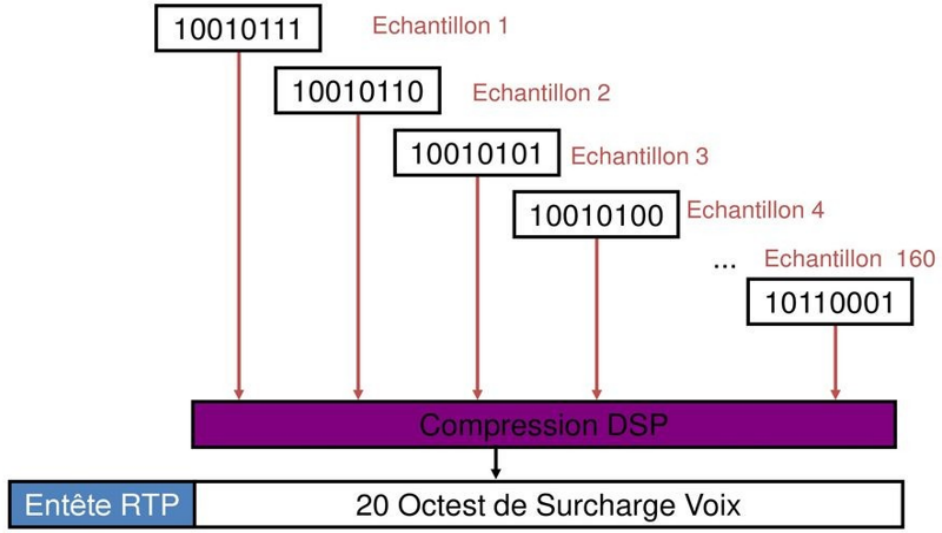
- G.711, G.729 sont les codecs les plus courants :

Exemple codec G.711 (64kb/s)



G.711 20 ms d'échantillon (160 octets)

Exemple codec G.729 (8kb/s)



G.729 20 ms de voix contenu dans un paquet

PARTIE 7

CHAPITRE 2

Décrire l'architecture VOIP

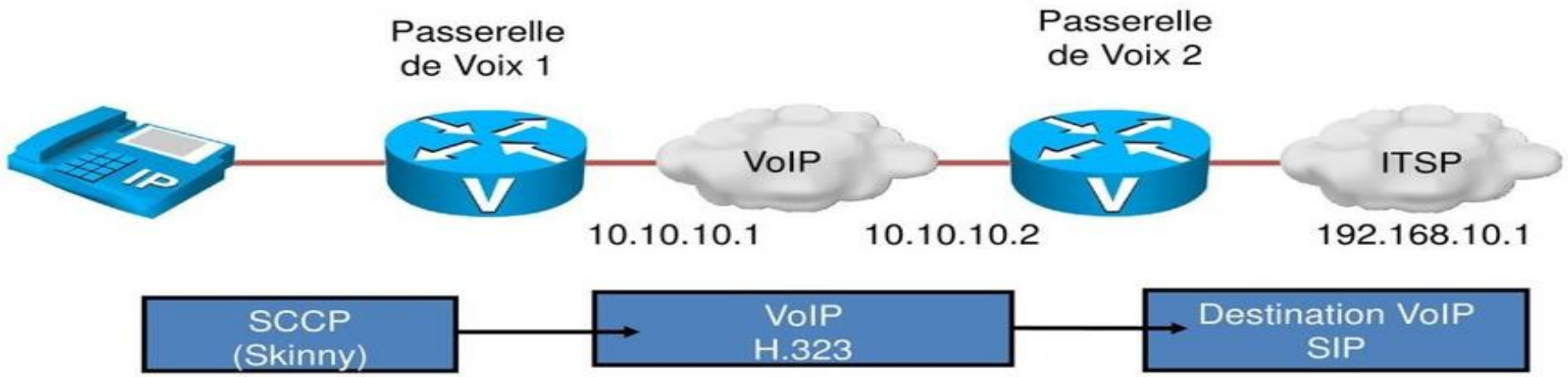
1. Voix sur IP (VoIP)
2. Protocoles de signalisation VOIP
3. Qualité de Services IP
4. Préparer le réseau pour la prise en charge de la voix

Protocoles de signalisation

- La signalisation génère et surveille les informations de contrôle d'appel entre deux points de terminaison pour:
  - Établir la connexion
  - Surveiller la connexion
  - Libérer la connexion
- Le protocole de signalisation doit passer la signalisation de surveillance, d'information, et d'adresse.
- Les protocoles de signalisation peuvent être Pair-à-pair ou basés sur le modèle Client/Serveur.
- Le modèle Pair-à-pair permet aux points de terminaison de contenir l'intelligence de passer des appels sans assistance.
- Le modèle Client / serveur met le point final sous le contrôle d'un point d'intelligence centralisée.

→ Les protocoles de signalisation sont utilisés dans les réseaux VoIP pour mettre en place de nouveaux appels, gérer les appels en cours, mettre fin à des appels, passer les informations de signalisation, passer la signalisation de surveillance, et passer la signalisation d'adresse.

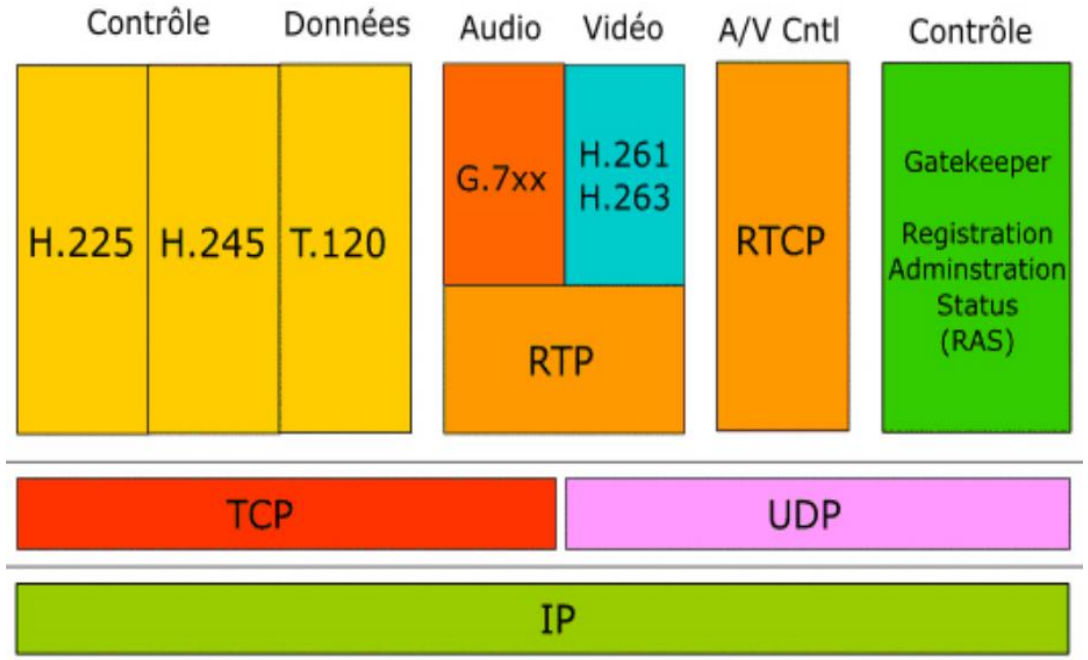
Protocoles de signalisation



- **SCCP** est un protocole propriétaire utilisé entre les téléphones IP unifiés Cisco et les produits de contrôle d'appel des communications unifiées Cisco.
- **H.323** est un protocole stable, mature, indépendant du vendeur, et largement déployé.
- **SIP** est un protocole émergent fondé sur les aspects des protocoles existants. Il est encore en évolution.

Le protocole H323

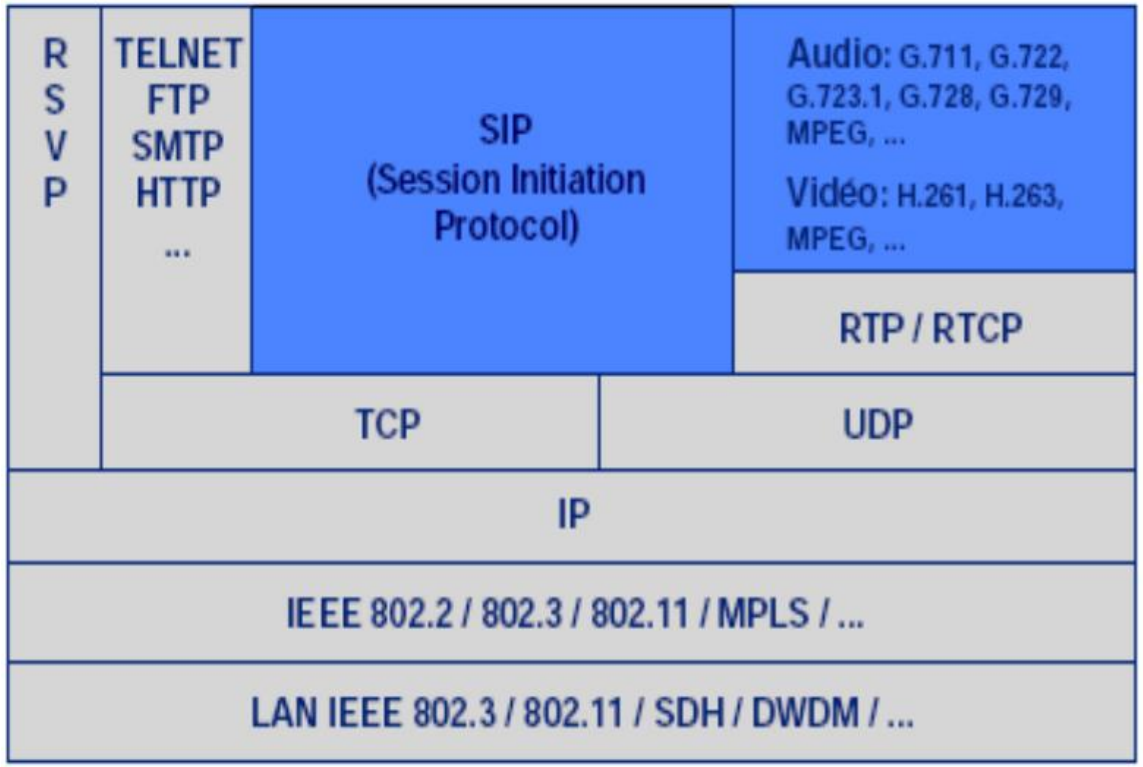
- Le protocole H323 défini : Les échanges de données Vidéo et Audio entre des terminaux multimédia en temps réel à travers le réseau Internet ou des LANs sans garantie de service.
  - Des terminaux.
  - Des passerelles.
  - Des Gatekeeper (portiers).
  - Des contrôleurs multipoints.
  - Il se décompose en un ensemble de sous protocoles.
- La norme H.323 propose des bases pour le transport de la voix, de la vidéo et des données sur des réseaux IP.
- Il fonctionne en mode non connecté et sans garantie de qualité de service
- Il définit les protocoles nécessaires à partir de la couche transport du modèle OSI



PARTIE 7

Le protocole SIP

- SIP ressemble au protocole HTTP (codage ASCII, codes de réponse par exemple). Le client envoie des requêtes au serveur, qui lui renvoie une réponse.
- Les méthodes de base sont :
  - INVITE permet à un client de demander une nouvelle session
  - ACK confirme l'établissement de la session
  - CANCEL annule un INVITE en suspens
  - BYE termine une session en cours.
- Les codes de réponse sont similaires à HTTP : 100 Trying / 200 OK / 404 Not Found
- En revanche, SIP diffère de HTTP du fait qu'un agent SIP (User Agent, UA) joue habituellement à la fois les rôles de client et de serveur. C'est-à-dire qu'il peut aussi bien envoyer des requêtes, que répondre à celles qu'il reçoit.
- Ouvert et standard tout comme le H323.
- Simple en version de base: SIP est simple voire simpliste et très similaire à HTTP. Le protocole s'est complexifié pour permettre une meilleurs interconnexion avec les réseaux téléphoniques classiques.
- Flexible : SIP peut être utilisé pour tout type de sessions multimédia.
- Points communs avec H323 : l'utilisation du protocole RTP

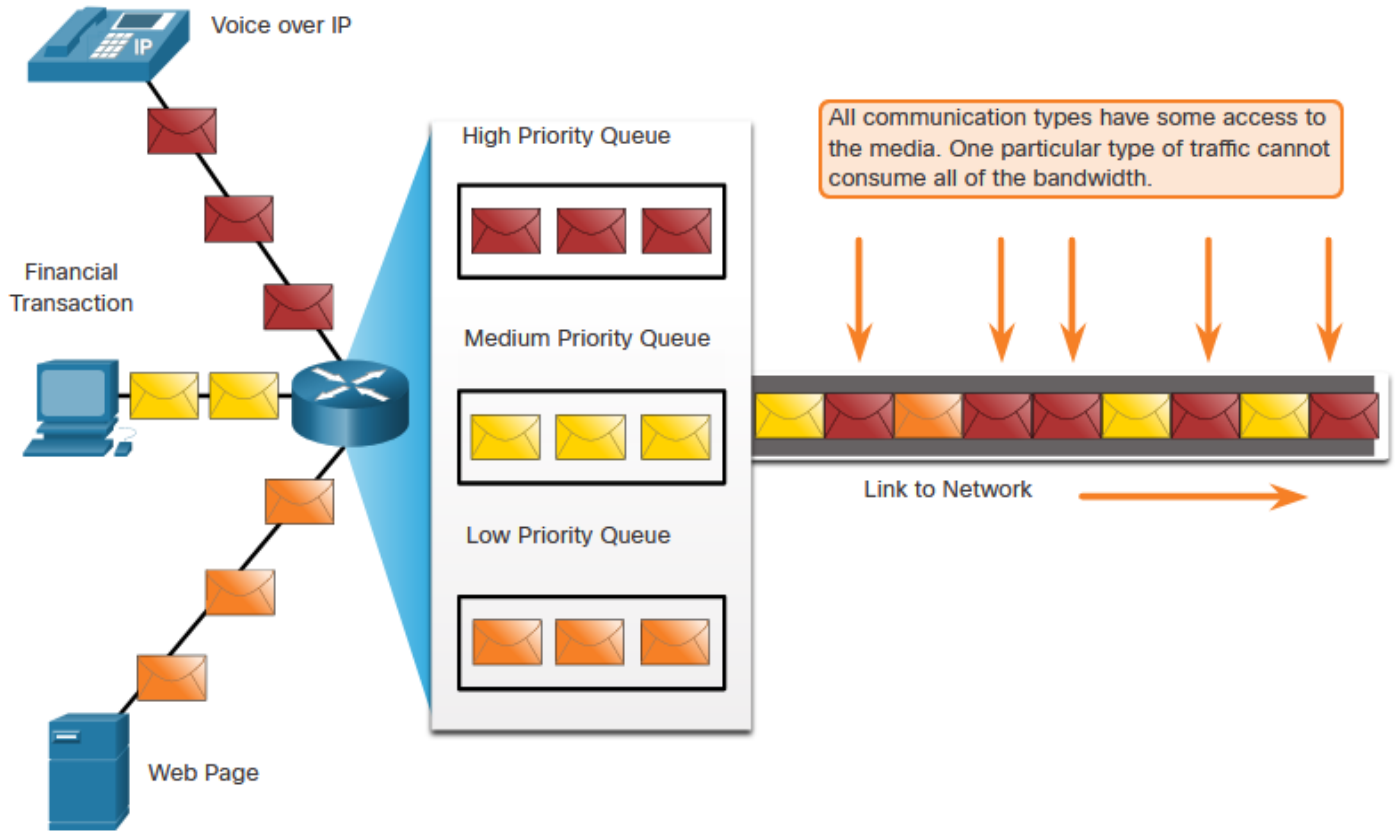


CHAPITRE 2

Décrire l'architecture VOIP

1. Voix sur IP (VoIP)
2. Protocoles de signalisation VOIP
3. Qualité de Services IP
4. Préparer le réseau pour la prise en charge de la voix

Hiérarchisation du trafic



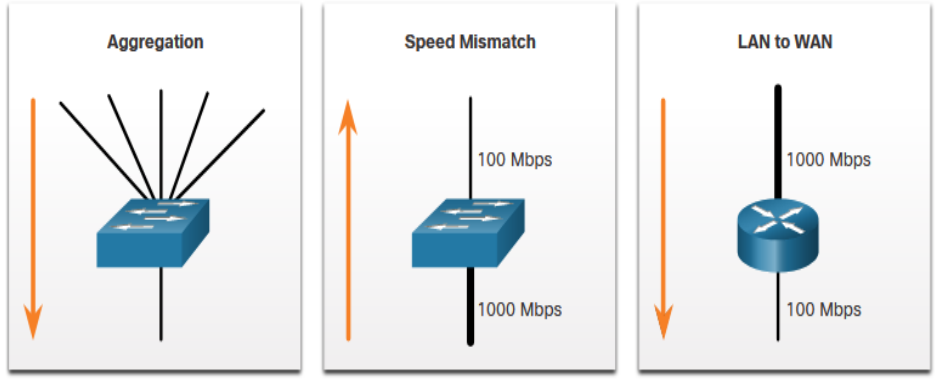
Bande passante, congestion, délai et gigue

Bande passante

- La bande passante réseau est mesurée en bits pouvant être transmis en une seconde, soit en «bits par seconde» (bits/s).

Congestion

- La congestion d'un réseau entraîne des délais. Une interface est encombrée lorsqu'elle reçoit plus de trafic que le volume qu'elle peut prendre en charge. Les points de congestion d'un réseau sont idéals pour l'implémentation d'un mécanisme de QoS.
- Les points de congestion typiques sont l'agrégation, la disparité de débit et la liaison du LAN vers le WAN.



Qualité de transmission réseau

- **Délai**

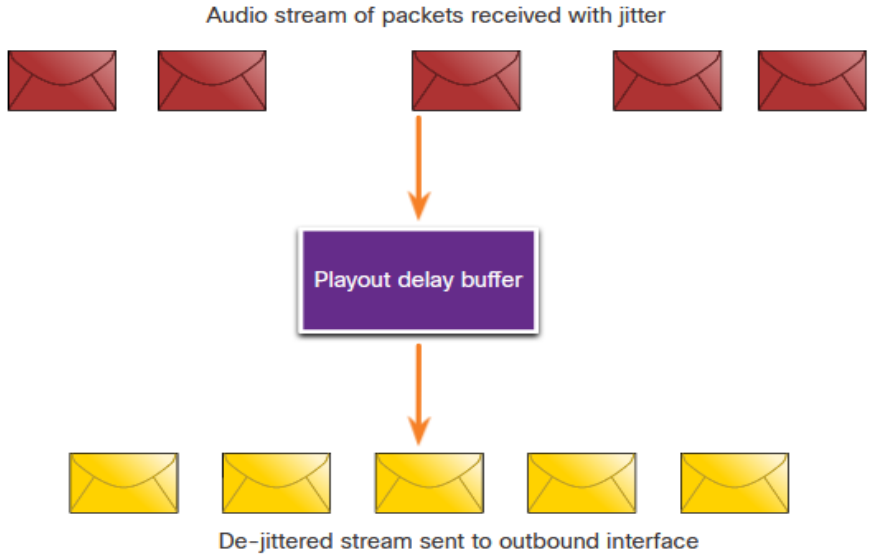
Le délai ou la latence désigne le temps nécessaire à un paquet pour passer de la source à la destination.

Délai	Description
Délai lié au code	Durée fixe nécessaire à la compression des données au niveau de la source avant la transmission au premier appareil d'interconnexion des réseaux, généralement un commutateur
Délai du groupage par paquets	Durée fixe nécessaire à l'encapsulation d'un paquet avec toutes les informations d'en-tête requises
Délai de mise en file d'attente	Durée variable d'attente d'une trame ou d'un paquet avant d'être transmis sur la liaison
Délai de sérialisation	Délai fixe nécessaire à la transmission d'une trame vers le câble.
Délai de propagation	Durée variable nécessaire au passage de la trame entre la source et la destination.
Délai de gigue	Durée fixe nécessaire au stockage en mémoire tampon d'un flux de paquets, puis à son envoi à intervalles réguliers

Perte de paquets

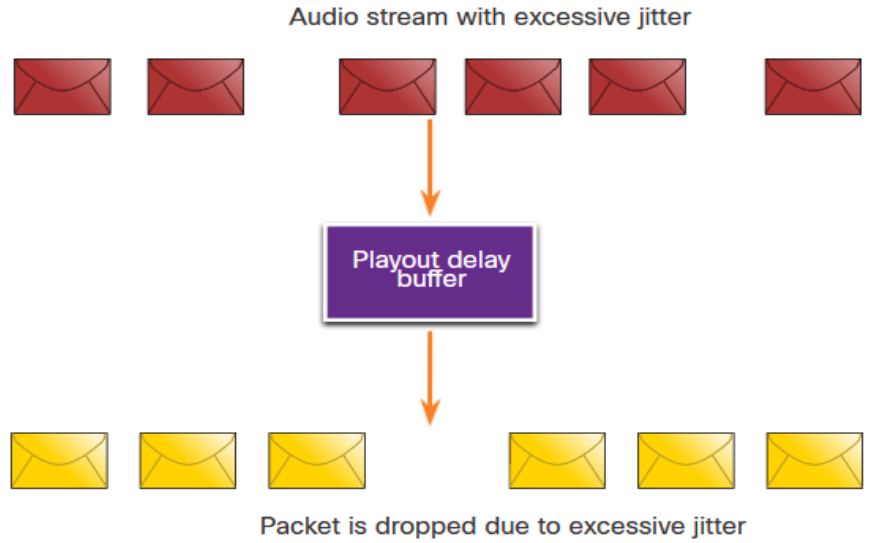
Sans mécanismes de QoS, soumis à une contrainte temporelle, tels que la vidéo en temps réel et la voix, seront abandonnés à la même fréquence que les données non soumises à cette contrainte

- Lorsqu'un routeur reçoit un flux de données audio numérique RTP (Real-Time Protocol) pour la voix sur IP (VoIP), il doit compenser la gigue générée en utilisant la mise en mémoire tampon.
- La mise en mémoire tampon consiste à mettre les paquets dans un tampon pour ensuite les diffuser en flux régulier.



Si la gigue est forte au point que certains paquets arrivent en dehors de la mise de ce tampon, ces paquets sont ignorés et les coupures s'entendent dans l'enregistrement sonore.

- Si un seul paquet est perdu, le processeur de signal numérique (DSP) rajoute ce qu'il pense correspondre à l'enregistrement sonore manquant et l'utilisateur n'entendra rien.
- Cependant, lorsque la gigue est trop importante pour que le DSP compense les paquets manquants, des problèmes de son surviennent.



Remarque: Dans un réseau correctement conçu, ce phénomène doit être proche de zéro.

Caractéristiques du trafic

Les différents types de trafics (voix, vidéo et données) impliquent des besoins extrêmement variés en termes de réseau.

○ Voix

Le trafic vocal est prévisible et fluide et très sensible aux délais et aux paquets abandonnés.

- Les paquets vocaux doivent bénéficier d'une priorité plus élevée que le reste du trafic.

Caractéristiques du trafic voix	Requêtes unidirectionnelles
• Fluide • Minimal • Sensible aux pertes • Sensible aux retards • Priorité UPD	• Latence ≤ 150ms • Gigue ≤ 30 ms • Perte ≤ 1% bande passante (30-128 Kbit/s)

○ Vidéo

Le trafic peut être imprévisible, incohérent et en salve. Contrairement à la voix, la vidéo récupère moins bien en cas de perte et comporte un plus grand volume de données par paquet.

Caractéristiques du trafic vidéo	Requêtes unidirectionnelles
• En salves • Gourmand • Sensible aux pertes • Sensible aux retards • Priorité UPD	• Latence ≤ 200-400 ms • Gigue ≤ 30-50 ms • Loss ≤ 0.1 – 1% • Bande passante (384 Kbps - 20 Mbps)

○ Données

Les applications de données qui ne tolèrent pas la perte de données, comme les e-mails et les pages web, utilisent le protocole TCP pour garantir que les éventuels paquets perdus lors du transit seront renvoyés.
Par rapport à la voix et à la vidéo, le trafic de données est relativement peu sensible aux pertes et aux retards. La qualité de l'expérience ou la QoE est importante à considérer avec le trafic de données.

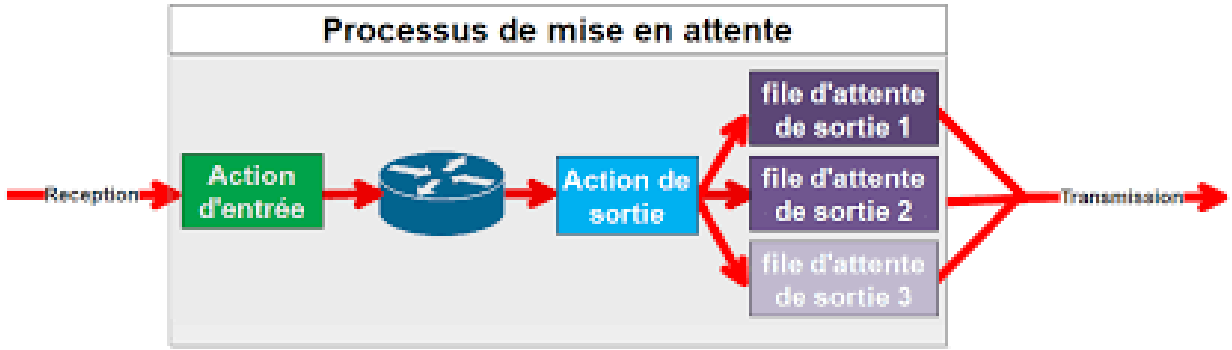
Caractéristiques du trafic de données
• Fluide/en salves (burst) • Minimal/gourmand • Insensible aux pertes • Insensible aux retards • Retransmission TCP

Algorithmes de mise en file d'attente

La mise en file d'attente est un outil de gestion des congestions qui permet de stocker en mémoire tampon, de hiérarchiser et, si nécessaire, de réorganiser les paquets avant leur transmission à la destination.

Différents algorithmes de mise en file d'attente sont disponibles:

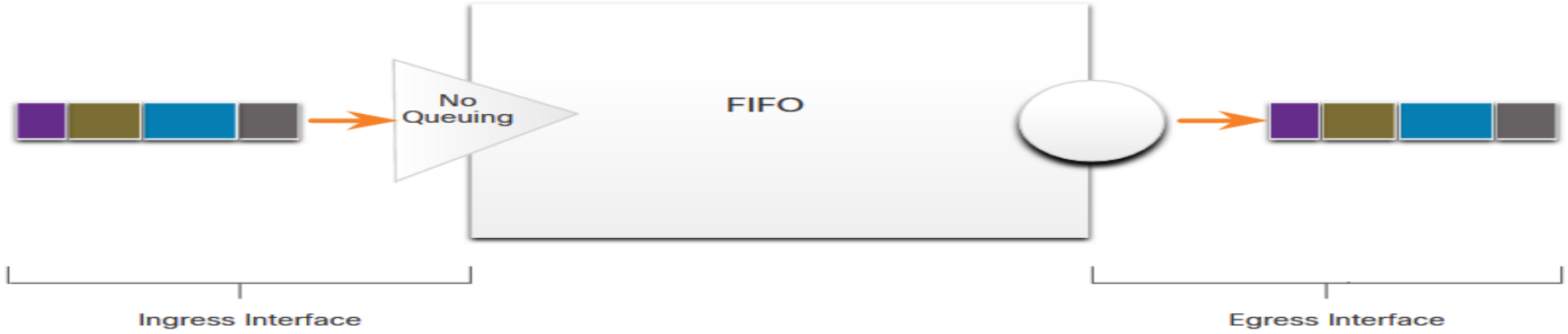
- **FIFO (First-In, First-Out)**
- **File d'attente équitable pondérée (WFQ)**
- **File d'attente équitable pondérée basée sur la classe (CBWFQ)**
- **File d'attente à faible latence (LLQ)**



Algorithmes de mise en file d'attente

- **Premier entrant premier sorti (FIFO)**

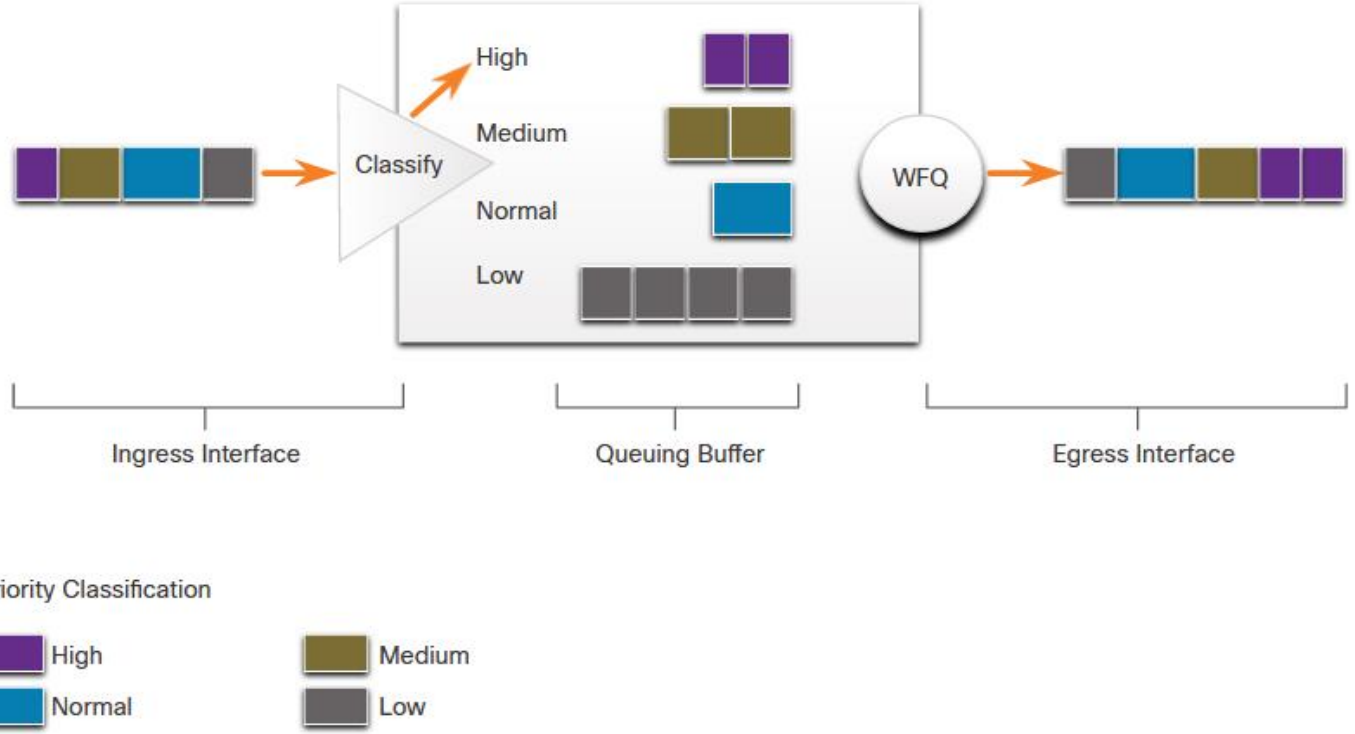
L'algorithme FIFO met en file d'attente les paquets et les transfère dans l'ordre de leur arrivée.



Algorithmes de mise en file d'attente

- **Mise en file d'attente équitable pondérée (WFQ)**

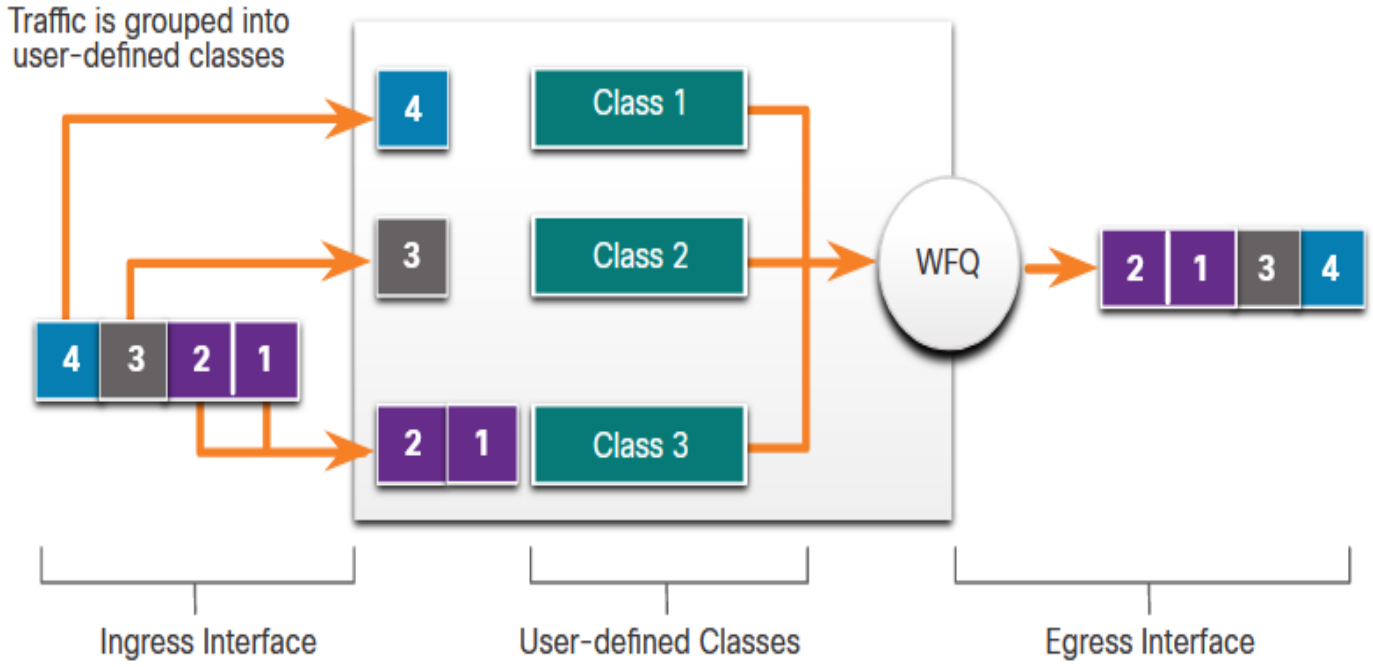
WFQ (Weighted Fair Queuing) est une méthode de programmation automatisée grâce à laquelle la bande passante est allouée au trafic réseau de façon équitable.



Algorithmes de mise en file d'attente

- **Mise en file d'attente pondérée basée sur les classes (CBWFQ)**

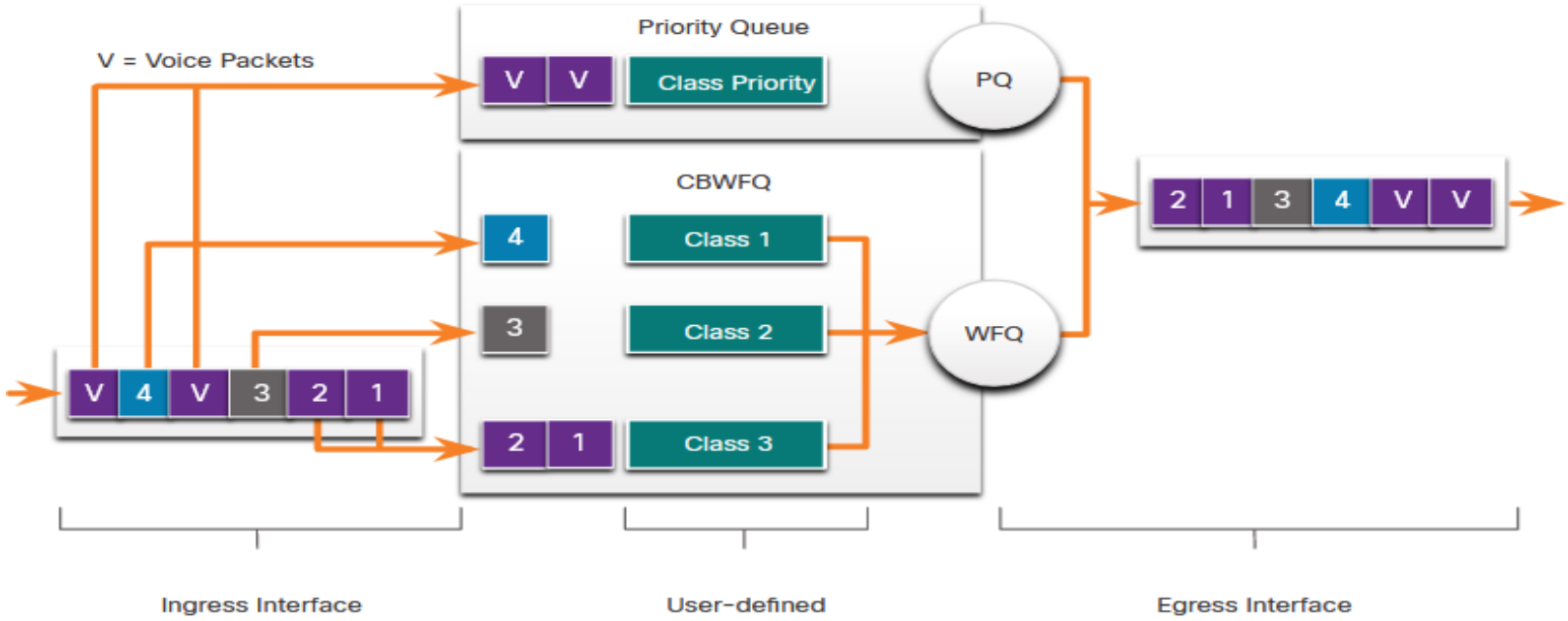
CBWFQ étend la fonctionnalité de mise en file d'attente pondérée (WFQ) standard afin de fournir la prise en charge des classes de trafic définies par l'utilisateur.



Algorithmes de mise en file d'attente

- **Mise en file d'attente à faible latence (LLQ)**

Avec la fonctionnalité LLQ, la stratégie CBWFQ bénéficie d'une capacité de mise en file d'attente à priorité stricte.



Sélection d'un modèle de politique de QoS approprié

Il existe trois modèles d'implémentation QoS. La QoS est implémentée dans un réseau à l'aide du modèle IntServ ou DiffServ.

Modèle	Description
Remise au mieux (**Best effort**)	• Il ne s'agit pas d'une implémentation dans la mesure où la stratégie QoS n'est pas explicitement configurée. • Ce modèle est utilisé lorsque la qualité de service n'est pas nécessaire.
Services intégrés (**IntServ**)	• Ce modèle propose une qualité de service très élevée aux paquets IP, avec remise garantie. • Il définit un processus de signalisation pour que les applications puissent indiquer au réseau qu'elles nécessitent une qualité de service spéciale pendant une certaine période et qu'il faut réserver de la bande passante. • Le modèle IntServ peut considérablement limiter l'évolutivité d'un réseau.
Services différenciés (**DiffServ**)	• Ce modèle offre une implémentation QoS très flexible et évolutive. • Les périphériques réseau détectent des classes de trafic et appliquent des niveaux de qualité de service spécifiques aux différentes classes de trafic.

Best Effort

La conception de base d'Internet prévoit la remise des paquets «Remise au mieux» et n'offre aucune garantie.

- Bénéfices et inconvénients du modèle Remise au mieux:

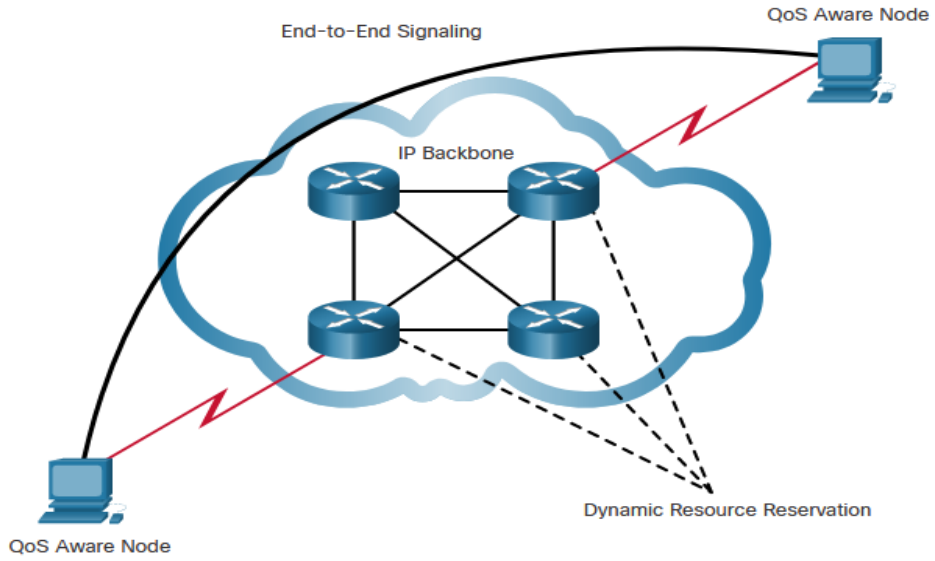
Bénéfices	Inconvénients
Il s'agit du modèle le plus évolutif.	Il n'offre aucune garantie de remise.
L'évolutivité est uniquement limitée par la bande passante disponible, laquelle affecte alors l'ensemble du trafic	Le délai et l'ordre de remise des paquets sont aléatoires et rien ne garantit leur arrivée.
Aucun mécanisme QoS spécial ne doit être implémenté.	Aucun paquet ne bénéficie d'un traitement préférentiel.
C'est le modèle le plus simple et rapide à déployer.	Les données essentielles sont traitées de la même façon que les e-mails normaux.

Services intégrés (IntServ)

IntServ offre la qualité de service de bout en bout dont les applications en temps réel ont besoin.

Dans le modèle IntServ, l'application demande un type de service spécifique au réseau avant de transmettre les données.

Bénéfices	Inconvénients
• Contrôle d'admission des ressources explicite, de bout en bout. • Contrôle d'admission de la stratégie par demande. • Signalisation des numéros de port dynamiques.	• Consommation importante de ressources due aux exigences de signalisation continue de l'architecture dynamique. • Approche basée sur les flux, inadaptée aux implémentations de grande taille, par exemple l'internet

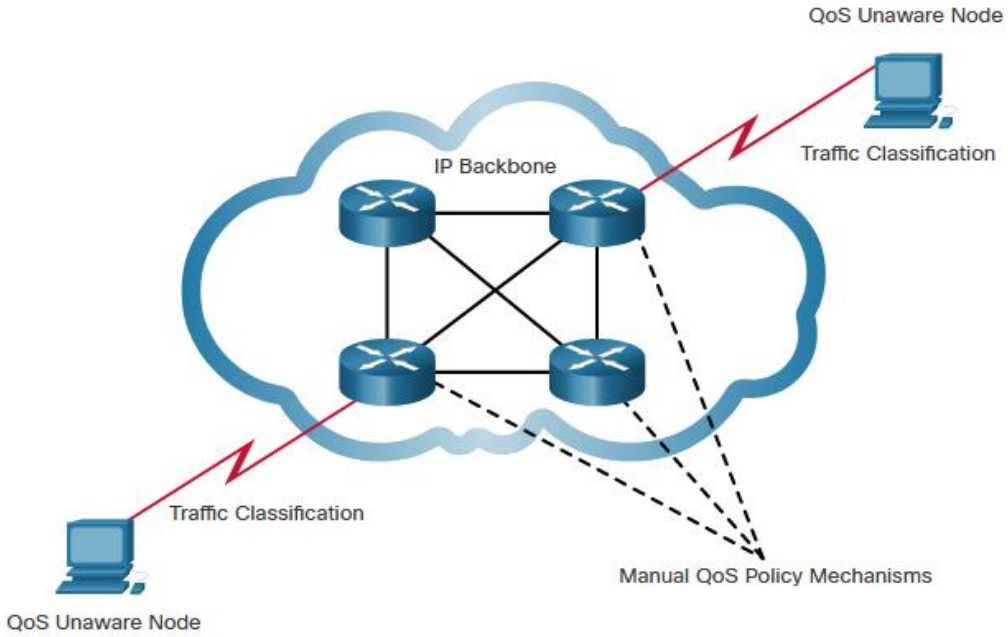


Services différenciés (DiffServ)

Le modèle QoS de services différenciés (DiffServ) propose un mécanisme simple et évolutif pour classer et gérer le trafic réseau.

DiffServ divise le trafic réseau en classes selon les besoins métier. Un niveau de service différent peut être ensuite affecté à chaque classe.

Bénéfices	Inconvénients
• Haute évolutivité • Large choix de niveaux de qualité	• Aucune garantie stricte de la qualité de service • Nécessite le fonctionnement conjoint de mécanismes complexes sur l'ensemble du réseau



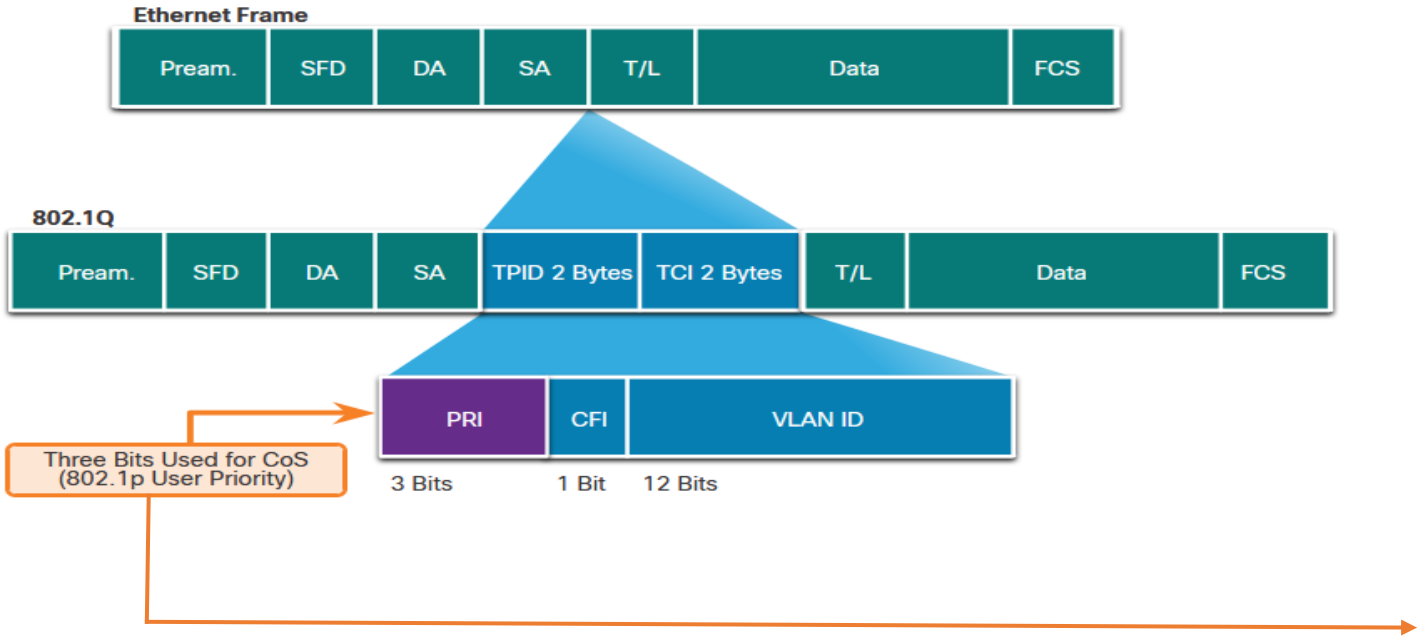
Outils d'implémentation QoS

Il existe trois catégories d'outils QoS, décrites dans le tableau.

Outils QoS	Description
Outils de classification et de marquage	• Les sessions, ou les flux, sont analysées afin de déterminer la classe de trafic à laquelle elles appartiennent. • Une fois la classe identifiée, les paquets sont marqués.
Outils de prévention de l'encombrement	• Les classes de trafic représentent des ressources réseau allouées, l'allocation étant définie dans la stratégie QoS. • La stratégie QoS identifie également le traitement appliqué au trafic (suppression sélective d'une partie du trafic, délai ou nouveau marquage) pour éviter la congestion du réseau. • Principal outil de prévention d'encombrement, WRED permet de réguler le trafic de données TCP en utilisant efficacement la bande passante avant que des dépassements de file d'attente n'entraînent des abandons de paquets.
Outils de gestion de l'encombrement	• Lorsque le trafic dépasse les ressources réseau disponibles, il est placé en file d'attente en attendant que des ressources se libèrent. • Le système Cisco IOS propose plusieurs outils de gestion de l'encombrement, dont les algorithmes CBWFQ et LLQ.

Marquage de couche 2

Le standard 802.1Q inclut également le schéma de hiérarchisation QoS plus connu sous le terme IEEE 802.1p. Le standard 802.1p utilise les trois premiers bits du champ Données de contrôle des balises (TCI). Ce champ de 3 bits, ou champ de Priorité (PRI), contient le marquage de la classe de service.

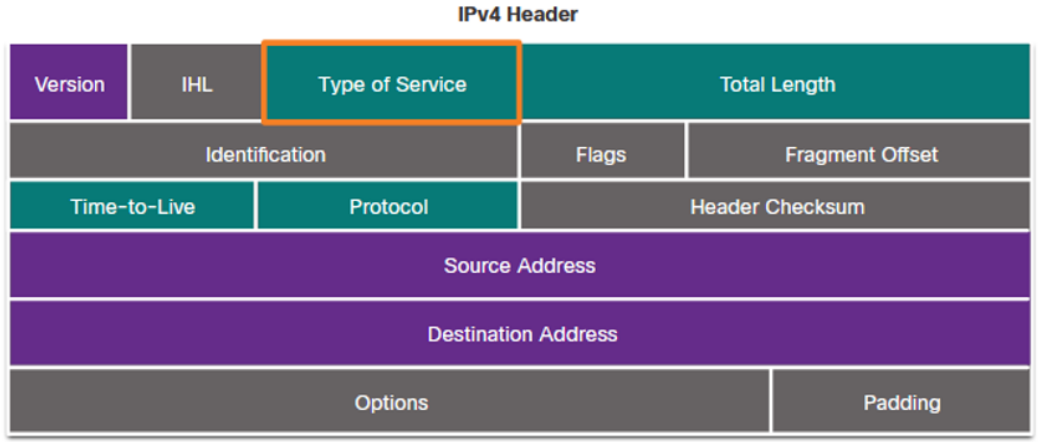


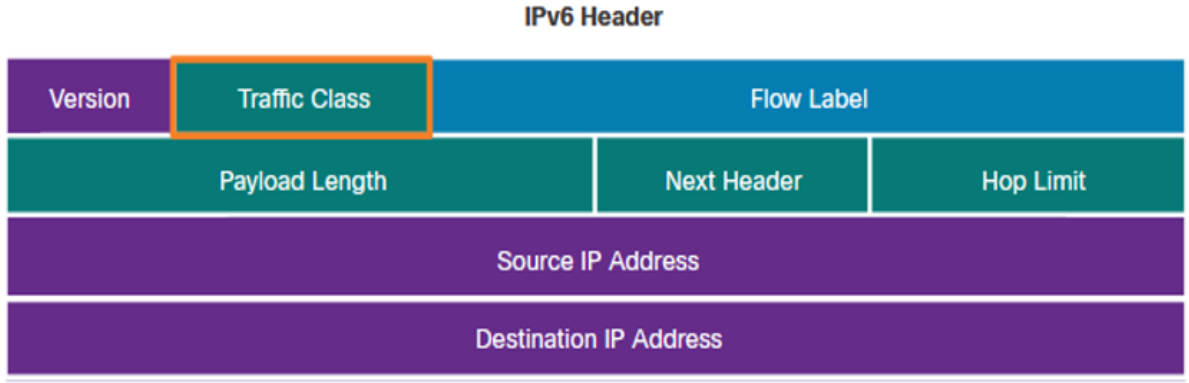
Valeur CoS	Valeur CoS binaire	Description
0	000	Données de Remise au mieux
1	001	Données de priorité moyenne
2	010	Données de priorité forte
3	011	Signalisation d'appels
4	100	Vidéoconférence
5	101	Support voix (trafic voix)
6	110	Réservé
7	111	Réservé

PARTIE 7

Marquage de couche 3

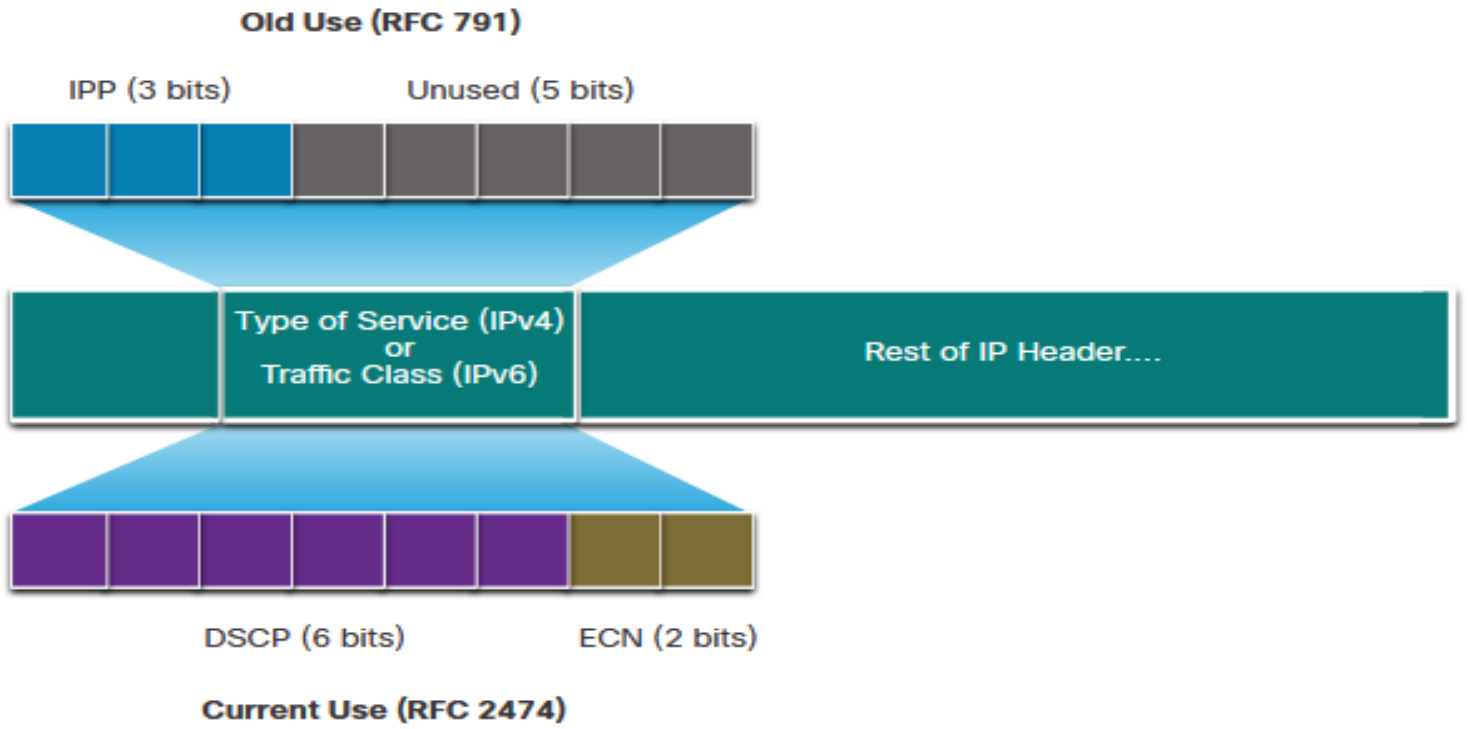
Le marquage des paquets avec IPv4 et IPv6 s'effectue à l'aide d'un champ de 8 bits situé au niveau des en-têtes de paquet.





Type de service et champ de classe de trafic

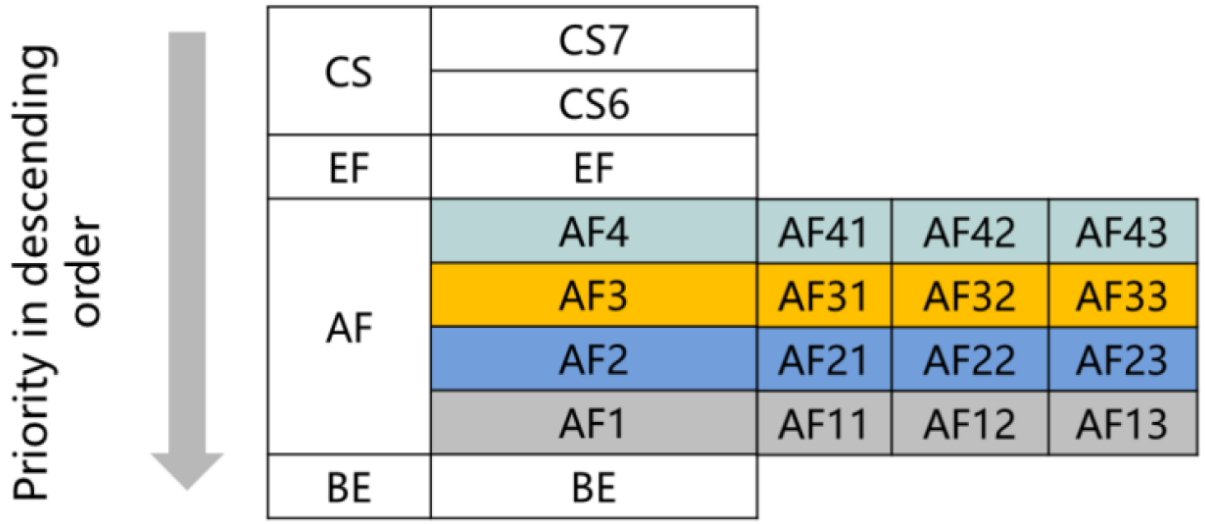
Le type de service (IPv4) et la classe de trafic (IPv6) portent le marquage des paquets tel qu'attribué par les outils de classification QoS.



Valeurs DSCP

Les 64 valeurs DSCP sont réparties en trois catégories:

- **Best effort** - Il s'agit de la catégorie par défaut pour l'ensemble des paquets IP. La valeur du champ DSCP est égale à 0. Un routage normal est appliqué au niveau de chaque saut. En cas de congestion sur un routeur, ces paquets seront abandonnés. Aucune politique de QoS n'a été implémentée.
- **Expedited Forwarding (EF)**: La RFC 3246 définit que le flux EF sera identifié comme un champ DSCP à 46 (binaire **101**110). Les trois premiers bits (101) correspondent à la valeur CoS 5, qui est utilisé à la couche 2 pour le trafic voix. Pour la couche 3, il est conseillé d'utiliser les valeurs EF uniquement pour marquer les paquets voix.
- **Assured Forwarding (AF)** - La norme RFC 2597 définit l'AF comme l'utilisation des 5 bits DSCP les plus significatifs pour indiquer les files d'attente et la préférence de suppression.
- **Class Selector (CS)** est utilisé pour transmettre des paquets de protocole par défaut. Mappez directement aux 3 bits du champ CoS et du champ IPP pour maintenir la compatibilité avec 802.1p et RFC 791.

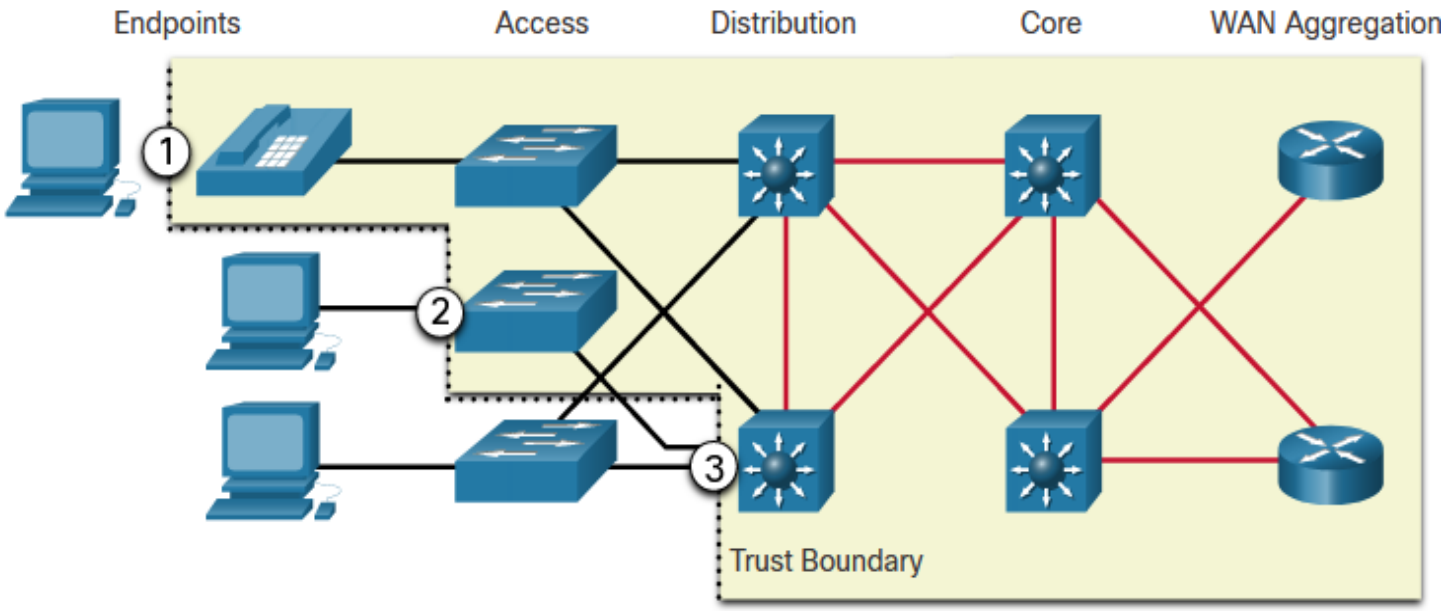


PARTIE 7

Limites de confiance

Le classement et le marquage du trafic doivent s'effectuer le plus près possible, techniquement et administrativement, de la source. Cela permet de définir la limite de confiance.

1. Les terminaux sécurisés disposent de fonctionnalités et de renseignements qui leur permettent de marquer le trafic des applications à l'aide de valeurs CoS de couche 2 et/ou DSCP de couche 3.
2. Pour les terminaux sécurisés, le trafic peut être marqué au niveau du commutateur de couche 2.
3. Le trafic peut également être marqué au niveau des commutateurs/routeurs de couche 3.



Prévention de la congestion

Les outils de prévention de congestion permettent de surveiller les charges de trafic sur les réseaux afin d'anticiper et d'éviter les encombrements au niveau des congestions du réseau commun et de l'internet avant que les encombrements ne deviennent un problème.

- WRED permet d'éviter l'encombrement des interfaces réseau en gérant les tampons et en autorisant la réduction ou la diminution du trafic TCP avant que ceux-ci soient remplis.

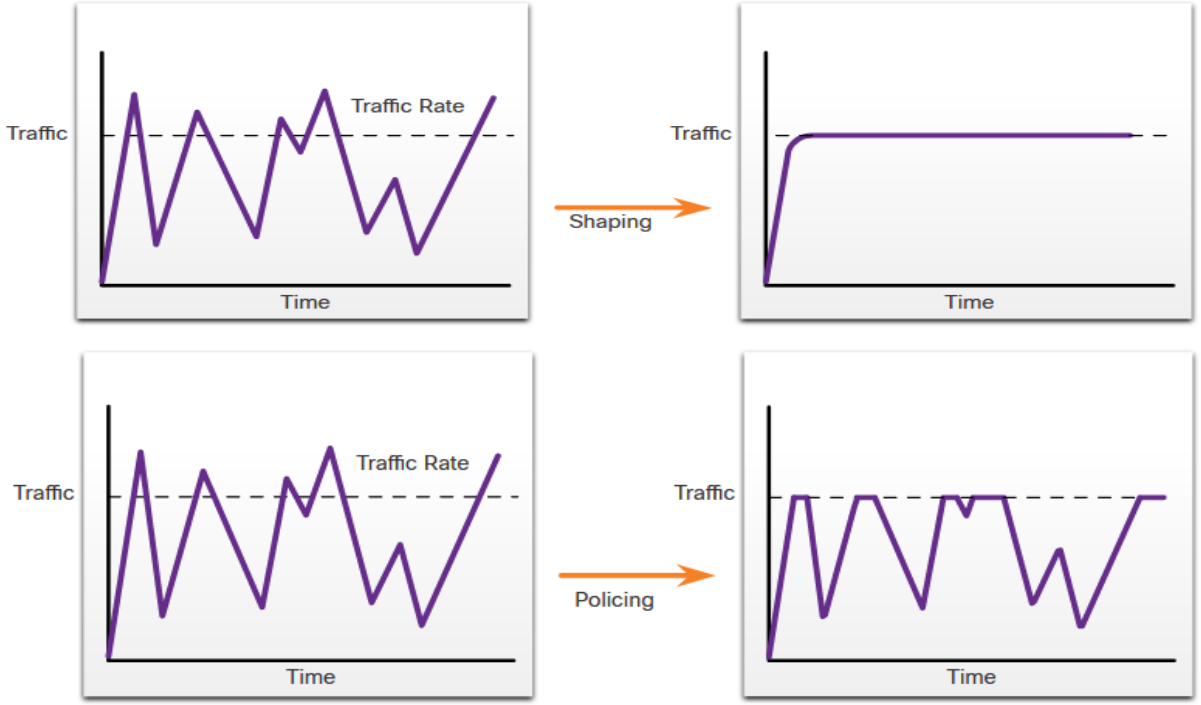
Mise en forme et régulation

La régulation et limitation du trafic sont deux mécanismes QoS qui permet d'éviter l'encombrement.

Conseils de régulation QoS

Voici quelques conseils qui aident à garantir la meilleure expérience pour les utilisateurs finaux:

- Activez la mise en file d'attente sur chaque périphérique dans le chemin entre la source et la destination.
- Classifier et marquer le trafic le plus près possible de la source.
- Mise en forme et régulation des flux de trafic le plus près possible de leurs sources.



CHAPITRE 2

Décrire l'architecture VOIP

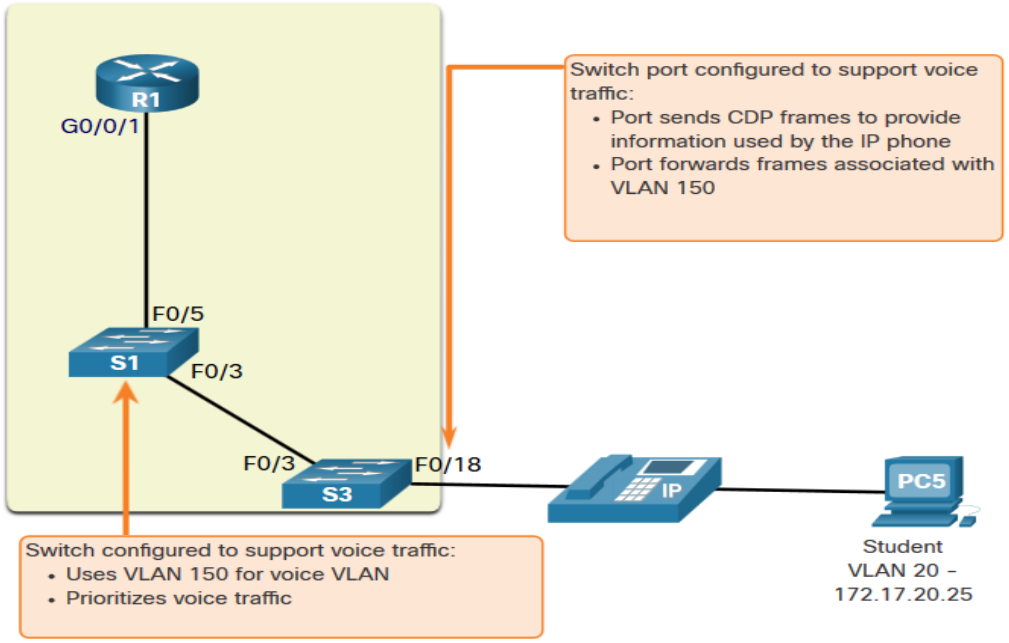
1. Voix sur IP (VoIP)
2. Protocoles de signalisation VOIP
3. Qualité de Services IP
4. Préparer le réseau pour la prise en charge de la voix

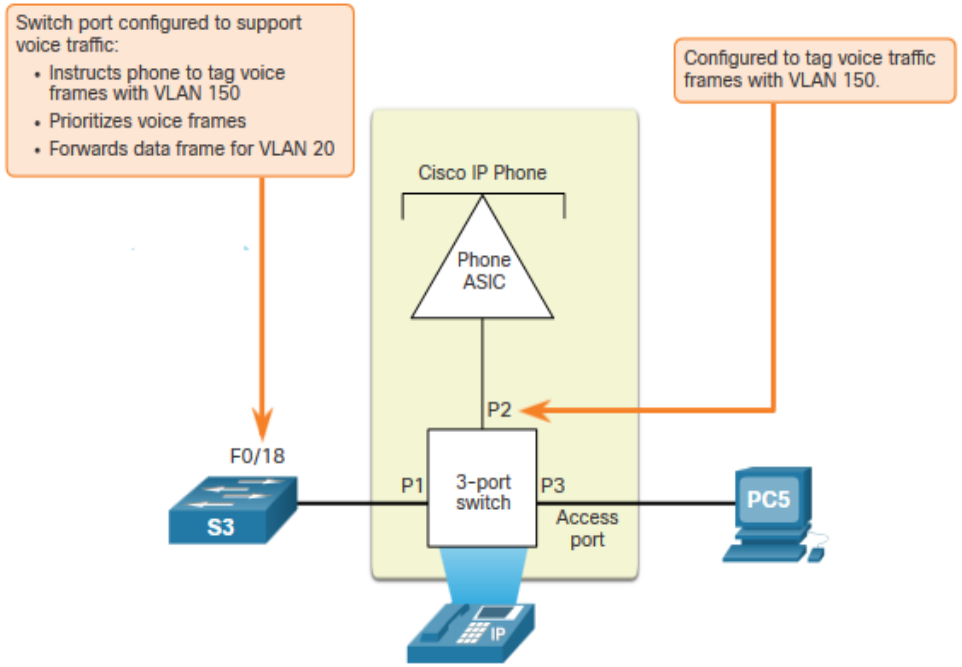
PARTIE 7

VLAN voix

L'ensemble du réseau doit être conçu pour prendre en charge la 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





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.

Configuration de VLAN Voix

Nécessite deux VLAN: un pour le trafic de données et un pour le trafic vocal

- Le VLAN d'accès (VLAN 20) est utilisé pour le PC qui est branché sur le téléphone IP.
- Le VLAN voix (VLAN 150) est utilisé pour la voix et la signalisation qui provient et se termine sur le téléphone IP Cisco.
- Le mode PortFast de spanning-tree permet au Spanning Tree d'activer le port plus rapidement.

```
S3(config)# interface FastEthernet 0/18
S3(config-if)# switchport access vlan 20
S3(config-if)# switchport mode access
S3(config-if)# switchport voice vlan 150
S3(config-if)# spanning-tree portfast
```

```
S3# show interface 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 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 150 (VLAN0150)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Appliance trust: none
```

Service DHCP

- Doit être personnalisé pour affecter un serveur TFTP au VLAN voix pour les téléphones IP correspondants.
- Configurer une étendue DHCP distincte pour les téléphones IP comme une meilleure pratique

1- Exclure toutes les adresses IP nécessaires.

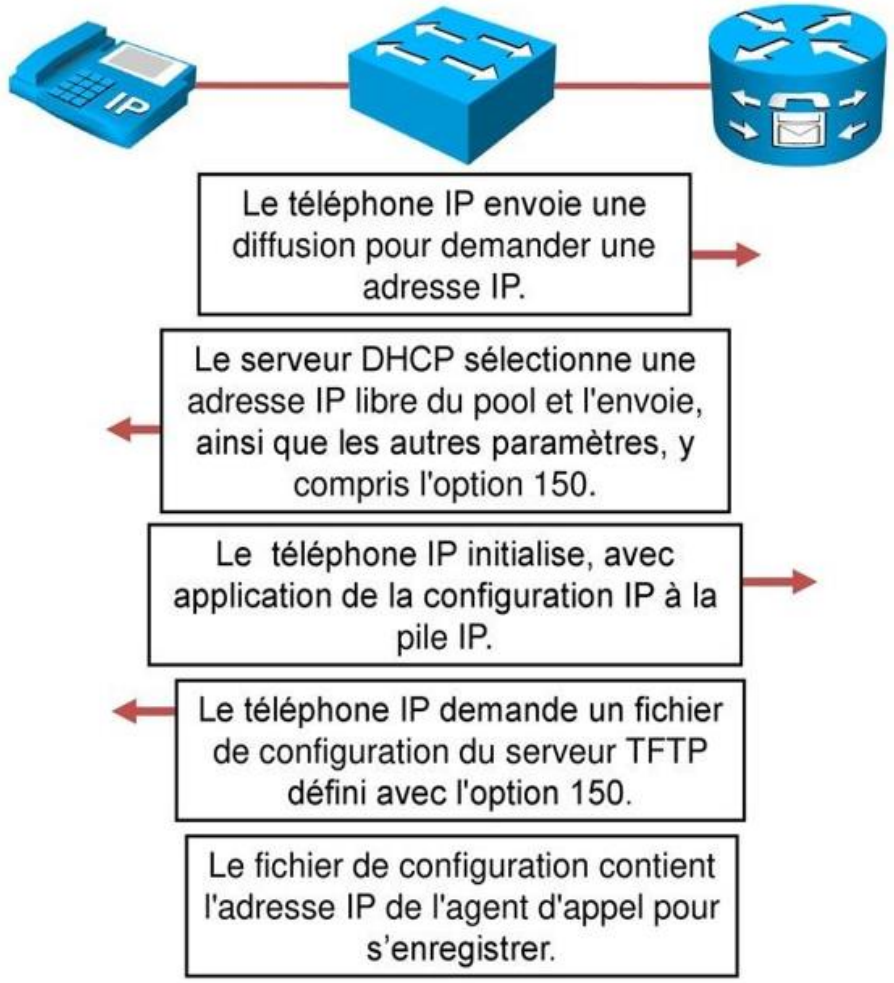
2- Créez un pool DHCP.

- Définir le réseau.
- Définir le routeur par défaut.
- Définir le paramètre DNS.
- Définir toute autre option (150).

3- Configurer l'adresse IP de l'assistant, si nécessaire

```
R1(config)# ip dhcp excluded-address 172.17.20.1  172.17.20.10
R1(config)# ip dhcp pool mypool
R1(dhcp-config)# network 172.17.20.0 255.255.255.0
R1(dhcp-config)# option 150 ip 172.17.20.1
R1(dhcp-config)# default-router 172.17.20.1
R1(dhcp-config)# dns-server 172.17.20.100
R1(dhcp-config)# exit
```

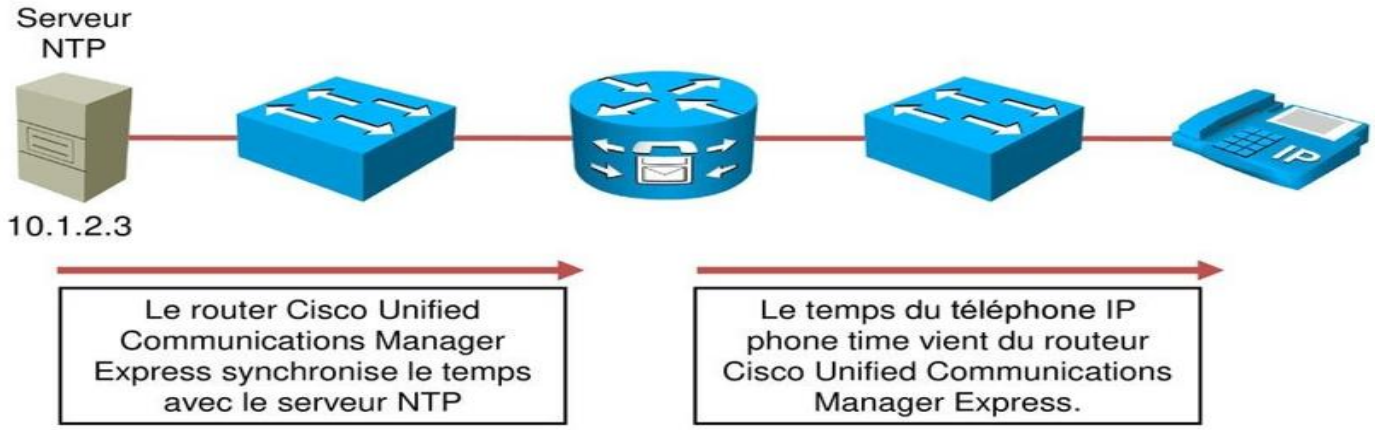
- Option 150 informe le téléphone IP de l'adresse IP du serveur TFTP
- Le serveur TFTP contient des fichiers de configuration et de firmware pour le téléphone IP.



Service NTP

- La synchronisation correcte de l'horloge est importante pour la performance, le dépannage et CDR (Call Detail Records).
- Le téléphone IP prend son temps affiché à partir de la plate-forme de contrôle d'appel à laquelle il est enregistré.

  (Exp : Cisco Unified Communications Manager Express)
- L'heure de l'horloge interne de la plate-forme de control des appels des communication unifiées Cisco doit être synchronisé avec un serveur NTP.
- Le temps de de la plate-forme de control des appels des communication unifiées est utilisé pour estampiller tous les messages syslog et les messages de trace.



Router(config)# **clock timezone** *zone hours-offset* : Définit le fuseau horaire local

Router(config)# **clock summer-time zone recurring** [*start-date end-date*] : Indique l'heure d'été

Router(config)# **ntp server** *ip-address* : Permet à l'horloge sur ce routeur pour être synchronisé avec le serveur NTP spécifié

CHAPITRE 3

Implémenter la solution de communication unifiée Cisco

Ce que vous allez apprendre dans ce chapitre :

- Mettre en oeuvre la solution VOIP de Cisco

1.5 heures

CHAPITRE 3

Implémenter la solution de communication unifiée Cisco

1. Gestionnaire de communications unifiées Cisco
2. Définition Ephone et Ephone-dn
3. Configuration de CallManager Expresse
4. Solutions de messagerie vocale et de présence
5. Les pairs de numérotation et les motifs de destination

Cisco Unified Communications

La structure de communications unifiées de Cisco combine le trafic voix, vidéo et données au sein d'une infrastructure réseau unique.

L'équipement de Cisco gère ces trois types de trafic tout en s'interfaçant avec tous les protocoles réseau basés sur des normes. En tirant parti d'un système multicouche, Cisco fournit un réseau de produits intégrés et coordonnés.

- **Couche d'infrastructure :**

  La couche d'infrastructure se compose de routeurs, de commutateurs et de passerelles vocales.

- **Couche de contrôle des appels :**

  La couche de contrôle des appels gère le traitement des appels, l'administration et les fonctionnalités du plan de numérotation et le contrôle des appareils.

- **Couche d'application :**

  Cisco maintient les applications indépendantes des fonctions de contrôle des appels et de l'infrastructure physique de traitement de la voix.

- **Couche de points de terminaison :**

  Les points de terminaison peuvent inclure un téléphone IP Cisco, un softphone d'ordinateur de bureau, du matériel d'appel vidéo, un smartphone et tout autre appareil de communication compatible.

Cisco Unified Communications

- Cisco fournit des services et des applications de communications IP depuis 1997, ce qui en fait le plus ancien de tous les fournisseurs.
- Ces services permettent aux clients de choisir parmi un nombre presque incalculable d'outils, permettant aux utilisateurs de structurer la plate-forme qui leur convient.

CUCM assure les avantages suivant :

- **Communications unifiées**

  CUCM permet aux organisations de consolider leur infrastructure de communication afin que les membres de l'équipe puissent communiquer uniquement via l'interface unifiée de Cisco.

- **Mobilité et flexibilité**

  Avec les communications unifiées, vous pouvez créer des espaces de travail transformationnels qui permettent aux employés de travailler là où c'est nécessaire.

- **Évolutivité**

  La licence pour CUCM est déterminée par le nombre total d'utilisateurs, de fonctionnalités utilisateur et d'appareils configurés, de sorte que les organisations ne paient que ce dont elles ont besoin.

- **Ouvert et interopérable**

  CUCM propose un vaste écosystème d'intégrations et de solutions tierces ainsi que des partenaires.

- **Sécurisé et conforme**

  CUCM prend en charge les derniers protocoles d'authentification, de cryptage et de communication.

Le système Cisco Unified Communications

Téléphone IP Cisco CP-7945G-CCME

Routeur (CME) CISCO 3825-CCME/K9

Téléphone IP Cisco CP-8865-K9=

Téléphone sans fil IP Cisco CP-8821-K9-BUN

Cisco Communications Manager BE 6000

Cisco Webex DX80

PARTIE 7

Cisco Unified Communications Manager

Cisco Unified Communications Manager (anciennement Cisco CallManager, maintenant connu sous le nom de Cisco Unified CM ou CUCM) est une infrastructure de gestion des appels et des sessions d'entreprise qui rationalise la communication et la collaboration d'équipe pour la main-d'œuvre hybride d'aujourd'hui.

CUCM réunit les téléphones IP enregistrés, les appareils mobiles, les ordinateurs de bureau et d'autres terminaux dans une seule plate-forme UC, quel que soit l'emplacement de l'utilisateur final. C'est l'architecture qui permet aux équipes et aux clients de se connecter sur leurs appareils préférés sur plusieurs canaux, notamment :

Téléphonie VoIP

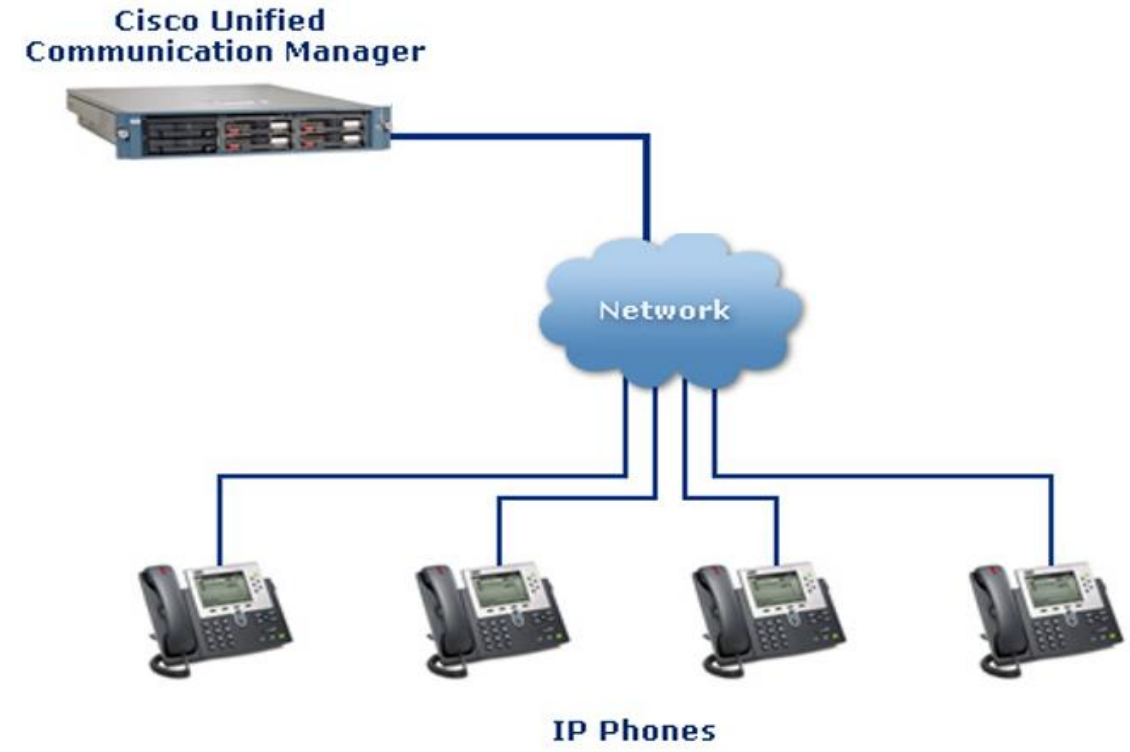
Conférences vidéo et rich-media

Chat d'équipe instantané

Messagerie avec présence de l'utilisateur

Centre de contact client

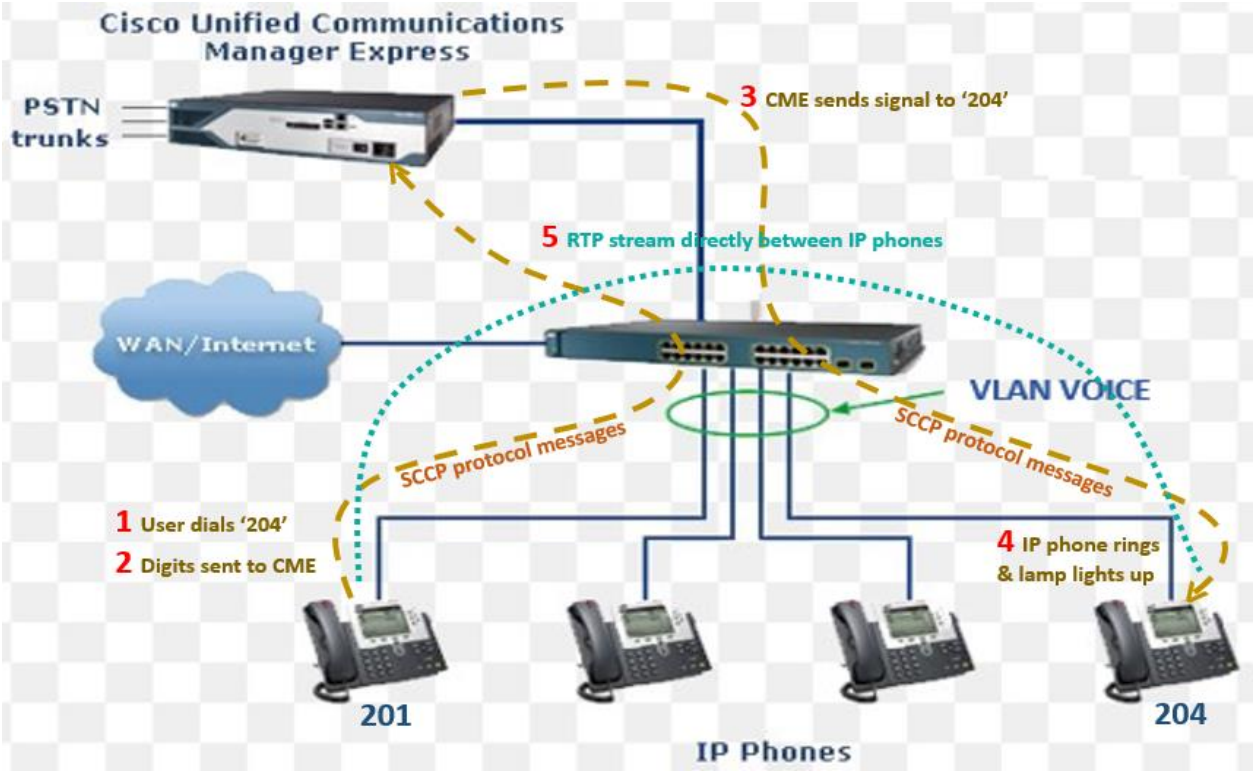
Applications externes Intégration de données



Le système Cisco CallManager Express

- Le système Cisco CallManager Express se compose d'un routeur (ou simplement d'un « boîtier » pour la gamme UC 500) qui sert de passerelle vocale (PBX) et d'un ou plusieurs VLAN qui connectent les téléphones IP et les appareils téléphoniques au routeur.
- Prend en charge les déploiements de jusqu'à 240 téléphones sur un seul routeur
- Etend les capacités d'un petit bureau qui étaient auparavant uniquement disponible pour les grandes entreprises
- Est basé sur le logiciel Cisco IOS
- Peut être administré par GUI ou CLI

- Une fois sous tension, les téléphones IP démarrent et s'enregistrent auprès de Cisco CallManager Express.
- S'il est configuré, le CallManager Express fournira une extension pour chaque téléphone IP et pourra alors établir ou supprimer des appels vers ou depuis les téléphones IP.
- Les téléphones IP et le routeur CallManager Express utilisent un protocole propriétaire appelé Skinny Client Control Protocol (SCCP) pour communiquer.
- Une fois l'appel établi, le protocole de transport en temps réel (RTP) sera utilisé pour transporter le flux audio.



PARTIE 7

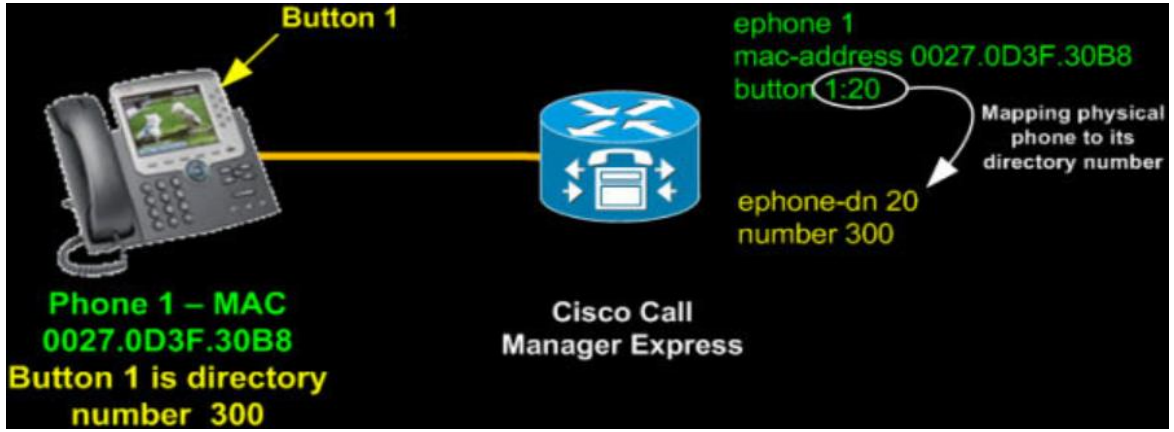
CHAPITRE 3

Implémenter la solution de communication unifiée Cisco

1. Gestionnaire de communications unifiées Cisco
2. Définition Ephone et Ephone-dn
3. Configuration de CallManager Expresse
4. Solutions de messagerie vocale et de présence
5. Les pairs de numérotation et les motifs de destination

Ephone et Ephone-dn

- Tous les types de PBX se composent de téléphones physiques et de leurs numéros de répertoire internes (extensions).
- Le même concept s'applique dans CallManager Express.
- Les téléphones physiques sont appelés « ephone » **Ephone = Ethernet Phone**
- Les numéros d'annuaire sont appelés « ephone-dn » **Ephone-dn = Ethernet Phone Directory Number**
- Un ephone peut représenter n'importe quel type/modèle de téléphone physique disponible et pris en charge par Cisco.
- CallManager Express reconnaîtra un appareil téléphonique physique à partir de sa configuration ephone qui contient également l'adresse MAC de l'appareil.
- Par exemple, un téléphone IP Cisco 7945 avec une adresse MAC de 0027.0D3F.30B8 représente l'ephone. Le numéro d'annuaire 32 attribué à ce téléphone représente le numéro ephone-dn.
- Les numéros de répertoire sont attribués aux touches de ligne sur les téléphones lors de la configuration.
- Cela signifie que chaque téléphone IP physique doit être configuré comme un ephone.



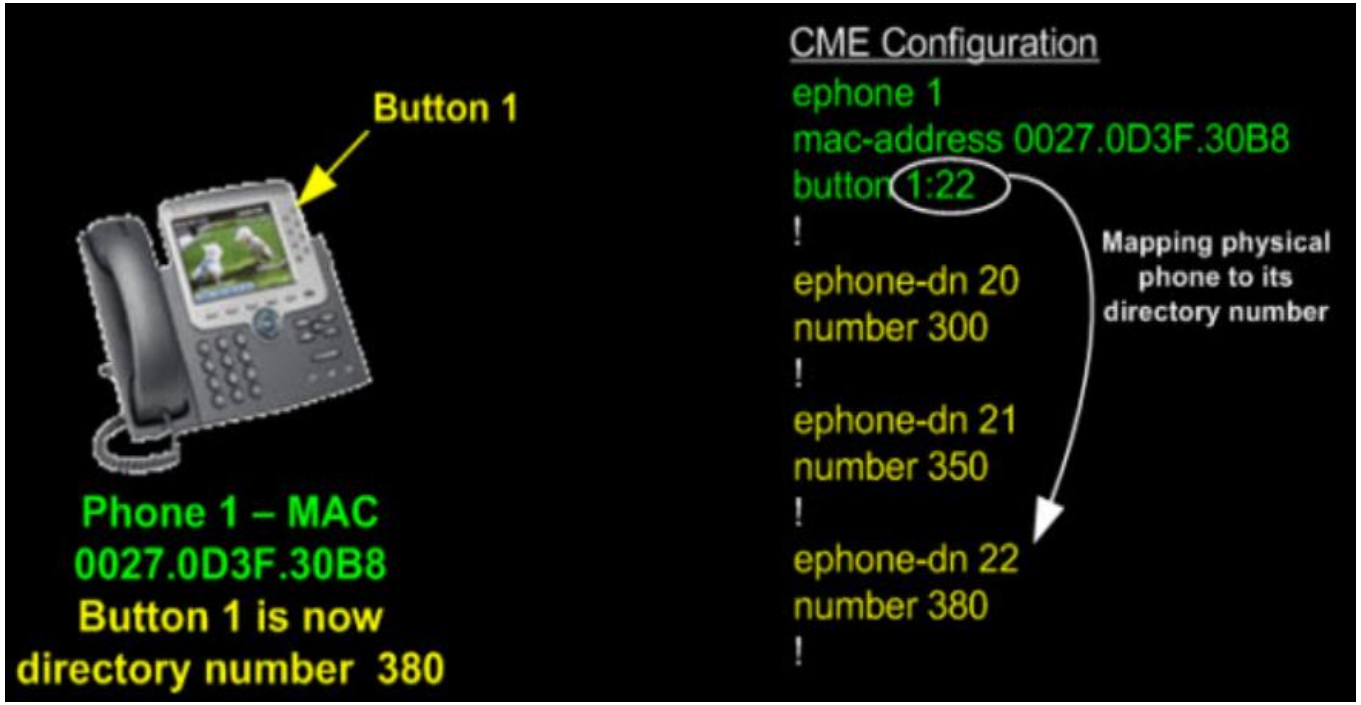
PARTIE 7

Configuration Ephone et Ephone-dn

La configuration d'un téléphone IP dans CME est un processus simple et implique la création d'une entrée ephone et ephone-dn.

L'ephone contient l'adresse MAC du téléphone et la configuration des boutons, tandis que l'ephone-dn contient le numéro d'annuaire attribué au téléphone IP.

Dans l'exemple ci-dessus, la configuration de l'ephone 1 lie le premier bouton du téléphone (bouton 1) à l'ephone-dn 20. Étant donné que l'ephone-dn 20 a été configuré avec le numéro d'annuaire 300, le téléphone IP se verra attribuer le numéro d'annuaire 300.



Configuration Ephone et Ephone-dn

- Crée une extension (ephone-dn) pour une ligne de téléphone IP Cisco
  CMERouter(config)# **ephone-dn *dn-tag***
- Associe un numéro de répertoire à l'instance de ephone-dn
  CMERouter(config-ephone-dn)# **number *dn-number***
- Définit le nombre définissable maximum de phone-dn qui peut être configuré dans le système
  CMERouter(config-telephony)# **max-dn *max-dn***
- Définit le nombre maximum d'ephones définissable qui peuvent être configurés dans le système
  CMERouter(config-telephony)# **max-ephones *max-ephones***

Configuration Ephone-dn

- Crée une instance d'ephone et passe en mode sous-configuration de l'ephone
  router(config)# **ephone *phone-tag***
- Associe l'adresse MAC définie du dispositif physique avec l'ephone
  router(config-ephone)# **mac-address *mac-address***
- Associe l'ephone-dn (s) avec un bouton spécifique (s) sur le téléphone IP
  router(config-ephone)# **button button-number {separator} dn-tag [[button-number {separator} dn-tag]]**

Configuration Ephone

Différents séparateurs sont disponibles depuis la ligne de commande :
- **:** — Sonnerie normale
- **b** — Bip mais pas de sonnerie
- **f** — Fonction de sonnerie
- **s** — Sonnerie silencieuse

PARTIE 7

CHAPITRE 3

Implémenter la solution de communication unifiée Cisco

1. Gestionnaire de communications unifiées Cisco
2. Définition Ephone et Ephone-dn
3. Configuration de CallManager Expresse
4. Solutions de messagerie vocale et de présence
5. Les pairs de numérotation et les motifs de destination

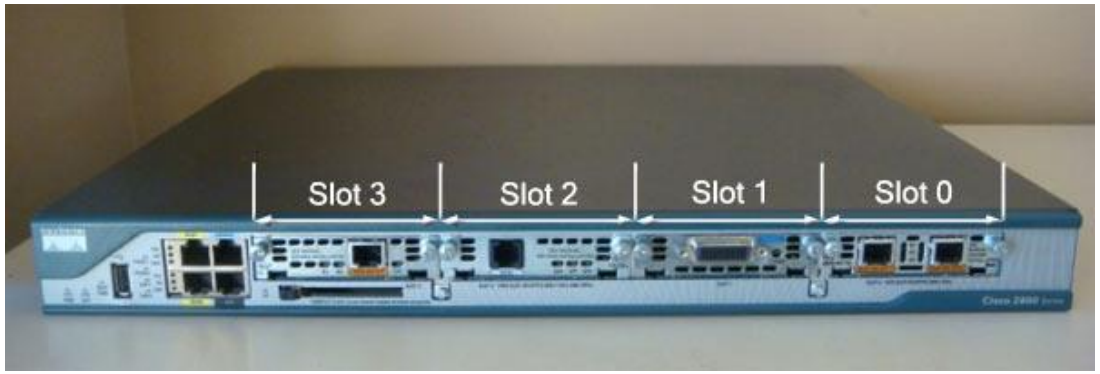
Interfaces de Cisco CallManager Express

Le système Cisco CallManager Express peut agir en tant que passerelle PSTN ainsi que gérer les téléphones IP.

Il existe différents types de connexions au RTPC, y compris les connexions numériques, VoIP et analogiques.

Le type de connexion utilisé dépendra de la densité des connexions nécessaires, de la technologie disponible dans la région, du coût des connexions et des interfaces présentes sur le routeur.

L'image ci-dessous montre un routeur Cisco 2801 rempli de 4 interfaces. Chaque interface est insérée dans l'un des quatre emplacements disponibles et, une fois le routeur sous tension, si l'IOS prend en charge l'interface installée, il la reconnaîtra automatiquement et fournira à l'administrateur l'accès aux commandes CLI appropriées afin qu'il puisse être configuré.



routeur Cisco 2801

Carte FXO 4 ports

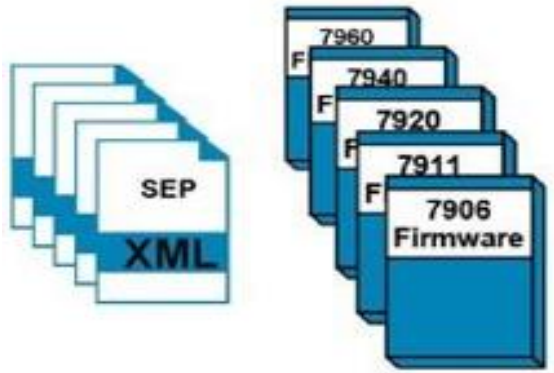
Cartes de données série et ISDN

PARTIE 7

Le firmware IP phone et les fichiers de configuration XML

- **Les fichiers de configuration XML**

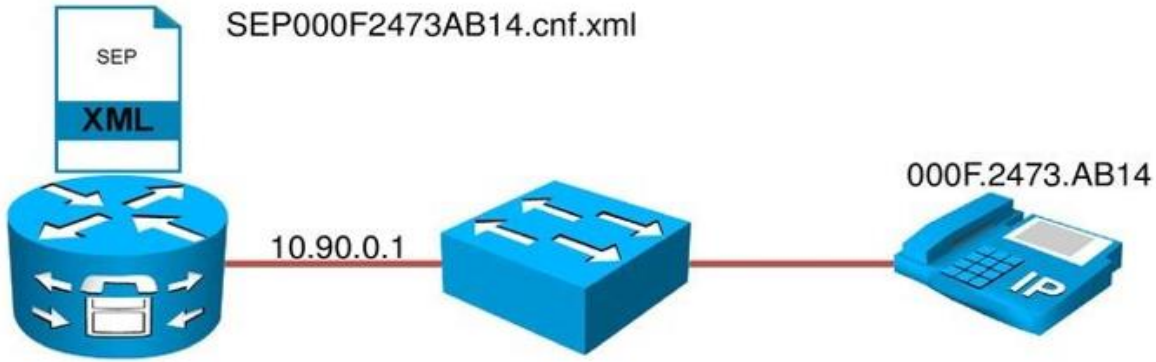
Certains fichiers sont nécessaires pour le bon fonctionnement d'un téléphone IP unifié Cisco :



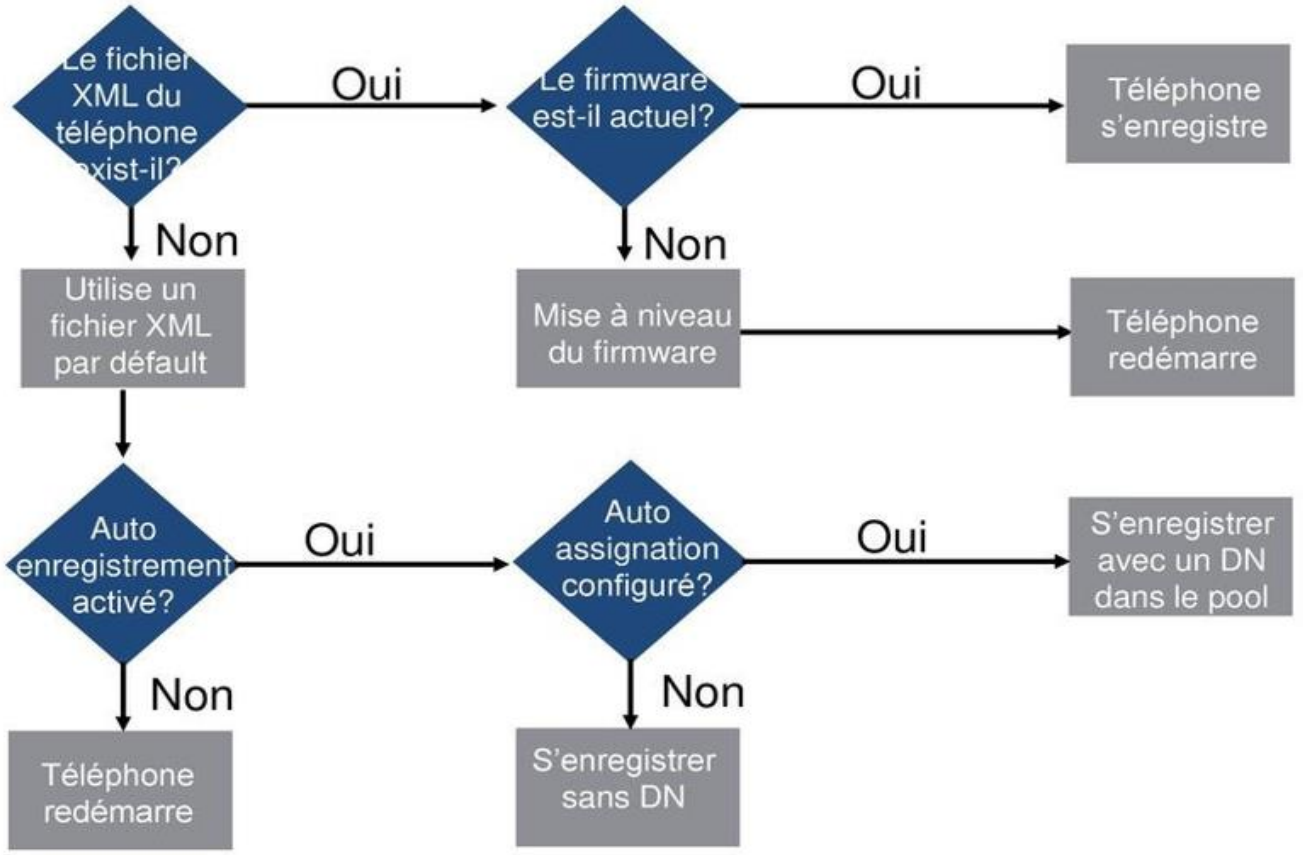
- **Le firmware IP Phone**

- XMLDefault.cnf.xml

- SEPAAAABBBBCCCC.cnf.xml (Sachant que AAAABBBBCCCC l'adresse MAC de l'appareil)



Organigramme d'enrengistrement



Fichier XML de configuration des appareils

XMLDefault.cnf.xml


```
<Default>
<callManagerGroup>
<members>
<member priority="0">
<callManager>
<ports>
<ethernetPhonePort>2000</ethernetPhonePort>
</ports>
<processNodeName>10.15.0.1</processNodeName>
</callManager>
</member>
</members>
</callManagerGroup>
<loadInformation6 model="IP Phone 7910">P00403020214</loadInformation6>
<loadInformation124 model="Addon 7914"></loadInformation124>
<loadInformation9 model="IP Phone 7935"></loadInformation9>
<loadInformation8 model="IP Phone 7940">P00303020214</loadInformation8>
<loadInformation7 model="IP Phone 7960">P00303020214</loadInformation7>
<loadInformation20000 model="IP Phone 7905"></loadInformation20000>
<loadInformation30008 model="IP Phone 7902"></loadInformation30008>
<loadInformation30002 model="IP Phone 7920"></loadInformation30002>
<loadInformation30019 model="IP Phone 7936"></loadInformation30019>
<loadInformation30007 model="IP Phone 7912"></loadInformation30007>
</Default>
```

SEP*AAAABBBBCCCC*.cnf.xml*

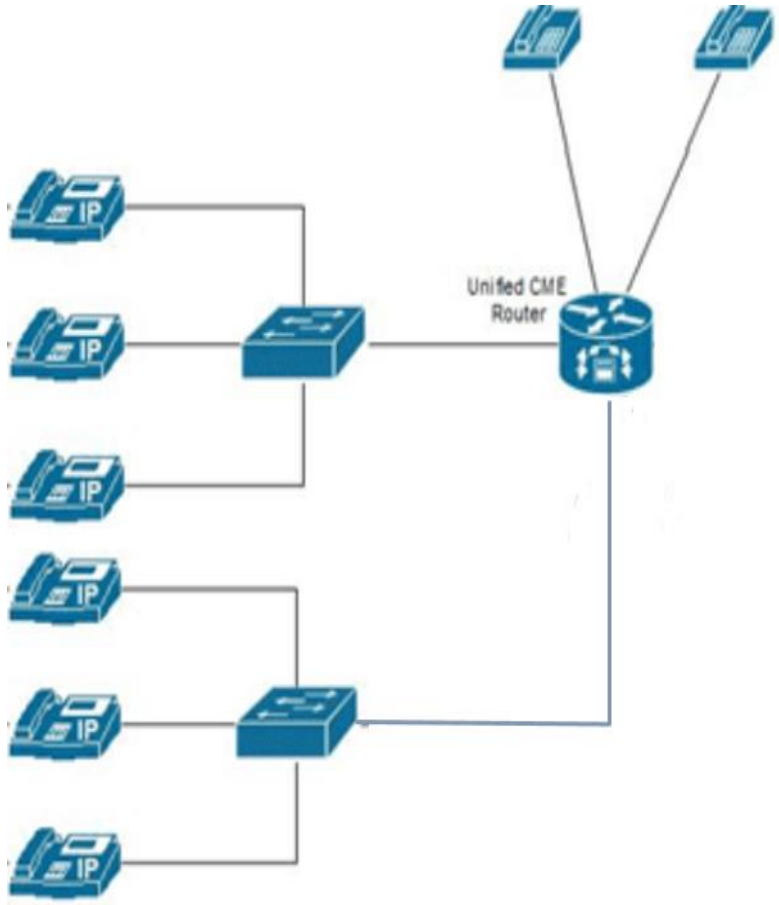
**AAAABBBBCCCC* = the MAC address

```
<device>
<devicePool>
<callManagerGroup>
<members>
<member priority="0">
<callManager>
<ports>
<ethernetPhonePort>2000</ethernetPhonePort>
</ports>
<processNodeName>10.15.0.1</processNodeName>
</callManager>
</member>
</members>
</callManagerGroup>
</devicePool>
<versionStamp>{Jan 01 2002 00:00:00}</versionStamp>
<loadInformation>P0030702T023</loadInformation>
<userLocale>
<name>English_United_States</name>
<langCode>en</langCode>
</userLocale>
<networkLocale>United_States</networkLocale>
<idleTimeout>0</idleTimeout>
<authenticationURL />
<directoryURL>http://10.15.0.1/localdirectory</directoryURL>
<idleURL />
<informationURL />
<messagesURL />
<proxyServerURL />
<servicesURL />
</device>
```

PARTIE 7

Déploiement automatisé des points de terminaison

- Dans une installation automatisée, vous n'avez pas à configurer les ephones.
- La configuration automatique automatise le déploiement des téléphones IP.
- Utilisez la commande d'affectation automatique de la téléphonie en mode de configuration de service telephony pour effectuer l'affectation automatique.
- Tous les phone-dns que vous souhaitez déployer doivent être du même type (Une ligne individuelle ou ligne double).
- Les ephone-dns sont automatiquement attribués aux nouveaux ephones qui sont configurés.Les téléphones peuvent prendre jusqu'à cinq minutes pour s'inscrire.
- Attendre l'inscription de tous les téléphones avant d'enregistrer la configuration.



Configuration Cisco CallManager Express avec CLI

- Passer en mode telephony-service

CMERouter(config)# **telephony-service**

- Définir le nombre maximum d'ephones qui peut être défini dans le système (par défaut est 0)

CMERouter(config-telephony)# **max-ephone *maximum-ephones***

- Définir le nombre maximum de phone-dns qui peut être défini dans le système (par défaut est 0)

CMERouter(config-telephony)# **max-dn *maximum-directory-numbers***

- Identifier l'adresse et le port par lequel les téléphones IP communiquent avec Cisco Unified Communications Manager Express

CMERouter(config-telephony)# **ip source-address *ip-address* [port port]**

- Permet l'enregistrement automatique de nouveaux ephones qui ne sont pas dans la configuration et sont activés par défaut

CMERouter(config-telephony)# **auto-reg-ephone**

- Crée les fichiers XML spécifiques qui sont nécessaires pour les téléphones IP

CMERouter(config-telephony)# **create cnf-files**

- Attribués les ephone-dns automatiquement aux nouveaux ephones qui sont configurés

CMERouter(config-telephony)# **auto assign *start-dn* to *stop-dn* [type *phone-type*]**

- Vérifier la configuration

CMERouter1# **show running-config**

CHAPITRE 3

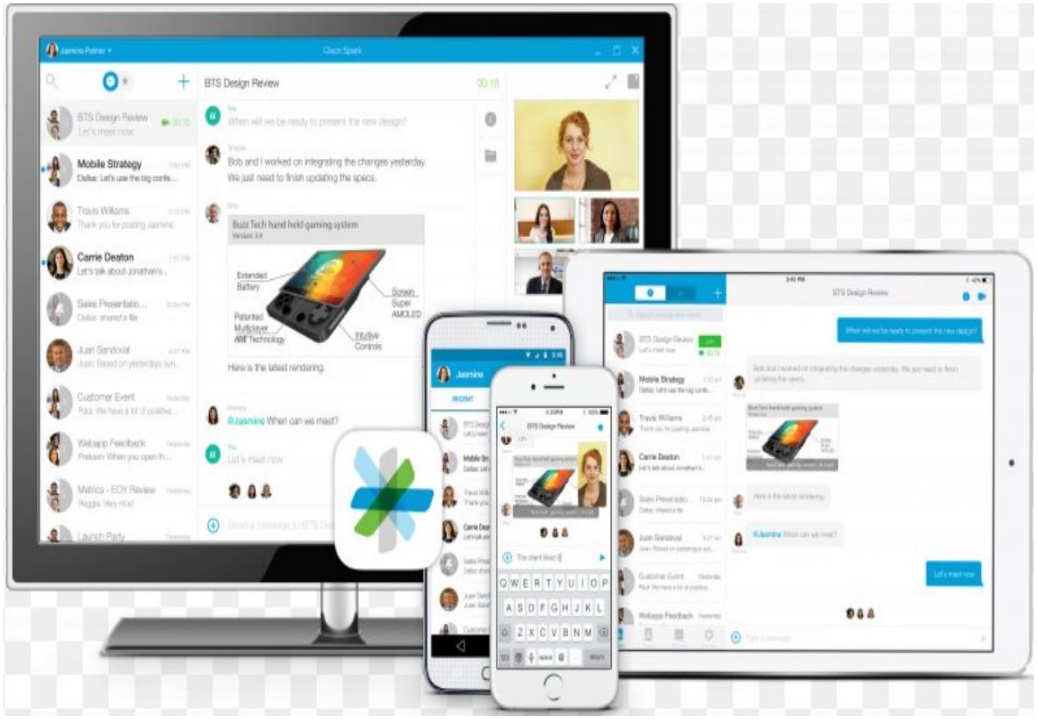
Implémenter la solution de communication unifiée Cisco

1. Gestionnaire de communications unifiées Cisco
2. Définition Ephone et Ephone-dn
3. Configuration de CallManager Expresse
4. Solutions de messagerie vocale et de présence
5. Les pairs de numérotation et les motifs de destination

PARTIE 7

Cisco Unified Presence

- La présence est la possibilité d'afficher le statut d'un utilisateur ; inactif/occupé/absent, les appareils sur lesquels ils sont joignables et la meilleure façon de les contacter.
- En termes simples, il "est le point d'agrégation de la disponibilité représenté par un ou plusieurs appareils associés à un compte d'utilisateur qui peut être surveillé par les utilisateurs"
- Cisco Unified Presence assure la messagerie instantanée et la présence via une plate-forme d'entreprise basée sur des normes.
- Ces outils facilitent une prise de décision plus rapide et améliorent la productivité en fournissant des connexions immédiates aux collègues.
- La disponibilité des travailleurs via les mises à jour du statut de présence permet de voir plus facilement qui est en ligne et prêt à aider. Cela aide les utilisateurs à éviter de perdre du temps en contactant les personnes indisponibles ou absentes du bureau.
- Cisco Jabber, la plate-forme de messagerie directe de l'entreprise, propose une multitude d'intégrations avec les produits de tous les principaux fabricants pour garantir que les employés restent en communication à tout moment.
- Cisco Jabber fait parti d'une suite d'outils Cisco :
  - **Cisco Jabber**
  - **Cisco WebEx Teams**
  - **Cisco Web Meetings**



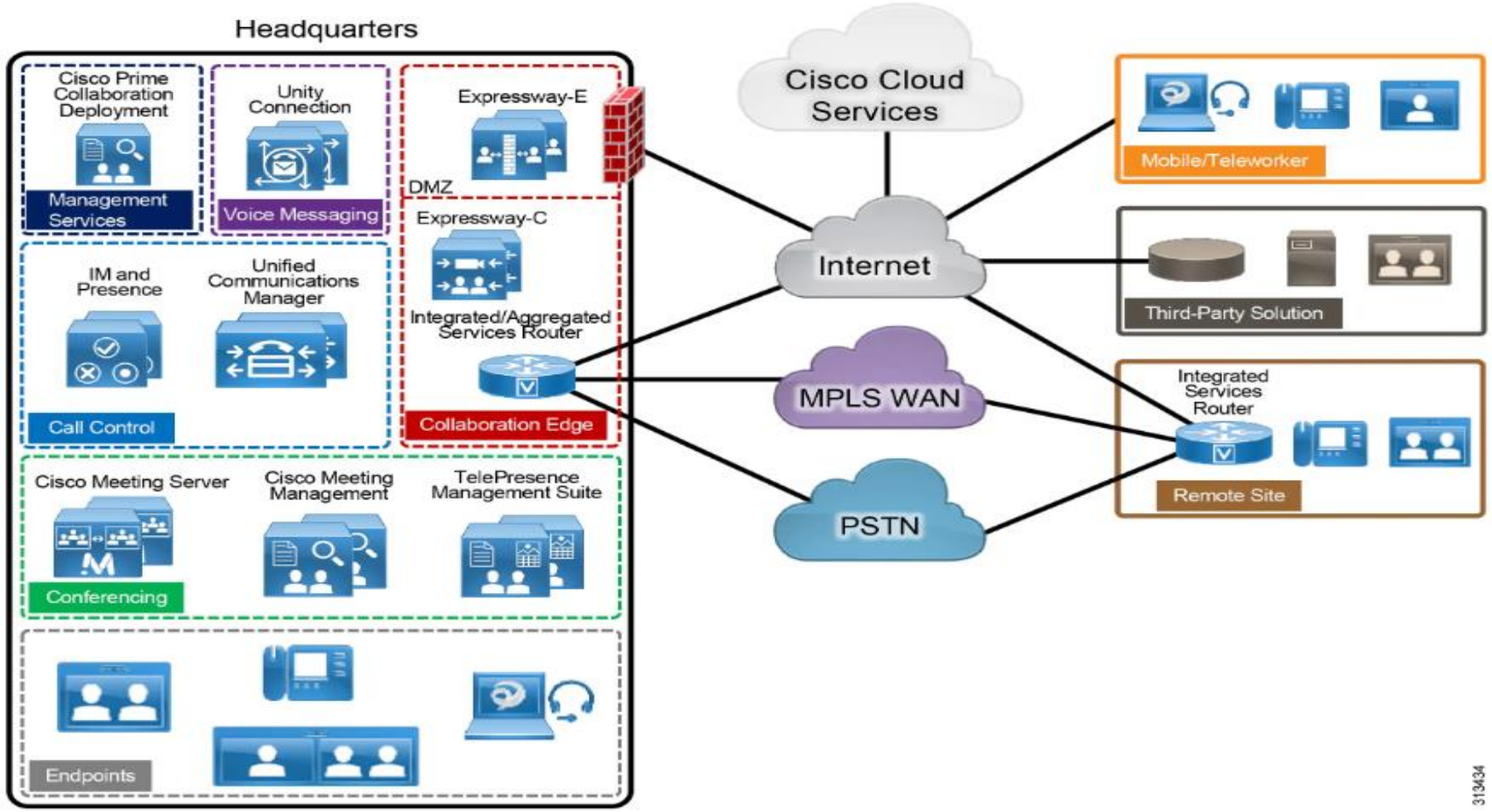
Cisco Unified Presence

- La comparaison entre ces trois outils selon les fonctionnalités suivantes :

	Cisco Jabber	Webex Teams	Webex Meetings
Caractéristiques de l'utilisation principale	Appels téléphonique	Outils de collaboration	Outils de vidéoconférence
Transfert des appels acheminé à un poste téléphonique de Polytechnique	X	X	
Accès à la boite vocale	X	Oui, en composant 7777	
Contrôle à distance / Partage d'écran	Entre clients Jabber	Partage d'écran	X
Capacité - conférences		200 personnes	1000 personnes
Chat	X	X	
Tableau blanc	X	X	X
Partage de fichiers	Oui entre clients Jabber	X	
Enregistrement de vidéoconférences		X	X

PARTIE 7

Système Cisco Unified Presence



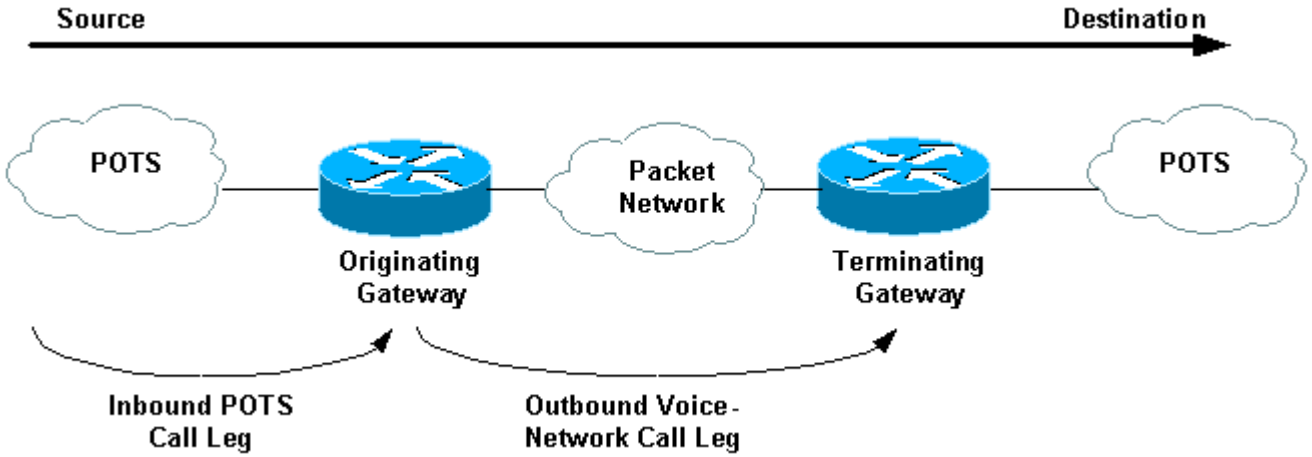
CHAPITRE 3

Implémenter la solution de communication unifiée Cisco

1. Gestionnaire de communications unifiées Cisco
2. Définition Ephone et Ephone-dn
3. Solutions de messagerie vocale et de présence
4. Les pairs de numérotation et les motifs de destination

Pairs de numérotation

- Les pairs de numérotation sont des points d'extrémité d'un appel adressable.
- Il établit des connexions logiques, ou des tronçons d'appel, pour terminer un appel de bout en bout
- Vous pouvez utiliser des pairs de numérotation entrants, sortants ou les deux.
- Les pairs de numérotation définissent les propriétés du tronçon d'appel: **codec, marquages QoS, VAD, Taux de fax**
- Les routeurs Cisco de Voix utilisent généralement deux types de pairs de numérotation:
  - **Pairs de numérotation POTS** - se connectent à un réseau de téléphonie traditionnelle comme FXO, FXS, E&M, BRI, PRI T1/E1, T1/E1 et CAS
  - **Pairs de numérotation VoIP** se connectent sur un réseau IP en utilisant une adresse IP



PARTIE 7

Motifs de destination

Caractères génériques de motif de destination commun :

- **Plus (+) :**

  Chiffre précédent se produit une ou plusieurs fois

- **Astérisque (*) et dièse (#) :**

  Caractères génériques non valides; sont des tonalités DTMF

- **Virgule (,) :**

  Insère une pause d'une seconde

- **Point (.) :**

  Indique un caractère générique quelconque

- **Crochets () :**

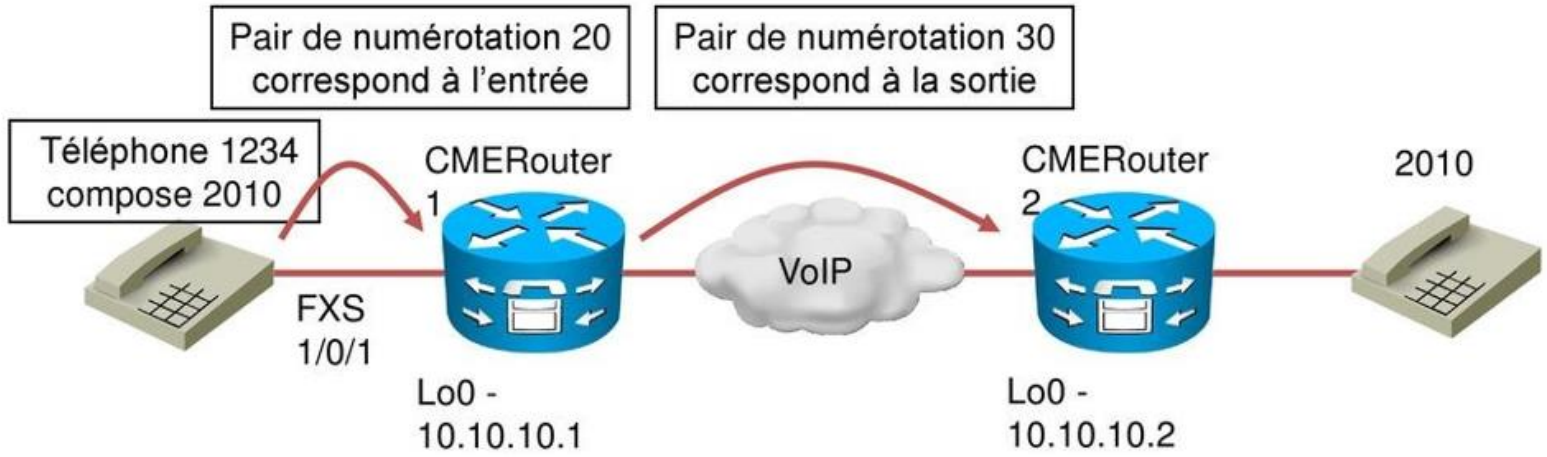
  Indique une série de chiffres à l'intérieur des crochets

- **T :**

  Indique un motif de longueur variable

PARTIE 7

Configuration Pair de numérotation




```
CMERouter1(config)# dial-peer voice 20 pots
CMERouter1(config-dialpeer)# destination-pattern 1234
CMERouter1(config-dialpeer)# port 1/0/1
```

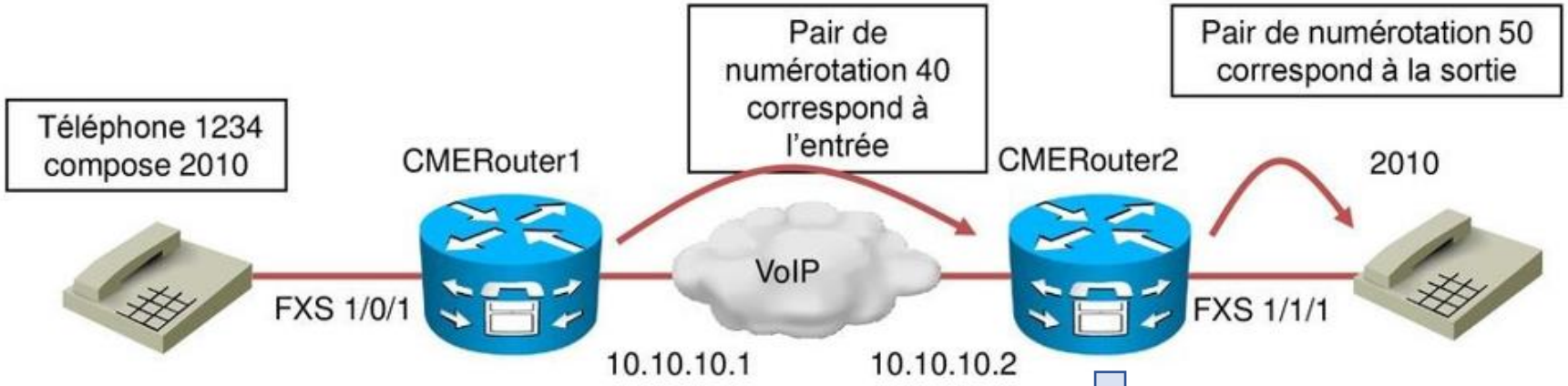
Pair de numérotation **pots**

```
CMERouter1(config)# dial-peer voice 30 voip
CMERouter1(config-dialpeer)# destination-pattern 2...
CMERouter1(config-dialpeer)# session target ipv4: 10.10.10.2
```

Pair de numérotation **voip**

PARTIE 7

Configuration Pair de numérotation



Pair de numérotation **pots**

```
CMERouter2(config)# dial-peer voice 50 pots
CMERouter2(config-dialpeer)# destination-pattern 2010
CMERouter2(config-dialpeer)# port 1/1/1
```

Pair de numérotation **voip**

```
CMERouter2(config)# dial-peer voice 40 voip
CMERouter2(config-dialpeer)# destination-pattern 1...
CMERouter2(config-dialpeer)# session target ipv4: 10.10.10.1
```

Correspondance avec des pairs de numérotation sortant

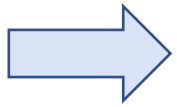
Motif de destination est mis en correspondance en se basant sur le numéro de correspondance le plus long

```
dial-peer voice 1 voip
destination-pattern .T
session target ipv4: 10.1.1.1

dial-peer voice 2 voip
destination-pattern 555[2-3]...
session target ipv4: 10.2.2.2

dial-peer voice 3 voip
destination-pattern
session target ipv4: 10.3.3.3

dial-peer voice 4 voip
destination-pattern
session target ipv4: 10.4.4.4
```



Exemple 1: Numéro composé correpond au pair de numérotation 4.
Exemple 2: Numéro composé correpond au pair de numérotation 3.
Exemple 3: Numéro composé correpond au pair de numérotation 2.
Exemple 4: Numéro composé correpond au pair de numérotation 1.

FIN.