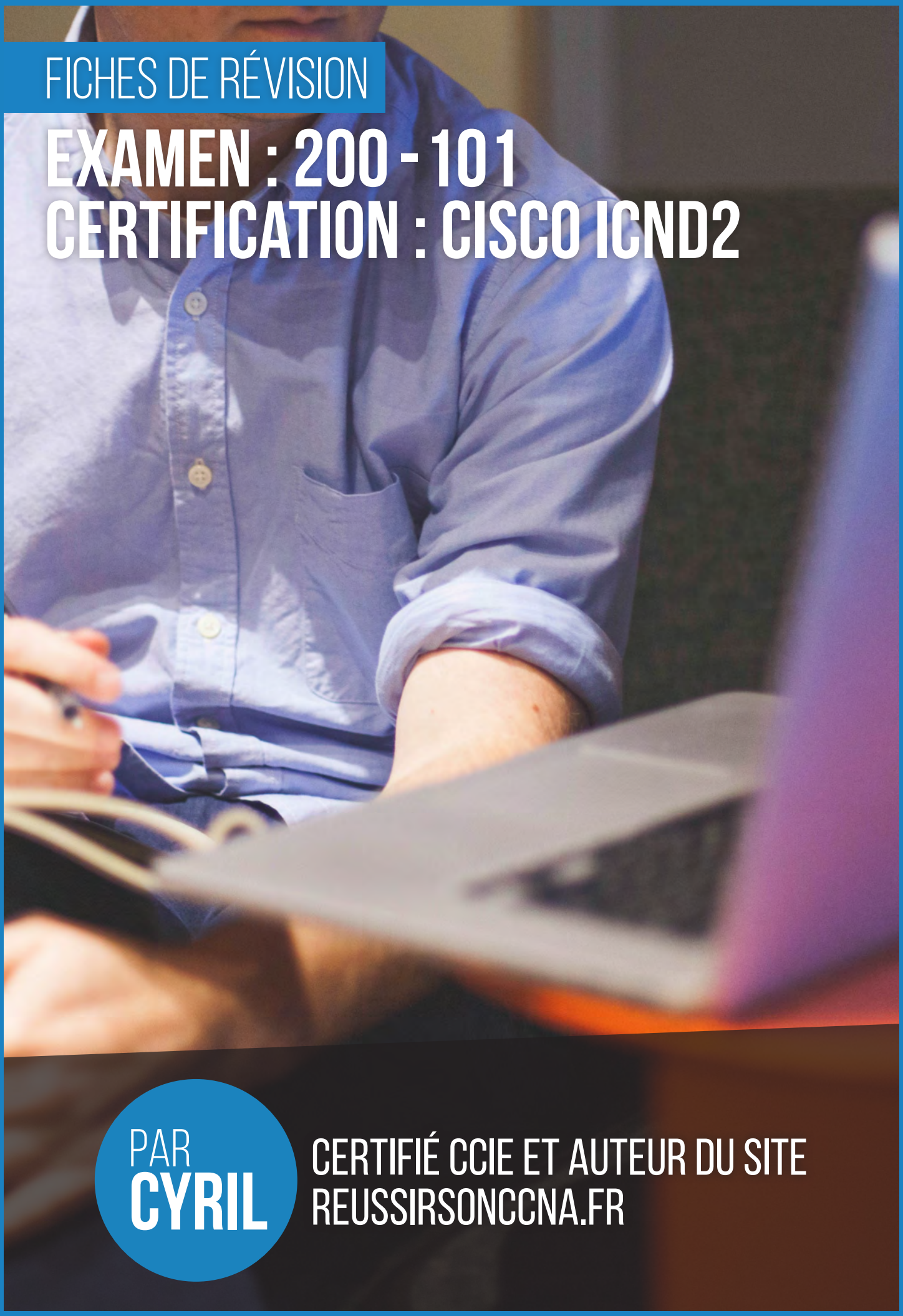
FICHES DE RÉVISION

EXAMEN : 200 - 101
CERTIFICATION : CISCO ICND2



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.

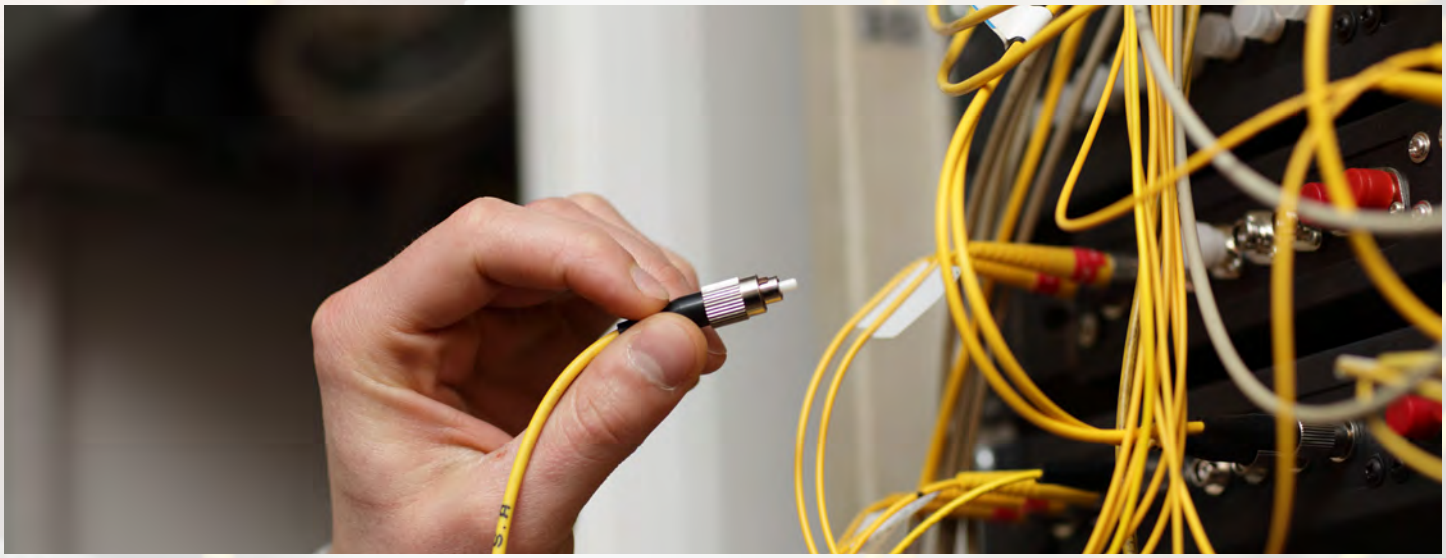
Toute personne procédant à une utilisation du contenu de ce guide, sans une autorisation expresse et écrite de l'auteur, encourt une peine relative au délit de contrefaçon détaillée à partir de l'article L 335-2 du même Code.

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 (ICND1) puis le CCNA (ICND1 + ICND2)

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 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

TÉLÉCHARGER LE GUIDE.

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 ? (inclus dans ce présent document)
- Quels sont les types de questions ? (inclus dans ce présent document)
- Comment optimiser sa mémoire? (inclus dans ce présent document)
- Comment pratiquer les labs ?
- Comment monter son propre lab Cisco ?
- Quel score atteindre pour être certifié(e) ? (inclus dans ce présent document)
- 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
- 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) 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.

INSCRIPTION ET DÉROULEMENT DE L'EXAMEN

La certification est **valide pour une durée de 3 ans**. Une fois ce délai passé, il faut repasser l'examen afin de prolonger la certification . Mais la plupart des personnes ne s'arrêtent pas au CCNA, ils continuent sur les certifications suivantes. L'avantage est que toute réussite à un examen supérieur revalide le CCNA pour 3 ans supplémentaires. Sympa !

L'examen CCNA dure **2h pour 45 à 55 questions** sous forme de QCM et de simulation de lab (configurer un switch par exemple). Si vous n'êtes pas anglophone, vous aurez droit à **30 minutes supplémentaires** car ce n'est pas votre langue natale.

Les QCM peuvent se présenter sous les formes suivantes:

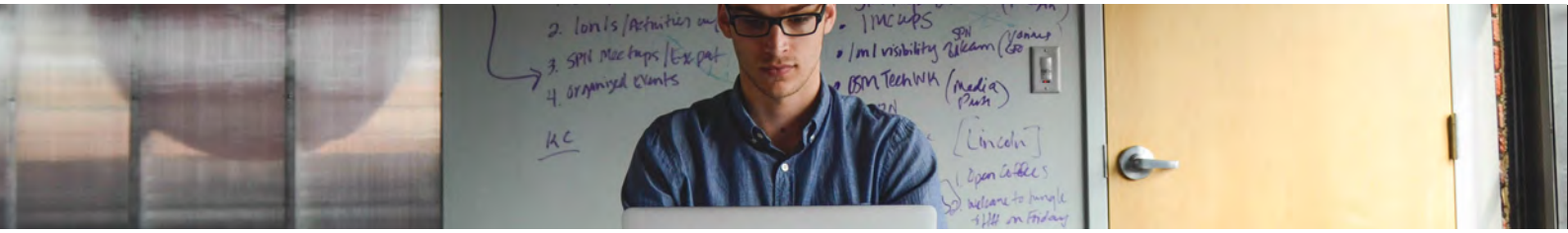
- choix unique
- choix multiple (dans ce cas, on vous précise le nombre de réponses souhaitées, 2, 3 ou 4)
- drag & drop (ou glisser-déposer). Permet de faire le lien entre 2 tableaux par exemple
- remise des éléments dans l'ordre
- …

Les labs sont généralement un accès en console à un ou plusieurs équipements avec un choix limité de commandes (n'oublions pas que c'est un simulateur logiciel et non de vrais équipements). Ne vous étonnez pas si en tapant une commande, vous avez un message d'erreur vous signifiant que la commande est inconnue. Elle existe bien mais vous n'en avez pas besoin pour résoudre l'exercice. Les commandes de complétion (via la touche Tabulation) et d'aide (via la touche ?) ne sont pas disponibles lors des labs, c'est voulu. Cisco souhaite que les gens connaissent par cœur les commandes principales.

L'examen est mélangé de questions de type QCM et de labs donc tout est possible: commencer directement avec un lab de configuration ou avec une question QCM.

Remarque importante:

vous n'avez pas le droit d'amener des notes, votre téléphone ou votre ordinateur portable. On vous fournit un stylo et un papier plastifié que vous remettrez à la fin de l'examen.



QUELS SONT LES TYPES DE QUESTIONS ?

On est jamais mieux servi que par soi-même et Cisco l'a bien compris : Cisco propose une simulation pour vous montrer visuellement comment se passe l'examen et le style de question sur lesquelles vous pouvez tomber. Je le trouve très bien fait, alors autant en profiter. Pour voir cette animation, **cliquez ICI !**

Si le lien ne fonctionne pas, tapez ces mots clés dans Google pour récupérer le lien a jour : **cisco CCNA tutorial swf.**

QUEL SCORE ATTEINDRE POUR ÊTRE CERTIFIÉ(E) ?

La question qui revient souvent via les blogs, forum et discussion lors des formations est la suivante:

Quel score faut-il pour être certifié(e) CCENT ?

C'est une excellente question et le plus amusant (ou stressant) est qu'il n'y a pas de score précis à avoir lors des examens Cisco car cela dépend essentiellement des questions proposées lors de l'examen.

Cisco a une base de données gigantesque de questions et pioche dedans pour l'examen. En fonction des questions piochées et de leur pondération, le score final requis est différent. C'est aussi pour cela que votre voisin d'examen n'aura pas du tout les mêmes questions.

Si on regarde sur le site officiel de Cisco, les informations suivantes sont mentionnées (traduites de l'anglais):

DÉTAIL DE L'EXAMEN ICND2

- **Nombre de questions:** **50-60**
- **Types de question:** choix multiple avec une seule ou plusieurs bonnes réponses, glisser/déposer, simulateur de lab contenant de la configuration (configure terminal), de la vérification (à base de commande show), des valeurs à entrer (par exemple donner une adresse IP)
- **Score à obtenir:** varie selon les questions proposées lors de l'examen mais **c'est entre 800 et 850 sur 1000**
- **Durée:** **75 minutes + 30 minutes** pour les non-anglophones

QUELS SONT LES PRÉREQUIS POUR LA CERTIFICATION ?

Il n'y a pas de prérequis pour passer le ICND2 que ce soit bien clair.

Ah si ! Il y en a un et de taille : savoir utiliser un ordinateur…

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.

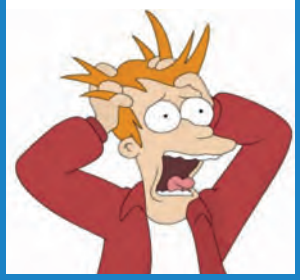
Alors je vous arrête tout de suite, je ne vais pas vous recommander tel ou tel médicament plus ou moins douteux que l'on trouve sur Internet et curieusement non autorisé en France et d'autres pays.

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.

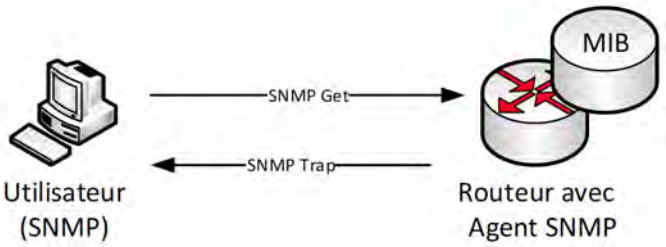
FICHES RÉSUMÉ

Les fiches résumés ICND2 sont découpés 7 grands domaines: l'administration, la commutation, le routage IPv4 , le routage IPv6, la résolution de problème, la redondance et VPN.

7 DOMAINES	SOUS-DOMAINE
L'ADMINISTRATION	Administrer les équipements
	Gérer les IOS et licences
LA COMMUTATION	Implémentation de la commutation
	Spanning-tree
LE ROUTAGE IPV4	OSPF
	EIGRP
LE ROUTAGE IPV6	OSPF
	EIGRP
LA RÉSOLUTION DE PROBLÈME	Problème de commutation
	Problème de routage
LE WAN	Frame-relay
	Autre type de WAN
REDONDANCE ET VPN	Redondance de passerelle
	VPN

ADMINISTRATION IOS

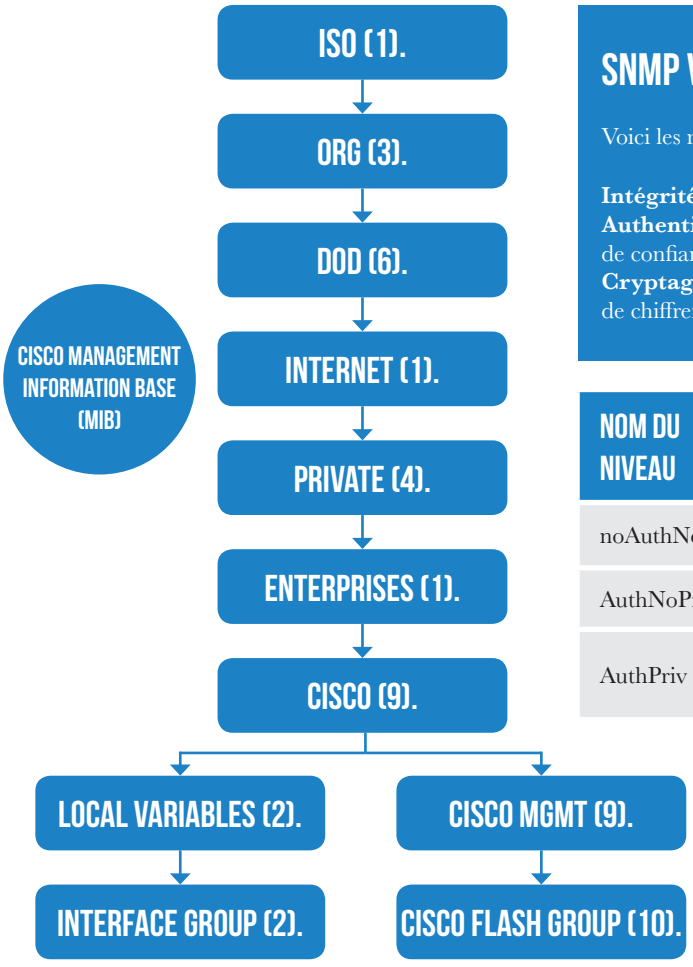
GESTION DE RÉSEAU



POINTS CLÉS SUR SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP):

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

Chaque appareil atteint par SNMP a une base de données de valeurs appelée Management Information Base (MIB). Cette base de données contient des valeurs qui peuvent être interrogées par SNMP.



SNMP VERSION 3

Voici les nouvelles fonctionnalités de SNMPv3:

Intégrité de Message - veille à ce que le paquet ne change pas pendant le transit.
Authentification – les paquets SNMP proviennent d'un hôte / emplacement connu et de confiance.
Cryptage - Si le paquet est capturé ou reniflé, le contenu ne peut pas être lu sans la clé de chiffrement.

NOM DU NIVEAU	MOT-CLÉ SNMP-SERVER	MÉTHODE D'AUTHENTIFICATION	CRYPTAGE
noAuthNoPriv	noauth	Nom d'utilisateur	Aucun
AuthNoPriv	auth	MD5 ou SHA	Aucun
AuthPriv	priv	MD5 ou SHA	DES ou DES-56

GESTION DE RÉSEAU

CONFIGURATION SNMPV2C SUR UN ROUTEUR CISCO

1) Configurer la chaîne de communauté et les droits d'accès avec la commande server community chaîne RO | RW. Remarque, RO est en lecture seule et RW est en lecture et écriture. Tous les appareils du réseau doivent avoir la même chaîne de communauté SNMP.

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

3) Configurer 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) Utiliser 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:

Configurer le routeur R1 avec une chaîne de communauté SNMP de valeur L!fetime2, avec des autorisations en lecture seule. Définir également l'emplacement comme Paris et le contact local comme John Smith. Créer une ACL avec le nom RESTRICT_SNMP permettant uniquement le sous-réseau de gestion de réseau de 172.30.21.0/24.

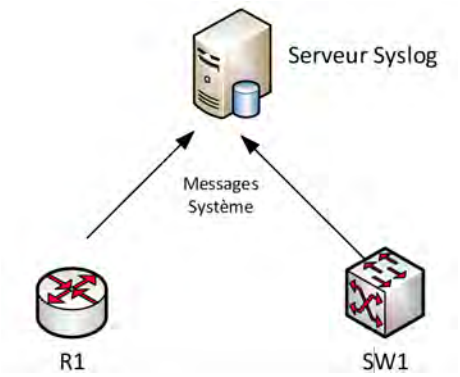
LA CONFIGURATION EST ILLUSTRÉE CI-DESSOUS:

```
!
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 John Smith
!
```

JOURNAL DES MESSAGES SYSTÈME (SYSLOG)

Chaque appareil réseau crée des messages au cours des opérations quotidiennes.

Alors que les messages peuvent être stockés sur chaque appareil, l'espace de stockage est limité. Pendant le dépannage, il est souhaitable de disposer d'un référentiel central pour les journaux système. Les routeurs Cisco peuvent être configurés pour envoyer des syslogs à un(des) serveur(s) central(aux) pour analyse.



NIVEAU	NOM DU NIVEAU	RAISON POUR LE MESSAGE
0	Urgence	Le système peut être complètement à l'arrêt
1	Alerte	Peut nécessiter une action immédiate
2	Critique	Un événement critique s'est produit
3	Erreur	L'élément a eu une erreur
4	Avertissement	L'événement peut nécessiter de l'attention
5	Notification	Un événement significatif s'est produit
6	Information	Message d'événement normal
7	Débogage	Sortie d'une commande de débogage

EXTRAIT DE SYSLOG CONFIG 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
```

GESTION DE RÉSEAU

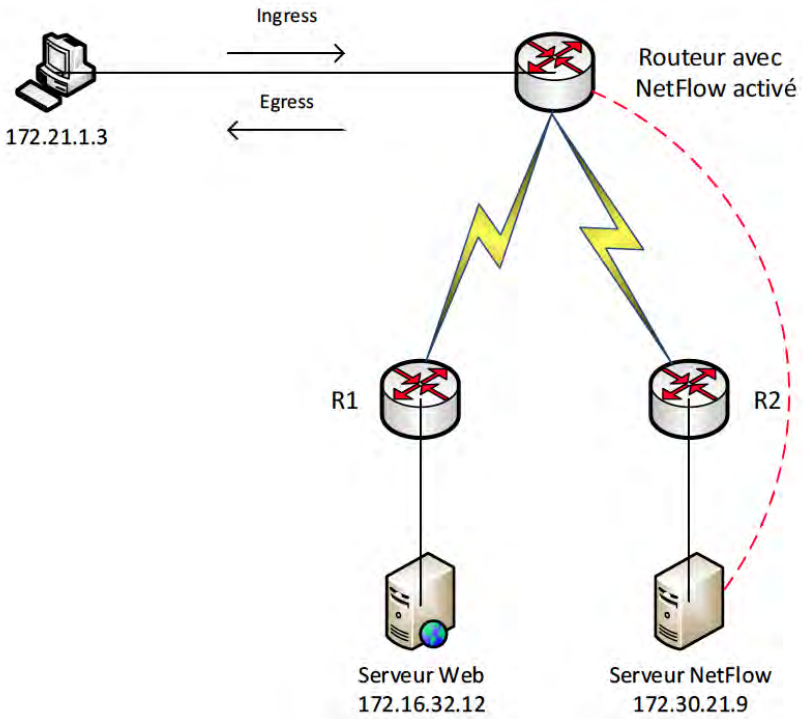
NETFLOW

NetFlow est utilisée pour recueillir des statistiques de trafic entre deux hôtes.
NetFlow compte les paquets et mesure le flux de trafic à travers ses interfaces. Un routeur compatible NetFlow peut classer les flux de trafic basé sur l'adresse IP de source ou de destination, les ports, le type de service de marquage ou le type de protocole de couche 3.

Configurer NetFlow sur un routeur en utilisant l'interface GigabitEthernet0/0 et envoyer les informations au serveur 172.30.21.9 en utilisant la version 9 de NetFlow.

CONFIGURATION CI-DESSOUS:

```
!
interface GigabitEthernet0/0
ip flow ingress
ip flow egress
!
ip flow-export destination 172.30.21.9
ip flow-export version 9
ip flow-export source loopback 0
!
```



GESTION DES FICHIER IOS

QUATRE TYPES DE MÉMOIRE DE ROUTEUR ET LES FONCTIONS DE CHACUN

RAM	FLASH	ROM	NVRAM
Mémoire de travail Configuration courante (running-config)	Logiciel Cisco IOS	Programme Bootstrap et ROMMON	Configuration de démarrage (startup-config)

SÉQUENCE DE DÉMARRAGE D'UN ROUTEUR

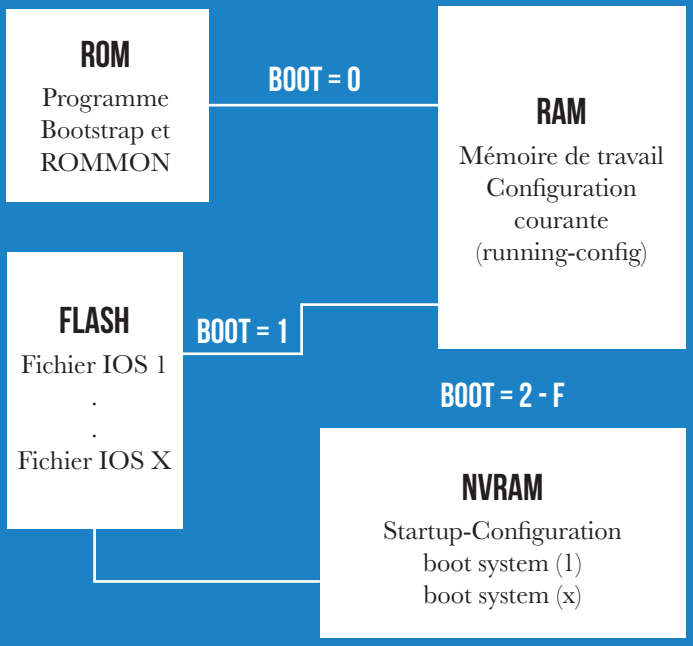
Quand un routeur est allumé, les choses suivantes se déroulent
1) Le Power On Self Test (POST) est effectué pour connaître tous les composants matériels et vérifier leur fonctionnement
2) Le routeur charge le programme boostrap de la ROM dans la RAM et l'exécute.
3) Le bootstrap décide quelle version d'IOS exécuter et démarre l'IOS à partir de la mémoire Flash.
4) Le logiciel IOS charge le fichier startup-config de la NVRAM et le copie dans le fichier running-config dans la RAM.

Remarque: Si les étapes 1 ou 2 échouent, Cisco TAC devra être appelé pour réparer le routeur.

CHOISIR QUEL IOS CHARGER?

Le registre de configuration contrôle un grand nombre d'éléments, y compris l'ordre de démarrage et la vitesse de transmission initiale du port de la console. Par défaut, le registre de configuration est 0x2102 ce qui met le port de la console à 9600 bps et charge une image IOS. Le dernier chiffre dans le registre de configuration détermine l'ordre de démarrage.

Si le dernier chiffre est 0, charger ROMMON
Si le dernier chiffre est 1, charger le premier fichier IOS trouvé en flash
Si le dernier chiffre est de 2 à F, essayer chaque commande boot system dans le fichier startup-configuration dans l'ordre. Si cela échoue, charger le premier fichier ISO trouvé dans flash



NOMS, FONCTIONS ET EMPLACEMENTS DES FICHIERS DE CONFIGURATION

NOM DU FICHIER DE CONFIGURATION	FONCTION	EMPLACEMENT DE STOCKAGE
Startup-config	La configuration initiale chargée par le routeur pendant toute recharge (reload)	NVRAM
Running-config	Enregistre les commandes de configuration courante et les mises à jour lorsque de nouvelles commandes sont entrées dans l'appareil	RAM

GESTION DES FICHIER IOS

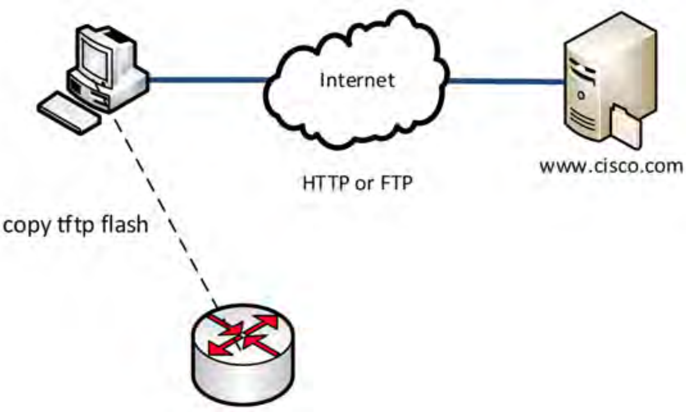
SORTIE DE SHOW VERSION

La commande show version montre beaucoup de choses importantes dans le routeur. Elles sont les suivantes:

Version d'IOS

Durée de fonctionnement (uptime) du dispositif
Motif de la dernière recharge
Temps de rechargement d'IOS
La source actuelle de l'IOS (flash, TFTP)
Quantité de RAM
Nombre et types d'interfaces
Quantité de mémoire Flash
Les paramètres actuels et futures de configuration-register

RouterA# show version
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), **Version 15.2(4)M1**,
RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 26-Jul-12 20:54 by prod_rel_team
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
R2 uptime is 44 minutes
System returned to ROM by reload at 19:44:01 UTC Tue Feb 12 2013
System restarted at 19:45:53 UTC Tue Feb 12 2013
System image file is «flash:c2900-universalk9-mz.SPA.152-4.M1.bin»
Last reload type: Normal Reload
Last reload reason: Reload Command
<snip>
Cisco CISCO2901/K9 (revision 1.0) with **483328K/40960K bytes of memory.**
Processor board ID FTX1628837T
2 Gigabit Ethernet interfaces
4 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity enabled.
255K bytes of non-volatile configuration memory.
3425968K bytes of USB Flash usbflash1 (Read/Write)
250880K bytes of ATA System CompactFlash 0 (Read/Write)
<snip>
Configuration register is 0x2102



Mise à jour des logiciels de routeur via PC et TFTP:
1) Récupérer le logiciel à partir de cisco.com
2) Définir l'adresse Ethernet du PC pour être dans le même sous-réseau que l'adresse Ethernet du routeur
3) Démarrer l'application serveur TFTP du PC
4) Lancer la commande copy tftp flash sur la console du routeur pour démarrer le transfert et suivre les instructions.

RouterA# **copy tftp flash**
Address or name of remote host []? **192.168.1.1**
Source filename []? **c3700-universalk9-mz.SPA.152-4.M1.bin**
Destination filename [c3700-universalk9-mz.SPA.152-4.M1.bin]?
Accessing tftp://192.168.1.1/c3700-universalk9-mz.SPA.152-4.M1.bin...
Loading c3700-universalk9-mz.SPA.152-4.M1.bin from 192.168.1.1 (via GigabitEthernet0/1):
!!
!!!!!!![OK - 74503236 bytes]

RouterA# **show flash**
-#- --length-- -----date/time------------------- path
1 74503236 Jun 12 2014 19:06:54 +00:00 **c3700-universalk9-mz.SPA.151-4.M4.bin**
2 97794040 Nov 19 2013 14:02:50 +00:00 **c3700-universalk9-mz.SPA.152-4.M1.bin**
78909440 bytes available (172297280 bytes used)

GESTION DES FICHIER IOS

COMMANDES BOOT SYSTEM

COMMANDE BOOT SYSTEM	RÉSULTAT
boot system flash	Le premier fichier du système de fichiers flash est chargé
boot system flash nom-defichier	Le routeur charge l'IOS spécifique avec le ***nom-de-fichier*** à partir du système de fichiers flash
boot system tftp 172.20.1.1 nom-de-fichier	Le routeur charge l'IOS spécifique avec le ***nom-de-fichier*** à partir du serveur TFTP à 172.20.1.1

RÉCUPÉRATION DE MOT DE PASSE

Alors que le processus de récupération de mot de passe varie à travers les appareils, le processus de base reste le même. Voici une procédure de base de récupération de mot de passe:
1) Éteignez le routeur
2) Retirez la carte Compact Flash du routeur
3) Allumez le routeur
4) Attendez l'invite rommon 1>
5) Insérez soigneusement la carte Compact Flash dans le routeur
6) Mettez le registre de configuration à 0x2142 avec la commande **confreg 0x2142**
7) Lancez la commande reset à l'invite rommon pour réinitialiser le routeur
8) Attendez qu'IOS entre en mode setup. Entrez no à l'invite.
9) Connectez-vous au routeur sans mot de passe et entrez enable pour avoir l'accès administrateur
10) Chargez la configuration de démarrage dans la RAM avec la commande copy startup-configuration running-configuration et appuyez sur Entrée aux deux invites.
11) Réinitialisez les mots de passe conformément aux politiques de mot de passe
12) Sauvegardez la nouvelle configuration en exécutant la commande copy running-configuration startup-configuration.

R1#! 1) **L'utilisateur se dirige vers le routeur et éteint le routeur**
R1#! 2) **L'utilisateur supprime toute la mémoire flash**
R1#! 3) **L'utilisateur rallume le routeur**
R1#
System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC enabled

! 4) Plusieurs lignes de messages omises: ROMMON initialisé
Readonly ROMMON initialized

! 5) rommon 1 > confreg 0x2142
You must reset or power cycle for new config to take effect
rommon 2 >

! 6) **L'utilisateur se dirige vers le routeur et rebranche la mémoire flash.**
rommon 3 > reset
System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2011 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2901/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC enabled
! Plusieurs messages d'initialisation d'IOS omis

--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!

! 9) **L'utilisateur se connecte à la console et établit un nouveau mot de passe secret.**
Router>
Router>**enable**

! 10) **L'utilisateur copie le startup-config pour que le routeur fasse son travail normal**
Router# copy startup-config running-config
Destination filename [running-config]?
3297 bytes copied in 0.492 secs (6701 bytes/sec)

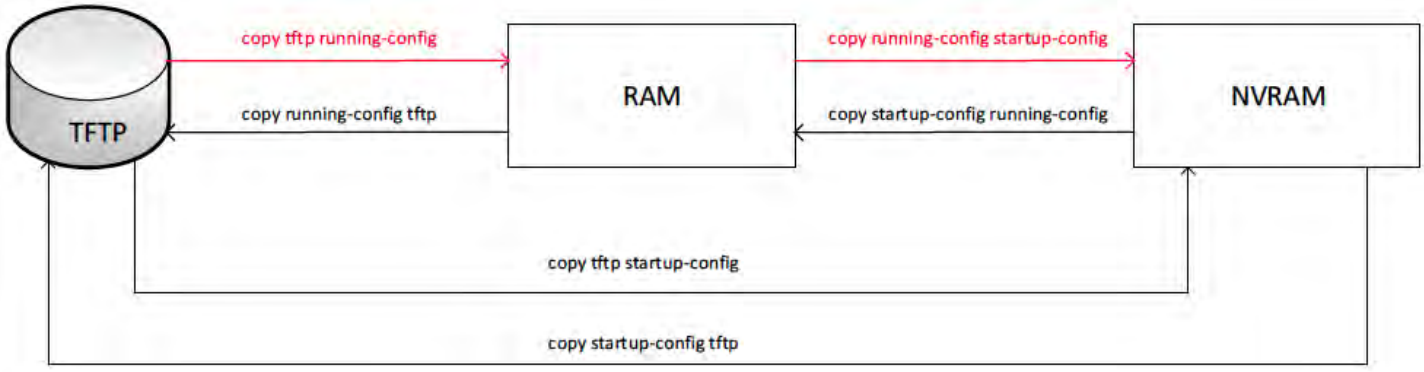
! 11) **L'utilisateur change le mot de passe enable secret oublié**
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# enable secret cisco
R1(config)# ^Z
R1#

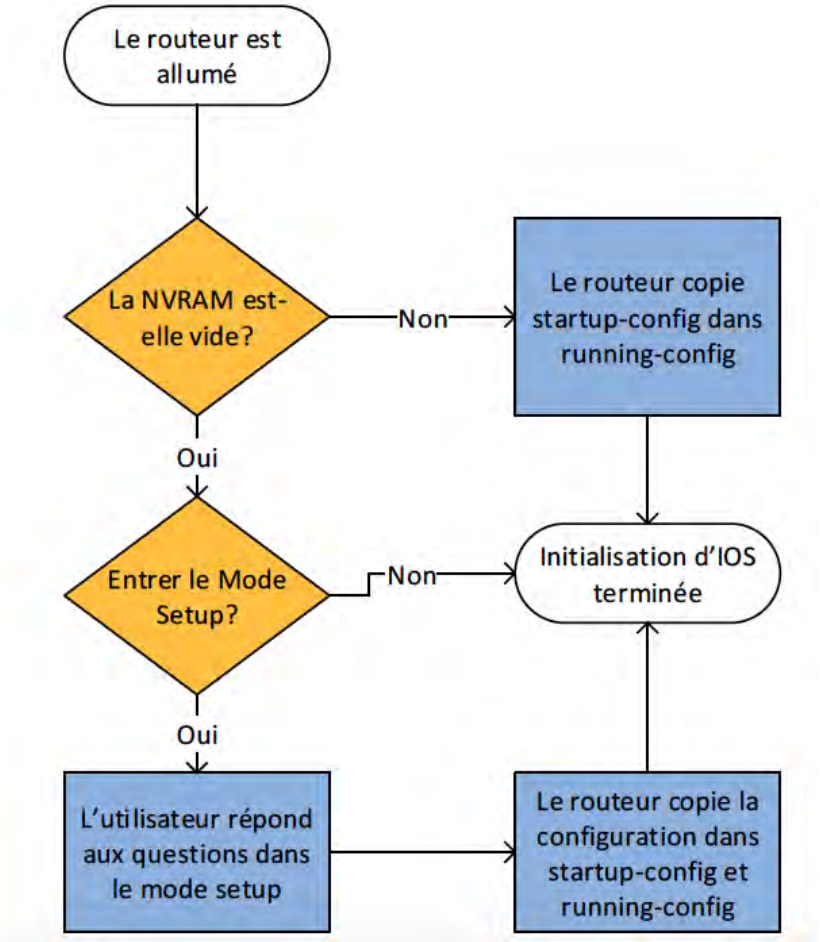
! 12) L'utilisateur enregistre ses modifications du mot de passe
R1# copy running-config startup-config
Destination filename [startup-config]?
3297 bytes copied in 0.492 secs (6701 bytes/sec)

! 13) L'utilisateur remet le registre de configuration à sa valeur normale 0x2102
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# config-reg 0x2102
R1(config)# ^Z

GESTION DES FICHIER IOS

Les commandes Copy et leurs emplacements





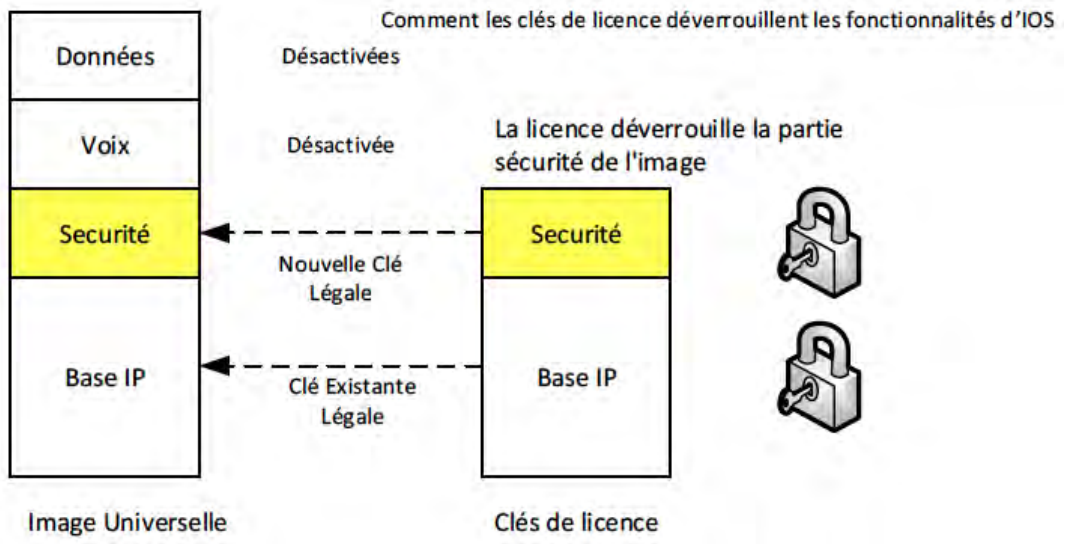
FLUX LOGIQUE POUR LE CHARGEMENT DE LA CONFIGURATION DANS LE ROUTEUR

LICENCE IOS

PARADIGME D'ORIGINE DES LICENCES CISCO

Dans le cadre du paradigme d'origine des licences Cisco, il existaient différentes versions du logiciel basé sur l'ensemble des fonctionnalités. La version de base est une base IP avec la Voix, la Sécurité, et des améliorations de données. Chacune de ces combinaisons était un fichier séparé.

En vertu du nouveau régime de licences, un fichier IOS est placé dans le routeur. Celui-ci est appelé l'image universelle et des parties de l'image universelle sont déverrouillées avec les fichiers de licence fournis par Cisco.



LICENCES POUR ENSEMBLE DE TECHNOLOGIES

LICENCE DE TECHNOLOGIE	FONCTIONALITÉS DÉVEROUILLÉES
Ipbasek9 (IP Base)	Fonctions IOS de base
Datak9 (data)	MPLS, ATM, et autres protocoles
Uck9 (Unified Comms)	VoIP, Téléphonie IP
Securityk9 (Security)	Pare-feu, IPSec, VPN

Utiliser la commande show license udi pour montrer les licences des composants de l'IOS dans ce routeur

```
RouterA# show license udi
Device# PID              SN              UDI
------------------------------------------------------------------------
*0      CISCO2901/K9     FTX165113H0     CISCO2901/K9:FTX165113H0
```

UTILISER SHOW LICENSE POUR VOIR LES LICENCES IOS ACTIVES DANS LE ROUTEUR

R1# show license
Index 1 Feature: ipbasek9
Period left: Life time
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium
Index 2 Feature: securityk9
Period left: Not Activated
Period Used: 0 minute 0 second
License Type: EvalRightToUse
License State: Not in Use, EULA not accepted
License Count: Non-Counted
License Priority: None
Index 3 Feature: uck9
Period left: Not Activated
Period Used: 0 minute 0 second
License Type: EvalRightToUse
License State: Not in Use, EULA not accepted
License Count: Non-Counted
License Priority: None
Index 4 Feature: datak9
Period left: Not Activated
Period Used: 0 minute 0 second
License Type: Permanent
License State: Active, Not in Use
License Count: Non-Counted
License Priority: Medium
! Lignes omises par souci de concision; 8 autres licences de fonctionnalités disponibles

LICENCE IOS

ÉTAPES POUR METTRE À JOUR OU AJOUTER DES COMPOSANTS DE LICENCE CISCO:

1) Au portail de licences Cisco, entrez l'UDI du routeur en utilisant les informations de la commande show license.

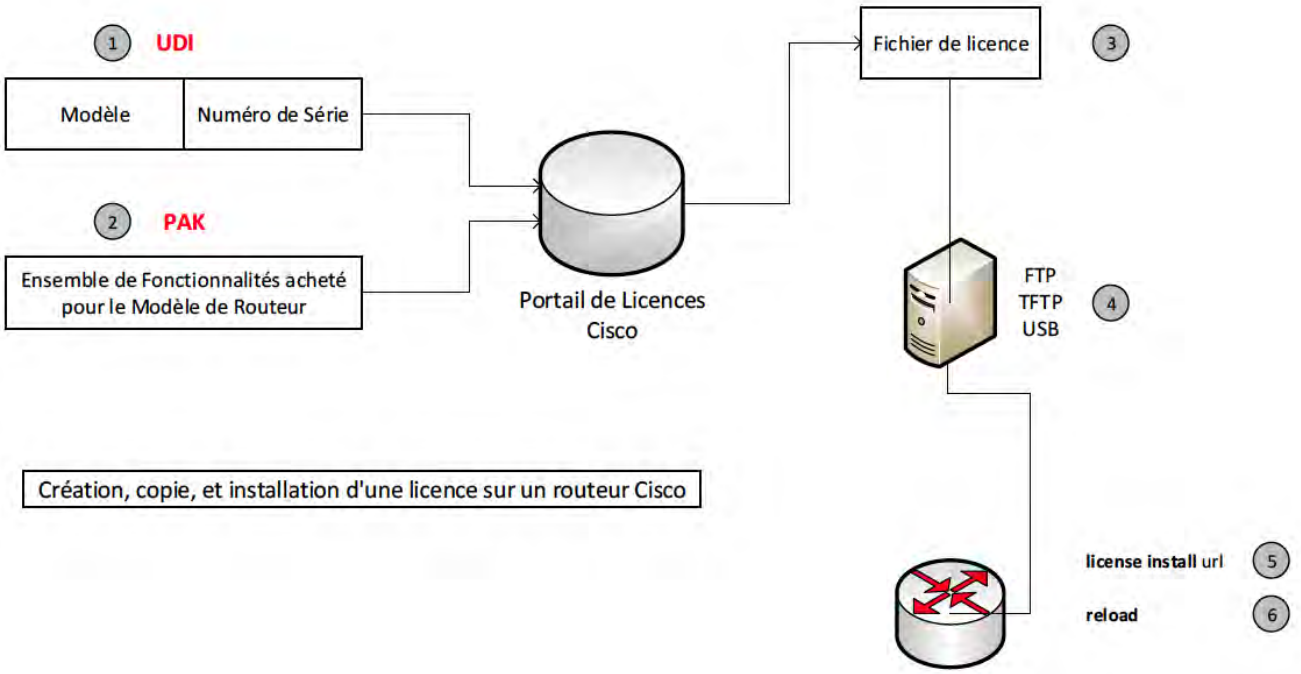
2) Tapez la PAK (clé d'accès du produit) que vous avez reçu de Cisco ou de votre revendeur

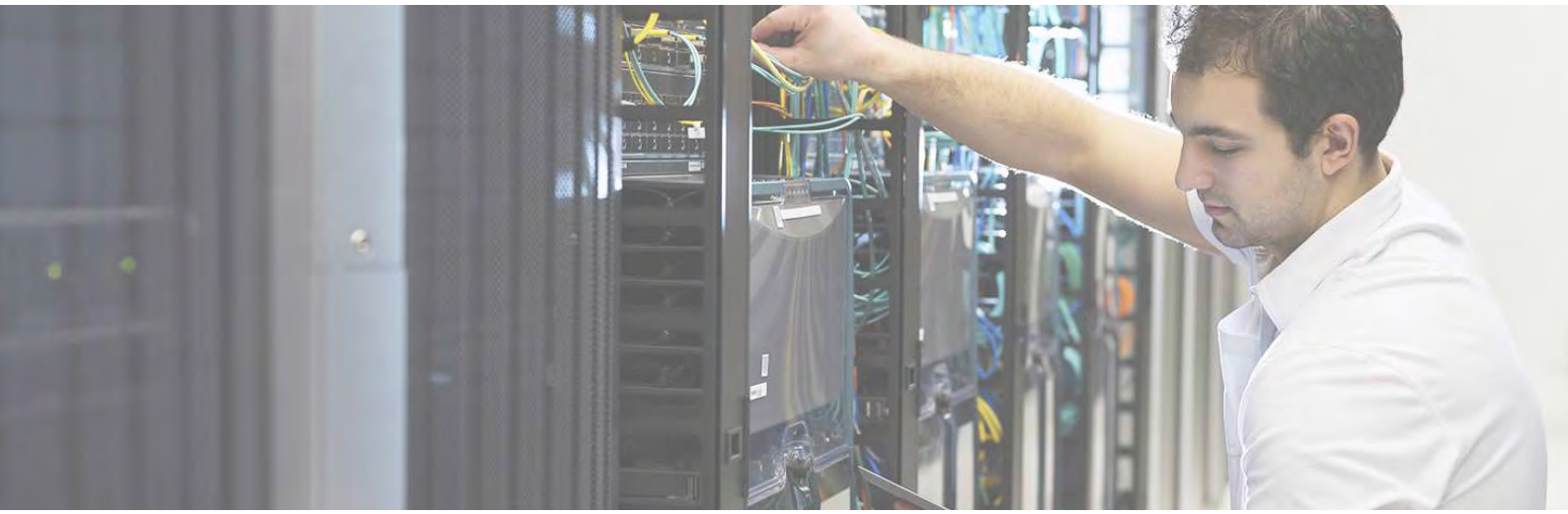
3) Copiez le fichier de la clé de licence lorsque vous y êtes invité par le portail.

4) Mettez la clé de licence à la disposition du routeur

5) Installez la clé avec la commande license install url (l'URL pointe vers le fichier de clé de licence)

6) Rechargez le routeur pour mettre à jour les fonctionnalités sous licence





IMPLÉMENTATION DE LA COMMUTATION

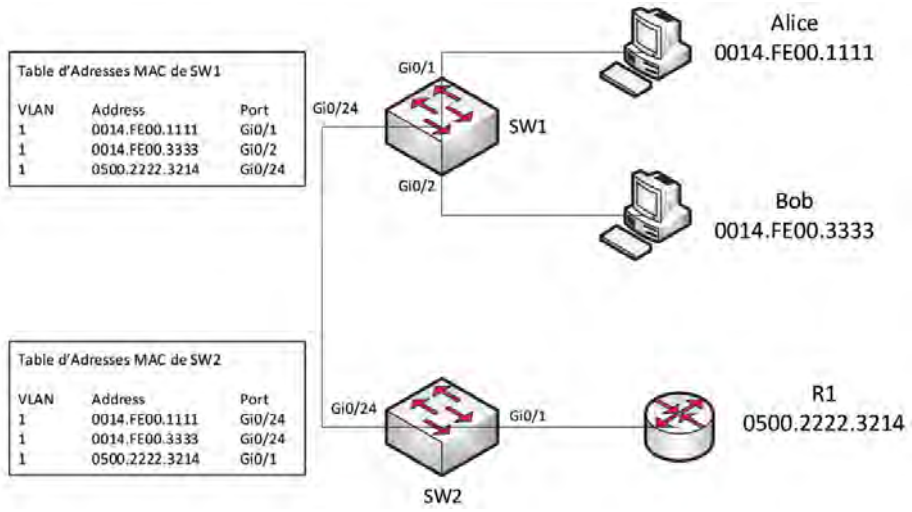
CONCEPTS DU PROTOCOLE SPANNING TREE

LOGIQUE DE TRANSMISSION D'UN COMMUTATEUR LAN:

Étape 1: Lire la trame et déterminer si la trame doit être transmise.
Si la trame est arrivée sur un port d'accès, utiliser le VLAN du port d'accès.
Si la trame est arrivée sur un port trunk, lire l'en-tête VLAN pour déterminer le VLAN (à laquelle la trame appartient)

Étape 2: Lire l'adresse MAC source de la trame et ajouter l'adresse MAC à la table d'adresses MAC (Mac-address-table) avec l'information de VLAN et d'interface

Étape 3: Essayer de faire correspondre l'adresse MAC de destination avec une entrée de la table d'adresses MAC
Si l'adresse MAC est trouvée, transmettre la trame sur l'interface en se basant sur l'entrée de la table d'adresses MAC (par ex: FastEthernet 0/3)
Si l'adresse MAC n'est pas trouvée, envoyer la trame vers tous les ports d'accès dans le même VLAN et les ports trunk qui transportent ce VLAN.



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

PROBLÈME	DÉSCRIPTION
Tempêtes de Broadcast	Une trame de broadcast est transmise à plusieures reprises sur les mêmes liens entraînant une saturation des liens et évinçant le trafic légitime
Table d'adresses MAC instables	Quant 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 sur 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	Le commutateur racine est au sommet de l'arbre et aucun port n'est bloqué
Port racine sur commutateur nonracine (non Root)	Transmission	Port avec le coût le plus bas vers le commutateur racine
Port Désigné	Transmission	Le port transmet les BPDU ou Hello sur ce segment LAN
Tous les ports du commutateur racine (Root)	Blocage	Les trames BPDU ne sont ni envoyées ni reçues sur cette interface

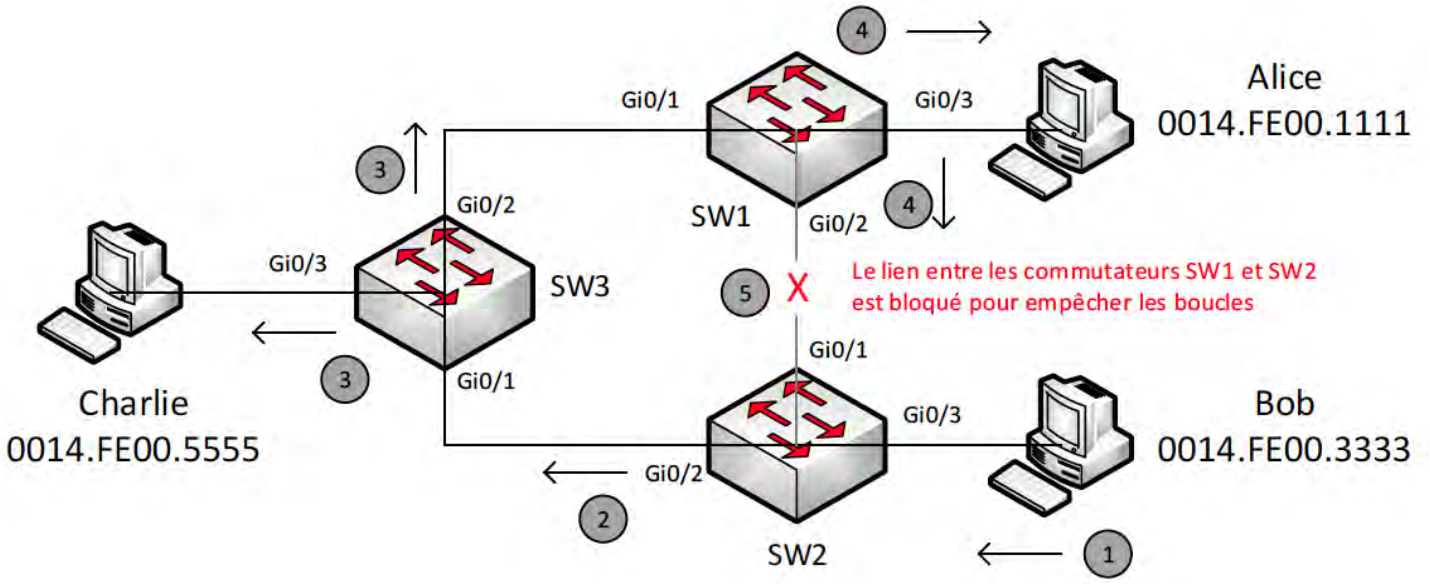
COÛTS PORTS IEEE

VITESSE ETHERNET	COÛT PORT
10 Mbps	100
100 Mbps	19
1 Gbps	4
10 Gbps	2

CHAMPS DE BRIDGE PROTOCOL DATA UNIT (BPDU)

CHAMP	DESCRIPTION
ID du commutateur racine (Root Bridge)	ID de commutateur de la source de ce hello pensant qu'il est le commutateur racine (Root Bridge)
ID du Commutateur d'origine	ID de commutateur du relai pour cet ID de hello
Coût racine (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

CONCEPTS DU PROTOCOLE SPANNING TREE



Exemple Spanning Tree quand Bob envoie une trame de broadcast

Étape 1: Bob transmet la trame à SW2

Étape 2: SW2 envoie la trame uniquement à SW3. Puisque SW3 GI0/1 est dans un état bloqué, la trame n'est pas envoyée à SW1.

Étape 3: SW3 envoie la trame à Gi0/2 et GI0/3.

Étape 4: SW1 envoie la trame à Gi0/2 et GI0/3.

Étape 5: SW2 reçoit la trame mais ignore la trame envoyée depuis SW1 parce l'interface SW2 GI0/1 est à l'état bloqué.

OPÉRATION STP À ÉTAT STABLE

Étape 1: Le commutateur racine (Root bridge) crée et envoie un BPDU Hello, de coût 0, vers toutes les interfaces de transmission

Étape 2: Chaque commutateur non-racine qui reçoit le BPDU Hello met l'ID de l'expéditeur à son propre ID de commutateur, met le coût racine (Root cost) à son propre coût racine, et transfert le BPDU modifié par les ports désignés.

Étape 3: Répéter les étapes 1 et 2 jusqu'à ce qu'un lien soit coupé.

ÉTATS D'INTERFACE SPANNING TREE

ÉTAT	TRANSITION OU ÉTAT STABLE	TRANSMETTRE LES TRAMES DE DONNÉES?	APPRENDRE LES ADRESSES MAC À PARTIR DES TRAMES REÇUES?
Blocage (Blocking)	Stable	Non	Non
Écoute (Listening)	Transition	Non	Non
Apprentissage (Learning)	Transition	Non	Oui
Transmission (Forwarding)	Stable	Oui	Oui
Désactlvativé (Disable)	Stable	Non	Non

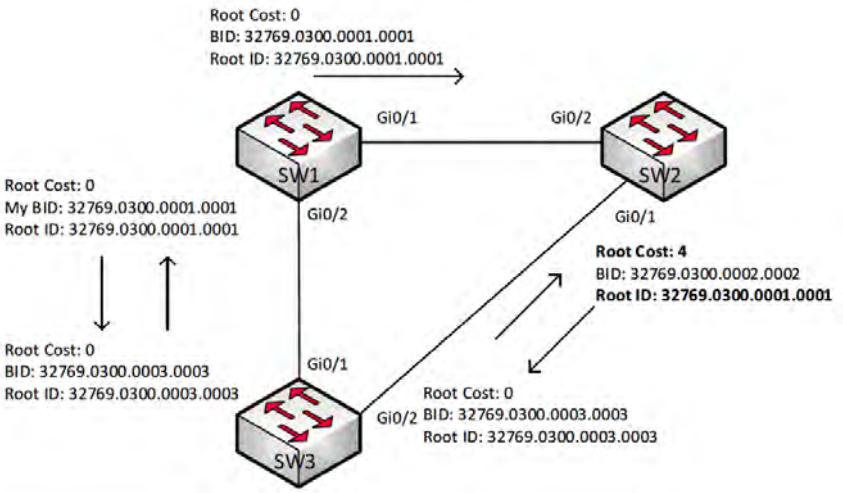
MINUTEUR	DÉSCRIPTION	VALEUR PAR DÉFAUT (SECONDES)
Hello	Le temps entre les Hello envoyés par le commutateur racine (Root bridge)	2 Secondes
MaxAge	Temps d'attente avant de tenter un changement de topologie STP	10 Secondes
Forward Delay	Durée des statuts d'Écoute et d'Apprentissage pendant la convergence STP	15 Secondes

ÉTATS TRANSITOIRES STP:

Écoute (Listening) – Ne transmet pas les trames et supprime les adresses MAC de la table associée à cette interface

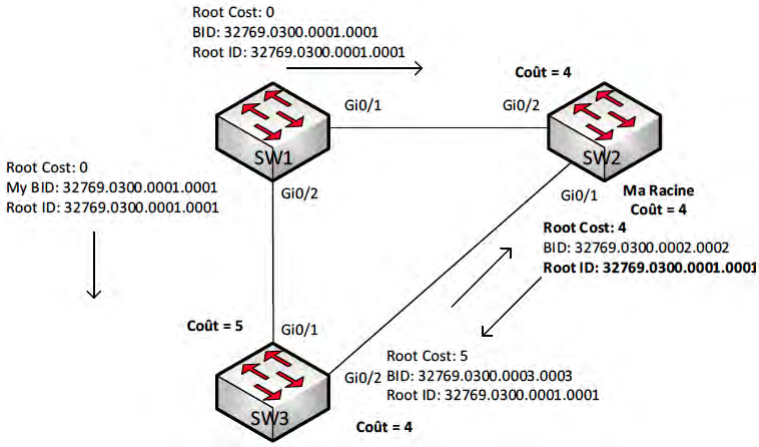
Apprentissage (Learning) – Ne transmet pas non plus les trames mais apprend les adresses MAC des trames

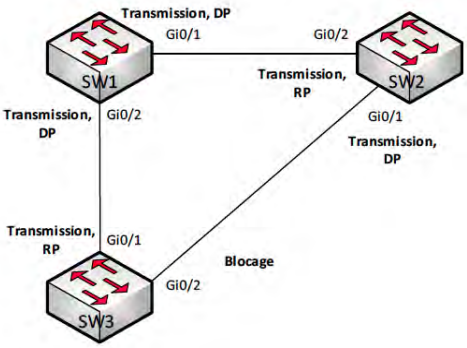
CONCEPTS DU PROTOCOLE SPANNING TREE



Au début du processus de sélection de la racine STP (Root Bridge), SW1 croit déjà qu'il est racine et envoie des BPDU avec son ID de pont (BID) comme le pont racine. SW2 a déjà décidé qu'il n'est pas le pont racine et annonce son BID plus le Root ID de SW1. SW3 pense qu'il est le pont racine mais puisque son BID est plus élevé que les deux autres, les BPDU de SW3 ne sont pas considérés par SW1 et SW2

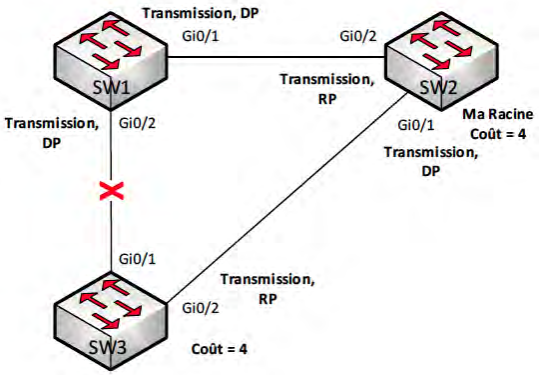
À ce stade, SW1 a gagné son élection. SW3 annonce que son coût racine à SW2 est 5. SW2 a un coût racine égal à 4. SW2 sait que le plus faible coût vers la racine est 4 en passant par GI0/2. SW3 sait que le coût racine par Gi0/1 vers SW1 est 5 et basé sur le hello de SW2, le coût racine par Gi0/2 est 8 (4 + 4).





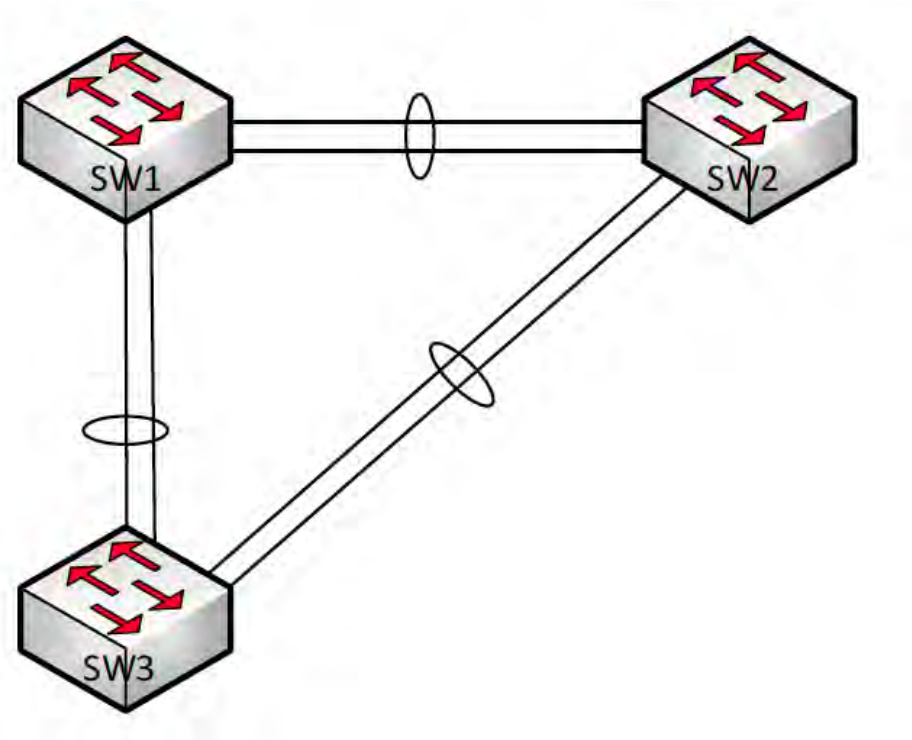
Après les calculs d'élection et de coût, STP prend ses décisions de transmission et de blocage sur chaque commutateur. SW1 est le commutateur racine, alors ses deux ports sont mis à transmission et port désigné (DP) sur leurs segments respectifs.
SW2 Gi0/2 et SW3 Gi0/1 sont des ports racines (RP) donc ils sont mis au statut de transmission. SW2 Gi0/1 est mis à transmission et est le DP sur sa connexion à SW3. SW3 Gi0/2
n'est ni un RP ni un DP, donc le port est mis à bloqué.

Ici, le lien entre SW1 et SW3 est tombé. Le recalcul de STP a été déclenché. À présent, SW2 annonce que son coût vers la racine est 4 et puisque SW3 n'a pas entendu d'autreS annonces de racine, son coût est 8 (4+4). SW3 change GI0/2 de Bloqué à Écoute, puis finalement, Transmission. Gi0/2 devient le RP pour SW3.



CONCEPTS DU PROTOCOLE SPANNING TREE

Etherchannel est la liaison de deux à huit liens entre deux commutateurs. Ceci permet la redondance de lien de telle sorte que si un des liens est défaillant, le recalcul STP ne se produit pas



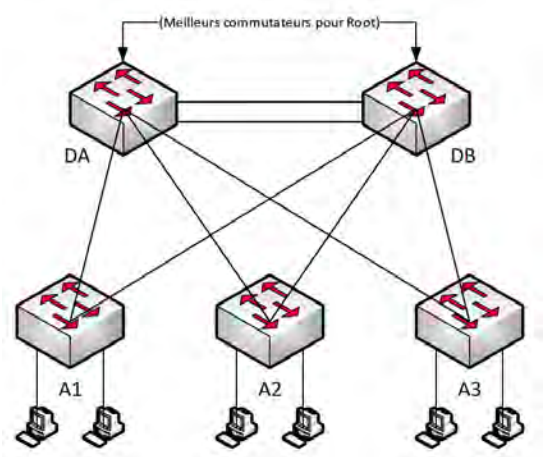
AUTRES CARACTÉRISTIQUES DU PROTOCOL SPANNING TREE:

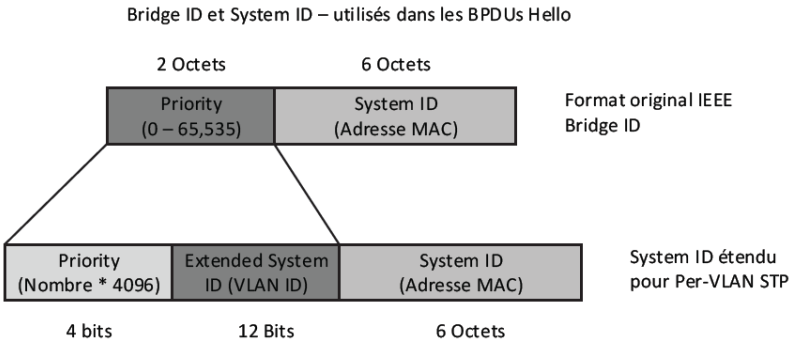
PortFast: Bien que STP soit très utile sur les commutateurs, pour les hôtes il n'est pas très utile. Quand un hôte est connecté à un commutateur, le port du commutateur passe par un état de blocage, écoute, apprentissage puis de transmission. Le processus peut prendre 50 secondes. Ceci pourrait causer des problèmes avec un hôte utilisant DHCP pour son adresse IP. PortFast permet aux ports configurés d'aller directement à l'état de transmission. Toutefois, ce réglage ne doit pas être utilisé sur des ports connectés à d'autres commutateurs.

BPDU Guard: Un réglage de sécurité intégré à STP peut prévenir des changements de l'architecture des commutateurs comme suit: Bloquer les annonces BPDU se proclamant commutateur racine et assumant ce rôle, ce qui dégraderait la performance du réseau de commutation, ou causerait des boucles par inadvertance parce qu'un commutateur bon marché est branché sur le réseau. BPDU Guard désactive un port lorsque ces BPDU arrivent et cette fonction est utile sur les ports d'accès. Seuls les ports connectés aux commutateurs ne devraient pas utiliser ce réglage.

Rapid STP: Cette fonction peut être utilisée de concert avec le STP régulier, mais le temps de convergence est réduit de 50 secondes à 10 secondes dans le cas d'une défaillance dans la topologie. RSTP offre un temps de convergence plus rapide que le STP régulier (Standard STP) et est souhaitable dans les grands réseaux de commutateurs grâce à son temps rapide de convergence.

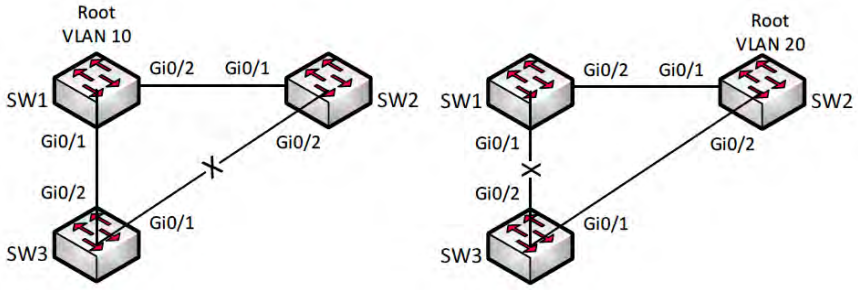
MISE EN OEUVRE DU PROTOCOLE SPANNING TREE





Détermination du commutateur racine (Root Bridge) dans un réseau commuté:
1) Commencer par un diagramme et faire la liste des commutateurs racines (Root Bridge) possibles
2) Se connecter à chaque commutateur racine (Root Bridge) possible et entrer la commande show spanning-tree.
S'il existe un port racine (RP), éliminer le commutateur parce que les commutateurs racines n'ont pas de RP.
3) Utiliser show spanning-tree et chercher le texte "This bridge is the root" ou bien utiliser show spanning-tree root. Si le texte est présent, vous avez le commutateur racine (Root Bridge). Dans le cas de cette dernière commande, un commutateur racine n'aura pas de RP.

Préparation à une simulation lors de l'examen:
Si vous rencontrez lors d'une simulation Avec plusieurs commutateurs, lisez d'abord les questions pour arriver à deviner les réponses. Ensuite, cherchez le commutateur racine (Root Bridge) en utilisant la commande show spanning-tree root pour localiser les RPs. Rappelez-vous que les RPs vous indiquent quel commutateur est le commutateur racine.
Si la simulation compte plusieurs VLANs, utilisez show spanning-tree vlan x pour trouver le commutateur racine pour chaque VLAN si nécessaire. Veuillez noter que le commutateur racine pour un VLAN peut être différent des autres VLANs.



EQUILIBRAGE DE CHARGE EN UTILISANT LE PROTOCOLE PER-VLAN SPANNING TREE. VOYEZ COMMENT LE VLAN 10 A UN COMMUTATEUR RACINE (ROOT BRIDGE) DIFFÉRENT DU VLAN 20.

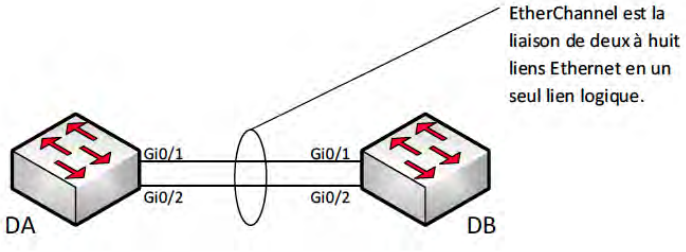
Pour designer un commutateur en particulier comme commutateur racine pour un VLAN, utiliser la commande **spanning-tree vlan x root primary**

Designer le SW2 comme commutateur root sur le VLAN 20
SW2(config)**# spanning-tree vlan 20 root primary**

Designer le SW1 comme commutateur root sur le VLAN 10
SW1(config)**# spanning-tree vlan 10 root primary**

A retenir 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 multiple de 4096 ce qui fait que le commutateur local devient racine (exemple: 4,096 - 8,192 - 16,384...)

MISE EN OEUVRE DU PROTOCOLE SPANNING TREE



Configuration manuelle des liens EtherChannel:

1) Ajouter la commande **channel group** numéro **mode on** sur les
interfaces souhaitées.
2) Utiliser le même numéro sur le même commutateur. Un numéro différent peut être utilisé sur le commutateur d'en face.
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 on**

DÉPANNAGE DES PROBLÈMES AVEC ETHERCHANNEL:

Généralement, les commandes channel-group doivent correspondre des deux côtés du lien à l'exception du numéro de groupe qui est localement significatif sur chaque commutateur.

PROCESSUS:

1) S'assurer que les interfaces dans le lien EtherChannel sur le même commutateur ont le même numéro de channel-group
2) Le numéro de channel-group est localement significatif sur chaque commutateur
3) Si vous utilisez le mot-clé on, il doit s'appliquer des deux côtés du lien EtherChannel
4) Si vous utilisez le mot-clé desirable d'un côté du lien, 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 d'un côté du lien, active ou passive doit être utilisé comme motclé de l'autre côté du lien si le commutateur utilise LACP.

AJOUT DE LIENS À DES ETHERCHANNELS EXISTANTS:

Vous devez vérifier les éléments suivants avant d'ajouter un lien à un lien EtherChannel existant:
vitesse, duplex, mode trunk ou access, VLAN d'accès si en mode access, VLAN natif et/ou VLANs autorisés pour ports trunk, et les réglages d'interface STP

PROBLÈMES DE PORT RACINE (ROOT PORT) LORS D'UNE SIMULATION:

Voici comment trouver les problèmes de port racine dans une simulation

1) Utiliser les commandes **show spanning-tree et show spanning-tree root** si la simulation le permet. Vous aurez le port racine avec les deux commandes et le coût racine avec la seconde commande

2) **show spanning-tree** liste le coût racine au début des informations affichées et le coût d'interface se trouve à la fin des informations affichées. Attention à ne pas confondre les deux.

3) Si vous devez calculer le coût racine pour un commutateur en particulier, rappelez-vous des valeurs par défaut des coûts (100 pour 10 Mbps, 19 pour 100 Mbps, 4 pour 1 Gbps, et 2 pour 10 Gbps)

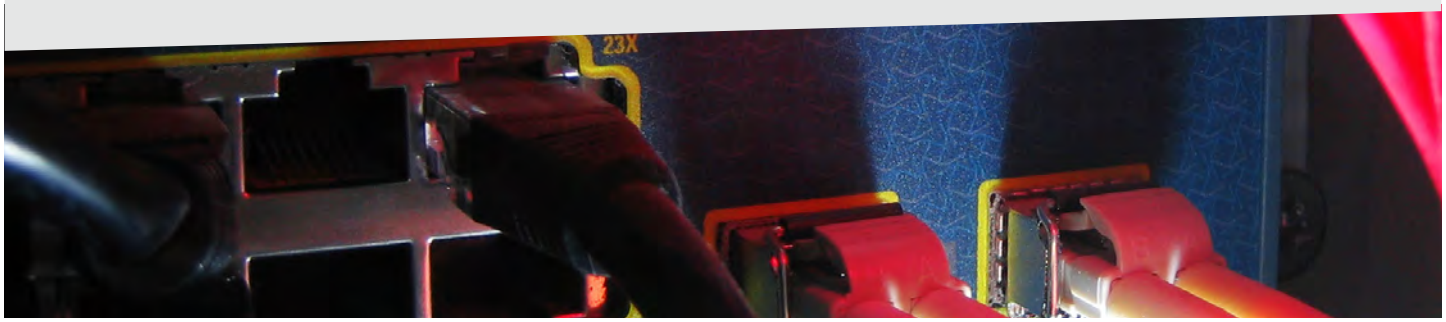
Passer en revue les configurations des interfaces et voir s'il existe une commande **spanning-tree cost** sur une des interfaces. La commande manuelle de coût aura priorité sur le coût par défaut.

Vérifier également les vitesses d'interface pour déterminer les coûts d'interfaces. Utiliser la commande **show interface** ou la commande **show interface status** pour identifier la vitesse d'interface.

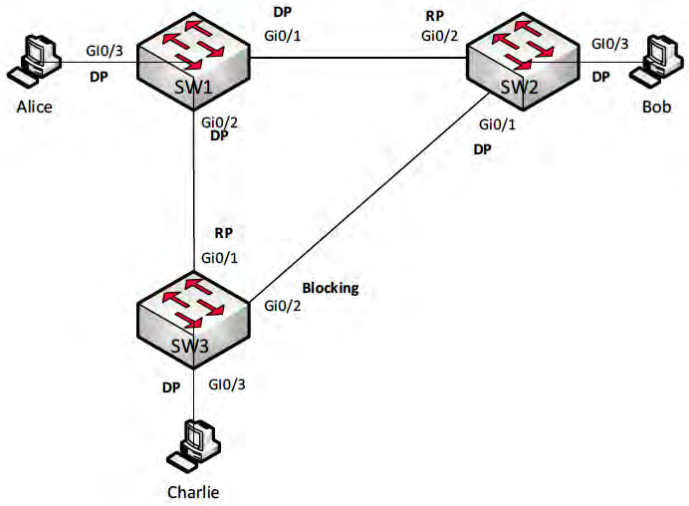
LOCALISATION DES PORTS DÉSIGNÉS (DP) SUR CHAQUE SEGMENT:

Rappelez-vous que le Port Désigné (Designated Port) est la connexion du commutateur au commutateur racine (Root Bridge). Voici comment trouver le port désigné sur n'importe quel commutateur

1) Si les commutateurs sont sur le même segment LAN, celui ayant le plus faible coût racine (Root cost) devient le DP sur ce segment.
2) S'il existe une égalité après l'étape 1, alors le commutateur ayant le plus faible bridge ID (BID) devient le DP sur ce segment.



MISE EN OEUVRE DU PROTOCOLE SPANNING TREE



Comparaison entre les commandes **show spanning-tree** de SW1 et SW2:

SW1# show spanning-tree

VLAN0001

Spanning tree enabled protocol 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

Spanning tree enabled protocol ieee

Root ID	**Priority**	**32769**
	Address	**0c00.2345.1211**
	Cost	**4**
	Port	**26 (GigabitEthernet 0/2)**
Bridge ID	**Priority**	**32769 (priority 32768 sys-id-ext 1)**
	Address	**0c00.2345.5504**

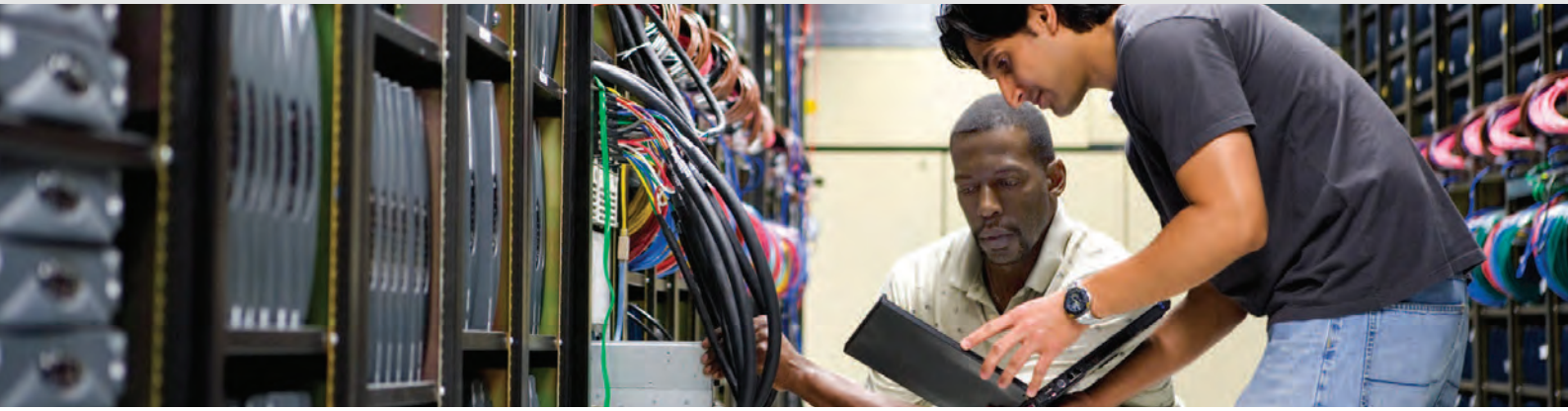
Comme vous le voyez, SW1 indique qu'il est le commutateur racine pour le VLAN 1. SW2 indique qui est le commutateur racine, son root ID, coût vers le commutateur racine, son port racine et l'adresse MAC du commutateur racine.

VÉRIFICATIONS DE CONFIGURATION AVANT D'AJOUTER DES PORTS À UN ETHERCHANNEL:

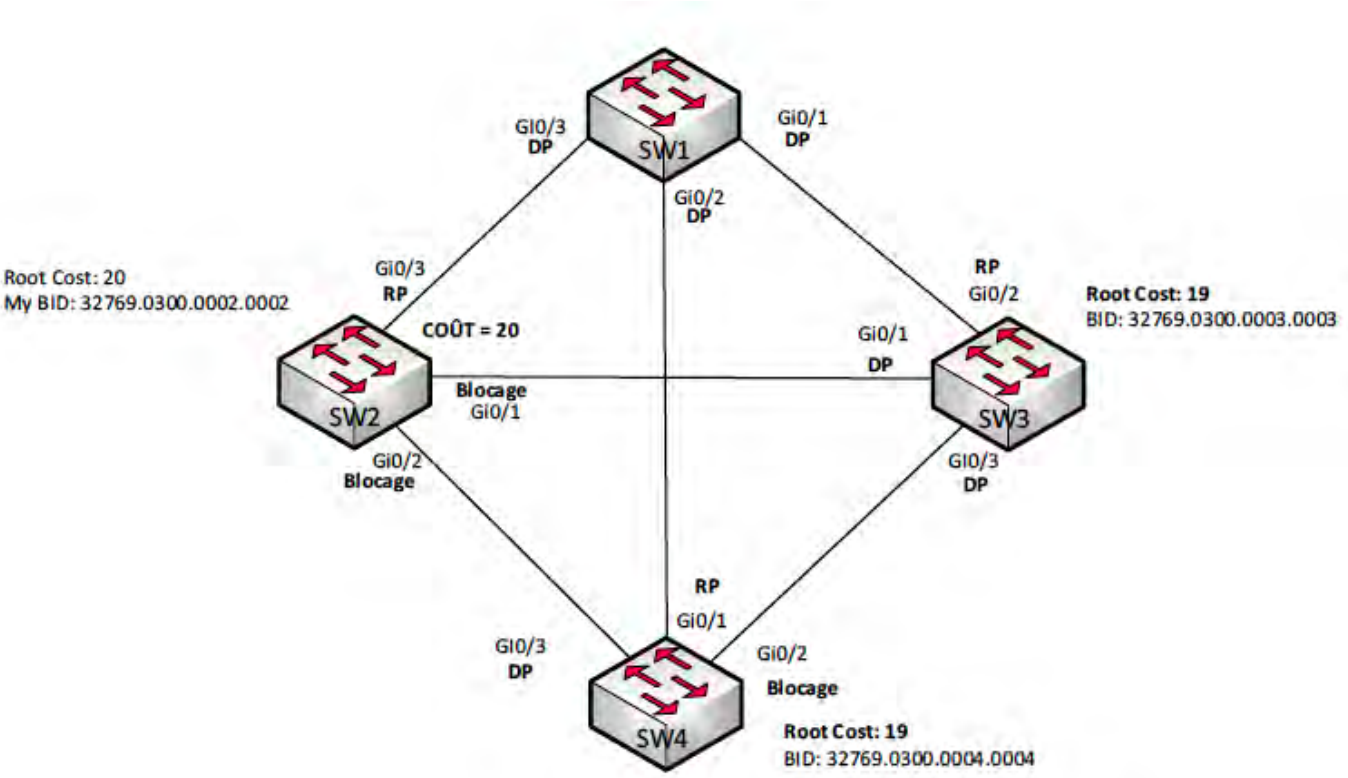
Avant d'ajouter un ou plusieurs ports à un Etherchannel, sur chaque port les éléments suivants doivent être vérifiés:

- **Vitesse**
- **Duplex**
- **Tous les ports doivent être soit à access soit à trunk (Le mélange de ports d'accès et trunk n'est pas autorisé sur Etherchannel)**
- **VLAN d'accès pour ports d'accès**
- **Liste de VLANs autorisés pour un port trunk (commande switchport trunk allowed vlan).**
- **VLAN natif si c'est un port trunk**
- **Réglages d'interface STP (portfast, BPDU guard)**

S'il existe une disparité de réglages sur n'importe lequel des ports Etherchannel, l'Etherchannel peut ne pas monter et passer le trafic



MISE EN OEUVRE DU PROTOCOLE SPANNING TREE



Dans ce schéma, vous pouvez voir comment les ports racines (Root Port) et ports désignés (Designated Port) sont sélectionnés. Les commutateurs SW2, SW3, et SW4 ont tous des connexions directes à SW1 qui est le commutateur racine (Root Bridge) et ces ports connectés sont les ports racines (Root Port).

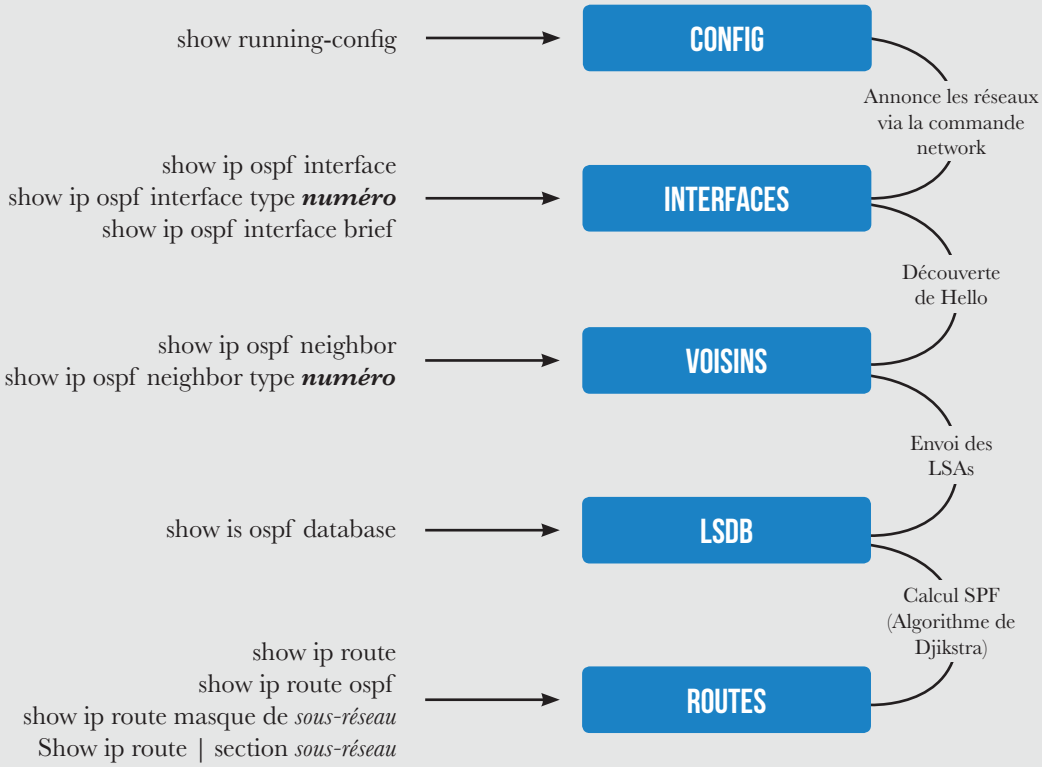
Si vous regardez SW3 et SW4, leur coût racine est 19 alors que le coût racine de SW2 est 20. Au moment de choisir les DP, le commutateur avec le Bridge ID le plus bas sur la connexion aura le DP pour cette connexion. Puisque c'est le cas, SW3 a le coût racine le plus bas pour chacune de ses connexion à SW2 et SW4. SW3 a les DPs pour ses segments. Cependant, si vous regardez SW4, Il a également un coût racine de 19 et son interface vers SW3 est dans un état de blocage. Puisque SW4 a un coût racine plus bas que SW2, le port sur SW4 connecté à SW2 est le DP pour ce segment.

Ceci signifie que SW2 a uniquement un RP et ses connexions à SW3 et SW4 sont placées dans un état de blocage (Blocking State).

IMPLÉMENTATION DU ROUTAGE IPV4

MISE EN OEUVRE DE OSPFV2 (IPV4)

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



CALCUL DE ROUTEUR-ID OSPF (RID)

1) Si le router-id rid est configuré sous router ospf, utilisez-le

2) Si OSPF RID n'est pas défini, choisissez l'adresse IP au numéro le plus élevé pour l'OSPF RID

3) Si le RID ne peut être fixé via une adresse IP loopback, utilisez l'adresse IP numérique la plus élevée sur une interface non-loopback

DÉFINITION D'ADJACENCE	ÉTAT DU VOISIN	DESCRIPTION
Adjacent (adjacency)	2-way	Les routeurs sont voisins sur la base des paquets hello. La relation d'adjacence est bonne
Complètement Adjacent (Fully adjacency)	Full	Les deux routeurs ont échangé les mêmes informations de base de données de l'état des liens

ÉTATS DES VOISINS OSPF

1) La couche physique est activée

2) Les paquets Hello sont échangés avec les IDs de routeur

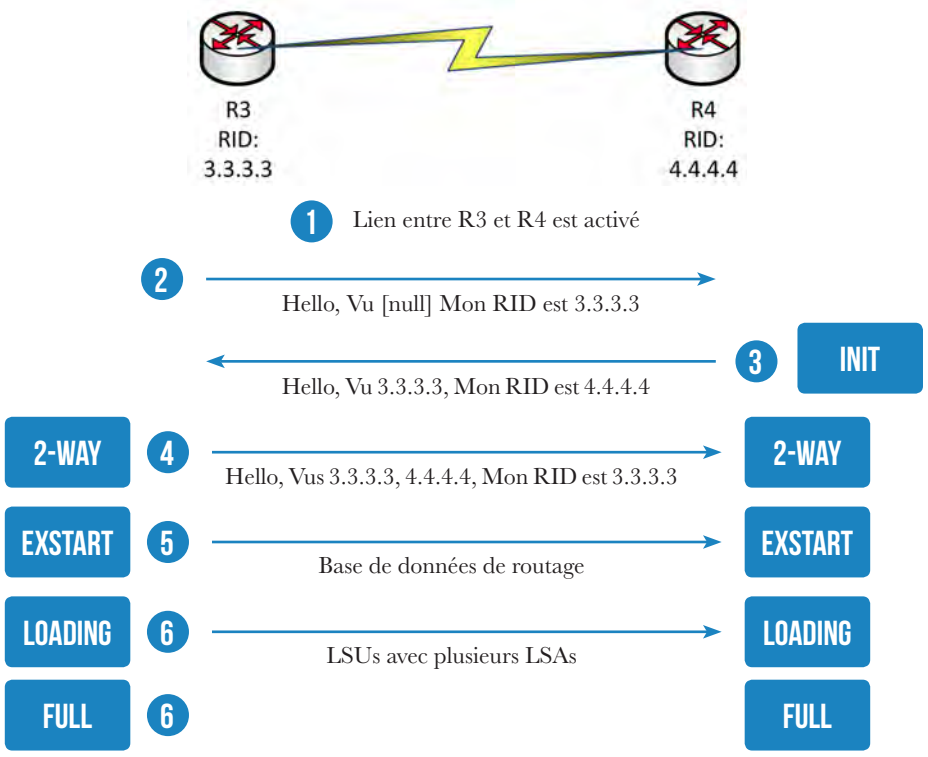
3) Le processus Init commence quand un routeur reconnaît l'autre routeur

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 d'état de liens sont échangées et les calculs SPF sont faits

7) Un état **Full** signifie que les routes sont échangées entre les deux routeurs



MISE EN OEUVRE DE OSPFV2 (IPV4)

POINTS CLÉS SUR LES AIRES (AREAS) OSPF:

Alors que tous les routeurs dans un réseau peuvent être situés dans l'area 0, c'est une bonne idée de diviser le réseau en aires de sorte que le calcul SPF sur chaque routeur soit limité. En outre, un changement d'interface sur un routeur n'affectera que les routeurs dans l'aire immédiate.

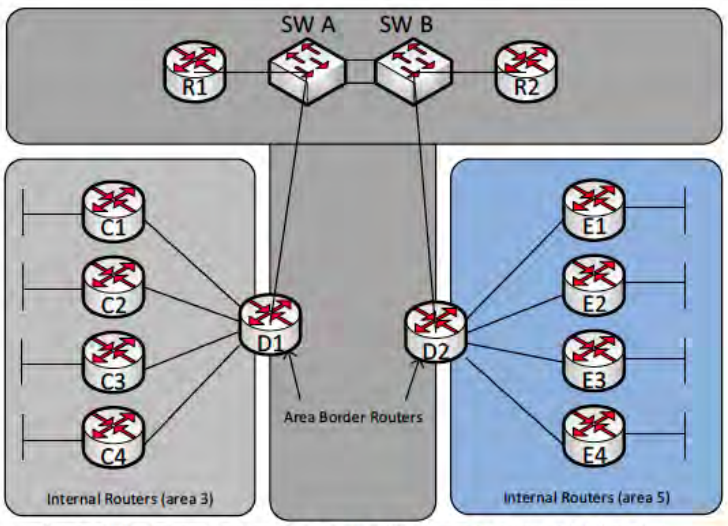
Les choix des interfaces de routeur à placer dans les aires sont réalisés compte tenu de ces contraintes:

- Les interfaces dans le même sous-réseau doivent être dans la même aire
- Les aires doivent être contiguës
- Un routeur peut avoir toutes ses interfaces dans une seule aire, ou pas
- Certains routeurs peuvent avoir des interfaces dans deux aires. Ce sont des routeurs à la frontière d'aire (Area Border Routers - ABR) où les interfaces se connectent à l'aire dorsale (backbone area 0) et d'autres interfaces se connectent à des aires non-zéro
- Toutes les aires doivent se connecter à l'aire dorsale (backbone area 0) par unou plusieurs ABR.

TYPES DE LSA OSPFV2 VUS DANS UN RÉSEAU OSPF MULTI-AREA

NOM LSA	NUMÉRO LSA	PRINCIPAL OBJECTIF	CONTENU LSA
Router	1	Description de routeur	RID, interfaces, adresses IP, états d'interfaces
Network	2	Réseau avec un DR (designated router)	Adresses pour DR et BDR, ID sous-réseau et masque
Summary	3	Sous-réseau dans autre aire	ID sous-réseau et masque de sous-réseau, RID ABR annonçant la route

Dans l'exemple en bas à gauche, les routeurs ABR D1 et D2 échangent et envoient des LSAs sommaires (LSA 3) pour annoncer les sous-réseaux dans d'autres aires. Tous les routeurs échangent des LSAs de routeur avec les autres routeurs dans leur aire et les ABRs si nécessaire.



Réseau OSPF de trois aires (areas) avec D1 et D2 servant de routeurs à la frontière de ces areas (ABR - Area Border Routers)

PRÉSENTATION DE LA CONFIGURATION D'OSPFV2

1) Entrer le mode de configuration de routeur OSPF en exécutant la commande **router ospf** ***processus-id***

2) Configurer l'ID de routeur par l'une des opérations suivantes

a. configurer manuellement l'ID de routeur via la commande **router-id** ***valeur***
b. ou configurer une adresse IP sur une interface de bouclage (loopback)
c. ou compter sur OSPF pour choisir l'adresse IP existante la plus élevée sur le routeur

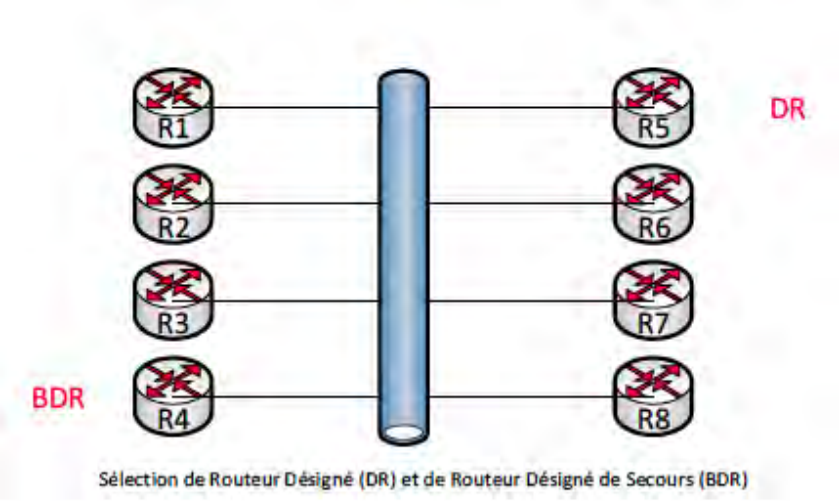
3) Configurer une ou plusieurs commandes **ip address** ***masque-générique*** **area** ***area-id*** pour placer des interfaces dans des aires OSPF

4) Vous pouvez également définir des interfaces passives via la sous-commande **passive interface** ***type numéro***

Voici le show running-config pour le routeur C1:

```
interface Gigabit0/0
ip address 192.168.10.1 255.255.255.0
!i
nterface Serial0/0/0
ip address 192.168.100.2 255.255.255.252
!
router ospf 1
network 192.168.10.1 0.0.0.0 area 3
network 192.168.100.2 0.0.0.0 area 3
router-id 3.3.3.1
```

MISE EN OEUVRE DE OSPFV2 (IPV4)



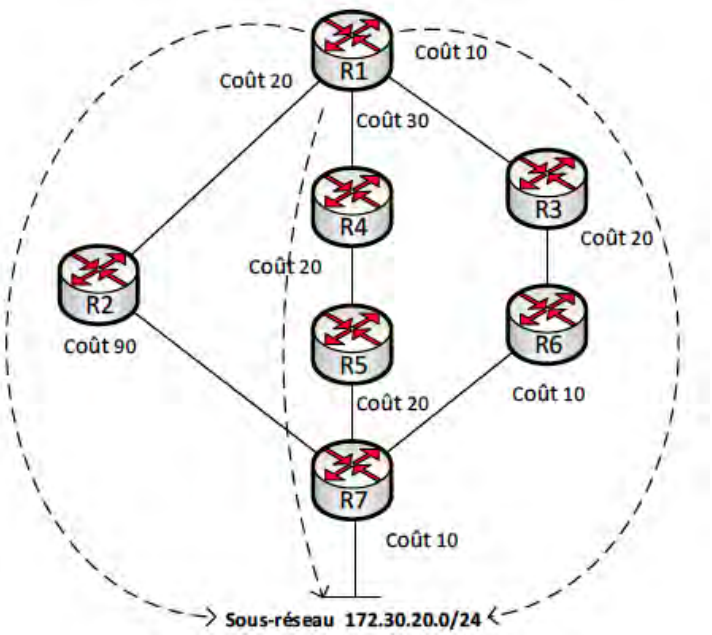
Sélection de Routeur Désigné (DR) et de Routeur Désigné de Secours (BDR)

SÉLECTION DE ROUTEUR DÉSIGNÉ (DR) ET DE ROUTEUR DÉSIGNÉ DE SECOURS (BDR)

Sur les réseaux Ethernet, les routeurs OSPF éliront un DR et un BDR. Le DR est le gardien des LSAs sur le segment Ethernet. Dans ce cas, le DR reçoit des routes des autres routeurs via des mises à jour multicast. Le DR envoie alors les mises à jour de LSA. Si le DR échoue, le BDR devient le DR et l'échange de route se poursuit. Les autres routeurs sur le segment élisent ensuite un nouveau BDR.

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

OSPF calcule la métrique pour une route comme étant la somme des coûts d'interfaces OSPF pour toutes les interfaces le long du chemin d'une route. En d'autres termes, la route avec le coût total le plus bas est placée dans la table de routage.



Calculer les coûts des routes possibles à partir de R1 vers le sous-réseau 172.30.20.0/24

Via R2: Le coût est de 20 + 90 + 10 = 120
Via R4: Le coût est de 30 + 20 + 20 + 10 = 80
Via R3: Le coût est de 10 + 20 + 10 + 10 = 50

Le route de plus bas coût vers 172.30.20.0/24 est via R3, alors R1 ajoute une route vers le sous-réseau dans sa table de routage

MISE EN OEUVRE DE OSPFV2 (IPV4)

DISTANCES ADMINISTRATIVES PAR DÉFAUT

TYPE DE ROUTE	DISTANCE ADMINISTRATIVE	TYPE DE ROUTE	DISTANCE ADMINISTRATIVE
Connected	0	IS-IS	115
Static	1	RIP	120
BGP External	20	EIGRP External	170
EIGRP Internal	90	BGP Internal	200
IGRP	100	Unreachable	255
OSPF	110		

TERMINOLOGIE DE CONCEPTION OSPF

TERME OSPF	DESCRIPTION
Area border router (ABR)	Un routeur avec des interfaces dans l'aire dorsale 0 (backbone) et une autre aire
Routeur Backbone	Un routeur avec toutes ses interfaces dans l'area dorsale 0
Routeur Interne	Un routeur avec toutes ses interfaces dans une aire non-zéro
Aire (area)	Un groupe de routeurs partageant des informations de routage entre eux, mais pas avec des routeurs dans les autres aires
Aire dorsale (Backbone area)	L'aire où toutes les aires OSPF doivent se connecter - également connu comme area 0
Route interene (Intra-area)	Une route partagée entre des routeurs de la même zone
Route Interarea	Une route vers un sous-réseau situé dans une autre aire à l'extérieur de sa propre aire

AVANTAGES DE LA CONCEPTION D'AIRES OSPF

- Des mises à jour plus petites de la base de données d'état de liens (LSDB, Link State DataBase) de l'aire nécessitent moins de cycles de processeur et de mémoire.

- Des mises à jour de LSDB plus petites signifient des temps de convergence plus rapides

- Les changements dans les informations d'état de liens restent dans une aire unique, ce qui signifie que moins de routeurs ont besoin d'exécuter le calcul du SPF basé sur un changement d'état des liens

- Moins d'information est annoncée entre les aires ce qui nécessitent moins de bande passante pour partager les mises à jour d'état de liens (LSA)

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 des largeurs de bande d'interface plus élevées

Trois façons de définir le coût d'interface OSPF

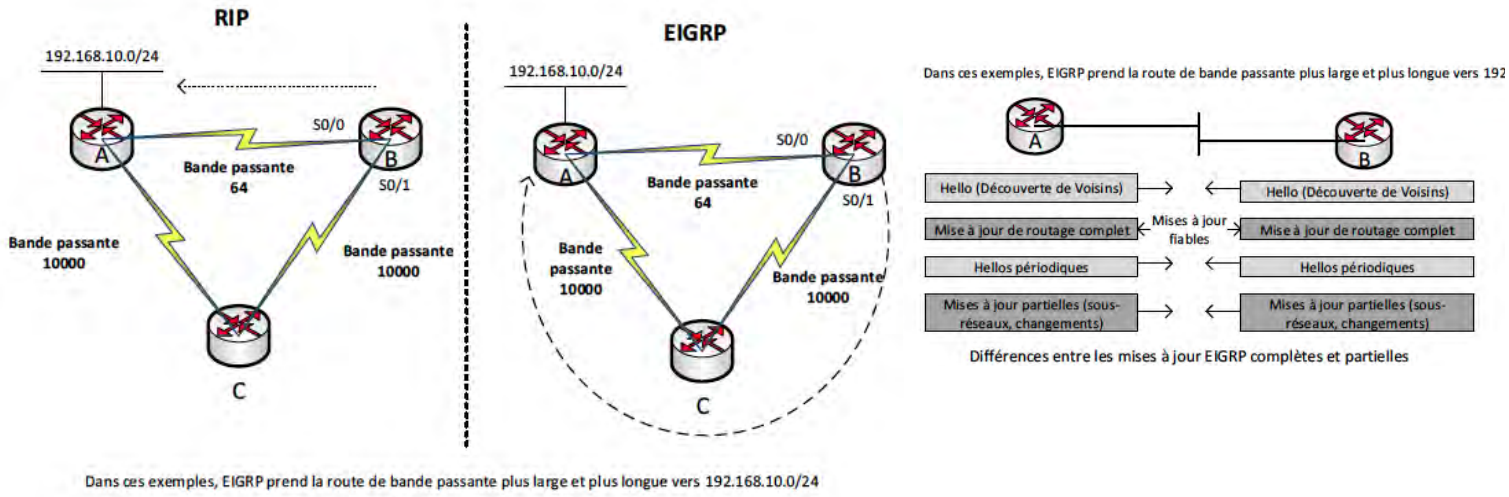
1) Définir le coût explicitement via la sous-commande **ip ospf cost** x (x est compris entre 1 et 65535)

2) Modifier de la vitesse d'interface avec la commande **bandwidth speed** en unités de Kbps
3) Changer la bande passante de référence avec la commande **auto-cost reference-bandwidth** ***ref-bw*** avec Mbps comme unité

CONCEPTS EIGRP

POINTS CLÉS SUR ENHANCED INTERIOR GATEWAY ROUTING PROTOCOL (EIGRP):

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 de rechange plus rapidement que d'autres protocoles de routage



Dans ces exemples, EIGRP prend la route de bande passante plus large et plus longue vers 192.168.10.0/24

COMPARAISON DES CARACTÉRISTIQUES DES PROTOCOLES DE ROUTAGE

CARACTÉRISTIQUE DE PROTOCOLE DE ROUTAGE	RIPV2	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 métriques?	Non	Oui	Oui
Convergence	Lente	Rapide	Rapide
Aires nécessaires?	Non	Non	Oui
Support de sommaire de route manuel	Oui	Oui	Oui
Mises à jour de routage via multicast IP?	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
Intoxication de route 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	$2^{32} - 1$ or $2^{56} - 1$	$2^{24} - 1$

Paramètres requis pour les voisins EIGRP:

- Si l'authentification est utilisée, les voisins doivent compléter l'authentification
- Les numéros de Système Autonome (AS) doivent correspondre
- Les adresses de port source des paquets Hello doivent être dans le même sous-réseau que l'adresse IP et le masque du routeur local pour l'interfacee à jour

CONCEPTS EIGRP

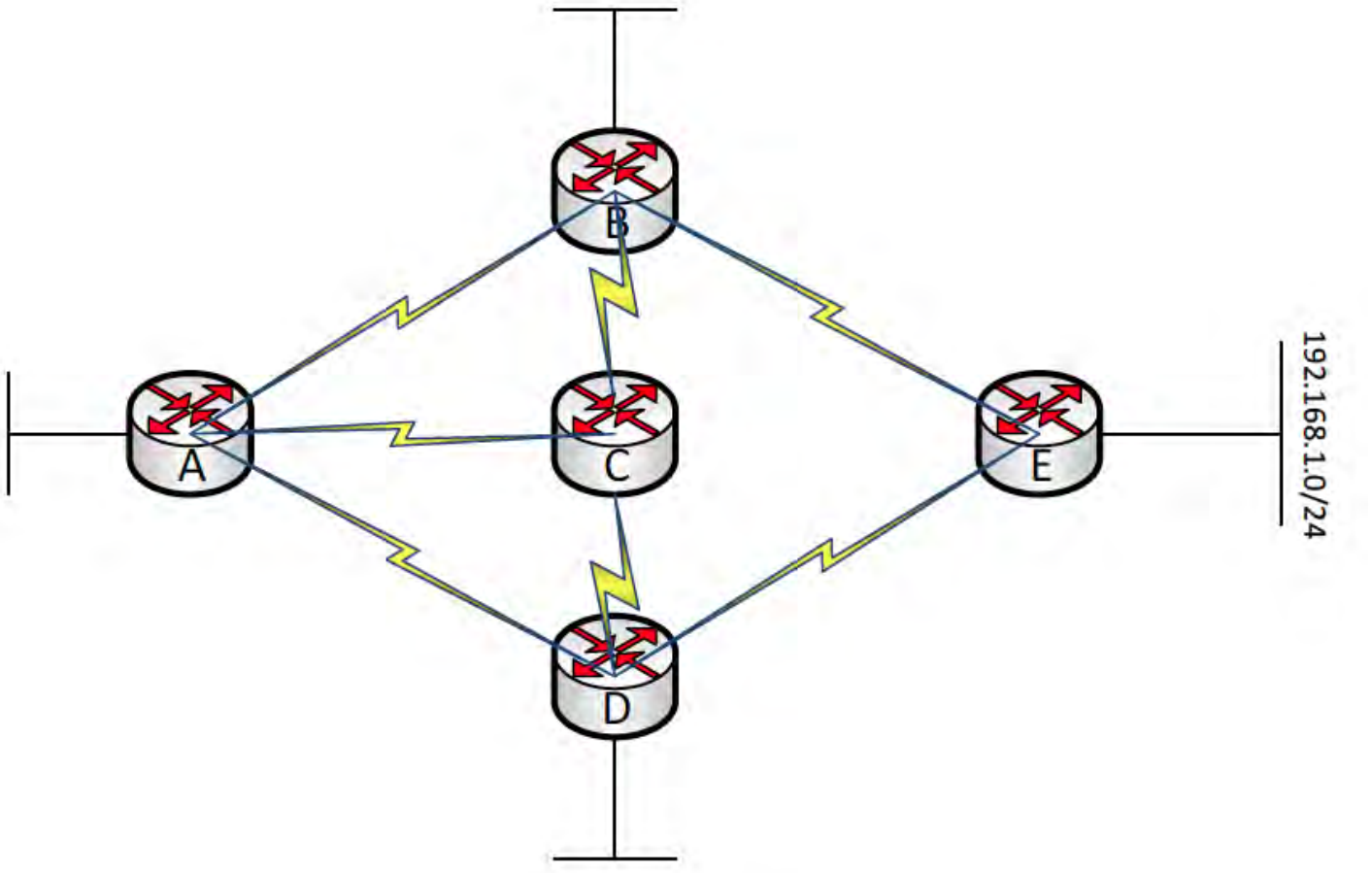
SÉLECTION DE ROUTE EIGRP

EIGRP utilise deux métriques pour déterminer la route. Ce sont celles qui suivent:

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 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.



	Metric	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.

MISE EN OEUVRE DE EIGRP POUR IPV4

CONFIGURATION DE EIGRP

Voici les étapes pour configurer un routeur pour EIGRP.
1) Entrer en mode de configuration EIGRP avec la commande **router eigrp *numéroas***. Veuillez noter que le numéro-as doit être identique sur chaque routeur. Les relations de voisinage ne s'établieront pas entre les routeurs avec des numéros d'AS différents.
2) Ajouter les déclarations **network *adresse-ip [masque-générique]*** 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 de processus de routeur eigrp **maximum-paths *nombre*** et v**ariance *multiplicateur***
7) (facultatif) Activer le résumé automatique de route avec la sous-commande de routeur eigrp **auto-summary**.

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**

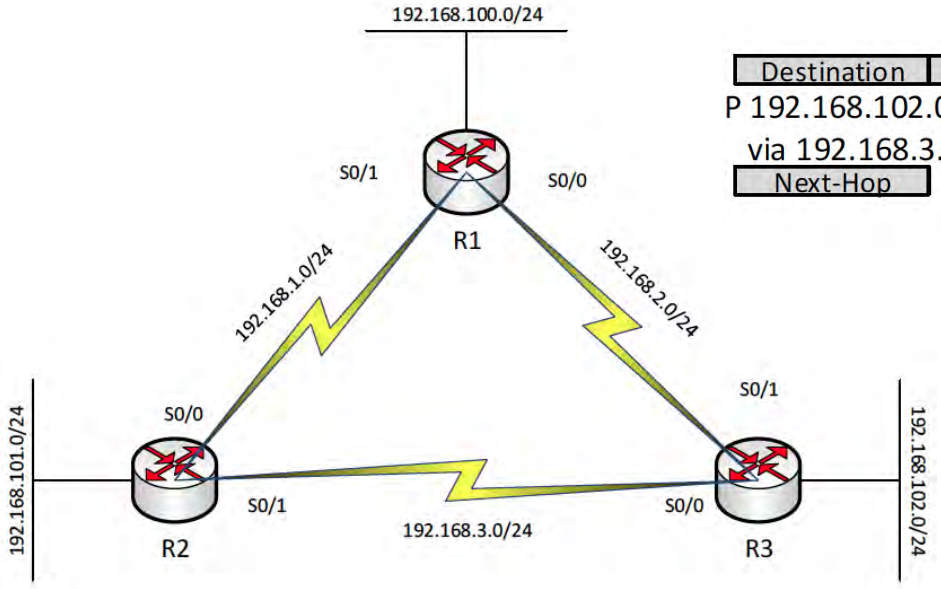
Remarque: C'est une bonne idée de ne pas modifier les minuteries par défaut. Le résumé automatique ne doit pas être utilisé sur les réseaux non contigus.

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

MISE EN OEUVRE DE EIGRP POUR IPV4

IDENTIFIER LA ROUTE SUCCESSEUR POSSIBLE

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

Voici la sortie d'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 successeurs possibles ne sont pas ajoutées à la table de routage afin d'éviter les boucles de paquets.

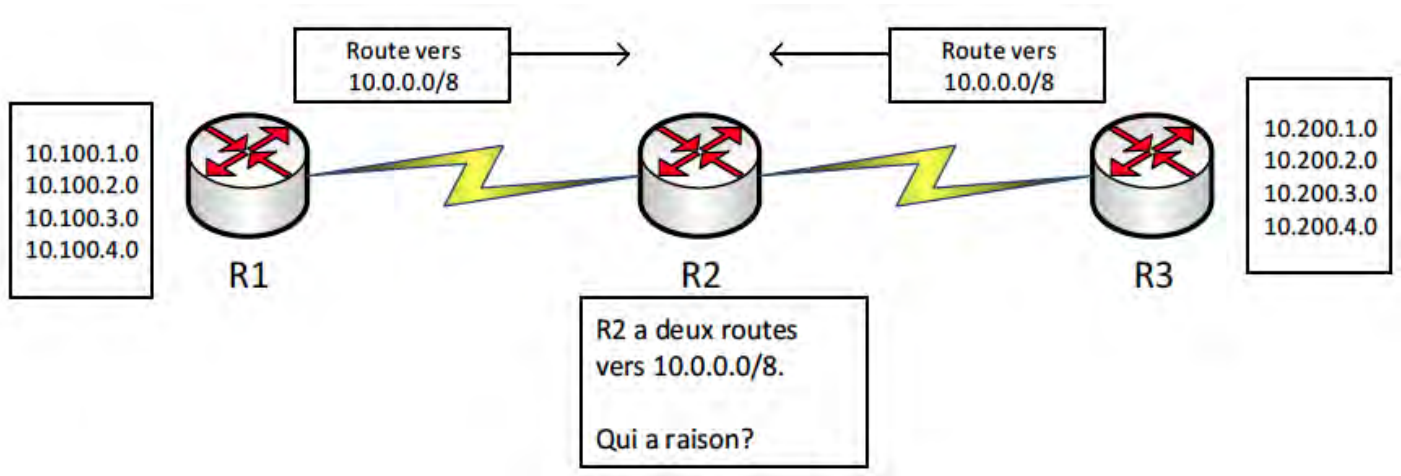
REMARQUES SUR LE RÉSUMÉ AUTOMATIQUE DE ROUTES :

Soyez très prudent lorsque vous activez le résumé automatique. Par défaut, le résumé automatique EIGRP a lieu à travers les frontières de classes. 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).les boucles de paquets.

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.

IMPLÉMENTATION DU ROUTAGE IPV6

MISE EN OEUVRE DE OSPF POUR IPV6

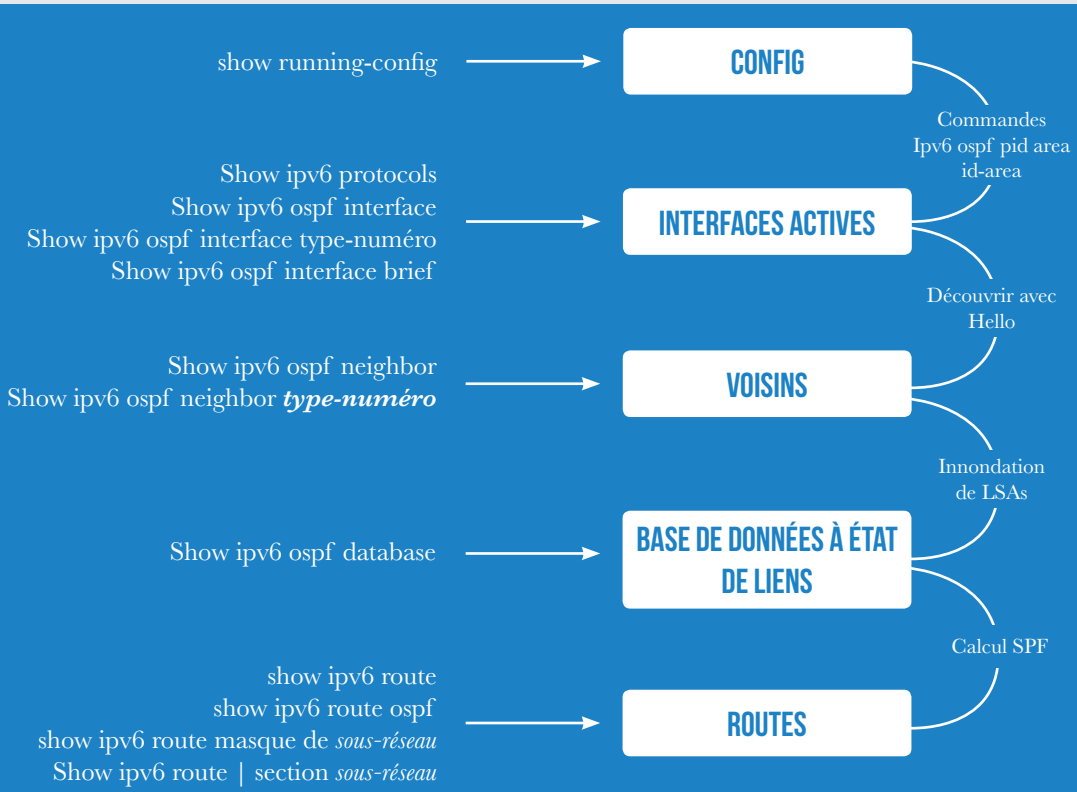
La mise en oeuvre de OSPFv3 pour IPv6 est très similaire à OSPFv2 pour IPv4, à part le fait que les commandes commençant par ip sous OSPFv2 commencent par **ipv6** dans OSPFv3.

Voici les étapes de configuration de OSPFv3 pour IPv6. (Assurez-vous d'activer **ipv6 unicast-routing** d'abord)

1. Créer le processus de routeur OSPFv3 avec la commande **ipv6 router ospf** ***id-processus***.
2. Mettre l'ID de routeur OSPF manuellement, dépendre de l'adresse loopback IPv6 la plus élevée, ou bien dépendre de l'adresse IPv6 la plus élevée sur une interface physique
3. Configurer chaque interface qui participera à OSPFv3 en ajoutant la sous-commande d'interface **ipv6 ospf** ***id-processus*** **area** ***numéro-area***
4. Définir les interfaces à fonctionnement passif avec la sous-commande **passive-interface** ***type numéro***.

Voici un exemple de configuration OSPFv3 d'un routeur dans l'area 0:

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



COMMANDES DE CONFIGURATION ET DE VÉRIFICATION DE OSPFV3

DIFFÉRENCES ENTRE OSPFV3 ET OSPFV2

Bien que les deux versions de OSPF soient les mêmes, des différences significatives existent:

Dans OSPFv3, le nom de la LSA de Type 3 est différent de OSPFv2.
Les voisins dans OSPFv3 n'ont pas besoin d'être dans le même sous-réseau, tandis que OSPFv2 exige que les voisins soient dans le même sous-réseau.
OSPFv3 a de nouveaux types de LSA qui ne sont pas utilisés dans OSPFv2.
Les types de LSA 1, 2 et 3 ont des éléments internes différents par rapport à OSPFv2.

MISE EN OEUVRE DE OSPF POUR IPV6

Influencer la métrique OSPF pour toute route est souhaitable lorsque le trafic entre deux points devrait suivre un certain chemin. Ce chemin peut être le moins encombré ou avoir la 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. Définir le coût manuellement avec la sous-commande d'interface **ipv6 ospf cost** valeur où la valeur est comprise entre 1 et 65.535.
2. Régler la bande passante sur l'interface avec la sous-commande d'interface **bandwidth** vitesse où la vitesse est mesurée en Kbps. Laisser ensuite le processus de routage déterminer la valeur par le calcul de la **bande passante de référence / bande passante d'interface**
3. Définir manuellement la bande passante de référence sur l'interface avec la sous-commande d'interface **auto-cost reference-bandwidth** ***ref-bp*** où ***ref-bp*** est en Mbps

Rappel – la vitesse de bande passante d'interface est en Kbps et la bande passante de référence est en Mbps !!

SIMILITUDES ENTRE OSPFV2 ET OSPFV3

Voici les similitudes entre OSPFv2 et OSPFv3:

- Termes et conception liés à l'area
- Activation du processus de routage sur chaque interface pour une area en particulier
- Le processus de découverte de voisin est le même avec les paquets Hello
- La transition entre l'établissement de voisinage à la topologie complète
- Les états Full et 2-way ont la même signification dans les deux protocoles
- Les types de LSA 1, 2 et 3 et la base de données d'états de liens sont les mêmes
- L'algorithme SPF est le même dans les deux protocoles
- Les adresses de multicast réservées pour les mises à jour dans OSPFv3 (FF02::5 pour tous les
- routeurs OSPF, FF02::6 pour les routeurs DR) fonctionnent de la même façon 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 area.
Une interface passive ne formera pas des relations de voisinage avec d'autres routeurs de l'area.

Lors de l'examen des relations de voisinage OSPFv3, assurez-vous que les interfaces sont dans les areas appropriées. Si les interfaces sont dans les areas correctes, vérifiez que les interfaces ne sont pas configurées pour un fonctionnement passif.

CONDITIONS POUR VOISINS POUR OSPFV2 ET OSPFV3

CONDITIONS	OSPFV2	OSPFV3
Les interfaces doivent être dans un état up/up	Oui	Oui
Les interfaces de voisins doivent être dans le même sous-réseau	Oui	Non
Les ACLs ne doivent pas filtrer les messages de protocole de routage	Oui	Oui
L'authentification du voisin doit être complète, si elle est configurée	Oui	Oui
Les minuteries hello et dead requises doivent correspondre	Oui	Oui
Des ID de routeurs uniques exigés?	Oui	Oui
Utilisation du même ID de processus sur la configuration du routeur obligatoire	Non	Non

CONDITIONS POUR VOISINS POUR OSPFV2 ET OSPFV3

CONDITIONS	COMMANDE POUR ISOLER LE PROBLÈME
Passer l'authentification de voisin	show ipv6 ospf interface
Faire correspondre les minuteries Hello et dead	show ipv6 ospf interface
Doivent être configurés pour la même area	show ipv6 ospf interface brief, show ipv6 protcols
Des ID de routeurs uniques exigés	show ipv6 ospf
Les interfaces peuvent ne pas être passives	show ipv6 ospf interface

MISE EN OEUVRE DE OSPF POUR IPV6

LA BASE DE DONNÉES DE L'ÉTAT DES LIENS ET LES LSAS DE OSPFV3

Voici les trois types clés de LSA pour OSPFv3:

Un LSA de Type 1 (LSA de routeur) pour chaque routeur dans l'area, y compris les routeurs à la frontière de l'area.
Un LSA de Type 2 LSA (LSA de réseau) pour chaque réseau avec un routeur désigné et un voisin d'un routeur désigné.
Un LSA de Type 3 (préfixe interarea) pour chaque sous-réseau IPv6 / préfixe situé dans une area différente.

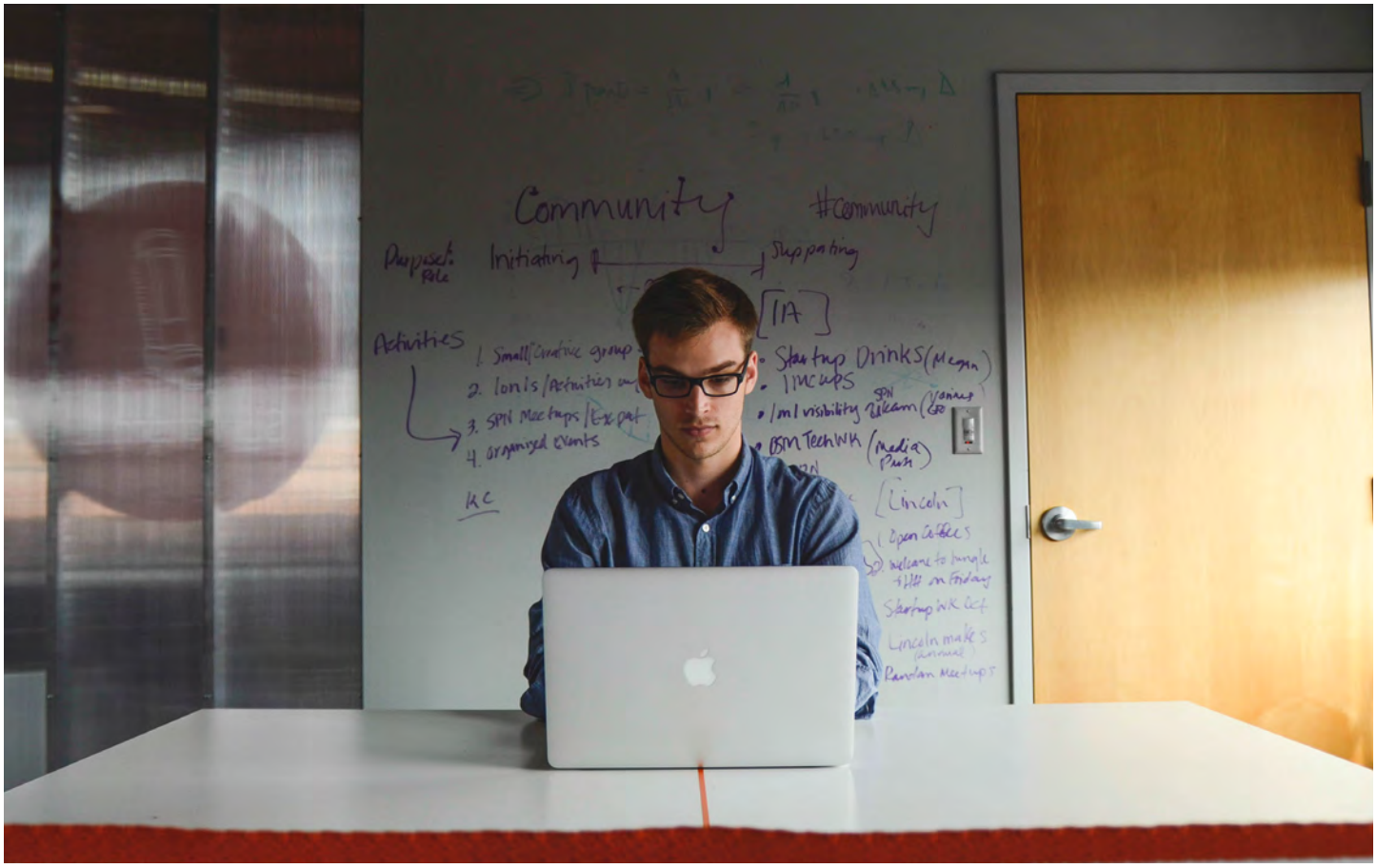
OSPFV3 ET AUCUNE ROUTE VERS UN SOUS-RÉSEAU

Quand aucune route n'existe vers un sous-réseau dans la table de routage, il est préférable de travailler à rebours à partir du sous-réseau. Utiliser ces tâches pour vérifier le sous-réseau
1) Vérifier les routeurs directement connectés au sous-réseau et assurezvous que l'IPv6 est activé sur les interfaces. OSPFv3 doit être activé sur ces interfaces.
2) Vérifier 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 la route vers une destination est sous-optimale ou semble être la mauvaise route, vérifier les éléments suivants:

1) Vérifier les relations de voisinage entre les routeurs sur le chemin optimal
2) Vérifier les paramètres de coût OSPFv6 sur les interfaces formant le meilleur chemin



MISE EN OEUVRE DE OSPF POUR IPV6

COMPARAISON ENTRE LES COMMANDES EIGRPV4 ET EIGRPV6

FONCTION	EIGRPV4	EIGRPV6
Créer le processus de routage, définir le numéro de AS	**router eigrp** numéro-as	**ipv6 router eigrp** numéro-as
Définir manuellement l'ID de routeur	**eigrp router-id** numéro	Pareil que EIGRPv4
Définir ou changer le nombre de chemins concurrents	**maximum-paths** numéro	Pareil que EIGRPv4
Définir ou changer le multiplicateur de variance	**variance** multiplicateur	Pareil que EIGRPv4
Affecter la métrique de calcul (interface)	**bandwidth** valeur, **delay** valeur	Pareil que EIGRPv4
Changer les minuteries hello et hold	**ip hello-interval eigrp** temps asn **ip hold-time eigrp** temps asn	Changer **ip** en **ipv6**
Activer EIGRP sur une interface	**network ip-address** [masque générique]	**ipv6 eigrp** numéro-as (souscommande d'interface)
Activer et désactiver le résumé automatique (commande de routeur)	**[no] auto-summary**	Non requis pour EIGRPv6

EXIGENCES POUR VOISINS POUR EIGRP V4 ET EIGRPV6

EXIGENCES	EIGRPV4	EIGRPV6
Les interfaces doivent être dans un état up/up	Oui	Oui
Le interfaces de voisins doivent être dans le même sous-réseau	Oui	Oui
Les ACLs ne doivent pas filtrer les messages de protocole de routage	Oui	Oui
L'authentification du voisin doit être complète, si elle est configurée	Oui	Oui
Les minuteries hello et dead exigées doivent correspondre	Non	Non
Des ID de routeurs uniques exigés?	Non	Non
Les valeurs K doivent correspondre	Oui	Oui

Exemple de configuration EIGRPv6 pour R1:

```
!
ipv6 router eigrp 2
  eigrp router-id 3.3.3.3
!
interface Serial0/0/0
  ipv6 address 2020:CCDD:15:15::2/64
  ipv6 eigrp 2
!
```

Comme vous pouvez le voir, nous avons démarré EIGRPv6 avec un numéro de AS de 2 et un ID de routeur 3.3.3.3. Nous avons également mis l'adresse IPv6 sur l'interface Serial0/0/0 et commencé à annoncer le réseau via EIGRPv6

PRINCIPALES DIFFÉRENCES ENTRE EIGRPV6 ET EIGRPV4

Bien que les deux protocoles fonctionnent d'une manière similaire, il existe des différences significatives entre les deux protocoles:

EIGRPv4 annonce des sous-réseaux, tandis que EIGRPv6 annonce des préfixes. Les commandes **show** de EIGRPv4 utilisent **ip** alors que les commandes **show** de EIGRPv6 utilisent **ipv6**.

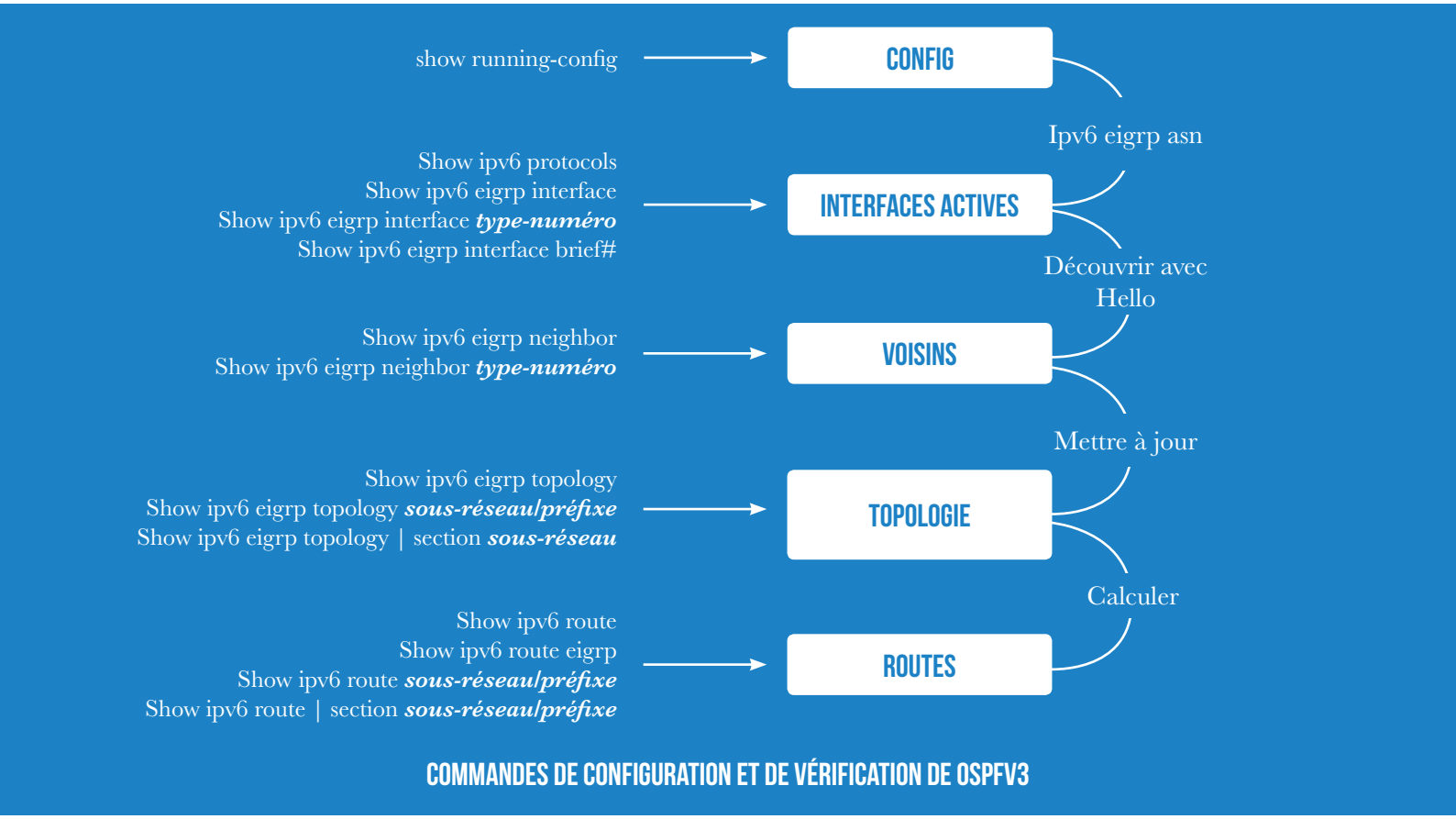
Alors que EIGRPv4 et EIGRPv6 utilisent le même processus pour devenir voisins, les routeurs EIGRPv6 peuvent devenir voisins s'ils sont dans différents sous-réseaux. On notera que les voisins EIGRPv4 doivent être dans le même sous-réseau.
EIGRPv6 peut effectuer le résumé automatique des routes, mais EIGRPv4 n'a pas de résumé automatique disponible.

DÉPANNAGE DE ROUTES EIGRPV6

Vérifier ces éléments pour trouver la raison pour laquelle un sous-réseau IPv6 est inaccessible:
1) Vérifier les routeurs directement connectés associés au sous-réseau. EIGRPv6 doit être activé sur les interfaces pour annoncer la route
2) Vérifier les relations de voisinage EIGRPv6 pour les routeurs entre le routeur local et le sous-réseau. Si certaines relations sont rompues, localiser la raison et résoudre.

S'il existe une route vers le sous-réseau mais le chemin n'est pas optimale, vérifier les points suivants:
1) Vérifier les relations de voisinage rompues le long du chemin optimal et résoudre les problèmes.
2) Vérifier le délai d'interface et les paramètres de bande passante. Rechercher la bande passante la plus lente sur la route. EIGRP utilise la bande passante la plus lente pour sa topologie de routage

MISE EN OEUVRE DE OSPF POUR IPV6



COMMANDES DE CONFIGURATION ET DE VÉRIFICATION DE OSPFV3

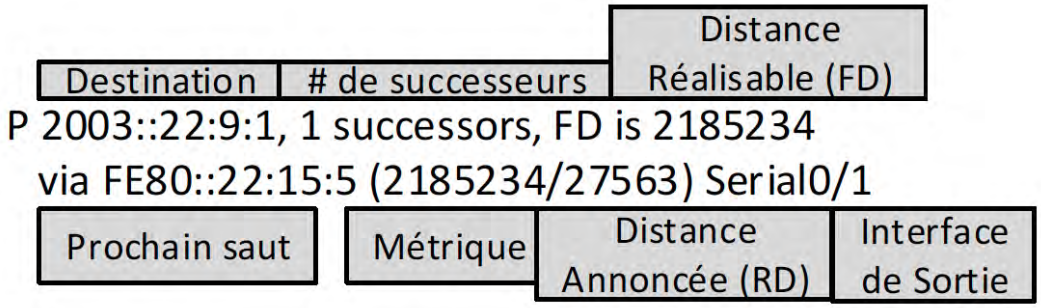
Comme OSPFv3, EIGRPv6 a un ID de routeur également. Le router-id de EIGRP est défini par l'une des règles suivantes dans l'ordre:

1) Configuré manuellement par la commande **ipv6 eigrp router-id**

2) L'adresse IP la plus élevée numériquement sur une interface loopback

3) L'adresse IP la plus élevée numériquement sur une interface physique

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



RÉSOLUTION DE PROBLÈME

DÉPANNAGE COMMUTATION LAN

POINTS CLÉS DE DÉPANNAGE:

Quel est le fonctionnement réseau normal: Le fonctionnement normal du réseau sert de base pour comparer la situation actuelle. Trouver comment les paquets sont censés voyager entre la source et la destination. Tracer le chemin du paquet de la source à la destination.

Où se situe le problème: Un changement récent a-t-il eu lieu? Utiliser ping ou traceroute pour localiser les endroits où peut se trouver le problème. Se rappeler de regarder les symptômes.

- Examiner le chemin de couche 3 et localiser tout problème possible entravant le chemin
- Examiner tout segment de couche 2 et localiser le problème tel que des ports bloqués, des filtres d'adresses MAC, ou tout ce qui pourrait arrêter une trame Ethernet.

Analyse des causes fondamentales: Pourquoi le problème s'est produit? Est-ce qu'un mauvais câble ou une mauvaise interface est présente?
- Continuez à isoler le problème jusqu'à ce que la cause soit trouvée
- Si vous ne pouvez pas isoler le problème globalement, isolez le problème à un équipement et faites un changement pour voir ce qui arrive.

Utilisez les trois premières couches du modèle OSI pour le dépannage:
Regardez la couche physique, la couche de liaison de données puis la couche réseau. Si vous pouvez isoler la couche, vous pouvez probablement isoler le composant.

CODES DE STATUT POUR LES INTERFACES D'UN COMMUTATEUR ETHERNET:

STATUT D'INTERFACE	STATUT DE LA LIGNE	STATUT DU PROTOCOLE	CAUSE TYPIQUE
Disabled	Admin. down	down	L'interface est arrêtée avec la commande shutdown
notconnect	down	down	Aucun câble, mauvais câble, brochage incorrect (droit vs croisé), disparité de vitesse, disparité des duplex, l'équipement à l'autre bout est éteint ou l'interface est arrêtée.
notconnect	up	down	Inattendu sur des interfaces LAN
err-diabled	down	down (errdisabled)	L'interface est désactivée en raison de la sécurité du port. Vu également quand les interfaces EtherChannel ne correspondent pas aux autres interfaces dans le groupe de canaux
connected	up	up	L'interface fonctionne

TRANSMET SUR 1,2 REÇOIT SUR 3,6	TRANSMET SUR 3,6 REÇOIT SUR 1,2
PC NIC	Concentrateurs
Routeurs	Commutateurs
Points d'Accès Sans Fil	-
Imprimantes Ethernet	-

RÉGLAGES DE VITESSE ET DE DUPLEX PAR DÉFAUT :

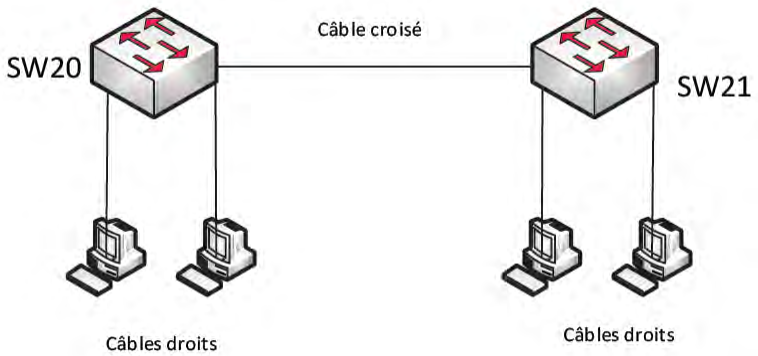
10 Mbps – semi-duplex par défaut
100 Mbps – semi-duplex par défaut
1 Gbps et plus – duplex intégral par défaut

Pour 10 Mbps et 100 Mbps, vous pouvez vouloir mettre les interfaces à duplex intégral pour éviter les problèmes de duplex

PROBLÈMES DE VITESSE ET DE DUPLEX:

Vitesse: S'il existe une non-concordance des vitesses, les interfaces de part et d'autre seront arrêtées suivant le statut d'interface pour chaque équipement
Duplex: S'il existe une non-concordance des duplex, une interface ne présentera aucun problème mais l'interface mis à semi-duplex (Half-Duplex) aura des erreurs. Une commande show interface montrera un nombre croissant de messages d'erreurs sur l'interface.

Note – il est hautement souhaitable de mettre la vitesse et le duplex manuellement sur les ports
Ethernet connectant les commutateurs et les routeurs.



DÉPANNAGE COMMUTATION LAN

Deux problèmes peuvent empêcher aux paquets de faire leur chemin sont la sécurité de port et le filtrage d'adresses MAC:

Filtrage d'adresses MAC – Faire un **show running-config** sur le commutateur et chercher des adresses statiques MAC configurées pour être rejetées. Ensuite, regarder l'adresse MAC source de la trame venant du commutateur précédent (ou en amont).

Sécurité de port – Faire une commande **show port-security** sur le commutateur et chercher les interfaces configurées pour la sécurité de port et leurs statuts.

SW1# **show port-security**

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
Fa0/1	1	1	1	Shutdown

LES ACTIONS DE SÉCURITÉ DE PORT

OPTIONS DE VIOLATION DE SÉCURITÉ DE PORT SWITCHPORT	PROTECT	RESTRICT	SHUT DOWN (DÉFAUT)
Rejette le trafic fautif	Oui	Oui	Oui
Rejette tout trafic, arrête l'interface	Non	Non	Oui
Incrémente le compteur de violation pour chaque trame en violation	Non	Oui	Oui

LES COMMANDES DE COMMUTATEUR POUR TROUVER LES PORTS D'ACCÈS ET LES VLANS

COMMANDE	DÉSCRIPTION
show vlan	Liste chaque VLAN et les interfaces associées (exclut les trunk)
show vlan brief	Liste une version plus courte de la commande show vlan
show vlan id num	Liste les ports d'accès et trunk dans le VLAN
show interfaces type numéro switchport	Identifie les VLANs associés à l'interface et le trunk
show mac address-table dynamic	Liste les adresses MAC dans la table et les VLANs associés

Étapes et exemples de configuration de sécurité de port

Étape 1: Régler l'interface en tant que port d'accès ou port trunk avec la commande d'interface access ou switchport mode trunk

Étape 2: Activer la sécurité de port via la commande d'interface switchport port-security

Étape 3: (Facultatif) Fixer le nombre maximum d'adresses MAC permises sur l'interface en utilisant la commande d'interface switchport port-security maximum nombre

Étape 4: (Facultatif) Préciser l'action à prendre lors d'une violation de sécurité avec la commande switchport port-security violation {protect | restrict | shutdown}

Étape 5: (Facultatif) Mettre les adresses MAC autorisées pouvant traverser avec la commande switchport port-security mac-address adresse-mac

Étape 6: (Facultatif) Configurer le commutateur pour se souvenir des adresses MAC apprises sur l'interface avec la commande switchport port-security mac-address sticky

Étapes de Configuration:

SW1(config)# **interface FastEthernet0/1**	Selection de l'interface
SW1 (config-if)# **switchport mode access**	Règle le port comme un port d'accès
SW1 (config-if)# **switchport port-security**	Active la sécurité de port

LISTER LES VLAN VIA LA COMMANDE SHOW INTERFACES TRUNK

LISTE	EN-TÊTE	SORTIE
Première	VLANs autorisés	VLANs 1 à 4094 exceptés ceux supprimés par la commande switchport trunk allowed vlan
Deuxième	VLANs autorisés et actifs	Pareille à la première liste mais exclut les VLANs pas presents sur le commutateur ou arrêtés
Troisième	VLANs en spanning tree	Pareille à la deuxième liste à part les interfaces bloquées par STP ou VTP

LISTER LES VLAN VIA LA COMMANDE SHOW INTERFACES TRUNK

MODE TRUNK	ACCESS	DYNAMIC AUTO	TRUNK	DYNAMIC DESIRABLE
Access	Access	Access	Access	Access
Dynamic auto	Access	Access	Trunk	Trunk
trunk	Access	Trunk	Trunk	Trunk
Dynamic desirable	Access	Trunk	Trunk	Trunk

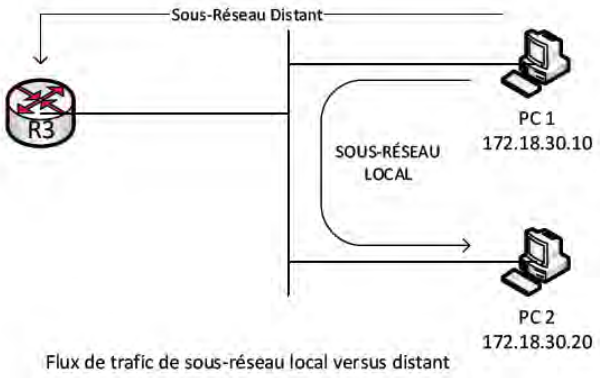
DÉPANNAGE DU ROUTAGE IP PARTIE 1

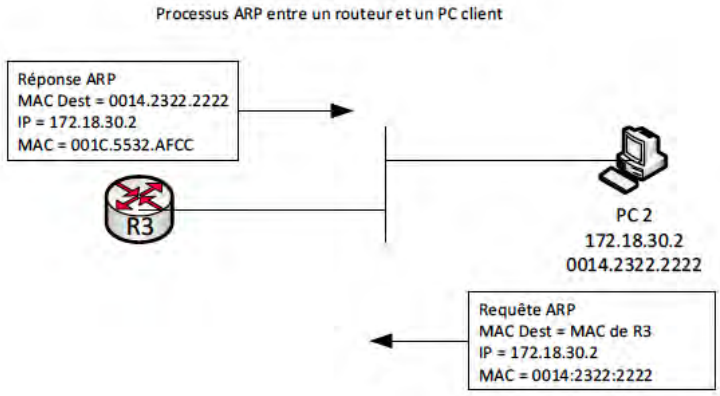
LOGIQUE DE ROUTAGE POUR LA TRANSMISSION D'UN PAQUET IPV4

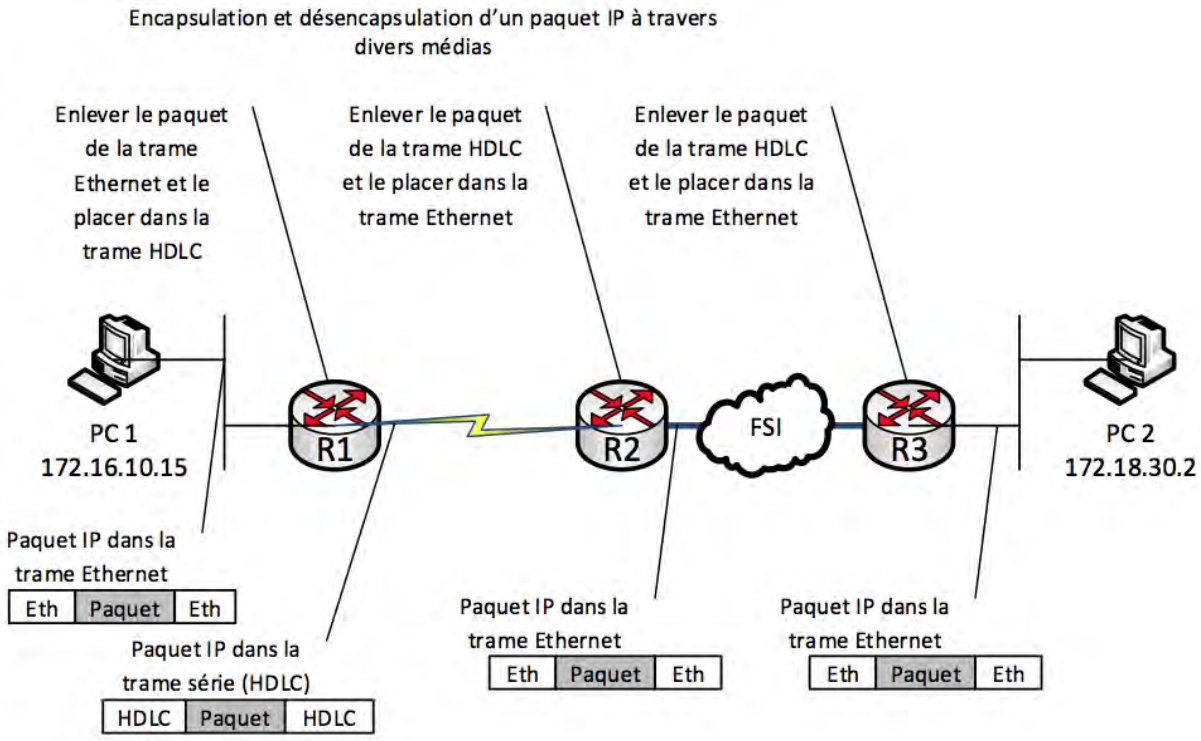
Si la destination est locale, envoyer directement à l'hôte
Trouver la MAC de destination via le Protocole de Résolution d'Adresse (ARP) à moins que l'adresse de destination se trouve déjà dans le cache ARP.
Attacher l'en-tête (header) et l'en-queue (trailer) de couche 2 avec la MAC de destination de l'hôte et envoyer la trame sur le câble.

Si la destination est en dehors du sous-réseau local, envoyer La trame au routeur/passerelle (gateway).
Trouver l'adresse MAC de la passerelle par défaut soit par le cache ARP local soit par le protocole ARP pour identifier l'adresse MAC de la passerelle par défaut
Attacher l'en-tête (header) et l'en-queue (trailer) de couche 2 avec la MAC de destination de la
passerelle par défaut et envoyer la trame sur le câble.

Basée sur la table de routage du routeur, une décision de transmission sera prise et le paquet sera envoyé vers sa destination via une des interfaces du routeur.





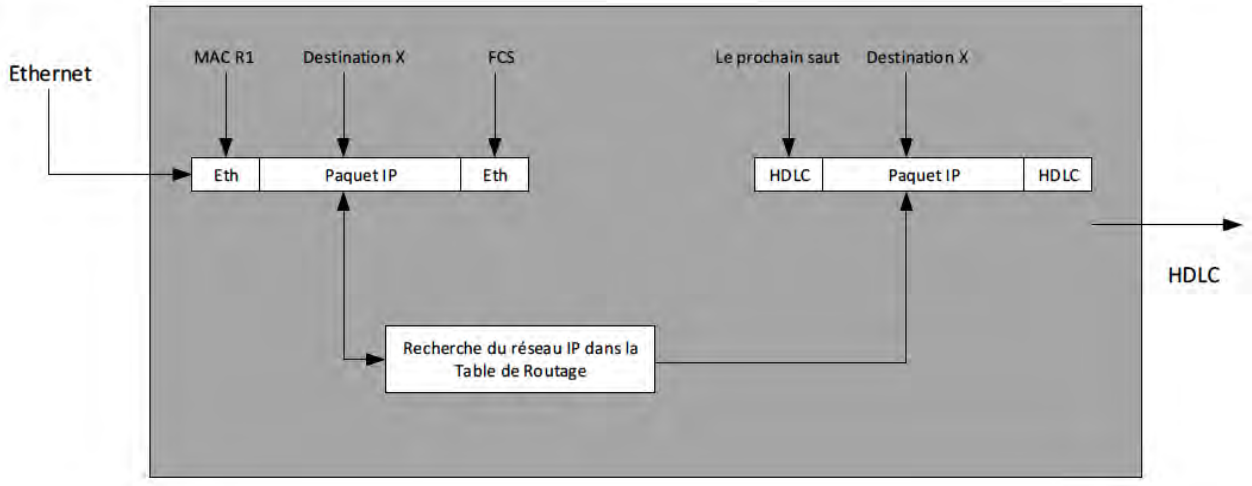


DÉPANNAGE DU ROUTAGE IP PARTIE 1

LES DÉCISIONS DE ROUTAGE AU SEIN D'UN ROUTEUR:

Traiter une trame sur une interface entrante si la séquence de contrôle de la trame est correcte et l'adresse MAC de couche 2 correspond à celle de l'interface du routeur. (Les adresses multicast et broadcast sont incluses)

Extraire de la trame le paquet de couche 3.
Prendre une décision d'acheminement basée sur l'adresse IP de destination inclu dans le paquet en utilisant des informations de la table de routage
Placez le paquet IP dans une trame Transmettre la trame sur l'interface de sortie



Ping est utilisé pour tester la connectivité entre deux extrémités.

La commande ping peut indiquer ce qui suit:
Teste le chemin de couche 3 entre les deux extrémités
Teste le chemin de couche 2 entre chaque saut

Le ping étendu a plus d'options, dont la spécification de l'IP source sur le routeur
Teste si une ACL autorise les paquets d'un hôte ou non
Teste si la sécurité d'un port est activée pour une combinaison d'adresses MAC / IP particulière
Teste si les routes entre le routeur et la destination fonctionnent

Ping sur une liaison WAN

Si un ping marche sur une liaison WAN, les énoncés suivants sont vrais:

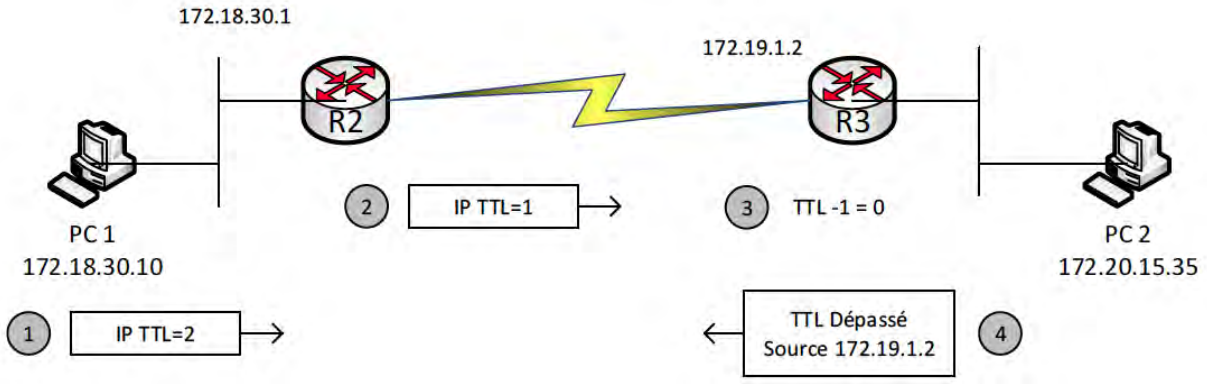
Les deux interfaces des routeurs sont up / up
Les couches 1 et 2 fonctionnent
Les ACLs entrants ne filtrent pas (ne suppriment pas) les paquets ping

Problèmes de connectivité des hôtes

Si une commande ping sur un hôte ne peut pas atteindre la destination désirée,
essayez le Ping vers le routeur par défaut. Si le routeur par défaut est inaccessible,
l'un des problèmes suivants pourrait en être la raison:

L'hôte a la mauvaise adresse IP
L'hôte n'a pas reçu une 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 / sécurité de port/ câblage / port)

DÉPANNAGE DU ROUTAGE IP PARTIE 1



Traceroute utilise les mêmes messages ICMP que la commande ping. Voici la comparaison entre les deux commandes:

Les deux envoient des messages ICMP pour tester la connectivité
Les deux répondent sur les équipements de réponse
Les deux sont largement pris en charge par de nombreux systèmes d'exploitation
L'IP ou le nom d'hôte peut être utilisé comme adresse de destination
Les routeurs ont une version étendue de chaque commande avec la possibilité de tester le routage inverse

Processus de traceroute pour le réseau ci-dessus

Étape 1 – La commande traceroute sur le PC envoie un paquet à 172.20.15.35 avec une durée de vie (TTL) de 2
Étape 2 – Le routeur R1 décrémente le TTL de 1 et transmet le paquet
Étape 3 – Le routeur R2 décrémente le TTL de 1. Le TTL est maintenant zéro. R2 rejette le paquet.
Étape 4 – Le routeur R2 envoie un message ICMP à 172.18.30.10 (l'adresse source) avec un TTL dépassé de 172.19.1.2.

Pour les paquets de traceroute successifs, la commande traceroute sur PC1 augmentera la durée de vie de 1 à chaque itération jusqu'à ce que l'hôte soit atteint ou 30 itérations (maximum) soient atteintes.

DÉPANNAGE DU ROUTAGE IP PARTIE 2

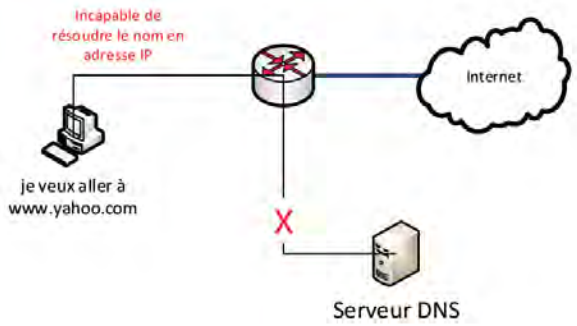
VÉRIFICATION DES PARAMÈTRES IPV4 DE L'HÔTE

1) Vérifier les serveurs DNS configurés par rapport aux adresses IP réelles des serveurs DNS
2) Vérifier les paramètres du routeur par défaut (gateway) configuré par rapport à la configuration de l'adresse IP sur le routeur
3) Vérifier le masque de sous-réseau configuré sur l'hôte
4) L'hôte et le routeur doivent être dans le même sous-réseau. Cela signifie que les deux adresses IP hôte et routeur doivent être dans la même plage d'adresses IP déterminée par le masque de sous-réseau.

PROBLÈMES DE DNS

L'échec dans la résolution DNS peut être causé par les problèmes suivants:
- L'hôte ou le routeur ne peut pas contacter le serveur DNS en raison d'un problème de connectivité
- Les paramètres du serveur DNS sont incorrects

Le PC ne peut pas résoudre www.yahoo.com en une adresse IP en raison d'une panne de connectivité. Cela peut aussi se produire lorsque l'adresse du serveur DNS configurée est incorrecte ou s'il n'existe pas de route vers le sous-réseau



CONFIGURATION DU "ROUTER ON A STICK" (ROAS)

Côté Routeur:

Pour chaque VLAN qui ne sera pas un VLAN natif, procéder comme suit:
1) Créer une sous-interface unique pour chaque VLAN
2) Utiliser la commande encapsulation dot1q vlan-id pour activer le 802.1Q
3) Régler l'adresse IP sur la sous-interface

Pour le VLAN natif, procéder comme suit:

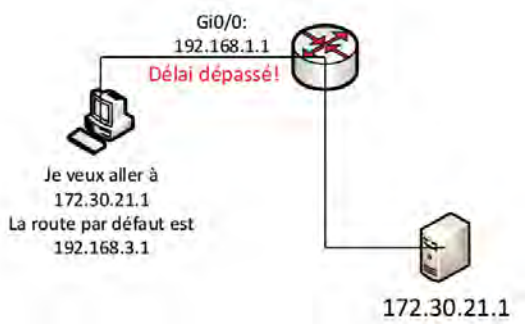
1) Créer la sous-interface et utiliser encapsulation dot1q vlan-id native pour définir la sousinterface native de VLAN, ou
2) Régler l'adresse IP sur l'interface physique sans commande encapsulation dot1q

Côté commutateur:

1) Sur l'interface, activer le trunking en utilisant la commande switchport mode trunk
2) Mettre le VLAN natif avec la commande d'interface switchport trunk native vlan vlan-id

Vérifier les configurations RoaS suivantes:

- Le commutateur doit avoir activé le trunking
- Le commutateur doit définir le VLAN natif correct si un VLAN natif est configuré sur le routeur
- Le commutateur doit connaître tous les VLAN configurés sur le routeur



CONFIGURATION DE ROUTE PAR DÉFAUT

Si une route par défaut ou passerelle par défaut est configurée de manière incorrecte, les hôtes pourront accéder à des ressources sur le même sous-réseau LAN, mais les hôtes ne pourront pas accéder à des ressources en dehors du sous-réseau.

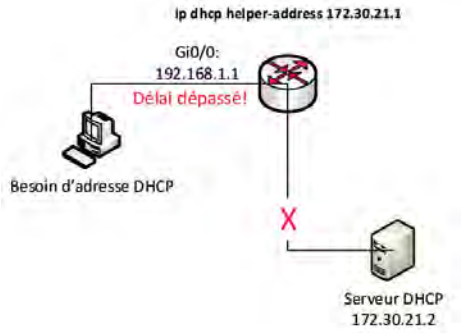
DÉPANNAGE DU ROUTAGE IP PARTIE 2

Un échec entre un hôte et un routeur sur un LAN peut être causé par un des deux problèmes

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

DESCRIPTIONS DES DÉFAILLANCES D'INTERFACE LAN

ÉTAT D'INTERFACE	RAISON	DESCRIPTION
Down/down	Speed mismatch	Les interfaces communiquent à des vitesses différentes, car la vitesse est réglée en statique sur les deux interfaces
Admin down/down	Shutdown	L'interface est arrêtée manuellement avec la commande shutdown
Down/down	Err-disabled Down/down (switch)	La sécurité de port a désactivé le port
Down/down	No cable or bad cable	Le câble n'est pas connecté ou le brochage du Down/down câble est incorrect



PROBLÈMES DE RELAIS DHCP:

Si un hôte ne peut pas recevoir d'information DHCP à partir d'un serveur DHCP, l'un de ceux-ci pourrait avoir lieu

- Problème de connectivité entre l'hôte et le serveur DHCP
- Mauvaise adresse DHCP helper configurée dans le routeur
- Problème de connectivité entre le routeur et le serveur DHCP distant

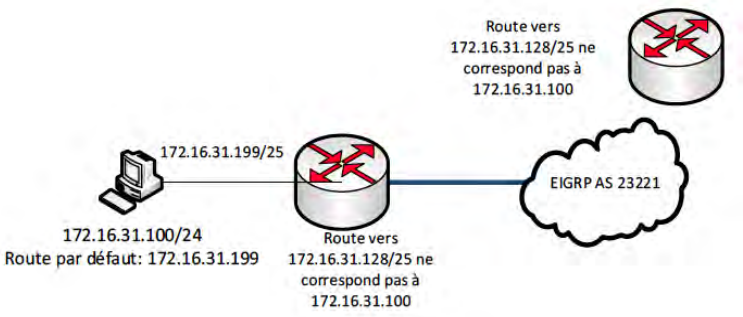
Dans cet exemple, le routeur ne dispose pas de connectivité au serveur DHCP donc le trafic DHCP n'atteindra pas sa destination voulue.

Rappelez-vous que le routeur utilisera la plus longue correspondance de préfixe pour acheminer le paquet. Le routeur enverra le paquet à l'ID de réseau ou de sous-réseau le plus spécifique.

Par exemple, ces routes sont dans la table de routage:

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

Si un paquet arrive 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 Ethernet0/0 car Ethernet0/0 a un ID de sous-réseau plus spécifique.



Disparité entre le masque de sous-réseau de l'hôte et du routeur.

Ici, nous avons un hôte avec un masque /24 et le routeur a un masque /25 (.129 à .254). Tandis que le routeur passera le trafic de l'hôte vers le réseau, le routeur distant n'aura qu'une route pour 172.16.31.128/25 qui exclut 172.16.31.100 (l'adresse IP de l'hôte).

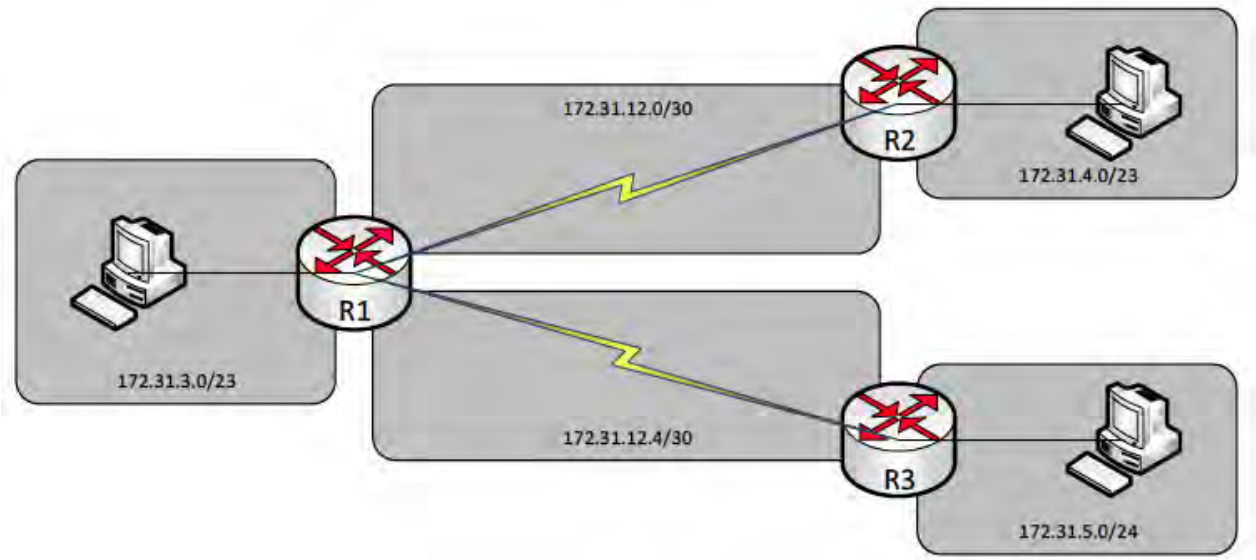
Il existe deux façons de corriger ce problème. La première consiste à corriger le masque de sous-réseau sur l'hôte et l'autre consiste à corriger le masque de sousréseau sur le routeur et s'assurer que le routeur publie le sous-réseau correct.

DÉPANNAGE DU ROUTAGE IP PARTIE 2

CHEVAUCHEMENT DE SOUS-RÉSEAUX VLSM

Sur un seul routeur, le routeur peut empêcher le chevauchement VLSM lorsqu'une commande d'interface ip address est configurée pour chevaucher avec une commande ip address déjà existante.

Toutefois, IOS ne peut pas détecter les souscommandes ip address placées sur différents routeurs. Par conséquent, le chevauchement VLSM ne peut être évité qu'au sein d'un même routeur.



Dans cet exemple, R2 a un sous-réseau chevauchant avec R3. La confusion se produit dans R1 quand les routes pour 172.31.4.0/23 et 172.31.5.0/24 sont reçues par R1. Le routeur ne saura pas où envoyer les paquets parce que la table de routage ne cesse de changer.

La solution consiste alors à modifier le sous-réseau sur R2 ou R3 afin d'éliminer le chevauchement. Par exemple, si l'on change le masque de sous-réseau sur R2 à /24, la table de routage convergera et le trafic atteindra sa destination visée.

DÉPANNAGE DES PROTOCOLES DE ROUTAGE IPV4

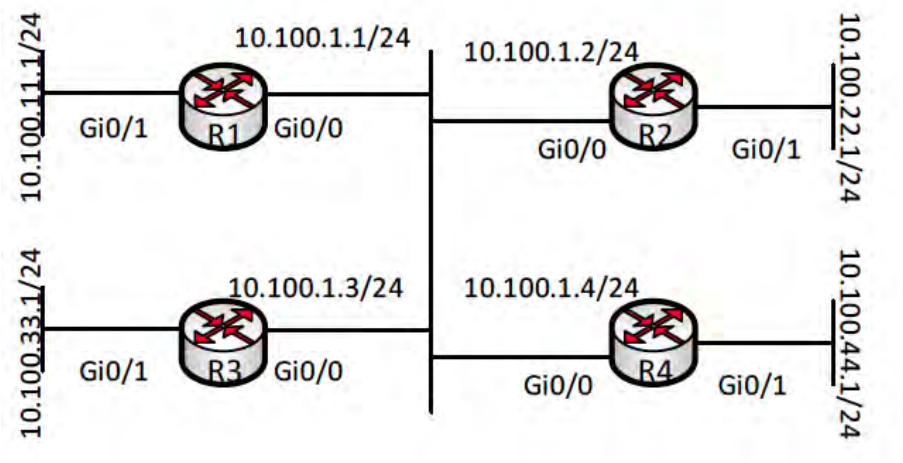
RÈGLES CLÉS POUR LE DÉPANNAGE DES PROTOCOLES DE ROUTAGE DANS LES QUESTIONS D'EXAMEN

1) Tout lire et regarder soigneusement
2) Tout lire et regarder soigneusement à nouveau
3) Regarder les interfaces où le protocole de routage doit être actif. Les relations de voisinage doivent être prévues
4) Vérifier que chaque interface prévue pour exécuter le protocole de routage a le protocole activé. Sinon, régler et vérifier à nouveau
5) 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.

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



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

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 configuration du réseau regroupées par processus de routage, y compris les interfaces passives	OUI

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 DES PROTOCOLES DE ROUTAGE IPV4

DÉPANNAGE OSPF POUR L'EXAMEN:

1) Examiner la configuration et assurez-vous que chaque routeur a des interfaces dans les aires appropriées.

2) 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.

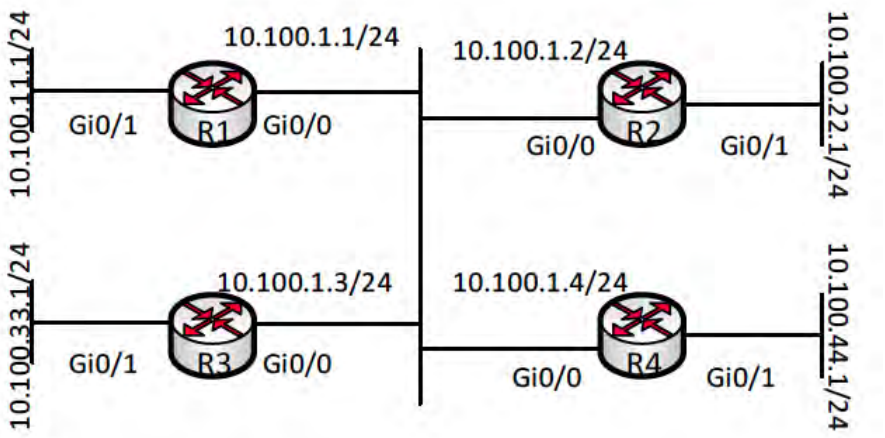
3) Vérifier que les relations de voisinage sont formées entre les routeurs appropriés.

4) 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.

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 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 passer l'authentification de voisin si configuré	Oui	Oui
Doit utiliser le même AS dans la commande de 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 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)	show ip ospf

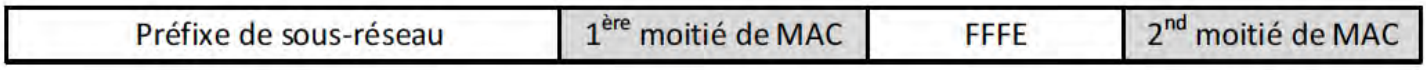
EXIGENCES POUR VOISIN EIGRP ET COMMANDES SHOW/DEBUG APPROPRIÉES

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

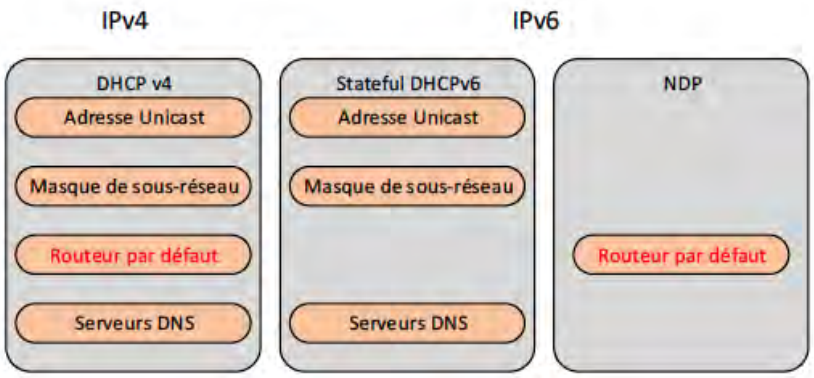
DÉPANNAGE DU ROUTAGE IPV6

TYPES D'ADRESSES IPV6

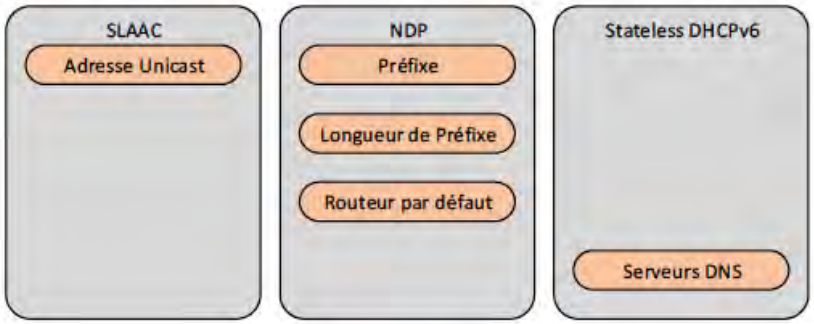
TYPE	PREMIERS CHIFFRES	COMME IPV4 PRIVÉE OU PUBLIQUE?
Global Unicast	2 à E	Publique
Unique local Unicast	FD	Privée
Link-local	FE80	Ni privée ni publique – Aucune comparaison directe



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



Sources d'information pour IPv6 Stateful DHCP



Sources d'information pour IPv6 Stateless DHCP

Exemple: Utilisant les règles de EUI-64, tirer la partie hôte de l'adresse IPv6 sur la base d'une adresse MAC 00: 1E: EB: C2: 25: 24

Étape 1: Diviser l'adresse MAC en deux et insérer FFFE entre les deux moitiés. Changer le résultat en un nombre de 64 bits.
Résultat: 001F: EBFF: FEC2: 2524

Etape 2: Prendre les deux premiers chiffres hexadécimaux, convertir en binaire, inverser le septième bit, et reconvertir en hex.

Les deux premiers chiffres sont 00, donc inverser le septième bit donne 0000 0010 ou 02.

L'adresse hôte EUI-64 résultante est 021E: EBFF: FEC2: 2524

CONFIGURATION DES ADRESSES IPV6 SUR LES ROUTEURS:

1) Activer le routage IPv6 avec la commande **ipv6 unicast-routing**
2) Utiliser la sous-commande d'interface **ipv6 address** ***adresse/longueur*** pour activer IPv6 sur chaque interface utilisant IPv6

DÉPANNAGE DU ROUTAGE IPV6

DÉPANNAGE DES PROBLÈMES DE IPV6

Problèmes liés aux hôtes:
1) Les hôtes doivent être dans le même sous-réseau IPv6 que le routeur par défaut
2) Les hôtes doivent utiliser la même longueur de préfixe que le routeur par défaut
3) L'hôte doit pointer vers une adresse de routeur réelle comme routeur par défaut
4) Les adresses DNS doivent être correctes sur chaque hôte

Problèmes liés aux Routeurs
1) Les interfaces des routeurs doivent être dans un état up/up pour passer le trafic
2) Deux routeurs locaux doivent avoir des adresses dans le même sous-réseau IPv6
3) Les routeurs doivent avoir des routes IPv6 vers tous les sous-réseaux IPv6 dans la conception

Problèmes de filtrage (routeurs et commutateurs)
1) Vérifier le filtrage d'adresses MAC sur les ports de commutation et commutateurs (surtout les mappages statiques d'adresses MAC)
2) Assurez-vous que les VLAN nécessaires sont sur les commutateurs. Des VLAN manquants sur un commutateur ne passeront pas le trafic
3) Tout comme pour les routeurs IPv4, surveiller les listes de contrôle d'accès (ACL) sur les routeurs IPv6

Le routeur par défaut (gateway) ne parvient pas à répondre aux pings de l'hôte

Vérifier les points suivants lorsque les pings échouent entre un hôte et son routeur par défaut:

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

Échec de résolution DNS

Vérifier les points suivants lorsque la résolution DNS échoue

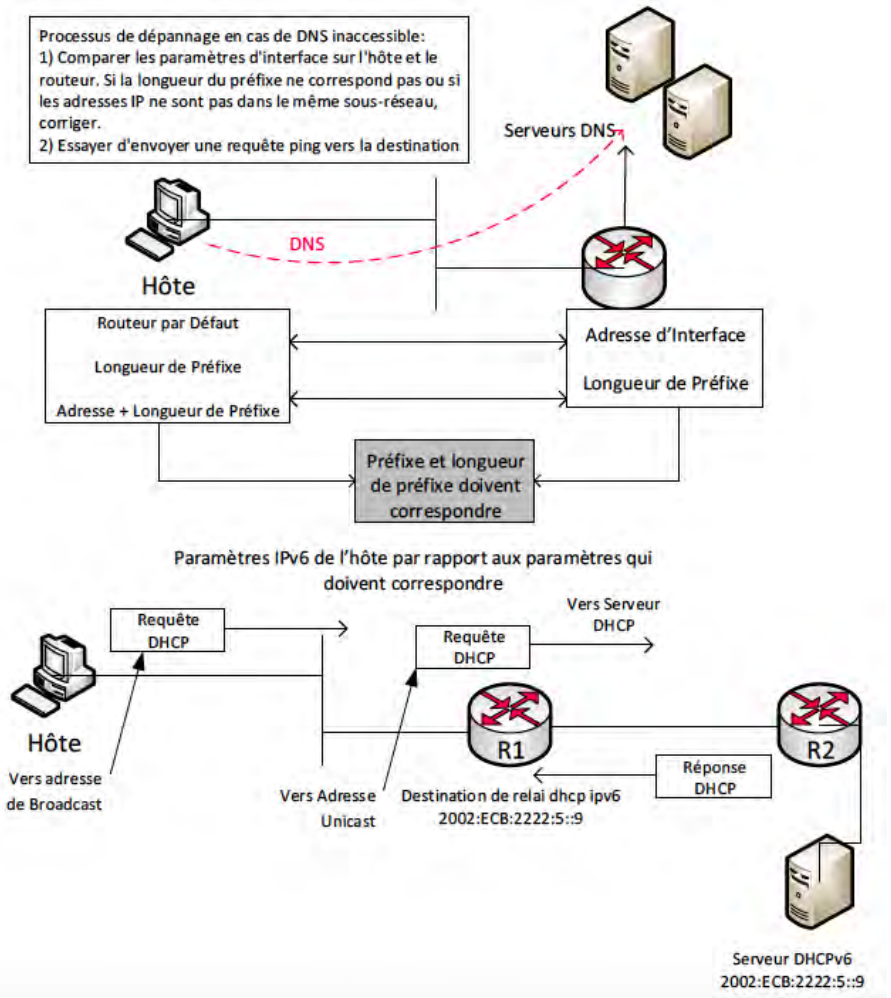
1. Si les serveurs DNS sont statiquement assignés, vérifier que les paramètres sont corrects
2. Vérifier si DHCPv6 a servi une adresse DNS incorrecte à l'hôte
3. Vérifier s'il existe un problème de connectivité IPv6 entre l'hôte et les serveurs DNS

Problèmes de Stateful DHCPv6

Pour que DHCPv6 marche, l'une des conditions suivantes doit être
remplie:

1) Le DHCP et l'hôte doivent être dans le même sous-réseau, ou
2) Le serveur DHCP peut être dans un autre sous-réseau à condition que
- Le routeur local ait mis en place le relais DHCPv6
- Il existe une connectivité entre le routeur local et le serveur DHCPv6

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



DÉPANNAGE DU ROUTAGE IPV6

Stateless DHCPv6 et les problèmes avec SLAAC

Si des problèmes se présentent avec DHCPv6 et SLAAC, nous avons besoin de savoir pourquoi les messages de sollicitation de routeur pour la découverte de réseau et d'annonce de routeur échouent. Voici les éléments à examiner lors de la validation de Stateless DHCPv6

1. Vérifier la connectivité LAN entre l'hôte et les routeurs dans le sous-réseau. En l'absence de connectivité, NPD ne fonctionnera pas
2. Le routeur peut ne pas avoir l'adresse ipv6 configurée sur une interface
3. Le routeur n'a pas ipv6 unicast-routing activé dans sa configuration

Problèmes de routage entre les sous-réseaux

Alors que les pings et l'accès sur le sous-réseau local semblent fonctionner, l'accès aux réseaux à l'extérieur du sous-réseau local peut avoir un problème. Traceroute est utilisé pour dépanner ces problèmes. Si traceroute montre certains routeurs mais échoue, voici les problèmes à examiner:

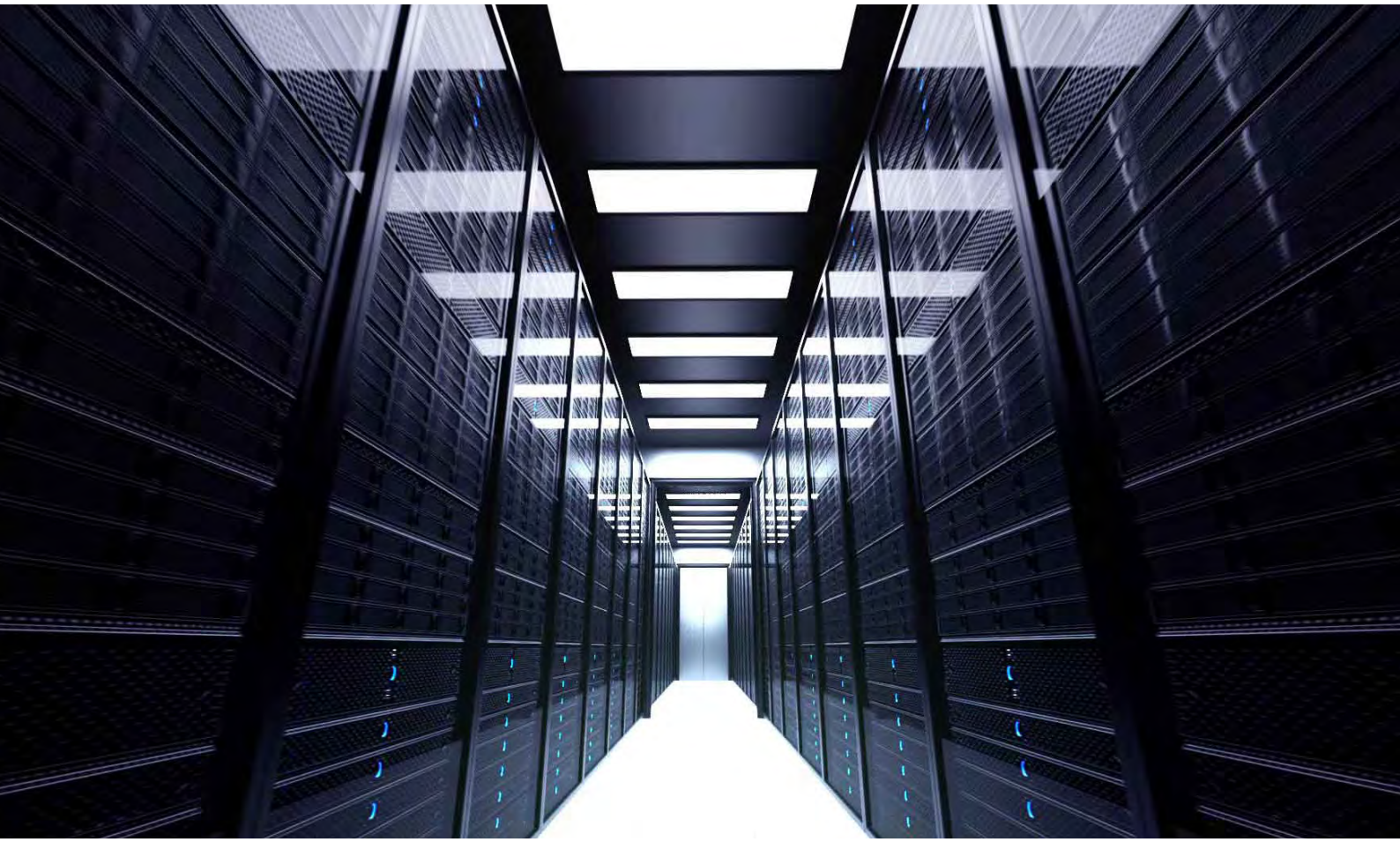
Les liaisons de données entre les routeurs sont inopérantes.

Les protocoles de routage ont des problèmes de voisinage.

Le filtrage de route peut empêcher à une route d'être ajoutée à la table de routage IPv6.

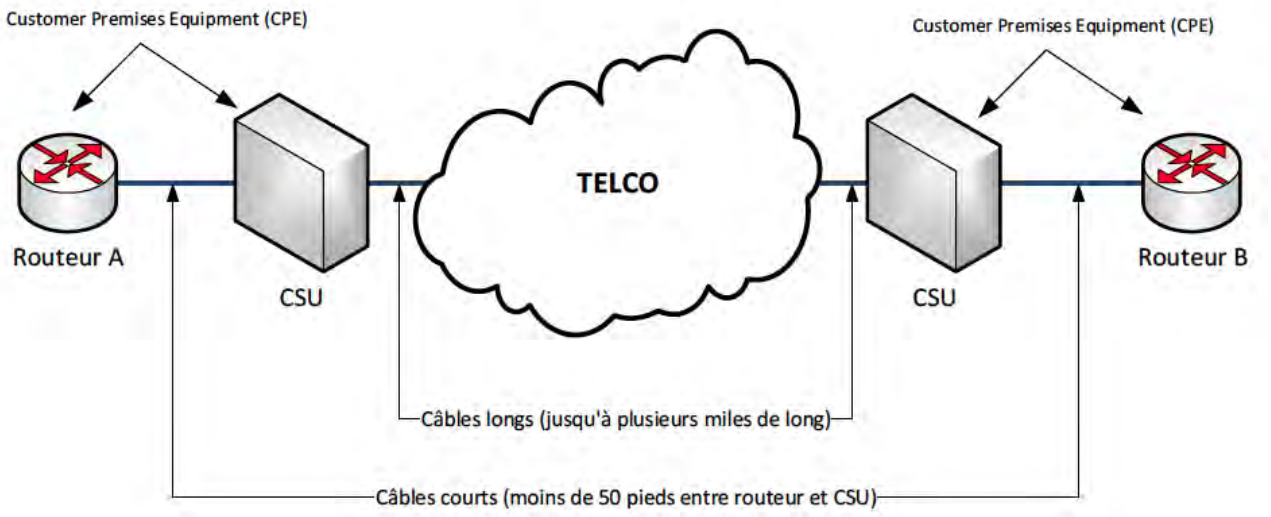
Des routes statiques mal configurées envoient des paquets à la mauvaise destination.

Une mauvaise conception réutilise des sous-réseaux dans différentes parties du réseau ce qui va provoquer des annonces de routes fausses et prévenir la convergence.



TECHNOLOGIES WAN

MISE EN OEUVRE DES WANS POINT À POINT



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

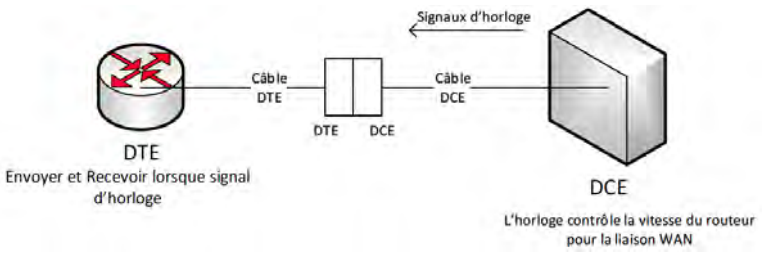
Router A# **show running-config**
<snip>
!
interface Serial0/0
ip address 10.100.1.1 255.255.255.0
description Link to Router B
clock rate 1544000
!

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
DS0	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)



DCE – Data Communications Equipment (Équipement Terminal de Traitement de pour la liaison WAN données) – Fournit l'horloge aux équipements connectés

DTE – Data Terminal Equipment (Équipement Terminal de Circuit de Données) – Termine le flux de données de bout distant et utilise l'horloge fournie pour
envoyer et recevoir des données.

MISE EN OEUVRE DES WANS POINT À POINT

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

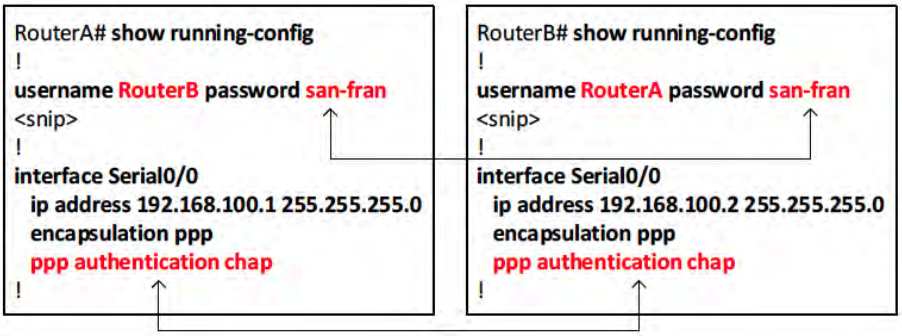
- Définit un en-tête (header)et en-queue (trailer) pour fournir des trames de données sur un lien
- Liaisons asynchrones (sans horloge) et synchrones (avec horloge) prises en charge
- Les protocoles de couche-3 peuvent passer sur le lien en raison d'un champ Type dans l'en-tête
- L'authentification est intégrée dans le protocole. Il utilise PAP (Password Authentication Protocol) 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:

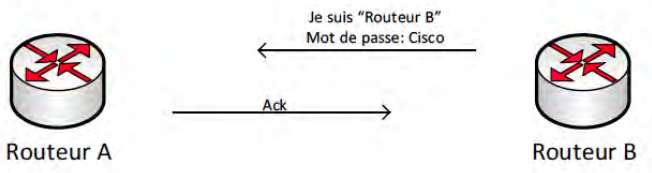
LCP – Link Control Protocol – Maintient la liaison PPP et ne s'inquiète pas au sujet des protocoles de couche 3. LCP est adjacente à la couche physique

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

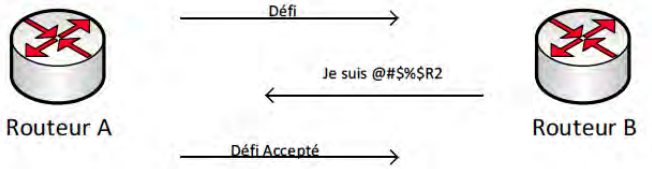
Configuration PPP sur une interface série - rappelez-vous que PPP doit être configuré explicitement sur les deux interfaces série. Afin de mettre en place CHAP, un nom d'utilisateur correspondant au nom d'hôte du routeur de destination et un mot de passe doivent être configurés. Dans cet exemple, le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



PAP (PASSWORD AUTHENTICATION PROTOCOL) – ENVOIE LE MOT DE PASSE EN CLAIR POUR AUTHENTIFIER L'AUTRE ROUTEUR

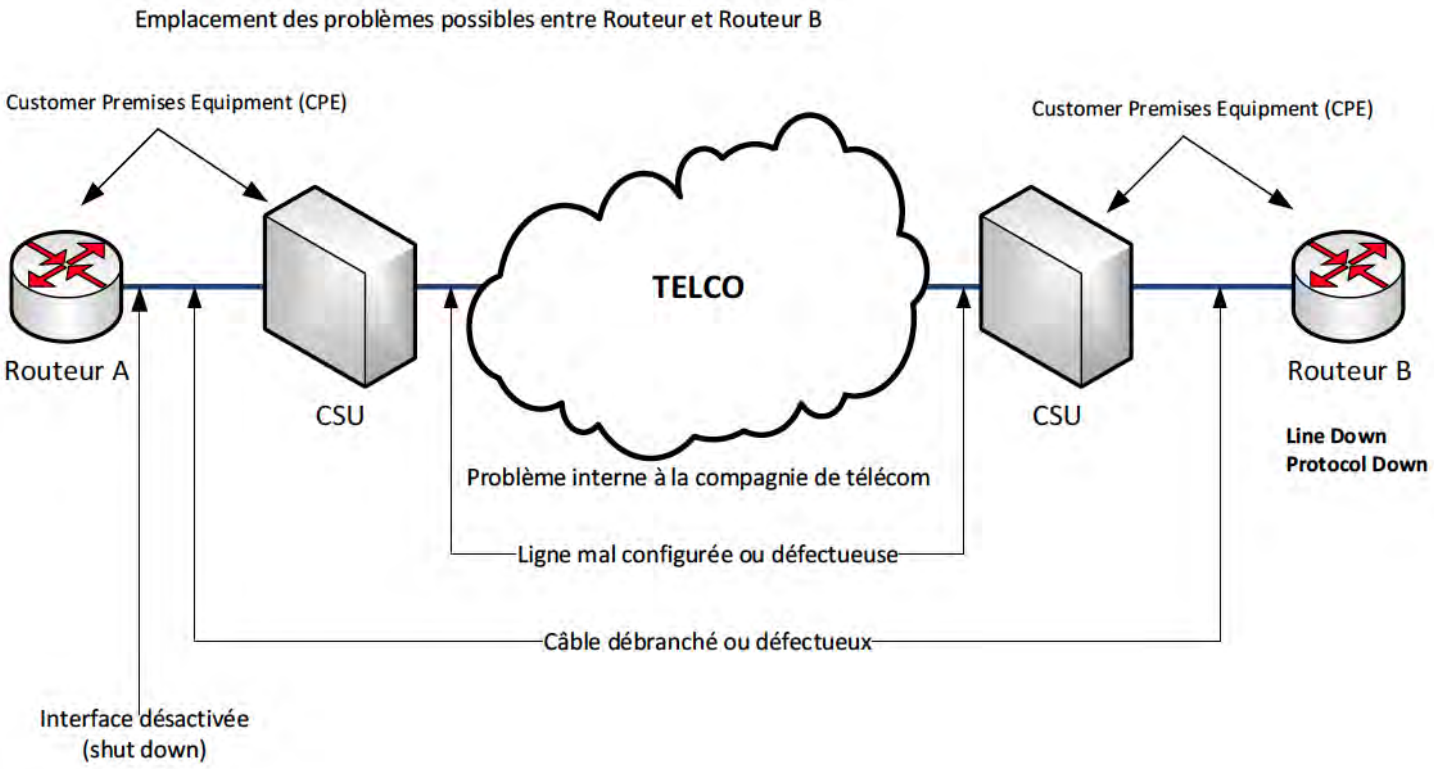


CHAP (Challenge Handshake Authentication Protocol) – Le routeur envoie son hash de mot de passe au routeur ayant fait la requête

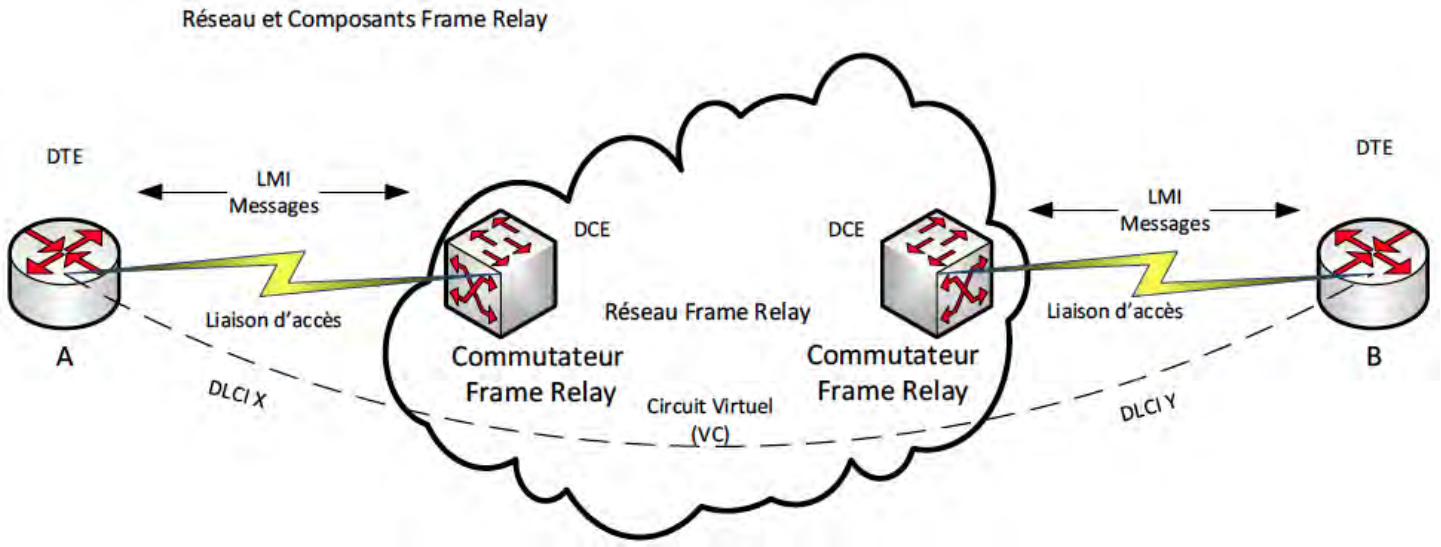


PROBLÈMES PROBABLES AVEC DES LIAISONS SÉRIES SUR LA BASE DES STATUTS D'INTERFACES

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


Emplacement des problèmes possibles entre Routeur et Routeur B
Customer Premises Equipment (CPE)
Customer Premises Equipment (CPE)
TELCO
Routeur A
CSU
CSU
Routeur B
Line Down
Protocol Down
Problème interne à la compagnie de télécom
Ligne mal configurée ou défectueuse
Câble débranché ou défectueux
Interface désactivée
(shut down)

COMPRENDRE LES CONCEPTS FRAME RELAY



TERMES ET CONCEPTS FRAME RELAY

TERME	DÉSCRIPTION
Virtual Circuit (VC)	Un concept qui indique le chemin qu'une trame prend de la source à la destination. Ceci est utile pour effectuer des comparaisons entre les lignes dédiées et les circuits Frame Relay
Permanent Virtual	Un VC défini. Ceci est équivalent à une ligne dédiée
Switched Virtual Circuit (SVC)	Un VC créé dynamiquement en fonction des besoins. Ceci est analogue à un circuit commuté
Data Terminal Equipment (DTE)	Équipement connecté aux services Frame Relay de la compagnie télécom (généralement des routeurs) sur le site du client
Data communications Equipment (DCE)	Généralement des commutateurs Frame Relay à l'intérieur du nuage de la compagnie télécom.
Access link	La ligne dédiée entre le DTE et le DCE, ou le lien entre le client et le fournisseur.

TERME	DÉSCRIPTION
Access Rate (AR)	La vitesse d'horloge de l'accès. Ce paramètre affecte le coût mensuel de la ligne
Committed Information Rate (CIR)	La vitesse minimale de ligne convenue entre le client et le fournisseur
Data Link Connection Identifier (DLCI)	Identifiant localement significatif dans l'en-tête frame relay
Nonbroadcast multiaccess (NBMA)	Les broadcasts ne sont pas pris en charge dans ce réseau, mais plus de deux appareils sont connectés
Local Management Interface (LMI)	Protocoles de communication utilisés entre le DTE et DCE pour gérer la connexion. Les messages relatifs au statut de PVC, la création de SVC et keepalives sont tous des messages LMI.

COMPRENDRE LES CONCEPTS FRAME RELAY

Points clés concernant la demande de statuts LMI (Local Management Interface) avec des connexions Frame Relay.

Le message de statut LMI remplit une fonction de keepalive entre le DCE et le DTE.
Si les keepalives s'arrêtent, le DTE et le DCE savent que la connexion est en panne.
Le message de statut LMI permet aux deux appareils de savoir si oui ou non un PVC est actif. Bien que le lien d'accès pourrait être physiquement actif, les VCs pourraient être en panne. Le LMI signale ceux qui sont actifs et ceux qui sont en
panne.

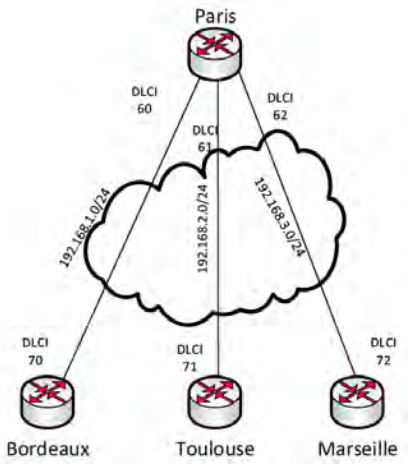
Alors que les routeurs Cisco peuvent détecter automatiquement le type de LMI sur le lien, la configuration manuelle du type de LMI est toujours disponible pour des raisons historiques et pour permettre au routeur de communiquer avec les commutateurs frame relay qui ne peuvent pas négocier automatiquement le type de LMI.

Adressage IP pour les PVCs Frame Relay

Nous avons trois options d'adressage dans un réseau Frame Relay:

- Tous les DTEs Frame Relay dans le même sous-réseau
- Un sous-réseau par VC
- Un mélange des deux options précédentes

TYPE LMI CISCO IOS	DOCUMENT SOURCE	NOM LMI
cisco	Propriétaire	Cisco
ansi	T1.617 Annexe D	ANSI
q933a	Q.933 Annexe A	ITU



En-têtes et en-queues Frame Relay

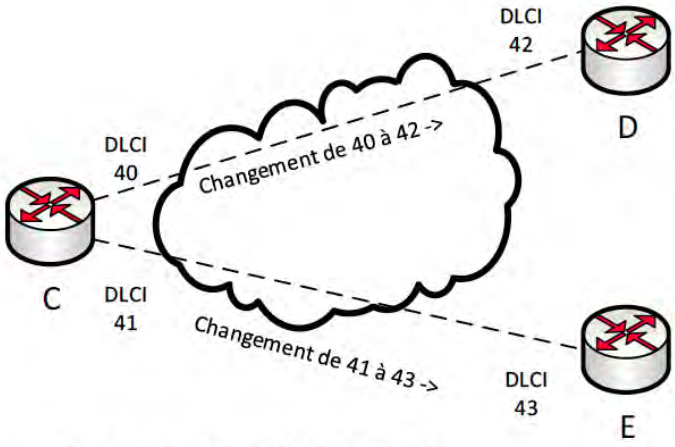
En-tête LAPF	Cisco	Paquet	En-queue LAPF
Inclut DLCI	Champ Type Protocole		
En-tête LAPF	RFC 1490	Paquet	En-queue LAPF

Remarques clés sur Data-Link Connection Identifier (DLCI)

Les DLCIs doivent être uniques sur le lien d'accès entre le DTE et le DCE pour chaque PVC.

Les DLCIs sont localement significatifs sur le lien d'accès seulement. Par exemple, l'extrémité locale du PVC peut avoir un DLCI de 40 et l'extrémité distante du PVC peut avoir un DLCI de 60.

Cela signifie que les DLCIs à chaque extrémité du VC peuvent être différents



Trois routeurs connectés via deux PVC.
Remarque: Regardez les DLCI comme s'ils sont localement significatifs sur chaque routeur

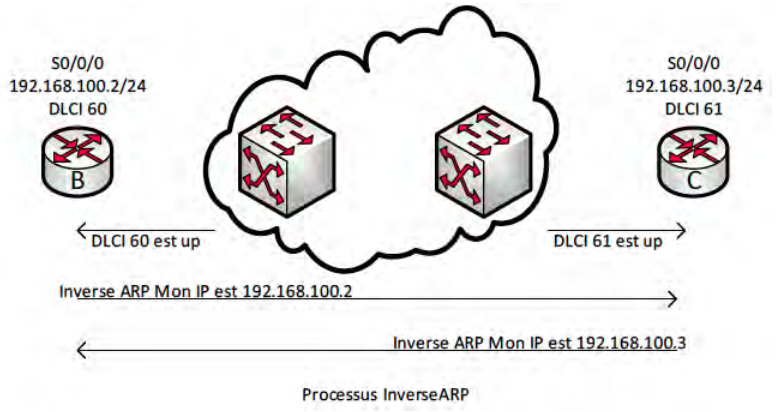
MISE EN OEUVRE DE FRAME RELAY

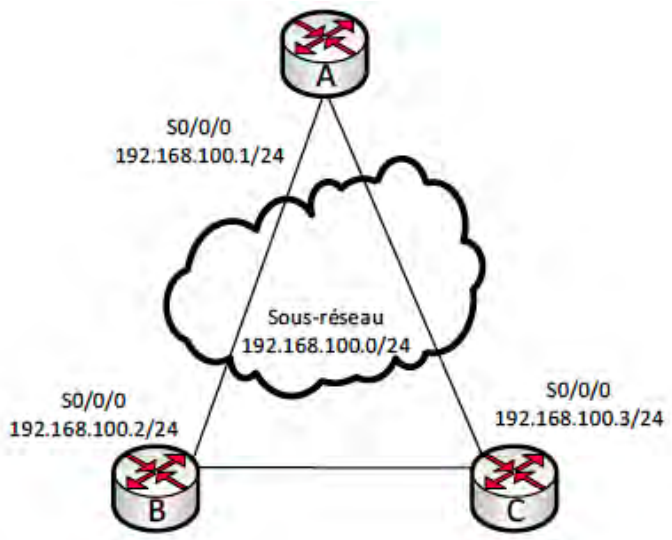
PLANIFICATION D'UNE INSTALLATION FRAME RELAY

1) Déterminer le nombre de sites et la fréquence d'horloge pour chacun
2) Définir les extrémités pour chaque VC (Circuit Virtuel) et définir le CIR (Committed Information Rate) pour chacune
3) Définir le type de LMI (Local Management Interface) – en accord avec le fournisseur
4) Choisir le design IP: un sous-réseau pour tous les VCs, un sous-réseau pour chaque VC ou un mélange des deux
5) Déterminer si les adresses IP seront attribuées aux interfaces physiques, sousinterfaces multipoint, ou sous-interfaces point à point
6) Choisir le type d'encapsulation frame relay (ietf ou cisco) basé sur l'équipement utilisé à chaque extrémité de la liaison d'accès

CONFIGURATION DE FRAME RELAY SUR UN ROUTEUR

1) Régler l'interface physique pour utiliser l'encapsulation frame relay avec la commande encapsulation frame-relay
2) Définir l'adresse IP sur l'interface physique ou la sous-interface
3) Définir manuellement le type de LMI si cela est requis par le fournisseur
4) Si vous avez besoin de changer l'encapsulation par défaut sur chaque VC, utilisez la sous-commande d'interface encapsulation frame-relay ietf
5) Si Inverse ARP n'est pas utilisé, définir l'adresse du routeur de saut suivant pour chaque DLCI avec la sous-commande frame-relay map adresse-ip dlci DLCI broadcast
6) Si vous utilisez des sous-interfaces, régler le DLCI associé avec la commande frame-relay interface-dlci DLCI.





RÉSEAU FRAME RELAY AVEC LES OPTIONS PAR DÉFAUT

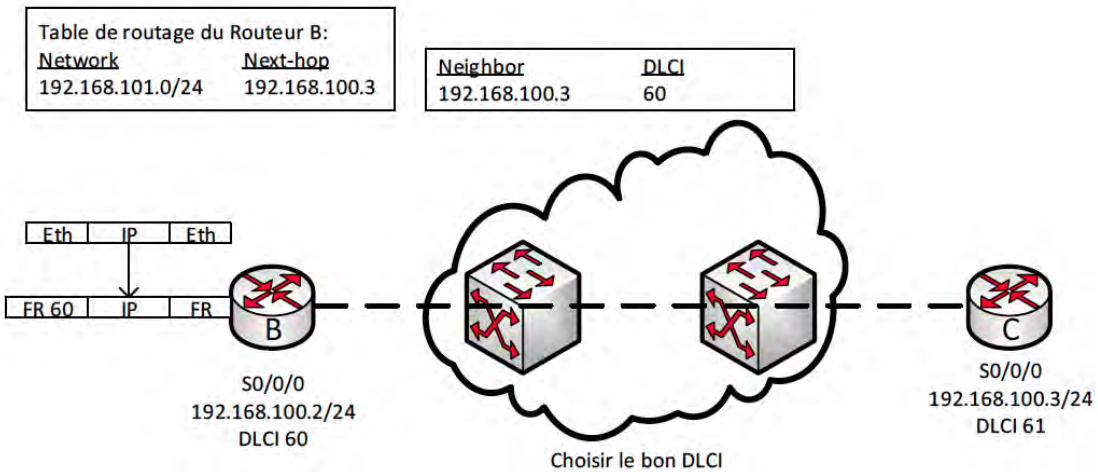
Configuration du Routeur A:
Interface Serial0/0/0
ip address 192.168.100.1 255.255.255.0
encapsulation frame-relay

Configuration du Routeur B:
Interface Serial0/0/0
ip address 192.168.100.2 255.255.255.0
encapsulation frame-relay

Configuration du Routeur C:
Interface Serial0/0/0
ip address 192.168.100.3 255.255.255.0
encapsulation frame-relay

Mappage des adresses IP Frame Relay

Le mappage est le processus où l'adresse IP de couche 3 est corrélée à l'adresse de liaison de données de couche 2. Dans le cas de Frame Relay, le mappage est l'association de l'adresse IP et du DLCI Frame Relay pour le PVC.



MISE EN OEUVRE DE FRAME RELAY

DÉPANNAGE FRAME RELAY

Si tous les routeurs distants échouent aux tests de ping et qu'il existe un seul lien physique commun (architecture hub-and-spoke), voici quelques étapes de dépannage:

1) Vérifier les problèmes de couche physique sur le lien d'accès entre le routeur et le commutateur frame relay du fournisseur
2) Vérifier les problèmes de liaison de données associés à frame relay en particulier l'encapsulation et le type de LMI.
3) Sur la base des statuts de PVC et LMI, vérifier les problèmes de PVC
4) Vérifier les problèmes de correspondance d'adresses de couche 3 à couche 2.
5) Vérifier les disparités de LMI ou d'encapsulation à chaque extrémité
6) Vérifiez les disparités de sous-réseau sur chaque PVC

Rappelez-vous que la LMI dans Frame Relay est essentielle pour un bon fonctionnement. LMI fonctionne dans les deux sens. La LMI sur le DCE informe le DTE sur chaque PVC sur le lien d'accès et le statut individuel de chaque VC. La LMI gère également le trafic keepalive entre le DTE et le DCE pour la surveillance de status.

Toujours vérifier la LMI sur le routeur local. Si la LMI ne fonctionne pas, il peut y avoir des problèmes plus larges empêchant aux VCs de passer le trafic.

PROBLÈMES DE MAPPAGE FRAME RELAY

Voici les mesures à prendre pour résoudre les problèmes de mappage entre les adresses IP et DLCI/VC

Pour les sous-interfaces point à point, vérifiez ce qui suit:

- Inverse ARP ou le mappage statique ne sont pas nécessaires
- Toute adresse IP dans le même sous-réseau est automatiquement mappée au même DLCI par l'IOS sur ces types d'interfaces
- Alors que la commande show frame-relay map liste des sous-interfaces point à point, les adresses IP de saut suivant ou notations dynamiques ne sont pas disponibles parce que ces paramètres ne sont pas appris par Inverse ARP

Pour les interfaces physiques et sous-interfaces point-à-multipoint:

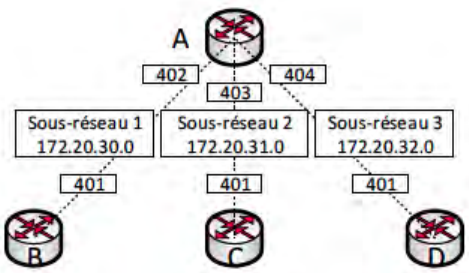
- Le mappage statique ou Inverse ARP sont nécessaires
- show frame-relay map devrait afficher l'adresse IP du routeur distant et le DLCI local parce que ces paramètres ont été statiquement définis ou appris par Inverse ARP
- Si le mappage statique est utilisé, le protocole de routage nécessite le mot-clé broadcast sur la carte DLCI.

VALEURS DES STATUTS DE PVC

STATUT	ACTIF	INACTIF	SUPPRIMÉ	STATIQUE
Le PVC est défini dans le réseau Frame Relay	Oui	Oui	Non	Inconnu
Le routeur va essayer d'utiliser un VC dans cet état pour envoyer des trames	Oui	Non	Non	Oui

Information sur les statuts des sous-interfaces
Notez les statuts suivants des sous-interfaces lors de l'examen des VCs de frame relay

Down/Down: Tout les DLCI sur la sous-interface sont inactifs ou supprimés, ou l'interface physique associée n'est pas dans un état up/up (shutdown, aucun transporteur, etc.)
Up/Up: Au moins un des DLCI sur la sous-interface est dans un état actif ou statique



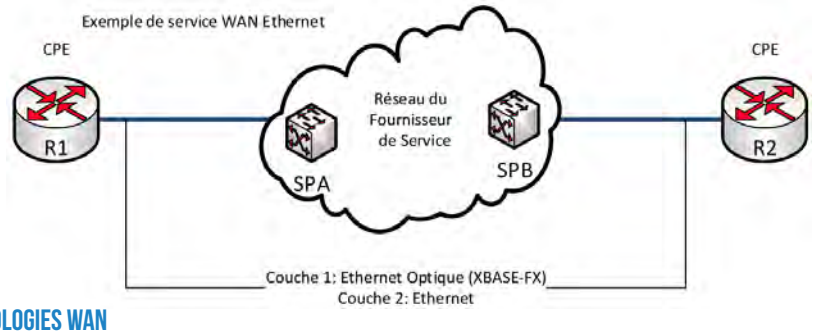

```
Configuration du Routeur A
!
interface Serial0/0/0
 encapsulation frame-relay
!
interface Serial0/0/0.1 point-to-point
 ip address 172.20.30.1 255.255.255.0
 frame-relay interface-dlci 402
!
interface Serial0/0/0.2 point-to-point
 ip address 172.20.31.1 255.255.255.0
 frame-relay interface-dlci 403
!
interface Serial0/0/0.3 point-to-point
 ip address 172.20.32.1 255.255.255.0
 frame-relay interface-dlci 404
```

```
Configuration du Routeur B
Interface Serial0/0/0
 encapsulation frame-relay
!
Interface Serial0/0/0.1 point-to-point
 ip address 172.20.30.2 255.255.255.0
 frame-relay interface-dlci 401
```

```
Configuration du Routeur C
Interface Serial0/0/0
 encapsulation frame-relay
!
Interface Serial0/0/0.1 point-to-point
 ip address 172.20.31.2 255.255.255.0
 frame-relay interface-dlci 401
```

```
Configuration du Routeur D
Interface Serial0/0/0
 encapsulation frame-relay
!
Interface Serial0/0/0.1 point-to-point
 ip address 172.20.32.2 255.255.255.0
 frame-relay interface-dlci 401
```

IDENTIFICATION D'AUTRES TYPES DE WAN



POINTS DE COMPARAISON DES TECHNOLOGIES WAN

ATTRIBUT	LIGNE DÉDIÉE	FRAME RELAY	WAN ETHERNET
Liens d'accès physique typiques	TDM (T1, E1, et plus)	TDM (T1, E1, et plus)	Fibre Ethernet
Interface de Routeur	Série	Série	Ethernet
Protocoles	HDLC, PPP	Frame Relay	Ethernet
Contrat de Service WAN	Transmettre les bits à l'autre extrémité du lien	Transmettre les trames FR à l'autre extrémité des PVC spécifiés	Transmettre des trames Ethernet à des destinations spécifiques

COMPARAISON ENTRE MPLS, FRAME RELAY, ET ETHERNET WAN

ATTRIBUT	MPLS	FRAME RELAY	WAN ETHERNET
Liens d'accès physique typiques	Toute technologie prenant en charge IP	TDM (T1, E1, et plus)	Fibre Ethernet
Interface de Routeur	Toute technologie prenant en charge IP	Série	Ethernet
Protocoles	Toute technologie prenant en charge IP	Frame Relay	Ethernet
Contrat de Service WAN	Transmettre des paquets IP	Transmettre les trames FR à l'autre extrémité des PVC spécifiés	Transmettre des trames Ethernet à des destinations spécifiques

FONDAMENTAUX DU SERVICE WAN ETHERNET

Bien que les liaisons d'accès utilisent une norme Ethernet, une norme Ethernet associée de couche physique est utilisée à travers les lignes de fibre optique. La fibre est utilisée parce que le lien peut se prolonger bien au-delà de la limite des 100 mètres pour le cuivre Ethernet.

Les routeurs CPE utilisent une interface Ethernet au lieu d'une interface série.
Les routeurs CPE utilisent des protocoles Ethernet.
Bien que les adresses MAC soient utilisées sur le WAN, les DLCI de Frame Relay ne seront pas affichés sur le diagramme.
Le dessin peut indiquer les commutateurs du fournisseur de services, mais seulement ceux que les routeurs CPE connectent.
Le lien est privé comme pour les lignes dédiées et Frame Relay.
Le fournisseur peut utiliser toute technologie dans le nuage.

Remarque: Le lien de fibre peut utiliser l'un de ceux-ci sans être limité à ces normes: 10BASE-FX, 100BASE-FX, 1000BASE-FX

COMPARAISON ENTRE LES TECHNOLOGIES D'ACCÈS À INTERNET

ATTRIBUT	MODEM ANALOGIQUE	ISDN	DSL	CÂBLE
Liens d'accès physique typiques	Ligne téléphonique (boucle locale)	Ligne téléphonique (boucle locale)	Ligne téléphonique (boucle locale)	Câble coaxial
L'internet est-il toujours disponible?	Non	Non	Oui	Oui
Promesse de service de données	Envoyer les bits c la partie appelée	Envoyer les bits à la partie appelée	Envoyer toutes les données au FSI	Envoyer toutes les données au FSI
Vitesse (générale)	56 Kbps	128 Kbps	1 – 8 Mbps	10+ Mbps
Asymétrique?	Non*	Non	Oui	Oui

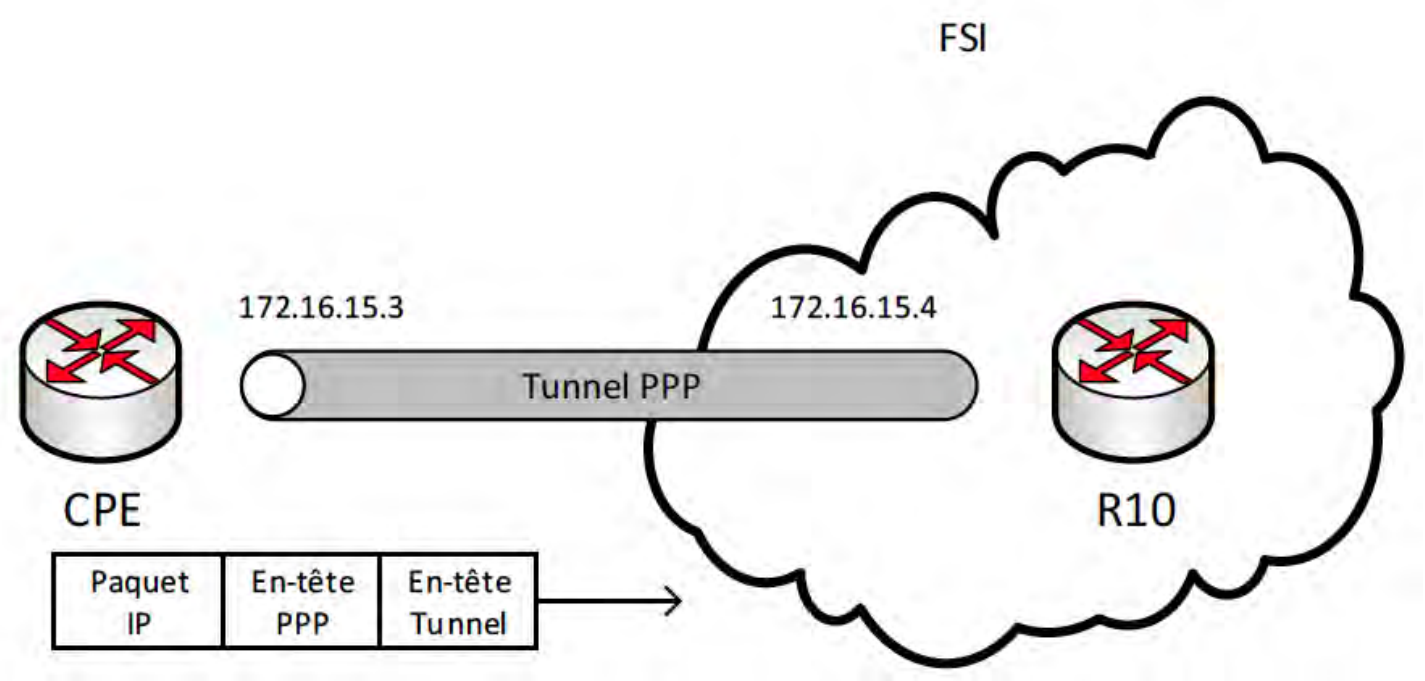
*** Remarque: Un modem analogique peut recevoir jusqu'à 56 Kbps mais transmet jusqu'à 28,8 Kbps**

ACCÈS À INTERNET PAR TÉLÉPHONE MOBILE / SMARTPHONE

Internet sans fil: Toute technologie d'accès qui utilise des ondes radio entre deux appareils mobiles ou un appareil mobile et une station de base.
Sans fil 3G/4G: Les technologies de troisième et quatrième générations utilisées par les téléphones mobiles.
LTE: Long Term Evolution, une partie de la technologie 4G qui offre des vitesses plus rapides que les technologies 3G.

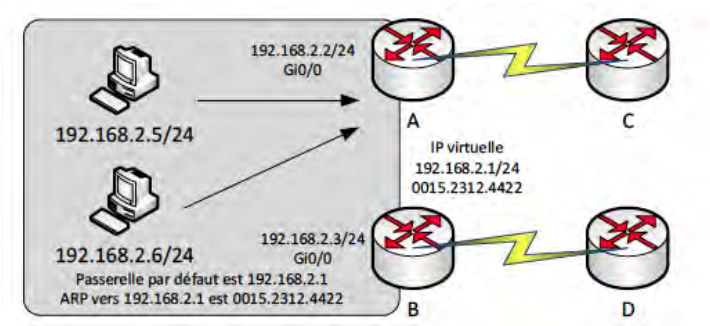
IDENTIFICATION D'AUTRES TYPES DE WAN

Point-to-Point Protocol over Ethernet (PPPoE): Utilisé par les modems DSL où la ligne d'accès du client au modem est via Ethernet. PPPoE crée un tunnel entre le modem et le routeur du FSI pour transmettre les paquets.

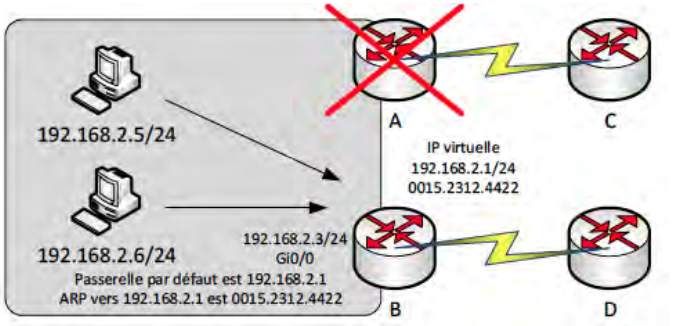


REDONDANCE ET VPN

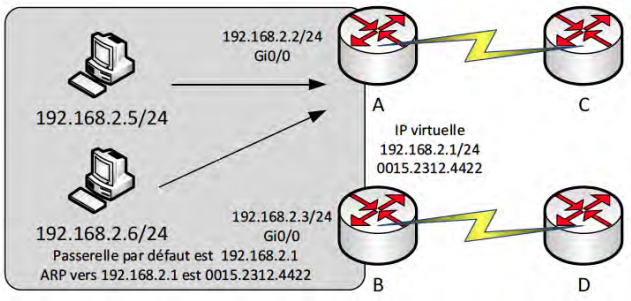
CRÉATION DE ROUTEURS DE PREMIER SAUT REDONDANTS



Exemple du Protocole HSRP (Hot Standby Router Protocol)
Ici, le routeur A assume l'adresse MAC de 0015.2312.4422



Une défaillance du routeur A signifie que le routeur B prend le relais.
Le routeur B assume l'adresse MAC de 0015.2312.4422
Remarque: les ordinateurs portables n'ont pas besoin de ARP à nouveau pour la passerelle par défaut

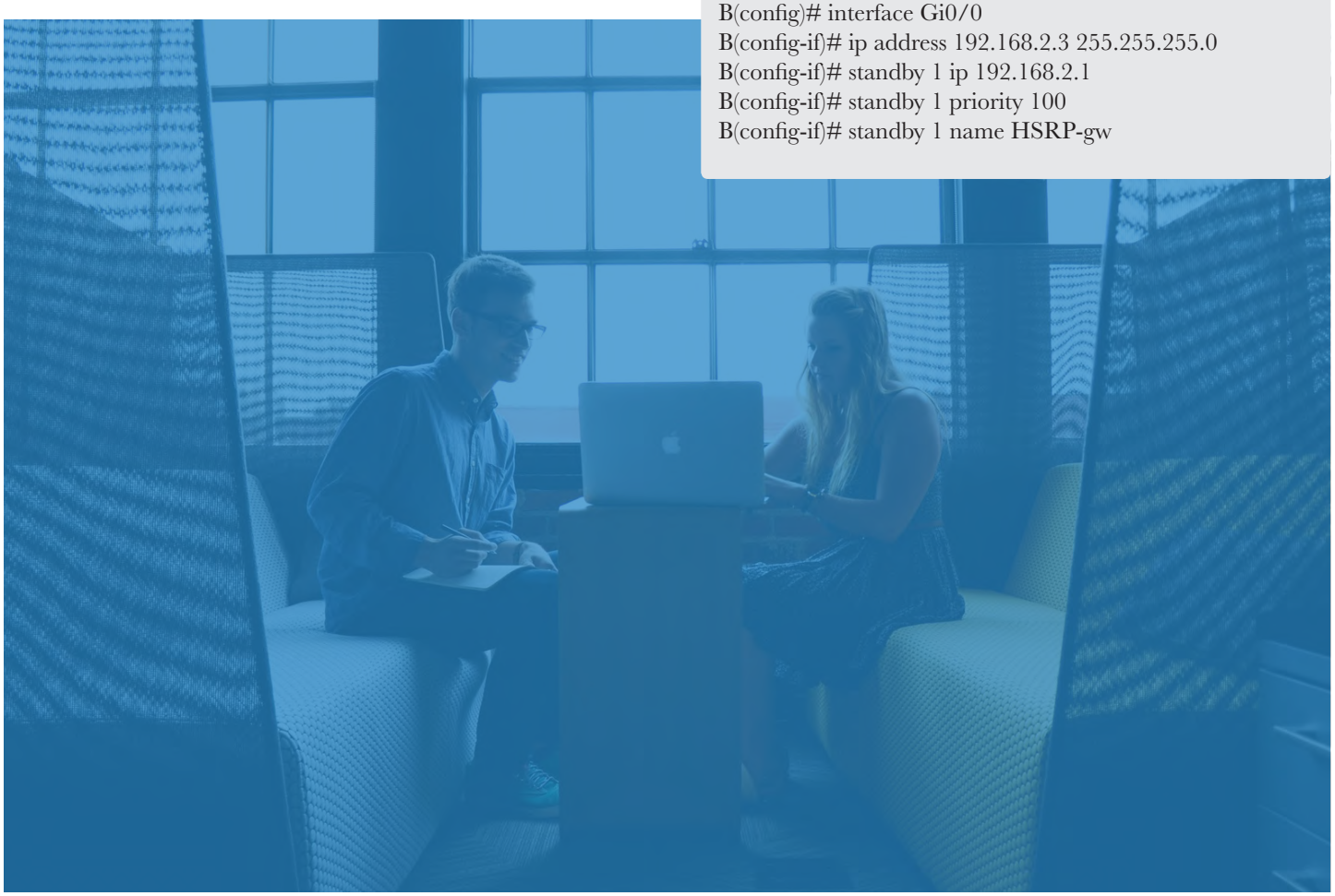


Restauration du Routeur A.

CONFIGURATION DE HSRP:

Mise en place de 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

Mise en place de 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



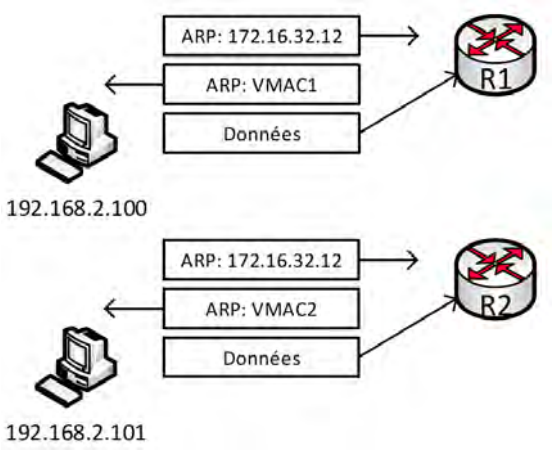
CRÉATION DE ROUTEURS DE PREMIER SAUT REDONDANTS

IDENTIFICATEURS DE COMMANDE SHOW STANDBY BRIEF

Interface: Interface de routeur local configurée pour HSRP
Grp: Numéro de groupe HSRP
Pri: Priorité HSRP sur le routeur local
State: État HSRP sur le routeur actuel
Active: Adresse IP de l'interface HSRP active (marquée locale si l'interface HSRP active est sur le routeur)
Standby: L'adresse IP de l'interface de veille HSRP (marquée locale si l'interface de veille HSRP est sur le routeur)
Virtual IP: Adresse IP virtuelle pour ce groupe HSRP

```
A# show standby brief
Interface  Grp  Pri  P  State   Active      Standby       Virtual IP
Gi0/0      1    110     Active  local       192.168.2.3   192.168.2.1

B# show standby brief
Interface  Grp  Pri  P  State   Active      Standby       Virtual IP
Gi0/0      1    110     Standby 192.168.2.2 192.168.2.3   192.168.2.1
```



PROCESSUS GLBP:

Étape 1: L'hôte 192.168.2.100 envoie un ARP pour localiser une adresse MAC 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: L'hôte 192.168.2.101 envoie un ARP pour localiser une adresse MAC 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 donnée à R2.

PROTOCOLE DE REDONDANCE AU PREMIER SAUT (FHRP)

Tous les Protocoles de Redondance au Premier Saut (First Hop Redundancy Protocol) comme HSRP, VRRP et GLBP doivent permettre à deux routeurs d'apparaitrent 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 routeur par défaut qui n'a pas à changer
2) Les routeurs par défaut 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 pair fonctionne
5) Une fois qu'un routeur dans la pair tombe en panne, le FHRP a pour responsabilité de faire prendre le relais par l'autre routeur.

COMPARAISON ENTRE MPLS, FRAME RELAY, ET ETHERNET WAN

FWD	SIGNIFICATION
-	Ce routeur agit comme Passerelle par Défaut Virtuelle Active (AVG)
1	Ce routeur est transporteur GLBP #1
2	Ce routeur est transporteur GLBP #2

SIGNIFICATIONS LOCALE DE "STATE" DANS LA COMMANDE SHOW GLBP BRIEF:

DESCRIPTION LIGNE	FWD	STATE R1	STATE R2
Passerelle Virtuelle Active	-	Active	Active
Transporteur #1	1	Listen	Listen
Transporteur #2	2	Active	Active

NOM DU PROTOCOLE	ABRÉVIATION	REDONDANCE	ÉQUILIBRAGE DE CHARGE	ORIGINE
Hot Standby Router Protocol	HSRP	Active/standby	Par sous-réseau	CISCO
Virtual Router Redundancy Protocol	VRRP	Active/standby	Par sous-réseau	IETF (RFC 5798
Gateway Load Balancing Protocol	GLBP	Active/active	Par hôte	CISCO

OPTIONS DE PROTOCOLES DE ROUTAGE AU PREMIER SAUT

CRÉATION DE ROUTEURS DE PREMIER SAUT REDONDANTS

CONFIGURATION DE GLBP:

Mise en place de 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**

Mise en place de 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	Fwd	Pri	State	Address	Active Router	Standby Router
Gi0/0	1	-	110	Active	192.168.2.1	local	192.168.2.2
Gi0/0	1	1	-	Listen	0023.b500.0001	192.168.2.2	-
Gi0/0	1	2	-	Active	0023.b500.0002	local	-

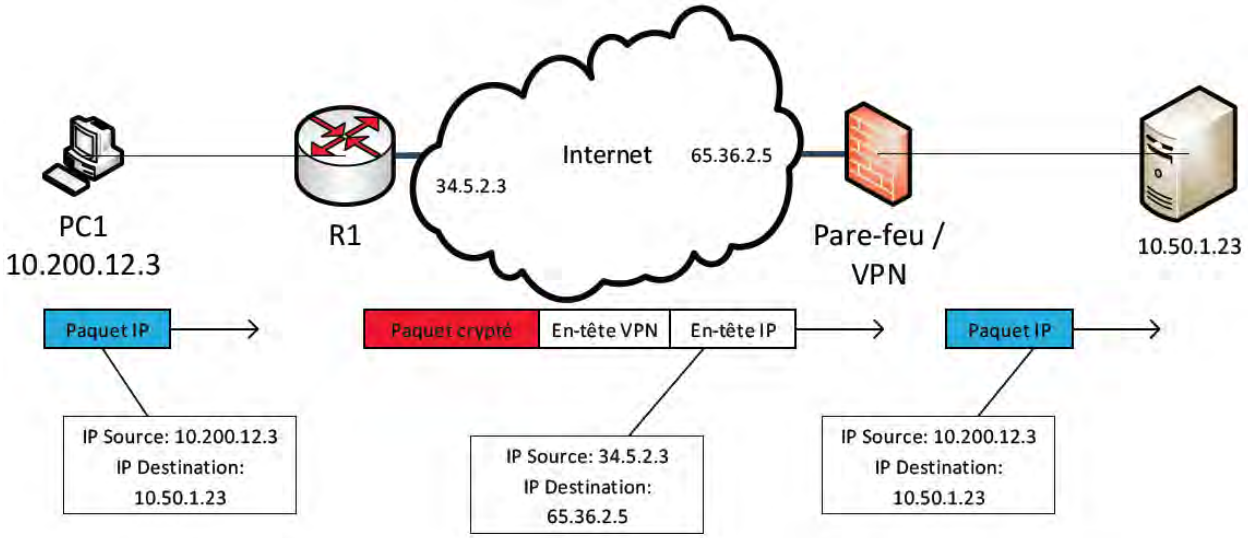
RÉSEAUX PRIVÉS VIRTUELS

POINTS CLÉS DES RÉSEAUX PRIVÉS VIRTUELS (VIRTUAL PRIVATE NETWORK):

Un Réseau Privé Virtuel (VPN) est un moyen d'avoir la sécurité d'une ligne louée sans les frais mensuels. Un VPN est établi entre deux points ou plus à travers un réseau non sécurisé tel que l'Internet et le trafic est crypté entre les points établis.
Un VPN est **privé** ce qui signifie que les données sont cryptées en transit et cela empêche les attaques du milieu appelée **man-in-the-middle.**
Un VPN fournit **l'authentification** parce que le récepteur peut vérifier que l'expéditeur du paquet est authentique
Un VPN fournit **l'intégrité** des données en s'assurant que le paquet n'a pas été modifié par un tiers alors qu'il était en transit vers la destination.
Un VPN empêche également les **attaques par rejeu** («replay»). Une attaque par rejeu prend un paquet, copie le paquet et envoie le paquet à la destination ce qui pourrait confondre l'hôte ou apparaître comme un utilisateur légitime.

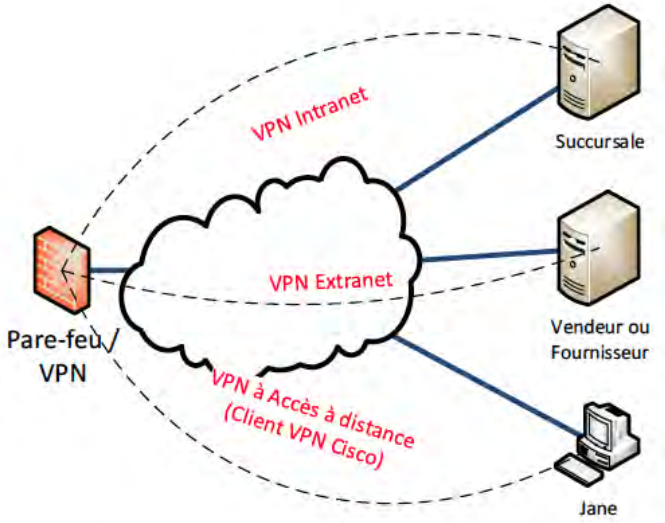
TYPES DE VPN ET UTILISATIONS TYPIQUES

TYPE DE VPN	UTILISATION TYPIQUE
Intranet	Utilisé pour connecter des sites distants appartenant à la même organisation
Extranet	Utilisé pour connecter des sites distants appartenant à différentes organisations
Accès à distance	Connecte les utilisateurs individuels à l'organisation d'attache via Internet



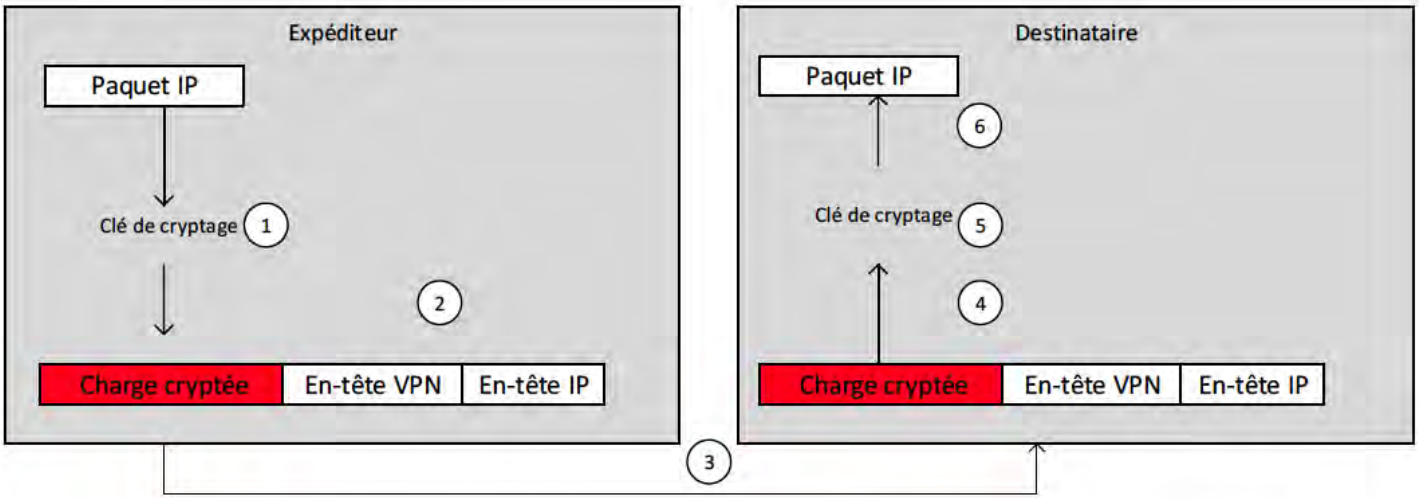
Envoi d'un paquet à travers un tunnel VPN de 10.200.12.3 au serveur 10.50.1.23:

1) L' hôte envoie les paquets de 10.200.12.3 à 10.50.1.23
2) Le routeur R1 crypte le paquet et ajoute un nouvel en-tête VPN. L'IP de destination 65.36.2.5 et l'IP source 34.5.2.3 sont ajoutés à un nouvel en-tête IP puis le paquet combiné est transmis.
3) Le pare-feu à 65.36.2.5 reçoit le paquet combiné, confirme l'authenticité du paquet, retire l'en-tête VPN et l'en-tête IP puis décrypte le paquet original de 10.200.12.3
4) Le pare-feu envoie le paquet d'origine vers le serveur 10.50.1.23



Comparaison entre différentes utilisations de VPN

RÉSEAUX PRIVÉS VIRTUELS



CRYPTAGE IPSEC / PROCESSUS DE DÉCRYPTAGE

1) L'expéditeur prend le paquet IP en clair et utilise la clé de cryptage pour générer la charge utile cryptée.
2) L'expéditeur ajoute un en-tête IP et VPN à la charge utile cryptée.
3) L'expéditeur envoie le paquet au destinataire
4) Le destinataire reçoit le paquet et retire les en-têtes en laissant la charge utile cryptée
5) Le destinataire décrypte la charge utile avec la clé de cryptage
6) Le destinataire sort le paquet IP d'origine.

Points clés sur les Tunnels d'Encapsulation Générique de Routage (GRE - Generic Routing Encapsulation):

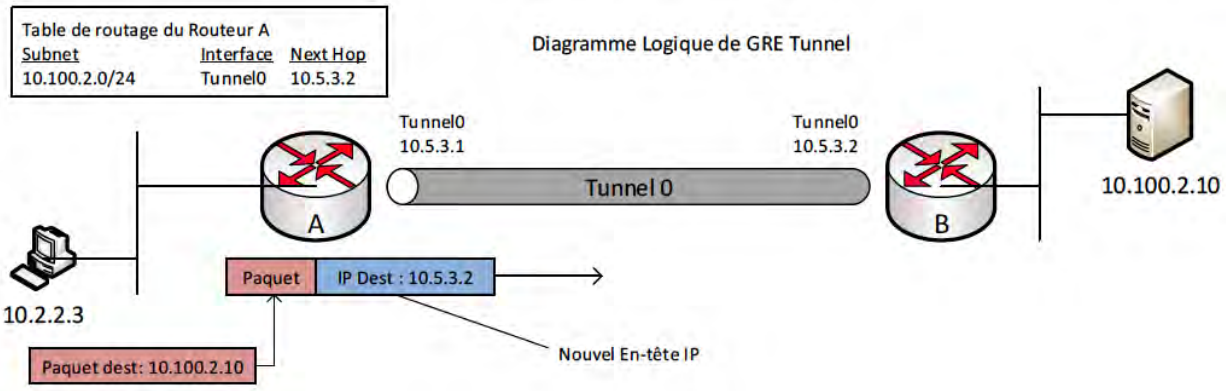
- Peuvent être utilisés à la place d'une liaison série entre deux routeurs
- Le trafic peut être acheminé à travers un tunnel
- Les tunnels GRE utilisent des interfaces virtuelles reliées à une interface physique de routeur

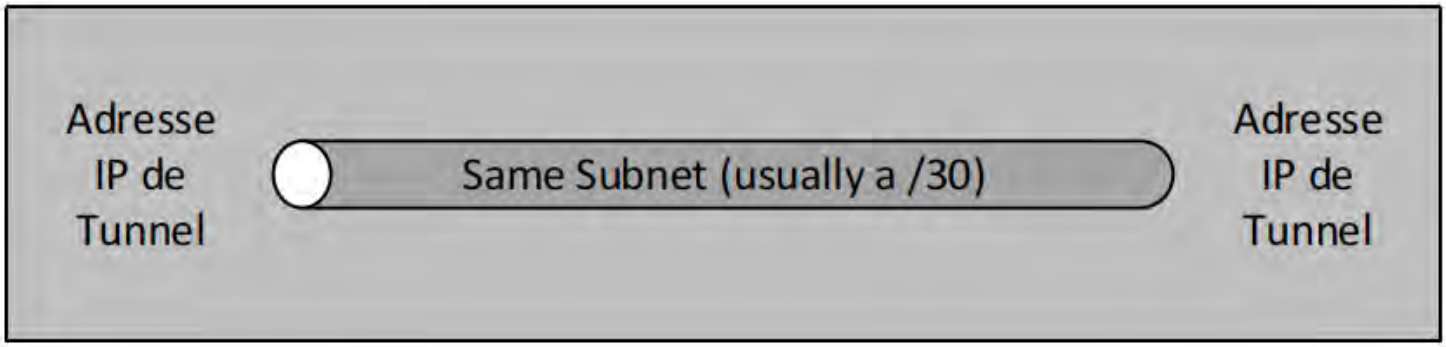
Remarque: les tunnels GRE ne cryptent pas le trafic entre les points d'extrémité. Les tunnels sont utilisés au sein d'une organisation et non utilisés pour le transport de l'information sur l'Internet ouvert.

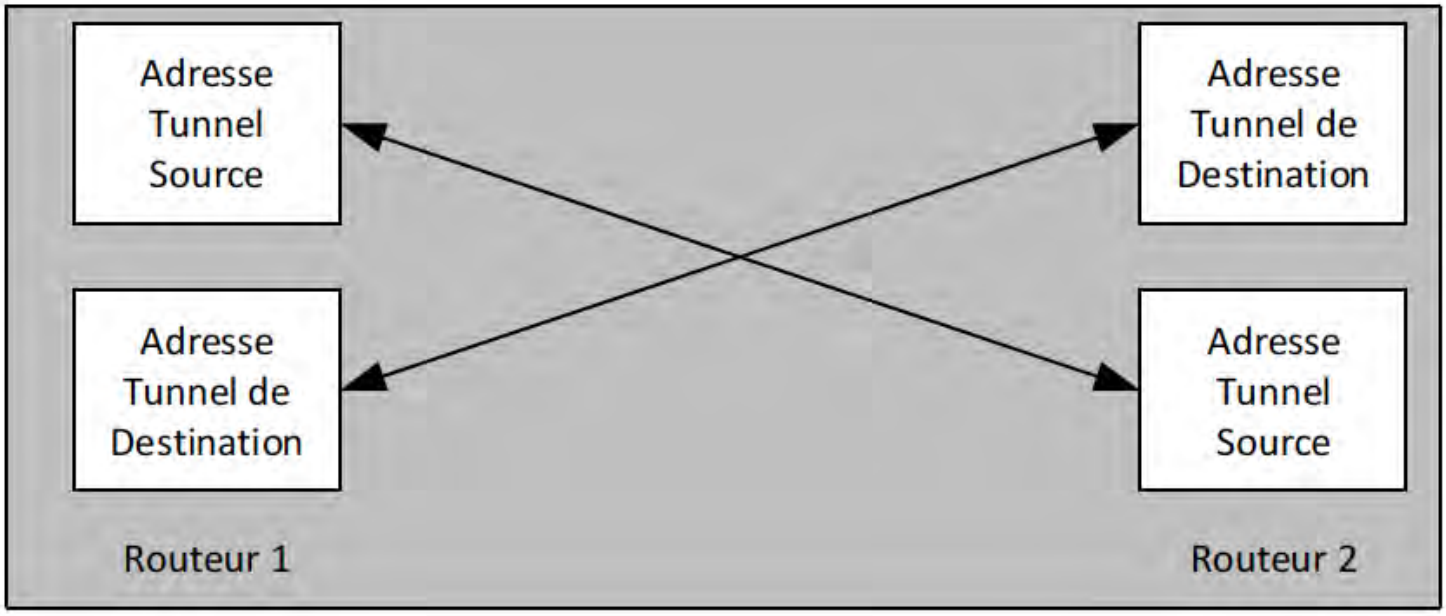
LES ALGORITHMES DE CRYPTAGE VPN

ALGORITHME	LONGUEUR DE CLÉ	COMMENTAIRES
Data Encryption Standard (DES)	56 bits	Algorithme de cryptage plus ancien qui est obsolète
Triple DES (3DES)	56 bits x 3	Utilise trois clés DES pour améliorer la force de cryptage
Advanced Encryption Standard (AES)	128 bit et 256 bit	Algorithme de cryptage récent

```
Configuration de GRE Tunnel du Routeur A
A(config)# interface Tunnel0
A(config-if)# ip address 10.5.3.1 255.255.255.252
A(config-if)# tunnel source Serial0/0/0
A(config-if)# tunnel destination 10.1.2.3
A(config-if)#exit
A(config)# route 10.100.2.0 0.0.0.255 Tunnel0
```







PARAMÈTRES DE CONFIGURATION DE TUNNEL GRE ET RELATIONS SOURCE/DESTINATION

ÉTAPES DE CONFIGURATION DE GRE TUNNEL (REMARQUE: DOIT ÊTRE FAIT SUR CHAQUE ROUTEUR)

1) Créer l'interface de tunnel avec la commande interface tunnel numéro. Veuillez noter que le numéro de tunnel est localement significatif.

2) Attribuer une adresse IP au tunnel avec la commande ip address masque d'adresse. Vous devez utiliser deux adresses dans le même sous-réseau.

3) Configurer l'adresse IP source de tunnel en utilisant tunnel source interface (si vous utilisez une interface de routeur) ou tunnel source adresse-ip (si vous spécifiez une adresse IP). Si vous utilisez l'interface du routeur, l'adresse IP de destination du tunnel doit correspondre à l'adresse IP de l'interface.

4) Configurez l'adresse IP de destination du tunnel avec la commande tunnel destination adresse-ip (Cette adresse IP doit être la même que l'adresse IP source de tunnel sur le routeur de destination).

5) Configurer le routage à travers le tunnel en utilisant des routes statiques ou activer le routage sur l'interface du tunnel.

FIN DES FICHES RÉSUMÉ

COMMENT OPTIMISER SA MÉMOIRE?

Comment faire pour assimiler toute la théorie réseau afin de réussir avec succès l'examen et obtenir la certification CCNA?

Cette question, beaucoup de personnes me l'ont posée. Et j'avoue que moi-même, j'étais dans le désarroi lorsque j'ai récupéré mes supports de cours ICND1 et ICND2 qui compose toute la théorie pour l'examen. **Plus de 1000 pages à apprendre par coeur !**

En plus, libre à de me croire ou non mais je fais partie des personnes qui ont des soucis avec leur cerveau. Je ne retiens quasiment rien. Le pire étant les **prénoms que j'oublie** en 30 secondes, **les films** dont j'oublie le titre le surlendemain, les **histoires et blagues de la veille**… alors dans ma vie professionnelle, je m'appuie sur l'agenda Outlook et Google. Merci à eux car ils m'ont sauvé plus d'une fois.

Alors comment faire pour réussir un examen où il y a une tonne d'informations à conserver dans sa mémoire?

A chacun sa formule mais en voici deux qui ont fonctionné à merveille pour moi:

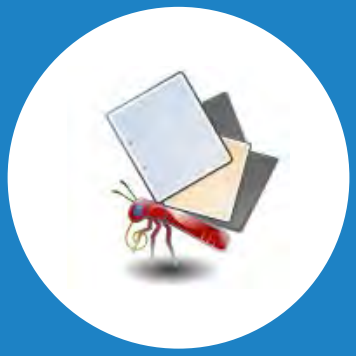
FLASHCARD

Pour vous aider dans la mémorisation, il existe un site web qui propose de tester vos connaissances avec l'utilisation de cartes de révision. Ce site, c'est **FlashCardExchange**.

Sur le site, faites une recherche de carte en tapant "**CCENT**" ou "**CCNA**" et vous allez trouver une quantité hallucinante de cartes de révision, et le tout gratuitement !

Faites tout de même attention, certaines cartes ne sont pas forcément à jour par rapport au contenu de l'examen.

Pour ceux qui veulent **créer leur propre carte mentale** pour pouvoir réviser directement sur leur ordinateur sans Internet, je vous conseille vivement le logiciel **Mnemosyne** qui est totalement gratuit. Je vous le présente ci-dessous.



PROJETMNEMOSYNE

Ce projet n'est en fait qu'un **logiciel libre et gratuit**.

C'est celui que j'ai utilisé pour mes révisions, non pas pour le CCNA que j'avais déjà, mais **pour le CCIE!** Et oui, imaginez-moi avec mes problèmes de mémoire, à engloutir des centaines de pages de configuration, de design, de conseils pour à la fin les ressortir le jour de l'écrit et le jour du Lab de 8h. Sans cette aide "extérieure", je n'aurai jamais réussi mon examen, j'en suis certain.

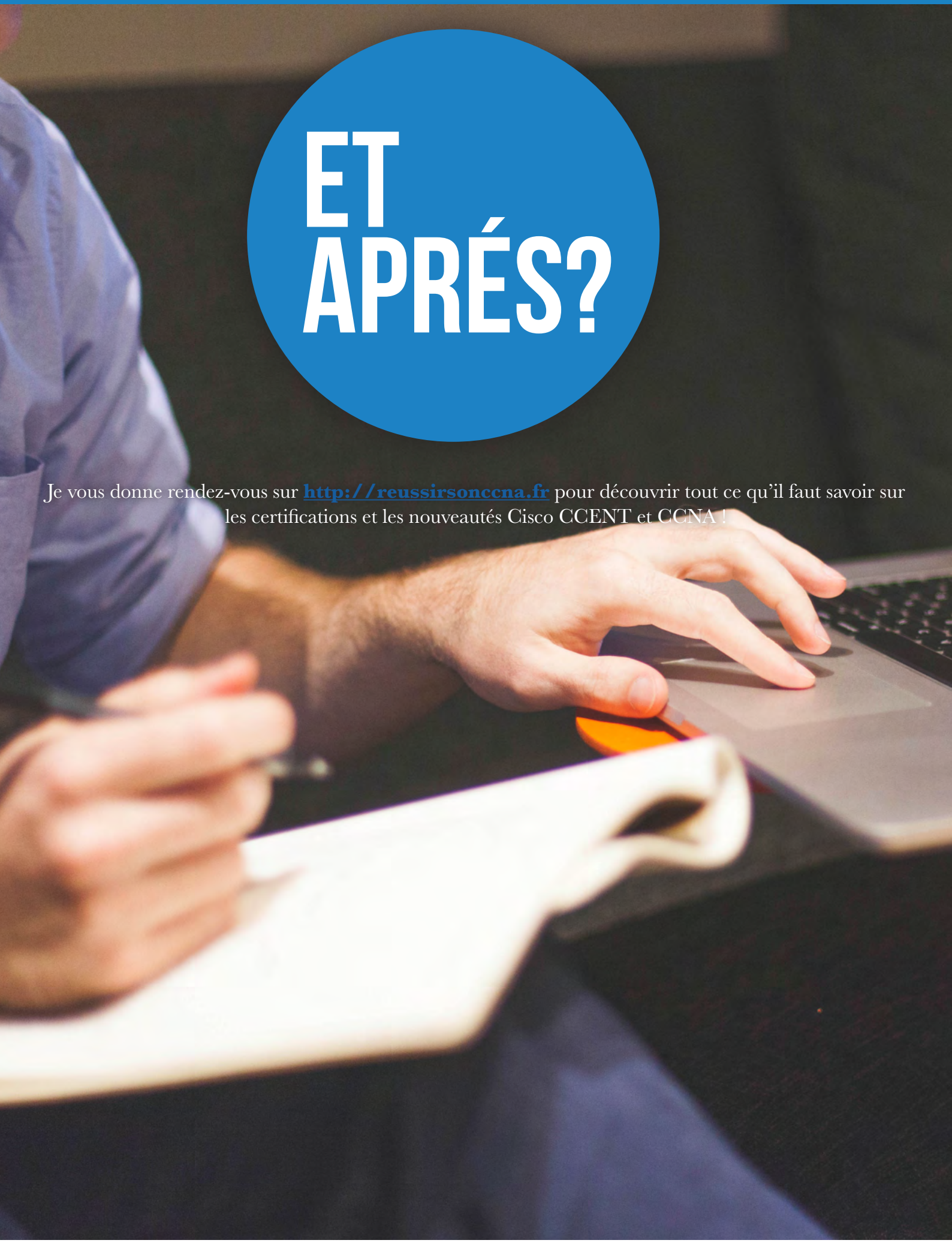
Alors comment fonctionne ce logiciel? Tout d'abord, malgré le fait qu'il soit en anglais, il est très simple d'utilisation. Le but est une fois que vous avez fini un chapitre, vous créez des cartes mémoires dans ce logiciel en y ajoutant des questions/réponses (par exemple: quel est le protocole de trunk? réponse: 802.1Q…). Au bout d'un certain temps, vous allez avoir plusieurs cartes mémoire et le logiciel va vous demander de ressortir vos connaissances à des temps prédéfinis (le lendemain, une semaine après, un mois après…) afin d'entrainer votre mémoire à récupérer les informations qui sont stockées quelque part dans votre cerveau.

Je vous avoue que le début est vexant car rien que le lendemain, on a déjà oublié pas mal de réponses des cartes mémoires. Mais au fur et à mesure, on devient une star en mémoire! Et c'est grâce à cette méthode que j'ai obtenu mon CCIE.

Certains me diront qu'il est possible de faire la même chose avec des fiches en papier. C'est vrai mais l'algorithme qui repose les questions en fonction de vos réponses est fait pour vous reposer la question au moment où votre mémoire va l'oublier. Et ça, ça vaut tout l'or du monde!

Essayez-le, soyez assidu dans la création de vos cartes et vous verrez les résultats!

Voici le site : **http://www.mnemosyne-proj.org**



ET APRÉS?

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 !