FICHES DE RÉVISION

EXAMEN

200-105 ICND2

CERTIFICATION

CISCO CCNA

PAR

CYRIL

CERTIFIÉ CCIE ET AUTEUR DU SITE

REUSSIRSONCCNA.FR

A LIRE - AVERTISSEMENT

Ce guide ne peut être utilisé que pour un usage privé uniquement.

Vous n'avez pas le droit de l'offrir ni de le revendre sans accord des auteurs. Toutes reproductions, partielles ou totales, sous quelque forme et procédé que ce soit sont interdites conformément à l'article L.122-4 du Code de la Propriété Intellectuelle.

Toute personne procédant à une utilisation du contenu de ce guide, sans une autorisation expresse et écrite de l'auteur, encourt une peine relative au délit de contrefaçon détaillée à partir de l'article L 335-2 du même Code.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation de l'Éditeur ou du Centre Français d'Exploitation du Droit de copie, 20, rue des Grands-Augustins, 75006 Paris.

A LIRE - NOTICE LÉGALE

L'auteur s'est efforcé d'être aussi précis et complet que possible lors de la création de cet ouvrage, et malgré ceci, il ne peut en aucun cas garantir ou représenter le contenu de cet ouvrage dû à l'évolution et la mutation rapide et constante de la technologie.

Bien que tout ait été fait afin de vérifier les informations contenues dans cet ouvrage, l'auteur n'assume aucune responsabilité concernant des erreurs, des omissions, une interprétation ou une compréhension contraire du sujet développé.

SOMMAIRE

Introduction
QUI SUIS-JE?

Bonjour je m'appelle Cyril.

Travaillant depuis des années dans le domaine de **l'architecture, l'expertise réseau et la formation,** je souhaite aider et accompagner les personnes vers l'obtention des certifications Cisco. J'ai créé ce guide car beaucoup de personnes ont demandé mon aide afin de comprendre les certifications Cisco CCENT et Cisco CCNA.

Il faut savoir qu'une simple formation Cisco de 5 jours coûte **entre 2000 et 3500€ hors taxe !** Quand votre entreprise vous refuse cette formation, peu de personnes peuvent se permettre de la financer sur ses propres deniers.

En partant de cet état de fait et étant certifié CCIE et CCSI (instructeur officiel Cisco), mon but à très court terme est que vous puissiez poser la première pierre de l'édifice, c'est-à-dire le CCENT puis le CCNA.

Pour plus d'informations sur la pyramide des certifications, je vous invite à faire un tour sur le site de Cisco en cliquant ici.

Je vous souhaite une excellente lecture et n'hésitez pas à vous rendre sur le site **http://reussirsonccna.fr** ou à me contacter directement sur **cyril@reussirsonccna.fr.** Votre réussite est mon objectif!

Je vous souhaite une excellente lecture et n'hésitez pas à vous rendre sur le site **http://reussirsonccna.fr** ou à me contacter directement sur **cyril@reussirsonccna.fr.**

Votre réussite est mon objectif!

TOUT SAVOIR SUR LE CCENT ET CCNA

Si vous ne l'avez pas déjà téléchargé, je propose un guide totalement gratuit sur tout ce qu'il faut savoir sur le CCENT et le CCNA. Ce guide est téléchargeable sur le site **http://reussirsonccna.fr**

VOUS Y DÉCOUVRIREZ LES POINTS SUIVANTS :

- Comment choisir son cursus ?
- Est-ce que le CCENT ou CCNA est suffisant?
- Quelle est la différence entre le CCNA académique vs CCNA Professionnel ?
- Comment s'inscrire à l'examen ?
- Comment se passe l'examen le jour J ?
- Quels sont les types de questions ?
- Comment optimiser sa mémoire?
- Comment pratiquer les labs ?
- Comment monter son propre lab Cisco ?
- Quel score atteindre pour être certifié(e) ?
- Quels sont les prérequis pour la certification ? (inclus dans ce présent document)
- Où puis-je trouver des livres de révision ? (inclus dans ce présent document)
- Mes 9 conseils avant et pendant l'examen (inclus dans ce présent document)
- Retour d'expérience de Fréderic
- Retour d'expérience de Remi
- Syllabus ICND 1 – 100-105
- Syllabus ICND2 – 200-105
- Syllabus CCNA (ICND1 + ICND2) – 200-125
- Les blogs Cisco

QU'EST-CE QUE LE CCENT ET LE CCNA?

La certification CCNA – Cisco Certified Network Associate est à ce jour la plus connue et la plus demandée dans le monde des réseaux informatiques.

La certification CCENT – Cisco Certified Entry Networking Technician est moins connue car plus récente, elle se situe en amont du CCNA.

Selon le site Cisco, ces deux certifications permettent de valider la capacité à installer, opérer et dépanner un réseau informatique pour TPE et PME.

A mon sens, elles permettent surtout de certifier une base de connaissances relativement large, passant de la couche physique (câble cuivre, fibre optique...), aux protocoles niveau 2 (arp, vtp, stp...), aux protocoles de routage (rip, eigrp, ospf...), pour finir sur les protocoles applicatifs (http, ftp, smtp...).

Dans ma carrière de formateur, j'ai été très surpris sur le nombre de personnes qui ont échoué à ces examens pensant qu'ils maitrisaient leur sujet malgré plus de 20 ans d'expérience. Surpris aussi de la mauvaise compréhension des protocoles parce que souvent c'est plug and play, "on branche et ça fonctionne", oui mais pourquoi ?

ALORS, POURQUOI AUTANT D'ÉCHECS AU CCNA ?

Parce que la quantité d'information à connaitre est gigantesque. En effet, rien que les livres officiels qui traitent de la théorie font plus de 1000 pages et il y en a deux ! L'un est dédié à la théorie ICND1 et l'un autre à la théorie ICND2. Et il faut connaitre les deux (ICND1 + ICND2) afin lors de l'examen CCNA.

Certains diront qu'il suffit juste de réviser des examens blancs pour réussir le jour J. Oui c'est possible, mais dans certains cas ce n'est pas suffisant. Cependant, est-ce vraiment ce que vous voulez ? Etre certifié CCNA pour ensuite être décrédibilisé en entretien technique ? La certification est certes un plus sur son CV mais l'entretien technique reste l'unique façon de vérifier que vous êtes à la hauteur.

C’est pour cela que Cisco a créé un examen intermédiaire, le CCENT, qui permet d’être certifié juste en passant la première théorie ICND1. Une fois cet examen réussi, vous serez certifié Cisco CCENT.

Une fois le CCENT réussi, il ne reste plus qu’à réviser et à passer la théorie ICND2 pour être certifié CCNA.

C’est tout de même plus simple que de passer les théories ICND1+ICND2 lors d’un même et unique examen, non ? Ces fiches résumé sont destinées à vous donner toutes les billes en main pour réussir votre ICND2.

QUELS SONT LES PRÉREQUIS POUR LA CERTIFICATION ?

Le prérequis pour passer l'examen ICND2 est d'avoir obtenu avec succès l'examen ICND1/CCENT

Des fiches résumé ICND1 sont disponibles sur le site **http://reussirsonccna.fr,** je vous conseille vivement d'aller faire un tour.

Un autre prérequis très important : être motivé(e) !

MES 9 CONSEILS AVANT ET PENDANT L'EXAMEN

Une demande revient régulièrement par email sur les conseils à savoir pendant les révisions et lors du jour « J » afin de limiter la casse et optimiser au mieux le rendement de ses capacités intellectuelles.

Alors je vous arrête tout de suite, je ne vais pas vous recommander tel ou tel médicament plus ou moins douteux que l'on trouve sur Internet et curieusement non autorisé en France et d'autres pays.

Voici une petite liste non exhaustive de conseils sur votre préparation à l'examen.

AVANT LE JOUR J

Avant le jour de l'examen, on se dit toujours qu'on pensera au jour « J » plus tard. Ce qui en soit est une bonne idée pour ne pas rajouter du stress pendant les révisions surtout si vous êtes dans un chapitre assez compliqué, comme le résumé de route par exemple.

Cependant, voici quelques conseils sur la préparation avant le jour J de l'examen qui sont importants à mes yeux:

1 **Pas la peine de réviser 12h par jour,** cela ne sert à rien sur le long terme. Ce mode de révision intense sert uniquement pour la dernière ligne droite. Par exemple la dernière semaine, c'est là où vous pouvez stimuler votre cerveau pour rafraîchir des chapitres vu il y a bien longtemps. Donc **révisez de manière modérée**, sans acharnement mais dans la continuité et la durée (pas la peine de me demander si 10 minutes par jour sont suffisantes... il vous faudra des années pour tout assimiler et le CCNA aura déjà changé plusieurs fois de version).

2 **Dormez… et dormez bien.** Conseil banal mais oh! combien important. Ne faites pas du Yo-Yo avec votre sommeil, c'est à dire un jour vous vous couchez à 21h et un autre jour à 3h du matin, surtout lors de la dernière semaine. Un sommeil long et constant est surement une des clés du succès Si vous ne me croyez pas, **faites le test suivant:** après une nuit courte, chronométrez-vous sur 10 questions en calcul binaire. Faites le même test après une nuit normale… vous constaterez la différence sur le temps que votre cerveau a mis et sur le taux de bonnes réponses.

3 **Rafraîchissez votre mémoire pendant** vos révisions, pas à la fin. Il est impératif que **régulièrement** vous consacriez du temps à revoir **les fiches résumés de ce livre.**

4 **Sortez !** oui sortez, voyez vos amis, aller au bar, au ciné, faites du sport… faites une activité régulière qui permet à votre cerveau **de décompresser!** Le sport est une très bonne activité pour "décrocher" mentalement et physiquement

Voyons maintenant un peu les conseils pour le jour J…

LE JOUR J

Voici quelques conseils pour que vous soyez dans les meilleures conditions le jour de l'examen:

5 Il faut arriver bien **en avance** au centre de certification. Arriver pile à l'heure ou en retard est une source de stress des plus horribles et vous mettrez facilement **20 minutes** à faire redescendre la pression. Profitez-en aussi pour aller aux toilettes (oui Papa j'y vais !)

6 Prenez **2 pièces d'identités** avec vous (carte d'identité, passeport, permis de conduire...). Certains centres demandent 2 pièces d'identité et ils ne plaisantent pas.

7 Asseyez-vous devant l'écran de l'ordinateur et mettez-vous dans la tête que **votre objectif** n'est pas d'avoir le CCNA mais de l'avoir avec le meilleure score ! **Échouer n'est pas une option !**

8 La première fois qu'on passe un examen Cisco, on ne fait pas attention mais les **10 premières minutes** sont dédiées à un **tutoriel qui** explique le déroulement de l'examen. Prenez votre temps pour bien comprendre car ce temps **n'est pas décompté** de l'examen. Les indications sont très importantes surtout pour les TP car les écrans d'énoncé, d'accès à la console CLI et de réponse ne sont pas forcément au même endroit !

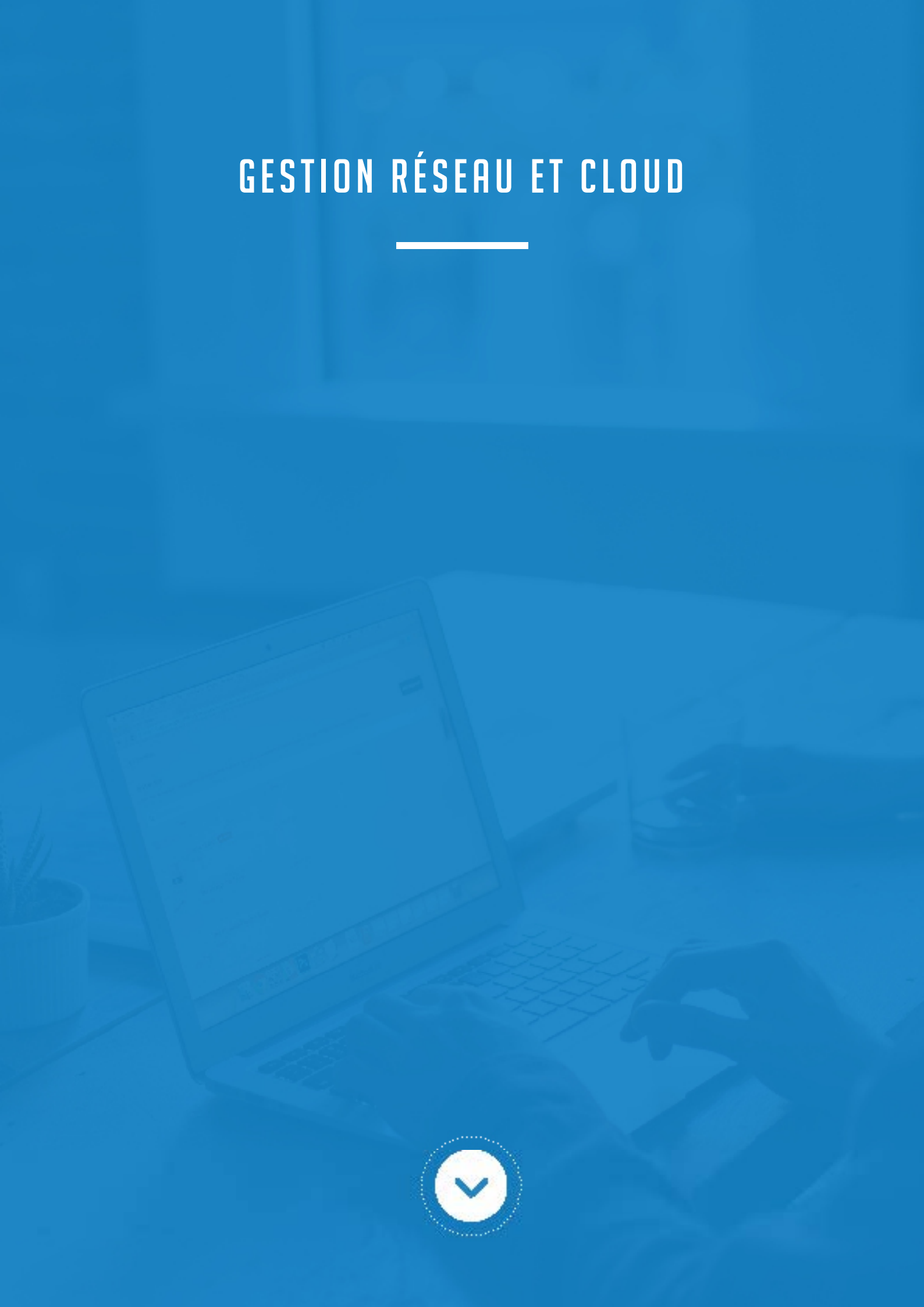
9 Dernière chose: une fois la question validée, **vous ne pouvez plus revenir en arrière,** contrairement à d'autres examens. Donc avant de cliquer sur SUIVANT, relisez rapidement une dernière fois votre réponse.

FICHES RÉSUMÉ

Les fiches résumés sont découpés 8 grands domaines:

8 domaines	Sous-domaine
Gestion réseau et Cloud	Cloud Computing
	SDN
Commutation	VLAN
	Spanning-Tree
Interconnexion niveau 2 / 3	Routage inter-VLAN
	HSRP / GLBP
	Qualité de service
Routage IPv4	OSPF
	EIGRP
Routage IPv6	OSPF
	EIGRP
Dépannage	Dépannage LAN
	Dépannage routage IPv4
	Dépannage routage IPv6
Listes de contrôle d'accès	ACL IPv4
	ACL IPv6
WAN	BGP
	MPLS
	VPN

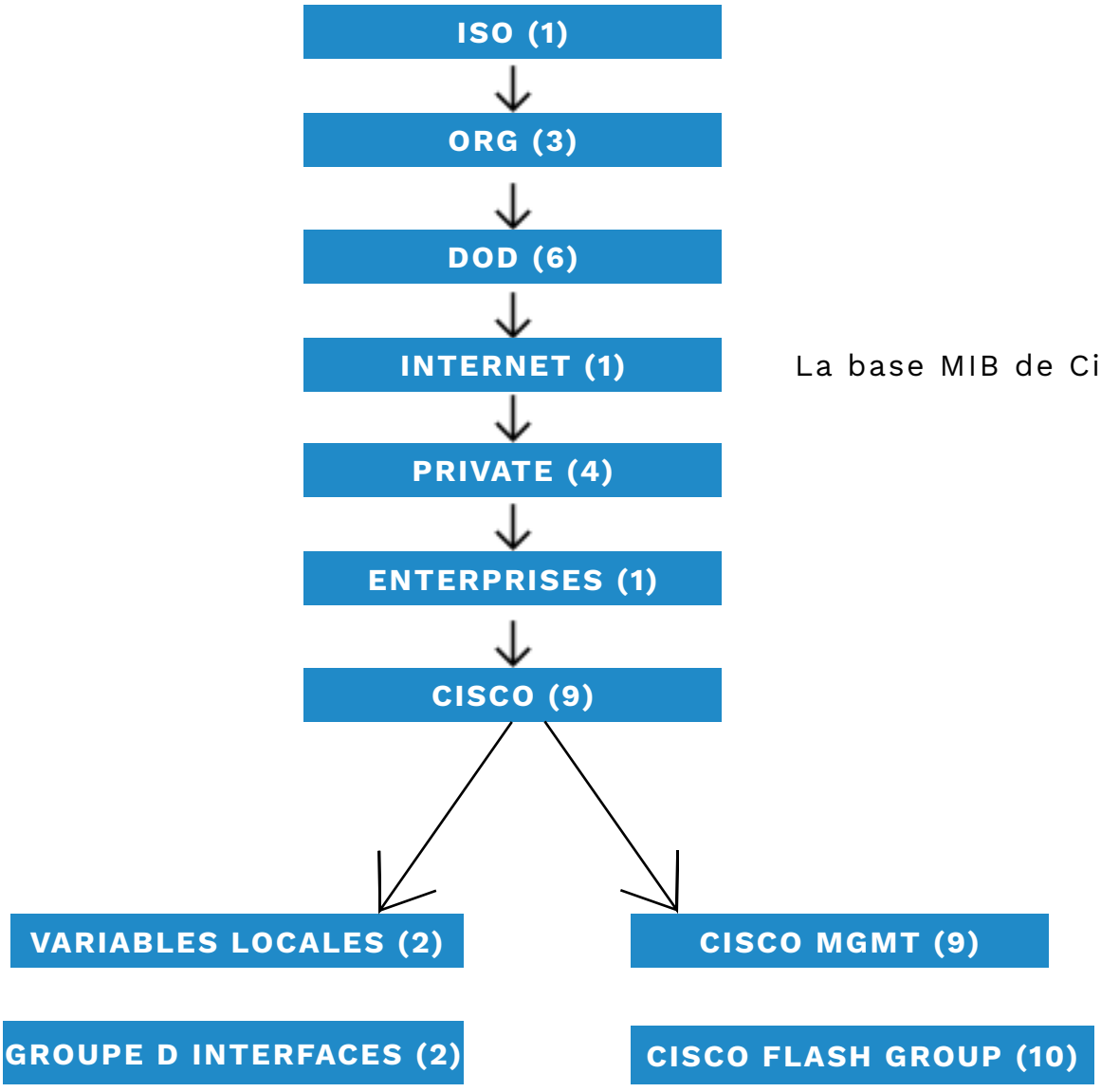
GESTION RÉSEAU ET CLOUD



POINTS CLÉS SUR LE PROTOCOLE DE GESTION DE RÉSEAU SIMPLE (SNMP)

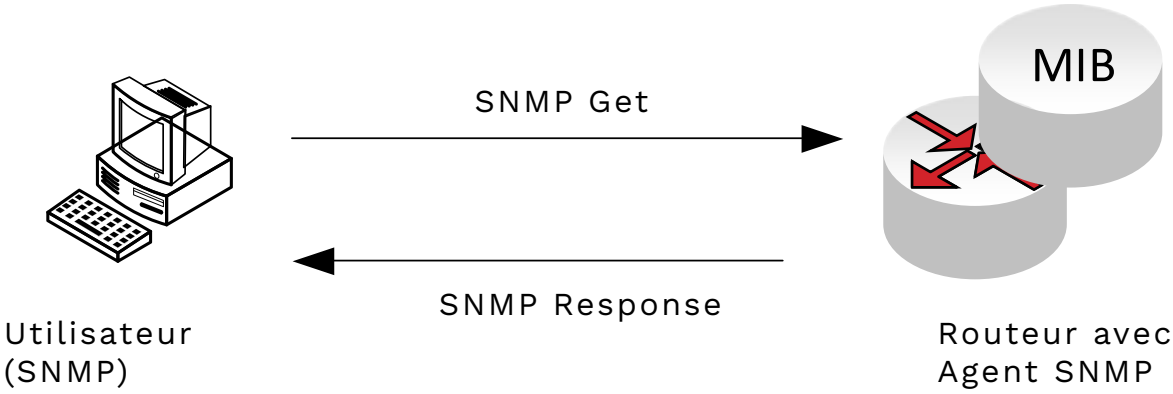
SNMP est un protocole de communication utilisé pour la gestion du réseau. Un serveur interroge les périphériques réseau et les périphériques réseau renvoient les informations d'état. Les périphériques peuvent également envoyer des notifications de pannes via des traps SNMP. Les traps sont utiles lorsque les périphériques réseau tombent en panne car elles fournissent des informations pour identifier le problème.

Chaque périphérique atteint par SNMP possède une base de données appelée MIB – Management Information Base. Cette base de données contient des valeurs qui peuvent être interrogées par SNMP.

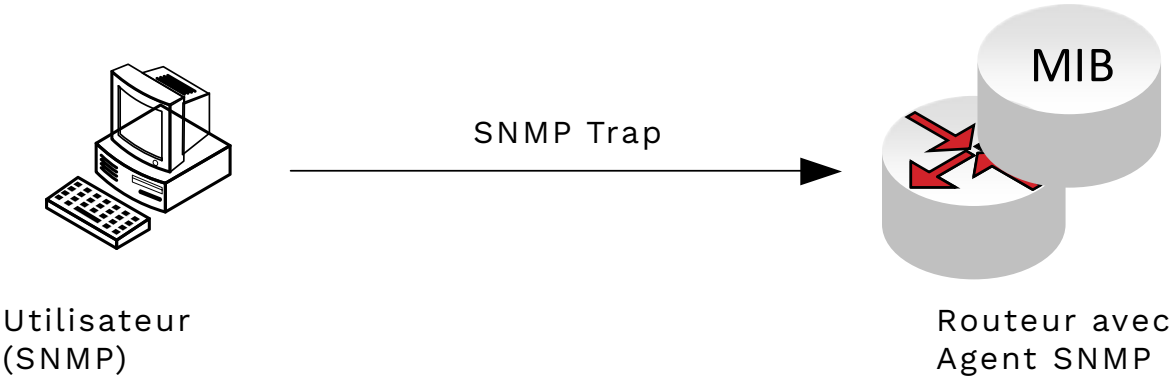


La base MIB de Cisco

SNMP GET / RESPONSE

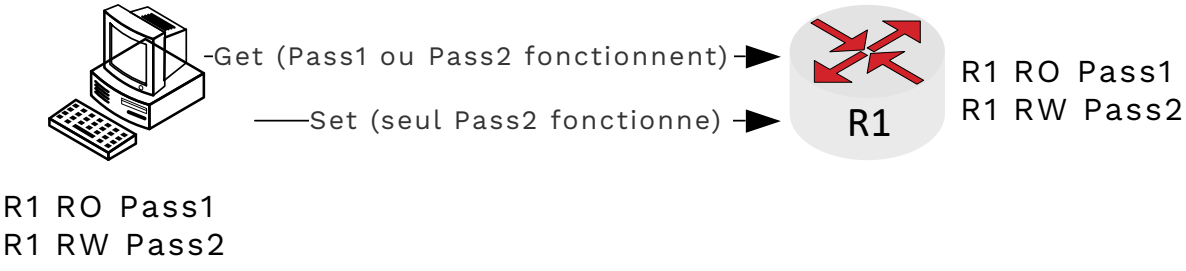


SNMP TRAP



MODE DE SÉCURITÉ SNMPV3

Nom de niveau	Mot de passe snmp-server	Méthode d'authentification	Chiffrement
Noauthnopriv	Noauth	Nom d'utilisateur	Aucun
AuthNoPriv	Auth	MD5 or SHA	Aucun
Auth Md5 Or Sha Aucun	Priv	MD5 or SHA	DES or DES-56



CONFIGURATION SNMPV2C SUR UN ROUTEUR CISCO

1. Configurez le nom de communauté et les droits d'accès avec la commande s**erver community** chaîne **RO | RW**. Remarque, RO esten lecture seule et RW esten lecture et écriture. Tous les appareils du réseau doivent avoir le même nom de communauté SNMP.

2. Configurez l'emplacement de l'appareil avec la commande globale **snmp-server location** description-texte. Cette option est facultative, mais bonne à configurer.

3. Configurez les informations de contact de l'appareil avec la commande snmp-server contact contact-texte. Cette commande est facultative, mais devrait être configurée. **Remarque**: Ceci est un bon endroit pour le nom et le numéro de téléphone du contact principal.

4. Utilisez une ACL pour limiter l'accès SNMP à l'appareil. Ce n est pas une bonne idée de laisser l'accès SNMP ouvert, car SNMP est un vecteur pour attaquer un réseau. La commande pour associer une ACL à SNMP est **snmp-server community** chaîne nom-acl ou numéro

EXEMPLE DE CONFIGURATION

Configurez le routeur R1 avec un nom de communauté SNMP de valeur L!fetime2, avec des **autorisations** en lecture seule. Définissez également l'emplacement Paris et le contact local comme Cyril Dupont. Créez une ACL avec le nom RESTRICT_SNMP permettant uniquement le sous-réseau de gestion de réseau de 172.30.21.0/24.

La configuration est illustrée ci-dessous

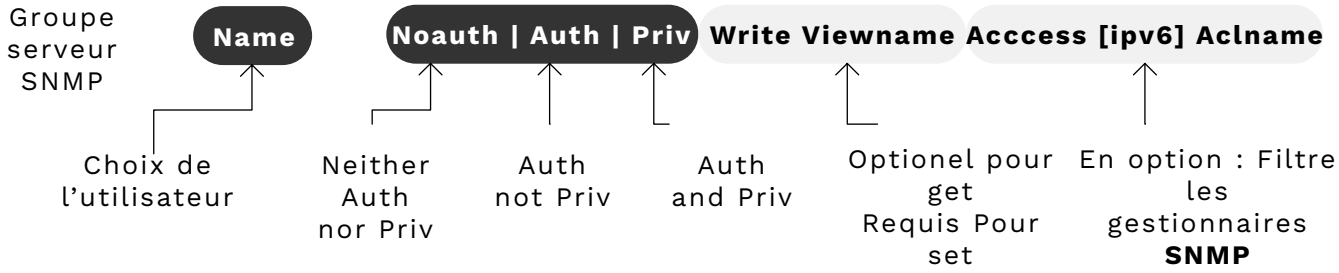
ip access-list standard RESTRICT_SNMP permit 172.30.21.0 0.0.0.255

snmp-server community L!fetime2 RO RESTRICT_SNMP

snmp-server location Paris

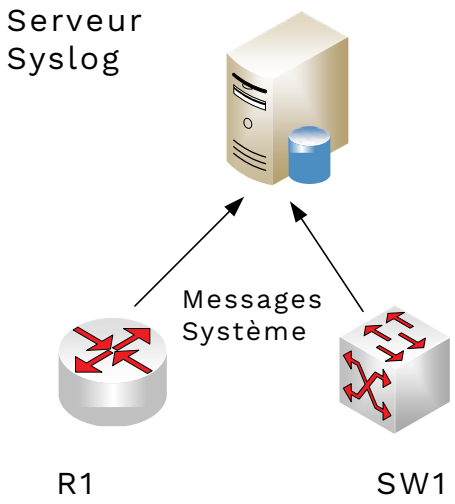
snmp-server contact Cyril Dupont

COMMANDE ET OPTIONS DE CONFIGURATION DU GROUPE DE SERVEURS SNMPV3



JOURNAL DES MESSAGES SYSTÈME (SYSLOG)

Chaque appareil réseau crée des messages (logs) lors des opérations quotidiennes. Bien que ces messages peuvent être stockés sur chaque appareil, l'espace de stockage est limité. Pendant le dépannage, il est souhaitable de disposer d'un serveur central pour collecter les journaux systèmes (logs). Les roteurs Cisco peuvent être configurés pour envoyer des syslogs à un (ou des) serveur central pour analyse.



Niveau	Nom du niveau	Raison du message
0	Emergency	Le système peut être complètement à l'arrêt
1	Alert	Peut nécessiter une action immédiate
2	Critical	Un événement critique s'est produit
3	Error	L'élément a eu une erreur
4	Warning	L'événement peut nécessiter de l'attention
5	Notification	Un événement significatif s'est produit
6	Information	Message d'événement normal
7	Debugging	Message de debug

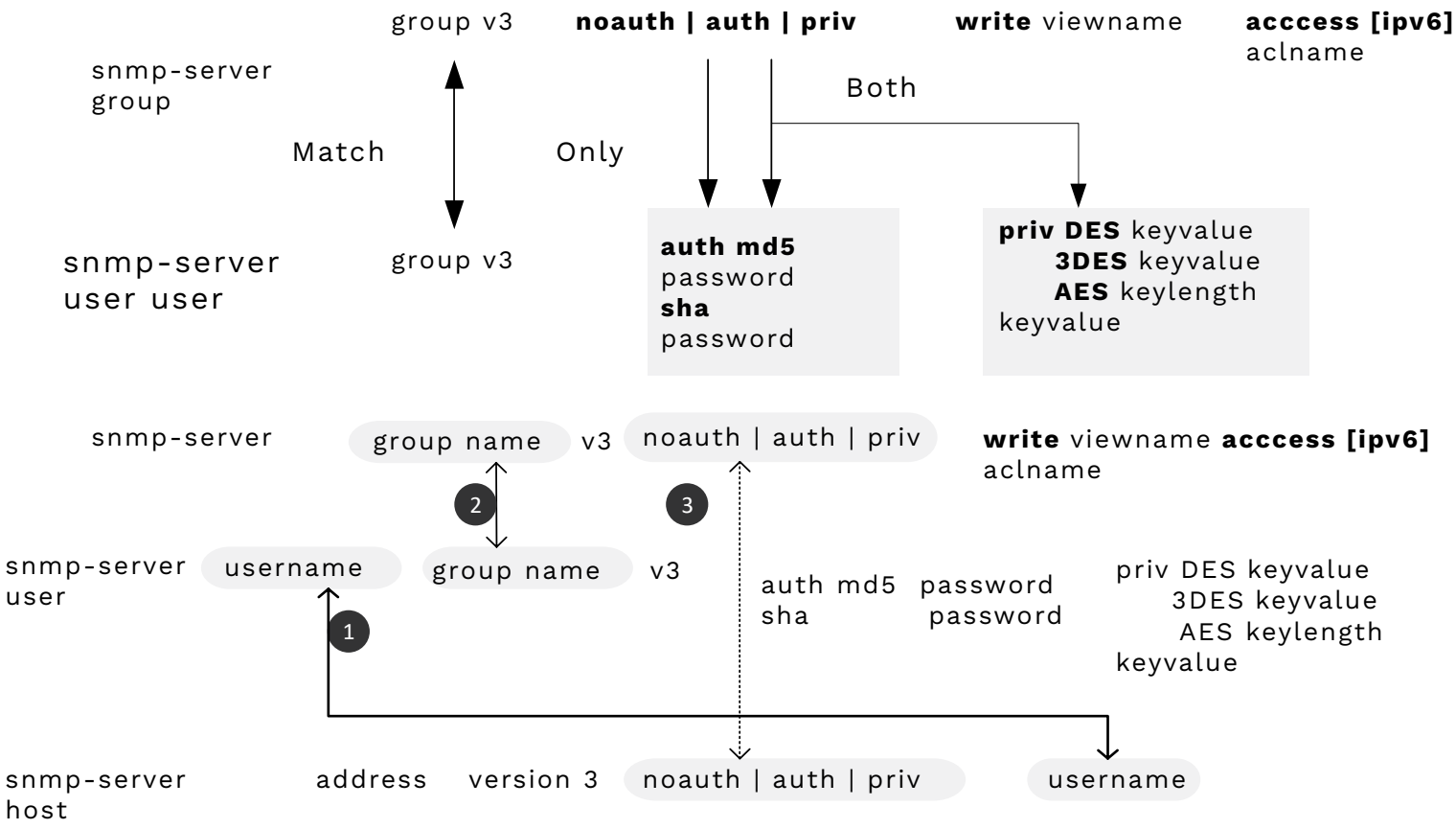
CONFIG SYSLOG POUR R1

```
!
logging 192.168.1.100          # adresse IP du serveur syslog
logging trap 4                 # rapporter uniquement les niveaux 0, 1, 2, 3, et 4
no service timestamps          # désactiver les horodateurs (à utiliser que dans
                                 certaines situations)
service sequence-
numbers                        # utiliser des numéros de séquence au lieu de
                                 l'horodatage
```

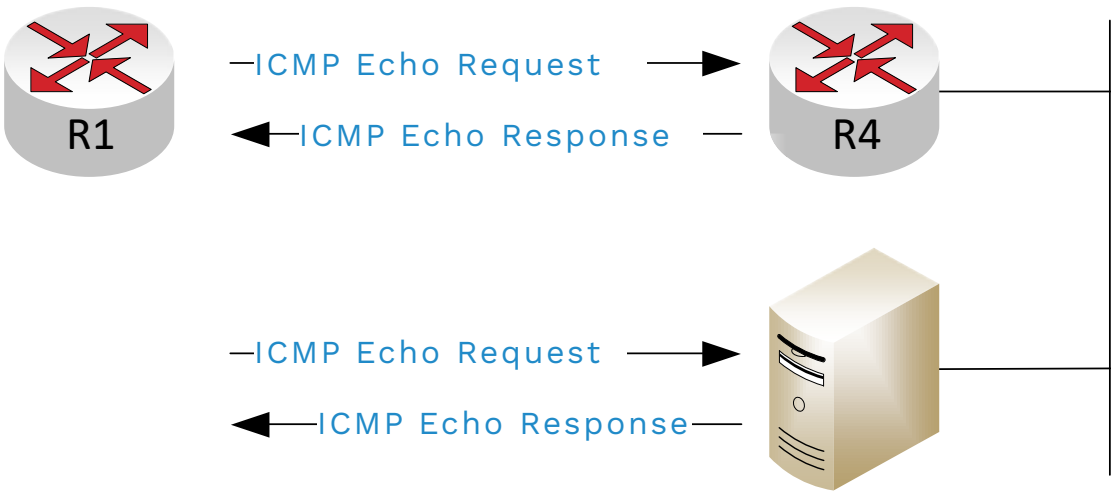
NOUVELLES FONCTIONNALITÉS DE SNMPV3 PAR RAPPORT A SNMPV1 ET V2

- **Intégrité des messages -** assure que le paquet n'est pas été modifié pendant le transit
- **Authentification:** les paquets SNMP proviennent d'un hôte / emplacement connu et approuvé
- **Chiffrement -** Si le paquet est capturé ou reniflé, le contenu ne peut pas être lu sans la clé de cryptage

CONFIGURATION SNMPV3 - USERS ET GROUPS



CONNEXION DE LA CONFIGURATION DE NOTIFICATION SNMPV3 AVEC L'UTILISATEUR ET LE GROUPE



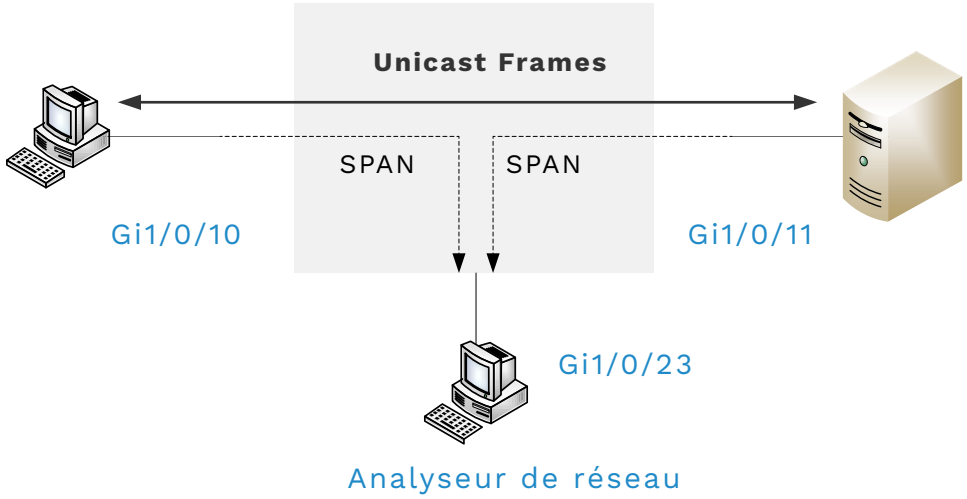
EXEMPLE DE CONFIGURATION IP DE SLA

ip sla 1
icmp-echo 10.1.3.2 source-ip 10.1.1.1 ! Echo de 10.1.1.1 vers 10.1.3.2
frequence 60 ! Envoyer toutes les 60 secondes
threshold 300 ! Round Trip Time de 300 milliseconds
history filter all ! Cela signifie GARDER toutes les données
history buckets-kept 6 ! Limite les données historiques à 6 groupe
!
ip sla schedule 1 life forever start-time now

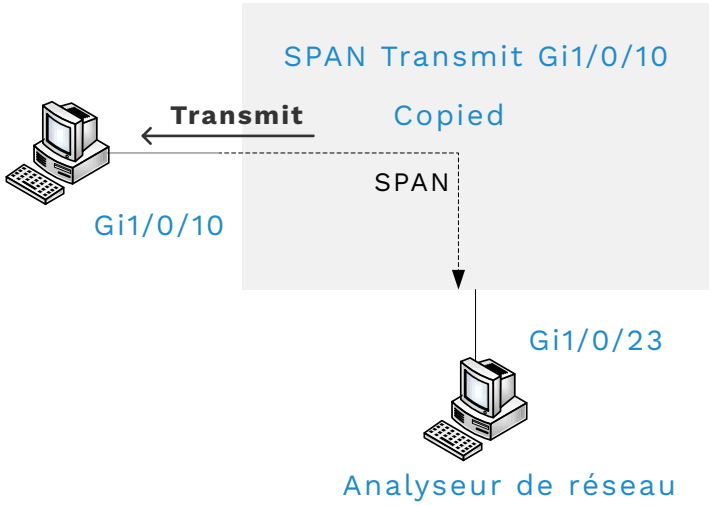
COMPTEUR SUCCESS/FAILURE DE LA COMMANDE IP SLA

R1**# show ip sla statistics 1**
IPSLAs Latest Operation Statistics
IPSLA operation id: 1
Latest RTT: 16 milliseconds
Latest operation start time: 12:40:39 EST Tue Jan 5 2016
Latest operation return code: OK
Number of successes: 7
Number of failures: 0
Operation time to live: Forever

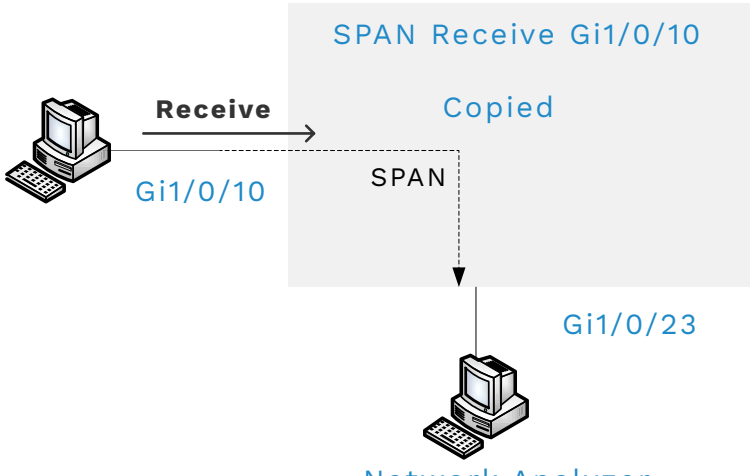
SPAN - COPIES DES TRAMES VERS L'ANALYSEUR DE RÉSEAU



SPAN CONSTRUCT – LES TRAMES TRANSMISES SUR GI1/0/10 SONT COPIÉS À GI1/0/23



SPAN CONSTRUCT – LES TRAMES ENVOYÉES PAR GI1/0/10 SONT COPIÉS À GI1/0/23



CONFIGURATION SPAN LOCALE A UN COMMUTATEUR

• Un port de destination SPAN peut être utilisé avec une seule session SPAN à la fois.

• Un port de destination SPAN ne peut pas non plus être un port source SPAN.

• Lorsqu'il est configuré comme un port de destination SPAN, le commutateur ne traite plus le port comme un port normal. C'est-à-dire que le commutateur n'apprend pas les adresses MAC pour les trames reçues, ou envoie des trames en fonction de la correspondance de la table MAC pour ce port.

• Un port de destination SPAN peut être enlevé d'une session SPAN **(no monitor session NUMERO destination interface TYPE NUMBER)** puis ajouté à une autre session SPAN.

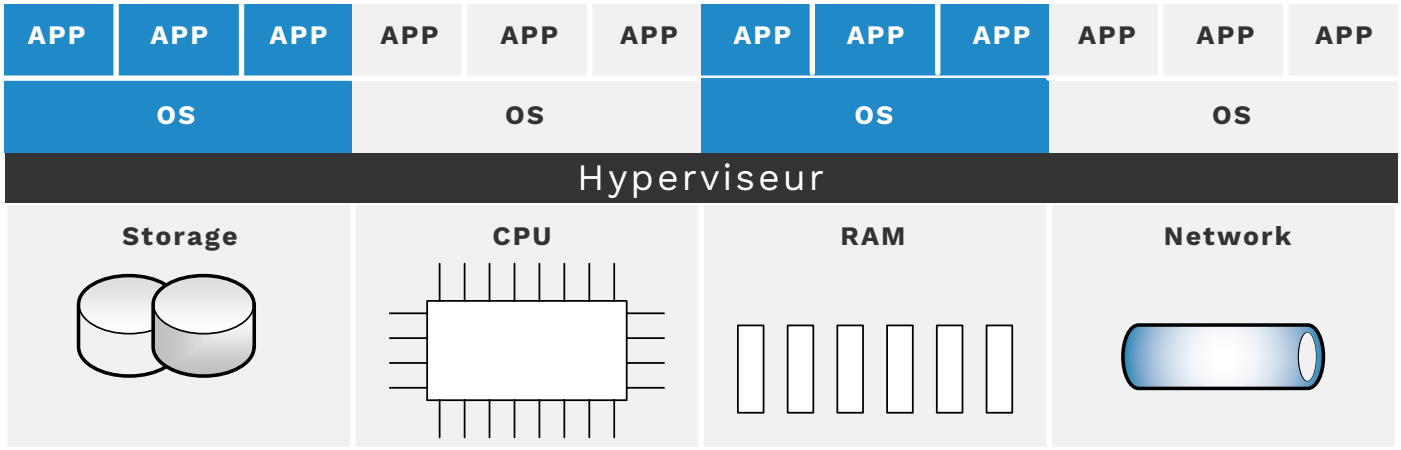
• Plusieurs sources SPAN peuvent être utilisées dans une seule session SPAN.

• Une session SPAN ne peut pas mélanger comme source; interfaces et VLAN. C'est-à-dire que les sources doivent toutes être des interfaces ou tous des VLAN.

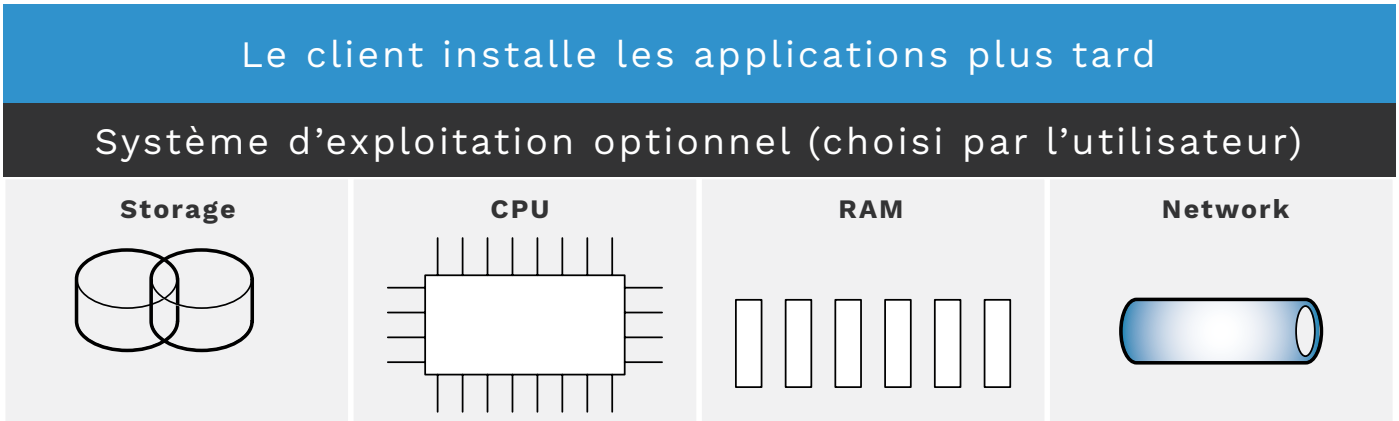
• Une session SPAN peut utiliser toute combinaison de directions (transmission, réception, et les deux) appliquée à différentes sources SPAN.

• Les interfaces EtherChannel peuvent être utilisées comme ports source.

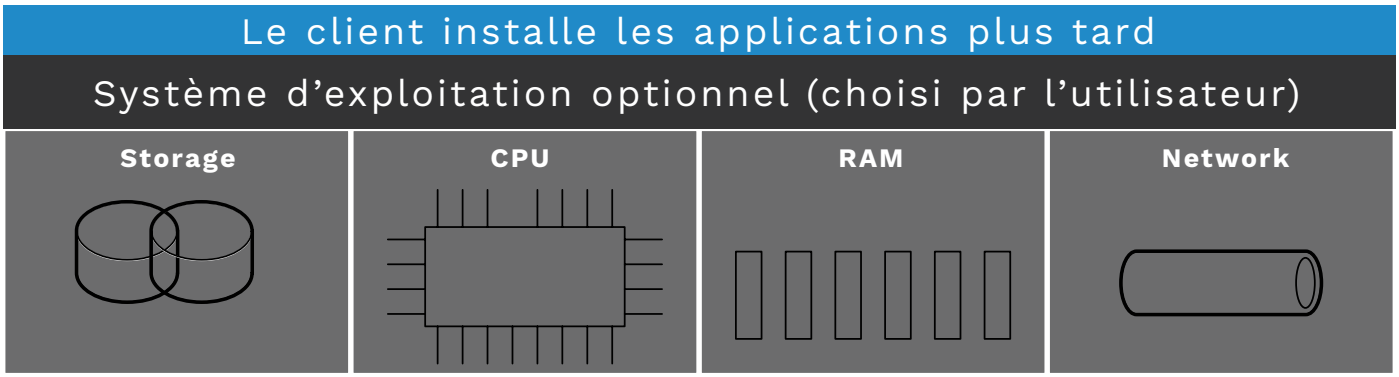
• Les Trunk peuvent être utilisés comme ports source. Lorsqu'il est utilisé, par défaut, SPAN inclut les trames de tous les VLAN de ce Trunk, mais le filtrage SPAN VLAN peut limiter les VLAN inclus



Quatre machines virtuelles fonctionnant sur un hôte, l'Hyperviseur gère le matériel



Concepts du IaaS - Infrastructure as a Service - Le client choisit le matériel du serveur



Concepts du SaaS - Software as a Service - Le client ne voit que les applications
(Le système d'exploitation et le matériel sont cachés au client)

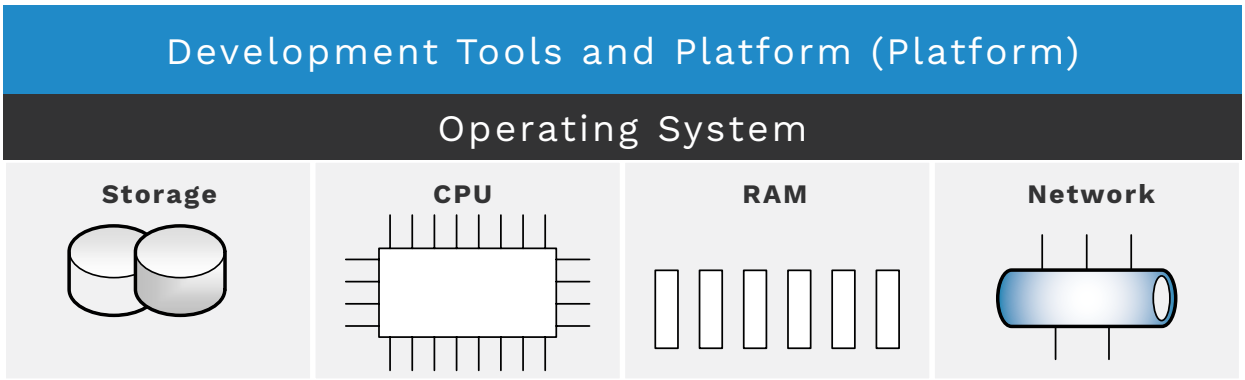
On-demand self-service: le client choisit de démarrer et d'arrêter l'utilisation du service, sans aucune interaction directe avec le fournisseur du service.

Broad network access: le service doit être disponible à partir de nombreux équipements et de nombreux types de réseaux (y compris Internet).

Ressource pooling: le fournisseur crée un pool de ressources (plutôt que de consacrer des serveurs spécifiques uniquement à certains clients) et alloue dynamiquement les ressources de ce groupe pour chaque nouvelle demande d'un client.

Rapid elasticity: pour le client, le pool de ressources semble être illimité (c'est-à-dire qu'il se développe rapidement, donc appelé élastique), et les demandes de nouveaux services sont remplies rapidement.

Measured service: le fournisseur peut mesurer l'utilisation et signaler cette utilisation au client, tant pour la transparence que pour la facturation.



Concept du PaaS - Platform as a Service

	Internet	Internet VPN	MPLS VPN	Ethernet WAN	Intercloud Exchange
Sécurité	Non	Oui	Oui	Oui	Oui
QoS	Non	Non	Oui	Oui	Oui
Nécessite une planification de la capacité	Oui	Oui	Oui	Oui	Oui
Migrations plus faciles vers un nouveau fournisseur	Oui	Oui	Non	Non	Yes
Utilisation rapide du cloud publique	Oui	Oui	Non	Non	Non

Comparaison des connexions

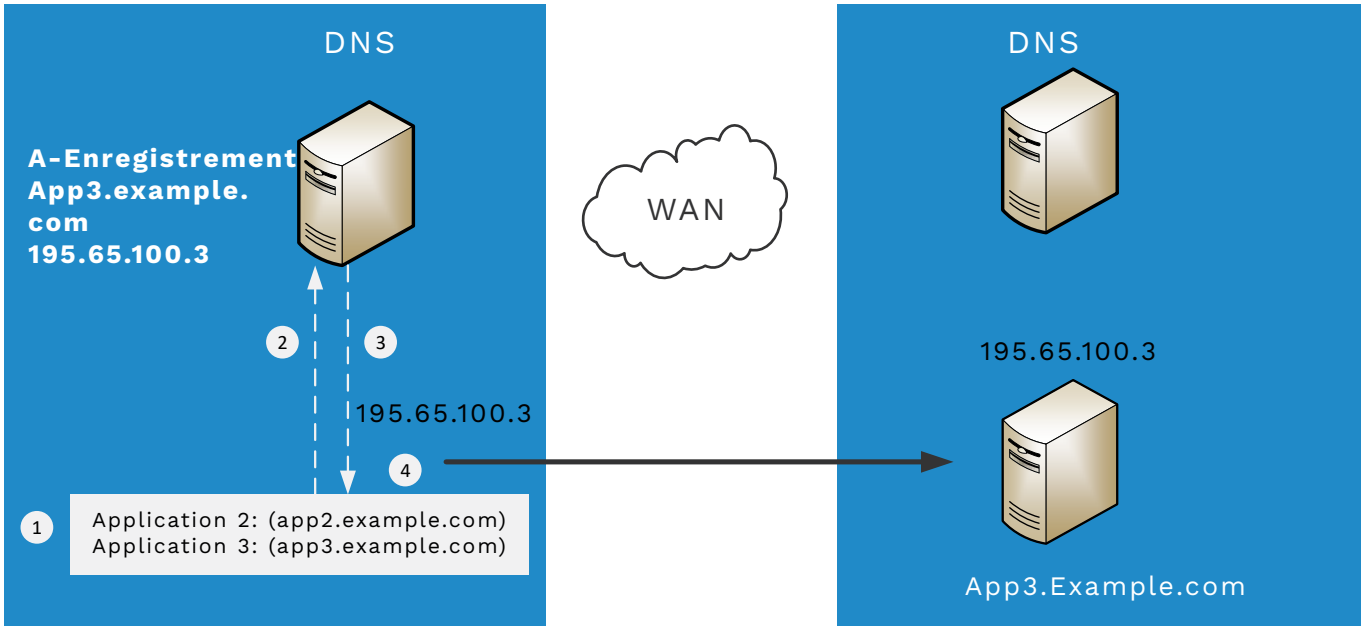
PROBLÈMES LIÉS À L'UTILISATION D'INTERNET COMME CONNEXION AU CLOUD PUBLIQUE

Sécurité - Étant donné qu'Internet est non sécurisé, une attaque de l'homme dans le milieu (Man-in-the-Middle) peut permettre à quelqu'un d'écouter les données.

Capacité - Déplacer une application vers le cloud peut augmenter le trafic réseau entre l'application et les utilisateurs. Il doit y avoir une capacité de réseau suffisante pour gérer la bande passante.

Qualité de service (QoS) - Internet ne fournit pas de QoS, mais une connexion WAN privée peut prioriser le trafic sur un lien.

Pas de niveau de service WAN (SLA) - Les FAI ne fournissent généralement pas de SLA. Les fournisseurs de WAN privés peuvent accepter un SLA dans le cadre du service.

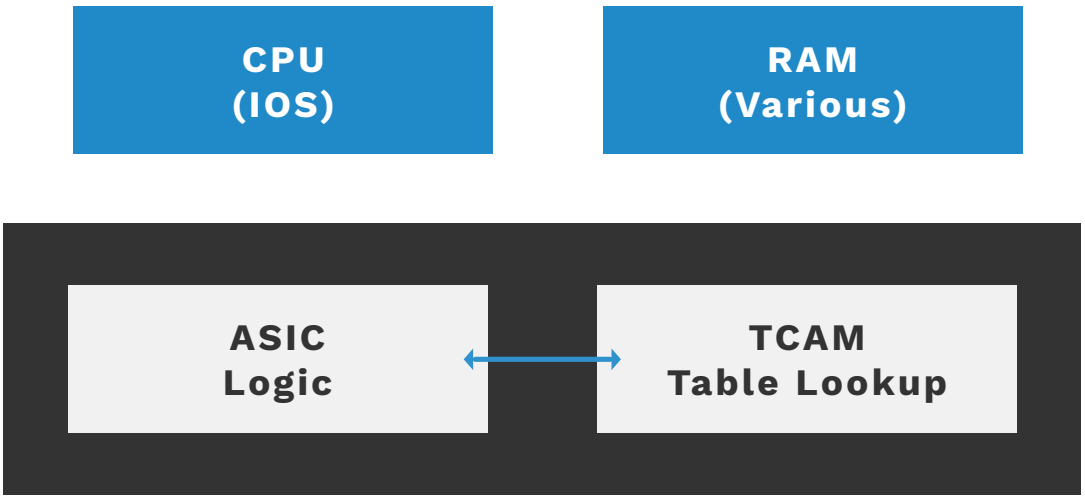


LE SERVEUR DNS EST MIS À JOUR AVEC LES ADRESSES IP PUBLIQUES DES APPLICATIONS DU CLOUD

1. l'utilisateur clique sur le lien pour app3.example.com
2. l'ordinateur envoie une requête DNS au serveur local
3. le serveur DNS renvoie l adresse IP de 195.65.100.3 pour app3.example.co
4. l'ordinateur se connecte à 195.65.100.3 pour compléter la transaction.transaction.

LES PÉRIPHÉRIQUES DU DATA PLANE EXÉCUTENT LES FONCTIONS SUIVANTES

- Encapsule et désactive les paquets (routeurs, commutateurs L3)
- Ajoute ou supprime les tags VLAN 802.1Q (routeurs et commutateurs)
- Correspondance de l'adresse MAC de destination dans la table d'adresses MAC (commutateurs L2)
- Correspondance de l'adresse IP de destination à la table de routage (routeurs, commutateurs L3)
- Chiffrement des données et ajout d'un nouvel en-tête IP (utilisé pour les connexions VPN)
- Modifie l'adresse IP source ou destination (utilisée dans les applications NAT)
- Supprime un paquet en raison d'un filtre (ACL ou sécurité du port)

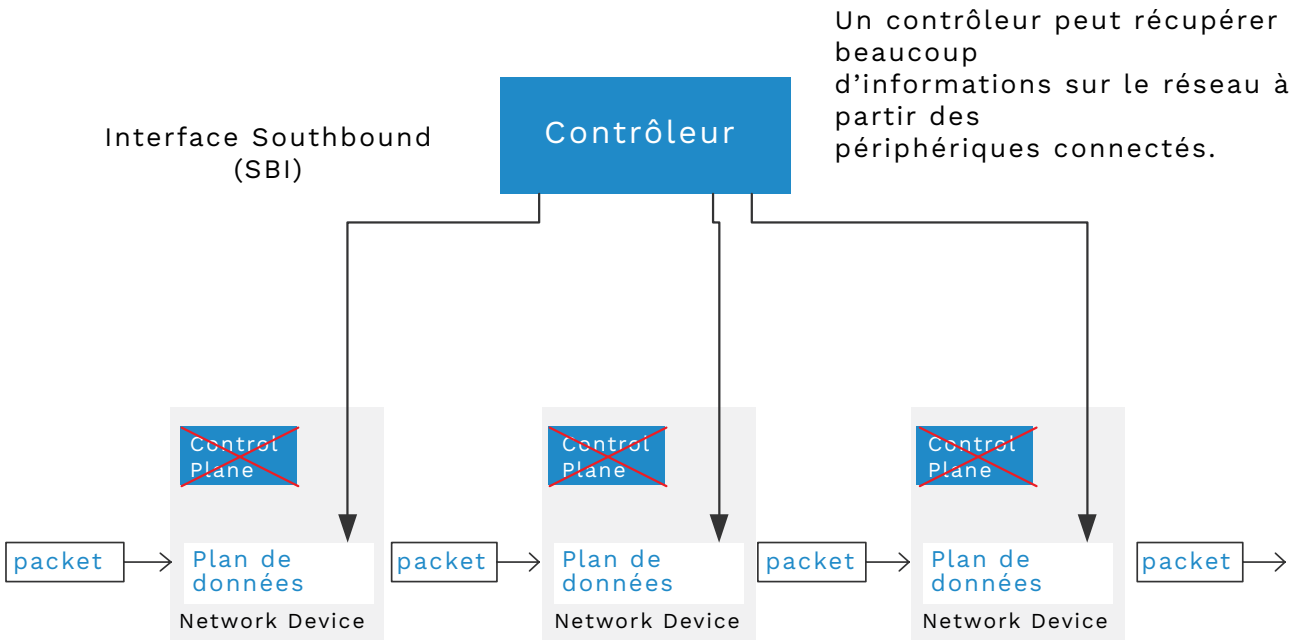


Data Plane du commutateur

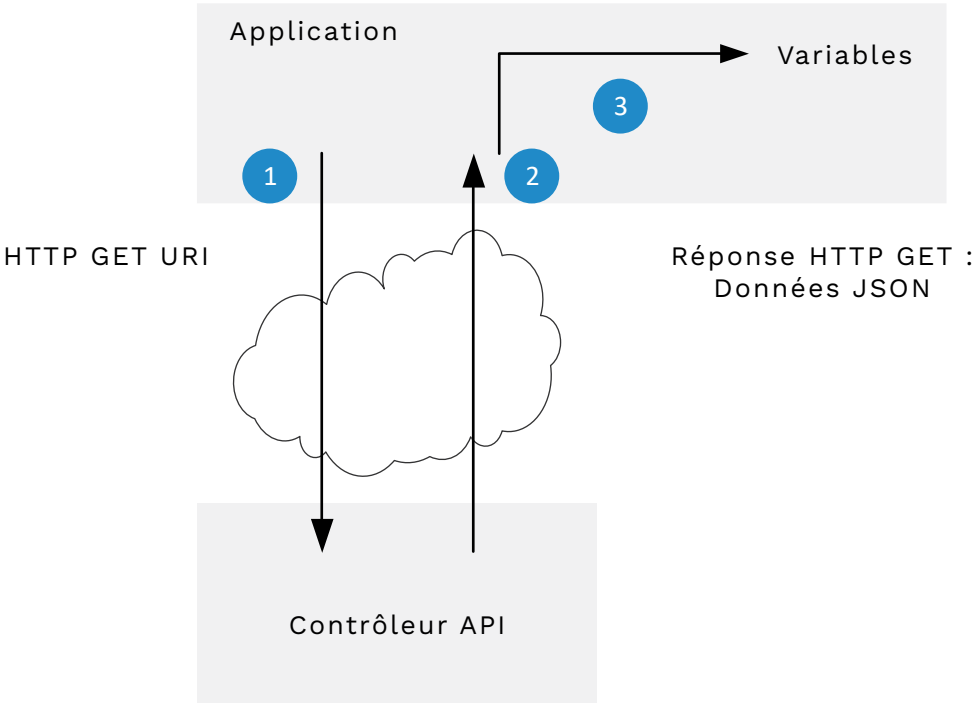
un contrôleur effectue une grande partie du travail nécessaire pour le Data Plane (plan de contrôle) dans un modèle de contrôle centralisé. Il rassemble toutes sortes d'informations utiles sur le réseau. Le contrôleur lui-même peut créer un référentiel centralisé de toutes ces informations utiles sur le réseau.

PROTOCOLES DU PLAN DE CONTRÔLE (DATA PLANE)

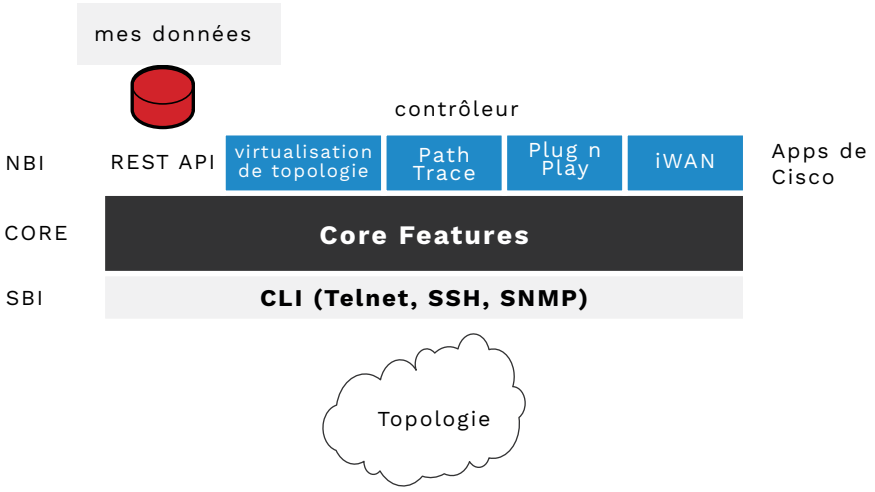
- Protocoles de routage (RIP, OSPF, EIGRP, BGP)
- IPv4 ARP
- IPv6 NDP
- Apprentissage de MAC niveau 2
- Spanning-Tree Protocol (STP)



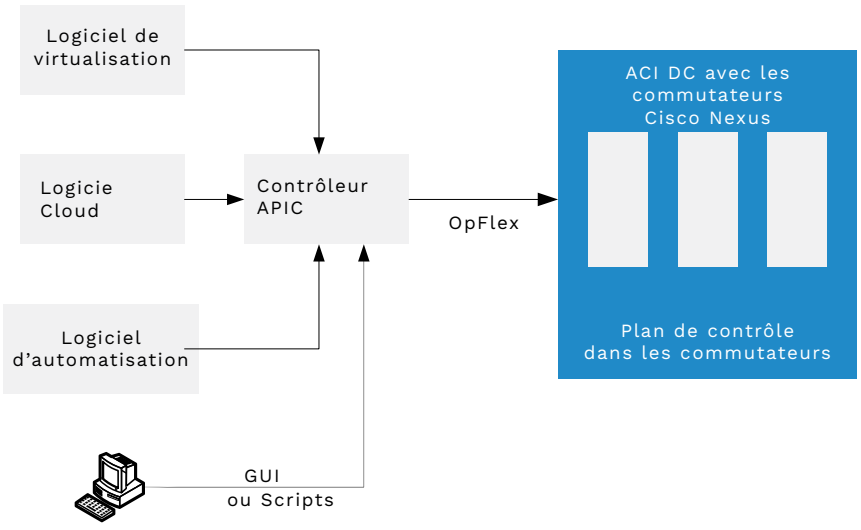
Plan de contrôle centralisé (Control Plane)
et plan de données distribuées (Data Plane) sur les périphériques réseau



Exemple de réponse GET à l'aide d'une API



Modèle de contrôleur APIC-EM

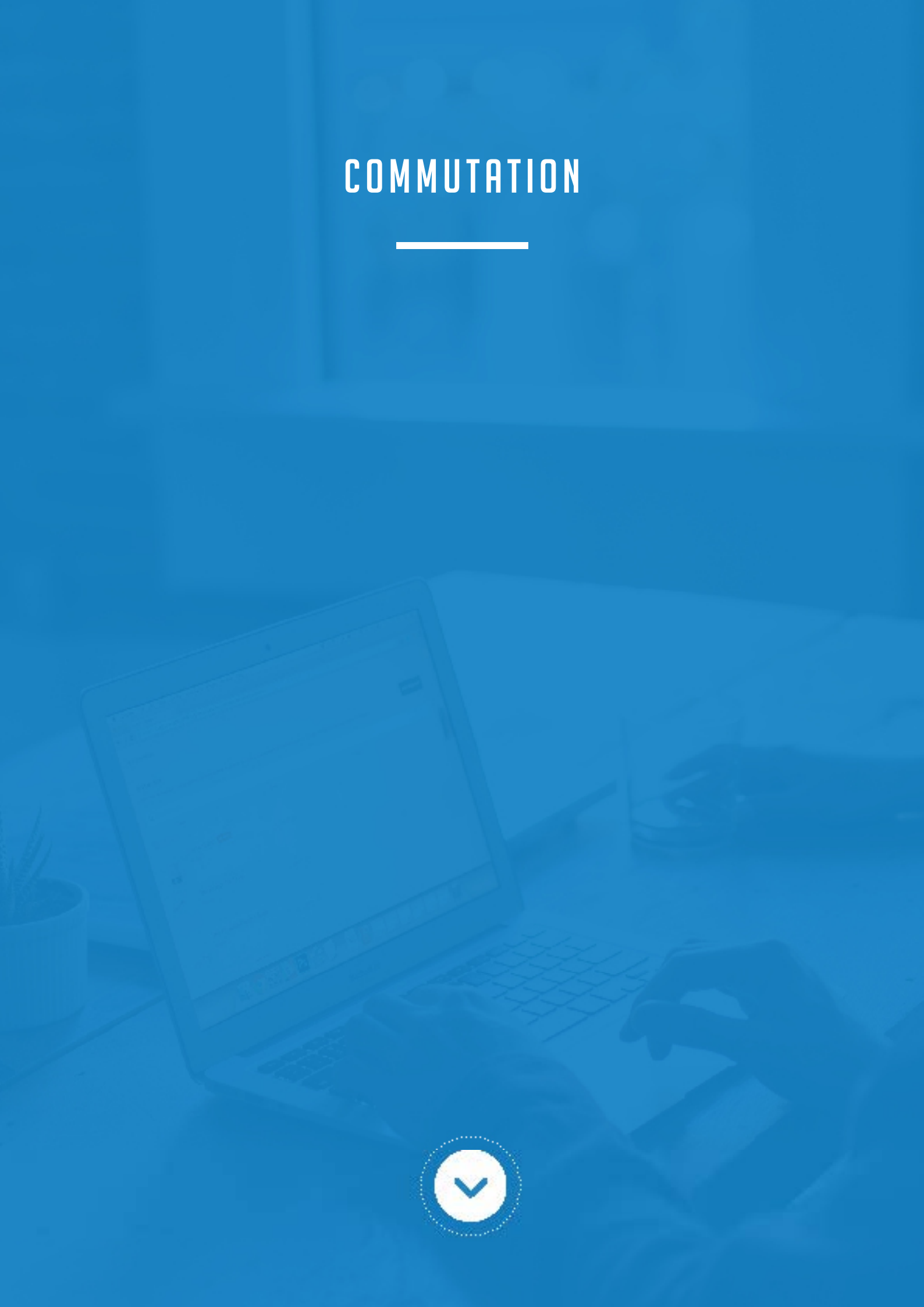


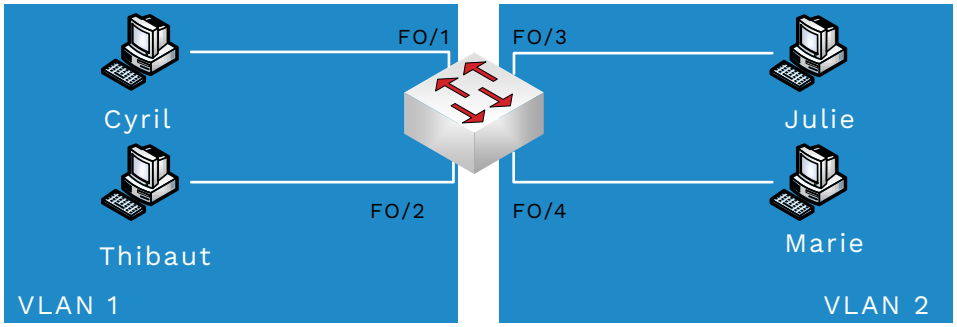
Contrôle de l'ACI DC via le contrôleur APIC

COMPARAISON DES POINTS CLÉS ENTRE OPEN SDN, ACI ET APIC ENTERPRISE

Critères	Open SDN	ACI	APIC Enterprise
Modifie le fonctionnement du Control Plane par rapport aux réseaux traditionnels	Oui	Oui	Non
Crée un point centralisé à partir duquel les humains et l'automatisation contrôlent le réseau	Oui	Oui	Oui
Degré dans lequel l'architecture centralise le plan de contrôle	Pour la plupart	Partially	N/A (1)
SBI utilisés	OpenFlow	OpEx	CLI,SNMP
Exemple de contrôleurs	OpenDaylight, Cisco ASC	APIC	APIC-EM
Organisation qui est l'auteur principal / propriétaire	ONF	Cisco	Cisco

COMMUTATION

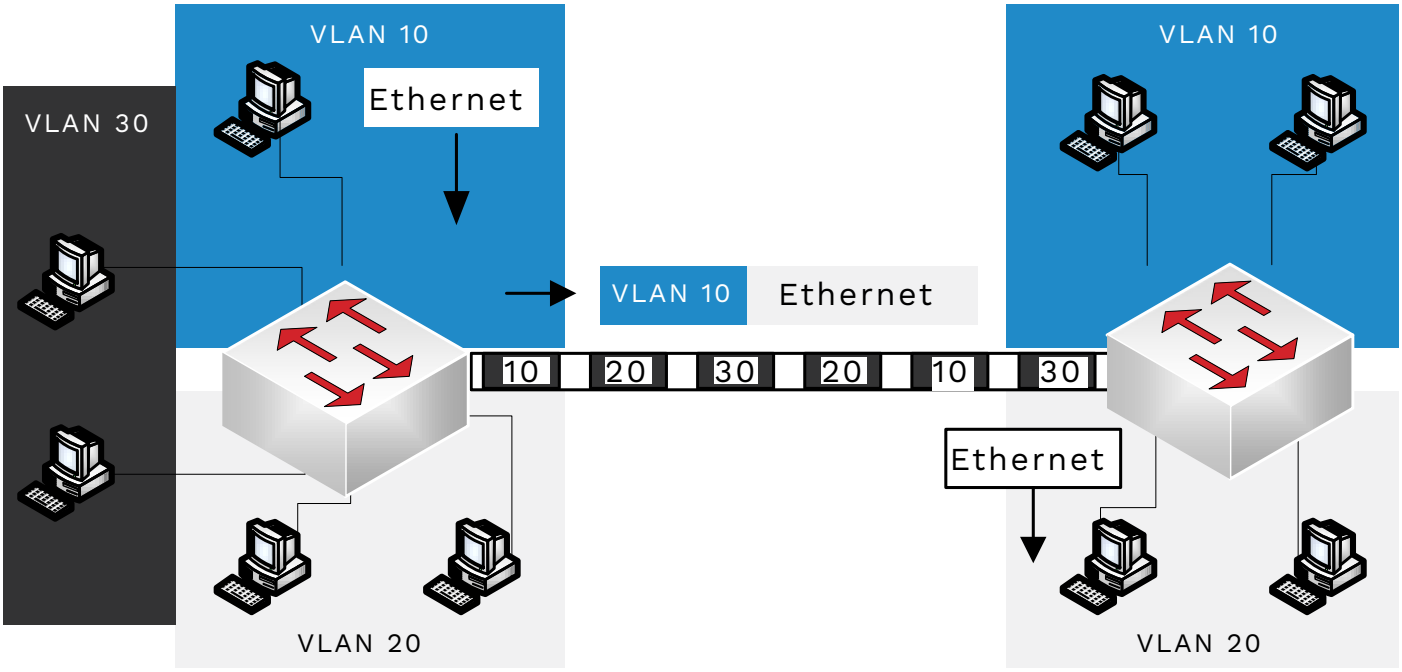




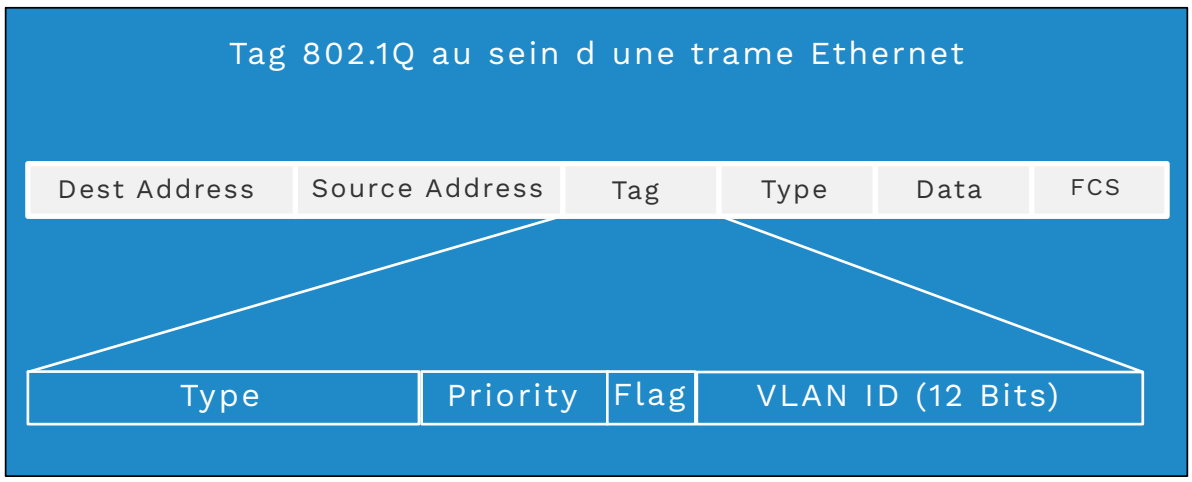
Création de deux domaines de diffusion avec un commutateur et deux VLAN

OBJECTIFS DU VLAN

- Réduire le nombre d'équipements qui reçoivent les trames de diffusion
- Réduire le risque de sécurité en diminuant le nombre de trames que chaque équipement reçoit
- Améliorer la sécurité de certains équipements en les isolants dans un VLAN distinct
- Créer des designs plus flexibles basés sur des groupes, des départements ou autres besoins métiers
- Résoudre les problèmes plus rapidement car chaque domaine de diffusion est séparé
- Réduire le temps de calcul du protocole Spanning-Tree en limitant un VLAN à un seul commutateur d'accès



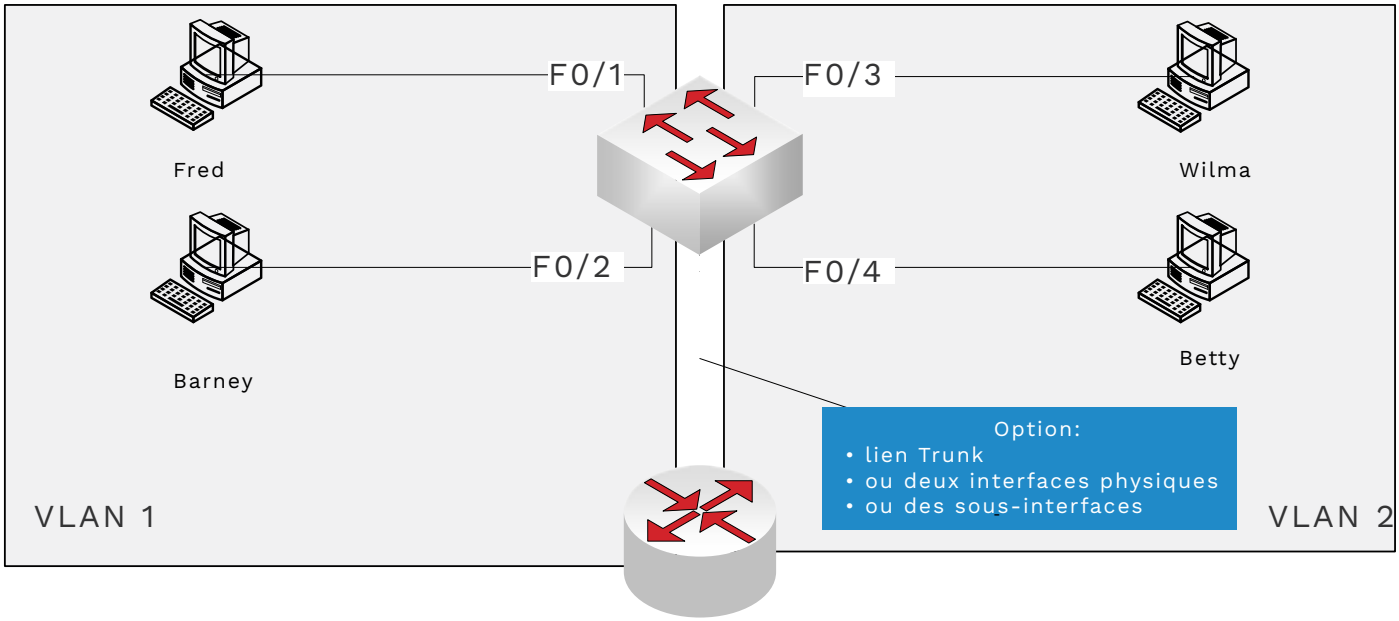
3 VLAN Trunking entre deux commutateurs



NOTIONS IMPORTANTES À SAVOIR SUR LES VLANS

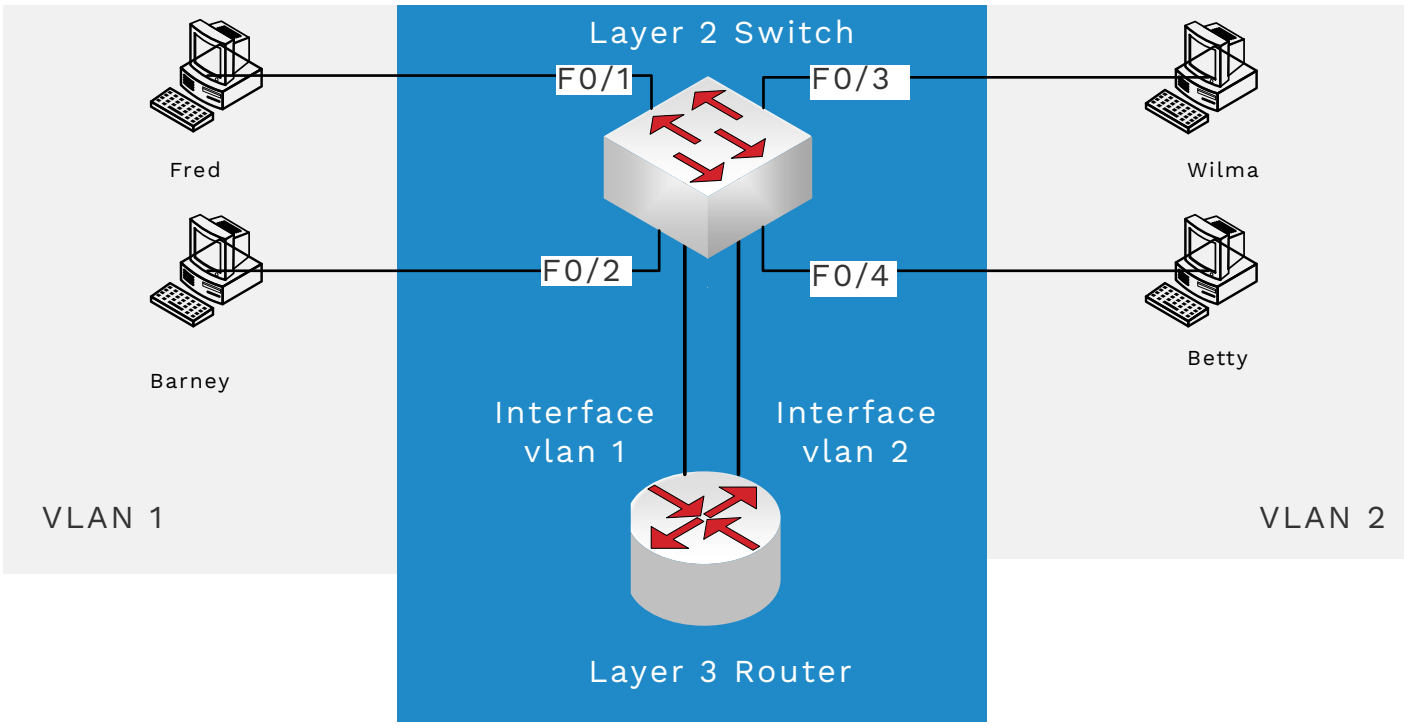
les commutateurs Cisco peuvent utiliser les VLAN 1 à 4094. Cette plage est divisée en deux sous-plages. Les VLAN 1 à 1005 sont présents sur les commutateurs anciens. Les récents commutateurs peuvent utiliser la plage d'origine et la plage qui contient les VLAN 1006 à 4094.

VLAN natif: ce VLAN, également appelé VLAN non taggé, se compose de paquets Ethernet sans tag 802.1q (étiquette) envoyés sur un réseau Ethernet. S'il y a un périphérique à l'autre extrémité qui ne comprend pas le Trunk, le commutateur peut prendre ce trafic non taggé et le placer sur le VLAN Natif. La modification du VLAN natif sur un port ou un Trunk peut être utilisée comme mesure de sécurité ou lorsqu'un périphérique tel qu'un téléphone VoIP Cisco utilise le trafic taggé pour le trafic voix et non taggé pour les données.



R1

Routage entre deux Vlans sur un commutateur



Routage entre deux vlans sur un commutateur de couche 3 (symbolisé par le carre bleu)

Note: 1 VLAN = 1 IP Subnet

CRÉATION DE VLAN ET ATTRIBUTION D'INTERFACES

Étape 1: à partir du mode de configuration, utilisez la commande **vlan vlan-id** pour créer le VLAN. Utilisez la sous-commande **name NOM** pour nommer le VLAN (par exemple, name Finance)

Étape 2: pour chaque interface qui rejoindra le vlan, utiliser la commande **switchport access vlan vlan-id** et définissez le port en mode accès avec la commande **switchport mode access.**

```
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name SALES
Switch(config-vlan)# exit
Switch(config)# interface FastEthernet 0/3
Switch(config-if)# switchport access vlan 2
Switch(config-if)# switchport mode access
Switch(config-if)# exit
Switch(config)# exit
Switch# show vlan

VLAN  Name                             Status    Ports
1     SALES                            active    Fa0/3

Switch#
```

Remarque: au lieu d'utiliser un routeur physique et un switch pour effectuer du routage entre VLAN, on peut utiliser des nouveaux commutateurs qui intègrent les fonctionnalités Layer-2 et Layer-3. Ces commutateurs sont appelés commutateurs multicouches et permettent à l'ingénieur réseau d'avoir une commutation Layer-2 et un routage Layer-3 dans la même boîte physique.

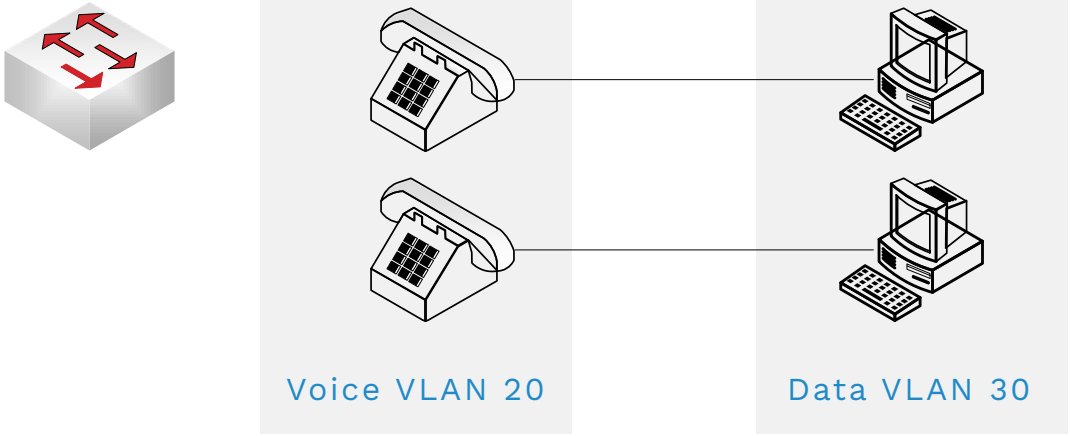
Option	Description
Access	Agi comme un port d'accès (pas de Trunk)
Trunk	Agi comme un port Trunk
Dynamic desirable	Initie des messages de négociation pour monter le Trunk
Dynamic Auto	Attend des messages de négociation pour monter le trunk

Options du mode trunk

Mode configuré	Access	Dynamic Auto	Trunk	Dynamic desirable
Access	Access	Access	Erreur	Access
Dynamic Auto	Access	Access	Access	Trunk
Trunk	Erreur	Trunk	Trunk	Trunk
Dynamic desirable	Access	Trunk	Trunk	Trunk

Mode attendu en fonction de la configuration du port

Si un port est configuré en **Access** et que l'autre port est défini en **Trunk**, le Trunk ne montera pas. Assurez-vous que ce que vous définissez d'un côté du lien correspond à l'autre côté du lien



CONTRÔLE DES VLANS SUR UN LIEN TRUNK

Il peut y avoir plusieurs raisons pour lesquelles le trafic pour un VLAN particulier ne passera pas sur un Trunk. Ci-dessous les raisons potentielles:

- Un VLAN a été supprimé de la liste de VLAN autorisée du Trunk
- Un VLAN n'existe pas dans la configuration du commutateur
- Un VLAN existe, mais il a été désactivé
- Un VLAN a été automatiquement élagué par VTP
- L'instance STP d'un VLAN a placé l'interface du Trunk dans un état de blocage

UTILISATION DE TÉLÉPHONES ET D'ORDINATEURS SUR LE MÊME PORT DU SWITCH

Les commutateurs Cisco peuvent marquer différemment le trafic voix et le trafic
donnés sur le même port physique du commutateur. Le VLAN donnée est configuré comme un port d'accès. Le VLAN voix a un tag différent. Le trafic pour le VLAN de données sera non taggé entre le téléphone et l'ordinateur.

CONFIGURATION DES VLAN VOIX ET DONNÉES

SW1# **configure terminal**
SW1 (config)# **interface FastEthernet 0/1**
SW1 (config-if)# **switchport mode access**
SW1 (config-if)# **switchport access vlan 30**
SW1 (config-if)# **switchport voice vlan 20**
SW1 (config-if)# **^Z**

Configurez l'interface en tant que port d'accès, puis définissez le VLAN donnée. Enfin, définissez le VLAN voix. Notez que le Trunk est implicite et n'est pas directement configuré sur l'interface.

POURQUOI METTONS-NOUS EN OEUVRE LE PROTOCOLE SPANNING TREE (STP)?

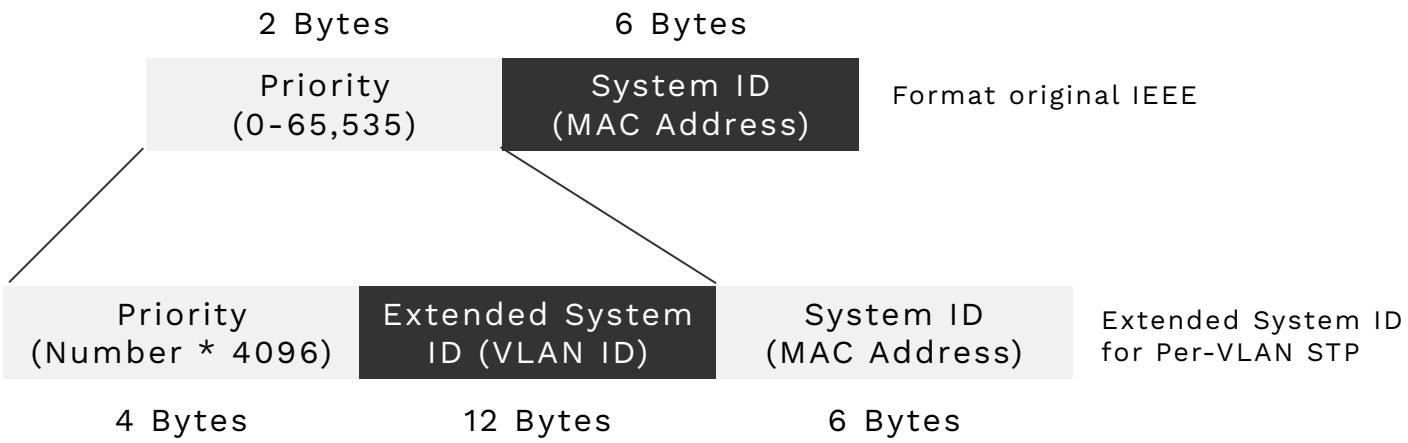
Problème	Description
Tempêtes de Broadcast (broadcast storm)	Une trame de broadcast est transmise à plusieurs reprises sur les mêmes liens entraînant une saturation des liens et évinçant le trafic légitime
Table d adresses MAC instable	Quand les tables MAC sont constamment mises à jour, des boucles apparaissent. Ainsi, les trames seront envoyées aux mauvaises destinations
Réception multiple de trames	Les hôtes peuvent recevoir de multiples copies de la même trame créant la confusion dans les protocoles de couche supérieure de l'hôte.

ÉTATS DE TRANSMISSION OU DE BLOCAGE STP BASÉS SUR LE STATUT DU PORT

Statut de Port	État STP	Description
Tous les ports du commutateur racine (Root)	Transmission (forwarding)	Le commutateur racine est au sommet de l'arbre et aucun port n'est bloqué
Port racine surcommutateur nonracine (non Root)	Transmission (forwarding)	Port avec le coût le plus bas vers le commutateur racine
Port Désigné	Transmission (forwarding)	Le port transmet les BPDU ou Hello sur ce segment LAN
Tous les ports du commutateur racine (Root)	Blocage (blocking)	Les trames BPDU ne sont ni envoyées ni reçues sur cette interface

CHAMPS DU BPDU (BRIDGE PROTOCOL DATA UNIT)

Champ	Description
Root Bridge ID	ID de commutateur de la source de ce Hello pensant qu'il est le commutateur racine (Root Bridge)
Sender Bridge ID	ID de commutateur du relai pour ce Hello
Sender root cost	Coût STP entre le commutateur racine et le commutateur relai
Valeurs des minuteurs du commutateur racine (Root bridge)	Minuteur pour hello, MaxAge, forward delay



Bridge ID et System ID – utilisé dans le Hello BPDU

L'ÉLECTION DU COMMUTATEUR RACINE (ROOT) EST LA SUIVANTE

- la priorité la plus basse
- en cas d'égalité, celui qui a la plus petite adresse MAC

Vitesse Ethernet (speed)	Cout IEEE (1998 et ultérieur)	Cout IEEE (2004 et postérieur)
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2,000
100 Gbps	N/A	200
1 Tbps	N/A	20

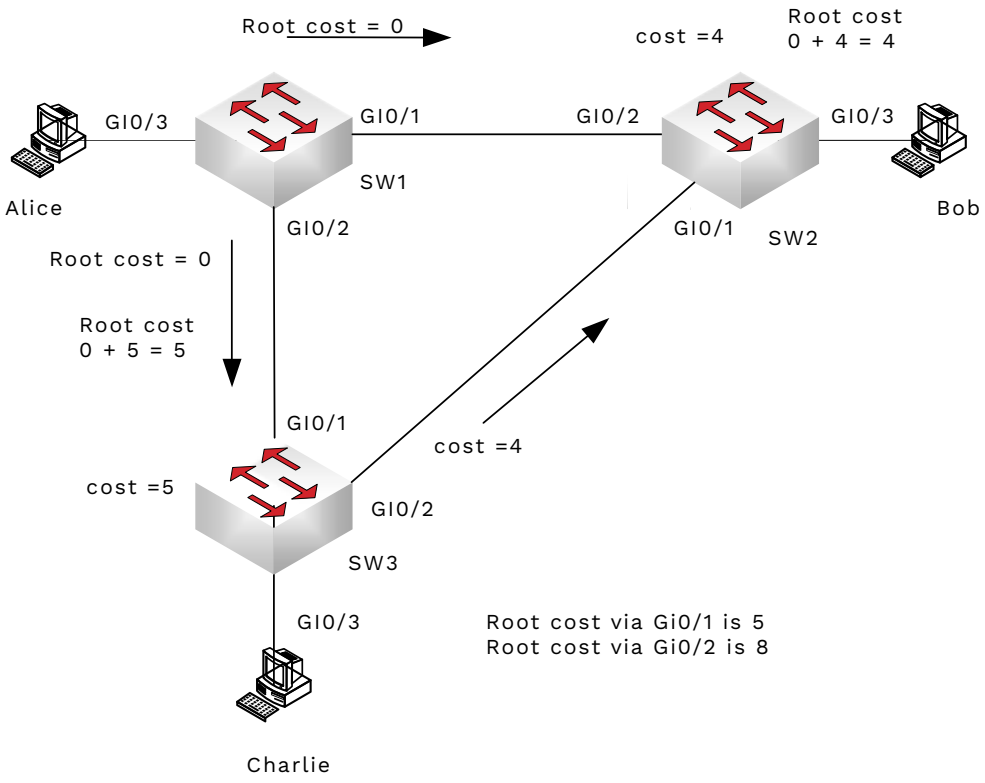
Couts par défaut des interfaces

FONCTIONNEMENT STP

1. Le commutateur racine envoie un Hello BPDU avec un coût racine de zéro sur toutes ses interfaces

2. Chaque commutateur non-root reçoit la BPDU hello sur le port racine, modifie le coût du port racine en conséquence et envoie le BPDU sur ses autres interfaces

3. Répétez jusqu'à ce que quelque chose change et force le recalcule STP



Timers STP

Heurest	Valeur par default	Description
Hello	2 seconds	Intervalle entre les BPDU Hello créées par le commutateur racine
Max Age	10 x Hello	Temps d'attente entre Hellos avant de forcer le recalcule STP
Forward delay	15 seconds	Temps pour une interface de passer de l'apprentissage (learning) à l'état de transfert (forwarding) après l'état d'écoute (listening)

STP ÉTATS TRANSITOIRES

Écoute (listening) - un état où le commutateur supprime les adresses MAC reçues sur le port.

Apprentissage (learning) - un état dans lequel le port n'est toujours pas actif, mais l'apprentissage des images d'adresse MAC reçues sur l'interface

Etat	Transmet les images de données?	Apprend les Macs en fonction des cadrest reçus?	État transitoire ou stable?
Blocking	Non	Non	Stable
Listening	Non	Non	Transitoire
Learning	Oui	Oui	Transitoire
Forwarding	Oui	Oui	Stable
Disabled	Non	Non	Stable

États d'interface Spanning Tree

COMPARAISON DE STP ET RSTP

RSTP fonctionne comme STP de la manière suivante:-

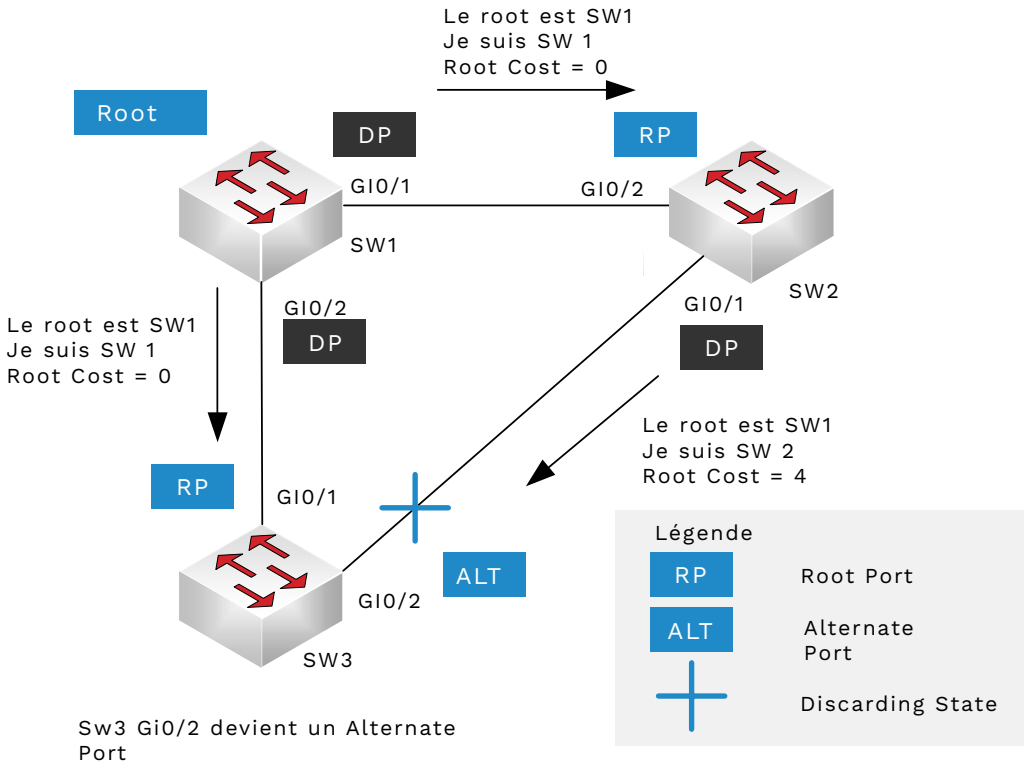
- Les élections de commutateur utilisent les mêmes paramètres
- Le port racine est déterminé sur les commutateurs non-root de la même manière
- Les ports désignés sont déterminés par les mêmes règles
- Chaque port est placé dans l'état de transfert ou de blocage, mais RSTP utilise un état de rejet (discarding) au lieu d'un état de blocage (blocking).

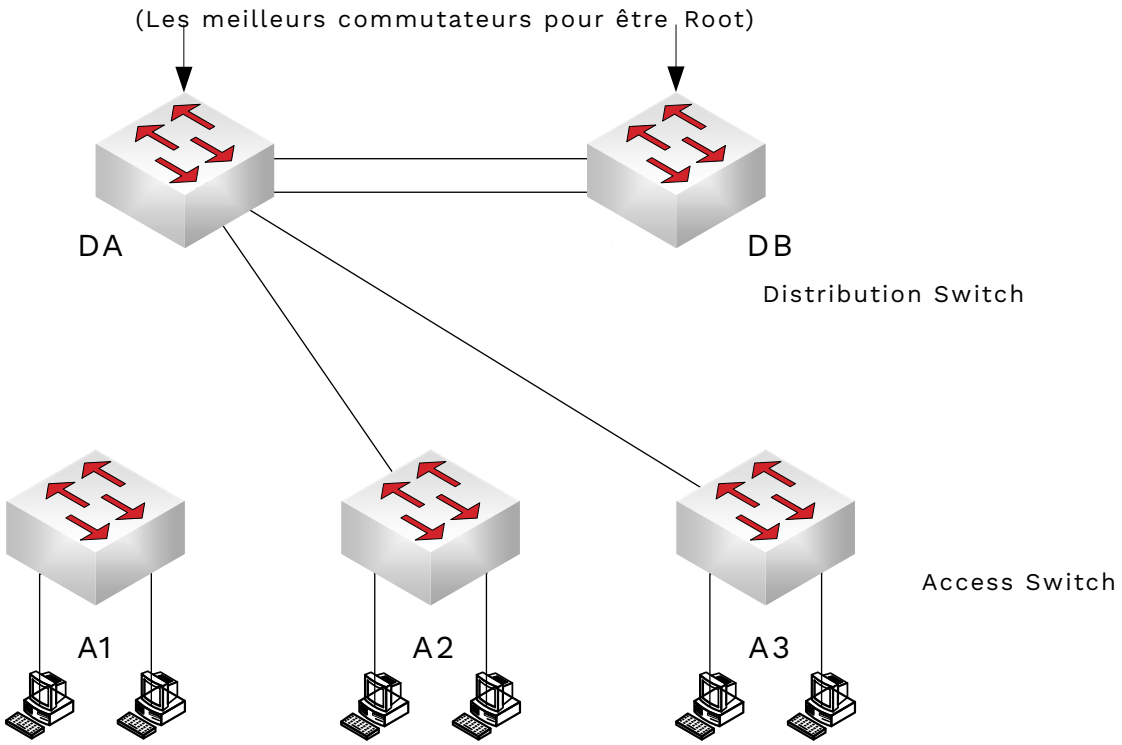
Rôles des ports en 802.1w RSTP

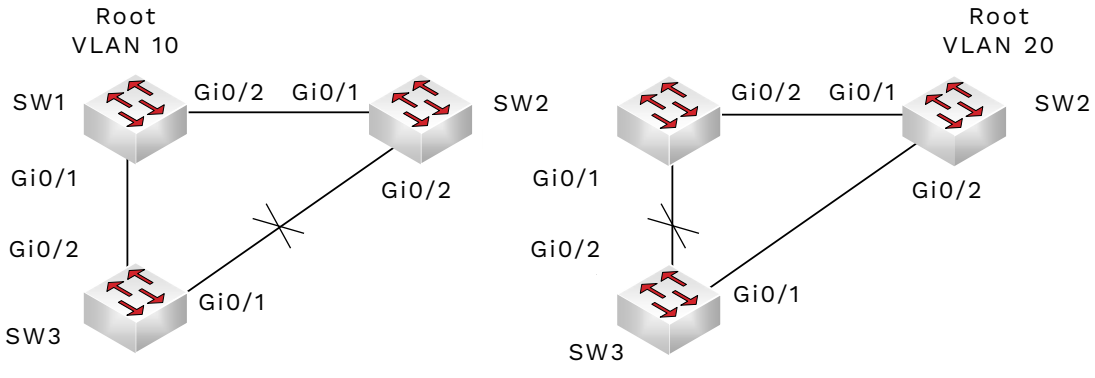
Fonction	Rôle du port
Non-root switch avec le meilleur chemin vers la racine	Root port
Remplace le port racine lorsque le port racine original échoue	Alternate Port
Port qui commute toutes les trames utilisateurs	Designated Port
Remplace un port désigné lorsque le port désigné échoue	Backup Port
Port qui est administrativement désactivé / arrêté	Disabled Port

Comparaison des ports entre 802.1d STP et 802.1w RSTP

Fonction	802.1D Etat	802.1tw État
Port qui est administrativement désactivé / arrêté	Disabled	Discarding
Etat stable qui ignore les trames entrantes et ne renvoie pas les trames	Blocking	Discarding
Etat provisoire sans connaissance adresse MAC ou transmission	Listening	Non utilisé
Etat provisoire sans connaissance adresse MAC mais toujours sans transmission	Learning	Learning
Etat Final avec connaissance adresse MAC et transmission	Forwarding	Forwarding

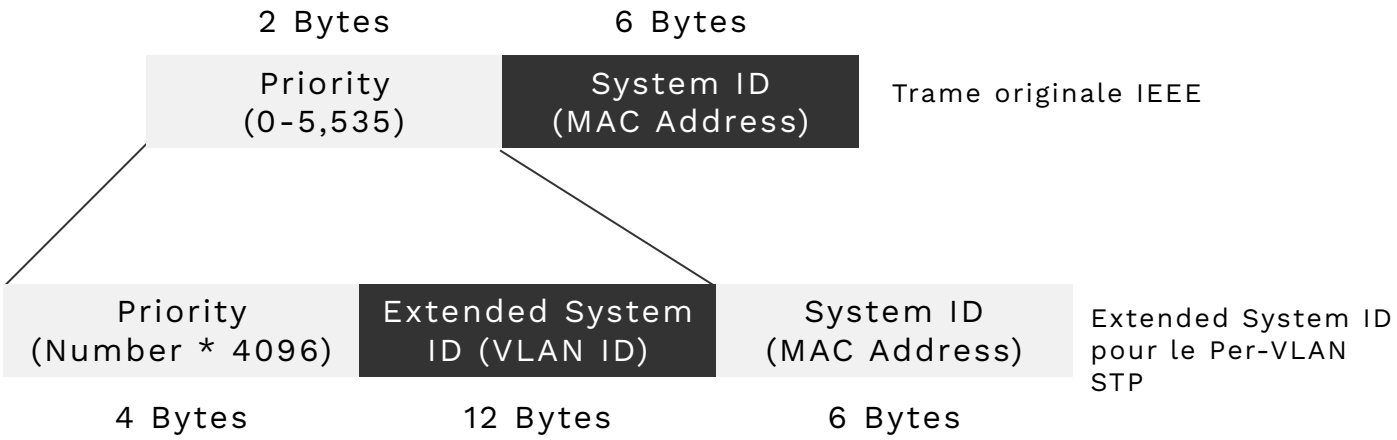






Equilibrage de charge (load-balancing) à l'aide du Per-VLAN Spanning Tree.
Le VLAN 10 a un commutateur racine différent du VLAN 20.

Bridge_ID et System_ID - utilisé dans les BPDU Hello



DÉTERMINATION DU COMMUTATEUR RACINE DANS UN RÉSEAU

1. Commencez par un diagramme et faites une liste des commutateurs root possibles

2. Connectez-vous à chaque potentiel commutateur racine et lancez la commande **show spanning-tree.** S'il existe un port racine (RP), supprimez le commutateur car le commutateur root n'a pas de RP.

3. Utilisez show spanning-tree et recherchez le texte **"This bridge is the root"** ou utilisez la commande **show spanning-tree root.** Si le texte apparaît, vous avez identifié le commutateur racine. Dans le cas de la dernière commande, un commutateur racine n'aura pas de RP.

Préparation à l'examen

Lors d'un lab avec plusieurs commutateurs, recherchez les commutateurs racine en utilisant la commande **show spanning-tree root** pour localiser les RP (Root Port). Pour rappel, les RP vous diront quel commutateur est le commutateur racine.

Si le lab possède plusieurs VLAN, utilisez **show spanning-tree vlan x** pour trouver le commutateur racine pour chaque VLAN si nécessaire. Notez que le commutateur root pour un VLAN peut être différent des autres VLAN.

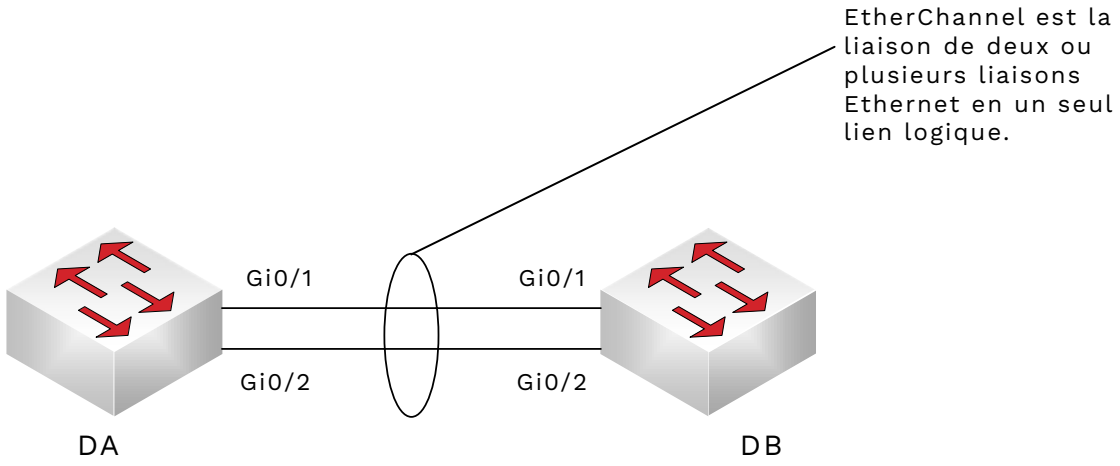
Pour définir un commutateur particulier pour être le commutateur racine sur un VLAN, utilisez la commande **spanning-tree vlan X root primary**

Définir SW2 comme Root sur VLAN 20
SW2 (config) **# spanning-tree vlan 20 root primary**

Définir SW1 comme Root sur VLAN 10
SW1 (config) **# spanning-tree vlan 10 root primary**

Veuillez noter ce qui suit avec cette commande:

- Si le commutateur racine actuel a une priorité supérieure à 24 576, le commutateur local utilise la priorité de base de 24 576.
- Si le commutateur racine actuel a une priorité inférieure à 24 576, le commutateur local utilise une priorité de base d'un multiple de 4096, ce qui fait que le commutateur local devient root (exemple 8,192, 16,384 ...)



CONFIGURATION MANUELLE DES LIENS ETHERCHANNEL

(1) ajoutez le **channel group NUMERO mode on** sur les interfaces souhaitées.
(2) utilisez le même **Channel-group** pour les commandes EtherChannel sur le même commutateur. Un numéro de **Channel-group** différent peut être utilisé sur d'autres commutateurs

DA(config)**# interface Gi0/1**
DA(config-if)**# channel group 1 mode on**
DA(config-if)**# interface Gi0/2**
DA(config-if)**# channel group 1 mode onGi0**

DÉPANNAGE DES PROBLÈMES ETHERCHANNEL

Généralement, les commandes Port-channel doivent correspondre des deux côtés de la liaison sauf pour le numéro du **Channel-group** qui est localement significatif sur chaque commutateur.

Processus:

1) Assurez-vous que toutes les interfaces du lien EtherChannel sur le même commutateur ont le même numéro **Channel-group**

2) Le numéro du **Channel-group** est localement significatif sur chaque commutateur

3) Si vous utilisez le mot-clé **on**, il doit s'appliquer aux deux côtés du lien EtherChannel

4) Si vous utilisez le mot-clé **desirable** d'un côté du lien, le mot-clé **desirable** ou **auto** doit être utilisé comme mot-clé de l'autre côté du lien si le commutateur utilise PAgP.

5) Si vous utilisez le mot-clé **active** sur un côté du lien, le mot-clé **active** ou **passive** doit être utilisé de l'autre côté du lien si le commutateur utilise LACP.

Ajout de liens vers EtherChannels existants:

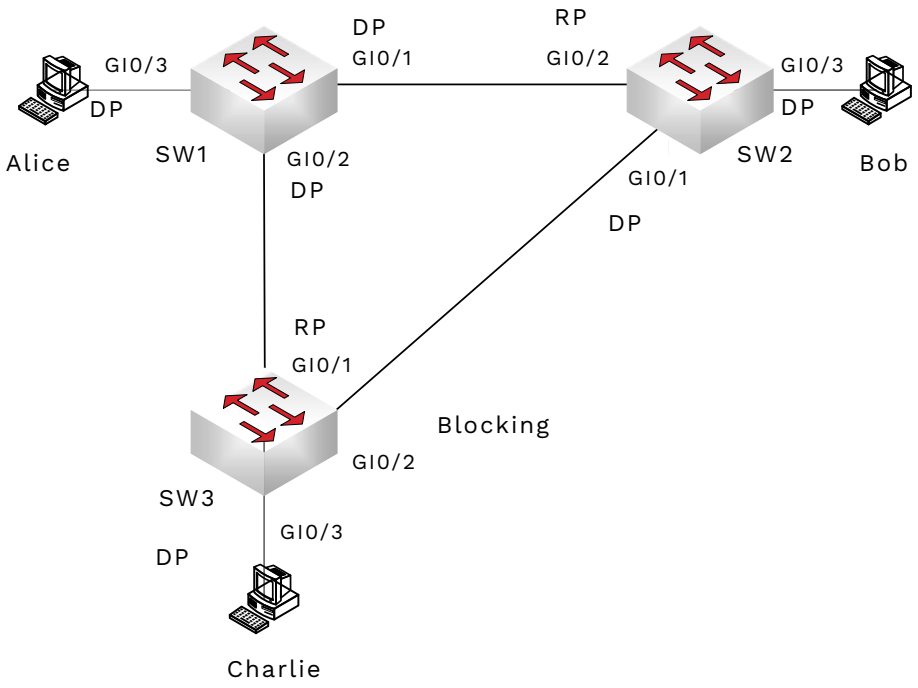
Vous devez vérifier les éléments suivants avant d'ajouter un lien vers un lien EtherChannel existant: vitesse, duplex, access ou Trunk, access VLAN, VLAN natif et / ou VLAN autorisés pour les ports et paramètres Spanning-tree.

LOCALISATION DU PORT DÉSIGNÉ (DP) SUR CHAQUE SEGMENT

Rappelez-vous que le port désigné est la connexion du commutateur au commutateur racine. Voici comment trouver le port désigné sur n'importe quel commutateur

1) Si les commutateurs sont sur le même segment LAN, celui avec le coût racine le plus bas devient le DP sur ce segment.

2) S'il y a une égalité après l'étape 1, le commutateur avec le plus petit Bridge_ID devient le DP sur ce segment.



CONTRÔLES DE CONFIGURATION AVANT D'AJOUTER DES PORTS À UN ETHERCHANNEL

Avant d'ajouter un port ou des ports à un Etherchannel, les éléments suivants sur chaque port doivent être vérifiés:

- Vitesse
- Duplex
- Tous les ports doivent être soit en **Access** ou en **Trunk** (pas de mélange de ports Access et Trunk sur un lien Etherchannel).
- VLAN d'accès sur le port en mode **Access**
- Liste VLAN autorisée pour un port **Trunk** (commande **switchport trunk vlan allowed...)**
- VLAN natif si un port Trunk
- Spanning-Tree (portfast, protection BPDU)

S'il y a un décalage de paramètres sur l'un des ports EtherChannel, le Etherchannel ne peut pas monter et le trafic réseau ne transitera pas.

COMPARAISON DES COMMANDES SW1 ET SW2 SHOW SPANNING-TREE

SW1# show spanning-tree

VLAN0001

Protocole de Spanning tree Activé ieee

Root ID	**Priority**	**32769**
	Address	**0c00.2345.1211**
	This bridge is the root	
Bridge ID	**Priority**	**32769 (priority 32768 sys-id-ext 1)**
	Address	**0c00.2345.1211**

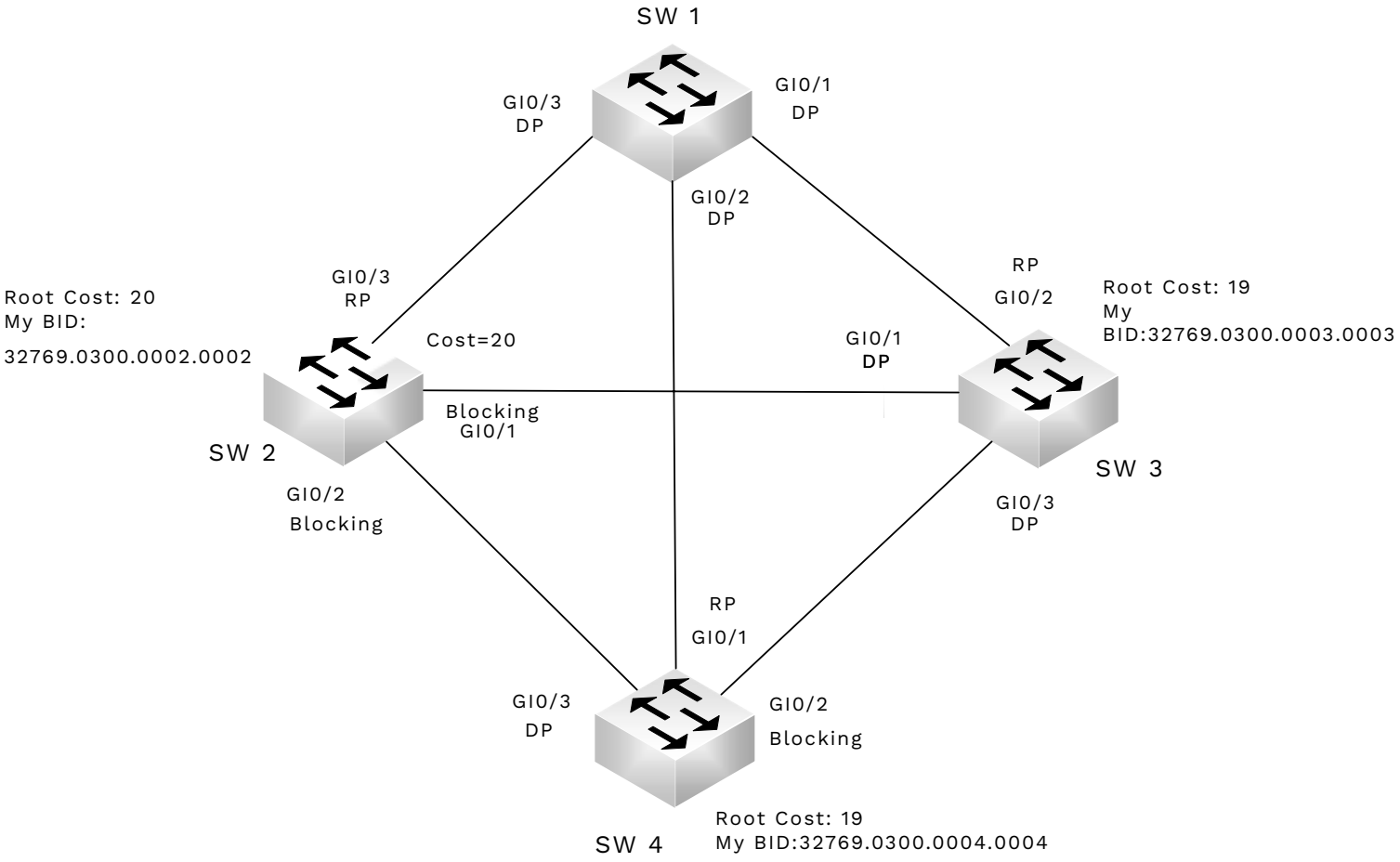
SW2# show spanning-tree

VLAN0001

Protocole de Spanning tree Activé ieee

Root ID	**Priority**	**32769**
	Address	**0c00.2345.1211**
	Cost	**4**
	Port	**26 (GigabitEthernet 0/2)**
Bridge ID	**Priority**	**32769 (priority 32768 sys-id-ext11)**
	Address	**0c00.2345.5504**

SW1 indique qu'il s'agit du commutateur racine sur le VLAN 1. SW2 indique le commutateur qui est le pont racine par les informations Root_ID, Root Cost et l'adresse MAC du commutateur racine.



Dans ce diagramme, vous pouvez voir comment les ports racine et les ports désignés (DP) sont sélectionnés. Les commutateurs SW2, SW3 et SW4 ont tous des connexions directes à SW1 qui est le commutateur racine et les ports connectés sont les ports racine.

Si vous regardez SW3 et SW4, leur coût racine est de 19, tandis que le coût racine SW2 est de 20. Lors de la sélection des DP, le commutateur avec l'ID du pont inférieur sur la connexion aura le DP pour cette connexion. SW3 a le coût de racine le plus petit pour chacune de ses connexions à SW2 et SW4. SW3 a les DP pour ses segments. Mais si vous regardez SW4, il a également un coût de racine de 19 et son interface pour SW3 est dans un état de blocage. Puisque SW4 a un coût de racine inférieur à SW2, le port sur SW4 connecté à SW2 est le DP pour ce segment.

Cela signifie que SW2 n'a qu'un RP et ses connexions à SW3 et SW4 sont placées dans un état de blocage.

Les éléments suivants sont nécessaires pour que VTP fonctionne entre deux commutateurs.

1) Le lien entre les commutateurs doit être un Trunk (802.1Q ou ISL)
2) Le nom de domaine VTP doit être identique sur deux commutateurs
3) Le mot de passe doit correspondre aux deux commutateurs si activé de passe (attention il est sensible à la casse)

Si VTP est utilisé, au moins un commutateur doit être En mode server et les autres en mode client.

Avertissement - avant de connecter un commutateur à un réseau existant, configurez le en mode transparent à l'aide de la commande vtp mode transparent.

CONFIGURATION DE VTP

Avant de configurer VTP, il faut déterminer les commutateurs qui utiliseront VTP et la façon dont ils seront regroupés.

1. Réglez le mode VTP sur le commutateur sur server ou client avec la commande **vtp mode server|client.**

2. Définissez le nom de domaine VTP sur chaque commutateur client et serveur avec la commande **vtp domain NOM_DOMAINE.**

3. Le réglage du mot de passe VTP est facultatif via la commande **vtp password MOT_DE_PASSE.**

4. Pour les serveurs, activez l'élagage VLAN avec la commande **vtp pruning.**

5. Définir la version VTP sur chaque serveur ou client en 1 ou 2 avec la commande **vtp version 1|2**

TABLEAU DES FONCTIONNALITÉS VTP

Fonction	Serveur	Client	Transparent
Envoie uniquement des msg VTP sur Le Trunk	Oui	Oui	Oui
Permet la configuration VLAN via CLI	Oui	Non	Oui
Peut utiliser les VLAN 1 - 1005 (plage normale)	Oui	Oui	Oui
Peut utiliser les VLAN 1006 - 4095 (gamme étendue)	Non	Non	Oui
La base de données est resynchronisée lorsqu'un message VTP avec un nombre plus élevé est reçu	Oui	Oui	Non
Envoie et crée des messages VTP toutes les 5 minutes	Oui	Oui	Non
Envoie les mises à jour VTP reçues sur les Trunk, mais n'agit pas sur les mises à jour	Non	Non	Oui

OÙ VTP STOCKE SES INFORMATIONS?

running-config

Attribuer un VLAN à l'interface
switchport access vlan X

vlan.dat

Commandes VLAN
vlan x
name NOM

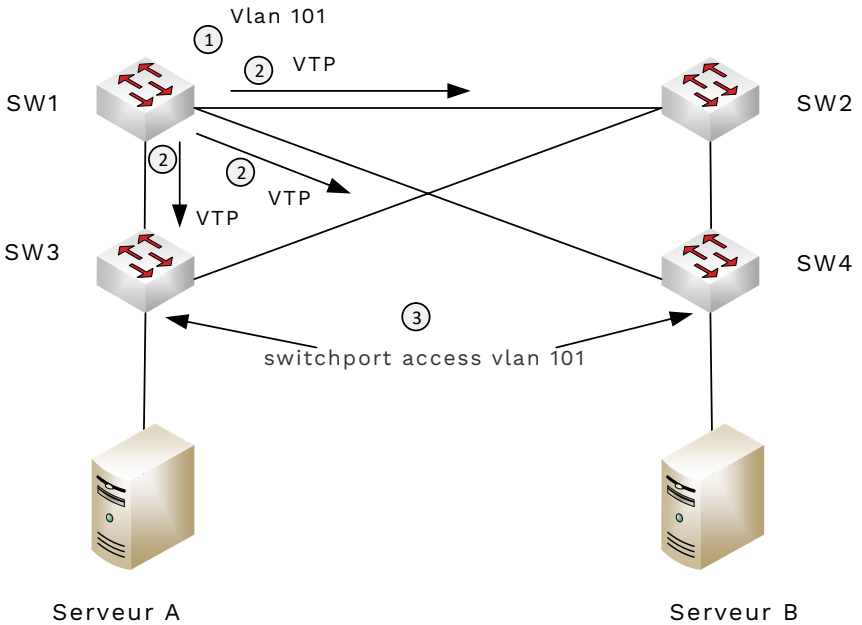
Commandes VTP
vtp domain NOM_DOMAINE
vtp mode server
vtp password MOT_DE_PASSE

COMMENT ÉVITER LES PIÈGES AVEC VTP

- Si VTP n'est pas utilisé, réglez le mode VTP sur transparent **(vtp mode transparent)** ou désactivez le VTP **(vtp mode disable)**
- Si vous utilisez le mode serveur ou client, définissez un mot de passe. Cela empêchera un nouveau commutateur de provoquer des problèmes avec VTP
- Si vous utilisez VTP dans une maquette, utilisez un nom de domaine différent de celui de la production
- Désactivez les interfaces Trunk indésirables avec la commande **switchport mode access** et **switchport nonegociate** pour empêcher les attaques basées sur VTP.

OÙ SONT STOCKÉES LES INFORMATIONS VTP?

Commande de configuration	Localisation	Comment affichert
vtp domain	vlan.dat	show vtp status
vtp mode	vlan.dat	show vtp status
vtp password	vlan.dat	show vtp password
vtp pruning	vlan.dat	show vtp status
vlan **vlan-id**	vlan.dat	show vlan [brief]
name vlan-name	vlan.dat	show vlan [brief]
[no] shutdown vlan vlan-id	running-config	show vlan [brief]
switchport access vlan **vlan-id**	running-config	show running-config, show interfaces switchport
switchport access voice vlan **vlan-id**	running-config	show running-config, show interfaces switchport



Distribution de VTP sur un réseau commuté

1. Vlan 101 est défini sur SW1 qui est la source VTP
2. VTP distribue le Vlan 101 aux 3 autres commutateurs
3. Pour les ports du serveur, les ports du commutateur sont définis comme des ports d'accès pour Vlan 101 (switch mode access)

DÉPANNAGE VTP

1 Confirmer le mode VTP sur les commutateurs, changer les hostname au besoin et la topologie

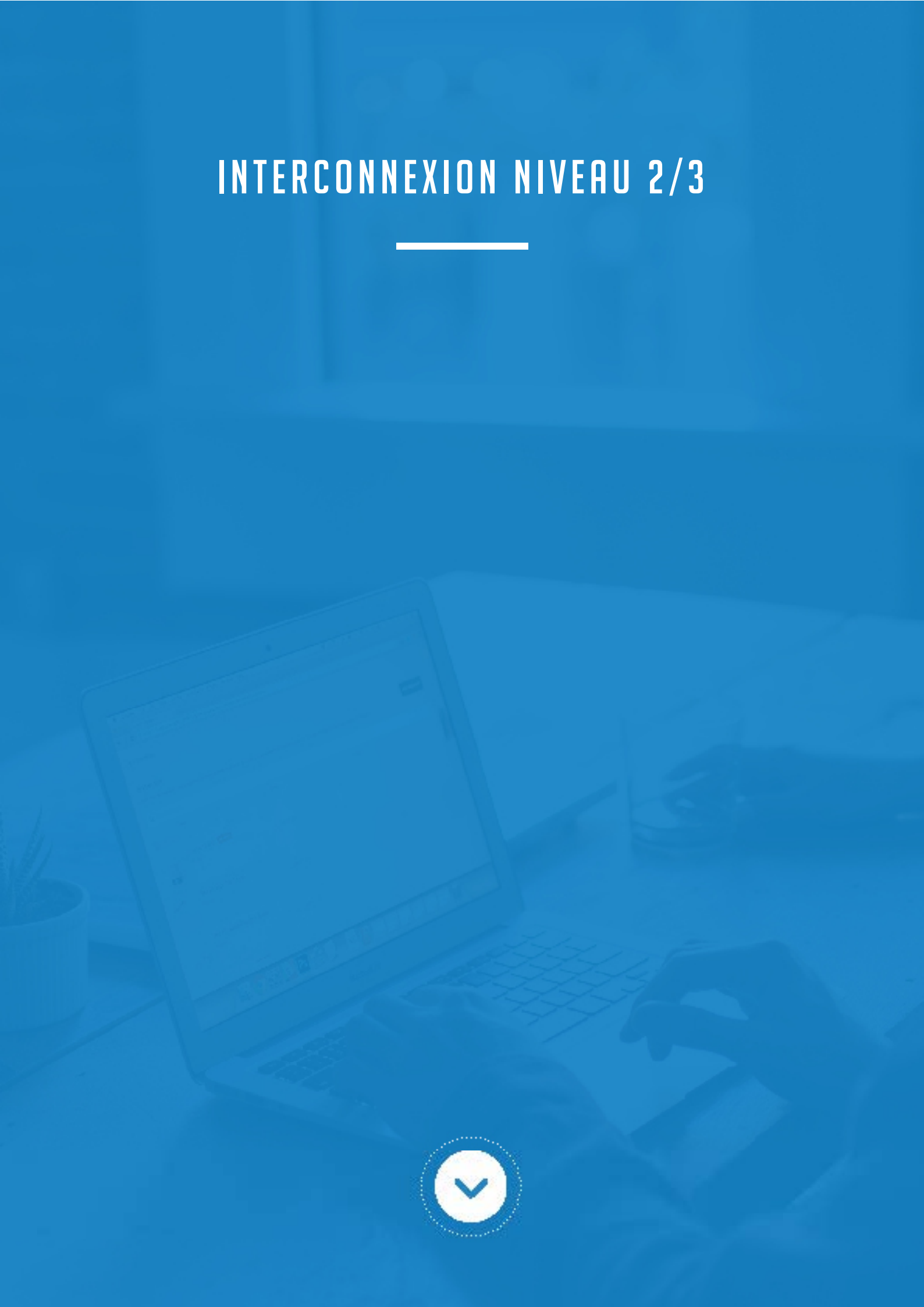
2 Trouvez deux commutateurs qui sont client et serveur avec différentes bases de données via la commande **show vlan.**

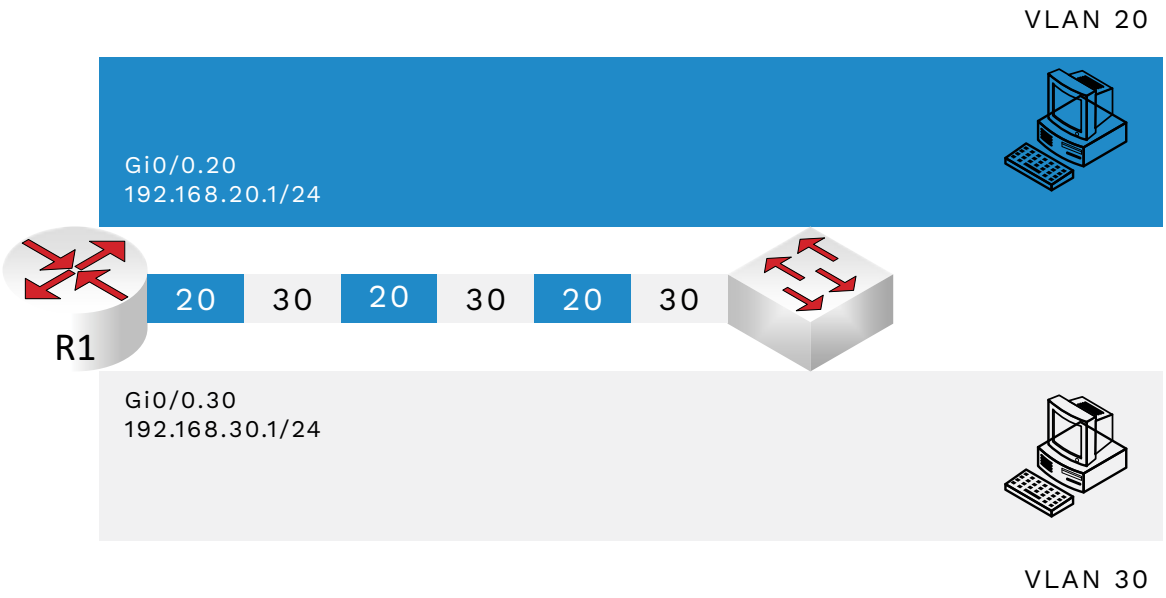
3 Sur les commutateurs voisins où les bases de données diffèrent, vérifiez les points
suivants:

- Assurez-vous qu'il existe au moins un Trunk entre les commutateurs.
- Le nom de domaine VTP sensible à la casse doit correspondre **(show vtp status).**
- Le mot de passe VTP sensible à la casse doit correspondre **(show vtp status).**
- Le hash MD5 doit être le même **(show vtp status).**

4 Si une paire de commutateurs est identifiée à l'étape 3, vérifiez les configurations ou reconfigurez au besoin.

INTERCONNEXION NIVEAU 2/3





DÉPANNAGE DU ROUTEUR SUR UN STICK (ROAS - ROUTER ON A STICK)

1. Est-ce que chaque réseau de VLAN a une sous-interface avec la commande d'encapsulation dot1q définie?

2. Est-ce que ces VLAN existent dans le commutateur connecté et sont-ils dans la liste autorisée? Sont-ils VTP-élagés ou bloqués par STP?

3. La sous-interface de chaque routeur a-t-elle une adresse IP et un masque de réseau qui correspondent à la configuration souhaitée pour chaque VLAN?

4. Si le VLAN natif est utilisé, est-il défini sur l'interface physique ou sur une sous-interface?

5. Les VLAN natifs sur le routeur et le commutateur sont-ils identiques?

6. Les interfaces du routeur ou du commutateur sont-elles arrêtées par la commande **shutdown?**

ÉTAPES DE CONFIGURATION POUR LE ROUTEUR R1 AVEC DES SOUS-INTERFACES

1. Créez une sous-interface pour chaque VLAN en utilisant la commande **interface TYPE NUMBER.SUBINTERFACE** pour définir la sous-interface.

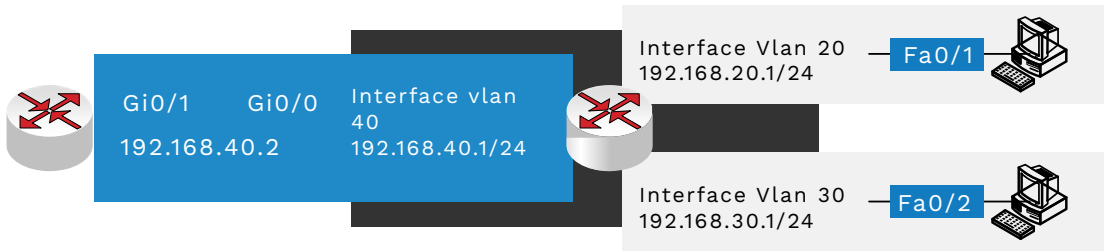
2. Définissez l'encapsulation VLAN et dot1q avec la commande **encapsulation dot1q VLAN**

3. Définissez l'adresse IP en utilisant la commande **ip address ADRESSE MASQUE**

CONFIGURATION DE L'INTERFACE DU ROUTEUR POUR LE VLAN NATIF

1. Définissez une adresse IP et un masque sur une interface physique. Le routeur supposera que c'est le vlan natif (ou non tagué)

2. Définissez l'adresse IP sur une sous-interface, puis utilisez la commande **encapsulation dot1q VLAN native** pour indiquer au routeur que cette sous-interface utilise un trafic non marqué



Switch niveau 3 (en gris)

CONFIGURATION DE ROUTAGE DE COUCHE 3 SUR UN COMMUTATEUR

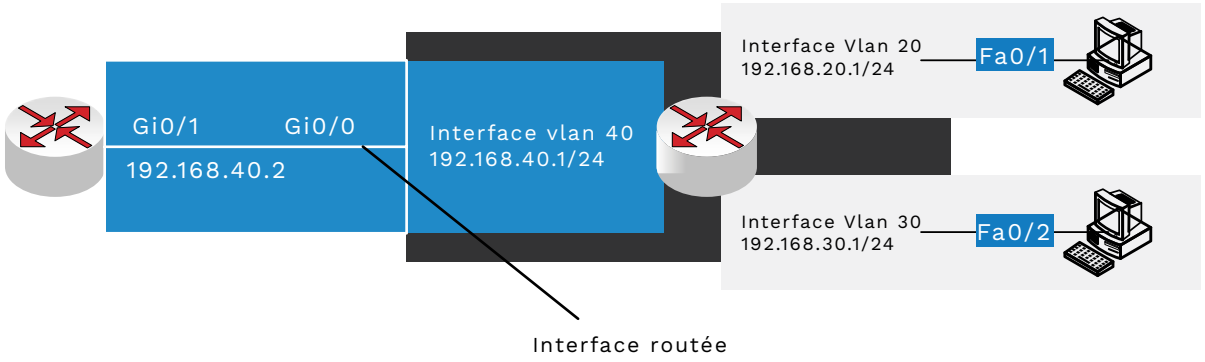
1 Activez le routage IP avec la commande globale **sdm prefer lanbase-routing** et rechargez le commutateur avec la commande **reload**. Ensuite, validez le routage IPv4 avec la commande **show ip route**.

2 Configurez chaque interface SVI comme suit:

a. Configurer la commande **interface vlan VLAN_ID** pour le VLAN
b. Définissez l'adresse IP avec la commande **ip address ADRESSE MASQUE**
c. Activez l'interface avec la commande **no shutdown**

DÉPANNAGE DU ROUTAGE AVEC LES SVI

- Le VLAN doit être défini sur le commutateur localement ou appris via VTP.
- Le commutateur doit avoir au moins une interface à l'état up / up sur le VLAN
  - -Une interface d'accès sur le VLAN doit être up / up
  - -Une interface réseau avec le VLAN autorisé et non bloqué
- Le VLAN lui-même doit être activé (no shutdown)
- L'interface VLAN doit être activée (no shutdown).



Switch niveau 3 (en gris)

Ici, l'interface routée n'est pas définie comme un switchport (Niveau 2, mais comme une interface de routeur (niveau 3) en utilisant la commande: no switchport

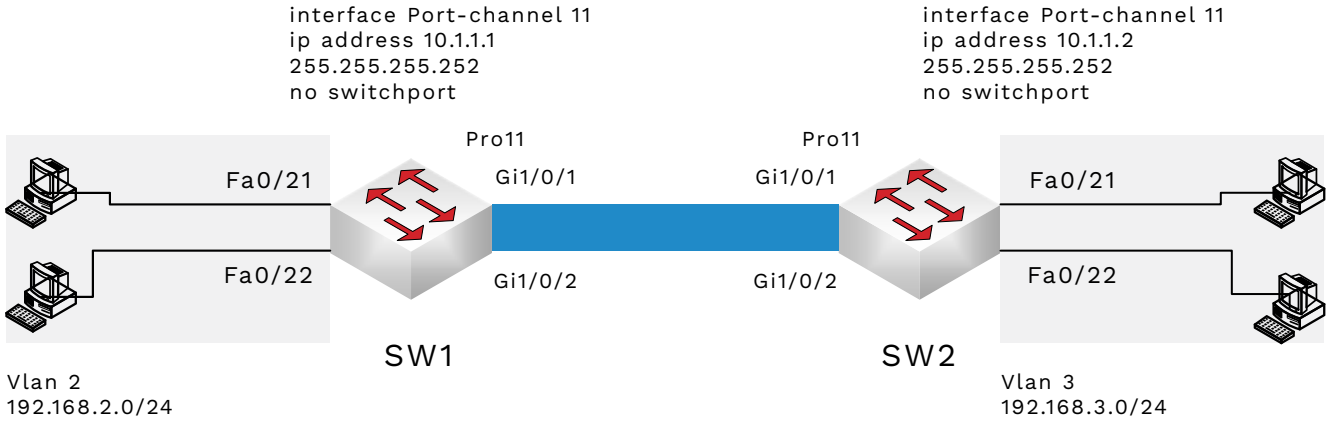
COMMANDES POUR VALIDER LES INTERFACES ROUTÉES SUR UN COMMUTATEUR

show interface: affiche l'adresse IP des interfaces
show interfaces status: sous la rubrique VLAN, l'interface routée indiquera Routed
show ip route: le port routé est répertorié dans les itinéraires de la table de routage
show interfaces TYPE NUMBER switchport: si un port routé, il n y a pas d'informations de couche 2 qui sera affichée

MISE EN OEUVRE DES LIENS LAYER-3 ETHERCHANNEL

- Configurez les interfaces:
  1. Utilisez la commande **channel-group NUMERO** pour ajouter le port à l'Etherchannel
  2. Utilisez la commande **no switchport** pour faire de l'interface un port routé

- Configurez les interfaces Port-channel:
  1. Émettre la commande **interface port-channel NUMERO** pour configurer
  2. Utilisez la commande **no switchport** pour rendre le Port-channel routé
  3. Définissez l'adresse IP avec la commande **ip address ADRESSE MASQUE**

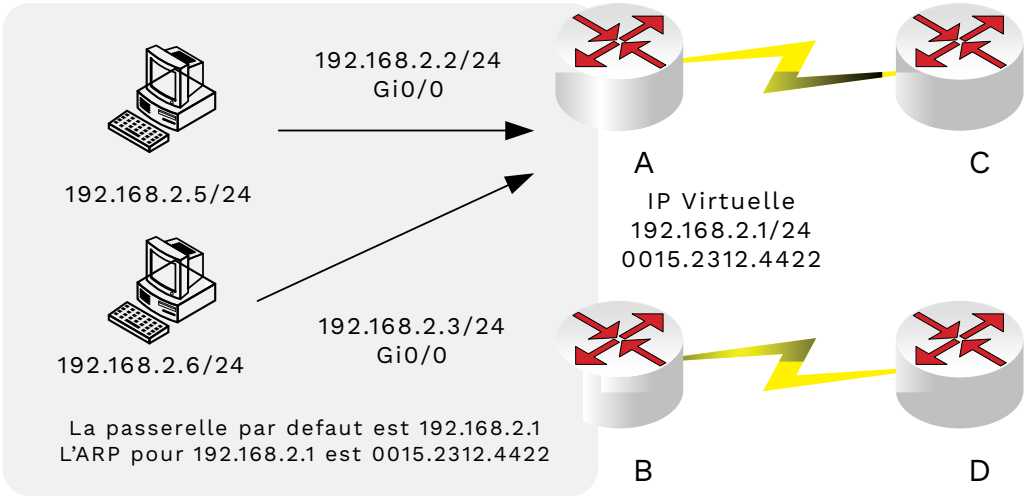


DÉPANNAGE DES ETHERCHANNELS DE COUCHE 3

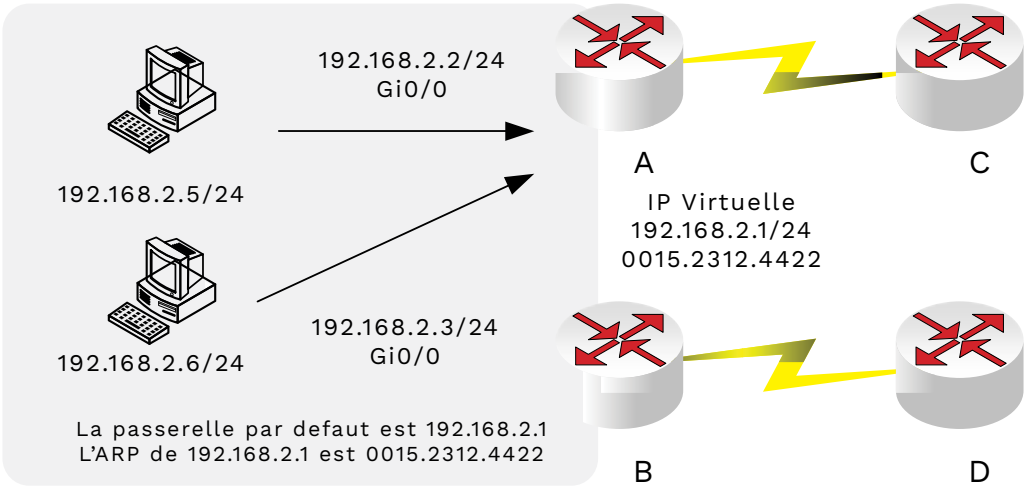
- no switchport: les interfaces Etherchannel doivent être configurées avec la commande **no switchport.** L'Etherchannel ne s'activera pas si une ou les deux interfaces Etherchannel sont configurées en mode switchport.

- speed: Les deux interfaces doivent être configurées pour la même vitesse.

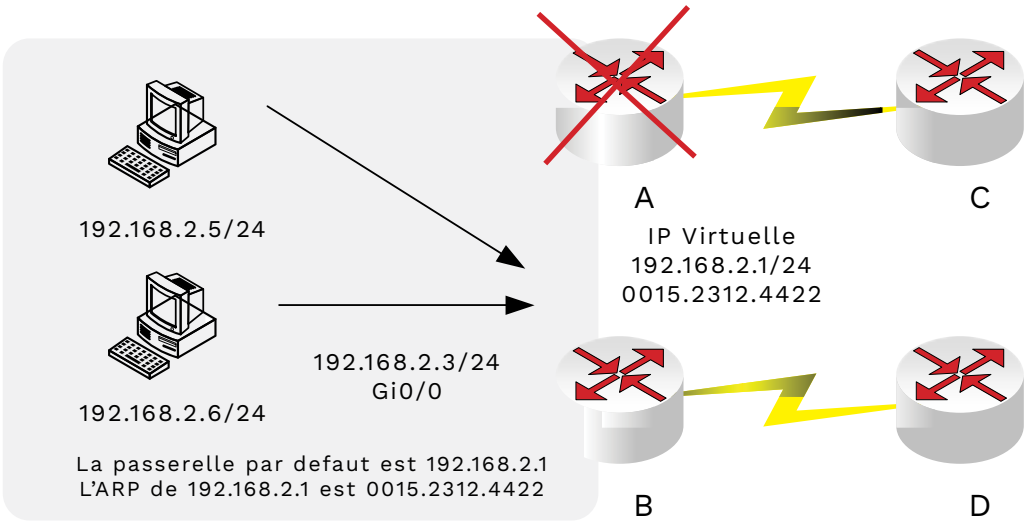
- duplex: Les deux interfaces doivent être configurées pour le même paramètre duplex.



Exemple de HSRP
Ici, le routeur assume l'adresse MAC 0015.2312.4422



Restauration du routeur A



L'échec du routeur A signifie que le routeur B prend le relais.
Le routeur B prend l'adresse MAC 0015.2312.4422
Remarque: les ordinateurs portables n'ont pas besoin de renvoyer une requête ARP pour la passerelle par défaut

CONFIGURATION DU HSRP

Configurer HSRP sur le routeur A:

```
A(config)# interface Gi0/0
A(config-if)# ip address 192.168.2.2 255.255.255.0
A(config-if)# standby 1 ip 192.168.2.1
A(config-if)# standby 1 priority 110
A(config-if)# standby 1 name HSRP-gw
```

Configurer HSRP sur le routeur B:

```
B(config)# interface Gi0/0
B(config-if)# ip address 192.168.2.3 255.255.255.0
B(config-if)# standby 1 ip 192.168.2.1
B(config-if)# standby 1 priority 100
B(config-if)# standby 1 name HSRP-gw
```

INFORMATION SUR LA COMMANDE SHOW STANDBY BRIEF

Interface: interface du routeur configurée en HSRP

Grp: numéro de groupe HSRP

Pri: priorité HSRP sur le routeur local

State: état HSRP sur le routeur

Active: adresse IP de l'interface HSRP active (marquée local si l'interface HSRP active est sur le routeur)

Standby: adresse IP de l'interface HSRP en attente (marquée local si l'interface HSRP en attente est sur le routeur)Virtual IP: adresse IP virtuelle pour ce groupe HSRPA

A# **show standby brief**

InterfaceG	rp	Pri	P	State	Active	StandbyV	irtual IP
Gi0/01		110		Active	local	192.168.2.3	192.168.2.1

B# **show standby brief**

InterfaceG	rp	Pri	P	State	Active	StandbyV	irtual IP
Gi0/01		110S		tandby	192.168.2.2	192.168.2.3	192.168.2.1

PROCESSUS GLBP

Étape 1 Host 192.168.2.100 envoie un ARP pour localiser une adresse physique pour 172.16.32.12

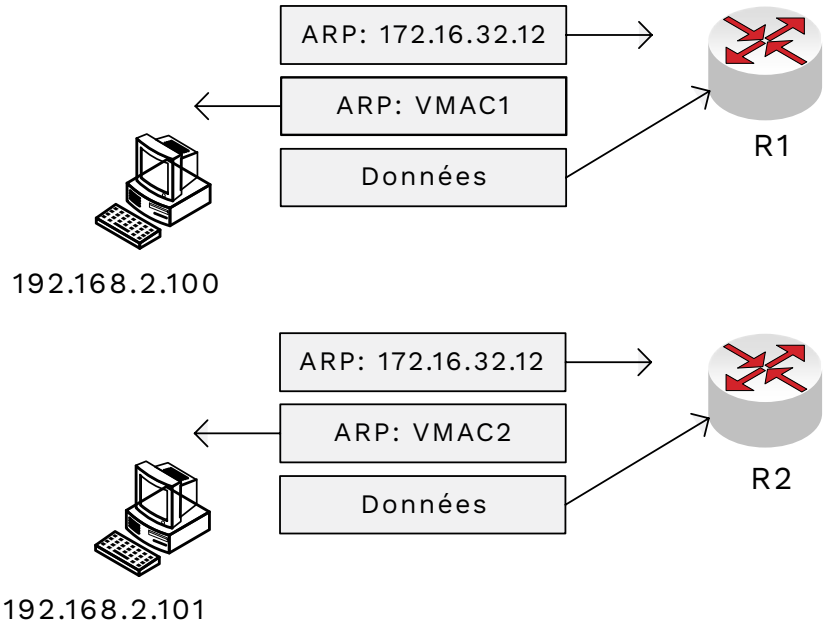
Étape 2 le routeur R1 envoie VMAC1 comme adresse physique pour 172.16.32.12

Étape 3 l'hôte envoie des données à R1.

Étape 4 Host 192.168.2.101 envoie un ARP pour localiser une adresse physique pour 172.16.32.12

Étape 5 le routeur R2 envoie VMAC2 comme adresse physique pour 172.16.32.12

Étape 6 l'hôte envoie des données à R2.



FIRST HOP ROUTING PROTOCOL (FHRP)

Tous les protocoles de routage First Hop (FHRP) doivent permettre à deux routeurs d'apparaître comme un seul routeur. Pour que le FHRP fonctionne, les cinq concepts suivants doivent être présents:

1. Tous les hôtes ont le même réglage de la passerelle par défaut du routeur qui ne doit pas changer.
2. Les passerelles par défaut (routeur HSRP) partagent une adresse IP virtuelle dans le même sous-réseau.
3. Les hôtes utilisent l'adresse IP virtuelle partagée comme passerelle par défaut.
4. Les deux routeurs échangent des messages pour s'assurer que chaque voisin fonctionne.
5. Si le routeur actif échoue, FHRP choisi un routeur voisin pour la reprise du service de la passerelle par défaut.

Forward	Signification
-	Ce routeur agit comme la passerelle virtuelle active (AVG)
1	Ce routeur est un transitaire #1 GLBP
2	Ce routeur est un transitaire #2 GLBP

Significations de Fwd dans la commande **show glbp brief**

Description de la ligne	Forward	État R1	État R1
Active virtual gateway	-	Actif	Actif
Forwarder #1	1	Ecoute	Ecoute
Forwarder #2	2	Actif	Actif

Significations de **Local State** dans la commande **show glbp brief**

Nom du protocole	Abréviation	Redondance	Équilibrage de charge	Origine
Hot Standby Router Protocol	HSRP	Actif / veille	Par sous-réseau	Cisco
Virtual Router Redundancy Protocol	VRRP	Actif / veille	Par sous-réseau	IETF (RFC 5798
Gateway Load Balancing Protocol	GLBP	Actif / veille	Par Host	Cisco

Options des protocoles FHRP

CONFIGURATION DU GLBP

Configurer HSRP sur le routeur A:

```
A(config)# interface Gi0/0
A(config-if)# ip address 192.168.2.2 255.255.255.0
A(config-if)# glbp 1 ip 192.168.2.1
A(config-if)# glbp 1 priority 110
A(config-if)# glbp 1 name GLBP-gw
```

Configurer HSRP sur le routeur B:

```
B(config)# interface Gi0/0
B(config-if)# ip address 192.168.2.3 255.255.255.0
B(config-if)# glbp 1 ip 192.168.2.1
B(config-if)# glbp 1 priority 100
B(config-if)# glbp 1 name GLBP-gw
```

A# **show glbp brief**

Interface/Grp	Forward	Pri	State	Address	Active	Standby
Gi0/01	-	110	Actif	192.168.2.1	local	192.168.2.2
Gi0/01	1	-é	couter	0023.b500.0001	192.168.2.2	-
Gi0/01	2	-	Actif	0023.b500.0002	local	

SCÉNARIOS DE MAUVAISE CONFIGURATION DE HSRP ET RÉSULTATS ESCOMPTÉS

Numéro de réference	Scenario	Les routeurs deviennent actifs?	L'adresse en double est-elle détectée?	Modifications VIP en fonction du routeur actif?
1	Incompatibilité de la version HSRP	oui	oui	N/A
2	Numéro de groupe HSRP incompatible	oui	oui	N/A
3	ACL bloque les paquets HSRP	oui	non	N/A
4	Les routeurs Avec différents VIP	non	N/A	oui

HSRPV1 VERSUS HSRPV2

Caractéristique	Version 1	Version 2
Support IPv6	Non	oui
Plus petite unité pour Hello Timer	Seconde	Milliseconde
Gamme de numéros de groupe	0 - 255	0 - 4095
Adresse MAC (xx ou xxx est le numéro de groupe hexadécimal)	0000.0C07. ACxx	0000.0C9F. Fxxx
Adresse de multicast utilisée	224.0.0.2	224.0.0.102
Le protocole possède-t-il un identifiant unique pour chaque routeur?	non	oui

PARAMÈTRES QUI DOIVENT OBLIGATOIREMENT CORRESPONDRE À HSRP POUR FONCTIONNER CORRECTEMENT

- Les routeurs doivent être configurés avec la même version HSRP **(version standby {1 | 2})**
- Les routeurs doivent être configurés avec le même numéro de groupe HSRP **(standby NUMBER...).**
- Les routeurs doivent configurer la même adresse IP virtuelle **(standby NUMBER ip ADDRESSE).**
- L'adresse IP virtuelle doit être:

  (a) dans le même sous-réseau que l'adresse IP de l'interface et
  (b) non utilisée par un autre périphérique du sous-réseau (y compris les autres routeurs HSRP)

- Dans le réseau de niveau 2, les interfaces sur les routeurs ou les commutateurs de couche 3 doit être dans le même VLAN.
- Aucune ACL ne doit filtrer les messages HSRP entre les deux routeurs. (HSRP utilise UDP, port 1985, la version 1 envoie à l'adresse de multidiffusion 224.0.0.2, tandis que la version 2 envoie au 224.0.0.102.)

QOS - QUALITÉ DE SERVICE

La qualité de service classe et gère le trafic sur quatre paramètres:
- Bande passante
- délai
- Gigue (variation du délai)
- Perte de paquet

1. La bande passante est la capacité de transmission disponible pour un type de trafic donné (10Mbps, 100Mbps, 1Gbps).

2. Le retard est le temps qu'une transmission de paquets peut mettre avant que le trafic ne devienne inutilisable

3. La gigue est le délai entre les paquets. La voix sur IP nécessite une gigue à valeur constante

4 La perte est la quantité de paquets qui ne sont pas reçus sans pour autant trop altérer la transmission.

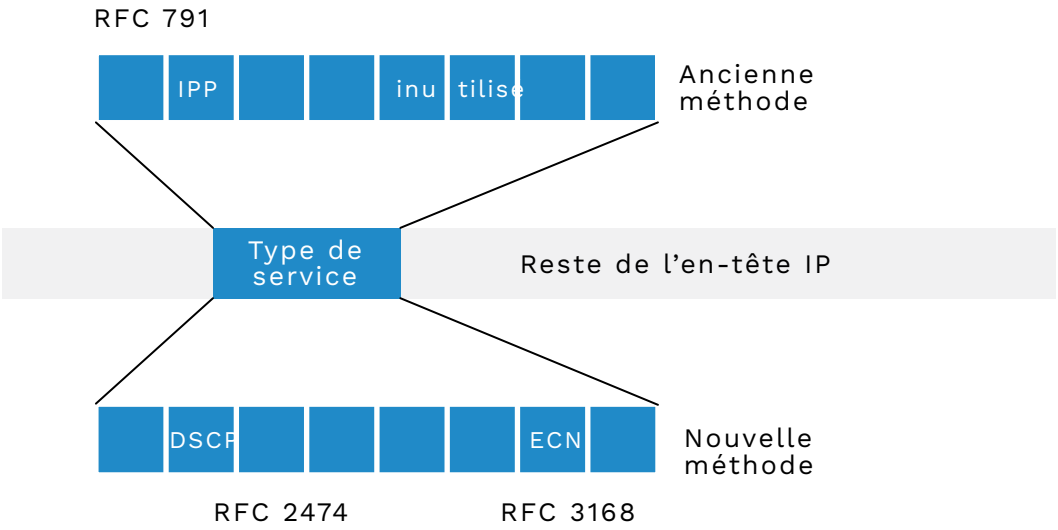
PARAMÈTRES QOS VOCAUX

la voix sur IP nécessite les paramètres de trafic suivants:

- délai à sens unique de 150 ms ou moins
- gigue à 30 ms ou moins
- perte de paquet de 1% ou moins

la vidéo nécessite les paramètres de trafic suivants:

- Bande passante comprise entre 384 Kbps et 20 Mbps ou plus
- délai à sens unique de 300 à 400 ms
- gigue de 30 à 50 ms
- perte inférieure à 0,1%



Différences entre la priorité IP et DSCP pour le marquage des paquets

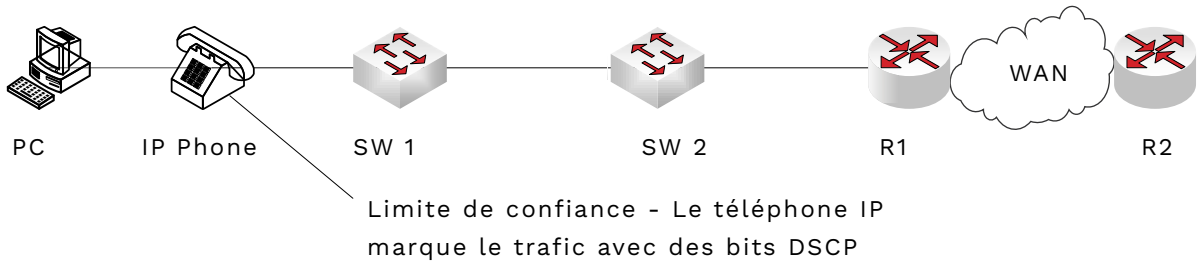
Marquage de l'en-tête Ethernet avec classe de service

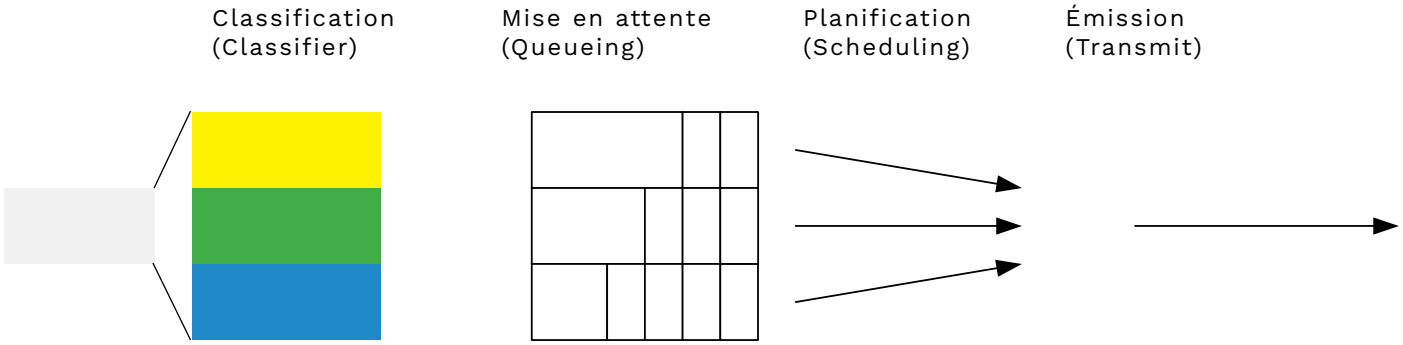
Ethernet		802.1Q			Type	Données	Fin trame

3 bits pour la classe de service (COS)

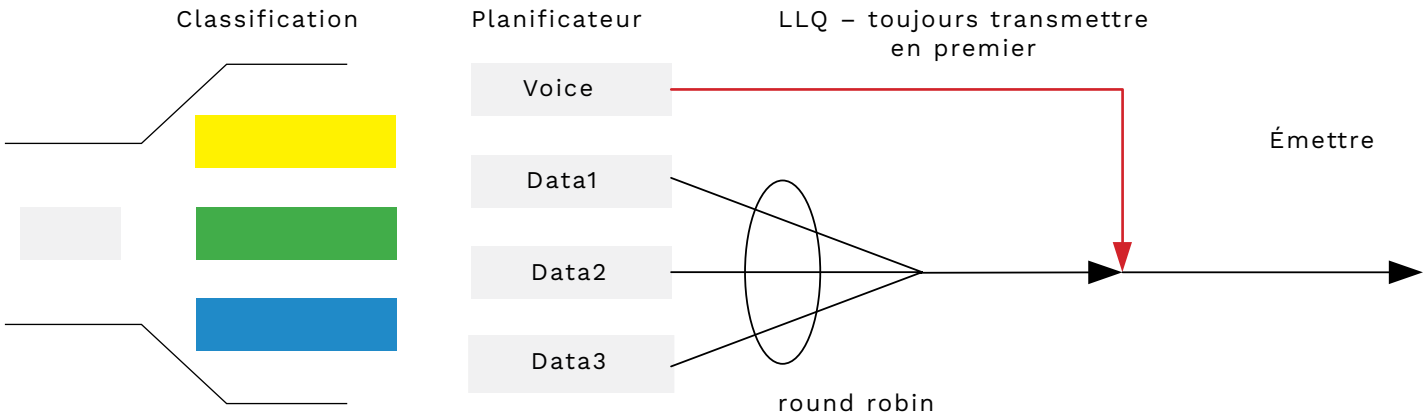
MARQUAGE QOS

le réglage des bits DSCP dans l'en-tête du paquet IP doit être effectué à la source si possible. Cependant, une limite de confiance peut être utilisée. La limite de confiance est l'endroit où le premier périphérique qui peut marquer des bits DSCP applique la QoS appropriée au paquet avant de quitter l'appareil.



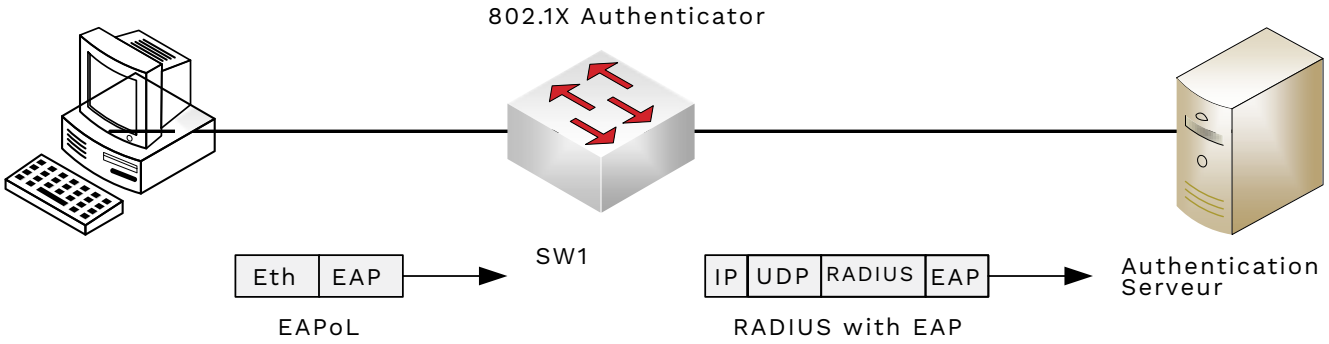


La classification des paquets et la mise en file d'attente pour la gestion de la congestion



LLQ planifie toujours le paquet de voix suivant

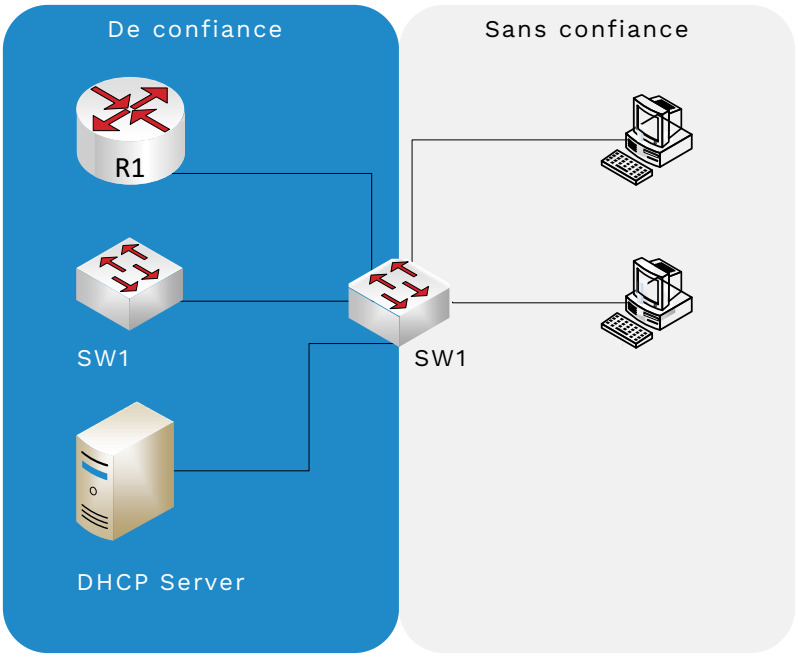
Flux EAP et RADIUS avec
802.1 x



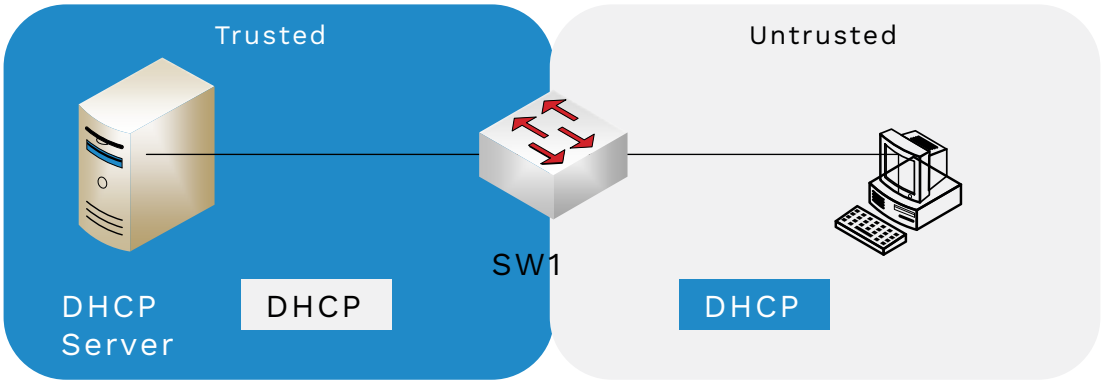
COMPARAISONS ENTRE TACACS+ ET RADIUS

Caractéristiques	TACACS+	RADIUS
Le plus souvent utilisé pour	équipements réseau	Utilisateurs
Protocole de transport	TCP	UDP
Numéros de port d'authentification	49	1645, 1812
Le protocole crypte le mot de passe	Oui	Oui
Le protocole crypte l'ensemble du paquet	Oui	Non
Autorisation pour chaque utilisateur à un sous-ensemble de commandes CLI	Oui	Non
Défini par	Cisco	RFC 2865

PRINCIPES DE BASE DU SNOOPING DHCP - SUPPOSONS QUE LES CLIENTS NE SONT PAS FIABLES



RÉSUMÉ DU SNOOPING DHCP



DHCP Server: Toutes les requêtes sont acceptée

DHCP Server Message: Rejeté!
DHCP client: vérification de la table DHCP

RESUME DES FONCTIONALITES DU DHCP SNOOPING

- Ports de confiance (Trusted port) - autorise les messages DHCP entrants.
- Ports **non-fiables**, messages du serveur (Untrusted port) - ignore tous les messages du serveur entrant (arrête les serveurs DHCP illégitimes).
- Ports non-fiables, messages clients (Untrusted port) – L base de données (binding table) est vérifiée et s'il y a conflit, le message est supprimée. Dans le cas contraire, le message client est validé et la Base de données mise à jour.
- Limitation du débit (Rate limiting) - un paramètre facultatif qui limite le nombre de requêtes clientes DHCP par seconde définie par port.

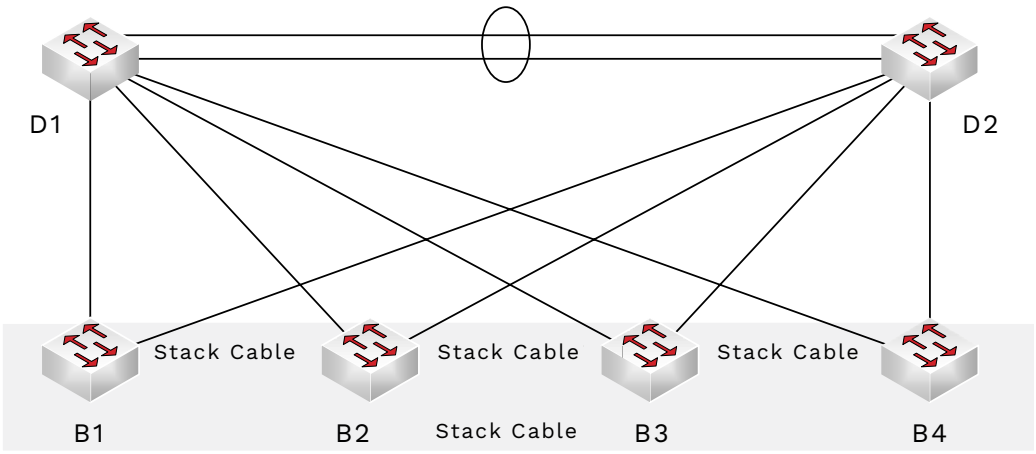
AVANTAGES D'EMPILEMENT DE COMMUTATEURS (STACK SWITCH)

- La pile de commutateurs possède une adresse IP de gestion unique.
- Seule cette adresse est utilisée pour se connecter à la pile via Telnet ou SSH au lieu de se connecter aux commutateurs individuellement.
- Un seul fichier de configuration contient les configurations pour tous les commutateurs dans la pile.
- STP, CDP et VTP fonctionneront sur un seul commutateur au lieu de tourner sur plusieurs commutateurs.
- Une seule table d'adresses MAC contenant les adresses MAC acquises par tous les commutateurs dans la pile.

En bref, l'empilement de deux commutateurs ou plus se traduit par un commutateur virtuel couvrant les commutateurs physiques.

AVANTAGES DE L'UTILISATION DE L'AGRÉGATION DE LIENS SUR UNE PILE DE COMMUTATEURS

- Multichassis EtherChannel - Utilisation d'EtherChannel entre deux commutateurs physiques.
- Active / Standby Control Plane - Les deux commutateurs agissent comme un seul commutateur pour STP, CDP et VTP, EtherChannel, les protocoles de routage et ARP.
- Active / Active Data Plane - Utilisation de la puissance de transfert des deux cartes de superviseur pour transférer les trames. Les adresses MAC sont synchronisées entre les cartes de gestion (management card).
- Gestion de commutateur unique - Simplifie la gestion en exécutant le Telnet, SSH et SNMP sur le commutateur principal (primary switch), mais synchronisé avec les autres commutateurs (standby switchs).

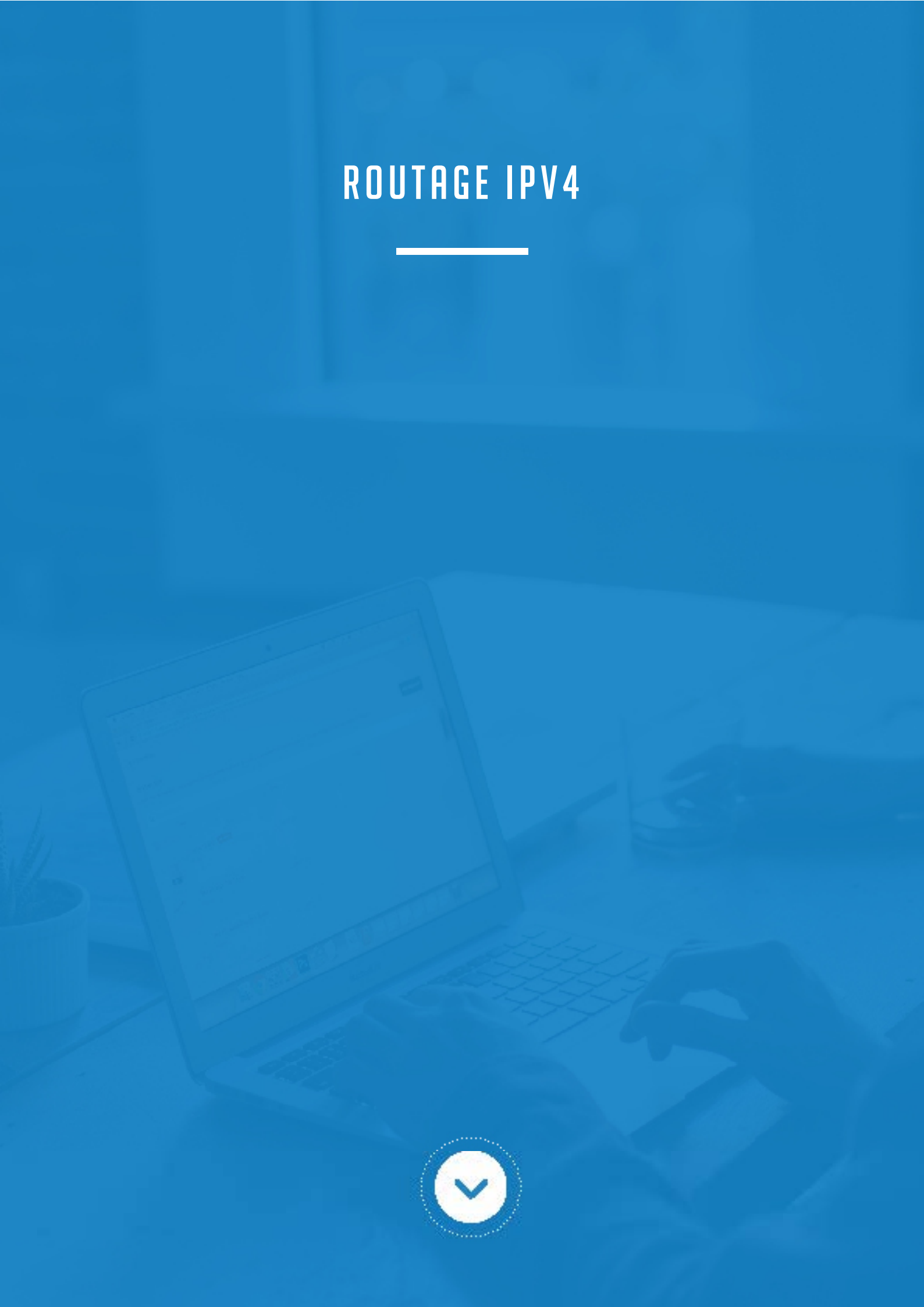


Pile de commutateurs (B1 - B4) dans le même rack physique

COMPARAISON ENTRE LES OPTIONS FLEXSTACK ET FLEXSTACK PLUS

Fonctionnalité	FlexStack	FlexStack Plus
Année de sortie	2010	2013
Série de commutateurs	2960-S, 2960-X	2960-X, 2960-XR
Vitesse du lien Stack	10 Gbps	12 Gbps
Nombre maximal de commutateurs dans une pile	4	8

ROUTAGE IPV4



FONCTIONS DU PROTOCOLE DE ROUTAGE

Ci-dessous les fonctions de base de tout protocole de routage:

1. Apprendre les itinéraires vers les réseaux des routeurs voisins
2. Annoncez les itinéraires aux routeurs voisins
3. Si plusieurs itinéraires existent pour une destination, utilise la métrique pour sélectionner le meilleur itinéraire vers cette destination
4. Si la topologie du réseau change pour une raison quelconque, annonce que certains itinéraires ont échoué et choisis un itinéraire alternatif (convergence deréseau)

DIFFÉRENCE ENTRE LES PROTOCOLES IGP ET EGP

Interior Gateway Protocol – protocole de routage conçu pour être utilisé dans le
même système autonome (AS – Autonomous system). Par exemple EIGRP et OSPF

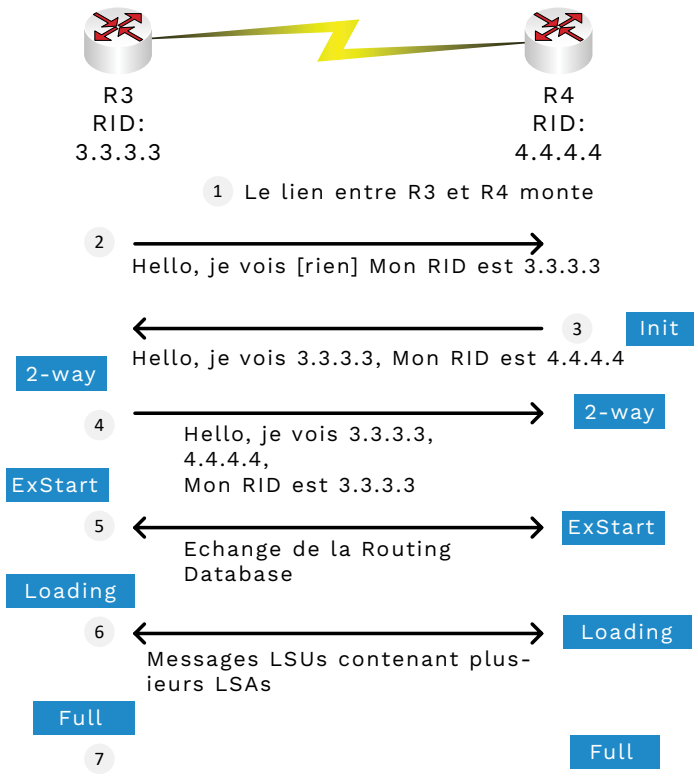
Exterior Gateway Protocol – protocole de routage conçu pour être utilisé entre différents systèmes autonomes. Le plus connu est BGP

ALGORITHMES DE ROUTAGE IGP - CI-DESSOUS LES DIFFÉRENTS TYPES D'IGP

- Distance Vector - Vecteur de distance (RIP)
- Link State - État du lien (OSPF)
- Hybrid - Hybride (EIGRP)

MÉTRIQUES IGP

IGP	Métrique	FlexStack Plus
RIPv2	Hop Count	Nombre de routeurs entre le routeur et un sous-réseau
OSPF	Cost	Somme de tous les coûts d'interface pour tous les liens d'une route (avec le coût basé sur la bande passante)
EIGRP	Composé de bandwidth et delay	Calculé en fonction du lien le plus lent de l'itinéraire et du retard associé à chaque interface



Etat des voisins (Neighbor) OSPF

ÉTATS VOISINS D'OSPF

1. La couche physique monte.
2. Bonjour, les paquets sont échangés avec les identifiants du routeur.
3. Le processus d'initialisation commence quand un routeur reconnaît l'autre routeur.
4. 2-way signifie que la communication bidirectionnelle est établie entre les deux routeurs.
5. ExStart est le point où les routeurs échangent des informations de routage.

6. Loading est l'état où les mises à jour de l'état des liens sont échangées et les calculs SPF sont effectués.

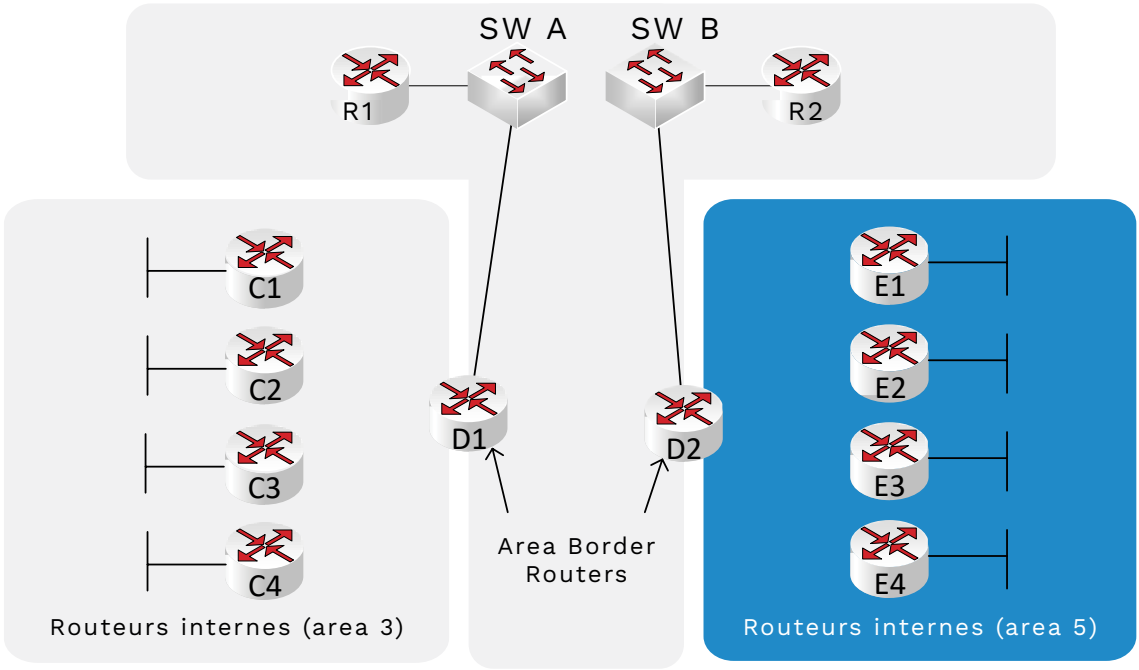
7. L'état complet signifie que les routes sont échangées entre les deux routeurs.

POINTS CLÉS SUR LES AIRES (AREA) OSPF

Alors que tous les routeurs dans un réseau peuvent être situés dans l'aire 0, il est judicieux de diviser le réseau en aire afin que le calcul SPF sur chaque routeur soit réduit. En outre, un changement d'interface sur un routeur affectera uniquement les routeurs dans l'aire en question.

Le choix des interfaces de routeur à placer dans une aire est effectué dans cescontraintes:

- Les interfaces dans le même sous-réseau doivent être dans la même aire.
- Les aires doivent être contiguës (fortement conseillé mais pas obligatoire).
- Un routeur peut avoir toutes ses interfaces dans une seule aire.
- Certains routeurs peuvent avoir des interfaces dans deux aires. Ce sont des routeurs de bordure d'aire (ABR – Area Border Router) où les inter faces se connectent à l'aire backbone (area 0) et d'autres interfaces se connectent à des aires non-nulles.
- Toutes les aires doivent se connecter à l'aire backbone (area 0) par un ou plusieurs ABR.



Réseau OSPF à trois aires avec D1 et D2 servant de routeurs de bordure d'aire (ABR)

LES TYPES DE LSA OSPFV2 VUS DANS UN RÉSEAU OSPF MULTI-AIRES

Nom LSA	Numéro LSA	Objectif principal	Contenu de LSA
Router	1	Description du routeur	RID, interfaces, adresses IP, états d'interface
Network	2	Réseau avec un DR (routage désigné)	Adresses pour DR et BDR, ID de sous-réseau et masque
Summary	3	Sous-réseau dans une autre aire	ID de sous-réseau et masque de sous-réseau, ABR RID annonçant l'itinéraire

Dans l'exemple precedent, les routeurs ABR D1 et D2 échangent et envoient des LSAs de synthèse pour annoncer des sous-réseaux dans d'autres aires. Tous les routeurs échangent des LSA de routeur avec les routeurs dans leur aire et les ABR selon les besoins.

COMPARAISON DES PROTOCOLES DE ROUTAGE IGP

Fonctionnalités	RIPv1	RIPv2	EIGRP	OSPF	IS-IS
Support de classe/masque de sous-réseau/VLSM	Non	Oui	Oui	Oui	Oui
Algorithme (DV, DV avancé, LS)	DV	DV	Adv DV	LS	LS
Supporte la synthèse manuelle	Non	Oui	Oui	Oui	Oui
Propriétaire de Cisco	Non	Non	Oui	Non	Non
Mises à jour de routage envoyés à une adresse de multidiffusion	Non	Oui	Oui	Oui	-
Convergence	Lent	Lent	Rapide	Rapide	Rapide

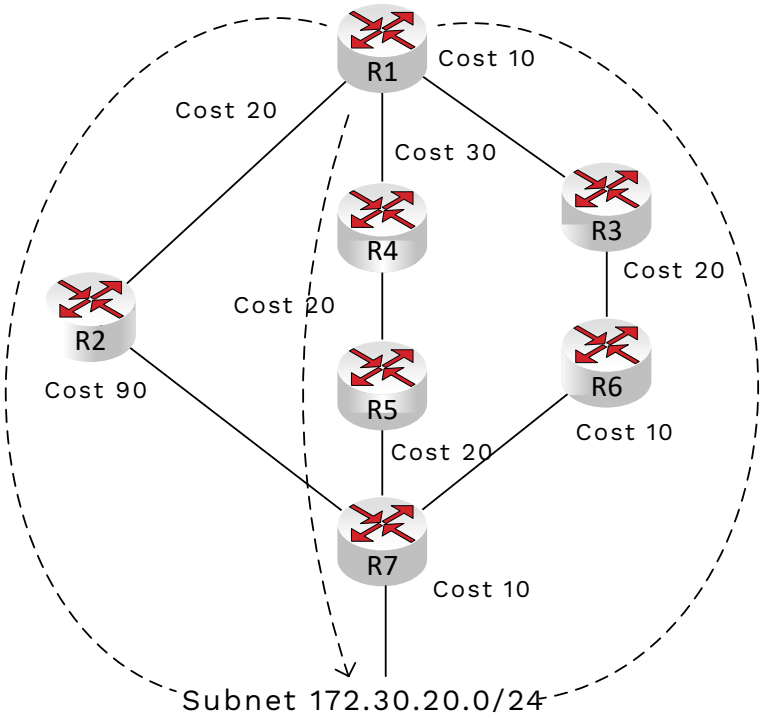
* EIGRP était propriétaire, mais le code a été publié par Cisco en 2013. D'autres fournisseurs peuvent implémenter EIGRP, mais Cisco maintient le protocole.

ÉTATS DE VOISINAGE OSPF STABLES

Définition de l'adjacence	État voisin	Description
Adjacent	2-way	Les routeurs sont des voisins basés sur les paquets hello. La relation de voisin est bonne
Fully adjacent	Full	Les deux routeurs ont échangé la base de données d état de lien

ALGORITHME DU PREMIER CHEMIN LE PLUS COURT (SPF - SHORTEST PATH FIRST)

OSPF calcule la métrique d'un réseau de destination comme la somme des coûts de l'interface OSPF pour toutes les interfaces le long du chemin pour atteindre ce réseau. En d'autres termes, l'itinéraire avec le coût total le plus bas est placé dans la table de routage.



Calculer les coûts des itinéraires possibles de R1 pour atteindre le sous-réseau 172.30.20.0/24

Via R2: Cost is 20 + 90 + 10 = 120
Via R4: Cost is 30 + 20 + 20 + 10 = 80
Via R3: Cost is 10 + 20 + 10 + 10 = 50

L'itinéraire le moins coûteux vers 172.30.20.0/24 est via R3, donc R1 ajoute une route vers le sous-réseau dans sa table de routage.

DÉFINITION DU ROUTER_ID OSPF (RID)

1. Si la commande router-id ID est configuré dans le mode **router ospf** alors la valeur est choisie pour être le **router-id**.

2. Si le RID OSPF n'est pas défini, on choisit l'adresse IP la plus élevée en tant que RID OSPF (172.1.1.1 plus élevé que 10.1.1.1).

3. Si RID ne peut pas être configuré via une adresse IP de bouclage (loopback), utilisez l'adresse IP la plus élevée sur une interface non loopback.

TERMINOLOGIE OSPF

Terme OSPF	Description
ABR – Area Border Router	Un routeur avec des interfaces dans l'aire backbone et une autre aire
Backbone router	Un routeur avec toutes ses interfaces dans l'aire 0
Internal router	Un routeur avec toutes ses interfaces dans une aire non nulle
Area	Un groupe de routeurs partageant l'information de route les uns avec les autres mais pas avec les routeurs dans d'autres aires
Backbone area	L'aire où toutes les autres aires OSPF doivent se connecter – également appelée aire 0
Intra-area route	Un itinéraire partagé entre les routeurs dans la même aire
Inter-area route	Un itinéraire vers un sous-réseau situé dans une autre aire en dehors de sa propre aire

AVANTAGES DE LA CONCEPTION D'AIRE OSPF

- Les mises à jour de base de données d'état de liaison d'aire plus petite (LSDB) nécessitent moins de cycles CPU et de mémoire.
- Les mises à jour de LSDB plus petites signifient des temps de convergence plus rapides.
- Les changements dans l'information d'état de lien restent dans une seule aire, ce qui signifie que moins de routeurs doivent exécuter le calcul de SPF basé sur un changement d'état de lien.
- Moins d'informations sont annoncées entre les aires qui nécessitent moins de bande passante pour partager les mises à jour de l'état des liens (LSAs).

COÛTS DE L'INTERFACE OSPF

Étant donné que le coût de l'interface dans OSPF ne peut pas être inférieur à 1, il est souhaitable de définir le coût en fonction de la bande passante d'interface supérieure.

Trois façons de définir le coût de l'interface OSPF:

- Définissez le coût explicitement via la sous-commande **ip ospf cost x** (x est entre 1 et 65 535).
- Modifiez la vitesse d'interface avec la commande **bandwidth speed** (en unités de Kbps).
- Modifiez la bande passante de référence avec la commande **auto-cost bandwidth REF** (en Mbps comme unité).

APERÇU DE LA CONFIGURATION OSPF V2

1) Entrez le mode de configuration du routeur OSPF en émettant la commande **router ospf process-id.**

2) Configurez l'ID du routeur par l'un des éléments suivants:
   a. Configurer manuellement l'ID du routeur via la commande **router-ID VALEUR**
   b. Configurer une adresse IP sur une interface de bouclage (loopback)
   c. S'appuyer sur OSPF pour choisir l'adresse IP la plus élevée sur le routeur

3) Configurez une ou plusieurs adresses IP pour placer des interfaces dans les zones OSPF via la commande **ip address VALEUR area AREA-ID.**

4) Vous pouvez également configurer certaines interfaces pour être passives via la souscommande d'interface **passive-interface TYPE NUMBER.**

Voici un **show running-config** d'un routeur configuré en OSPF:

```
interface Gigabit0/0
ip address 192.168.10.1 255.255.255.0
!
interface Serial0/0/0
ip address 192.168.100.2 255.255.255.252
!
router ospf 1
network 192.168.10.1 0.0.0.255 area 3
network 192.168.100.2 0.0.0.255 area 3
router-id 3.3.3.1
```

WILDCARD ET LEURS SIGNIFICATIONS

Wildcard 0.0.0.0 - Fait correspondre exactement tous les 4 octets.
Wildcard 0.0.0.255 - Ne correspond que les trois premiers octets et ignore le dernier octet.
Wildcard 0.0.255.255 - Ne correspond que les deux premiers octets et ignore les deux octets.
Wildcard 0.255.255.255 - Ne correspond que le premier octet et ignore les trois derniers octets.
Wildcard 255.255.255.255 - Ne rien comparer, cela correspond à tous les réseaux dans la commande réseau.

VALIDATION DES VOISINS OSPF

R3# **show ip ospf neighbor**

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           0   FULL/  -        00:00:33    10.1.13.1       Serial0/0/0
10.1.24.4         1   FULL/DR         00:00:35    10.1.3.130      GigabitEthernet0/0.342
10.1.24.4         1   FULL/DR         00:00:36    10.1.3.4        GigabitEthernet0/0.341
```

Remarque: Seuls les ports / segments Ethernet auront un routeur désigné. Les interfaces série n'élisent pas de DR ou de BDR sur la liaison série.

IDENTIFICATION DU ROUTEUR OSPF (RID)

- Si le router-id est configuré sous la commande **router ospf**, utilisez-le.
- Si le RID OSPF n'est pas défini, choisissez l'adresse IP numérotée la plus élevée en tant que RID OSPF.
- Si RID ne peut pas être configuré via une adresse IP de bouclage (loop-back), utilisez l'adresse IP numérique la plus élevée sur une interface non-loopback.

FONCTIONS DES INTERFACES PASSIVES OSPF

- Arrêter l'envoi d'OSPF Hellos sur l'interface
- Ignorer Hellos reçu sur l'interface
- Ne pas former les relations de voisinage sur l'interface en question

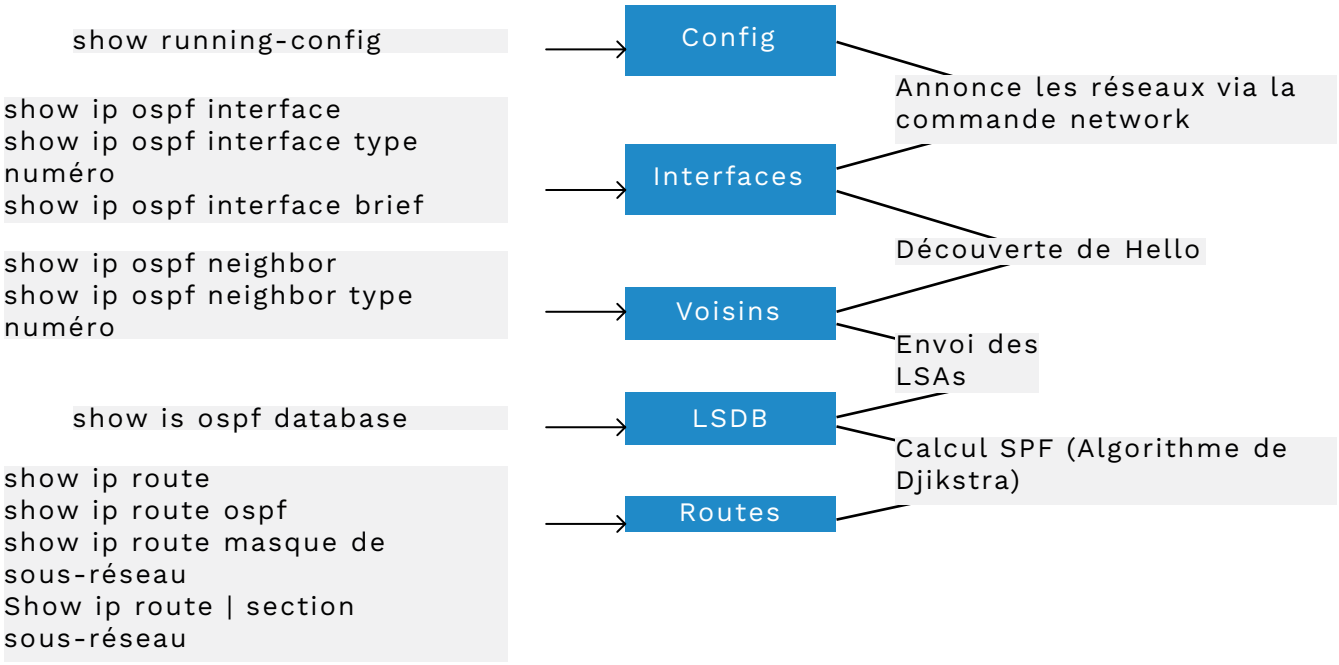
CONFIGURATION OSPF MULTI-AIRE (MULTIAREA)

```
interface GigabitEthernet0/0
ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/1
ip address 192.168.20.1 255.255.255.0
!
interface GigabitEthernet0/2
ip address 192.168.30.1 255.255.255.0
!
interface GigabitEthernet0/3
ip address 192.168.40.1 255.255.255.0
!
interface Serial0/0/0
ip address 192.168.100.2 255.255.255.252
!
router ospf 1
network 192.168.10.1 0.0.0.255 area 3
network 192.168.20.1 0.0.0.255 area 4
network 192.168.30.1 0.0.0.255 area 5
network 192.168.40.1 0.0.0.255 area 6
network 192.168.100.2 0.0.0.255 area 7
router-id 3.3.3.1
```

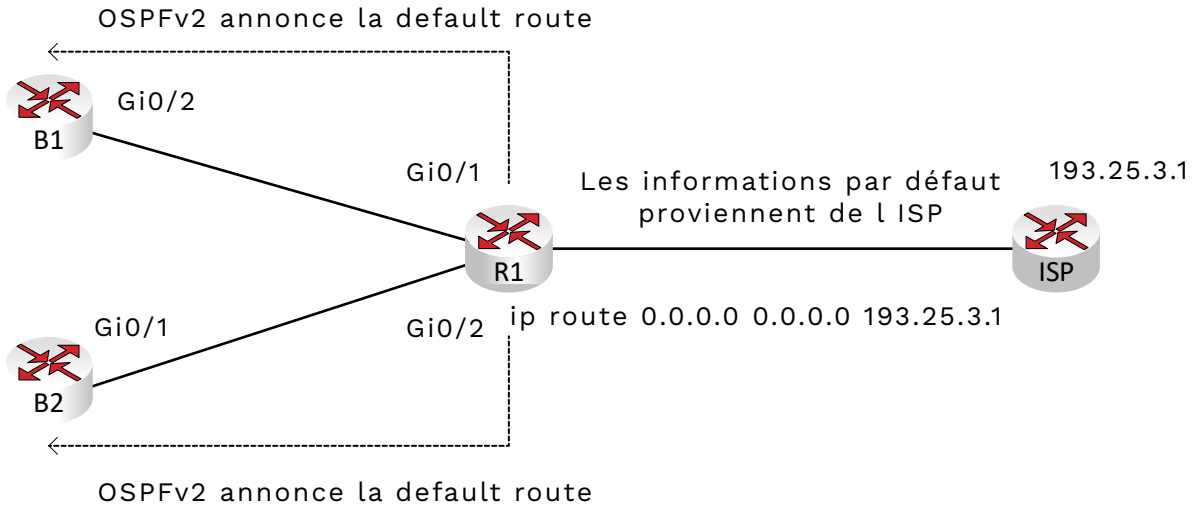
LISTER LES INTERFACES OSPF ACTIVES

```
R1# show ip ospf interface brief
Interface PID Area IP Address/Mask Cost State Nbrs F/C
Gi0/0     1   3    192.168.10.1/24  1    DR    0/0
Gi0/1     1   4    192.168.20.1/24  1    DR    0/0
Gi0/2     1   5    192.168.30.1/24  1    BDR   1/1
Gi0/3     1   6    192.168.40.1/24  1    BDR   1/1
Se0/0/0   1   7    192.168.100.s/24 64   P2P   1/1
```

COMMANDES DE VISUALISATION DU PROCESSUS OSPF ET LA PROGRESSION DE LA CONVERGENCE



UTILISATION D'OSPF POUR INONDER L'ITINÉRAIRE PAR DÉFAUT R1 (DEFAULT ROUTE) À TOUS LES ROUTEURS



COÛTS D'INTERFACE OSPF

Étant donné que le coût d'interface OSPF ne peut pas être inférieur à 1, il est souhaitable de fixer le coût en fonction de la bande passante la plus élevée.

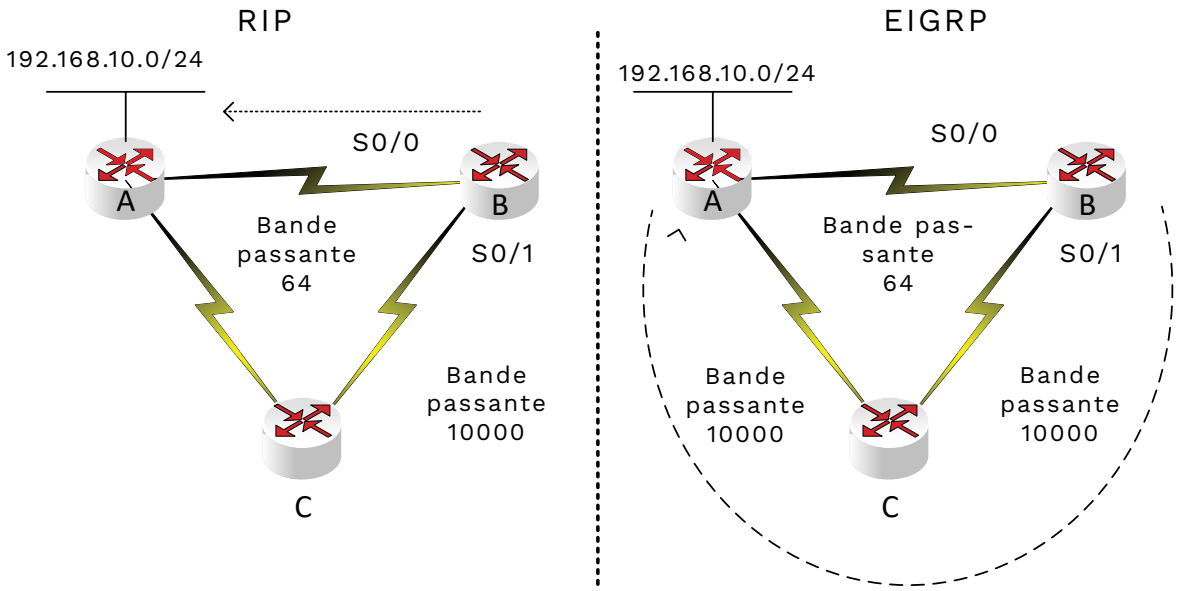
Trois façons de définir le coût d'interface OSPF

- Définir le coût explicitement via la sous-commande **ip ospf cost x** (x est compris entre 1 et 65535)
- Modifier de la vitesse d'interface avec la commande **bandwidth speed** en unités de Kbps
- Changer la bande passante de référence avec la commande **auto-cost reference-bandwidth ref-bw** avec Mbps comme unité.

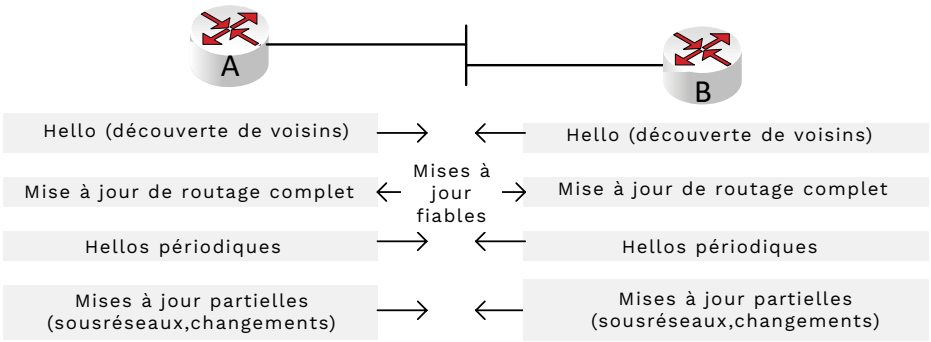
```
R2# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet Address 10.1.23.2/24, Area 23, Attached via Interface Enable
Process ID 1, Router ID 22.2.2.2, Network Type BROADCAST, Cost: 1
Topology-MTID Cost Disabled Shutdown Topology Name
       0        1    no        no        Base
Enabled by interface config, including secondary ip addresses
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 2. 2.2.2, Interface address 10.1.23.2
Backup Designated router (ID) 3.3.3.3, Interface address 10.1.23.3


! Showing only the part that differs on R3:
R3# show ip ospf interface g0/0
GigabitEthernet0/0 is up, line protocol is up
Internet Address 10.1.23.3/24, Area 23, Attached via Network Statement
```

POINTS CLÉS SUR EIGRP - ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL

- EIGRP utilise une combinaison de bande passante et de délai pour déterminer la meilleure route vers une destination.
- EIGRP converge très rapidement par rapport à d'autres protocoles de routage. S'il y a un changement dans la topologie, EIGRP trouvera des routes alternatives plus rapidement que d'autres protocoles de routage



Dans ces exemples, EIGRP prend la route avec la bande passante la plus importante



Différences entre les mises à jour EIGRP complètes et partielles

COMPARAISON DES CARACTÉRISTIQUES DES PROTOCOLES DE ROUTAGE

Caractéristique de protocole de routage	RIPv1	EIGRP	OSPF
Supporte VLSM	Oui	Oui	Oui
Vecteur de Distance-DV ou État de Liens-LS	DV	Hybride	Ls
Était propriétaire à Cisco?	Non	Oui	Non
La bande passante du lien affecte les métr-iques?	Non	Oui	Oui
Convergence	Lente	Rapide	Rapide
Configuration d'aires nécessaires?	Non	Non	Oui
Support de résumé de route manuel	Oui	Oui	Oui
Mises à jour de routage via multicast?	Oui	Oui	Oui

LES PROTOCOLES À VECTEUR DE DISTANCE ET L'APPRENTISSAGE DE ROUTE ONT DEUX RÈGLES

- Split Horizon - Ne pas publier les routes sur la même interface où elles ont été apprises
- Poison inverse - Si une route est inactive (down), la marquer comme inaccessible et envoyer la mise à jour

COMPARAISON DES CARACTÉRISTIQUES DES PROTOCOLES DE ROUTAGE INTÉRIEUR

Caractéristique de protocole de routage	RIPv2	EIGRP	OSPF
Métriques basée sur	Nombre de sauts	Bande passante et délai	Coût
Envoie périodiquement des mises à jour complètes	Oui	Non	Non
Messages Hello périodiquement	Non	Oui	Oui
Route poisoning pour les défaillances de la route	Oui	Oui	Oui
Limite les mises à jour via split horizon	Oui	Oui	Non
Adresse de mise à jour multicast	224.0.0.9	224.0.0.10	224.0.0.5, 224.0.0.6
Métrique infinie	16	232 – 1 or 256 – 1	224 – 1

PARAMÈTRES REQUIS POUR LES VOISINS EIGRP

- Si l'authentification est utilisée, les voisins doivent compléter l'authentification.
- Les numéros de Système Autonome (AS) doivent obligatoirement correspondre.
- Les adresses de l'interface source des paquets Hello doivent être dans le même sous-réseau que l'adresse IP et le masque de l'interface qui a reçu ce Hello.

SÉLECTION DE ROUTE EIGRP

EIGRP utilise deux métriques pour déterminer la route:

Distance Acceptable (FD - Feasible Distance): métrique calculée sur le routeur local pour trouver la meilleure route vers un sous-réseau particulier.

Distance Relevée (RD - Reported Distance): la distance acceptable (FD) calculée par le routeur de saut suivant.

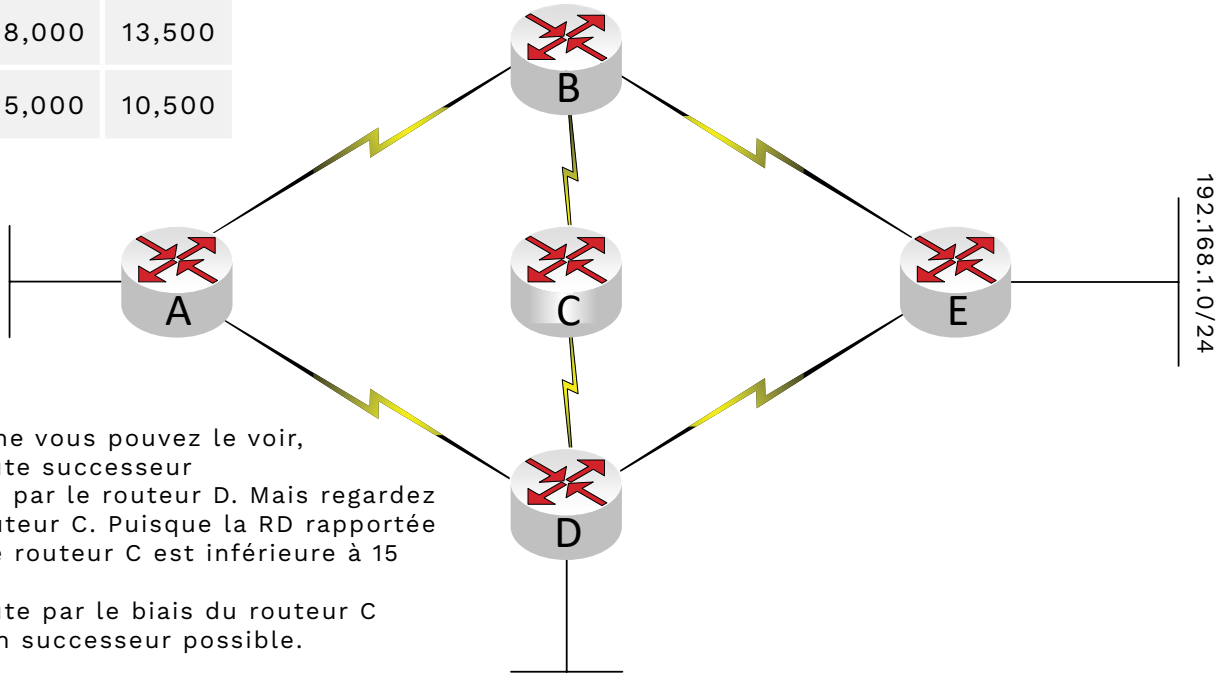
Après que les FD et RD soient connues, EIGRP calcule les routes en fonction de la FD/RD. La meilleure route est appelée la route successeur (route successor) et le processus EIGRP place la route successeur dans la table de routage. Cependant, EIGRP conserve une liste des routes successeurs possibles, ou routes qui sont immédiatement disponibles. Ces routes successeurs possibles sont utilisées au cas où le successeur, ou la route primaire calculée, échoue.

Le successeur possible est déterminé en regardant la RD d'une route calculée. Si la RD d une route est inférieure à la FD, la route est un successeur possible et est conservée comme une route alternative par EIGRP.

MÉTRIQUES POUR LES PROTOCOLES DE ROUTAGE À DISTANCE

Distance – la métrique d'un itinéraire possible
Vecteur - la direction pour l'itinéraire basé sur le routeur de saut suivant

	Met-ric	RD
Router B	20,000	16,000
Router C	18,000	13,500
Router D	15,000	10,500



Comme vous pouvez le voir, la route successeur passe par le routeur D. Mais regardez le routeur C. Puisque la RD rapportée par le routeur C est inférieure à 15 000, la route par le biais du routeur C est un successeur possible.

CONFIGURATION DE EIGRP

Voici les étapes pour configurer un routeur pour EIGRP.

1. Entrer en mode de configuration EIGRP avec la commande **router eigrp numéro-AS**. Veuillez noter que le numéro-as doit être identique sur chaque routeur. Les relations de voisinage ne s'établiront pas entre les routeurs avec des numéros d AS différents.

2. Ajouter les déclarations **network adresse-ip [Wildcard mask]** pour démarrer EIGRP sur les interfaces et rapporter les sous-réseaux attachés

3. (facultatif) Configurer l'identifiant du routeur (RID) avec la commande **eigrp router-id** valeur

4. (facultatif) Changer les minuteries hello et hold sur les interfaces désirées via les sous-commandes **ip hello-interval eigrp asn time** et **ip hold-time eigrp asn time**

5. (facultatif) Ajuster les calculs des métriques de bande passante et de délai via les sous-commandes d interface **bandwidth valeur** et **delay valeur**

6. (facultatif) Permettre le support de plusieurs routes à coût égal via les commandes **maximum-path**s nombre et **variance** multiplicateur

7. (facultatif) Activer le résumé automatique de route avec la commande **autosummary.**

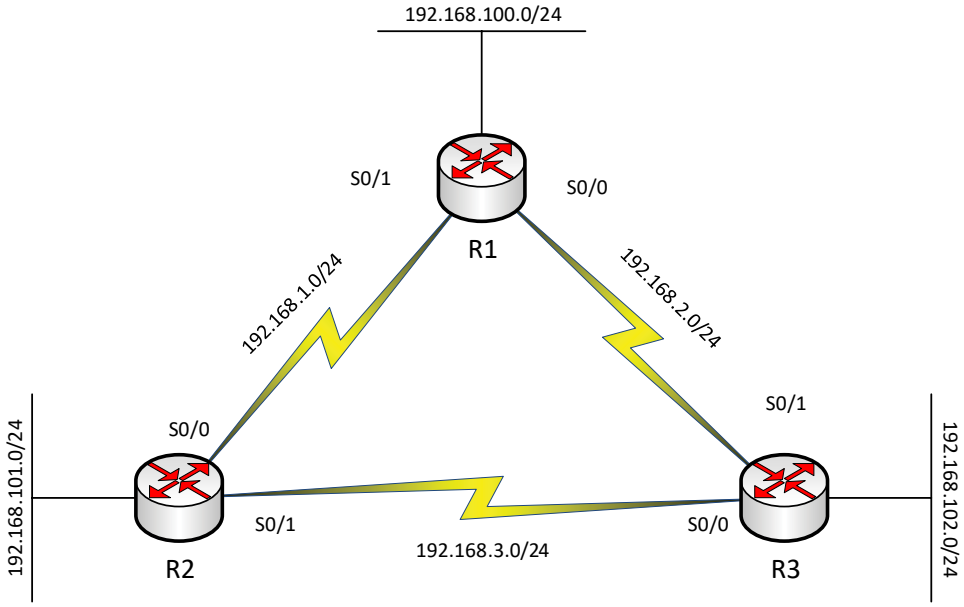
Voici les configurations pour R2:

R2(config)# **router eigrp 200**
R2(config-router)# **network 192.168.1.0 0.0.0.255**
R2(config-router)# **network 192.168.101.0 0.0.0.255**
R2(config-router)# **network 192.168.3.0 0.0.0.255**
R2(config-router)# **maximum-paths 2**

Remarque: il est préférable de ne pas modifier les minuteries par défaut. De plus le résumé automatique ne doit pas être utilisé sur les réseaux non-contigus.

Réseaux annoncés comme le montre la commande **show ip protocols**

```
R2# show ip protocols
<snip>
Routing for Networks:
192.168.1.0/24
192.168.3.0/24
192.168.101.0/24
<snip>
```



Comme OSPF, EIGRP a aussi un ID de routeur. Le routeur-id EIGRP est défini par l'une
des règles suivantes dans l'ordre:

1) Configuré manuellement par la commande eigrp router-id
2) L'adresse IP la plus élevée numériquement sur une interface de bouclage (loopback)
3) L'adresse IP la plus élevée numériquement sur n importe quelle interface physique

Voici un exemple d'une route de la table de topologie de R2

Destination	# of successors	Feasible Distance (FD)

P 192.168.102.0, 1 successors, FD is 2185234
via 192.168.3.2 (2185234/27563) Serial0/1

Next-Hop	Metric	Reported Distance (RD)	Outgoing Interface

IDENTIFIER LA ROUTE SUCCESSEUR POSSIBLE (FEASIBLE SUCCESSOR ROUTE)

Rappelez-vous que la route successeur possible aura une distance déclarée inférieure à la distance possible de la route successeur.

Voici une route de R2:

P 192.168.100.0/24, 1 successors, FD is 2736587
via 192.168.1.1 (2736587/2251423), Serial 0/0 — Successor
via 192.168.3.2 (2854325/2631254), Serial 0/1 — Feasible Successor

Regardez la deuxième route. Comme vous pouvez le voir, sa distance déclarée (2631254) est inférieure à la distance possible de la première route (2736587). Puisque la RD de la deuxième route est inférieure à la FD de la première route, la deuxième route répond aux exigences d'un successeur possible.

REMARQUES CLÉS SUR LA VARIANCE EIGRP

- La variance est multipliée par la distance acceptable actuelle (FD).
- Toute route successeur possible, où la métrique calculée est inférieure à la FD de la route et à la variance du successeur, est placée dans la table de routage si le réglage **maximum-paths** permet plus d'une route.
- Les routes qui ne sont pas des routes successeurs ou routes succes seurs possibles ne sont pas ajoutées à la table de routage afin d'éviter les boucles de routage de paquets.

REMARQUES SUR LE RÉSUMÉ AUTOMATIQUE DE ROUTES (ROUTE SUMMARIZATION)

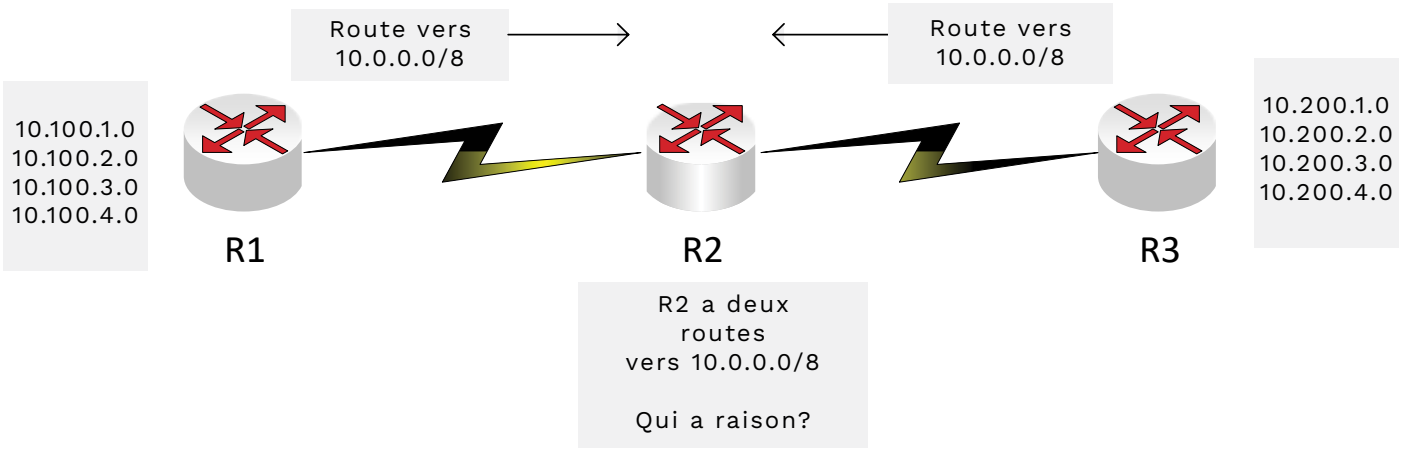
Soyez très prudent lorsque vous activez le résumé automatique. Par défaut, le résumé automatique EIGRP a lieu à travers les frontières de classes (classful). Si les routes liées à un sous-réseau A sont annoncées sur une interface n'appartenant pas au sous-réseau A, les routes sont résumées comme une seule route le long des frontières de classes (classes A, B, C).

DÉFINITIONS DES RÉSEAUX CONTIGUS ET NON-CONTIGUS

Un réseau contigu est un réseau où les paquets envoyés à n'importe quel réseau passe uniquement par les sous-réseaux du même réseau classful en route vers leur destination sans passer par d'autres réseaux classful.

Un réseau non-contigu est un réseau où les paquets envoyés à n'importe quel réseau peut transiter par un ou plusieurs réseaux classful différents du réseau classful d'origine en route vers sa destination.

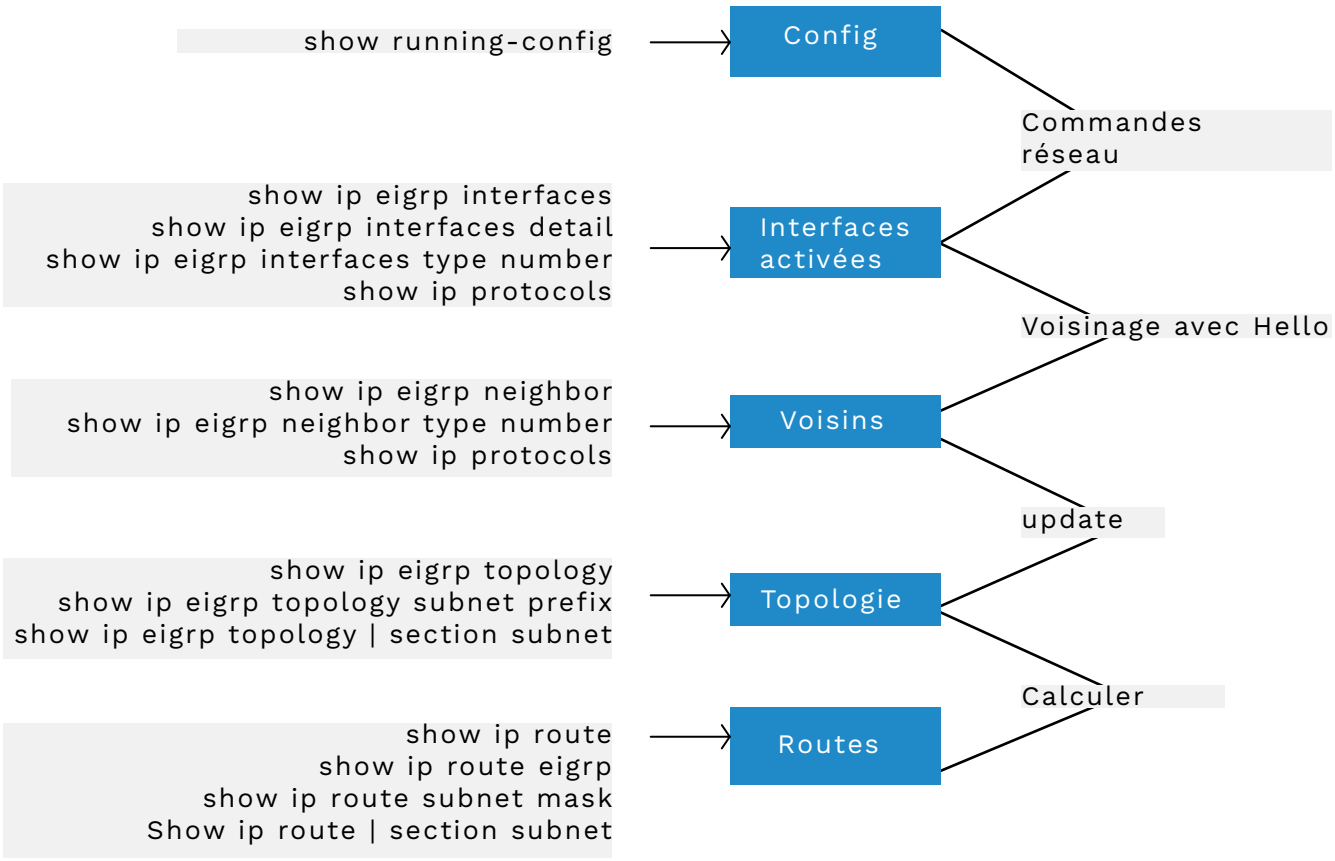
REGARDEZ L'EXEMPLE CI-DESSOUS



Comme vous pouvez le voir ici, R2 a reçu deux mises à jour de routage vers 10.0.0.0/8 de deux routeurs différents sur deux interfaces différentes. Cela signifie que le routeur n'a pas les routes correctes et la convergence n'est pas possible.

Il existe deux solutions: La première consiste à utiliser un système d'adressage IP qui respecte les frontières des classes. Cependant, ce n'est pas possible maintenant avec VLSM. La meilleure solution est de garder le résumé automatique désactivé. Le résumé manuel est possible mais doit être soigneusement planifié.

RECOMMENDATIONS DES COMMANDES DE VÉRIFICATION (À GAUCHE) ET DES SUJETS (À DROITE)



RÉSEAUX ANNONCÉS VU PAR LA COMMANDE SHOW IP PROTOCOLS

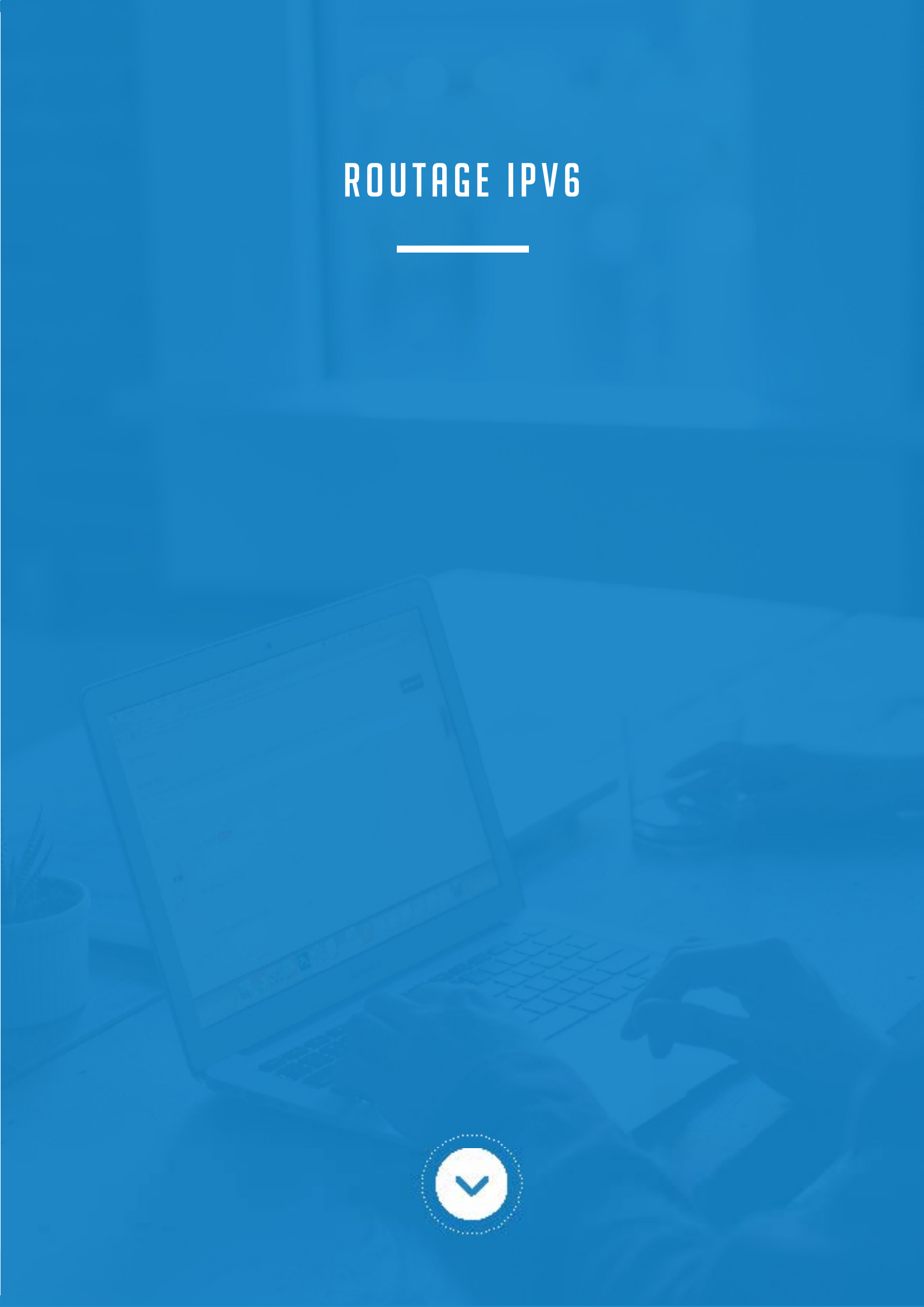
R2# **show ip protocols**
<snip>
RoutIng for Networks:
192.168.1.0/24
192.168.3.0/24
192.168.101.0/24

<snip>

DÉTAILS DE LA COMMANDE SHOW IP PROTOCOLS POUR EIGRP

- La valeur configurée avec la commande **eigrp router-id number.**
- L'adresse IP numériquement la plus élevée d'une interface up/up de bouclage (loopback) au moment où EIGRP démarre.
- L'adresse IP numériquement la plus élevée d'une interface physique up/up au moment où EIGRP démarre.

ROUTAGE IPV6



MISE EN OEUVRE D'OSPF POUR IPV6

La mise en oeuvre d'OSPFv3 pour IPv est très similaire à OSPFv2 pour IPv4 sauf pour le fait que les commandes commençant par ip sous OSPFv2 commencent par **ipv6** dans OSPFv3.

Voici les étapes pour configurer OSPFv3 pour IPv6. (assurez-vous d'activer la commande **ipv6 unicast-routing** en premier):

1) Créez le processus du routeur OSPFv3 avec la commande **ipv6 router ospf PROCESSID.**
2) Configurez manuellement l'ID du routeur OSPF, identifiez l'adresse IPv6 la plus élevée
3) Configurez chaque interface qui participera à OSPFv3 en ajoutant la commande dans le mode interface **ipv6 ospf PROCESS-ID area AREA_NUMBER.**
4) Définissez toutes les interfaces pour un fonctionnement passif avec la souscommande **passive-Interface TYPE NUMBER.**

Voici un exemple de configuration OSPFv3 d'un routeur dans la zone 0:

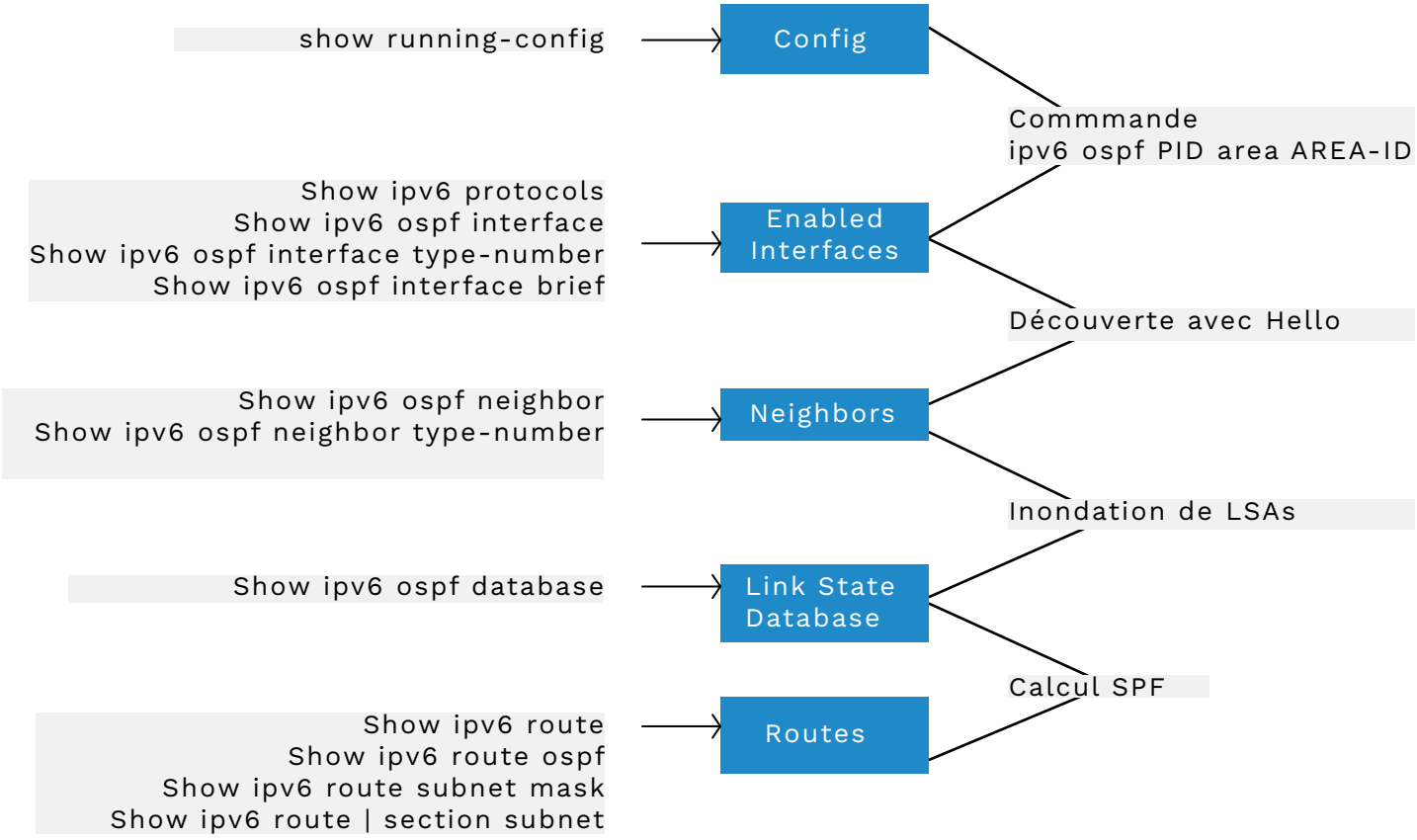
!
ipv6 unicast-routing
!
router ipv6 ospf 1
router-id 2.2.2.2
!
interface Serial0/0/0
adress ipv6 2001:CC::2/64
ipv6 ospf 1 area 0
OSPFv3

OSPFV3 DIFFÉRENCES PAR OSPFV2

Bien que les deux versions de OSPF soient identiques, il existe des différences
importantes:

- Dans OSPFv3, le nom du type 3 LSA est différent de OSPFv2.
- Les voisins dans OSPFv3 ne doivent pas obligatoirement être dans le même sous-réseau, tandis que OSPFv2 exige que les voisins soient dans le même sous-réseau
- OSPFv3 a de nouveaux types LSA non utilisés dans OSPFv2.
- Les types 1, 2 et 3 de LSA ont des composants internes différents par rapport à OSPFv2.

COMMANDES DE CONFIGURATION ET DE VÉRIFICATION OSPFV3



Influencer la métrique OSPF pour les routes est souhaitable lorsque le trafic entre deux points devrait suivre un chemin particulier. Ce chemin peut être moins congestionné ou avoir une plus grande bande passante disponible. Cela se fait en manipulant les coûts d'interface.

Comme pour OSPFv2, voici les commandes pour influencer les coûts d'interface dans OSPFv3:

1) Réglez le coût manuellement avec la sous-commande d'interface **ipv6 ospf cost VALEUR** où la valeur est comprise entre 1 et 65535.

2) Réglez la bande passante sur l'interface avec la sous-commande interface **bandwidth VALEUR** où la vitesse est mesurée en Kbps. Ensuite, laissez le processus de routage déterminer la valeur par le calcul reference-bandwidth / interface-bandwidth.

3) Réglez la bande passante de référence manuellement sur l'interface avec la sous-commande **auto-cost reference-bandwidth VALEUR où VALEUR** est en Mbps.

Attention à l'erreur ! - la vitesse de bande passante de l'interface est en Kbps et la bande passante de référence est en Mbps!.

SIMILITUDES OSPFV2 ET OSPFV3

- Termes et conception liés à l'aire.
- Activation du processus de routage sur chaque interface pour une aire particulière.
- Le processus de découverte voisine est le même que les paquets Hello.
- Les états FULL et 2-WAY signifient la même chose dans les deux protocoles.
- LSA types 1, 2 et 3 et la base de données LSA sont les mêmes.
- L'algorithme SPF est identique dans les deux protocoles.
- Les adresses multidiffusion (multicast) réservées pour les mises à jour dans OSPFv3 (FF02::5 pour tous les routeurs OSPF et FF02::6 pour les routeurs DR) fonctionnent de la même manière que 224.0.0.5 et 224.0.0.6 dans OSPFv2.

DÉPANNAGE DES INTERFACES SOUS OSPFV3

Deux problèmes avec les configurations d'interface peuvent causer des problèmes avec OSPFv3:

- l'interface est dans la mauvaise aire
- une interface passive ne formera pas de relations de voisinage avec d'autres routeurs dans l'aire

Lors de l'analyse des relations de voisinage OSPFv3, assurez-vous que les interfaces sont dans les bonnes aires. Si les interfaces sont dans les bonnes aires, vérifiez que les interfaces ne sont pas configurées pour un fonctionnement passif (passive-interface).

EXIGENCES DU VOISIN POUR OSPFV2 ET OSPFV3

Exigence	OSPFv2	OSPFv3
Les interfaces doivent être dans un état up/up	Oui	Oui
Les interfaces des voisins doivent être dans le même sous-réseau	Oui	Non
Les ACL ne doivent pas filtrer les messages de protocole de routage	Oui	Oui
L'authentification voisine doit être terminée, si elle est configurée	Oui	Oui
Les timer HELLO et DEAD doivent correspondre	Oui	Oui
Les identifiants router-id sont-ils uniques?	Oui	Oui
Utilisation du même ID de processus sur la configuration du routeur requise?	Non	Non

EXIGENCES DU VOISIN POUR OSPFV2 ET OSPFV3 ET LES COMMANDES

Exigence	Commande pour isoler le problème
Authentification du voisin?	show ipv6 ospf interface
Timer HELLO et DEAD?	show ipv6 ospf interface
Même aire?	show ipv6 ospf interface brief, show ipv6 protcols
Identification unique du router-id ?	show ipv6 ospf
Les interfaces sont-elles passives?	show ipv6 ospf interface

OSPFV3 LINK STATE DATABASE ET LSA

Voici les trois principaux types de LSA pour OSPFv3:

- LSA de type 1 (router LSA) pour chaque routeur dans l'aire, y compris les routeurs de bordure d'aire.
- LSA de type 2 (network LSA) pour chaque réseau avec un routeur désigné et un voisin du routeur désigné.
- LSA de type (interarea prefix) pour chaque sous-réseau/préfixe IPv6 situé dans une aire différente.

OSPFV3 ET AUCUNE ROUTE VERS UN SOUS-RÉSEAU

Lorsqu'il n'y a pas d'itinéraire vers un sous-réseau dans la table de routage, effectuez ces vérifications:

1) Vérifiez les routeurs directement connectés au sous-réseau et assurez vous que IPv6 est activé sur les interfaces. OSPFv3 doit aussi être activé sur ces interfaces.

2) Vérifiez les relations de voisinage OSPFv3 entre le routeur local et les routeurs directement connectés au sous-réseau en question.

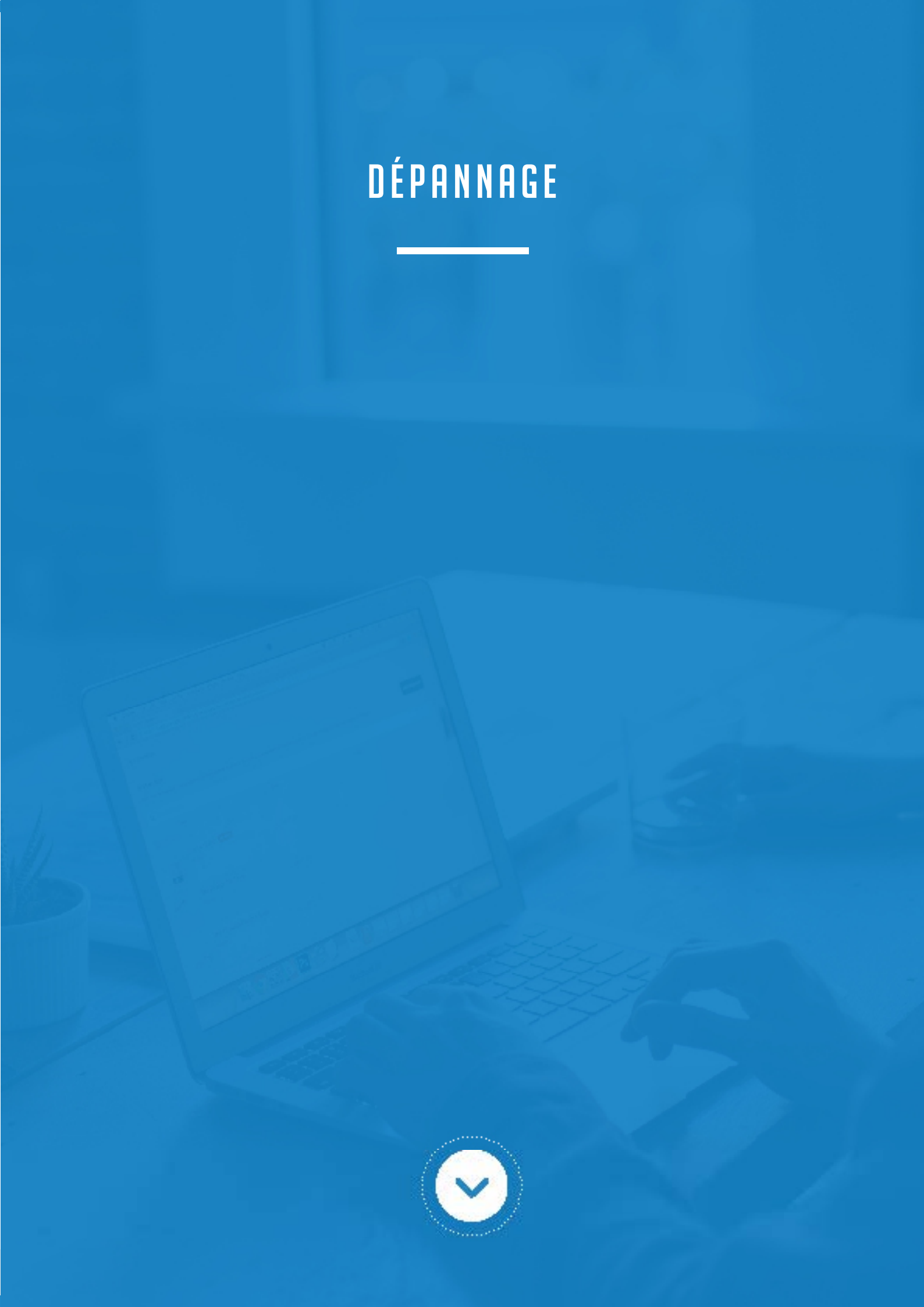
OSPFV3 ET UNE ROUTE SOUS-OPTIMALE

Si l'itinéraire vers une destination est sous-optimal ou semble être le mauvais itinéraire, vérifiez ces éléments:

1) Vérifiez les relations entre les routeurs sur le chemin optimal.

2) Vérifiez les paramètres de coûts OSPFv6 sur les interfaces formant le meilleur chemin.

DÉPANNAGE



Déterminer le commutateur racine

- Commencez par un diagramme et regardez tous les commutateurs possibles comme commutateurs racine.
- En utilisant la commande **show spanning-tree**, éliminez tous les commutateurs avec un port racine.
- La cinquième ligne de la commande **show spanning-tree** indique si le commutateur est la racine.
- Utilisez la commande **show spanning-tree** root comme moyen indirect de déterminer la racine. S'il n'y aucune information sur la racine alors vous avez le commutateur racine.

CONVERGENCE STP

- Si les interfaces ne modifient pas l'état STP, rien ne se produit.
- Si les interfaces doivent passer de l'état **Forwarding** à l'état **Blocking**, la transition est presque immédiate
- Si les interfaces doivent passer de l'état **Blocking** à l'état **Forwarding**, les interfaces passent d'abord à un état **Listening** (Écoute), puis passent à l'état **Forwarding** après un intervalle prédéterminé, habituellement 50 secondes.

AJOUT D'INTERFACES DANS UN ETHERCHANNEL

Vérifiez les points suivants sur chaque interface pour faire correspondre les interfaces Etherchannel:

- Vitesse, Duplex, Access ou Trunk.
- Si un port d'accès, le VLAN d'accès doit être identique.
- Si un port Trunk, le VLAN natif doit être identique.
- Si un port Trunk, la liste des VLAN autorisés doit correspondre.
- Les paramètres STP doivent correspondre.

Le switch n'ajoutera par l'interface à l'Etherchannel si ces paramètres ne sont pas corrects.

PROBLÈME DE SWITCH ROOT LORS DE L'EXAMEN

1. Utilisez les commandes **show spanning-tree** et **show spanning-tree** root pour localiser le switch root. Une fois trouve, notez-le.
2. Regardez le coût de l'interface et pas le Root Cost (couts cumulés)!
3. Si vous devez calculer le Root cost, procédez comme suit:

- Rappelez vous les coûts des interfaces - 2 pour 10 Gbps, 4 pour 1 Gbps, 19 pour 100 Mbits, 100 pour 10 Mbps.
- Voyez si le coût a été configuré manuellement sur l'interface. C'est une erreur classique, ne présumez pas que les coûts sont réglés sur les valeurs par défaut.
- Vérifiez également la vitesse de l'interface. STP n'utilise pas la vitesse maximale de l'interface, mais la vitesse d'interface active (une interface 1Gbps peut fonctionner en 100Mbps).

RÉSOLUTION DES PROBLÈMES ETHERCHANNEL

- Sur le commutateur local, toutes les interfaces participant à l'Etherchannel doivent être sous le même groupe de chaînes.
- Les commutateurs voisins peuvent avoir différents nombres de groupes de canaux.
- Si un mot-clé est utilisé, le même mot-clé doit être utilisé sur les interfaces des deux commutateurs.
- Si le mot-clé desirable est utilisé sur un commutateur, PAgP est utilisé sur le commutateur donc l'autre interface de commutateur doit utiliser desirable ou auto comme mot-clé.
- Si le mot-clé active est utilisé sur un seul commutateur, LACP est utilisé sur le commutateur donc l'autre interface de commutateur doit utiliser active ou passive.

CHOISIR LE VLAN DES TRAMES ENTRANTES SUR UN PORT DU SWITCH

- Si un port d'accès, les trames entrantes sont ajoutés avec le tag VLAN **(switchport access vlan vlan_id).**
- Si le port est configuré comme un port voix:
  - Les trames de données sont associées au VLAN spécifié dans la commande **switchport access vlan vlan_id.**
  - Les trames voix sont associées au VLAN spécifié dans la commande **switchport voice vlan vlan_id.**
- Si le port est un Trunk, le commutateur utilisera le tag VLAN de la trame reçue. S'il n'y a pas de tag sur la trame reçue, on ajoute le tag VLAN spécifiée via la commande **switchport trunk native vlan vlan_id** (sinon, l'ID VLAN est 1).

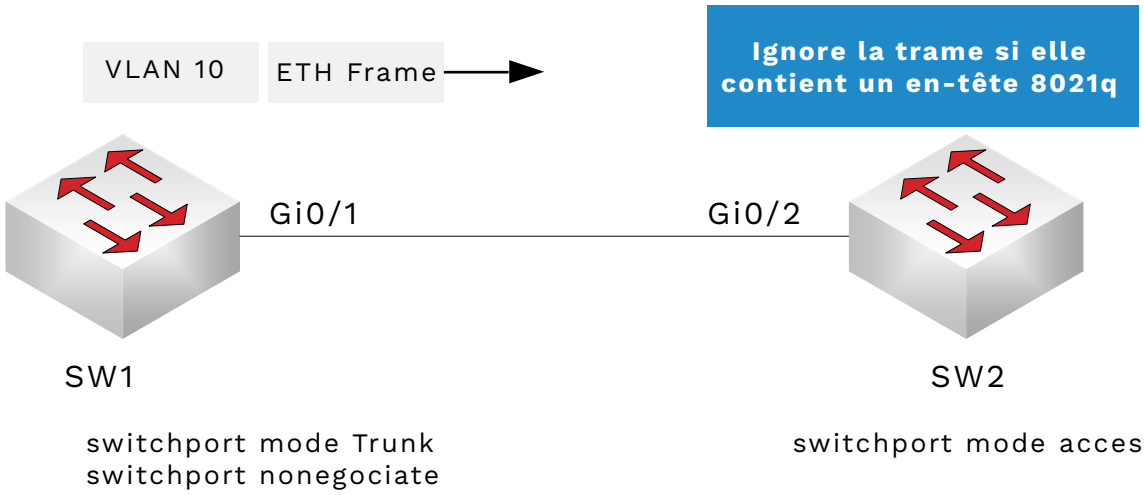
DÉPANNAGE DES VLAN ET DES TRUNK

- Identifiez tous les ports d'accès et VLAN. Réaffecter si nécessaire.
- Déterminez si les VLAN sont configurés ou appris via VTP (VLAN Trunking Protocol). Ajouter et configurer des VLAN si nécessaire pour résoudre le problème.
- Vérifiez les listes VLAN autorisées sur chaque interface Trunk. Si nécessaire, modifiez la liste VLAN autorisée si nécessaire.
- Vérifiez le mode de fonctionnement de chaque interface, comme par exemple une interface en Trunk d un côté et l'autre interface en Access
- Vérifiez les VLAN autorisés sur chaque Trunk et assurez-vous que chaque commutateur n'a pas automatiquement supprimé un VLAN requis.

COMMANDES POUR LES PORTS D'ACCÈS ET LES VLAN

Commande EXEC	Description
show vlan brief show vlan	Énumére chaque VLAN et toutes les interfaces affectées à ce vlan, à l'exclusion des Trunk.
show vlan id num	Liste des ports en Access et en Trunk affecté à ce VLAN
show interfaces type number switchport	Identifie le mode de l'interface (Access ou Trunk), le VLAN voix...
show mac address-table	Affiche les adresses MAC apprises par le commutateur et leurs VLAN associés

MAUVAISE CONFIGURATION TRUNK ET ACCESS



Alors que les commutateurs transmettront le trafic dans cette configuration, CDP continuera à enregistrer les entrées concernant l'inadéquation des ports sur les deux commutateurs!

COMMANDE SHOW INTERFACE TRUNK

Position	Titre	Description
Premier	VLANs allowed	VLAN 1 à 4094 moins ceux supprimés par la commande switch trunk allowed vlan
Deuxième	VLANs allowed an active	La première liste moins les VLAN non définis localement ou par VTP
Troisième	VLANs in in spanning tree	La deuxième liste moins les VLAN bloqués par spanning tree et élagués par le trunk.

RÈGLES CLÉS POUR LE DÉPANNAGE DES PROTOCOLES DE ROUTAGE LORS DE L'EXAMEN

- Tout lire et regarder soigneusement.
- Tout lire et regarder soigneusement une deuxième fois !
- Regarder les interfaces où le protocole de routage doit être actif. Les relations de voisinage doivent être prévues.
- Vérifier que chaque interface prévue pour exécuter le protocole de routage a le protocole activé.Sinon, régler et vérifier à nouveau.
- Vérifier les routeurs attendus pour les relations de voisinage. Si les relations ne se font pas, dépanner et vérifier à nouveau.

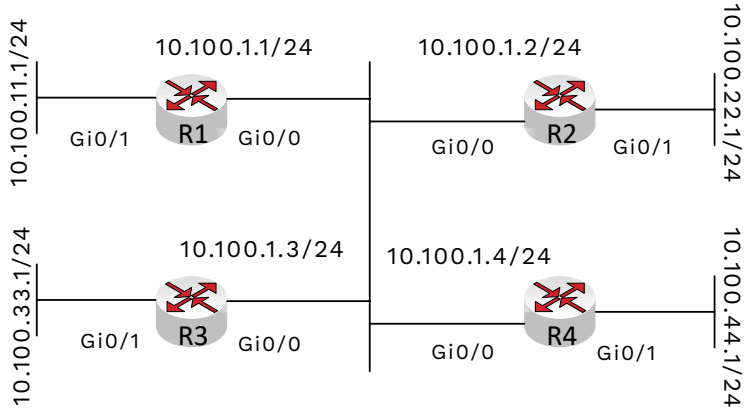
Rappelez-vous ce que fait la sous-commande **routeur network**. Lorsque la commande **network** est entrée dans la configuration, le routeur annoncera le sous-réseau couvert par la commande **network** et essayera d'établir une relation de voisinage sur l'interface associée au sous-réseau.

LES COMMANDES POUR TROUVER LES INTERFACES AVEC DES PROTOCOLES DE ROUTAGE ACTIVÉS DESSUS

Commande	Information sur la Commande	Les interfaces passives,sont-elles listées?
show ip eigrp interfaces	Liste les interfaces où EIGRP est activé par la commande **network**, sauf pour les interfaces passives	NON
show ip ospf interface brief	Liste les interfaces où EIGRP est activé par la commande **network**, y compris les interfaces passives	OUI
show ip protocols	Liste les commandes de la configuration du réseau regroupées par processus de routage, y compris les interfaces passives	OUI

DANS L'EXEMPLE À DROITE, NOUS AVONS LES PROBLÈMES SUIVANTS

- Le sous-réseau du LAN de R3 n'est pas annoncé.
- Le sous-réseau du LAN de R4 n'est pas annoncé
- R4 n'a pas établi des relations de voisinage avec les trois autres routeurs



Vérifier la configuration EIGRP sur R3. De **show ip protocols**, nous voyons que le sous-réseau du LAN de R3 n'est pas dans la configuration du réseau. Après avoir saisi la configuration du réseau, le sous-réseau du LAN de R3 est maintenant annoncé.

Vérifier la configuration EIGRP sur R4. De **show ip protocols**, nous voyons que R4 Gi0/0 est une interface passive. Une fois que nous enlevons la configuration d'interface passive de Gi0/0, R4 établira des relations de voisinage et le sous-réseau du LAN de R4 sera annoncé.

DÉPANNAGE OSPF POUR L'EXAMEN

- Examinez la configuration et assurez-vous que chaque routeur a des interfaces dans les aires appropriées.
- Une fois assuré que les configurations de l'aire sont correctes, assurez-vous que les numéros routeur-id sont uniques à chaque routeur. Des IDs de routeur en double peuvent causer des problèmes.
- Vérifier que les relations de voisinage sont formées entre les routeurs appropriés.
- Si plusieurs routeurs OSPF sont sur le même LAN, assurez-vous que les adresses réseau sont correctes, que les interfaces ne sont pas passives, et que les routeurs désignés (DRs) et routeurs désignés de secours (BDRs) sont élus.

EXIGENCES POUR VOISINS OSPF ET EIGRP

Exigences	EIGRP	OSPF
Les interfaces sont up/up	Oui	Oui
Les interfaces sont dans le même sous-réseau?	Oui	Oui
Des ACLs ne filtrent pas les messages des protocoles de routage	Oui	Oui
Doit réussir l'authentification de voisin	Oui	Oui
Doit utiliser le même AS dans la commande de la configuration du routeur	Oui	Non
Les minuteries Hello et Dead doivent correspondre	Non	Oui
Les IDs de routeur doivent être uniques	Non	Oui
Les valeurs K doivent correspondre sur les deux routeurs	Oui	N/A
Les interfaces des routeurs doivent être dans la même aire	N/A	Oui

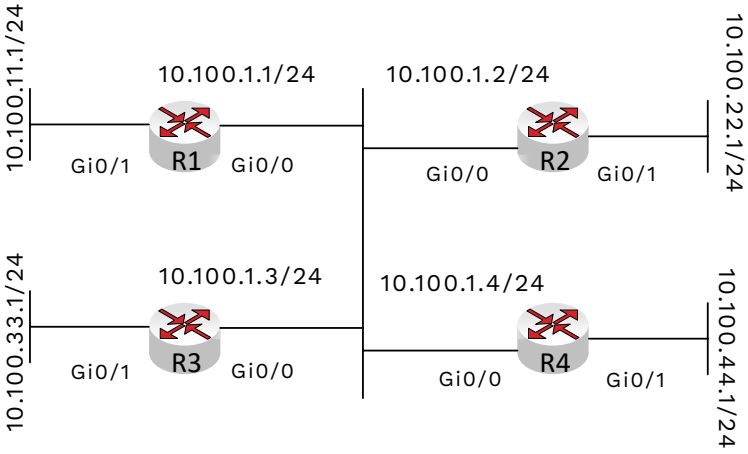
EXIGENCES POUR VOISIN EIGRP ET COMMANDES SHOW/DEBUG APPROPRIÉES

Exigences	Commandes
Doit être dans le même sous-réseau IP	show interfaces, show ip interface
Doit utiliser le même numéro AS	show eigrp interfaces, show ip protocols
Passer l'authentification de voisin	debug eigrp packets, show run
Valeurs K doivent correspondre	show ip protocols

DANS L'EXEMPLE À DROITE, NOUS AVONS LES PROBLÈMES SUIVANTS

R3 est dans sa propre area sans connexion à l area 0.

Solution: Vérifier la configuration de l'interface Gi0/0 et modifier la configuration pour l'area 0.



EXIGENCES DE VOISIN OSPF ET COMMANDES SHOW/DEBUG APPROPRIÉES

Exigences	Commandes
Doit être dans le même sous-réseau IP	show interfaces, debug ip ospf hello
Passer l'authentification de voisin	show ip ospf interface, debug ip ospf adj
Minuteries Hello et Dead correspondants	show ip ospf interface, debug ip ospf hello
Interfaces dans la même aire	show ip ospf int brief, debug ip ospf adj
IDs de routeur unique (RID)	sshow ip ospf

PROBLÈMES DE CONNECTIVITÉ DE L'HÔTE

Si une commande **ping** sur un hôte ne peut pas atteindre une destination, essayez le routeur par défaut. Si le routeur par défaut est inaccessible, l'un des problèmes suivants pourrait être le problème:

- L'hôte possède une mauvaise adresse IP
- L'hôte n'a pas reçu d'adresse IP attribuée par DHCP
- L'interface Ethernet du routeur peut être configurée différemment de l'interface du commutateur (Trunk ou Access).
- Autres problèmes LAN (vitesse / duplex / Port-Security / câblage / port).

PING SUR UN LIEN WAN

Si un **ping** fonctionne sur un lien WAN, les éléments suivants sont vrais:

- Les deux interfaces du routeur (interface interne et externe) sont en up / up
- Les couches Layer-1 et Layer-2 fonctionnent correctement
- Les adresses IP du routeur sont dans le même sous-réseau
- Les ACL entrantes ne filtrent pas les paquets ping

VÉRIFICATION DES PARAMÈTRES DE L'HÔTE IPV4

- Vérifiez les serveurs DNS configurés par rapport aux adresses IP du serveur DNS réelles.
- Vérifiez les paramètres du routeur par défaut configuré en fonction de la configuration de l'adresse IP du routeur
- Vérifiez le masque de sous-réseau configuré sur l'hôte
- L'hôte et le routeur doivent se trouver dans le même sous-réseau IP. Cela se détermine avec le masque de sous-réseau.

Point	Nom	Valeur dans l'exemple	Description
1	Classful network	10.0.0.8	La table de routage est organisée pour chaque réseau classful
2	Nb de sous-réseaux	13 sous-réseaux	Liste le nombre de routes connues de ce routeur, y compris les interfaces connectées
3	Nb de masques	5 masques	Le nombre de masques connus du routeur associé à ce réseau classful
4	code de légende	C, L, O	Comment l'itinéraire a été appris. C est connecté, L est Local, et O est OSPF
5	ID de sous-réseau	10.2.2.0	Le numéro de sous-réseau de cette route particulière
6	Longueur du préfixe	/30	Le masque de préfixe utilisé avec ce sous-réseau
7	Administrative Distance	110	Selon le protocole de routage de l'itinéraire, il existe unemétrique associée au protocole. L'AD le plus bas permet de déterminer l'itinéraire utilisé.
8	Métrique	128	La métrique pour cet itinéraire
9	Routeur Next-hop	10.2.2.5	Utilisez cette destination pour les paquets associés à ce routeur
10	Timer	14:31:52	C'est le temps écoulé depuis que cet itinéraire ait été annoncé par OSPF ou EIGRP
11	Interface sortante	Serial0/0/1	L'interface sortante pour les paquets correspondant à ce routeur

Une panne entre un périphérique hôte et un routeur sur un réseau local peut être causée par l'un des deux problèmes:

- Erreur de l'interface LAN du routeur
- Problèmes au sein du LAN lui-même

ERREUR CLASSIQUE SUR UNE INTERFACE LAN

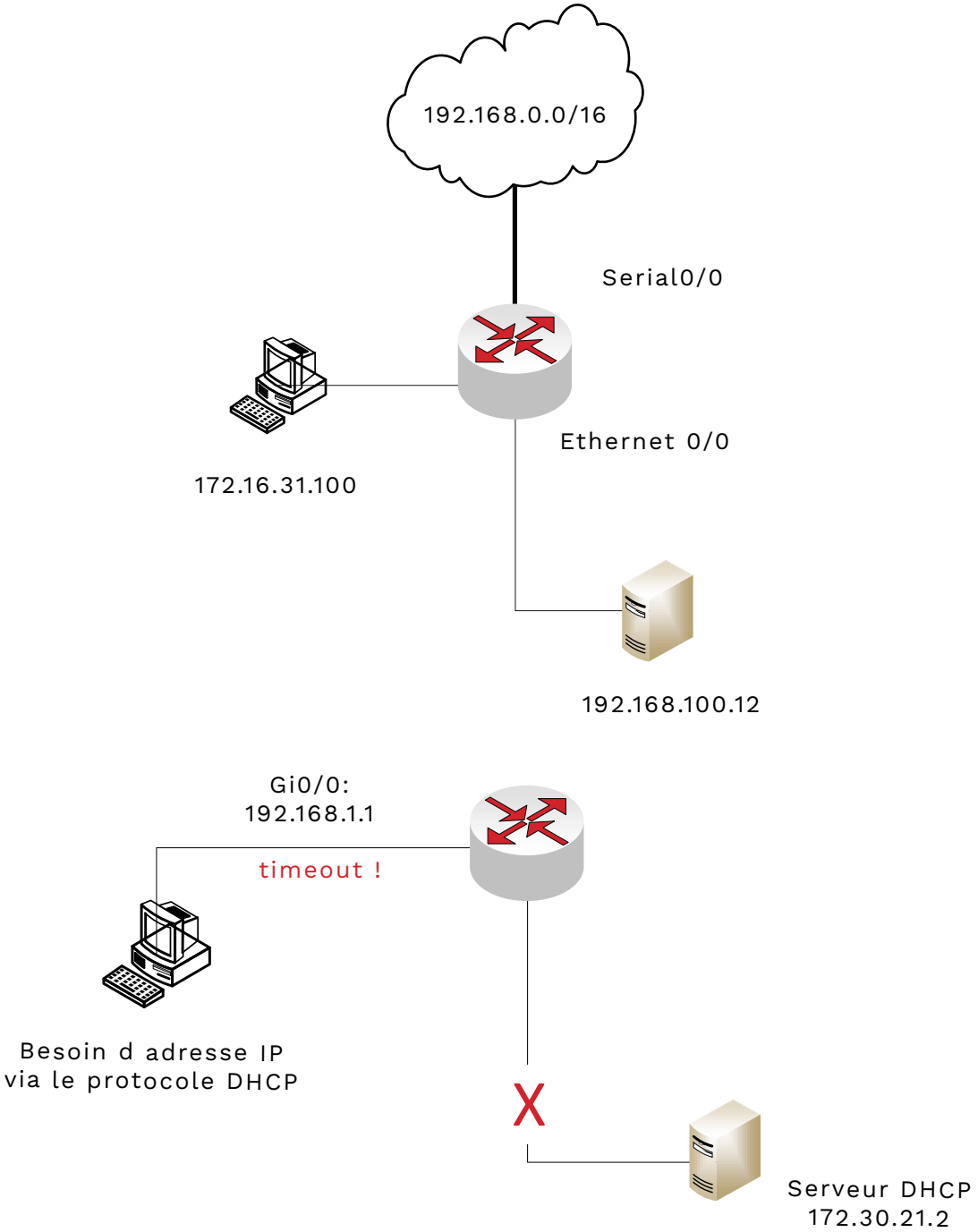
Etat de l inter-face	Raison	Description
down/down	Incompatibilité de vitesse	Les interfaces fonctionnent à des vitesses différentes car la vitesse est définie sur les deux interfaces
admin down/down	Shutdown	L'interface est arrêtée manuellement (commande **shutdown**)
down/down	Err-disabled (switch)	La sécurité du port arrête le port
down/down	Pas de câble ou mauvais câble	Le câble n'est pas connecté ou mauvais contact sur le câble

N’oubliez pas que le routeur utilisera la correspondance de préfixe la plus longue pour acheminer le paquet. Le routeur enverra le paquet sur le réseau ou l’identifiant de sous-réseau le plus spécifique.

Par exemple, ces routes se trouvent dans la table de routage:

192.168.0.0/16 Serial0/0
192.168.100.0/28 Ethernet0/0

Si un paquet entre avec une adresse de destination de 192.168.1.4, le routeur enverra le paquet sur l’interface Serial0/0. Toutefois, si le paquet a une adresse de destination de 192.168.100.1 à 192.168.100.14, le paquet sera envoyé Sur l’interface Ethernet0/0 car cette interface a un identifiant de sous-réseau plus spécifique.



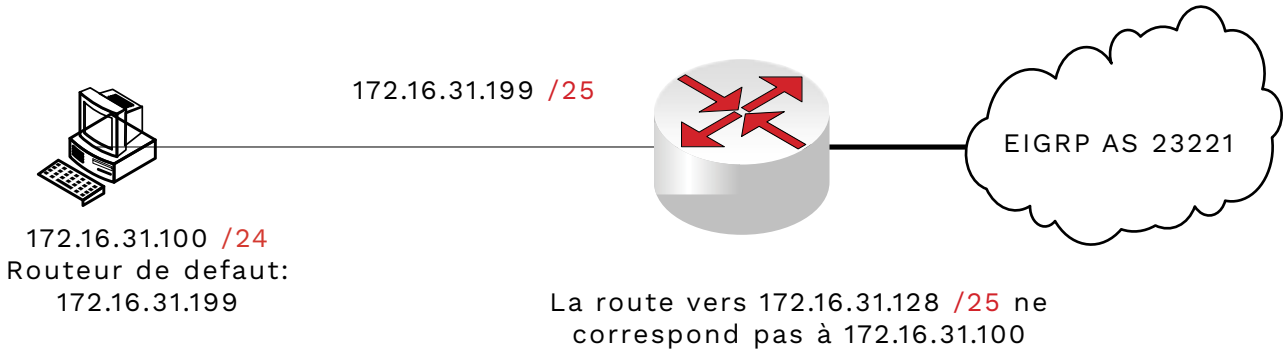
ip dhcp helper-address 172.30.21.1

PROBLÈMES DE RELAIS DHCP

Si un hôte ne peut pas recevoir des informations DHCP à partir d'un serveur DHCP, l'une des raisons pourrait être:

- Problème de connectivité entre l'hôte et le serveur DHCP
- Adresse de l'assistant DHCP (helper-address) incorrecte configurée dans le routeur
- Problème de connectivité entre le routeur et le serveur DHCP distant

Dans cet exemple, le routeur n'a pas de connectivité au serveur DHCP, de sorte que le trafic DHCP n'atteindra pas sa destination.



ERREUR DE MASQUE DE SOUS-RÉSEAU ENTRE L'HÔTE ET LE ROUTEUR

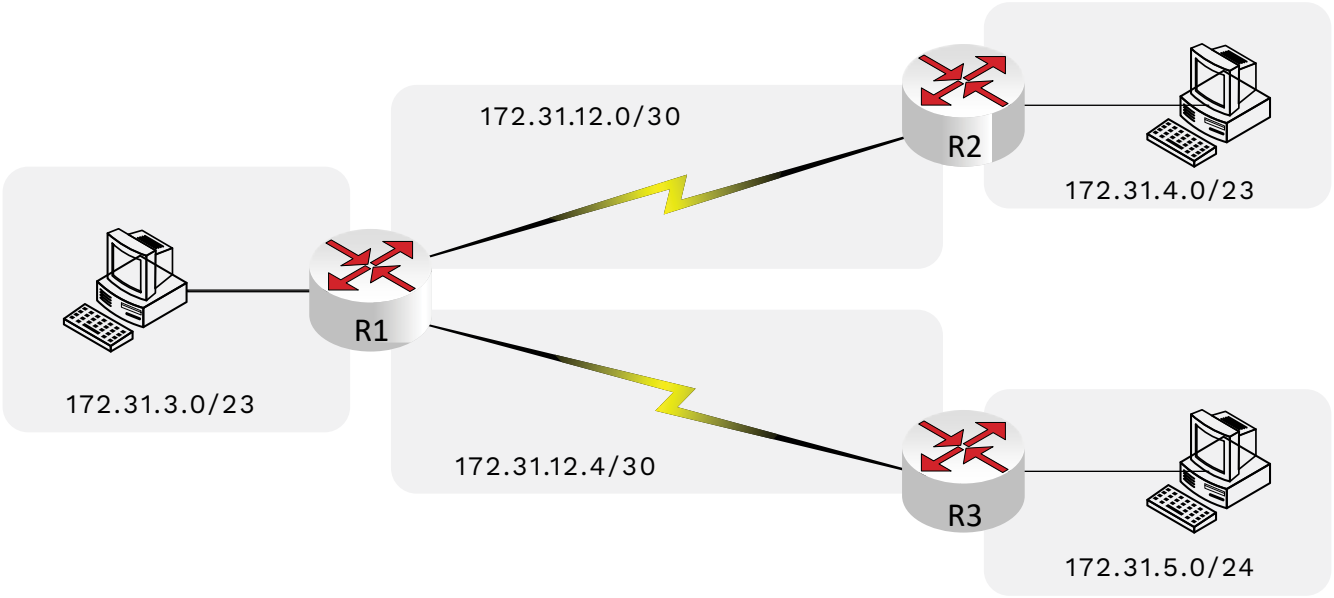
Nous avons ici un hôte avec un masque /24 et le routeur possède un masque /25 (.129 à .254). Bien que le routeur passe le trafic de l'hôte vers le réseau, le routeur distant ne disposera que d'un itinéraire pour 172.16.31.128/25 qui exclut 172.16.31.100 (l'adresse IP de l'hôte).

Il existe deux façons de corriger ce problème. L'un consiste à corriger le masque de sous-réseau sur l'hôte. L'autre est de corriger le masque de sous-réseau sur le routeur et de s'assurer que le routeur annonce le sous-réseau approprié.

LES SOUS-RÉSEAUX VLSM SE CHEVAUCHANT

Sur un seul routeur, le routeur peut empêcher le VLSM de se chevaucher lorsqu'une sous-commande d'interface d'adresse IP est configurée pour se chevaucher avec une sous-commande d'adresse IP déjà existante. Un message d erreur est alors affiché.

Cependant, le système IOS ne peut pas détecter les sous-commandes d'adresse IP placées sur différents routeurs. Par conséquent, le chevauchement VLSM ne peut être évité que dans un seul routeur.



Dans cet exemple, R2 possède un sous-réseau superposé avec R3. La confusion se produit dans R1 lorsque les routes pour 172.31.4.0/23 et 172.31.5.0/24 sont reçues par R1. Le routeur ne sait pas où envoyer les paquets car la table de routage est instable et change constamment.

La solution ici est de changer le sous-réseau sur R2 ou R3 afin que le chevauchement soit supprimé. Par exemple, si nous modifions le masque de sous-réseau sur R2 à /24, la table de routage converge et le trafic atteindra sa destination.

TYPES D'ADRESSES IPV6

Typet	Premiers chiffres	Similaire à IPv4 privé ou publique?
Global Unicast	2 to E	Publique
Unique local Unicast	FD	Privé
Link-local	FE80	Pas de comparaison directe

FORMAT D'ADRESSE IPV6 AVEC ID D'INTERFACE ET CONFIGURATION EUI-64

Préfixe de sous-réseau	MAC 1er moitié	FFFE	MAC 2nd moitié

Exemple: en utilisant les règles EUI-64, dérivez la partie de l'adresse hôte de l'adresse IPv6 en fonction d'une adresse MAC = 00: 1E: EB: C2: 25: 24

Étape 1: divisez l'adresse MAC en deux et insérez FFFE entre les deux moitiés. Changez le résultat en un numéro de 64 bits.
Résultat: 001E: EBFF: FEC2: 2524

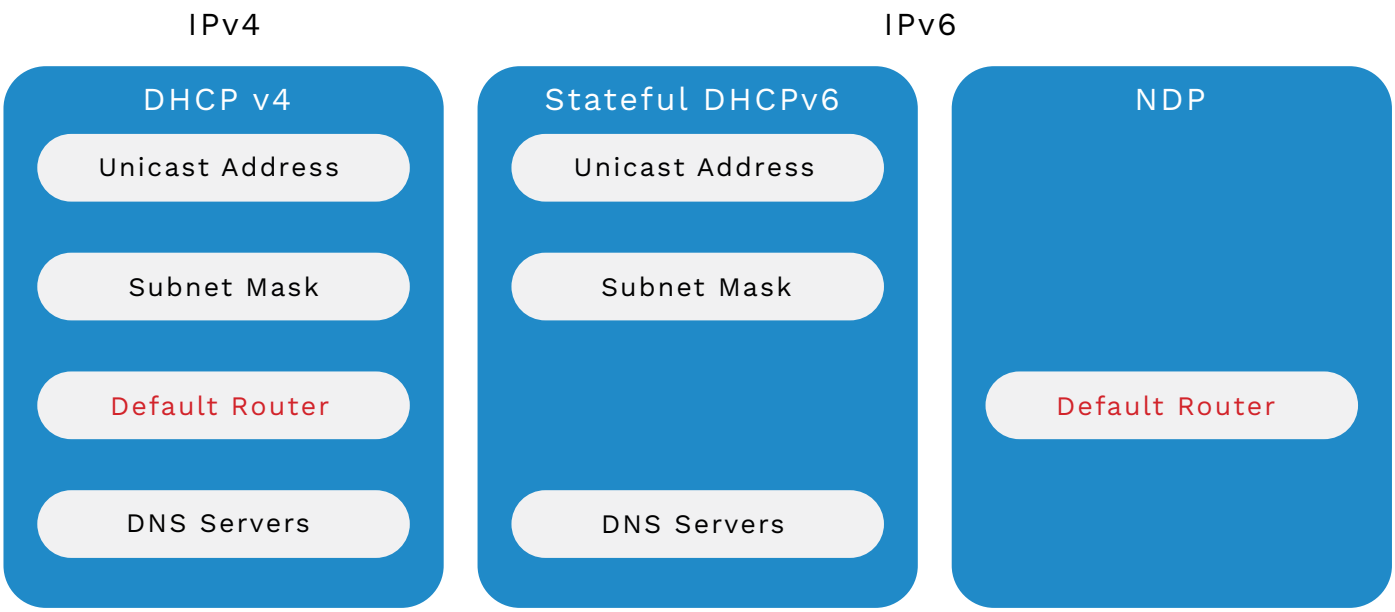
Étape 2: prenez les deux premiers chiffres hexadécimaux, convertissez en binaire pour inverser le septième bit et convertissez-le en hexadécimal.

Les deux premiers chiffres sont 00, alors l'inversion du septième bit donne 0000 0010 soit 02. L'adresse hôte EUI-64 résultante est 021E: EBFF: FEC2: 2524

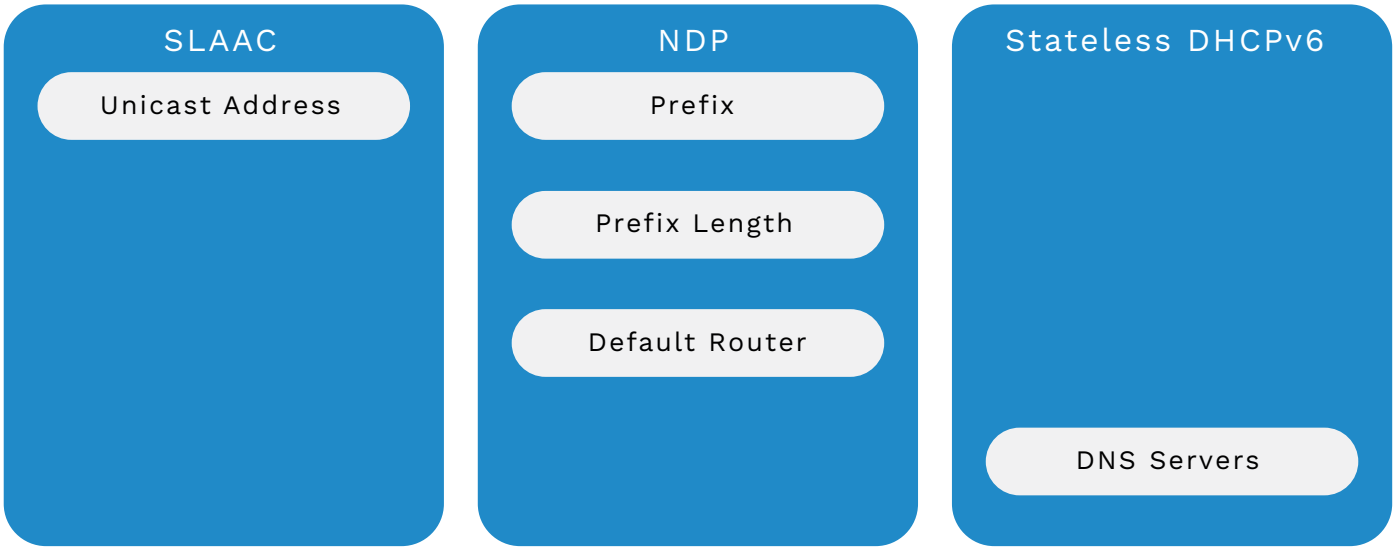
Configuration des adresses IPv6 sur les routeurs:

- Activez le routage IPv6 avec la commande **ipv6 unicast-routing**.
- Utilisez la sous-commande **ipv6 address ADRESSE/PREFIXE** pour activer IPv6 sur chaque interface à l'aide d'IPv6.

SOURCES D'INFORMATION POUR IPV6 STATEFUL DHCP



SOURCES D'INFORMATION POUR IPV6 STATELESS DHCP



DÉPANNAGE DES PROBLÈMES IPV6

Problèmes liés à l'hôte:

- Les hôtes doivent être dans le même sous-réseau IPv6 que le routeur par défaut.
- Les hôtes doivent utiliser la même longueur de préfixe que le routeur par défaut.

- L'hôte doit indiquer une adresse de routeur réelle en tant que routeur par défaut.
- Les adresses DNS doivent être correctes sur chaque hôte.

Problèmes liés aux routeurs:

- Les interfaces du routeur doivent être dans un état up/up pour transmettre le trafic.
- Deux routeurs utilisant le même LAN pour la communication doivent avoir des adresses dans le même sous-réseau IPv6.
- Les routeurs devraient avoir des routes IPv6 vers tous les sous-réseaux IPv6 dans la conception.

Problèmes du a un filtrage potentiel (routeurs et commutateurs):

- Vérifiez le filtrage des adresses MAC sur les ports de commutation et dans les commutateurs.
- Assurez-vous que les VLAN nécessaires sont présents dans les commutateurs.
- Tout comme dans les routeurs IPv4, regardez les listes de contrôle d'accès (ACL) dans les routeurs IPv6.

Exemple de problème: le routeur par défaut ne répond pas aux PING de l'hôte.

Vérifiez ce qui suit lorsque le ping échoue entre un hôte et son routeur par défaut:

- Vérifiez les interfaces LAN sur l'hôte et le routeur. Assurez-vous qu'elles sont activées.
- Il peut y avoir un problème sur le LAN empêchant les trames de voyager entre l'hôte et le routeur
- Un composant LAN (commutateur) arrête les Trames en raison de la sécurité du port ou du filtrage des adresses MAC.

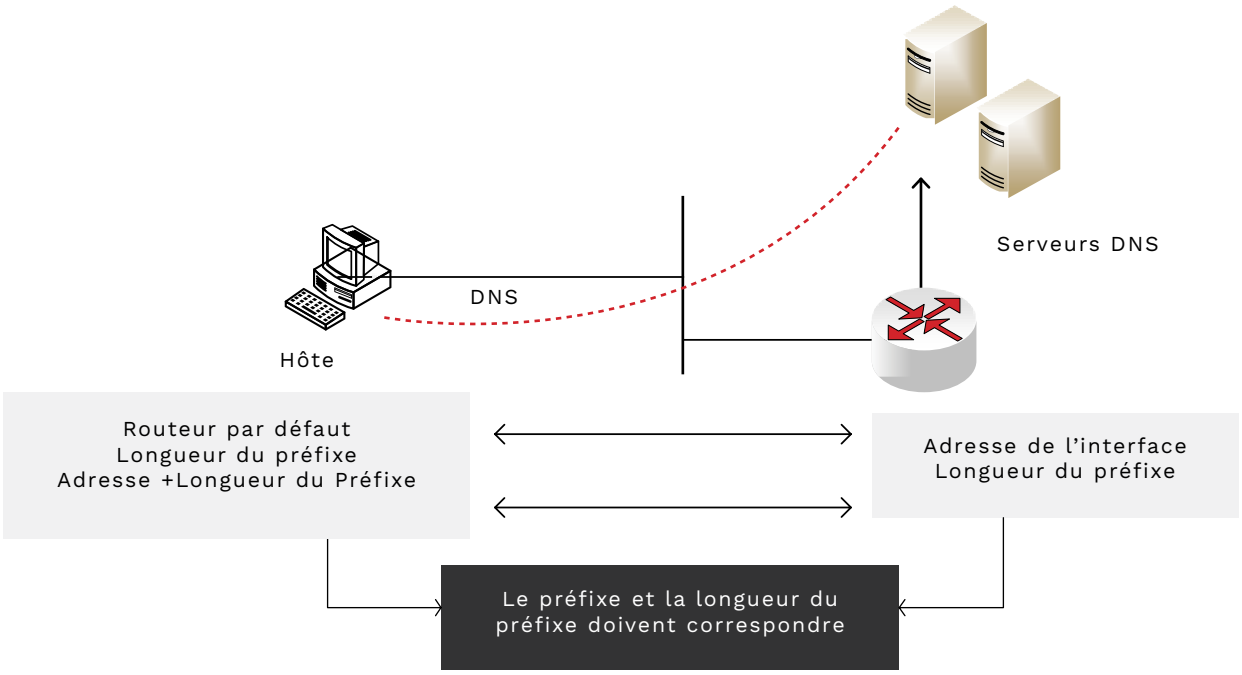
PANNE DE RÉSOLUTION DNS

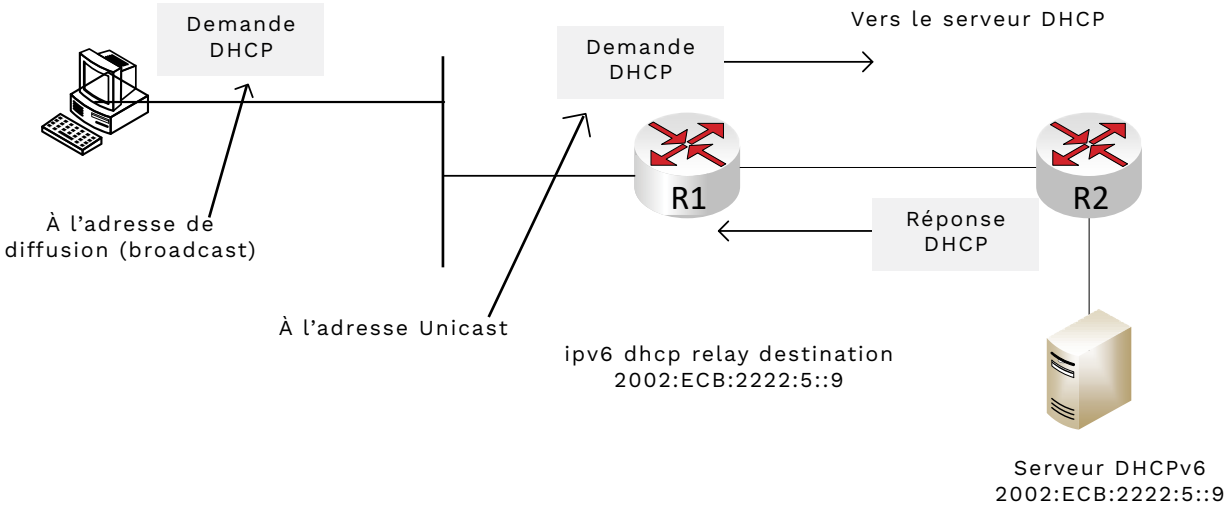
Vérifiez ce qui suit lorsque la résolution DNS échoue:

- Si les serveurs DNS sont déclarés en statique, vérifiez que les paramè-tres sont corrects
- Vérifiez si DHCPv6 a fourni une adresse DNS incorrecte à l'hôte
- Vérifiez s'il existe un problème de connectivité IPv6 entre l'hôte et les serveurs DNS

Processus de dépannage dans le cas où DNS est inaccessible:

- Comparez les paramètres de l'interface sur l'hôte et le routeur. Si la longueur du préfixe ne correspond pas ou si les adresses IP ne se rouvent pas dans le même sous-réseau, corrigez.
- Essayez de faire un ping sur la destination.





Paramètres Host IPv6

PROBLÈMES DHCPV6 STATEFUL

Pour que DHCPv6 fonctionne, l'une des conditions suivantes doit être vraie:

- Le DHCP et l'hôte doivent être dans le même sous-réseau, ou
- Le serveur DHCP peut se trouver dans un sous-réseau différent pourvu que
    - Le routeur local a configuré le relais DHCPv6
    - Il existe une connectivité entre le routeur local et le serveur DHCPv6

Ping et **traceroute** du routeur local peuvent aider à isoler les problèmes de connectivité

PROBLÈMES DHCPV6 STATELESS AVEC SLAAC

S'il y a des problèmes avec DHCPv6 et SLAAC, nous devons découvrir pourquoi les messages Network Discovery Router Sollicitation et Router Advertisement ont échoués. Voici les éléments à examiner lors de la validation DHCPv6 Stateless:

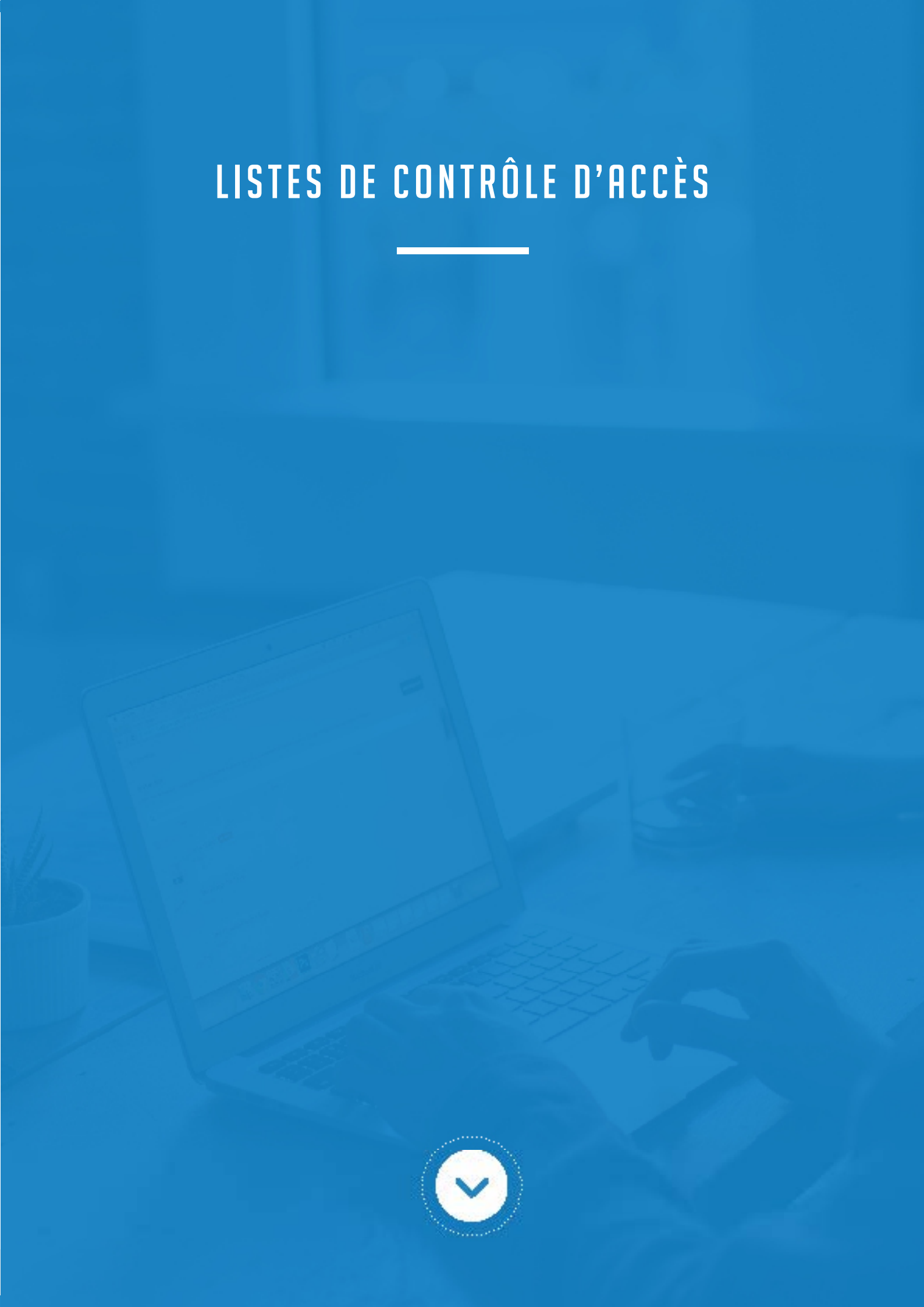
- Vérifiez la connectivité LAN entre l'hôte et les routeurs dans le sous-réseau. S'il n'y a pas de connectivité, le NPD ne fonctionnera pas.
- Le routeur peut ne pas avoir l'adresse ipv6 configurée sur une interface.
- Le routeur n'a pas la commande **ipv6 unicast-routing** activée dans sa configuration.

PROBLÈMES DE ROUTAGE À TRAVERS LES SOUS-RÉSEAUX

Si les pings et le réseau local semblent fonctionner mais que l'accès aux réseaux distants non, la commande traceroute est alors utilisé pour résoudre ce problème. Si traceroute affiche certains routeurs mais échoue tout de même, voici les problèmes à étudier:

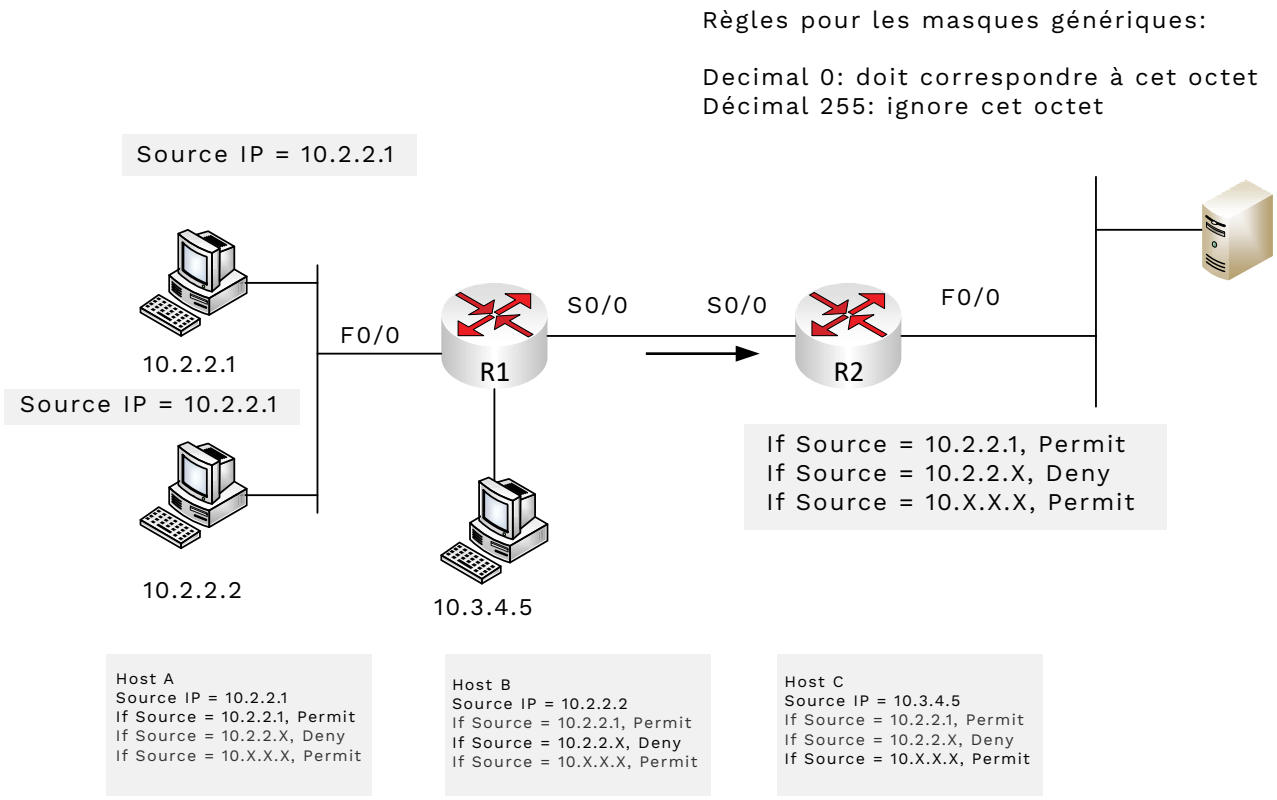
- Les liens entre les routeurs sont inopérants
- Les protocoles de routage ont des problèmes de voisinage
- Le filtrage d'itinéraire peut empêcher l'ajout d'un itinéraire à la table de routage IPv6
- Les routes statiques mal configurées envoient des paquets à la mauvaise destination
- Une mauvaise conception réutilise les sous-réseaux dans différentes parties du réseau, ce qui entraînera des annonces vers de mauvais chemins.

LISTES DE CONTRÔLE D'ACCÈS



LISTES DE CONTRÔLE D'ACCÈS IPV4 DE BASE (ACL)

Une liste de contrôle d'accès (ACL) doit être utilisée lorsqu'il est nécessaire de filtrer un paquet à mesure qu'il traverse une interface d'un routeur. L'ACL doit être appliqué sur l'interface du routeur et dans le même sens que le flux initial de paquets.



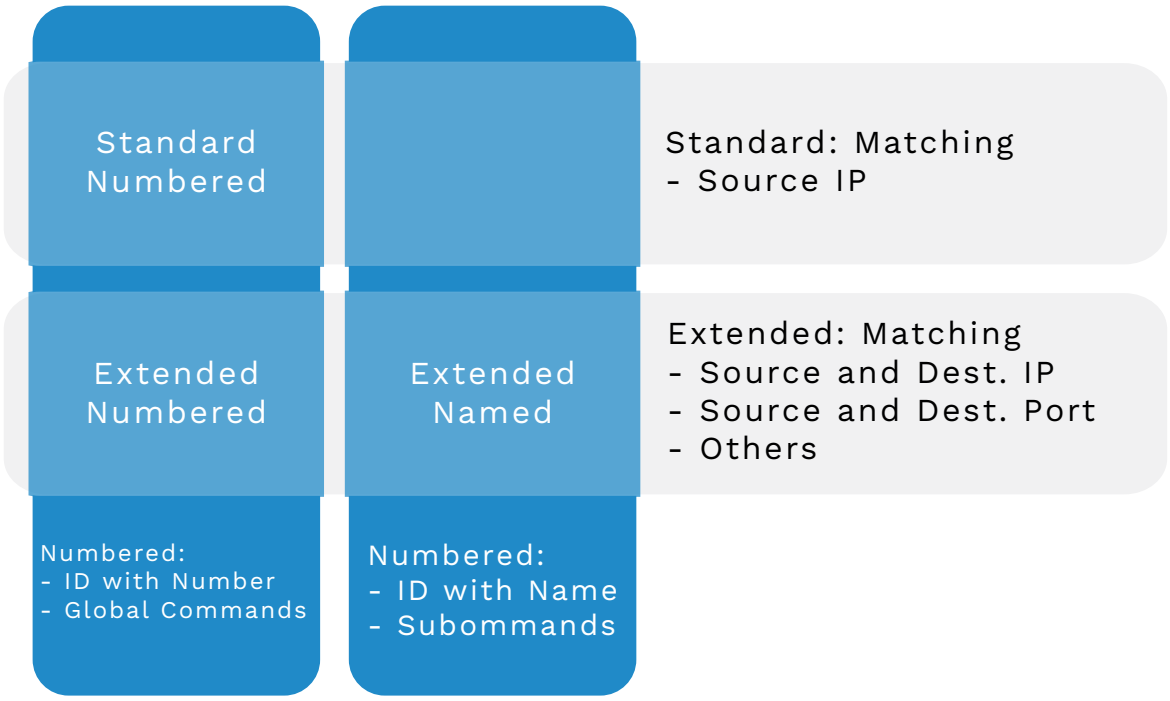
COMMANDES DE LISTE D'ACCÈS

correspondance d'adresse IP exacte: **permit 10.2.2.2** ou **permit host 10.2.2.2**
Faire correspondre un sous-réseau / 24: **permit 10.2.2.0 0.0.0.255** (notez le Wildcard mask)

Dans le masque générique, un 0 signifie ignorer et 255 signifie doit correspondre exactement".

COMMANDES POUR IMPLÉMENTER L'ACL SUR R2

```
access-list 1 permit 10.2.2.1
access-list 1 deny 10.2.2.0 0.0.0.255
acces-list 1 permit 10.0.0.0 0.255.255.255

interface S0 / 0
ip access-group 1 in
```



Comparaison des types de ACL IP

TYPES D'ACL DE CISCO

- ACL numérotées standard (1 - 99)
- ACL numérotées étendues (100 - 199)
- Numéros ACL supplémentaires (standard 1300 - 1399, étendu 2000 - 2699)
- ACL nommé
- Amélioration de l'édition avec les numéros de séquence

Les ACL correspondront à la première déclaration (permit ou deny) et s'arrêteront. Si un paquet correspond à la première déclaration, alors le paquet sera traité conformément aux règles puis l'ACL cessera de traiter ce paquet. N'oubliez jamais l'implicite "deny any" ou "deny all" à la fin de chaque ACL

TROUVER LE BON MASQUE GÉNÉRIQUE POUR UN JEU DE SOUS-RÉSEAU

Utilisez l'identifiant de sous-réseau comme valeur source dans la commande de la liste d'accès.

Utilisez un masque générique trouvé en soustrayant le masque de sous-réseau de 255.255.255.255

Exemple: recherchez le masque générique pour faire correspondre le masque de sous-réseau 255.255.255.0

255.255.255.255
- 255.255.255.0
  0. 0. 0.255

Le masque générique résultant est 0.0.0.255

ÉTAPES POUR METTRE EN OEUVRE LES ACL STANDARD IP

Étape 1: identifiez le routeur, l'interface et la direction de la liste d'accès IP Les ACL standard devraient être des endroits aussi près que possible de la destination afin que les paquets qui devraient être transmis ne soient pas rejetés. Les ACL standard ne peuvent inspecter que l'adresse IP source pour correspondre à l'adresse source dans le sens du flux de trafic pour les paquets correspondant.

Étape 2: configurez une ou plusieurs commandes globales de liste d'accès pour créer l'ACL en tenant compte des réserves suivantes: la liste est associée séquentiellement en utilisant la logique du premier match . L'action par défaut qui se trouve à la fin de l'accès est implicite "deny any" ou "deny all".

Étape 3: activez la liste d'accès sur l'interface et la direction du routeur choisi avec la commande **ip access-group NUMERO {in | out}.**

COMMANDES POUR IMPLÉMENTER L'ACL SUR R2

```
R2(config)# access-list 1 permit 10.2.2.1
R2(config)# access-list 1 deny 10.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 10.0.0.0 0.255.255.255

R2(config)# interface S0/0
R2(config-if)# ip access-group 1 in
```

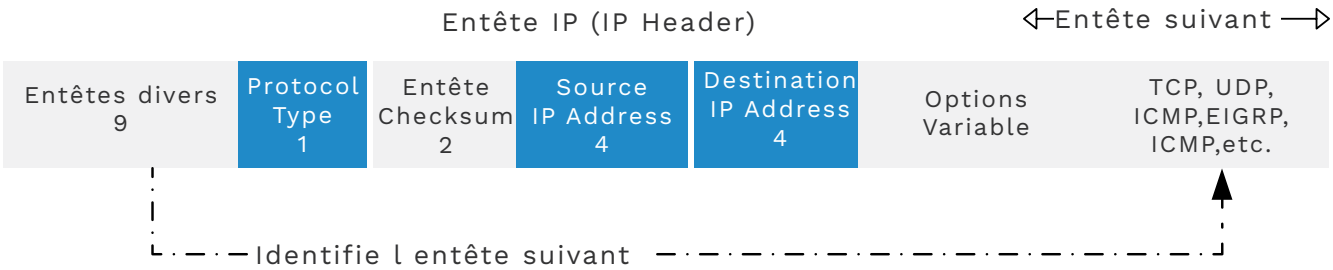
NOTES SUR LA CONSTRUCTION DES LISTES D'ACCÈS

Pour associer une adresse ou un hôte spécifique, utilisez uniquement l'adresse. Pour correspondre à toutes les adresses, utilisez le mot-clé **any**

Pour correspondre seulement à un, deux ou trois octets, utilisez les masques génériques (wildcard) 0.255.255.255, 0.0.255.255 et 0.0.0.255 respectivement.

Pour faire correspondre un ID de sous-réseau, utilisez l'ID de sous-réseau comme source et recherchez le masque générique en soustrayant le masque de sous-réseau de 255.255.255.255

Lorsque les routeurs appliquent une ACL pour filtrer les paquets dans le sens sortant (mot clé **out**), le routeur vérifie les paquets qu'il envoie vers l'interface de sortie. Cependant, un routeur ne filtre pas les paquets que le routeur crée lui-même avec une ACL sortante. Des exemples de ces paquets incluent des messages de protocole de routage OSPF et des paquets envoyés par les commandes ping et traceroute sur ce routeur.

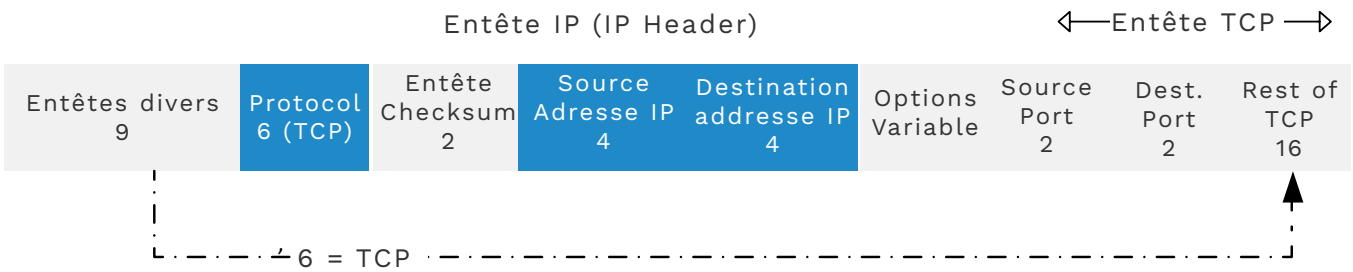


En-tête IP avec en gris les champs requis pour les ACL IP étendues

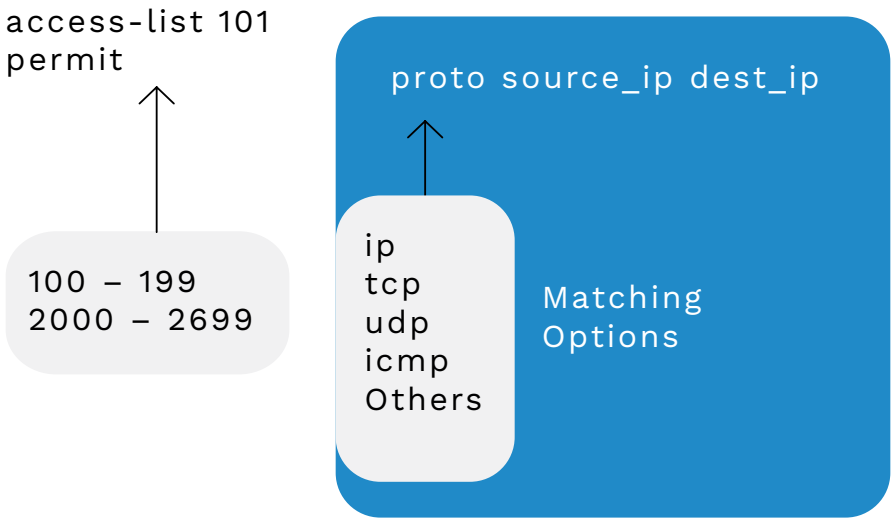
COMMANDES DES ACCESS-LIST ÉTENDUES

Déclaration de la liste d'accès	Correspondance
access-list 101 deny tcp any any	Tout paquet IP avec un entête TCP
access-list 101 deny udp any any	Tout paquet IP avec un entête UDP
access-list 101 deny icmp any any	Tout paquet IP avec un entête ICMP
access-list 101 deny ip host 1.1.1.1 host 2.2.2.2	Tout paquet du hôte 1.1.1.1 allant vers le hôte 2.2.2.2, quelque soit l'entête suivant
access-list 101 deny udp 1.1.1.0 0.0.0.255 any	Tout paquet avec un entête UDP provenant du réseau 1.1.1.1/24 et quelque soit la destination

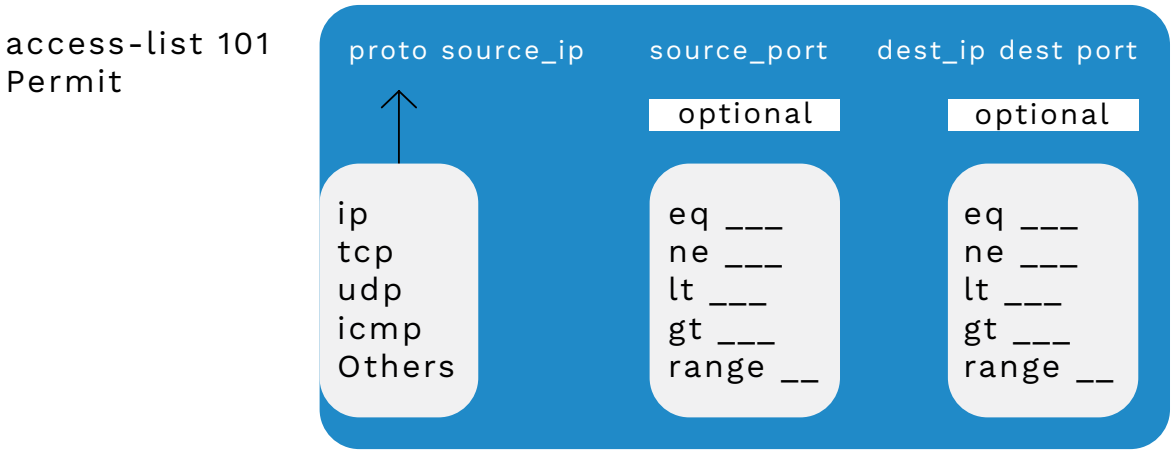
Dans une ACL étendue, tous les paramètres de la commande doivent correspondre au paquet afin de traiter le paquet



En-tête IP avec en-têtes TCP et champs de numéro de port



Syntaxe de l'ACL étendue

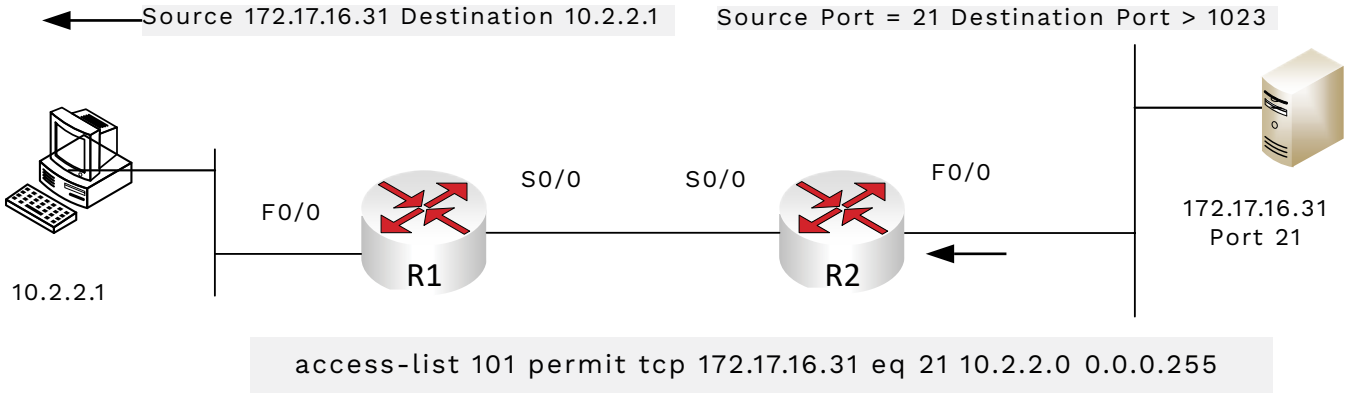


Syntaxe de l ACL étendue avec le numéro de port

REMARQUES SUR LE PLACEMENT DES ACL ÉTENDUES

- Placez les ACL étendues le plus près possible de la source de paquets. Un filtrage près de la source permettra d'économiser la bande passante.
- Tous les champs d'une access-list doivent correspondre au paquet pour qu'une correspondance ait lieu.
- Il n'y a pas de différence entre les plages 100 – 199 et 2000 – 2699.

FILTRAGE BASÉ SUR LE PORT SOURCE




```
access-list 101 permit tcp 172.17.16.31 eq 21 10.2.2.0 0.0.0.255
```

COMMANDES ET EXPLICATIONS DE LISTE D'ACCÈS ÉTENDUE

Déclaration de la liste d'accès	Logique de commande
access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23	Les paquets avec un en-tête TCP, de n'importe quelle adresse source, avec un port source de 1023 ou supérieur et allant à l'hôte 10.1.1.1 avec un port de destination de 23 seront supprimés
access-list 101 deny tcp any host 10.1.1.1 eq 23	Identique à l'exemple précédent, mais avec un port source quelconque
access-list 101 deny tcp any host 10.1.1.1 eq telnet	Comme l'exemple précédent, telnet est l'alias du port 23
access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any	Les paquets provenant du réseau source 1.0.0.0/8 et un port source inférieur à 1023 allant à n'importe quelle destination seront supprimés

LISTES D'ACCÈS NOMMÉES

- L'utilisation de noms au lieu de nombres pour identifier les listes d'accès a rendu plus facile sa compréhension.
- L'utilisation de sous-commandes ACL permet de définir l'action et les paramètres correspondants.
- Les fonctions d'édition ACL permettent d'éditer l'ACL afin que des lignes puissent être ajoutées ou supprimées sans.
- Redéfinir l'intégralité de l'ACL.

CONSIDÉRATIONS RELATIVES À LA MISE EN OEUVRE DE L'ACL

- Placez les ACL étendues aussi proches que possible de la source pour jeter les paquets rapidement.
- Placez les ACL standard aussi proches que possible de la destination parce que certains paquets peuvent etre supprimes accidentellement
- Positionner les règles les plus précises en premier et les plus larges ensuite.
- Désactivez une ACL de son interface avant de la modifier

MODIFICATION DES ACL VIA LES NUMÉROS DE SÉQUENCE

- Les ACL numérotés ont désormais un style de configuration, comme les ACL nommées, de sorte que chaque ligne possède un numéro de séquence
- La suppression de lignes est possible en utilisant le numéro de séquence de la ligne
- L'insertion de nouvelles lignes permet d'insérer une ligne dans une ACL via un numéro de séquence
- La numérotation de séquence automatique permet à l'utilisateur d'ajouter une ligne à la fin d'une ACL et la ligne aura automatiquement son numéro de séquence.

ACL numérotée

```
access-list 1 permit 3.3.3.3
access-list 1 permit 4.4.4.4
access-list 1 permit 5.5.5.5
```

ACL nommée

```
ip access-list standard name
access-list 1 permit 3.3.3.3
access-list 1 permit 4.4.4.4
access-list 1 permit 5.5.5.5
```

EDITION D UNE ACL AVEC LES NUMÉROS DE SÉQUENCE

R1(config)# ip access-**list standard 25**
R1(config-std-nacl)# **permit 10.1.1.0 0.0.0.255**
R1(config-std-nacl)# **permit 10.2.2.0 0.0.0.255**
R1(config-std-nacl)# **do show access-list 25**

10 permit 10.1.1.0 0.0.0.255
20 permit 10.2.2.0 0.0.0.255

R1(config-std-nacl)# **no 20** (ici on supprime la seconde ligne de l ACL)
R1(config-std-nacl)# **do show access-list 25**

10 permit 10.1.1.0 0.0.0.255

R1(config-std-nacl)# **5 deny 10.1.1.1** (ici insère une ligne avant la ligne 10)
R1(config-std-nacl)# **do show access-list 25**
5 deny 10.1.1.1
10 permit 10.1.1.0 0.0.0.255

DÉPANNAGE DES LISTES DE CONTRÔLE D'ACCÈS

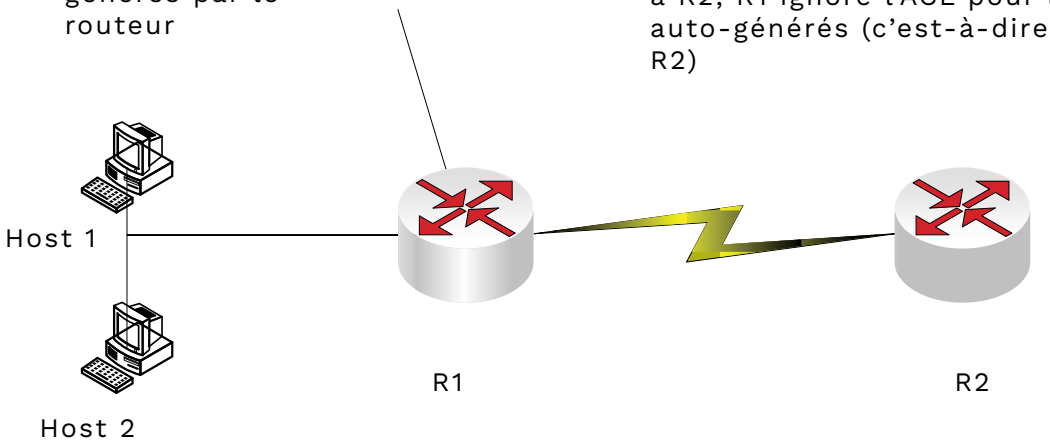
1) Déterminez les ACL activées sur chaque interface (**show running-config** ou **show ip interfaces**)
2) Trouvez la configuration de chaque ACL (**show access-lists, show ip access-lists)**
3) Analyser les ACL par les paramètres suivants:

- Voyez si les lignes sont mal placées
- Adresse IP de source / destination inversée
- Ports de destination / destination inversée
- Syntaxe - assurez-vous que les mots-clés **tcp** et **udp** sont utilisés correctement
- Syntaxe (ICMP) - rappelez-vous que ping utilise ICMP, pas TCP ou UDP
- Présence d'un **deny any** - était-il inclus au début de l ACL?
- Emplacement ACL standard - l'ACL est-elle à un emplacement correct? Si c'est près de

la destination, il pourrait y avoir des problèmes

Ignorer les ACL pour les paquets générés par le routeur

Rappel: sur le routeur R1, s'il existe une ACL outbound sur l'interface connectée à R2, R1 ignore l'ACL pour les paquets auto-générés (c'est-à-dire ping de R1 à R2)



SIMILITUDES ENTRE LES LISTES D'ACCÈS IPV4 ET IPV6

- Les deux vérifient les adresses source ou de destination
- Les deux vérifient les adresses IP d'un hôte ou sous-réseau
- Les deux peuvent être appliqués sur l'entrée ou la sortie de l'interface
- Les deux peuvent combiner les informations Layer-4 associées à TCP ou UDP et les numéros de port
- Les deux peuvent correspondre à des types et codes de messages ICMP spécifiques.
- Les deux ont une déclaration deny implicite à la fin de l'ACL qui corre spond à tous les paquets restants.
- Les deux supportent l'activation basée sur le temps (time-based ACL)

PRINCIPALES DIFFÉRENCES ENTRE LES LISTES D'ACCÈS IPV4 ET IPV6

- Les ACL IPv4 peuvent uniquement vérifier des paquets IPv4 et les ACL IPv6 peuvent uniquement vérifier des paquets IPv6.
- Les ACL IPv4 peuvent être identifiées par numéro ou nom, tandis que les ACL IPv6 utilisent uniquement les noms.
- Les ACL IPv4 identifient qu'une ACL est standard ou étendue en fonction de la plage de numé ros ACL ou en utilisant le mot-clé standard ou extended. Les ACL IPv6 ont un concept ACL extended et standard similaire, mais ne différencient pas les styles avec un mot-clé de configuration différent.
- Les ACL IPv4 peuvent vérifier des valeurs spécifiques uniques à un en-tête IPv4 (par exemple, option, priorité, ToS TTL, fragments...).
- Les ACL IPv6 peuvent vérifier des valeurs spécifiques uniques à un en-tête IPv6 (par exemple, une étiquette de flux, un DSCP) ainsi que des valeurs d'en-tête d'extension et d'option.

- Les ACL IPv6 ont une instruction de permit implicite à la fin de chaque ACL, juste avant le refus implicite tout à la fin de l'ACL, tandis que les ACL IPv4 n'ont pas d'instruction de permit implicite.

SYNTAXE DE L'ACL IPV6

[permit | deny] ipv6 {source-ipv6-prefix/prefix-length | **any | host** source-ipv6- address} {destination-ipv6-prefix/prefix-length | **any | host** destination-ipv6-address} **[log]**

Commande	Port correspondant
permit tcp	[eq | gt | lt | neq {port | protocol}] [range {port | protocol}]
Commande	Port correspondant
permit udp	[eq | gt | lt | neq {port | protocol}] [range {port | protocol}]
Commande	Types de messages ICMP
permit icmp	[icmp-type [icmp-code] | icmp-message]

Champs de correspondance TCP, UDP et ICMP dans les ACL IPv6 étendues

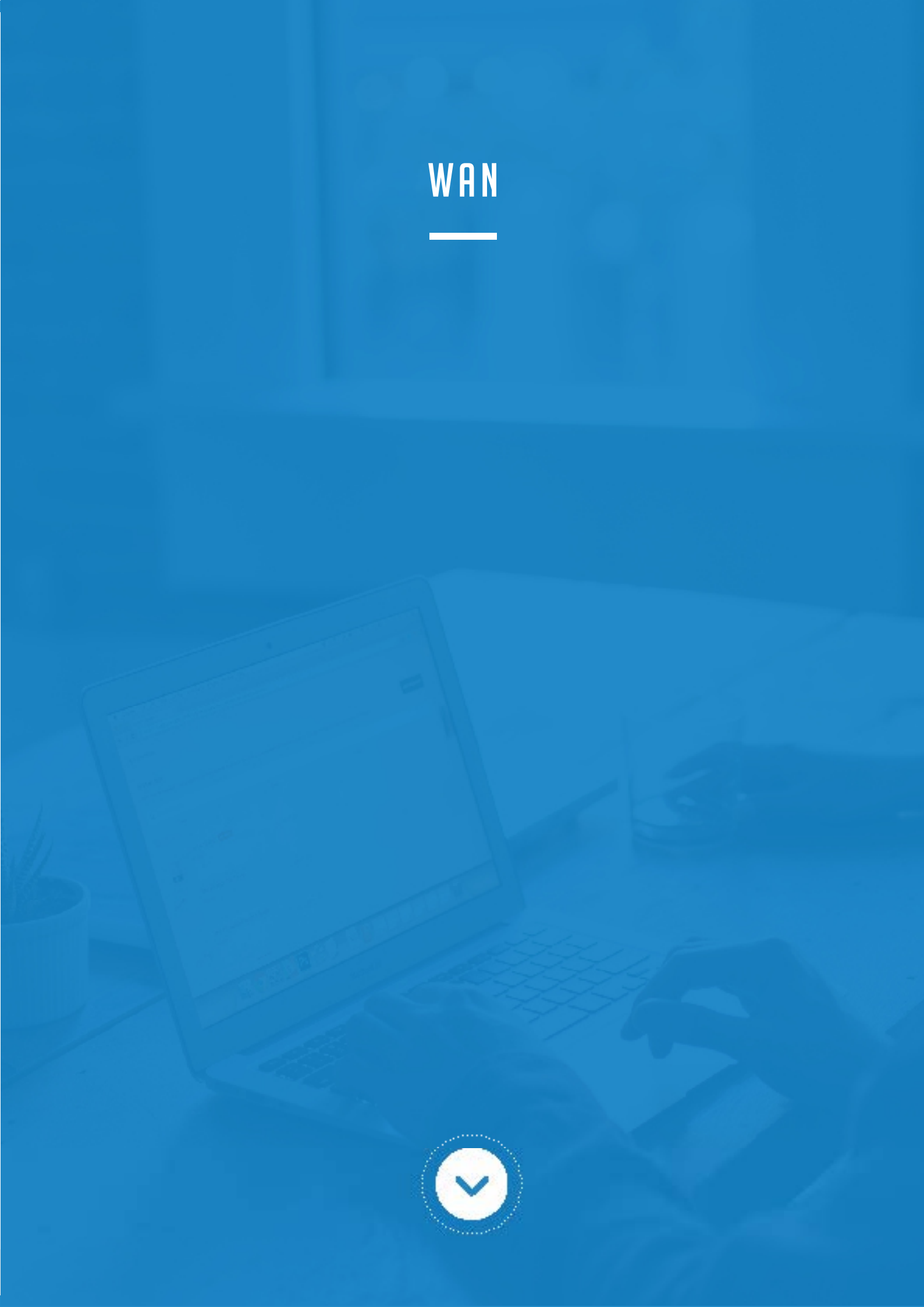
CRÉATION DE LISTES DE CONTRÔLE D'ACCÈS IPV6

- Pour faire vérifier une adresse spécifique, il suffit de lister l'adresse après le mot-clé **host.**
- Pour faire correspondre toutes les adresses, utilisez le mot-clé **any**.
- Pour vérifier uniquement sur le préfixe IPv6, utilisez la notation "slash" pour désigner le nom bre de bits dans la longueur du préfixe. Par exemple, une longueur de préfixe / 24 correspond aux premiers 24 bits de l'adresse IPv6 de 128 bits et tout identifiant d'interface (IID) dans les 24 bits les moins significatifs de cette adresse se situe dans cette plage de préfixe.

ENTRÉES ACL IPV6 IMPLICITES - CES ENTRÉES SONT DANS CHAQUE ACL IPV6

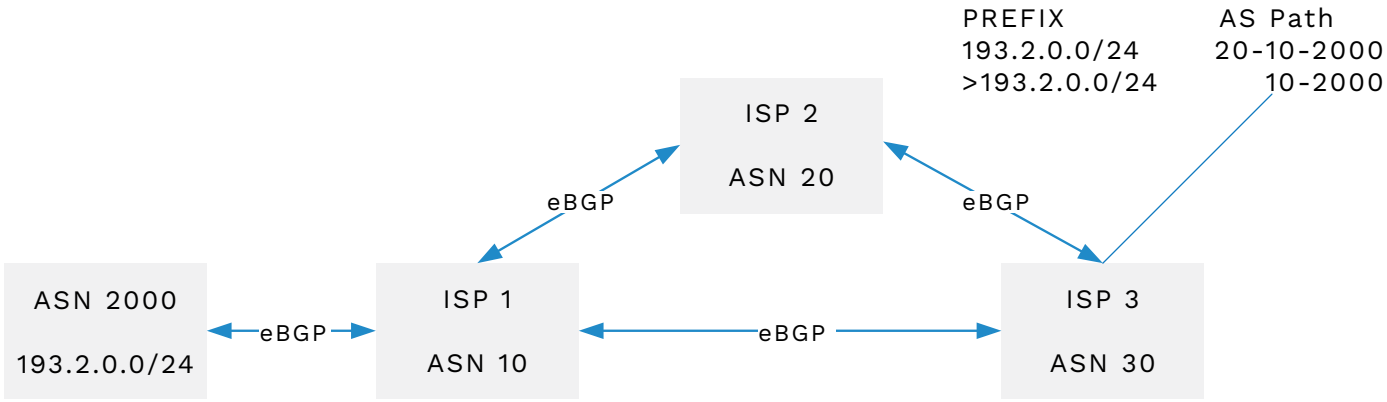
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any

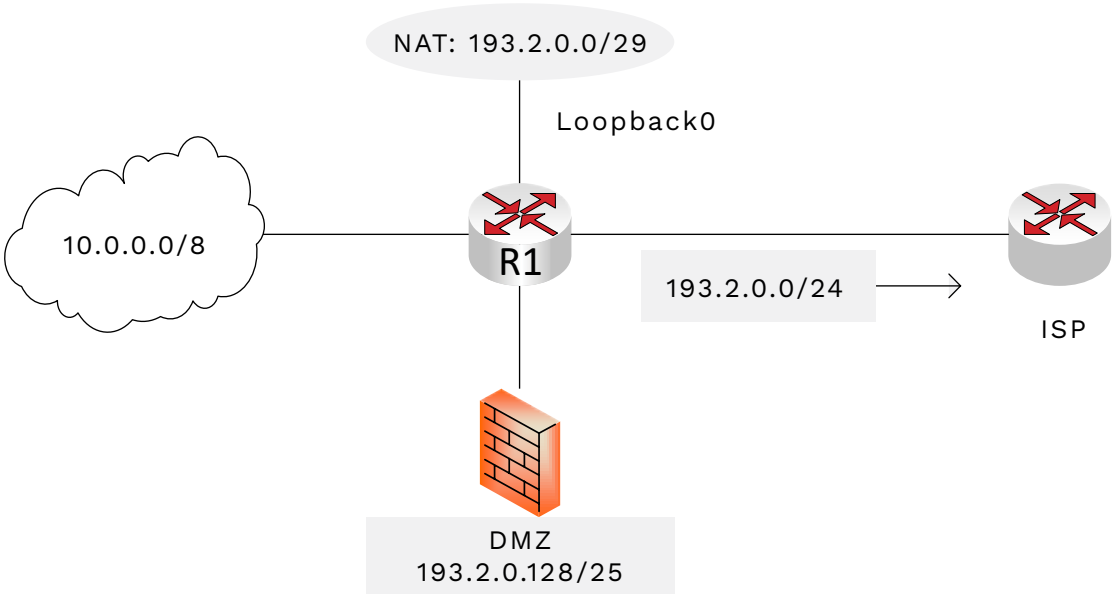
WAN



DÉTERMINATION DU CHEMIN POUR LA CIRCULATION DES PAQUETS IP

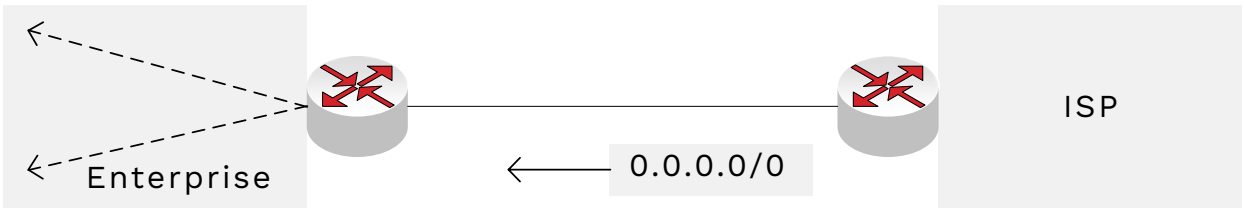
Dans cet exemple, il existe deux chemins vers 193.2.0.0/24 dans ASN 2000. Depuis ISP 3, il existe deux chemins. Un chemin passe par ISP 2, puis sur ISP 1, puis sur ASN 2000. L'autre chemin passe directement par ISP 1 et le chemin parcourant le moins de nombre de Systèmes autonomes (AS) est choisi.





Annonce du sous-réseau 193.2.0.0/24 à L ISP via EBGP
Remarque – le masque de sous-réseau minimum annoncé sur Internet est/24.

Exemple de réseau dit BGP Single-Home Network



Annonce EBGP

Annonce de l'itinéraire par défaut (Default route) à l'intérieur de l'entreprise

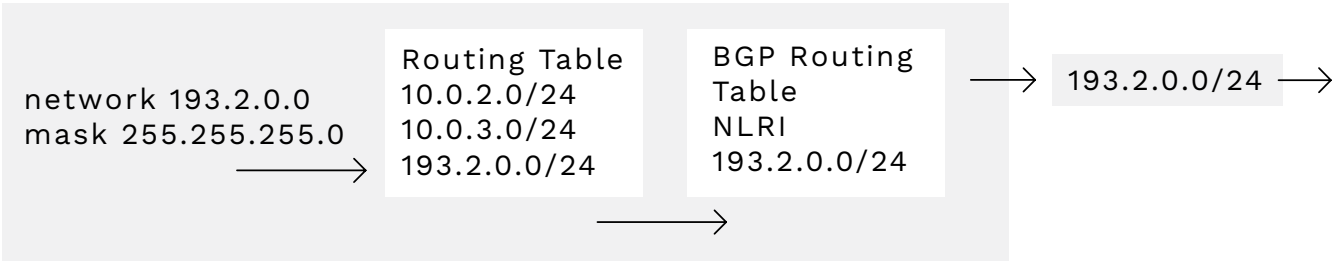
CONFIGURATION BGP

Contrairement aux protocoles de routage intérieurs, la configuration BGP effectue les opérations suivantes:

Définissez les voisins BGP avec la commande **neighbor IP_ADDRESS remote-as ASN** Annoncez les préfixes dans la table BGP apprise par ce qui suit:

- La commande BGP **network**
- Redistribution d'itinéraires à partir d'un autre protocole de routage intérieur
- Préfixes d'apprentissage d'un voisin BGP

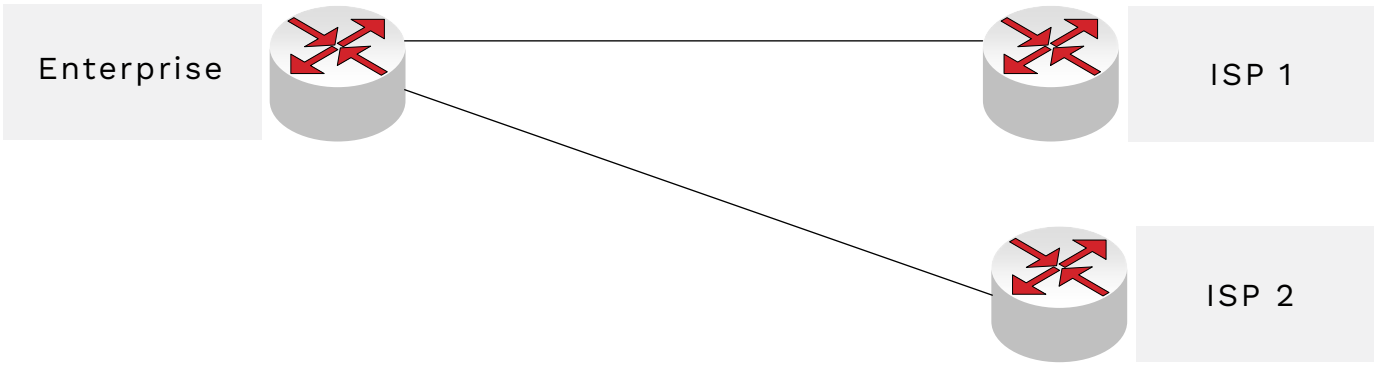
CONFIGURATION DU ROUTEUR



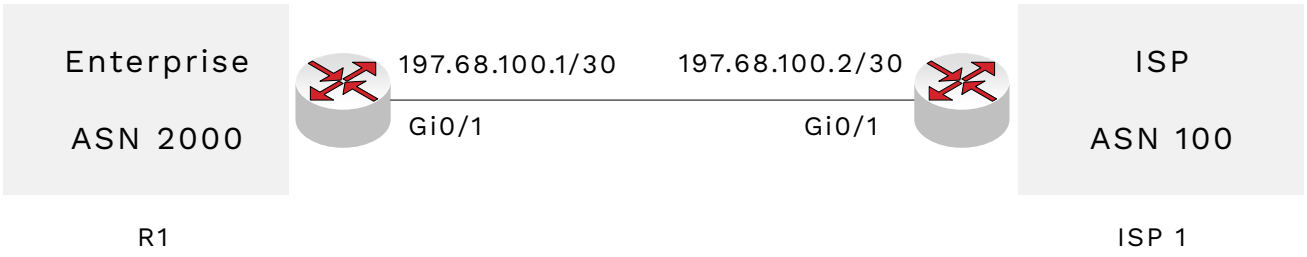
Concept de configuration: la commande BGP network et ses impacts sur la table de routage BGP.

Dual Homed

Single Multihomed



router bgp 100
neighbor 197.68.100.1 remote-as 2000



R1

ISP 1

router bgp 2000
neighbor 197.68.100.2 remote-as 100

Exemple de configuration BGP entre deux routeurs pour une Single Homed connection

EXEMPLE DE L'ÉTAT DE VOISINAGE BGP ET DES CONNEXIONS TCP

R1# **show tcp brief**

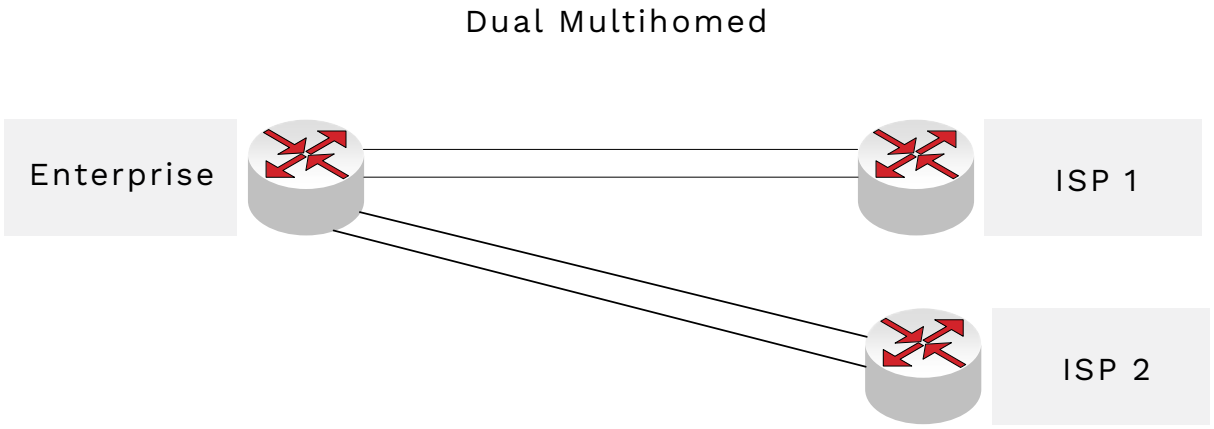
TCB	Local Address	Foreign Address	(state)
0D0D3F00	197.68.100.1.6367	197.61.100.2.179	ESTAB

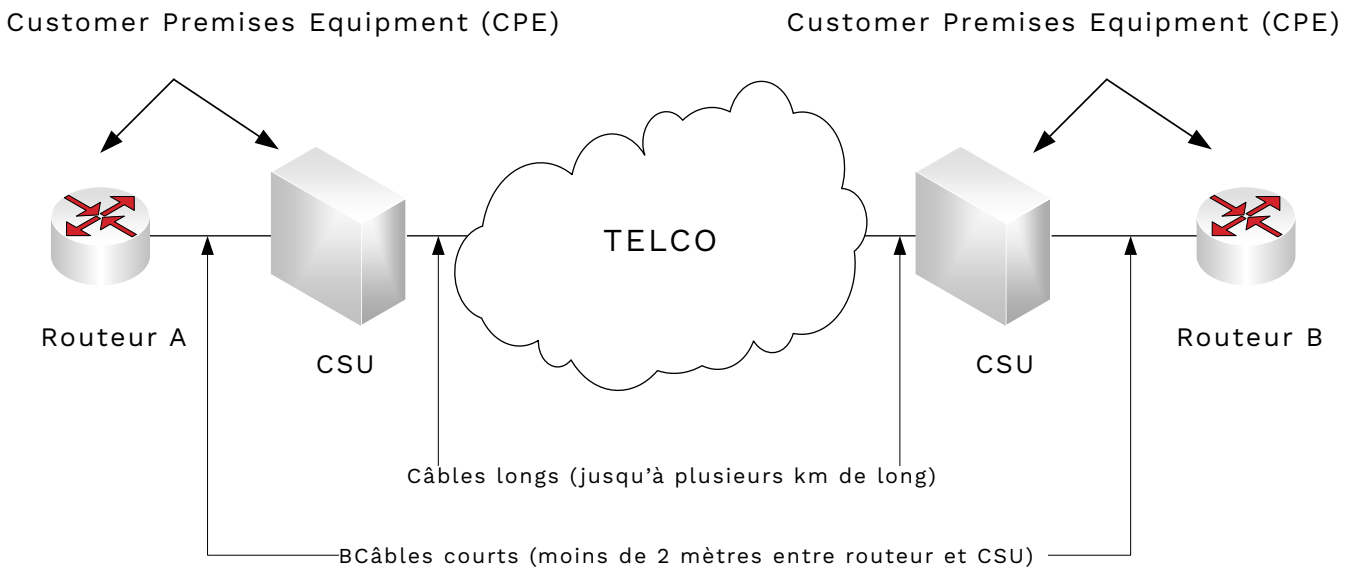
R1# **show ip bgp summary**
BGP router identifier 193.0.2.1, local AS number 2000
BGP table version is 1, main routing table version 1

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
197.68.100.2	4	100	2	2	1	0	0	00:00:49	0

R1#
R1# **show ip bgp**
R1#

DIFFÉRENTS MODÈLES D'INTERNET EDGE





Configuration HDLC – c'est l'encapsulation par défaut pour les ports série sur les routeurs Cisco.

Router A# show running-config
<snip>
!

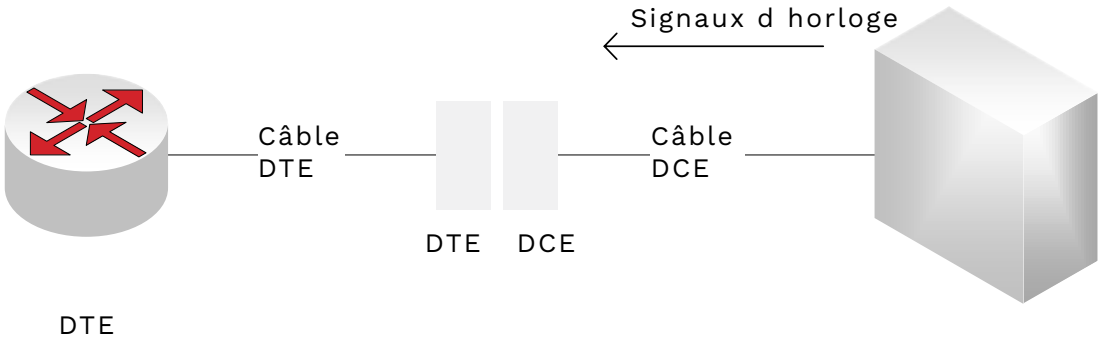
interface Serial0/0
ip address 10.100.1.1 255.255.255.0
description Link to Router B
clock rate 1544000
!

Pour une interface série, sachez que l'encapsulation par défaut sera HDLC sauf indication contraire dans la configuration de l'interface.

Dans la configuration ci-dessus, nous avons une adresse IP, la description et la vitesse (fréquence d'horloge) configurés sur le port série. Cette interface simule un équipement terminal de circuit de données (DCE).

NOMS ET VITESSES CLASSIQUES DES LIGNES DÉDIÉES

Noms de Ligne	Débit binaire ou Vitesse
DSO	64 Kbps
Fractional T1	Multiples de 64 Kbps jusqu à 23
DS1 (T1)	1.544 Mbps (24 DS0)
Fractional DS3 / T3	Jusqu à 28 fois 1.536 Mbps
DS3 (T3)	44.736 Mbps (28 DS1s)
E1	2.048 Mbps (32 DS0s)



DTE

Envoi et reçoit une fois qu'il est synchronisé avec l'horloge du voisin

DCE

L'horloge contrôle la vitesse du routeur pour la liaison WAN

DCE – Data Communications Equipment (Équipement Terminal de Traitement de données) – Fournit l'horloge aux équipements connectés.

DTE – Data Terminal Equipment (Équipement Terminal de Circuit de Données) – Utilise l'horloge fournie pour envoyer et recevoir des données.

POINTS CLÉS SUR LE PROTOCOLE POINT À POINT (PPP - POINT-TO-POINT PROTOCOL)

- Définit un en-tête (header) et en-queue (trailer) pour fournir des trames de données sur un lien.
- Liaisons asynchrones (sans horloge) et synchrones (avec horloge) prises en charge.
- Les protocoles de couche-3 peuvent passer sur le lien en raison d'un champ Type dans l'en-tête.
- L'authentification est intégrée dans le protocole. Il utilise PAP (Password Authentication Proto col) ou CHAP (Challenge Handshake Authentication Protocol).
- Peut être utilisé sur des liaisons série, des liaisons Ethernet point-à-point (modems DSL) et d'autres appareils.
- PPP est pris en charge entre les équipements de différents fournisseurs

Protocoles de Contrôle utilisés par PPP:

LCP – Link Control Protocol – Maintient la liaison PPP et ne s'inquiète pas au sujet des protocoles de couche 3. LCP est adjacente à la couche physique.

NCP – Network Control Protocol – chaque protocole de couche 3 a un NCP correspondant qui facilite la communication entre le LCP et le protocole de couche 3. NCP est adjacent au protocole de couche 3.

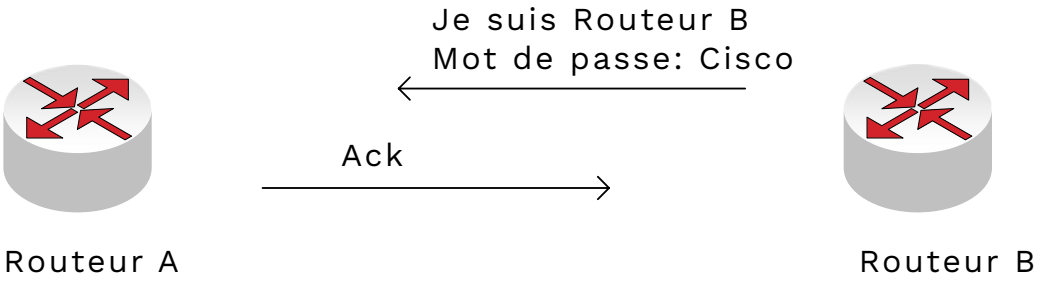
CONFIGURATION PPP SUR UNE INTERFACE SÉRIE

Rappelez-vous que PPP doit être configuré explicitement sur les deux interfaces série. Afin de mettre en place CHAP, un nom d'utilisateur correspondant au nom d'hôte du routeur de destination et un mot de passe doivent être configurés. Dans cet exemple, le routeur A a un nom d'utilisateur et mot de passe pour l'authentification avec le routeur B.

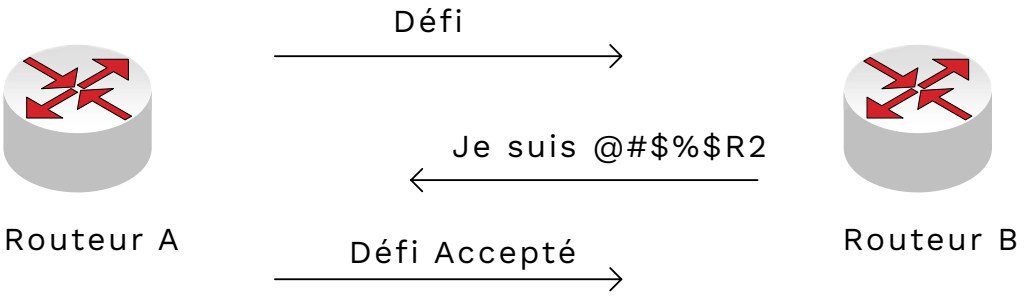
```
RouterA# show running-config
!
username RouterB password
san-fran
<snip>

!
interface Serial0/0
ip address 192.168.100.1
255.255.255.0
encapsulation ppp
ppp authentication chap
!
```

```
RouterA# show running-config
!
username RouterA password
san-fran
<snip>

!
interface Serial0/0
ip address 192.168.100.2
255.255.255.0
encapsulation ppp
ppp authentication chap
!
```

PAP (PASSWORD AUTHENTICATION PROTOCOL) - ENVOIE LE MOT DE PASSE EN CLAIR POUR AUTHENTIFIER L'AUTRE ROUTEUR. DONC AUTHENTIFICATION NON SÉCURISÉ



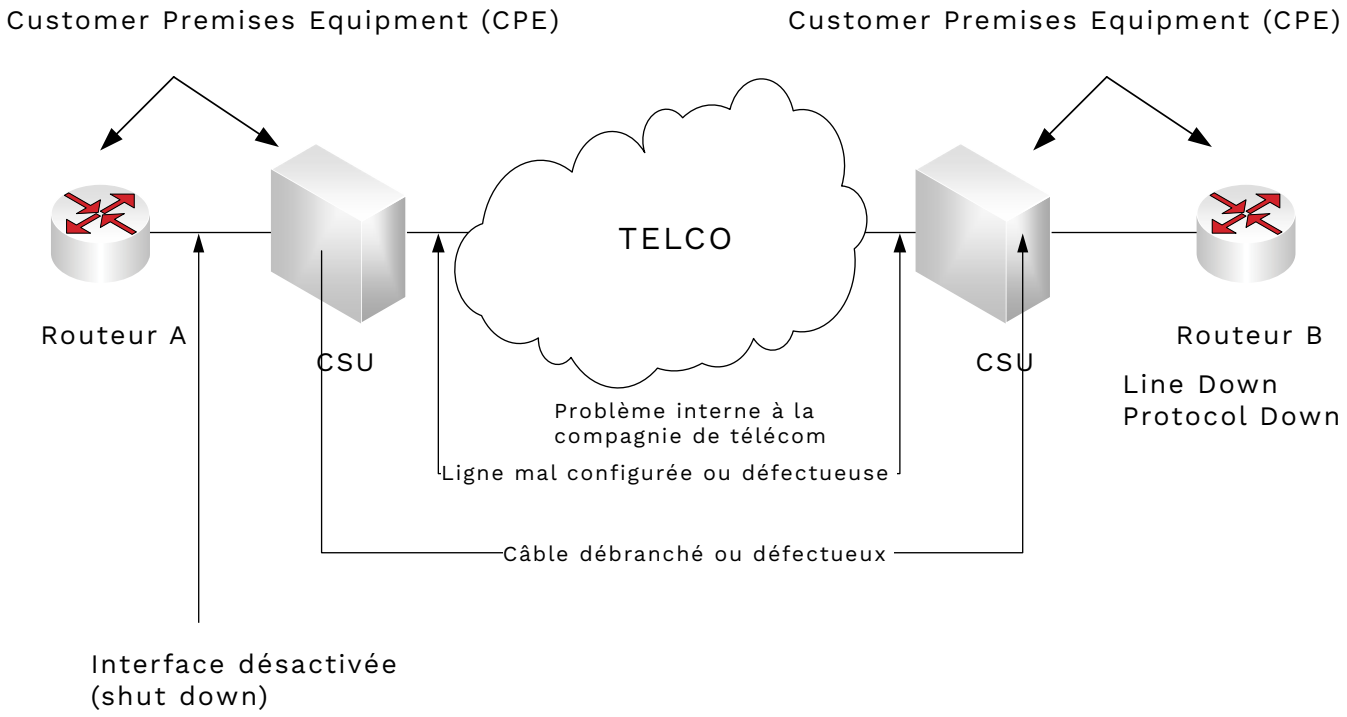
CHAP (CHALLENGE HANDSHAKE AUTHENTICATION PROTOCOL) - LE ROUTEUR ENVOIE SON HASH DE MOT DE PASSE AU ROUTEUR AYANT FAIT LA REQUÊTE



PROBLÈMES PROBABLES AVEC DES LIAISONS SÉRIES SUR LA BASE DES STATUTS D'INTERFACES

Statut Ligne	Statut Protocole	Débit Binaire ou Vitesse
Up	Down – aux deux bouts	Encapsulation dépareillée sur un bout
Up	Down – sur un bout	Aucun keepalive réglé sur une interface tout en utilisant HDLC
Up	Down – aux deux bouts	Echec de l'authentification avec CHAP/PAP

LOCALISATION DES PROBLÈMES POSSIBLES ENTRE ROUTEUR A ET ROUTEUR B



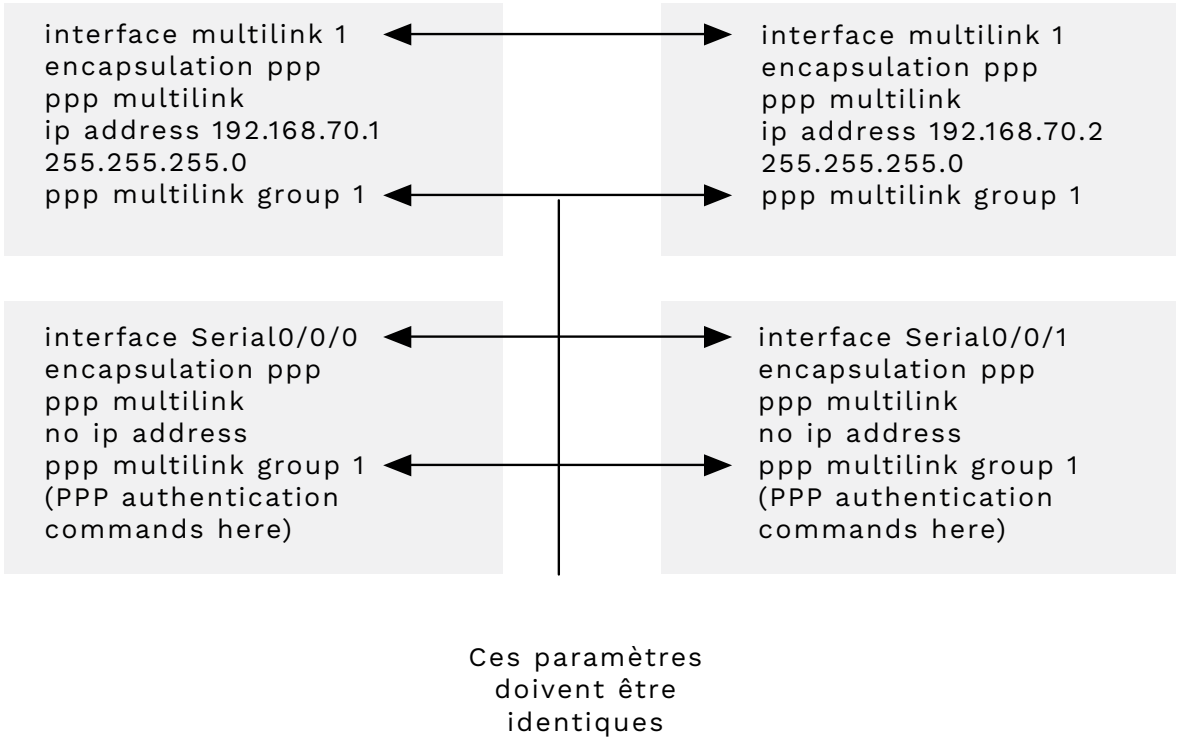
CONFIGURATION DU PPP MULTILINK (MLPPP)

Étape 1: configurez les interfaces multilink correspondantes sur les deux routeurs. Sur ces interfaces, configurez les adresses IP, le routage et d'autres paramètres couche-3.

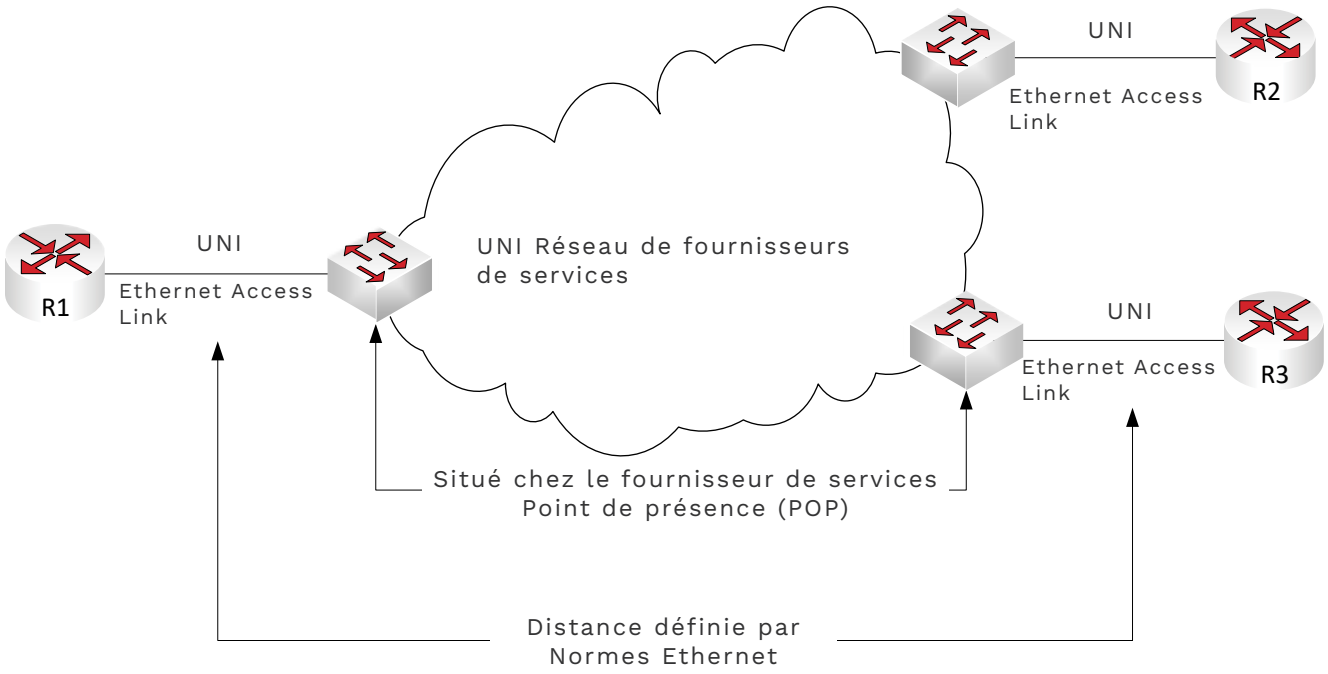
Étape 2: configurez les interfaces série avec les informations de couche 1 comme le taux d'horloge et les informations de couche 2 comme l'authentification PPP.

Étape 3: configurez les commandes PPP sur les interfaces multilink et série et associez les interfaces multilink et série

MLPPP CONFIGURATION

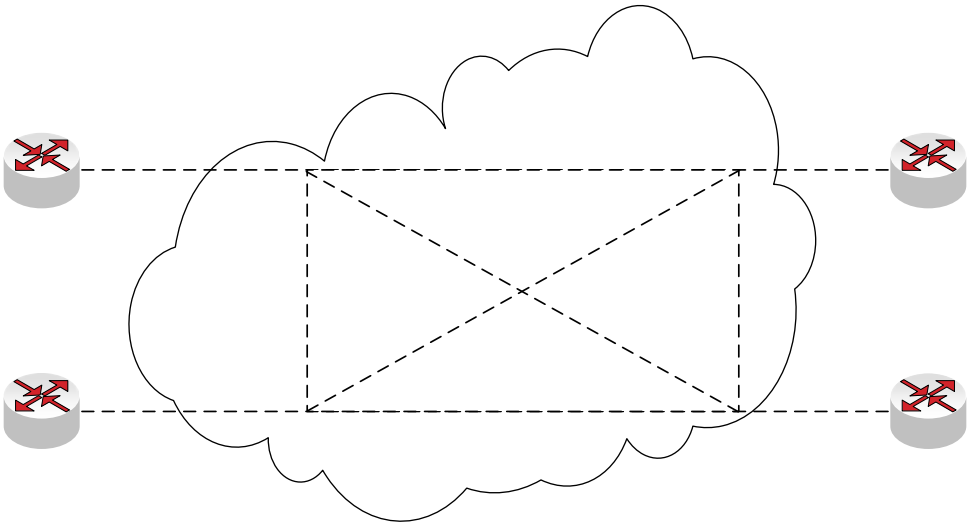


LIENS D'ACCÈS ETHERNET DANS UN SERVICE METRO ETHERNET

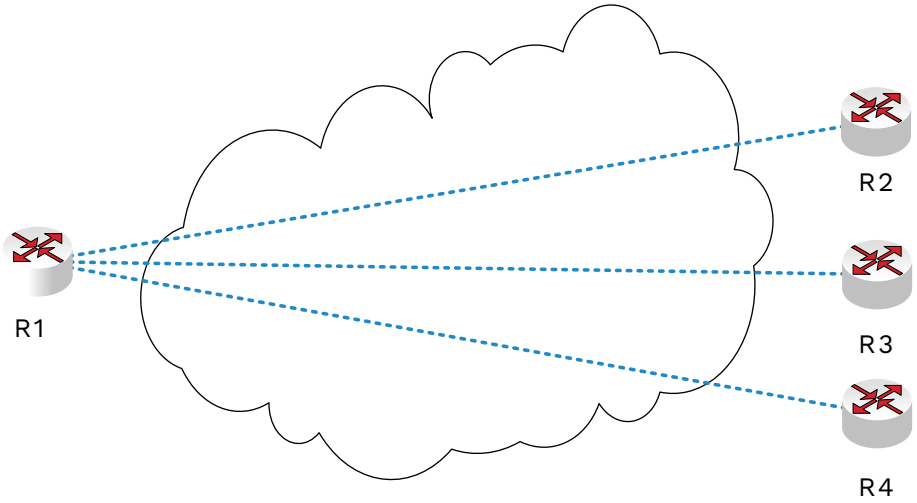


TYPES DE SERVICE MEF (METRO ETHERNET FORUM) ET LEURS DESCRIPTIONS

Nom du service MEF	Nom court du MEF	Conditions de topologie	Description
Ethernet Line Service	E-line	Point to point	Deux appareils CPE peuvent se parler. Ceci est similaire à une ligne louée
Ethernet LAN Service	E-LAN	Full mesh	Agit comme un réseau local où tous les appareils peuvent communiquer avec tous les autres appareils
Ethernet Tree Service	E-Tree	Partial Mesh	Un site central peut communiquer avec un certain nombre de sites distants, mais pas tous



SERVICE METRO-E TREE – TOPOLOGIE HUB ET SPOKE



CONCEPTION D'AIRE OSPF SUR UN RÉSEAU MPLS

L'OSPF super backbone est un élément de conception utilisé lorsque OSPF est le protocole de routage entre les routeurs CE et PE.

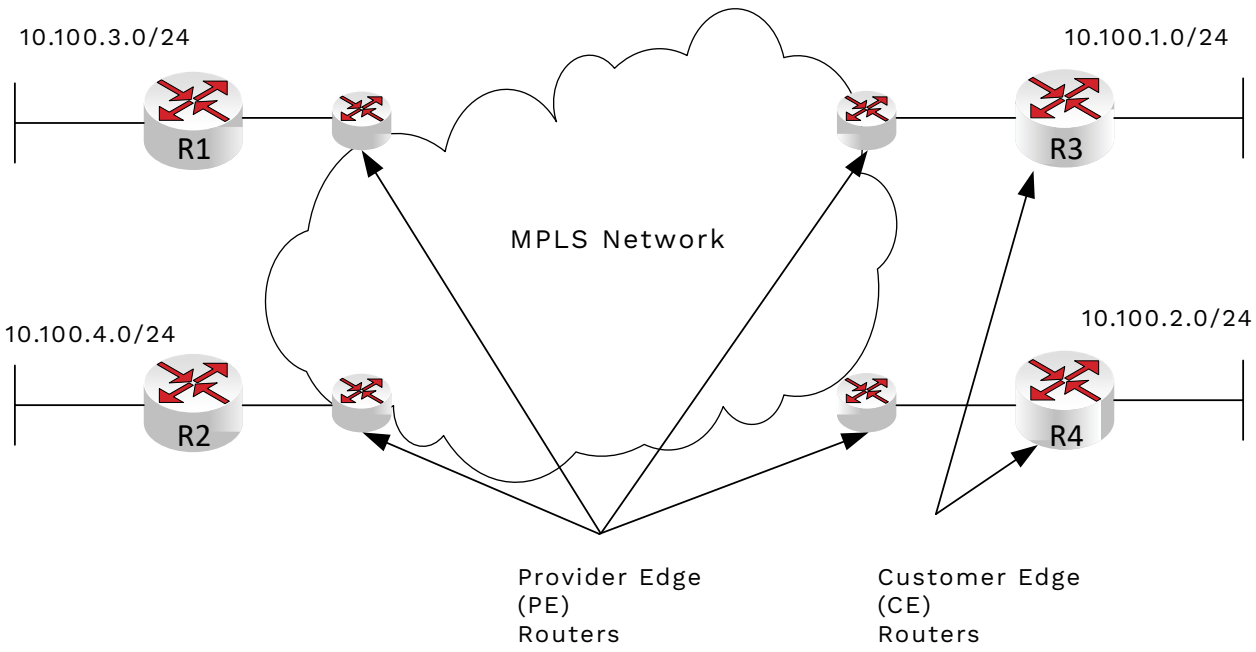
Les PE constituent l'aire super backbone
Les routeurs CE-PE peuvent être dans leurs propres aires non backbone ou dans l'aire backbone.

FOURNISSEUR DE SERVICES RÉSEAU MPLS

Le réseau SP Multiprotocol Label Switching (MPLS) doit connaître ce qui suit sur le réseau
client:

- Besoin de connaître les sous-réseaux du client.
- Utilisera des protocoles de routage IP pour apprendre les routes vers les sous -réseaux du client
- Utilisera les routes sur les sous-réseaux pour prendre des décisions d'expédition.

ARCHITECTURE MPLS LAYER-3 AVEC ROUTEURS PE ET CE

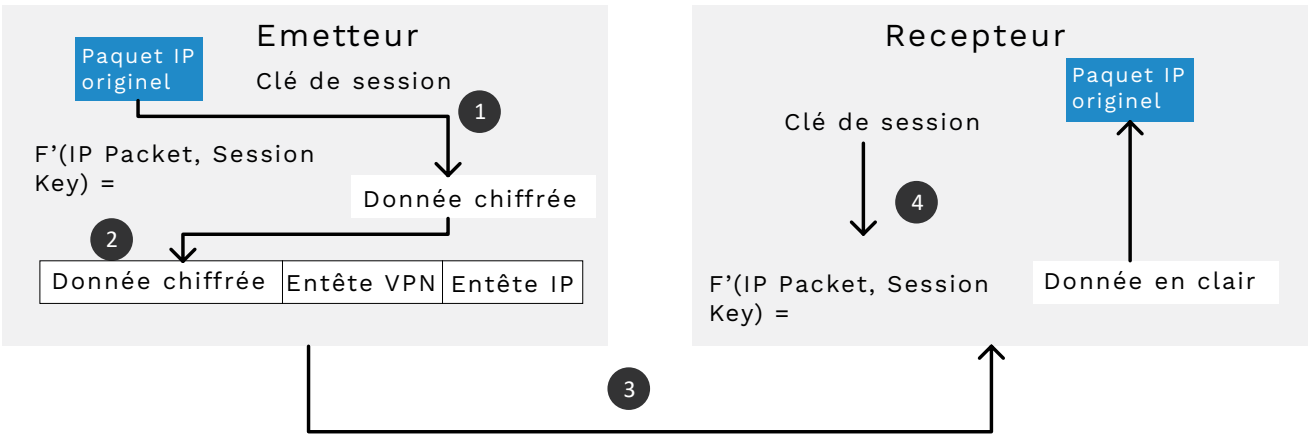


REMARQUES CONCERNANT LES ROUTEURS CE

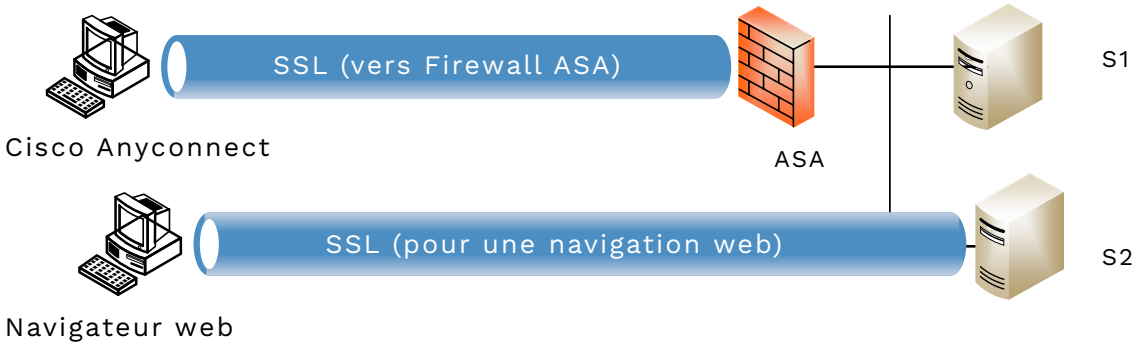
Les routeurs périphériques client (R1 à R4 dans le schéma ci-dessus) effectuent les opérations suivantes:

- Le routeur CE établira une relation de voisinage avec le routeur PE de l'autre côté du lien d'accès.
- Chaque routeur CE ne deviendra pas voisin avec les autres routeurs CE.
- Le réseau fera l'annonce des itinéraires entre les routeurs PE et chaque routeur CE se renseignera sur les itinéraires du routeur PE voisin.

PROCESSUS DE SÉCURITÉ IP DE BASE (IPSEC)



OPTIONS AVEC LE CLIENT VPN SSL



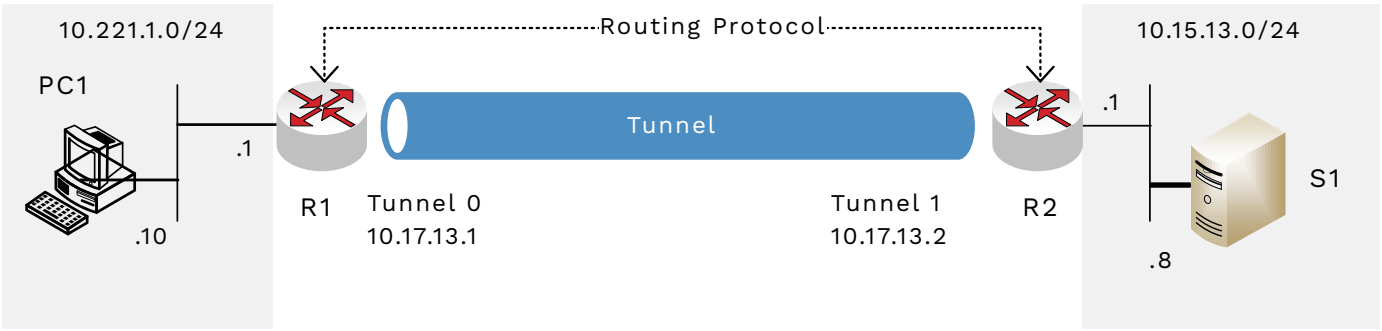
ÉTAPES POUR L'ENVOI D'UN PAQUET VIA IPSEC

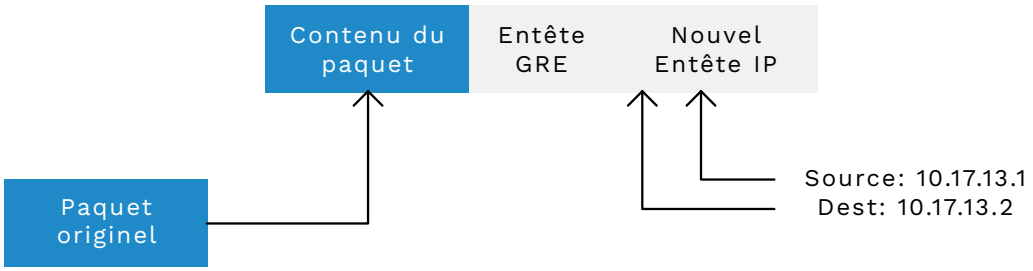
- L'émetteur VPN prend le paquet IP d'origine et la clé de session et alimente les deux paramètres dans l'algorithme de cryptage. Les données chiffrées sont le résultat.
- L'émetteur place les données chiffrées dans un paquet, attache un en-tête IP et un en-tête VPN.
- L'émetteur envoie le nouveau paquet forge vers le récepteur tel qu'un firewall ASA.
- Le récepteur déchiffre les données en utilisant les données chiffrées et la clé de session. La sortie est la donnée en clair et ces données reconstituent le paquet IP d'origine.

LES ITINÉRAIRES (ROUTE) APPRIS PAR UN PROTOCOLE DE ROUTAGE AU TRAVERS D'UN TUNNEL VPN

R1 OSPF Routes		
Subnet	Interface	Next Hop
10.15.13.0/24	Tunnel0	10.17.13.2

R2 OSPF Routes		
Subnet	Interface	Next Hop
10.221.1.0/24	Tunnel1	10.17.13.1

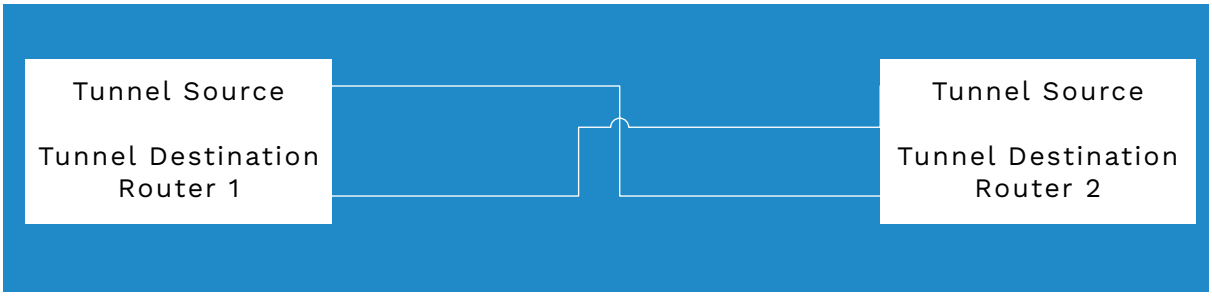




Encapsulation d'un paquet GRE
GRE – Generic Router Encapsulation

Adresse GRE sur un tunnel sécurisé

Adresse GRE sur un réseau insécurisé



DÉPANNAGE DES TUNNELS GRE

L'état de l'interface Tunnel dépend de l'état du tunnel et des interfaces tunnel. Les points suivants doivent être pris en considération sur la source du tunnel:

- Si la commande tunnel source fait référence au nom d'une interface source, l'interface doit obligatoirement avoir une adresse IP attribuée et être dans un état up/up.

- Si la commande tunnel source fait référence à une adresse IP, l'adresse IP doit résider sur le routeur et l'interface affectée à cette adresse IP doit être dans un état up/up.

POUR LA DESTINATION DU TUNNEL

- Si la commande tunnel destination fait référence à une adresse IP, le routeur doit avoir un itinéraire vers cette adresse IP sinon le routeur ne considérera pas l'interface en up/up.

- Si la commande tunnel destination fait référence à un nom d'hôte, le routeur tentera de résoudre le nom d'hôte sur une adresse IP.
    a. Le nom d'hôte ne résout pas à une adresse IP, la commande est rejetée par le routeur.
    b. Si le nom d'hôte résout une adresse IP, l'IOS stocke cette adresse IP dans la configuration et le nom d'hôte n'est pas stocké.

ÉTAPES DE CONFIGURATION GRE TUNNEL

1. Créez une interface tunnel sur chaque routeur à l'aide de la commande **interface tunnel NUMERO.** Notez que le numéro du tunnel est localement significatif.

2. Utilisez la commande **tunnel mode gre** pour définir l'encapsulation GRE sur l'interface du tunnel. (optionnel).

3. Définissez l'adresse IP du tunnel avec la commande **ip address ADRESSE_IP.** Utilisez un sous-réseau. à partir du réseau sécurisé (à l'intérieur du tunnel).

4. Configurez l'IP source du tunnel dans le réseau non sécurisé comme suit:
   a. Utilisez-la commande **tunnel-source ADRESSE_IP** pour définir l'adresse IP
   b. **Utilisez-la** commande **tunnel-source SOURCE** pour définir l'adresse IP faisant référence à l'une des interfaces du routeur (par exemple Gi0/1).

5. Utilisez la commande **tunnel destination ADRESSE_IP (ou HOSTNAME)** pour définir l'adresse de destination du routeur terminant le tunnel.

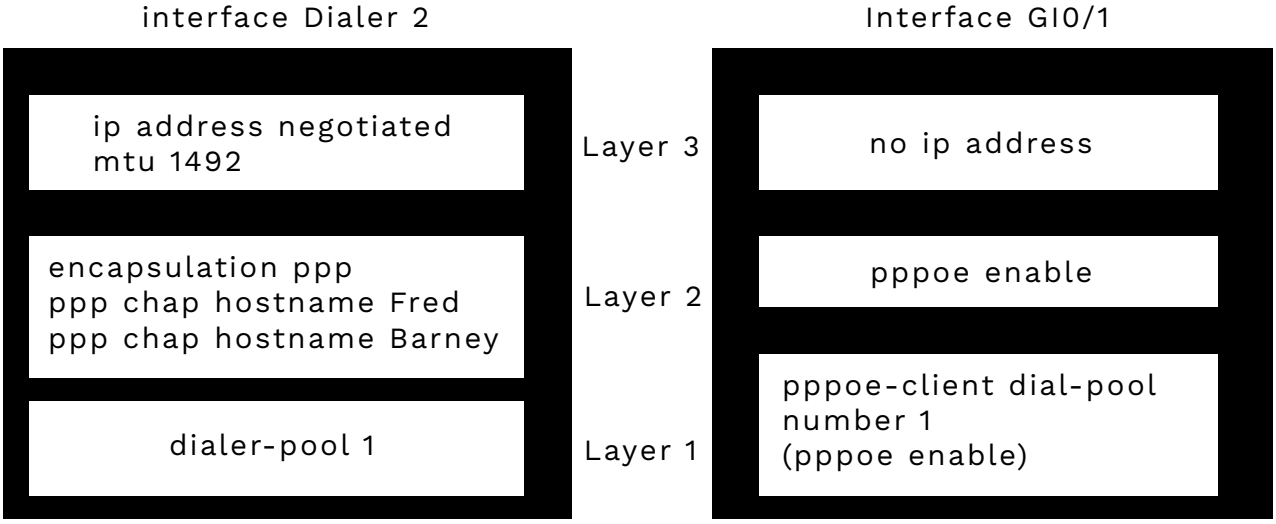
6. Définissez les routes en définissant des itinéraires statiques ou en au torisant un protocole de routage dynamique.

CONFIGURATIONS PPPOE DIALERS ET LAYER 1

- (config à droite) L'interface Gi0/1 est placée dans le groupe dialer (numérotation) 1 avec la commande **pppoe-client dial-pooL-number 1.**

- (config à gauche) L'interface Dialer 2 fait référence au dialer 1 avec la commande **dialerpool 1.**

PANNE DE CONFIGURATION PPPOE SUR LE ROUTEUR R1



RÉSUMÉ DE LA CONFIGURATION PPPOE

Détails de la couche 1

1. Configurez une interface Dialer
    a. Utilisez-la commande **interface dialer NUMERO** pour créer l'interface. Utilisez un numéro qui n'est pas déjà utilisé pour une autre interface dialer
    b. Utilisez la sous-commande **dialer-pool NUMERO** pour se référer à un pool d'interface Ethernet pour PPPoE.

2. Configurez l'interface physique (s)
    a. Utilisez la sous-commande **pppoe-client dial-pool-number NUMERO** pour ajouter l'interface à l'interface dialer.

Détails de la couche 2

3. Configurez PPP sur l'interface Dialer
    a. Activer PPP sur l'interface avec la commande **encapsulation ppp**
    b. Définissez le nom d'utilisateur PPP avec la commande **ppp chap hostname NOM**
    c. Définis sez le mot de pas se PPP avec la commande **ppp chap password PASSWORD**

4. Configurez PPPoE sur l'interface Ethernet (s)
    a. Activer PPPoE avec la commande **pppoe enable** sur les interfaces concernées.

Détails de la couche 3

5. Définissez l'adresse IP sur l'interface Dialer
    a. Utilisez la commande **ip address negotiated** pour que le routeur suive les adresses IP
    b. Réglez **mtu 1492** pour permettre les 8 octets supplémentaires requis par PPPoE.

6. Désactiver IP sur les interfaces Ethernet
    a. Utilisez la commande de l'interface **no ip address** pour supprimer les adresses IP de l'interface Ethernet (s).

SOMMAIRE DU DÉPANNAGE PPPOE

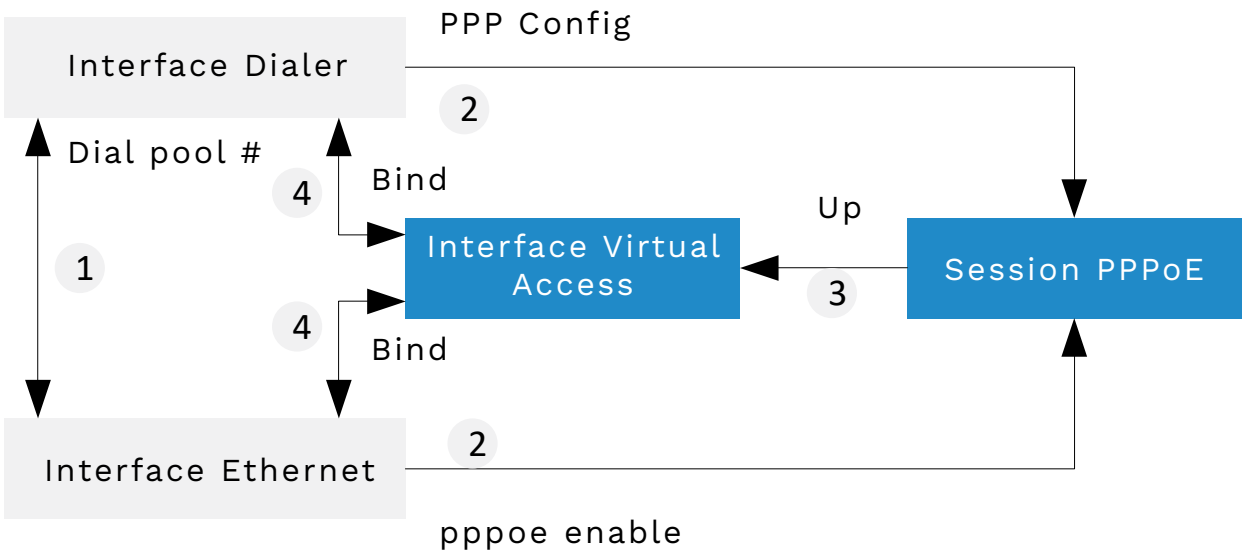
Layer 1: si la commande **show pppoe session NUMERO** ne donne rien, vérifiez les interfaces physiques et assurez-vous qu'elles sont dans un état up/up.

Layer 2: si la commande **show pppoe session NUMERO** donne une sortie, mais ne répertorie pas l'interface virtuelle, vérifiez la configuration de la couche 2, y compris le mot de passe ppp.

Layer 2: si la commande **show interfaces dialer NUMERO** affiche un état up / up (spoofing), vérifiez la configuration PPP sur l'interface de numéroteur.

Layer 2: pour s'assurer que PPPoE fonctionne, la commande s**how pppoe session** doit afficher un état up, trois interfaces listées dans les abréviations et les adresses MAC des deux routeurs.
Layer 3: si **show interfaces** ou **show ip interfaces brief** ne répertorie pas une adresse IP pour l'interface de numérotation, vérifiez les commandes de la couche 3

CONCEPTS ET VÉRIFICATION PPPOE



POINTS-CLÉS SUR LA FIGURE CI-DESSUS

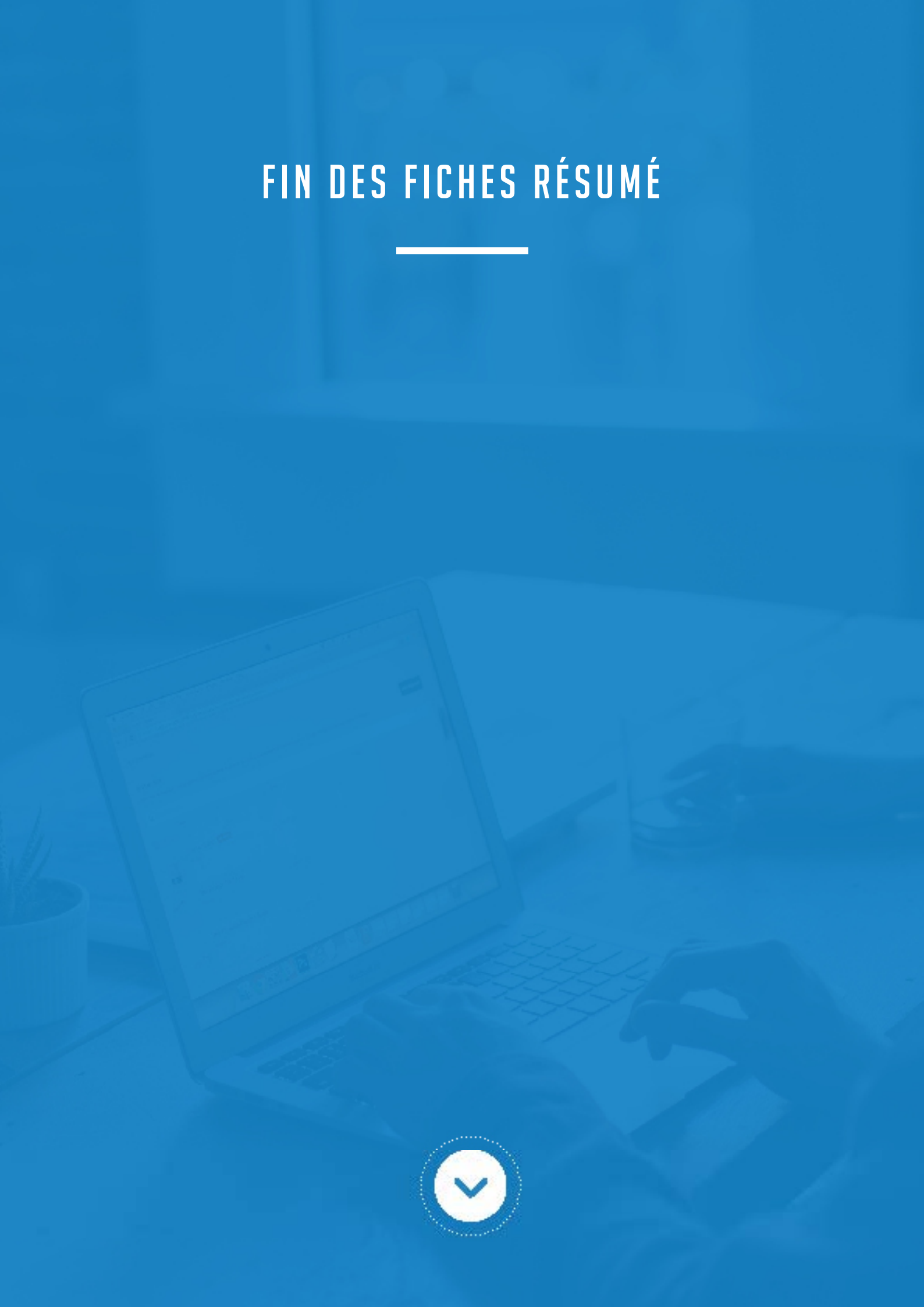
- 1. L'interface de numérotation et l'interface Ethernet sont associées en référençant le même **dialer pool member.**
- 2. IOS utilise la configuration PPP et la commande **pppoe enable** sur les interfaces Ethernet pour configurer et configurer le lien PPP.
- 3. Une fois la session PPP terminée, l'interface Virtual Access est créée.
- 4. L'interface Virtual Access est alors liée à l'interface dialer et à l'interface Ethernet

PPPOE FAUX POSITIFS

Recherchez ce qui suit lors du dépannage PPPoE:
l'interface de numérotation affichera toujours un état d'interface up/up (spoofing) que PPPoE fonctionne ou non.

Adresse IP de l'interface physique: l'interface physique Ethernet n'a pas d'adresse IP. Recherchez la commande **no IP adress** sous la configuration de l'interface Ethernet.

FIN DES FICHES RÉSUMÉ



Et après ?

Je vous donne rendez-vous sur
http://reussirsonccna.fr pour découvrir
tout ce qu'il faut savoir sur les certifications
et les nouveautés Cisco CCENT et CCNA !

REUSSIRSONCCNA.FR