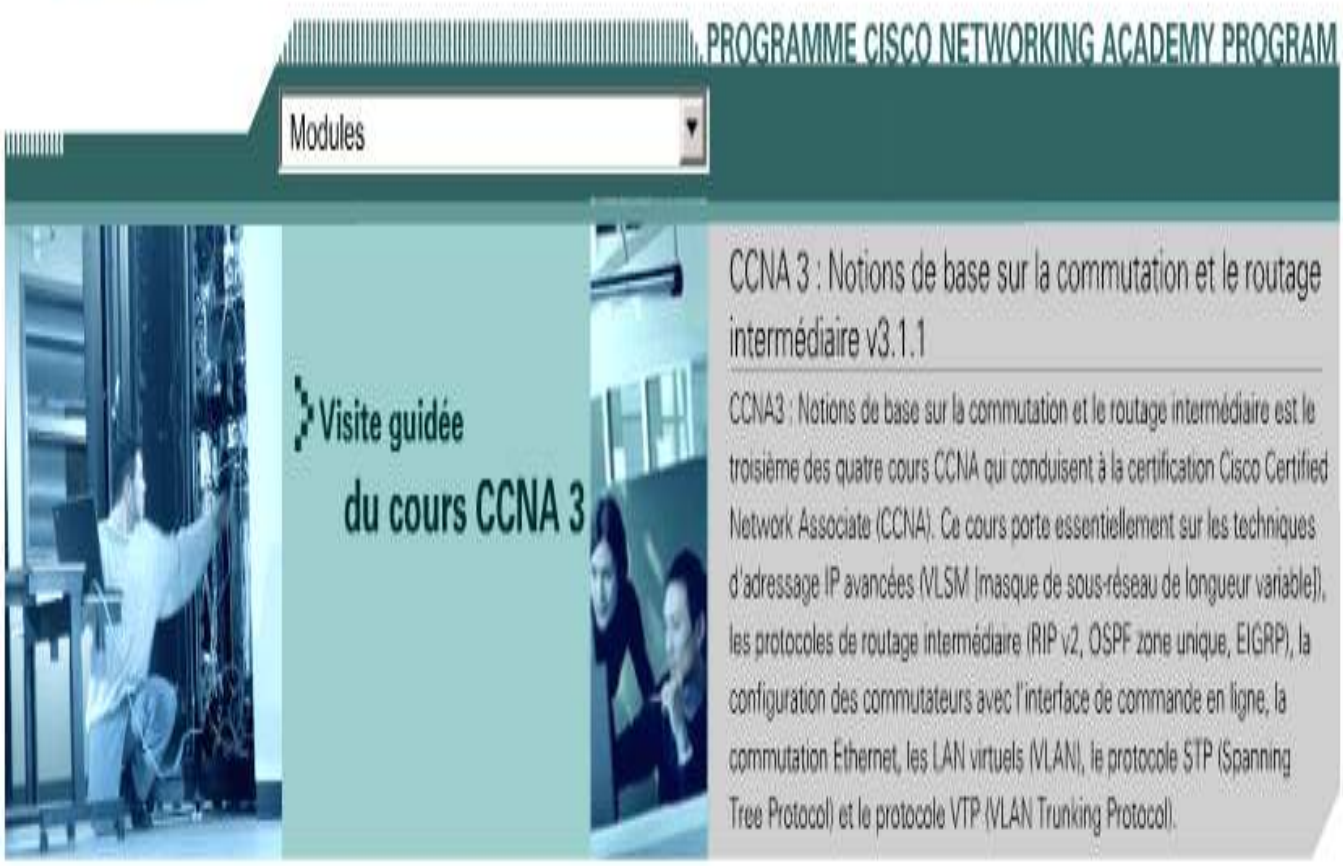


Vue d'ensemble

Un administrateur réseau doit anticiper et gérer la croissance physique du réseau, éventuellement en achetant ou en louant un autre étage de l'immeuble pour héberger de nouveaux équipements réseau tels que des bâtis, des tableaux de connexion, des commutateurs et des routeurs. Le concepteur de réseau doit choisir un système d'adressage capable de prendre en compte la croissance. La technique VLSM (Variable-Length Subnet Masking) permet de créer des schémas d'adressage efficaces et évolutifs.

Avec le développement prodigieux d'Internet et de TCP/IP, quasiment toutes les entreprises doivent désormais mettre en œuvre un système d'adressage IP. De nombreuses organisations choisissent TCP/IP comme unique protocole routé sur leur réseau. Malheureusement, les créateurs de TCP/IP ne pouvaient pas prévoir que leur protocole finirait par soutenir un réseau mondial d'informations, de commerce et de divertissement.

Il y a vingt ans, la version 4 d'IP (IPv4) offrait une stratégie d'adressage qui, bien qu'évolutive au début, s'avéra être un système d'allocation d'adresses inefficace. La version 6 (IPv6), avec un espace d'adressage pratiquement illimité, est progressivement mise en oeuvre sur des réseaux pré-établis et pourrait remplacer IPv4 en tant que protocole dominant sur Internet. Au cours des deux dernières décennies, les ingénieurs ont réussi à faire évoluer IPv4 pour qu'il puisse résister au développement exponentiel d'Internet. VLSM est une des modifications ayant contribué à combler le fossé entre IPv4 et IPv6.

Les réseaux doivent être évolutifs afin de répondre aux changements des besoins des utilisateurs. Un réseau évolutif est capable de se développer d'une façon logique, efficace et économique. Le protocole de routage utilisé dans un réseau joue un grand rôle dans la détermination de l'évolutivité du réseau. Par conséquent, il est important de choisir le protocole de routage de façon avisée. Le protocole RIP (Routing Information Protocol) est toujours adapté aux réseaux de petite taille mais pas aux réseaux de grande taille en raison de limitations inhérentes. Pour dépasser ces limites et conserver la simplicité de la première version de RIP (RIP v1), la version 2 du protocole (RIP v2) a été développée.

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
1.1	VLSM
1.2	RIP Version 2

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un modèle d'adressage IP répondant aux besoins • Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des • Création d'une configuration initiale sur un routeur	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
• Conception d'un modèle d'adressage IP qui prenne en charge un adressage par classes, sans classe et privé répondant aux besoins • Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des utilisateurs • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

1.1 VLSM

1.1.1 Qu'est-ce que la technique VLSM et à quoi sert-elle?

Au fur et à mesure de l'expansion des sous-réseaux IP, les administrateurs ont cherché des solutions pour utiliser l'espace d'adressage plus efficacement. Une des techniques existantes s'appelle VLSM (Variable-Length Subnet Masks). Avec VLSM, un administrateur réseau peut utiliser un masque long sur les réseaux qui ne comportent pas beaucoup d'hôtes et un masque court sur les sous-réseaux qui comportent beaucoup d'hôtes. [1] [2] [3]

Qu'est-ce que la technique VLSM et à quoi sert-elle ?

- Crise d'adressage
- L'IETF (Internet Engineering Task Force) a identifié deux problèmes en 1992
- Pénurie d'adresses réseau IPv4 non affectées, en particulier pour la classe B
- Augmentation rapide de la taille des tables de routage de l'Internet

Voici quelques solutions à court terme quant à la pénurie d'adresse IPv4:

Extensions à court terme à IPv4
- Sous-réseaux 1985
- Sous-réseaux de longueur variable 1987
- Routage CIDR 1993
- Adresses IP privées

VLSM est utilisé pour les raisons suivantes:

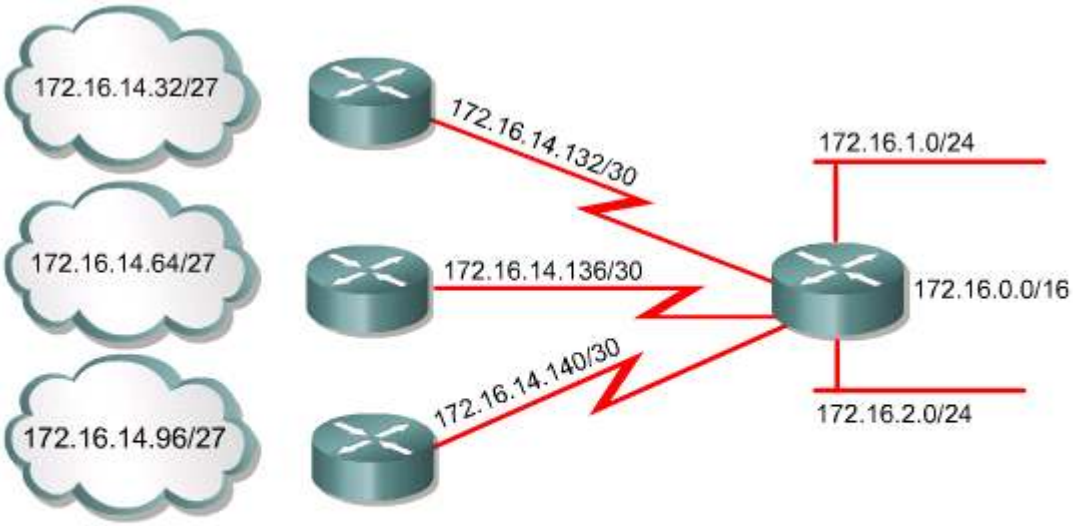
- Dernière solution : espace d'adressage IPv6 sur 128 bits
- Offre 340 283 366 920 938 463 374 607 431 768 211 456 possibilités

Pour pouvoir utiliser VLSM, un administrateur réseau doit utiliser un protocole de routage compatible avec cette technique. Les routeurs Cisco sont compatibles avec VLSM grâce aux solutions OSPF (Open Shortest Path First), Integrated IS-IS (Integrated Intermediate System to Intermediate System), EIGRP (Enhanced Interior Gateway Routing Protocol), RIP v2 et au routage statique. [4]

VLSM est supporté par les types de protocoles suivants:

- OSPF
- Integrated IS-IS
- EIGRP
- RIP v2
- Routage statique

La technique VLSM permet à une entreprise d'utiliser plusieurs sous-masques dans le même espace d'adressage réseau. La mise en œuvre de VLSM est souvent appelée « subdivision d'un sous-réseau en sous-réseaux » et peut être utilisée pour améliorer l'efficacité de l'adressage. [5]



Le sous-réseau 172.16.14.0/24 est divisé en sous-réseaux plus petits

- Découpage en sous-réseaux avec un masque (/27)
- Puis découpage de l'un des sous-réseaux /27 inutilisés en plusieurs sous-réseaux /30

Avec les protocoles de routage par classes (classful), un réseau doit utiliser le même masque de sous-réseau. Par conséquent, le réseau 192.168.187.0 doit utiliser un seul masque de sous-réseau tel que 255.255.255.0.

VLSM est simplement une fonction qui permet à un système autonome unique d'inclure des réseaux avec différents masques de sous-réseau. Si un protocole de routage autorise VLSM, utilisez un masque de sous-réseau de 30 bits sur les connexions réseau, 255.255.255.252, un masque de sous-réseau de 24 bits sur les réseaux utilisateurs, 255.255.255.0, voire même un masque de sous-réseau de 22 bits, 255.255.252.0, sur les réseaux pouvant accueillir jusqu'à 1000 utilisateurs. [6] [7]

Adresse de réseau subdivisé : 172.16.32.0/20
Format binaire : 10101100.00010000.00100000.00000000
Adresse VLSM : 172.16.32.0/26
Format binaire : 10101100.00010000. 0010 0000.00 000000

1er sous-réseau :	172	•	16	.0010	0000.00	000000	= 172.16.32.0/26
2e sous-réseau :	172	•	16	.0010	0000.01	000000	= 172.16.32.64/26
3e sous-réseau :	172	•	16	.0010	0000.10	000000	= 172.16.32.128/26
4e sous-réseau :	172	•	16	.0010	0000.11	000000	= 172.16.32.192/26
5e sous-réseau :	172	•	16	.0010	0001.00	000000	= 172.16.33.0/26
	Réseau			Sous-réseau	Sous-réseau VLSM	Hôte	

Masques de sous-réseau		
255.255.255.252	11111111 11111111 11111111 11111100	30 bits
255.255.255.0	11111111 11111111 11111111 00000000	24 bits
255.255.252.0	11111111 11111111 11111100 00000000	22 bits

1.1 VLSM

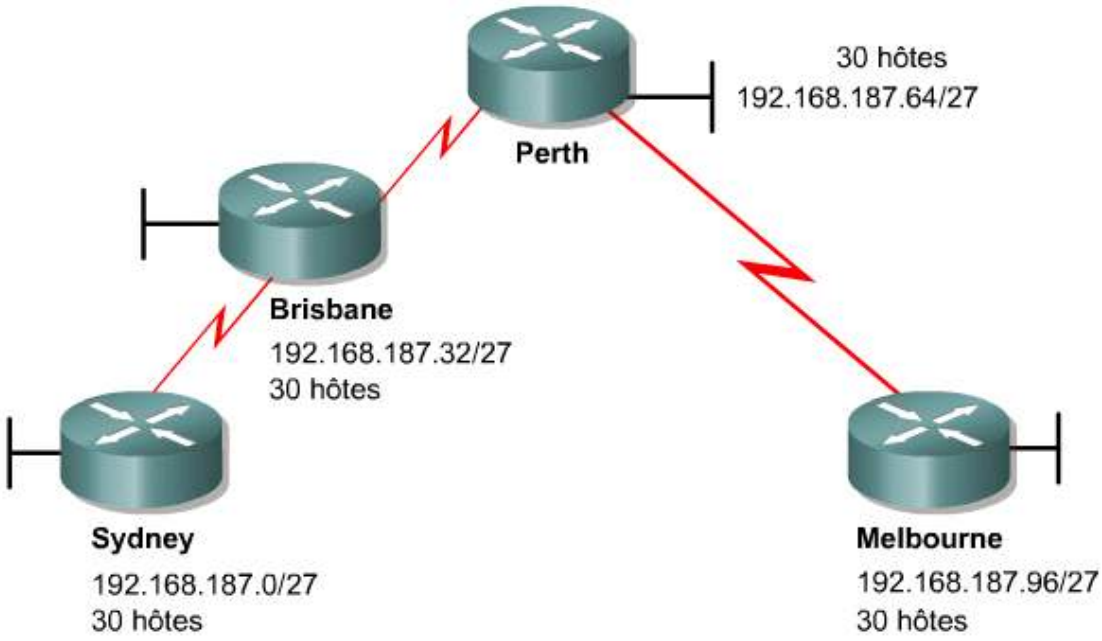
1.1.2 Gaspillage de l'espace

Auparavant, il était recommandé de ne pas utiliser le premier et le dernier sous-réseau. L'utilisation du premier sous-réseau (appelé sous-réseau zéro) pour l'adressage d'hôtes était déconseillée en raison de la confusion possible lorsqu'un réseau et un sous-réseau ont la même adresse. Pour la même raison, l'utilisation du dernier sous-réseau (appelé sous-réseau tout à 1) était également déconseillée. On pouvait utiliser ces sous-réseaux, mais ce n'était pas une pratique recommandée. Avec l'évolution des technologies de réseau et la pénurie anticipée d'adresses IP, il est devenu acceptable d'utiliser le premier et le dernier sous-réseau dans un réseau subdivisé en sous réseaux, en association avec la technique VLSM.

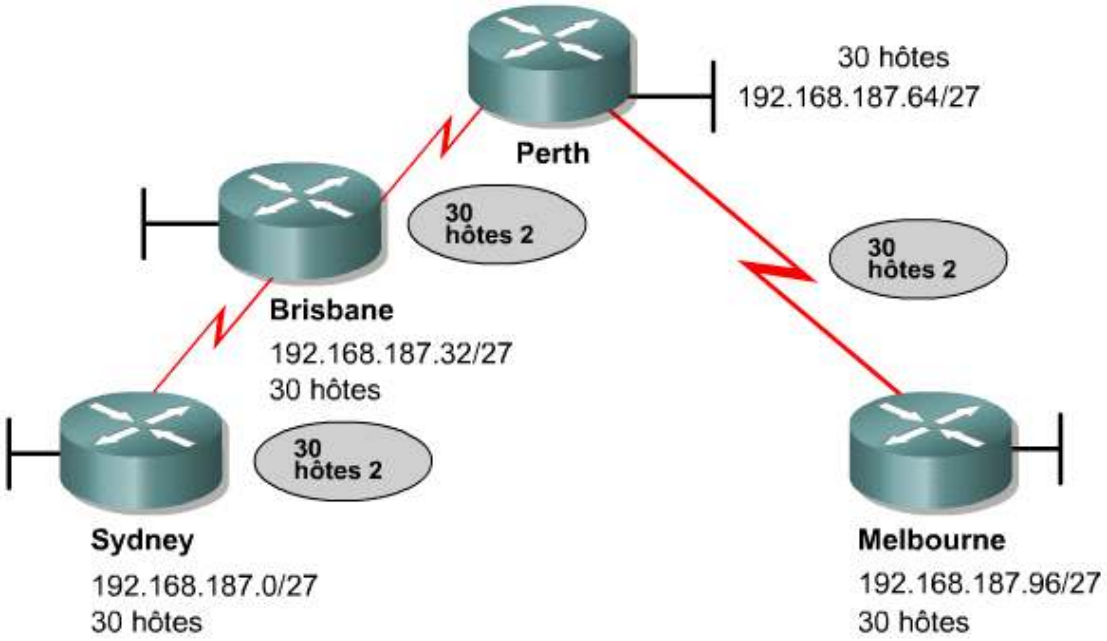
L'équipe d'administration de ce réseau a décidé d'emprunter trois bits de la portion hôte de l'adresse de classe C sélectionnée pour ce système d'adressage. 1

N° de sous-réseau	Adresse de sous-réseau	
Sous-réseau 0	192.168.187.0	/27
Sous-réseau 1	192.168.187.32	/27
Sous-réseau 2	192.168.187.64	/27
Sous-réseau 3	192.168.187.96	/27
Sous-réseau 4	192.168.187.128	/27
Sous-réseau 5	192.168.187.160	/27
Sous-réseau 6	192.168.187.192	/27
Sous-réseau 7	192.168.187.224	/27

Si l'équipe d'administration décide d'utiliser le sous-réseau zéro, elle peut alors utiliser huit sous-réseaux supplémentaires. Chacun de ces sous-réseaux peut accueillir 30 hôtes. Si l'équipe d'administration décide d'utiliser la commande **`no ip subnet-zero`**, elle pourra utiliser sept sous-réseaux de 30 hôtes chacun. Notez qu'à partir de la version 12.0 de Cisco IOS, les routeurs Cisco utilisent le sous-réseau zéro par défaut. Ainsi, les bureaux distants de Sydney, Brisbane, Perth et Melbourne peuvent accueillir jusqu'à 30 hôtes chacun. 2 L'équipe réalise qu'elle doit définir l'adressage des trois liaisons WAN point à point entre Sydney, Brisbane, Perth et Melbourne. Si elle utilise les trois sous-réseaux restants pour les liaisons WAN, c'est-à-dire les dernières adresses disponibles, il n'y aura plus d'espace disponible pour une future extension. L'équipe aura également gaspillé 28 adresses hôte sur chaque sous-réseau uniquement pour l'adressage de trois réseaux point à point. Avec ce système d'adressage, un tiers de l'espace d'adressage potentiel a été gaspillé.



Un tel système d'adressage convient pour un petit LAN. Néanmoins, il entraîne un gaspillage énorme lorsqu'il est utilisé avec des connexions point à point. 3

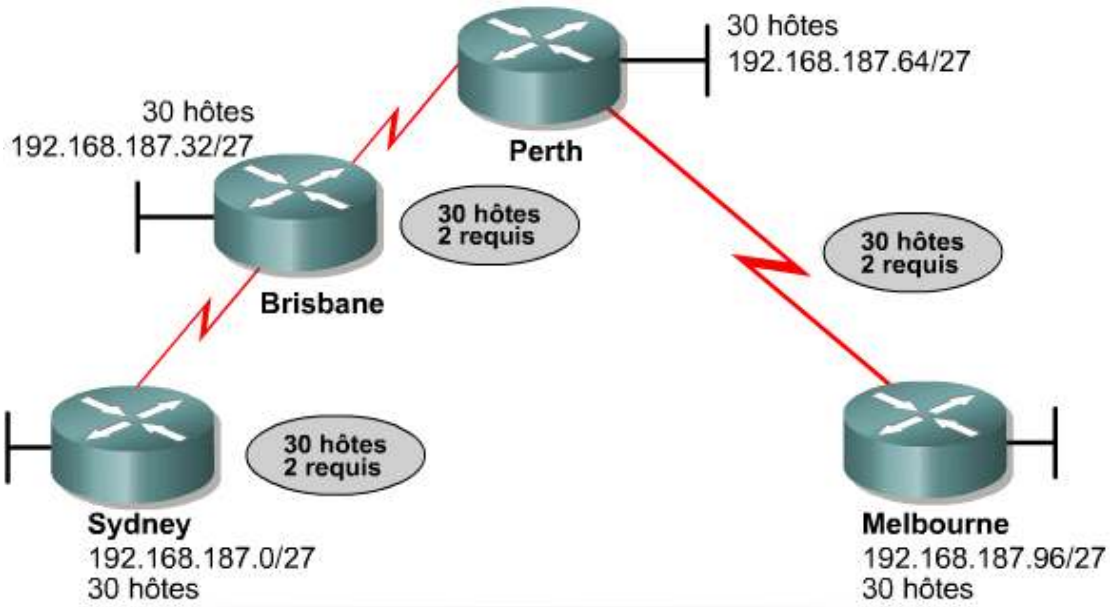


1.1 VLSM

1.1.3 Quand utiliser VLSM?

Il est important de concevoir un système d'adressage évolutif en termes de croissance et sans gaspillage d'adresses. Cette section explique comment l'utilisation de VLSM permet d'éviter le gaspillage d'adresses avec les liaisons point à point.

Cette fois-ci, l'équipe réseau a décidé de ne plus gaspiller le masque /27 sur les liaisons point à point. Elle a donc choisi d'appliquer la technique VLSM pour résoudre le problème d'adressage. 1



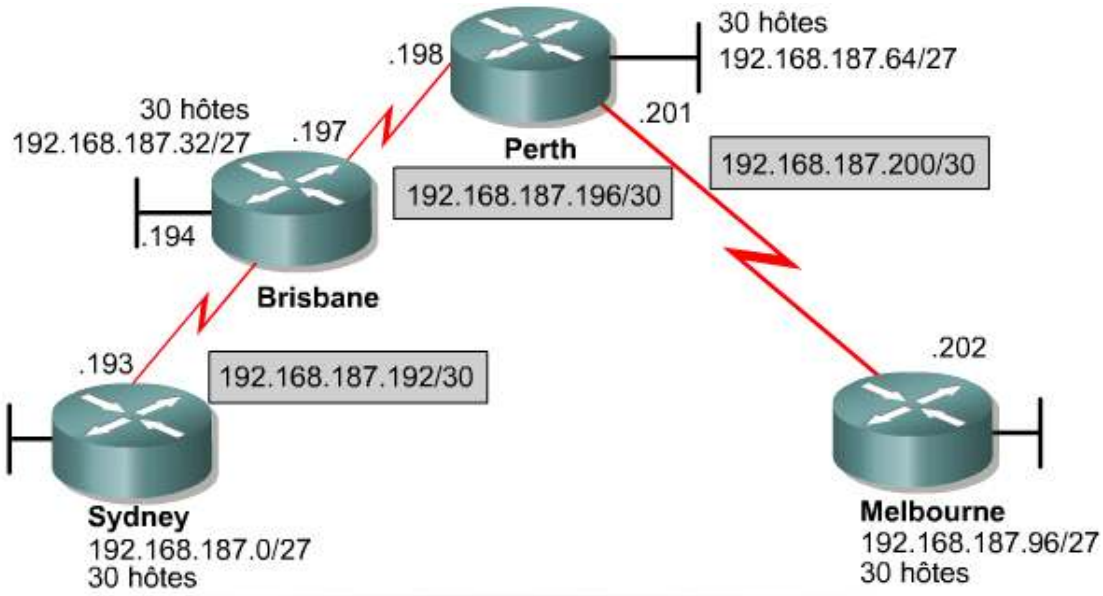
Utilisez VLSM sur les liaisons point-à-point pour n'utiliser que deux adresses hôte valides au lieu d'en gaspiller 28.

Pour appliquer la technique VLSM au problème d'adressage, l'équipe va décomposer l'adresse de classe C en plusieurs sous-réseaux de tailles variables. De grands sous-réseaux sont créés pour l'adressage des LAN. De très petits sous-réseaux sont créés pour les liaisons WAN et dans d'autres cas particuliers. Un masque de 30 bits est utilisé pour créer des sous-réseaux avec uniquement deux adresses hôte valides. Il s'agit de la meilleure solution pour les connexions point à point. L'équipe va récupérer un des trois sous-réseaux qu'elle avait précédemment affectés aux liaisons WAN et le diviser à nouveau en sous-réseaux avec un masque de 30 bits.

Dans cet exemple, l'équipe a récupéré un des trois derniers sous-réseaux, le sous-réseau 6, et l'a encore subdivisé en sous-réseaux. Cette fois-ci, l'équipe utilise un masque de 30 bits. Les figures 2 et 3 montrent qu'après l'utilisation de la technique VLSM, l'équipe dispose de huit plages d'adresses à utiliser pour les liaisons point à point.

N° de sous-réseau	Adresse de sous-réseau	
Sous-réseau 0	192.168.187.0	/27
Sous-réseau 1	192.168.187.32	/27
Sous-réseau 2	192.168.187.64	/27
Sous-réseau 3	192.168.187.96	/27
Sous-réseau 4	192.168.187.128	/27
Sous-réseau 5	192.168.187.160	/27
Sous-réseau 6	192.168.187.192	/27
Sous-réseau 7	192.168.187.224	/27

N° de sous-réseau	Adresse de sous-réseau	
Sous-sous-réseau 0	192.168.187.192	/30
Sous-sous-réseau 1	192.168.187.196	/30
Sous-sous-réseau 2	192.168.187.200	/30
Sous-sous-réseau 3	192.168.187.204	/30
Sous-sous-réseau 4	192.168.187.208	/30
Sous-sous-réseau 5	192.168.187.212	/30
Sous-sous-réseau 6	192.168.187.216	/30
Sous-sous-réseau 7	192.168.187.220	/30



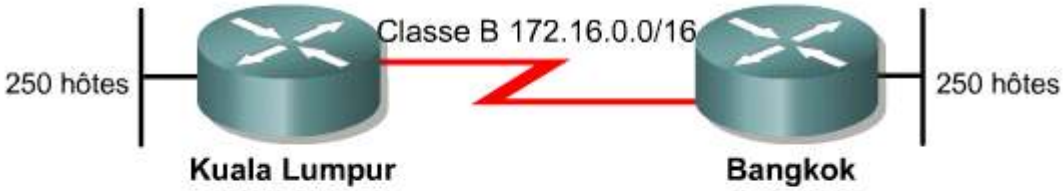
Notez les masques de bits /27 pour les LAN et les masques de bits /30 pour les liaisons série.

1.1 VLSM

1.1.4 Calcul des sous-réseaux avec VLSM

La technique VLSM permet de gérer les adresses IP. VLSM permet de définir un masque de sous-réseaux répondant aux besoins de la liaison ou du segment. Un masque de sous-réseau devrait en effet répondre aux besoins d'un LAN avec un masque de sous-réseau et à ceux d'une liaison WAN point à point avec un autre. [1]

Observez l'exemple de la figure [1] qui illustre le mode de calcul des sous-réseaux avec VLSM.

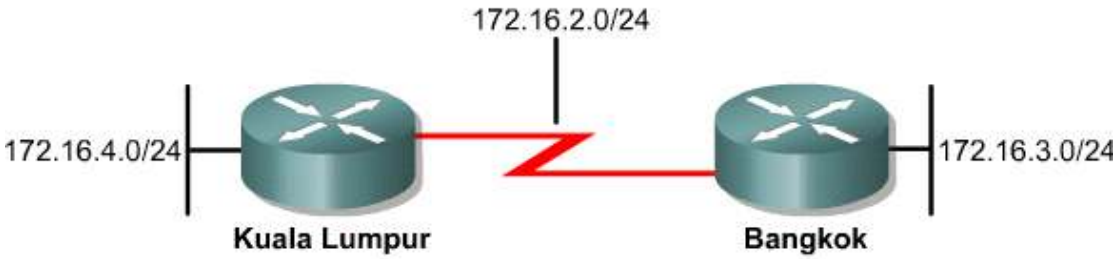


Chaque réseau LAN doit accepter jusqu'à 250 hôtes. Le réseau de classe B 172.16.0.0/16 peut être subdivisé avec un masque sur 24 bits (255.255.255.0) pour créer des sous-réseaux suffisamment importants pour chaque LAN.

L'exemple contient une adresse de classe B, 172.16.0.0, et deux LAN nécessitant au moins 250 hôtes chacun. Si les routeurs utilisent un protocole de routage par classes, la liaison WAN doit être un sous-réseau du même réseau de classe B, à condition que l'administrateur n'utilise pas le type de connexion IP non numéroté. Les protocoles de routage par classes tels que RIP v1, IGRP et EGP ne sont pas compatibles avec VLSM. Sans VLSM, la liaison WAN devrait utiliser le même masque de sous-réseau que les segments LAN. Un masque de 24 bits (255.255.255.0) peut accueillir au moins 250 hôtes. / Un masque de 24 bits (255.255.255.0) peut accueillir 254 hôtes. [2] [3]

Classe B subdivisée sous la forme 255.255.255.0

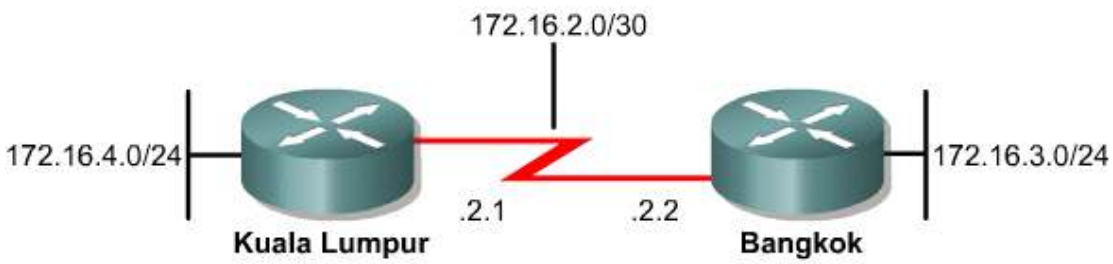
N°	Sous-réseau	Plage d'adresses	Adresse de broadcast
0	172.16.0.0	172.16.0.1 - 172.16.0.254	172.16.0.255
1	172.16.1.0	172.16.1.1 - 172.16.1.254	172.16.1.255
2	172.16.2.0	172.16.2.1 - 172.16.2.254	172.16.2.255
3	172.16.3.0	172.16.3.1 - 172.16.3.254	172.16.3.255
4	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
5	172.16.5.0	172.16.5.1 - 172.16.5.254	172.16.5.255
6	172.16.6.0	172.16.6.1 - 172.16.6.254	172.16.6.255
7	172.16.7.0	172.16.7.1 - 172.16.7.254	172.16.7.255
8	172.16.8.0	172.16.8.1 - 172.16.8.254	172.16.8.255
9	172.16.9.0	172.16.9.1 - 172.16.9.254	172.16.9.255
10	172.16.10.0	172.16.10.1 - 172.16.10.254	172.16.10.255
11	172.16.11.0	172.16.11.1 - 172.16.11.254	172.16.11.255
12	172.16.12.0	172.16.12.1 - 172.16.12.254	172.16.12.255
13	172.16.13.0	172.16.13.1 - 172.16.13.254	172.16.13.255
14	172.16.14.0	172.16.14.1 - 172.16.14.254	172.16.14.255
15	172.16.15.0	172.16.15.1 - 172.16.15.254	172.16.15.255



Chaque liaison peut accepter jusqu'à 254 hôtes, mais la liaison WAN n'en nécessite que deux, un pour chaque interface de routeur. 252 adresses seraient donc gaspillées.

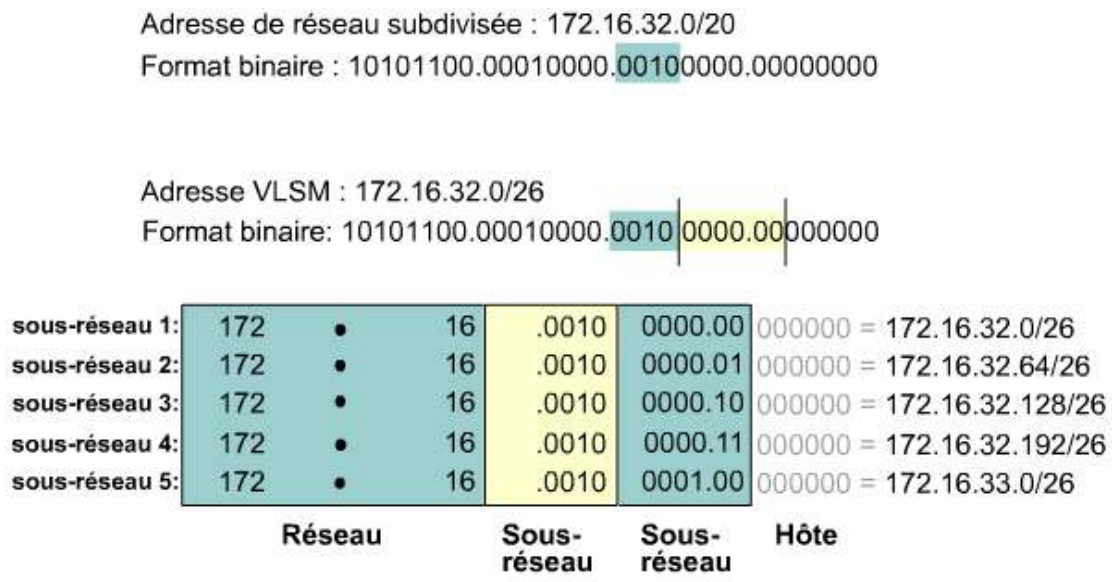
La liaison WAN n'utilise que deux adresses, une pour chaque routeur. 252 adresses seraient donc gaspillées.

Si la technique VLSM était utilisée dans cet exemple, il serait toujours possible d'utiliser un masque de 24 bits sur les segments LAN pour les 250 hôtes. Un masque de 30 bits pourrait alors être utilisé pour la liaison WAN qui ne requiert que deux adresses hôte. 4

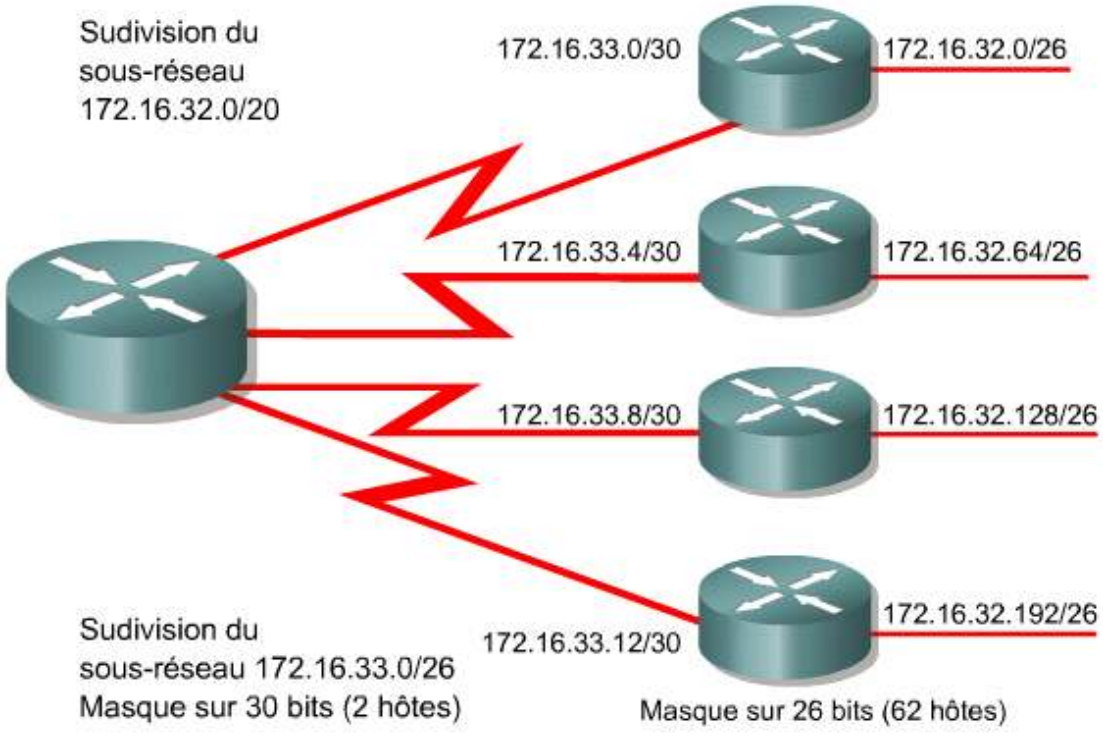


/30 permet de gaspiller moins d'adresses.

Dans la figure 5, les adresses de sous-réseau utilisées sont celles générées après la subdivision du sous-réseau 172.16.32.0/20 en plusieurs sous-réseaux /26. La figure indique où les adresses de sous-réseau peuvent être appliquées en fonction du nombre d'hôtes requis. Par exemple, les liaisons WAN utilisent les adresses de sous-réseau qui ont le préfixe /30. Ce préfixe n'autorise que deux hôtes, juste assez pour une connexion point à point entre deux routeurs.



Pour calculer les adresses de sous-réseau utilisées sur les liaisons WAN, vous devez subdiviser un des réseaux /26 inutilisé. Dans cet exemple, 172.16.33.0/26 est subdivisé avec le préfixe /30. Quatre bits de sous-réseau supplémentaires sont ainsi générés ce qui crée 16 (2^4) sous-réseaux pour les WAN. La figure 6 indique comment travailler avec un système de masque VLSM.



VLSM autorise la subdivision en sous-réseaux d'une adresse déjà divisée. Par exemple, considérons l'adresse de sous-réseau 172.16.32.0/20 et un réseau ayant besoin de 10 adresses hôte. Cette adresse de sous-réseau permet d'utiliser plus de 4000 ($2^{12} - 2 = 4094$) adresses hôte, mais la plupart d'entre elles seront gaspillées. La technique VLSM permet de diviser encore l'adresse 172.16.32.0/20 pour obtenir davantage d'adresses réseau avec moins d'hôtes par réseau. Par exemple, en subdivisant les sous-réseaux 172.16.32.0/20 à 172.16.32.0/26, vous obtenez 64 (2^6) sous-réseaux supplémentaires pouvant chacun gérer 62 ($2^6 - 2$) hôtes.

Étape 1 Écrivez 172.16.32.0 au format binaire.

Étape 2 Tracez une ligne verticale entre le 20ème et le 21ème bit, comme l'illustre la figure 5. /20 correspond à la frontière d'origine.

Étape 3 Tracez une ligne verticale entre le 26ème et le 27ème bit, comme l'illustre la figure 5. La frontière d'origine /20 est déplacée de six bits vers la droite, devenant /26.

Étape 4 Calculez les 64 adresses de sous-réseau en utilisant les bits qui se trouvent entre les deux lignes verticales, de la plus petite à la plus grande valeur. La figure montre les cinq premiers sous-réseaux disponibles.

Il est important de garder à l'esprit que seuls les sous-réseaux inutilisés peuvent être subdivisés. Si une des adresses d'un sous-réseau est utilisée, ce sous-réseau ne peut plus être subdivisé. Dans notre exemple, quatre numéros de sous-réseau sont utilisés sur les LAN. Un autre sous-réseau, inutilisé (172.16.33.0/26), est subdivisé pour être utilisé sur les WAN.

Activité de TP

Exercice: Calcul des sous-réseaux VLSM

Au cours de ce TP, les étudiants utiliseront la technique VLSM (Variable-Length Subnet Mask) pour gérer plus efficacement l'attribution des adresses IP et réduire le nombre d'informations de routage au niveau supérieur.

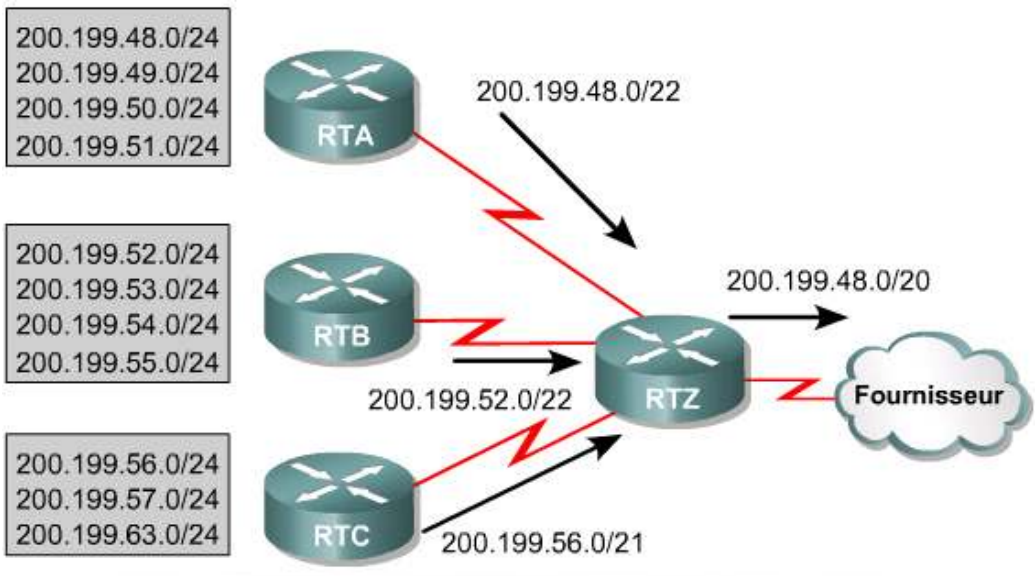
1.1 VLSM
1.1.5 Regroupement de routes avec VLSM

Lorsque vous utilisez VLSM, essayez de grouper les numéros des sous-réseaux du réseau pour pouvoir utiliser le regroupement. Par exemple, les réseaux 172.16.14.0 et 172.16.15.0 doivent être proches l'un de l'autre pour que les routeurs n'aient qu'une route à gérer pour 172.16.14.0/23. 1

Fournisseur

- La proximité des réseaux permet de minimiser la taille de la table de routage.
- À chaque réseau doit correspondre une entrée séparée dans la table de routage.
- À chaque sous-réseau doit correspondre une entrée séparée dans la table de routage.
- Le regroupement peut réduire la taille de la table de routage.

L'utilisation du routage CIDR (Classless InterDomain Routing) et de VLSM permet non seulement d'éviter le gaspillage d'adresses mais favorise également le regroupement et le résumé de routes. Sans le résumé de routes, le routage du backbone Internet se serait probablement effondré peu avant 1997. 2



Le résumé de routes réduit la taille de la table de routage en regroupant les routes vers plusieurs réseaux en une même route SUPERNET.

La figure 2 illustre comment le résumé de routes permet de réduire la charge sur les routeurs en amont. Cette hiérarchie complexe de réseaux et de sous-réseaux de tailles variables est résumée en différents points, à l'aide d'une adresse avec préfixe, jusqu'à ce que le réseau entier soit annoncé comme une route unique globale, 200.199.48.0/22. Le résumé de routes, aussi appelé « supernetting », ne peut être utilisé que si les routeurs d'un réseau exécutent un protocole de routage CIDR tel qu'OSPF ou EIGRP. Les protocoles de routage CIDR adoptent un préfixe formé d'une adresse IP de 32 bits et d'un bit de masque dans les mises à jour de routage. Dans la figure 2, la route sommaire qui atteint finalement le fournisseur contient un préfixe de 20 bits commun à toutes les adresses de l'organisation, 200.199.48.0/22 ou 11001000.11000111.0011. Pour que le mécanisme de résumé fonctionne correctement, veillez à affecter les adresses de façon hiérarchique pour que les adresses résumées partagent les mêmes bits de valeur supérieure.

N'oubliez pas les règles suivantes:

- Un routeur doit parfaitement connaître les numéros des sous-réseaux qui lui sont connectés.
- Un routeur n'a pas besoin de signaler individuellement chaque sous-réseau aux autres routeurs s'il peut se contenter d'envoyer une route globale.
- Un routeur qui utilise des routes globales peut réduire le nombre d'entrées de sa table de routage.

VLSM permet le résumé de routes et améliore la flexibilité en basant entièrement le mécanisme de résumé sur le partage des bits de valeur supérieure situés à gauche, même si les réseaux ne sont pas contigus. 3

Adresses	Premier Octet	Second Octet	Troisième Octet	Quatrième Octet
192.168.98.0	11000000	10101000	01100010	00000000
192.168.99.0	11000000	10101000	01100011	00000000
192.168.100.0	11000000	10101000	01100100	00000000
192.168.101.0	11000000	10101000	01100101	00000000
192.168.102.0	11000000	10101000	01100110	00000000
192.168.105.0	11000000	10101000	01101001	00000000

La route sommaire est 192.168.96.0/20

192.168.96.0	11000000	10101000	01100000	00000000

Le tableau montre que les adresses, ou les routes, partagent les 20 premiers bits, 20ème inclus. Ces bits apparaissent en rouge. Le 21ème bit peut varier d'une route à l'autre. Par conséquent, la longueur du préfixe de la route sommaire sera de 20 bits. Ce préfixe est utilisé pour calculer le numéro de réseau de la route sommaire.

Dans la figure 4, les adresses, ou les routes, partagent les 21 premiers bits, 21ème inclus. Ces bits apparaissent en rouge. Le 22ème bit peut varier d'une route à l'autre. Par conséquent, la longueur du préfixe de la route sommaire sera de 21 bits. Ce préfixe est utilisé pour calculer le numéro de réseau de la route sommaire.

Adresses	Premier Octet	Second Octet	Troisième Octet	Quatrième Octet
172.16.0.0	10101100	00010000	00000000	00000000
172.16.2.0	10101100	00010000	00000010	00000000
172.16.3.128	10101100	00010000	00000011	10000000
172.16.4.0	10101100	00010000	00000100	00000000
172.16.4.128	10101100	00010000	00000100	10000000

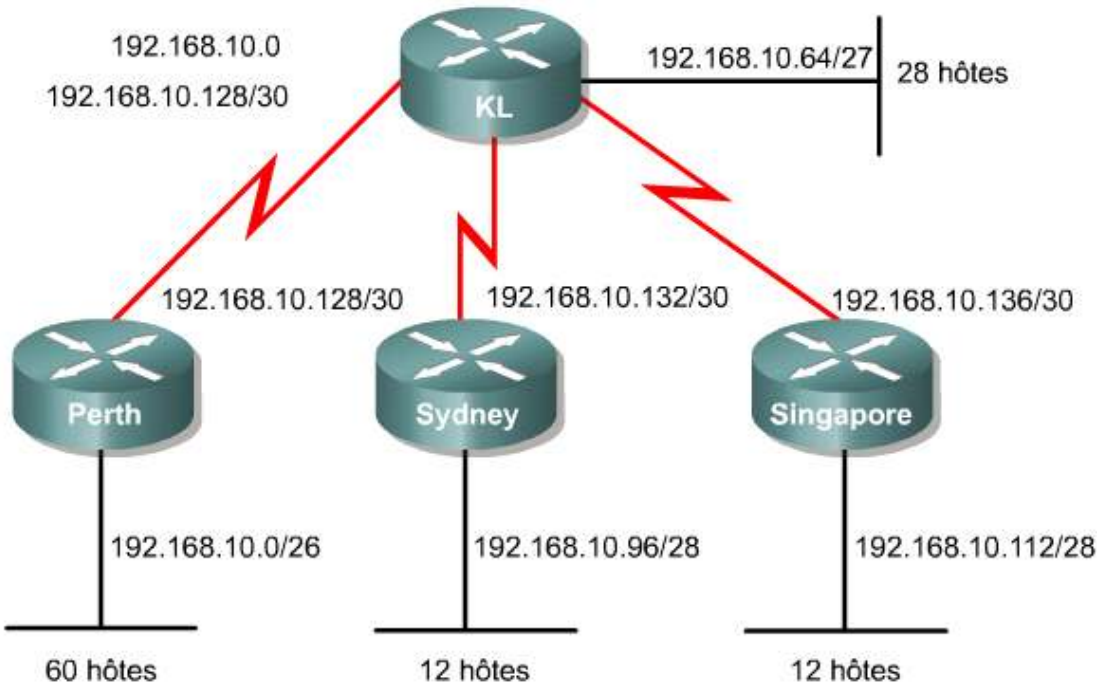
Réponse :

172.16.0.0/21	10101100	00010000	00000000	00000000

1.1 VLSM

1.1.6 Configuration de VLSM

Si le système d'adressage VLSM est choisi, il doit être calculé et configuré correctement. 1



Cet exemple présente les caractéristiques suivantes:

Adresse réseau: 192.168.10.0

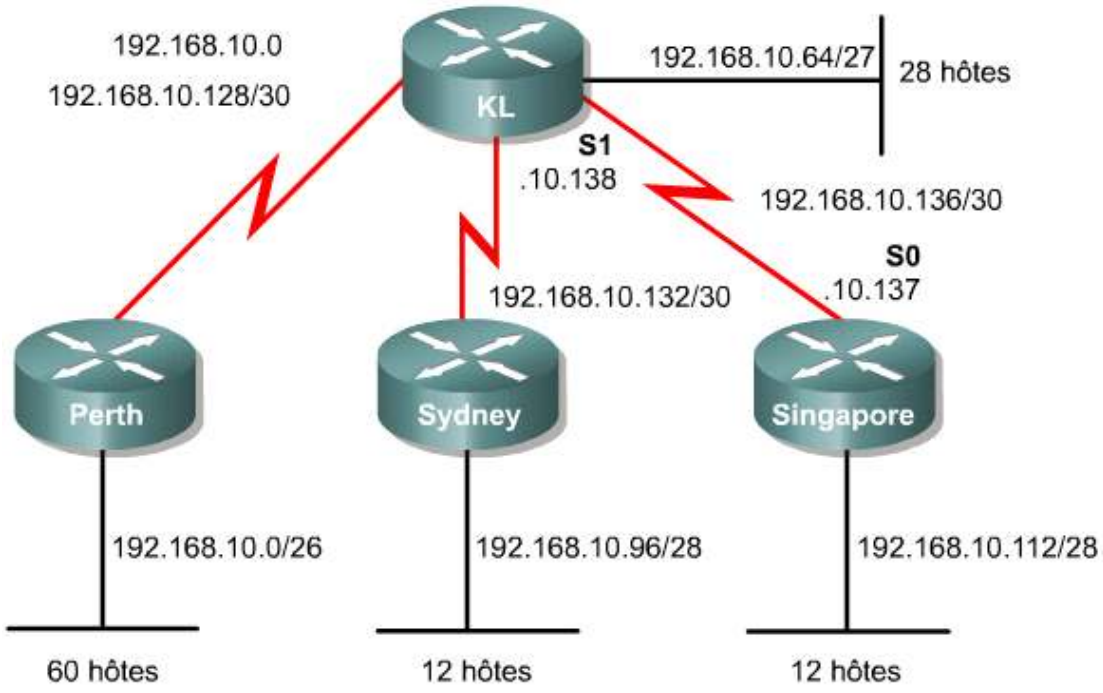
Le routeur Perth doit accueillir 60 hôtes. Dans ce cas, il faut au moins six bits dans la portion hôte de l'adresse. Six bits permettent de générer 62 adresses hôte, $2^6 = 64 - 2 = 62$, la division donne donc 192.168.10.0/26.

Les routeurs Sydney et Singapore doivent gérer 12 hôtes chacun. Dans ce cas, il faut au moins quatre bits dans la portion hôte de l'adresse. Quatre bits permettent de générer 14 adresses hôte, $2^4 = 16 - 2 = 14$, la division donne donc 192.168.10.96/28 pour Sydney et 192.168.10.112/28 pour Singapore.

Le routeur Kuala Lumpur doit gérer 28 hôtes. Dans ce cas, il faut au moins cinq bits dans la portion hôte de l'adresse. Cinq bits permettent de générer 30 adresses hôte, $2^5 = 32 - 2 = 30$, la division donne donc ici 192.168.10.64/27.

Les connexions suivantes sont des connexions point à point:

- **Perth vers Kuala Lumpur 192.168.10.128/30** – Comme il ne faut que deux adresses, la portion hôte de l'adresse doit contenir au moins deux bits. Deux bits permettent de générer 2 adresses hôte ($2^2 = 4 - 2 = 2$), la division donne donc ici 192.168.10.128/30.
- **Sydney vers Kuala Lumpur 192.168.10.132/30** – Comme il ne faut que deux adresses, la portion hôte de l'adresse doit contenir au moins deux bits. Deux bits permettent de générer 2 adresses hôte ($2^2 = 4 - 2 = 2$), la division donne donc ici 192.168.10.132/30.
- **Singapore vers Kuala Lumpur 192.168.10.136/30** – Comme il ne faut que deux adresses, la portion hôte de l'adresse doit contenir au moins deux bits. Deux bits permettent de générer 2 adresses hôte ($2^2 = 4 - 2 = 2$), la division donne donc ici 192.168.10.136/30. 2



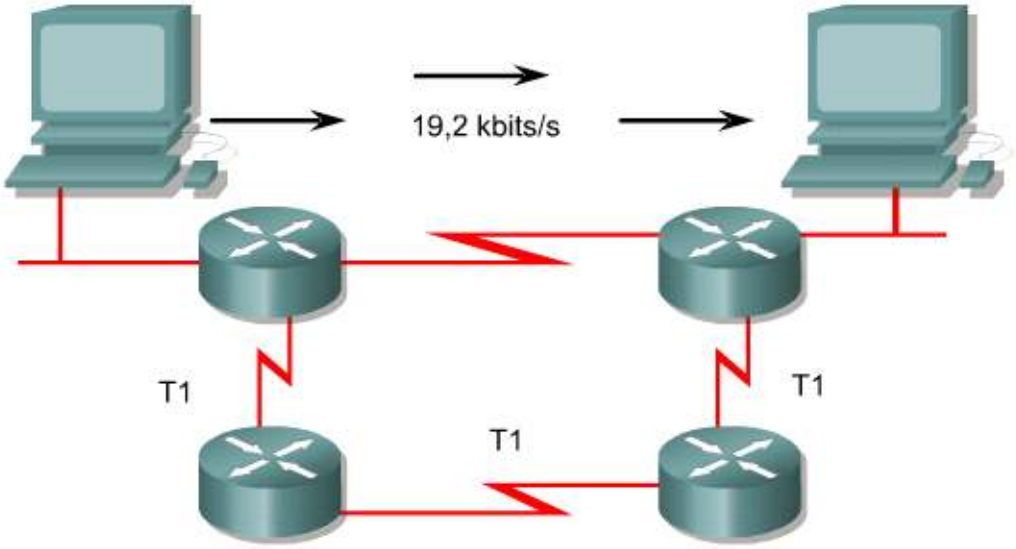
L'espace d'adressage hôte est suffisant pour deux points d'extrémité hôte sur une liaison série point à point. L'exemple Singapore vers Kuala Lumpur est configuré comme suit:

```
Singapore(config)#interface serial 0
Singapore(config-if)#ip address 192.168.10.137 255.255.255.252
KualaLumpur(config)#interface serial 1
KualaLumpur(config-if)#ip address 192.168.10.138 255.255.255.252
```

1.2 RIP Version 2

1.2.1 Historique du protocole RIP

Internet est un ensemble de systèmes autonomes (SA). En règle générale, chaque SA est administré par une entité unique. Chaque SA a sa propre technologie de routage, qui peut être différente de celle des autres systèmes autonomes. Le protocole de routage utilisé au sein d'un SA est appelé IGP (Interior Gateway Protocol). Un protocole distinct, appelé EGP (Exterior Gateway Protocol), est utilisé pour transférer des informations de routage entre différents systèmes autonomes. Le protocole RIP a été conçu pour fonctionner comme un IGP dans un SA de taille moyenne. Il n'est pas censé être utilisé dans des environnements plus complexes.



Quelques caractéristiques de RIP:

- 6 chemins au maximum. La valeur par défaut est 4.
- La métrique utilisée est le nombre de sauts. La limite maximale de sauts autorisé est 15.
- Mise à jour de routage à chaque 30 secondes.

RIP v1 est considéré comme un protocole IGP par classes (classful). 1RIP v1 est un protocole à vecteur de distance qui diffuse intégralement sa table de routage à chaque routeur voisin, à intervalles prédéfinis. L'intervalle par défaut est de 30 secondes. RIP utilise le nombre de sauts comme métrique, avec une limite de 15 sauts maximum.

Si le routeur reçoit des informations concernant un réseau et que l'interface de réception appartient au même réseau mais se trouve sur un sous-réseau différent, le routeur applique le masque de sous-réseau configuré sur l'interface de réception:

- Pour les adresses de classe A, le masque de classe par défaut est 255.0.0.0.
- Pour les adresses de classe B, le masque de classe par défaut est 255.255.0.0.
- Pour les adresses de classe C, le masque de classe par défaut est 255.255.255.0.

RIP v1 est un protocole de routage très populaire car il est compatible avec tous les routeurs IP. Son succès repose essentiellement sur sa simplicité et sa compatibilité universelle. RIP v1 est capable de gérer l'équilibrage de charge sur au plus de six chemins de coût égal, avec quatre chemins par défaut.

RIP v1 comporte les limitations suivantes:

- Il n'envoie pas d'informations sur les masques de sous-réseau dans ses mises à jour.
- Il envoie des mises à jour sous forme de broadcasts sur 255.255.255.255.
- Il ne prend pas l'authentification en charge.
- Il ne prend en charge ni VLSM, ni le routage CIDR (Classless Interdomain Routing).

RIP v1 est facile à configurer, comme l'illustre la figure 2

Configuration RIP v1

```
Sydney(config)#router rip
Sydney(config-router)#network network-number
Sydney(config-router)#network network-number
Sydney(config-router)#network network-number
Sydney(config-router)#network network-number
```

.

1.2 RIP Version 2

1.2.2 Caractéristiques de RIP v2

RIP v2 est une version améliorée de RIP v1. Les deux protocoles partagent un certain nombre de caractéristiques: 1

Caractéristique	Description
Transmet le masque de sous-réseau avec la route	Active VLSM en transmettant le masque avec chaque route de manière à définir exactement le sous-réseau.
Prend en charge l'authentification	Texte clair ou, le cas échéant, MD5
Inclut une adresse IP de saut suivant dans sa mise à jour de routage	Un routeur peut annoncer une route et diriger tout équipement à l'écoute vers un autre routeur du même sous-réseau (si ce dernier a une meilleure route).
Utilise des étiquettes de route externe	RIP peut transmettre des informations sur des routes acquises d'une source externe et de les redistribuer dans RIP. Cela permet de séparer les routes RIP des routes apprises de sources externes.
Fournit des mises à jour de routage multicast	Au lieu d'envoyer des mises à jour à 255.255.255.255, l'adresses IP de destination est 224.0.0.9. Cela réduit le nombre d'opérations de traitement nécessaires sur les hôtes non-RIP d'un sous-réseau commun.

- Il s'agit d'un protocole à vecteur de distance utilisant le nombre de sauts comme métrique.
- Il utilise des compteurs de retenue pour empêcher les boucles de routage (valeur par défaut: 180 secondes).
- Il utilise la règle «split horizon» pour empêcher les boucles de routage.
- Il utilise 16 sauts comme métrique de mesure infinie.

RIP v2 présente une fonctionnalité de routage CIDR lui permettant d'envoyer des informations sur les masques de sous-réseau avec la mise à jour des routes. Par conséquent, RIP v2 prend en charge le routage CIDR qui permet à différents sous-réseaux du même réseau d'utiliser des masques de sous-réseau distincts, comme dans VLSM.

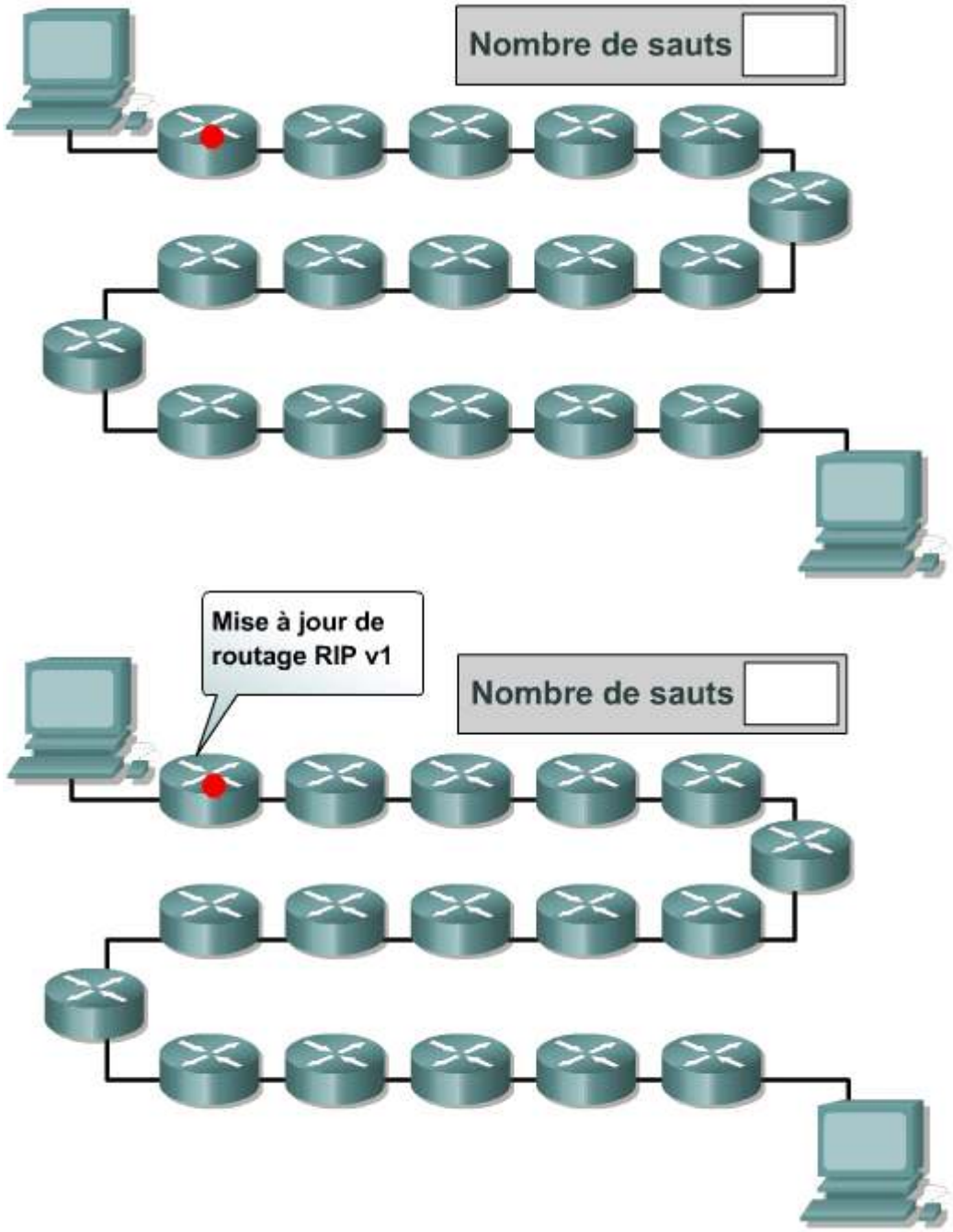
RIP v2 permet l'authentification dans ses mises à jour. Il est possible d'utiliser une combinaison de clés sur une interface comme vérification d'authentification. RIP v2 permet de choisir le type d'authentification à utiliser dans les paquets RIP v2. Il peut s'agir de texte en clair ou d'un cryptage basé sur l'algorithme d'authentification MD5. Le type d'authentification par défaut est le texte en clair. L'algorithme MD5 peut être utilisé pour authentifier la source d'une mise à jour de routage. MD5 est généralement utilisé pour le cryptage des mots de passe enable secret et n'a pas d'algorithme de réversibilité connu.

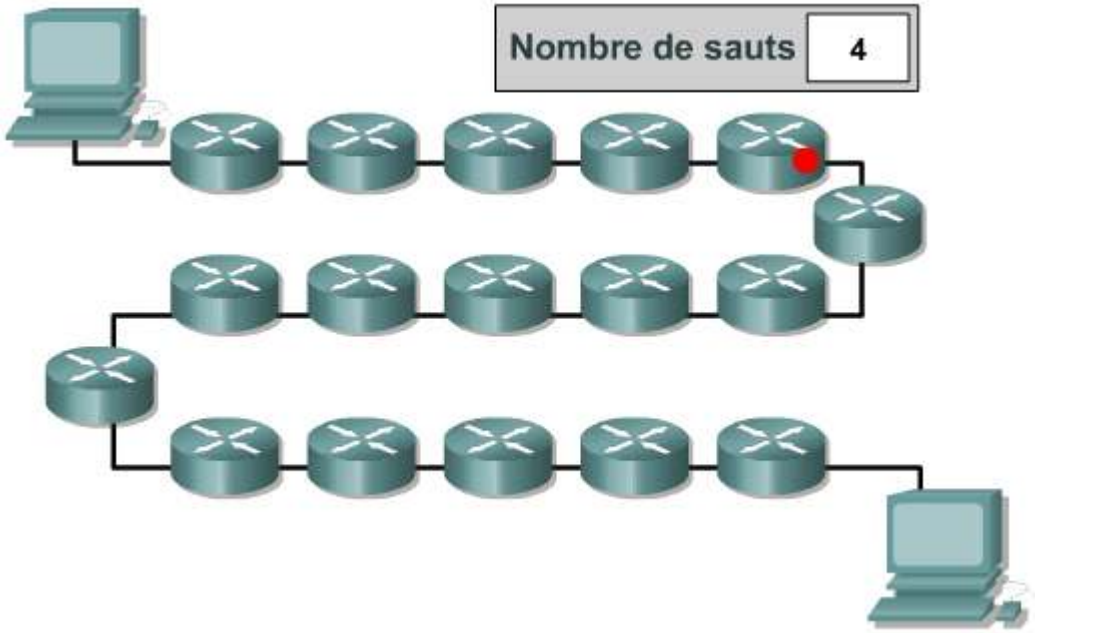
Pour une meilleure efficacité, RIP v2 utilise l'adresse de classe D 224.0.0.9 pour envoyer les mises à jour de routage en multicast.

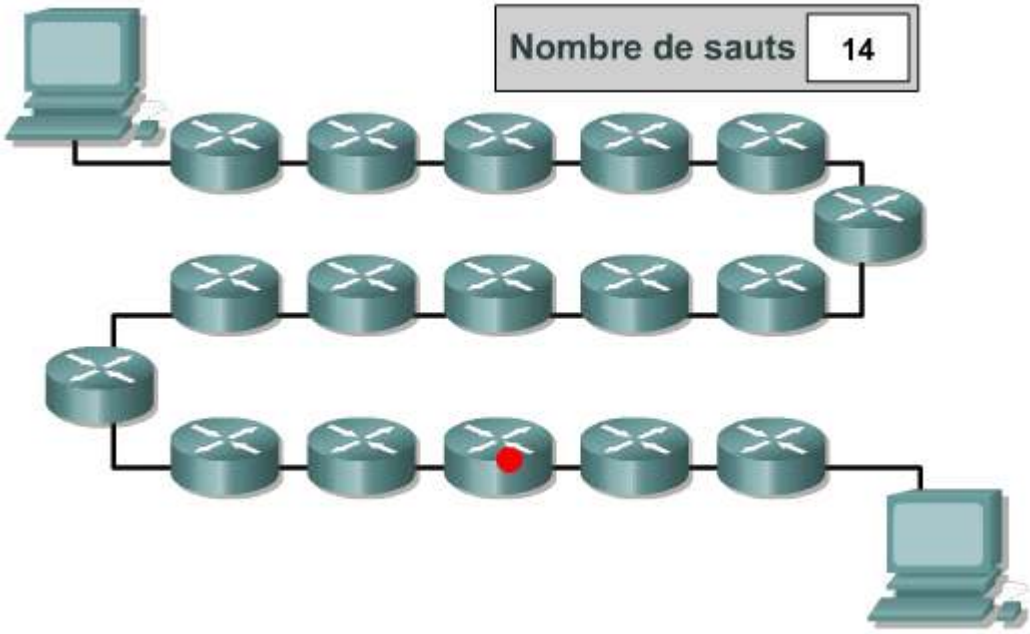
1.2 RIP Version 2

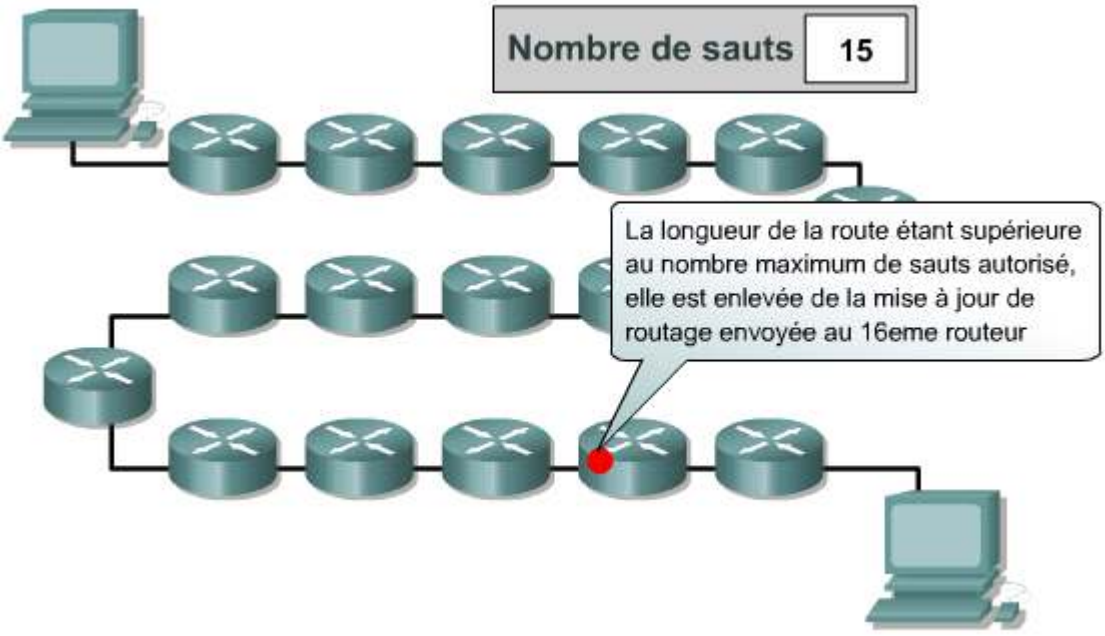
1.2.3 Comparaison des versions 1 et 2 de RIP

Le protocole RIP utilise des algorithmes à vecteur de distance pour déterminer la direction et la distance jusqu'à une liaison quelconque de l'interréseau. S'il existe plusieurs chemins vers une destination, le protocole RIP sélectionne celui qui comporte le moins de sauts. Toutefois, comme le nombre de sauts est la seule métrique de routage utilisée par le protocole RIP, il n'est pas garanti que le chemin sélectionné soit le plus rapide. 1




Nombre de sauts
4


Nombre de sauts
14


Nombre de sauts
15
La longueur de la route étant supérieure au nombre maximum de sauts autorisé, elle est enlevée de la mise à jour de routage envoyée au 16eme routeur

RIP v1 permet aux routeurs de mettre à jour leurs tables de routage à des intervalles programmables. L'intervalle par défaut est de 30 secondes. L'envoi continu de mises à jour de routage par RIP v1 signifie que le trafic réseau augmente rapidement. Pour éviter qu'un paquet ne tourne en boucle indéfiniment, le protocole RIP limite le nombre de sauts à 15 maximum. Si le réseau de destination se trouve à une distance de plus de 15 routeurs, on considère que ce réseau est inaccessible et le paquet est abandonné. Se pose alors la question de l'évolutivité pour le routage au sein d'importants réseaux hétérogènes. RIP v1 utilise la règle «split horizon» pour empêcher les boucles de routage. Cela signifie que RIP v1 annonce les routes en sortie d'une interface uniquement lorsqu'elles n'ont pas été apprises via des mises à jour en entrée de cette interface. Le protocole utilise des compteurs de retenue pour empêcher les boucles de routage. Les gels permettent d'ignorer les nouvelles informations provenant d'un sous-réseau en affichant une moins bonne métrique au cours du délai de retenue.

La figure 2 résume le comportement de RIP v1 lorsque ce dernier est utilisé par un routeur.

Comportement de RIP v1	Explication
Les sous-réseaux directement connectés sont déjà connus du routeur.	Ces routes sont annoncées aux routeurs voisins.
Les mises à jour de routage sont de type broadcast.	Tous les routeurs voisins apprennent les routes via un broadcast unique.
Les routeurs sont à l'écoute des mises à jour.	Aide les routeurs à apprendre de nouvelles routes.
Une métrique décrit chaque route dans la mise à jour.	Décrit le fonctionnement de la route optimale. S'il existe de nombreuses routes, la route ayant la plus faible métrique est utilisée.
Les mises à jour de routage contiennent des informations de topologie.	Inclut au moins les informations de métrique.
Des mises à jour périodiques sont attendues des routeurs voisins.	L'échec de réception des mises à jour dans les temps résulte en la suppression des routes précédemment apprises des réseaux voisins.
Les routes apprises des routeurs voisins sont présumées provenir de ces routeurs.	Les routeurs envoient les mises à jour de leur table de routage à leurs routeurs voisins
Une route défaillante est annoncée temporairement avec une métrique impliquant une distance " infinie ".	RIP v1 utilise 16 comme distance infinie, car le nombre maximum de sauts valides est 15.

RIP v2 est une version améliorée de RIP v1. Ils ont beaucoup de fonctions communes. RIP v2 est également un protocole à vecteur de distance qui utilise le nombre de sauts, les compteurs de retenue et la règle «split horizon». La figure 3 compare RIP v1 et RIP v2.

RIP v1	RIP v2
Facile à configurer	Facile à configurer
Prend en charge uniquement un protocole de routage par classes (classful).	Prend en charge l'utilisation du routage CIDR (Classless).
La mise à jour de routage ne contient aucune information de sous-réseau.	Envoie des informations sur les masques de sous-réseau avec les mises à jour des routes.
Ne supporte pas le routage CIDR ce qui oblige tous les équipements d'un même réseau à utiliser le même masque de sous-réseau	Supporte le routage CIDR ce qui permet à des équipements d'un même réseau d'utiliser différents masques de sous-réseau
Aucune authentification dans les mises à jour	Permet l'authentification dans ses mises à jour de routage
Envoie les broadcasts sur 255.255.255.255.	Envoie les mises à jour de routage en multicast sur 224.0.0.9 ce qui est plus efficace.

Activité de TP

Exercice: Révision de la configuration de base des routeurs avec le protocole RIP

Au cours de ce TP, les étudiants vont configurer un système d'adressage en utilisant des réseaux de classe B et configurer le protocole de routage RIP sur des routeurs.

Activité de TP

Activité en ligne: Configuration de base et du protocole RIP

Au cours de ce TP, les étudiants vont revoir la configuration de base des routeurs.

Activité de média interactive

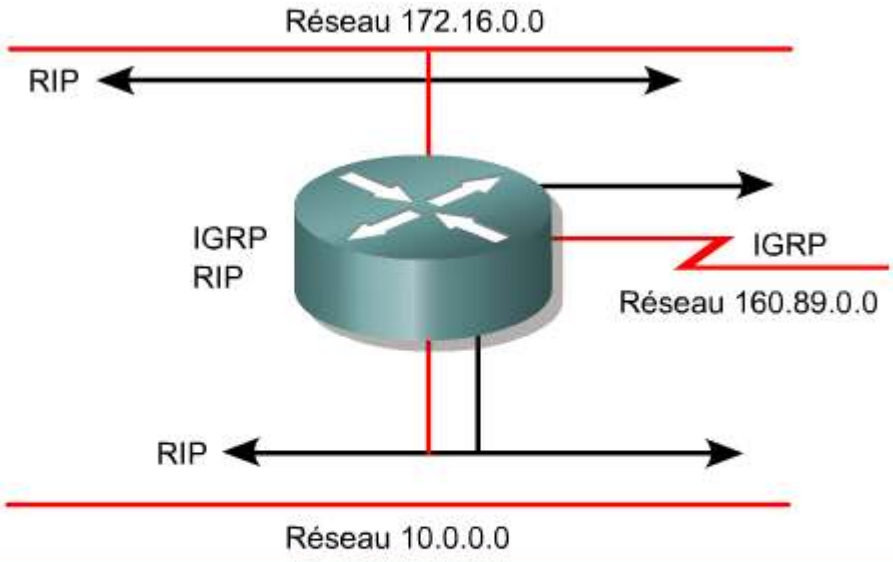
Case à cocher: Comparaison entre RIP v1 et RIP v2

Une fois qu'il aura terminé cette activité, l'étudiant sera en mesure de faire la différence entre RIP v1 et RIP v2.

1.2 RIP Version 2

1.2.4 Configuration de RIP v2

RIP v2 est un protocole de routage dynamique configuré en spécifiant le protocole de routage RIP Version 2, puis en attribuant des numéros de réseau IP sans préciser de valeurs de sous-réseau. Cette section décrit les commandes de base permettant de configurer RIP v2 sur un routeur Cisco. 1



Les tâches suivantes sont nécessaires pour configurer un protocole de routage:

- Indication des réseaux ou des interfaces
- Configuration du routeur
- Sélection des protocoles de routage

Pour activer un protocole de routage dynamique, il suffit d'accomplir les tâches suivantes:

- Sélectionner un protocole de routage tel que RIP v2.
- Attribuer des numéros de réseau IP sans préciser de valeurs de sous-réseau.
- Attribuer des adresses de réseau ou de sous-réseau et le masque de sous-réseau approprié aux interfaces.

RIP v2 utilise des messages de diffusion multicast pour communiquer avec les autres routeurs. La métrique de routage aide les routeurs à trouver le meilleur chemin menant à chaque réseau ou sous-réseau.

```
Router(config)#router protocol [keyword]
```

• Définit un protocole de routage IP.

```
Router(config-router)#version 2
```

• Active RIP v2. Utiliser la commande **no version** pour revenir au réglage par défaut

```
Router(config-router)#network network-number
```

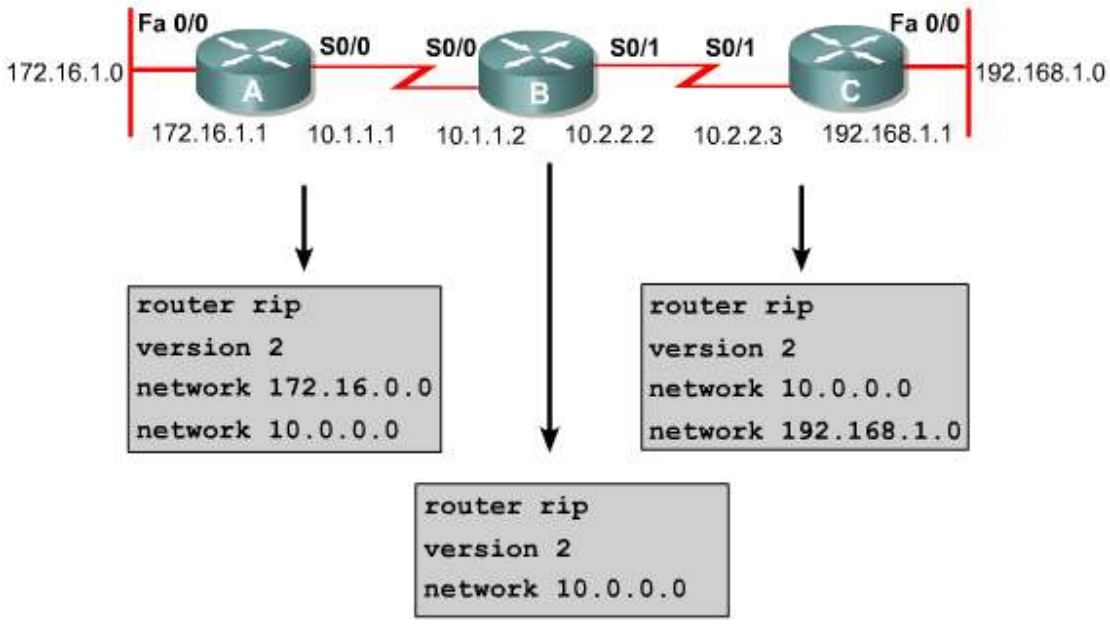
• Commande de configuration obligatoire pour chaque processus de routage IP
• Identifie le réseau physiquement connecté auquel sont transmises les mises à jour de routage.

La commande **router** lance le processus de routage. 2 La commande **network** entraîne la mise en œuvre des fonctions suivantes:

- Diffusion multicast des mises à jour de routage en sortie d'une interface.
- Traitement des mises à jour de routage en entrée de cette même interface.
- Annonce du sous-réseau directement connecté à cette interface.

La commande **network** est nécessaire, car elle permet au processus de routage de déterminer les interfaces qui participeront à l'envoi et à la réception des mises à jour du routage. Cette commande lance le protocole de routage sur toutes les interfaces que comporte le routeur sur le réseau spécifié. Elle permet aussi au routeur d'annoncer ce réseau.

La combinaison des commandes **router rip** et **version 2** désigne RIPv2 comme protocole de routage, alors que la commande **network** identifie un réseau attaché qui participe au routage. 3

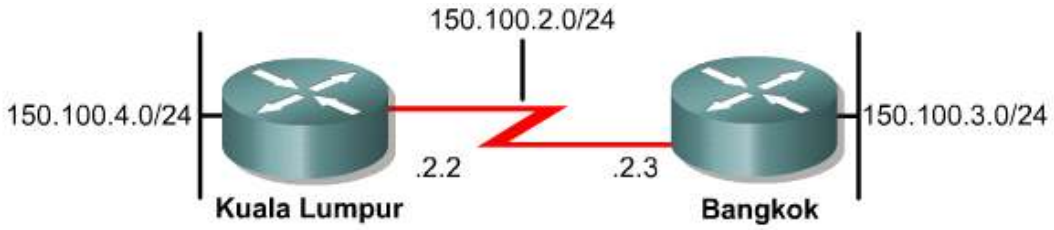


Dans cet exemple, la configuration du routeur A inclut les commandes suivantes:

- **`router rip`** – Active RIP comme le protocole de routage
- **`version 2`** – Désigne la version 2 comme la version de RIP qui doit être utilisée
- **`network 172.16.0.0`** – Spécifie un réseau directement connecté.
- **`network 10.0.0.0`** – Spécifie un réseau directement connecté.

Les interfaces du routeur A, connectées aux réseaux 172.16.0.0 et 10.0.0.0 (ou à leurs sous-réseaux), envoient et reçoivent les mises à jour du protocole RIP v2. Ces mises à jour permettent au routeur d'apprendre la topologie du réseau. Les configurations RIP des routeurs B et C sont similaires mais leurs numéros de réseau sont différents.

La figure 4 présente un autre exemple de configuration RIP v2.




```
Kuala Lumpur(config)#router rip
Kuala Lumpur(config-router)#version 2
Kuala Lumpur(config-router)#network 150.100.0.0
```

```
Bangkok(config)#router rip
Bangkok(config-router)#version 2
Bangkok(config-router)#network 150.100.0.0
```

Activité de TP

Exercice: Conversion de RIP v1 en RIP v2

Au cours de ce TP, les étudiants apprendront à configurer RIP v1 sur les routeurs puis à convertir RIP v1 en RIP v2.

Activité de TP

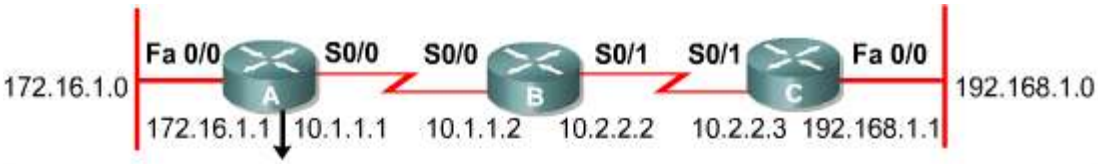
Activité en ligne: Conversion de RIP v1 à RIP v2

Au cours de ce TP, les étudiants vont configurer RIP v1, puis convertir RIP v1 en RIP v2.

1.2 RIP Version 2

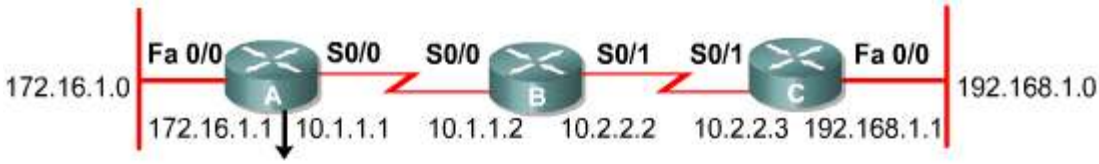
1.2.5 Vérification de RIP v2

Les commandes **`show ip protocols`** et **`show ip route`** affichent des informations sur les protocoles de routage et sur la table de routage. 1Cette section explique comment utiliser les commandes **`show`** pour vérifier la configuration RIP.




```
RouterA#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing rip
  Default version control: send version 1, receive any version
     Interface         send   Recv  Triggered  RIP  Keychain
     Ethernet           1      1 2
     Serial2            1      1 2
Routing for Networks:
     10.0.0.0
     172.16.0.0
Routing Information Sources:
     Gateway         Distance       Last Update
     (this router)   120              0:2:12:15
     10.1.1.2        120              0:1:09:01
Distance: (default is 120)
```

La commande **`show ip protocols`** affiche les valeurs des protocoles de routage et les informations relatives aux compteurs de routage associées à ce routeur. Le routeur de l'exemple est configuré avec RIP et envoie des mises à jour de la table de routage toutes les 30 secondes. Il est possible de configurer cet intervalle. Si un routeur RIP ne reçoit pas de mise à jour d'un autre routeur pendant au moins 180 secondes, le premier routeur déclare non valides les routes desservies par le routeur qui n'envoie pas de mise à jour. Dans la figure 2, le compteur de retenue est de 180 secondes. Par conséquent, la mise à jour d'une route qui, après avoir été indisponible redevient disponible, pourrait rester gelée pendant 180 secondes.




```
RouterA#show ip route
Codes:C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2, * - candidate
      default
       U - Per-user static route, 0 = CCR
       T - Traffic engineered route

Gateway of last resort is not set
   172.16.0.0/24 is subnetted, 1 subnets
C     172.16.1.0 is directly connected, Ethernet0
   10.0.0.0/24 is subnetted, 2 subnets
R     10.2.2.0 (120/1) via 10.1.1.2, 00:00:07, Serial 0/0
C     10.1.1.0 is directly connected, Serial 0/0
R   192.168.1.0/24 (120/2) via 10.1.1.2, 00:00:07, Serial 0/0
```

Si aucune mise à jour n'a eu lieu après un délai de 240 secondes, le routeur supprime les entrées correspondantes dans la table de routage. Le routeur insère des routes pour les réseaux répertoriés sous la ligne Routing for Networks. Le routeur reçoit des routes des routeurs RIP voisins, répertoriés sous la ligne Routing Information Sources. La distance par défaut de 120 correspond à la distance administrative d'une route RIP.

La commande **`show ip interface brief`** peut aussi être utilisée pour obtenir un résumé des informations relatives à une interface et à son état.

La commande **`show ip route`** affiche le contenu de la table de routage IP. 2 Cette table contient des entrées pour tous les réseaux et les sous-réseaux connus, ainsi qu'un code indiquant comment ces informations ont été apprises..

Examinez ces informations pour savoir si la table de routage contient des informations de routage. S'il manque des entrées, aucune information de routage ne sera échangée. Utilisez les commandes **`show running-config`** ou **`show ip protocols`** disponibles en mode privilégié sur le routeur pour chercher un éventuel protocole de routage mal configuré.

Activité de TP

Exercice: Vérification de la configuration RIP v2

Au cours de ce TP, les étudiants apprendront à configurer RIP v1 et v2 sur les routeurs, puis à utiliser les commandes show pour vérifier le fonctionnement de RIP v2.

1.2 RIP Version 2

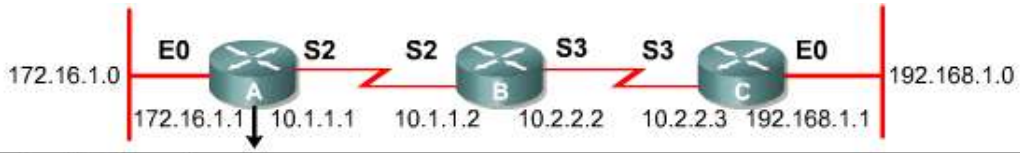
1.2.6 Dépannage de RIP v2

Cette section explique le fonctionnement de la commande **`debug ip rip`**.

Utilisez cette commande pour afficher les mises à jour de routage RIP lors de leur envoi et de leur réception. 1 Les commandes **`no debug all`** ou **`undebug all`** permettent de désactiver toutes les opérations de débogage.

Commande	Explication
`debug ip rip`	Affiche les mises à jour de routage RIP à l'envoie et à la réception.
`no debug all`	Désactive la fonction de débogage.

Dans l'exemple utilisé, le routeur dépanné a reçu des mises à jour d'un routeur situé à l'adresse source 10.1.1.2. 2 Le routeur situé à l'adresse source 10.1.1.2 a envoyé des informations concernant deux destinations dans la mise à jour de la table de routage. Le routeur en train d'être débogué envoie aussi des mises à jour, dans les deux cas à l'adresse multicast 224.0.0.9, comme adresse de destination. Le nombre entre parenthèses représente l'adresse source encapsulée dans l'en-tête IP.




```
RouterA#debug ip rip

RIP protocol debugging is on
RouterA#
00:32:56.656: RIP: received v2 update from 10.1.1.2 on Serial0/0
00:32:56.656:      10.2.2.0/24 via 0.0.0.0 in 1 hops
00:32:56.660:      192.168.1.0/24 via 0.0.0.0 in 2 hops

00:33:07.557: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0
                   (172.16.1.1)
00:33:07.557: RIP: build update entries
00:33:07.557:      10.0.0.0/8 via 0.0.0.0, metric 1, tag 0

00:33:07.557:      192.168.1.0/24 via 0.0.0.0, metric 3, tag 0

00:33:07.557: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (10.1.1.1)

00:33:07.557: RIP: build update entries

00:33:07.557:      172.16.0.0/16 via 0.0.0.0, metric 1, tag 0

00:33:25.006: RIP: received v2 update from 10.1.1.2 on Serial0/0
```

La commande **`debug ip rip`** peut également générer les messages suivants:

```
RIP: broadcasting general request on Ethernet0
RIP: broadcasting general request on Ethernet1
```

Ces messages apparaissent au démarrage ou lorsqu'un événement survient tel qu'une transition d'interface ou la réinitialisation de la table de routage par un utilisateur.

Si vous obtenez le message suivant, il est probable que l'émetteur a envoyé un paquet mal formé:

```
RIP: bad version 128 from 160.89.80.43
```

La figure 3 présente des exemples de messages obtenus à partir de la commande **`debug ip rip`** et leur signification.

Affichage	Signification possible
RIP: broadcasting general request on Ethernet0	Interface effacée manuellement par un utilisateur
RIP: bad version 128 from 160.89.80.43	Paquet incorrect de l'émetteur
RIP: received v2 update from 150.100.2.3 on Serial0	Indique que RIP Version 2 est en mode réception
RIP: sending v1 update to 255.255.255 via Serial0 (150.100.2.2)	Indique que RIP Version 1 est en service
RIP: ignored v1 packet from 150.100.2.2 (illegal version)	Indique que le routeur ne peut pas prendre en charge un paquet RIP v1
RIP: sending v2 update to 224.0.0.9 via FastEthernet0 (150.100.3.1)	Indique que RIP Version 2 est en mode envoi
RIP: build update entries 150.100.2.0/24 via 0.0.0.0 metric 1, tag	Indique l'utilisation de la route par défaut et de l'étiquetage

Exercice: Dépannage de RIP v2 avec la commande **debug**

Au cours de ce TP, les étudiants utiliseront des commandes **debug** pour vérifier le fonctionnement du protocole RIP et analyser les données transmises entre les routeurs.

Activité de TP

Activité en ligne: RIP v2 avec **debug**

Au cours de ce TP, les étudiants vont activer le routage sur le routeur, enregistrer la configuration et envoyer des requêtes **ping** aux interfaces des routeurs.

1.2 RIP Version 2

1.2.7 Routes par défaut

Par défaut, les routeurs apprennent les chemins vers les destinations données à l'aide des trois méthodes suivantes:

- **Route statique** – L'administrateur système définit manuellement une route statique en tant que prochain saut vers une destination. L'utilisation des routes statiques contribue à renforcer la sécurité et à réduire le trafic lorsqu'aucune autre route n'est connue.
- **Route par défaut** – L'administrateur système définit aussi manuellement une route par défaut en tant que chemin à suivre lorsqu'il n'existe aucune route connue menant à la destination. Les routes par défaut réduisent le nombre d'entrées des tables de routage. Lorsqu'il n'existe pas de réseau de destination dans une table de routage, le paquet est envoyé au réseau par défaut.
- **Route dynamique** – Le routeur apprend les routes menant aux destinations par la réception de mises à jour périodiques provenant des autres routeurs.

Commande	Description
`Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.19.2`	Commande complète de configuration de route statique.
`192.168.20.0`	Réseau de destination
`255.255.255.0`	Le masque de sous-réseau indique que 8 bits de découpage en sous-réseaux sont effectifs.
`192.168.19.2`	Adresse IP du routeur voisin vers la destination

Dans la figure 1, la route statique est configurée à l'aide de la commande suivante:

```
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.19.2
```

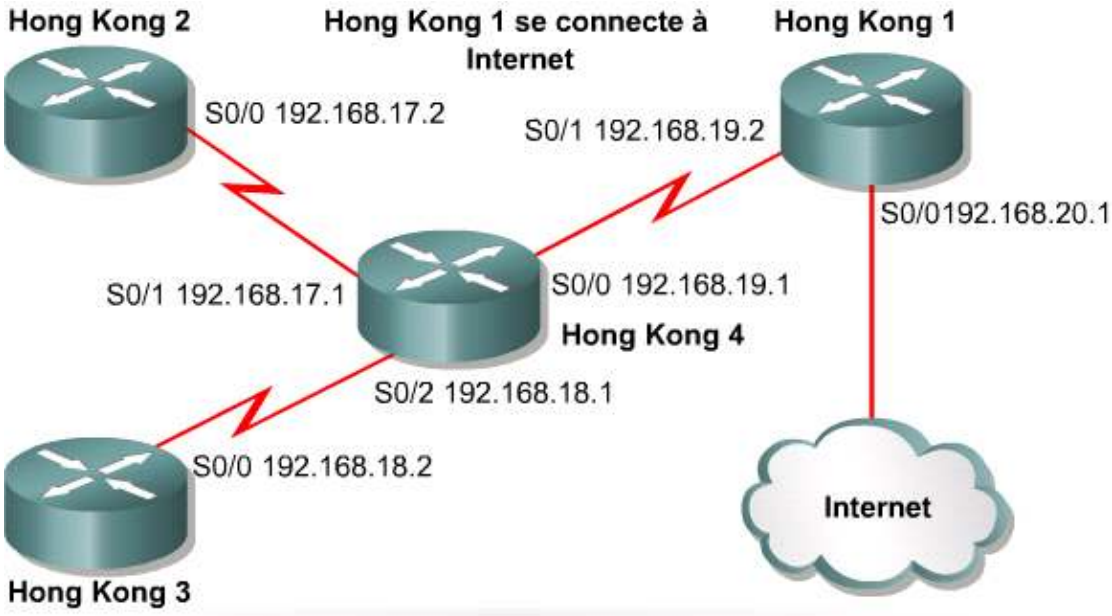
La commande **ip default-network** permet de définir une route par défaut sur les réseaux utilisant des protocoles de routage dynamique. 2

Commande	Description
`Router(config)#ip default-network 192.168.20.0`	Numéro de réseau IP défini en tant que valeur par défaut. Le numéro de réseau spécifié ici doit être sans classe puisqu'il s'agit d'une commande sans classe (classful).

```
Router(config)#ip default-network 192.168.20.0
```

En règle générale, une fois que la table de routage qui gère tous les réseaux devant être configurés a été définie, il est utile de s'assurer que les autres paquets sont dirigés vers un emplacement spécifique. Il s'agit de la route par défaut du routeur. Prenons l'exemple d'un routeur connecté à Internet. Tous les paquets qui ne sont pas définis dans la table de routage seront envoyés vers l'interface désignée du routeur par défaut.

La commande **ip default-network** est habituellement configurée sur les routeurs qui se connectent à un routeur avec une route statique par défaut.



Configuration de Hong Kong 2, Hong Kong 3 et Hong Kong 4 en utilisant ip default-network 192.168.20.0

Dans la figure 3, Hong Kong 2 et Hong Kong 3 utiliseraient Hong Kong 4 comme passerelle par défaut. Hong Kong 4 utiliserait l'interface 192.168.19.2 comme passerelle par défaut. Hong Kong 1 assurerait le routage des paquets vers Internet pour les hôtes internes. Pour autoriser Hong Kong 1 à acheminer ces paquets, il faut configurer une route par défaut à l'aide de la commande suivante:

```
HongKong1(config)#ip route 0.0.0.0 0.0.0.0 s0/0
```

Dans la commande, les zéros dans l'adresse IP et le masque représentent n'importe quelle destination associée à n'importe quel masque. Les routes par défaut sont appelées "routes à quatre zéros". Dans le diagramme, HongKong 1 ne peut accéder Internet que par l'intermédiaire de l'interface s0/0.

Résumé

La compréhension des points clés suivants devrait être acquise:

- VLSM et les raisons justifiant son utilisation
- Subdivision des réseaux en réseaux de différentes tailles avec VLSM
- Regroupement et résumé de routes, en rapport avec VLSM
- Configuration d'un routeur à l'aide de VLSM
- Fonctions clés de RIP v1 et RIP v2
- Différences notables entre RIP v1 et RIP v2
- Configuration de RIP v2
- Vérification et dépannage du fonctionnement de RIP v2
- Configuration des routes par défaut à l'aide des commandes **ip route** et **ip default-network / default-information-originate**

Résumé

- Avec VLSM, un administrateur réseau peut utiliser un masque long sur les réseaux qui ne comportent pas beaucoup d'hôtes et un masque court sur les réseaux comportant beaucoup d'hôtes.
- RIP v2 est une version améliorée de RIP v1 et partage les caractéristiques suivantes :
  - Il s'agit d'un protocole vecteur de distance qui utilise la métrique nombre de sauts.
  - Il utilise les compteurs de retenue pour empêcher les boucles de routage (valeur par défaut : 180 secondes).
  - Il utilise la règle du "split horizon" pour empêcher les boucles de routage.
  - Il utilise 16 sauts comme valeur métrique de distance infinie.

Vue d'ensemble

Les deux classes principales de protocoles IGP (interior gateway routing protocol) sont le vecteur de distance et l'état de liens. Ces deux types de protocoles de routage ont pour but de trouver des routes parmi les systèmes autonomes. Les protocoles de vecteur de distance et d'état de liens utilisent des méthodes différentes pour accomplir les mêmes tâches.

Les algorithmes de routage à état de liens, également appelés algorithmes du plus court chemin d'abord (SPF), gèrent une base de données topologiques complexe. Un algorithme de routage à état de liens gère une base de connaissances complète sur les routeurs distants et leurs interconnexions. Par contre, les algorithmes à vecteur de distance comprennent des informations non spécifiques sur les réseaux distants et ne fournissent aucune information sur les routeurs distants.

Il est essentiel de comprendre le fonctionnement des protocoles de routage à état de liens pour savoir comment activer, vérifier et dépanner leur fonctionnement. Ce module explique comment les protocoles d'état de liens fonctionnent, il décrit leurs fonctions, l'algorithme qu'ils utilisent, ainsi que les avantages et les inconvénients de ce type de routage.

Les premiers protocoles de routage comme le RIP étaient tous des protocoles de vecteur de distance. Beaucoup de protocoles importants utilisés aujourd'hui sont aussi des protocoles à vecteur de distance, dont RIP v2, IGRP et le protocole de routage hybride EIGRP. Cependant, à mesure que les réseaux ont crû en taille et en complexité, certaines des limitations des protocoles de routage à vecteur de distance se sont révélées. Les routeurs connectés à un réseau utilisant un système de vecteur de distance pouvaient seulement deviner la topologie du réseau en se basant sur les tables de routage complètes transmises par les routeurs voisins. L'utilisation de la bande passante est élevée, en raison de l'échange périodique de mises à jour de routage. De plus, la convergence du réseau ne se fait que lentement, d'où des décisions de routage médiocres.

Les protocoles de routage à état de liens sont différents des protocoles à vecteur de distance. Les protocoles de routage à états de liens diffusent des informations de routage, ce qui permet à chaque routeur d'obtenir une vue complète de la topologie réseau. Les mises à jour déclenchées permettent une utilisation efficace de la bande passante et une convergence plus rapide. Les changements de l'état d'un lien sont envoyés à tous les routeurs du réseau dès leur survenue.

L'un des protocoles à état de liens les plus importants est l'OSPF (Open Shortest Path First). Ce protocole est basé sur les normes ouvertes, ce qui signifie qu'il peut être développé et amélioré par les fournisseurs. C'est un protocole complexe dont la mise en œuvre au sein d'un grand réseau représente un vrai défi. Dans ce module, nous abordons les bases de l'OSPF.

La configuration de l'OSPF sur un routeur Cisco est similaire à celle des autres protocoles de routage. En effet, le processus de routage OSPF doit être activé et les réseaux que l'OSPF annoncera doivent être identifiés. Cependant, l'OSPF offre un certain nombre de fonctions et de procédures de configuration qui sont uniques. Ces fonctions font de l'OSPF un choix judicieux en matière de protocole de routage malgré le fait que la configuration de l'OSPF est un processus des plus complexes.

Dans les grands réseaux complexes, l'OSPF peut être configuré pour recouvrir un grand nombre de zones de types différents. La possibilité de concevoir et de mettre en œuvre de grands réseaux OSPF est due à la capacité de configurer OSPF dans une zone unique. Ce module traite également de la configuration d'une zone unique OSPF.

À la fin de ce module, les étudiants doivent être en mesure de:

- Identifier les caractéristiques clés du routage à état de liens
- Expliquer comment les informations de routage à état de liens sont mises à jour
- Décrire l'algorithme de routage à état de liens

- Examiner les avantages et les inconvénients du protocole à état de liens
- Comparer et distinguer le routage à état de liens et le routage à vecteur de distance
- Activer OSPF sur un routeur
- Configurer une adresse d'essai en mode bouclé pour définir la priorité du routeur
- Changer la préférence de route OSPF en modifiant la métrique de coût
- Configurer l'authentification OSPF
- Modifier les compteurs OSPF
- Décrire les étapes de création et de propagation d'une route par défaut
- Utiliser les commandes **show** pour vérifier le fonctionnement de l'OSPF
- Configurer le processus de routage OSPF
- Définir les termes clés de l'OSPF
- Décrire les types de réseau OSPF
- Décrire le protocole HELLO de l'OSPF
- Identifier les étapes de base du fonctionnement de l'OSPF

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
2.1	Protocole de routage à état de liens
2.2	Concepts de zone unique OSPF
2.3	Configuration d'une zone unique OSPF

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des utilisateurs • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des • Configuration d'un routeur en vue de fonctionnalités d'administration supplémentaires • Création d'une configuration initiale sur un routeur	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes • Configuration d'un routeur en vue de fonctionnalités d'administration supplémentaires	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

2.1 Protocole de routage à état de liens

2.1.1 Vue d'ensemble du routage à état de liens

Les protocoles d'état de liens fonctionnent différemment des protocoles de vecteur de distance. Il est essentiel que les administrateurs réseau comprennent ces différences. Une des différences essentielles est que les protocoles à vecteur de distance font appel à une méthode plus simple pour échanger des informations de routage. La figure 1met en évidence les caractéristiques de ces deux protocoles.

Les protocoles à états de liens gèrent une base de données complexe d'informations topologiques. Alors que l'algorithme à vecteur de distance comprend des informations non spécifiques sur les réseaux distants et ne fournit aucune information sur les routeurs distants, l'algorithme de routage à état de liens gère une base de connaissances complète sur ces routeurs distants et sur leurs interconnexions.

Protocole	Exemples	Caractéristiques
Vecteur de distance	Protocoles RIP v1 et RIP v2 Protocole IGRP (Interior Gateway Routing Protocol)	• Envoie la table de routage aux voisins • Effectue des mises à jour fréquentes • Protocoles RIP v1 et RIP v2 utilisent le nombre de sauts comme métrique • Visualise le réseau du point de vue des voisins • Converge lentement • Sensible aux boucles de routage • Facile à configurer et à administrer • Consomme une grande partie de la bande passante • Utilise les mises à jour déclenchées comme mesure de prévention des boucles de routage
État de liens	Protocole OSPF (Open Shortest Path First) Protocole IS-IS (Intermediate System-to-Intermediate System)	• Mises à jour déclenchées par des événements • Envoie des paquets à état de liens à tous les routeurs du réseau • Converge rapidement • Dispose d'une vue commune du réseau • Non sensible aux boucles de routage • Plus difficile à configurer • Nécessite plus de mémoire et de puissance de traitement qu'un protocole à vecteur de distance • Consomme moins de bande passante qu'un protocole à vecteur de distance

Activité de média interactive

Glisser-Positionner: Vue d'ensemble du routage à état de liens

À la fin de cette activité, l'étudiant sera en mesure d'identifier les différences entre les protocoles à vecteur de distance et à état de liens.

2.1 Protocole de routage à état de liens

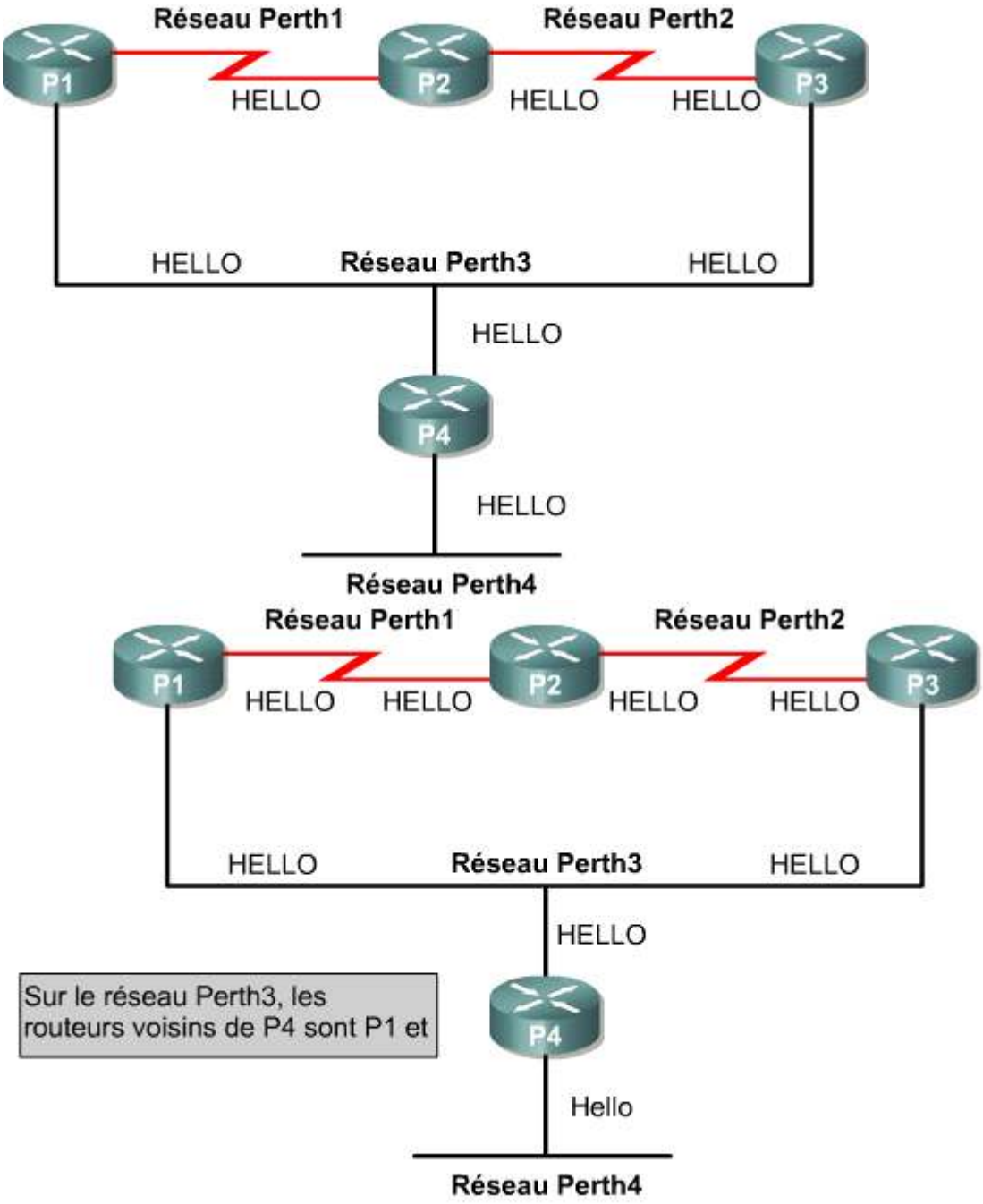
2.1.2 Fonctions du protocole de routage à état de liens

Les protocoles de routage à état de liens recueillent les informations de tous les autres routeurs du réseau ou à l'intérieur d'une zone du réseau préalablement définie. Une fois toutes les informations collectées, chaque routeur, indépendamment des autres, calcule ses meilleurs chemins vers toutes les destinations du réseau. Étant donné que chaque routeur met à jour sa propre vue du réseau, il y a moins de risque qu'il propage les informations incorrectes fournies par un de ses voisins.

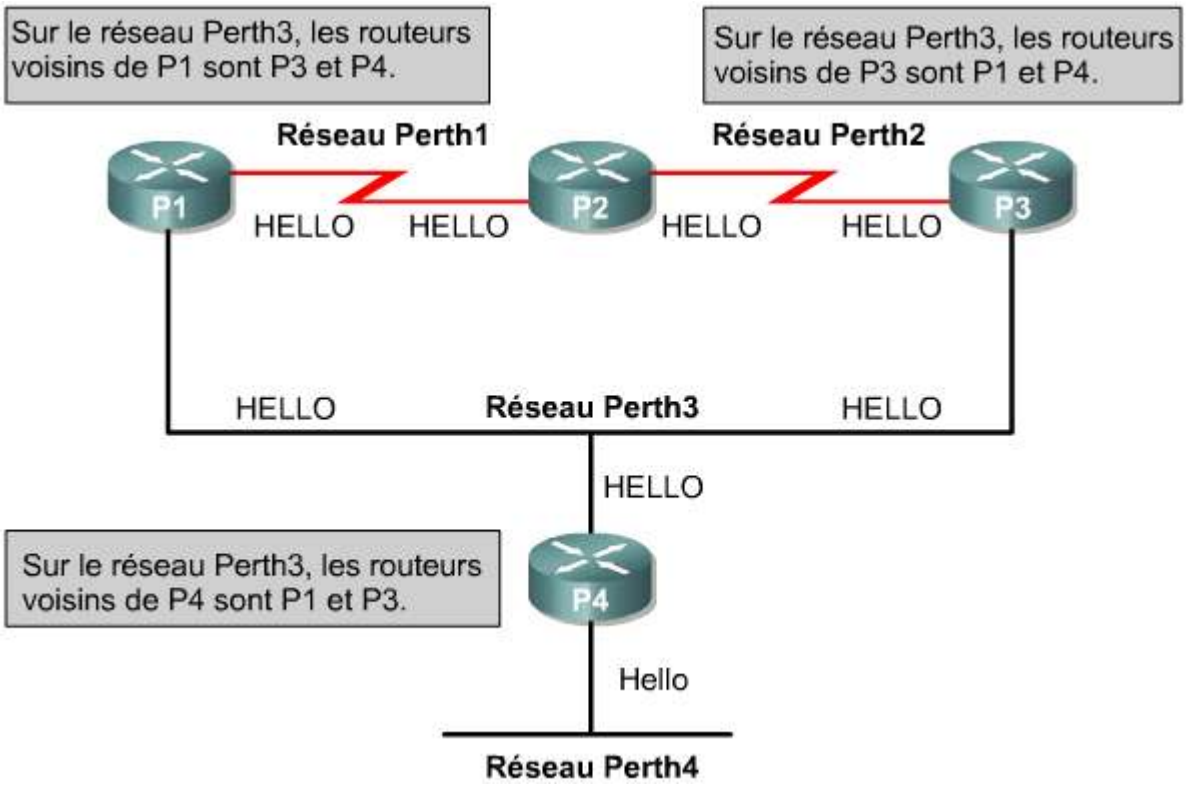
Les protocoles de routage à état de liens assurent les fonctions suivantes:

- ils réagissent rapidement aux changements qui interviennent sur le réseau
- ils envoient des mises à jour déclenchées lorsqu'un changement se produit sur le réseau,
- ils envoient des mises à jour périodiques appelées rafraîchissements d'état de liens,

- ils utilisent un mécanisme HELLO pour déterminer l'accessibilité de leurs voisins [1] [2].



Chaque routeur surveille l'état de ses voisins directement connectés par la diffusion multicast de paquets HELLO. Chaque routeur surveille aussi tous les routeurs de son réseau ou de sa zone au moyen de mises à jour de routage à état de liens (LSA). Le paquet HELLO contient des informations sur les réseaux qui sont reliés au routeur. Dans la figure [3], P4 a pris connaissance de ses voisins, P1 et P3, sur le réseau Perth3. Les LSA fournissent des mises à jour sur l'état des liens qui constituent des interfaces sur tous les routeurs du réseau.



Un routeur qui exécute un protocole d'état de liens assure les fonctions suivantes:

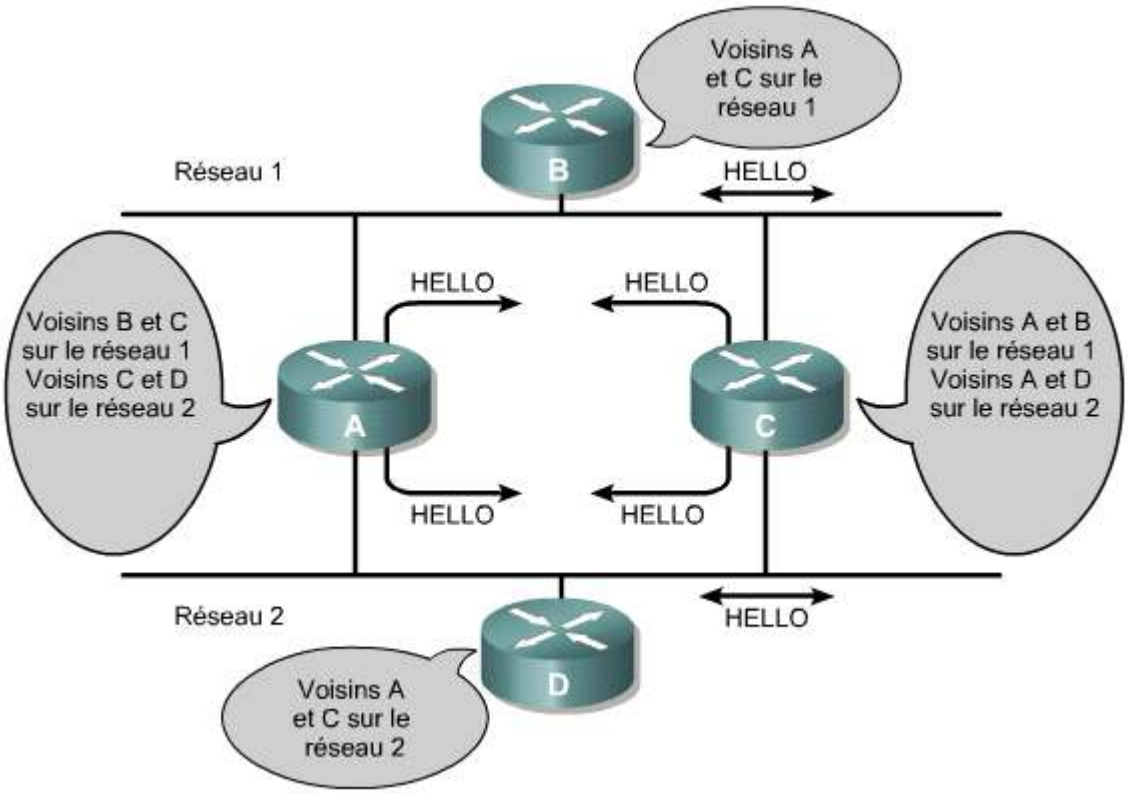
- il utilise les informations HELLO et les mises à jour de routage à état de liens qu'il reçoit des autres routeurs pour construire une base de données relative au réseau,
- il utilise l'algorithme du plus court chemin d'abord (SPF) pour calculer la route la plus courte vers chaque réseau,
- il stocke ces informations de route dans sa table de routage.

2.1 Protocole de routage à état de liens

2.1.3 Comment les informations de routage sont mises à jour

Le routage à état de liens utilise les fonctions suivantes:

- des mises à jour de routage à état de liens (LSA),
- une base de données topologiques,
- l'algorithme du plus court chemin d'abord (SPF),
- l'arbre SPF résultant,
- une table de routage des chemins et des ports vers chaque réseau afin de déterminer les meilleurs chemins pour les paquets 1.



Les protocoles de routage à état de liens ont été conçus pour surmonter les limitations des protocoles de routage à vecteur de distance. Par exemple, les protocoles à vecteur de distance échangent uniquement des mises à jour de routage avec des voisins immédiats tandis que les protocoles à état de liens échangent des informations de routage sur une zone plus étendue.

Quand une défaillance survient dans un réseau, comme un voisin qui devient inaccessible, les protocoles à état de liens inondent le réseau de LSA, envoyés partout en utilisant une adresse multicast spécifique. Le processus d'inondation consiste à diffuser une information sur tous les ports, sauf celui par lequel cette information a été reçue. Chaque routeur à état de liens capture un copie de la LSA et met à jour son état de liens ou sa base de données topologique. Le routeur à état de liens transmet ensuite la LSA à tous les équipements voisins. Les LSA entraînent le recalcul des routes par chaque routeur de la zone. Du fait que les LSA doivent être diffusées sur l'ensemble d'une zone, et que tous les routeurs au sein de cette zone doivent recalculer leurs tables de routage, le nombre de routeurs à état de liens pouvant se trouver dans la zone devrait être limité.

Un lien joue le même rôle qu'une interface sur un routeur. L'état d'un lien correspond à la description d'une interface et de la relation avec les routeurs voisins. Par exemple, une description de l'interface pourrait inclure l'adresse IP de l'interface, le masque de sous-réseau, le type de réseau auquel elle est connectée, les routeurs connectés à ce réseau, etc. L'ensemble des états de liens forme une base de données d'état de liens, parfois appelée base de données topologiques. La base de données d'état de liens permet de calculer les meilleurs chemins au sein du réseau. Les routeurs à état de liens trouvent les meilleurs chemins vers les destinations. Ils appliquent pour cela l'algorithme du plus court chemin d'abord (SPF) de Dijkstra sur la base de données d'état de liens pour construire l'arbre du plus court chemin d'abord, ayant pour racine le routeur local. Les meilleurs chemins sont ensuite sélectionnés dans l'arbre SPF et insérés dans la table de routage.

2.1 Protocole de routage à état de liens

2.1.4 Algorithmes du routage à état de liens

Les algorithmes de routage à état de liens actualisent une base de données complexe sur la topologie du réseau en échangeant des mises à jour de routage à état de liens avec les autres routeurs du réseau. Cette section décrit l'algorithme de routage à état de liens.

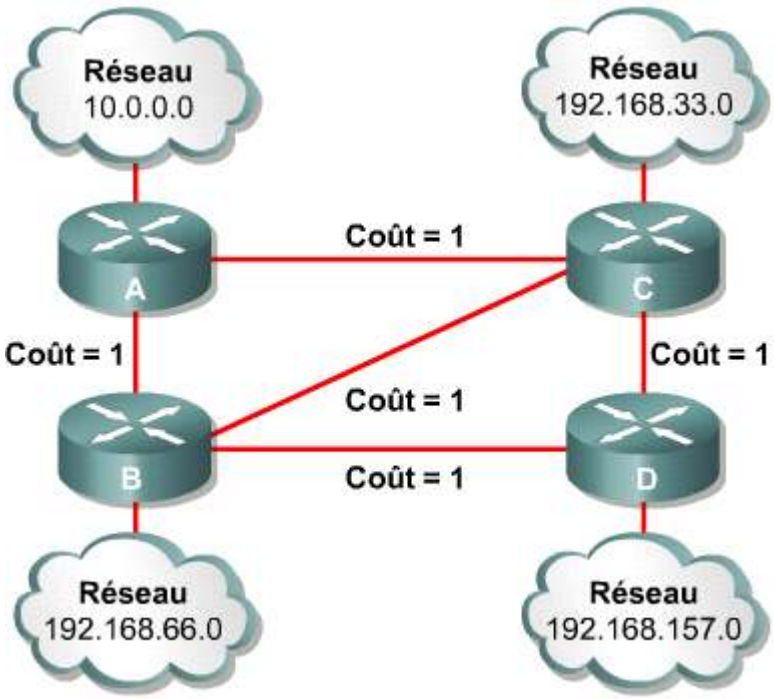
Ces algorithmes ont les caractéristiques suivantes:

- ils sont désignés collectivement comme protocoles du plus court chemin d'abord (SPF),
- ils actualisent une base de données complexe sur la topologie du réseau,
- ils sont basés sur l'algorithme de Dijkstra.

Contrairement aux protocoles à vecteur de distance, ils développent et actualisent une connaissance complète des routeurs du réseau ainsi que de leur mode d'interconnexion. Cela est possible grâce à l'échange de mises à jour de routage à état de liens (LSA) avec les autres routeurs du réseau.

Chaque routeur qui échange des LSA construit une base de données topologiques à l'aide de toutes les LSA reçues. Un algorithme SPF est ensuite utilisé pour calculer l'accessibilité des destinations en réseau. Ces informations sont utilisées pour mettre à jour la table de routage. Ce processus a la capacité de découvrir les modifications de la topologie réseau provoquées par la panne d'un composant ou par la croissance du réseau.

L'échange de LSA est déclenché par un événement sur le réseau plutôt que par des mises à jour périodiques. Cela peut accélérer considérablement le processus de convergence car il n'a pas besoin d'attendre l'expiration d'une série de compteurs pour que les routeurs en réseau puissent commencer de converger.



c

Si le réseau illustré à la Figure 1 utilise un protocole de routage à état de liens, il n'y a pas de souci quant à la connectivité entre les routeurs A et D. En fonction du protocole réellement employé et des métriques sélectionnées, il est hautement probable que le protocole de routage pourra faire la distinction entre les deux chemins vers la même destination et tentera d'utiliser le meilleur. Dans la Figure 2, il y a deux entrées de route dans la table pour la route du routeur A au routeur D. Dans cet exemple, le protocole à état de liens enregistre les deux routes, parce qu'elles ont un coût identique. Certains protocoles à état de liens donnent la possibilité d'évaluer le potentiel de performance de deux routes et de choisir la meilleure. Si la route passant par le Routeur C était le chemin préféré et rencontrait des difficultés opérationnelles, telles qu'une congestion ou la panne d'un composant, le protocole d'état de liens détecterait ce changement et commencerait d'acheminer les paquets par le Routeur B.

Routeur	Destination	Saut suivant	Coût
A	192.168.66.0	B	1
A	192.168.33.0	C	1
A	192.168.157.0	B	2
A	192.168.157.0	C	2
B	10.0.0.0	A	1
B	192.168.33.0	C	1
B	192.168.157.0	D	1
C	10.0.0.0	A	1
C	192.168.66.0	B	1
C	192.168.157.0	D	1
D	10.0.0.0	B	2
D	10.0.0.0	C	2
D	192.168.66.0	B	1
D	192.168.33.0	C	1

2.1 Protocole de routage à état de liens

2.1.5 Avantages et inconvénients du protocole à état de liens

La liste suivante présente les nombreux avantages des protocoles de routage à état de liens par rapport aux algorithmes à vecteur de distance traditionnels, tels que RIP v1 (Routing Information Protocol) ou IGRP (Interior Gateway Routing Protocol): 1

- Les protocoles d'état de liens utilisent des métriques de coût pour choisir des chemins à l'intérieur du réseau. La métrique de coût reflète la capacité des liens sur ces chemins.
- Les protocoles à état de liens utilisent des mises à jour déclenchées et diffusées et peuvent signaler immédiatement les changements de la topologie réseau à tous les routeurs du réseau. Cette indication immédiate entraîne généralement des délais de convergence plus brefs.
- Chaque routeur dispose d'une image complète et synchronisée du réseau. Cela rend très difficile l'apparition des boucles de routage.
- Les routeurs se basent toujours sur le dernier ensemble d'informations pour rendre leurs décisions de routage, parce que les LSA sont numérotées et datées.
- La taille des base de données d'état de liens peut être réduite par le biais d'une conception soignée du réseau. Cela conduit à des calculs Dijkstra simplifiés et à une convergence plus rapide.
- Chaque routeur est capable de mapper une copie de l'architecture tout entière, au moins de sa propre zone du réseau. Cet attribut peut être extrêmement utile pour le dépannage.
- Le routage CIDR (Classless interdomain routing) et la technique VLSM (variable-length subnet masking) sont pris en charge.

Voici quelques inconvénients des protocoles de routage à état de liens: 1

- Ils requièrent davantage de mémoire et de puissance de traitement que les routeurs à vecteur de distance, ce qui peut rendre le routage à état de liens inabordable pour les organisations ne disposant que de budgets réduits et de matériels hérités.
- Ils nécessitent une conception de réseau hiérarchique stricte, où un réseau peut être décomposé en zones plus petites pour réduire la taille des tables topologiques.
- Ils requièrent un administrateur possédant une bonne compréhension du routage à état de liens.
- Ils diffusent des mises à jour de routage à état de liens sur le réseau durant le processus initial de découverte, ce qui peut réduire considérablement la capacité du réseau à transporter des données. Ce processus de diffusion peut dégrader de façon non négligeable les performances du réseau en fonction de la bande passante disponible et du nombre de routeurs qui échangent des informations.

Avantages	Inconvénients
• Convergence rapide: modifications signalées immédiatement par les sources affectées • Robustesse face aux boucles de routage • Les routeurs connaissent la topologie • Les paquets à état de liens sont séquencés et horodatés • La taille des bases de données d'état de liens peut être réduite avec une conception réseau soignée	• Demandes significatives sur la mémoire et la puissance de traitement • Nécessite une conception de réseau rigoureuse • Nécessite un administrateur réseau ayant des compétences en routage à état de liens • Le flux initial peut ralentir les performances

2.1 Protocole de routage à état de liens

2.1.6 Comparer et distinguer le routage à vecteur de distance et le routage à état de liens

Tous les protocoles à vecteur de distance prennent connaissance des routes puis envoient ces routes aux voisins directement connectés. Cependant, les routeurs à état de liens annoncent les états de leurs liens à tous les autres routeurs de la zone pour que chaque routeur puisse construire une base de données d'état de liens complète. Ces annonces sont appelées mises à jour de routage à état de liens (LSA). Contrairement aux routeurs à vecteur de distance, les routeurs à état de liens peuvent former des relations spéciales avec leurs voisins et avec les autres routeurs à état de liens. Cela permet de s'assurer que les informations des LSA sont échangées de façon appropriée et efficace.

La diffusion initiale des LSA fournit aux routeurs les informations dont ils ont besoin pour construire une base de données d'état de liens. Les mises à jour de routage ne se produisent que lors des changements sur le réseau. En l'absence de changement, les mises à jour du routage ont lieu après un intervalle spécifique. Si un changement se produit sur le réseau, une mise à jour partielle est immédiatement envoyée. Cette dernière contient uniquement des informations sur les liens qui ont changé, et non pas une table de routage complète. Tout administrateur soucieux de l'utilisation des liens WAN trouvera dans ces mises à jour partielles et sporadiques une alternative efficace au routage à vecteur de distance, qui envoie une table de routage complète toutes les trente secondes. Lorsqu'un changement a lieu, les routeurs à état de liens en sont simultanément notifiés par la mise à jour partielle. Les routeurs à vecteur de distance attendent que leurs voisins prennent acte du changement, mettent en œuvre le changement, puis le transmettent à leur tour à leurs voisins. 1

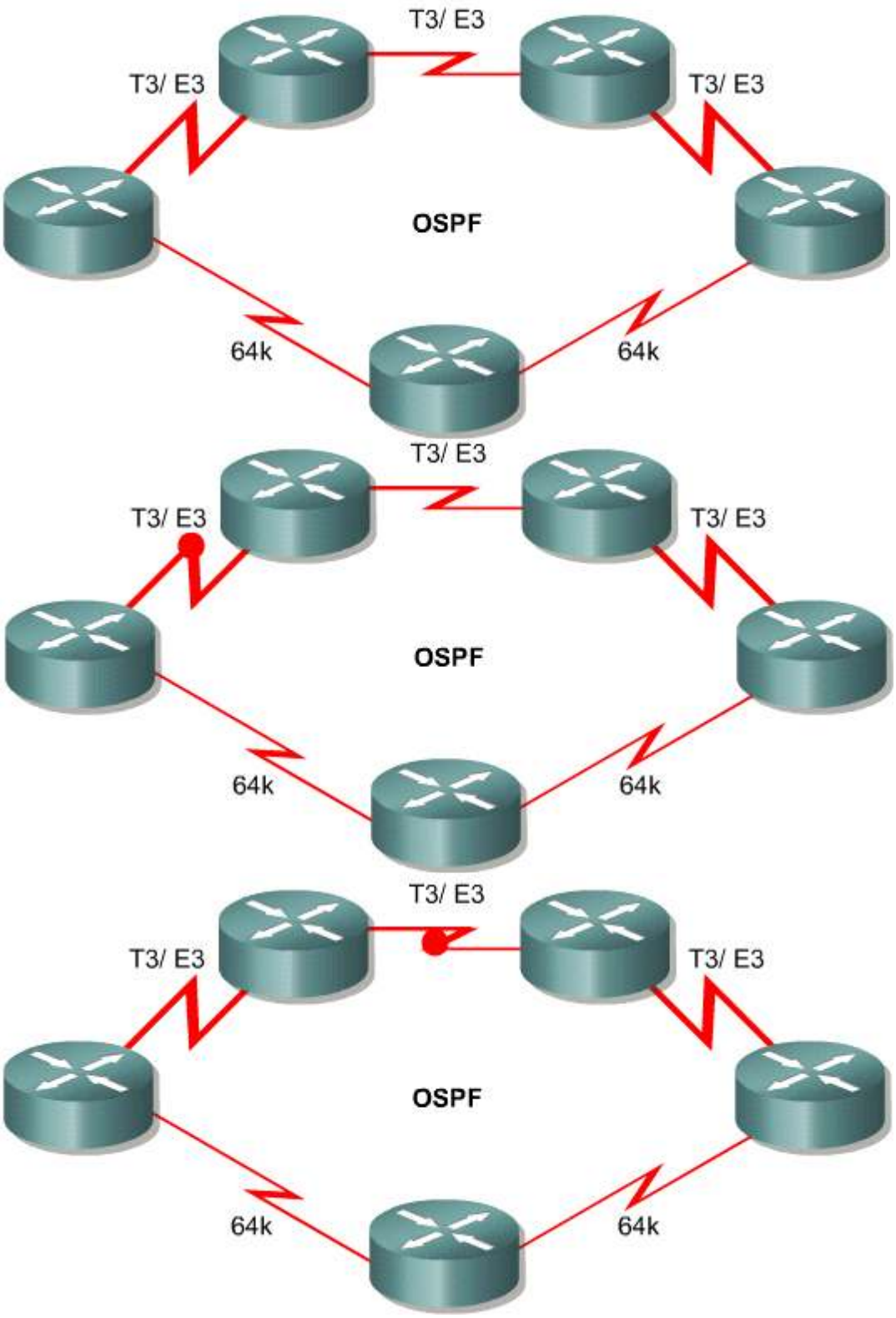
Vecteur de distance	État de lien
• Visualise la topologie du réseau du point de vue de leurs voisins • Ajoute des vecteurs de distance d'un routeur à l'autre • Mises à jour périodiques fréquentes et convergence lente • Passe des copies des tables de routage aux routeurs voisins	• Dispose d'une vue commune de la topologie • Calcule le plus court chemin vers les autres routeurs • Mises à jour déclenchées par événement et convergence plus rapide • Passe les mises à jour du routage à état de liens aux autres routeurs

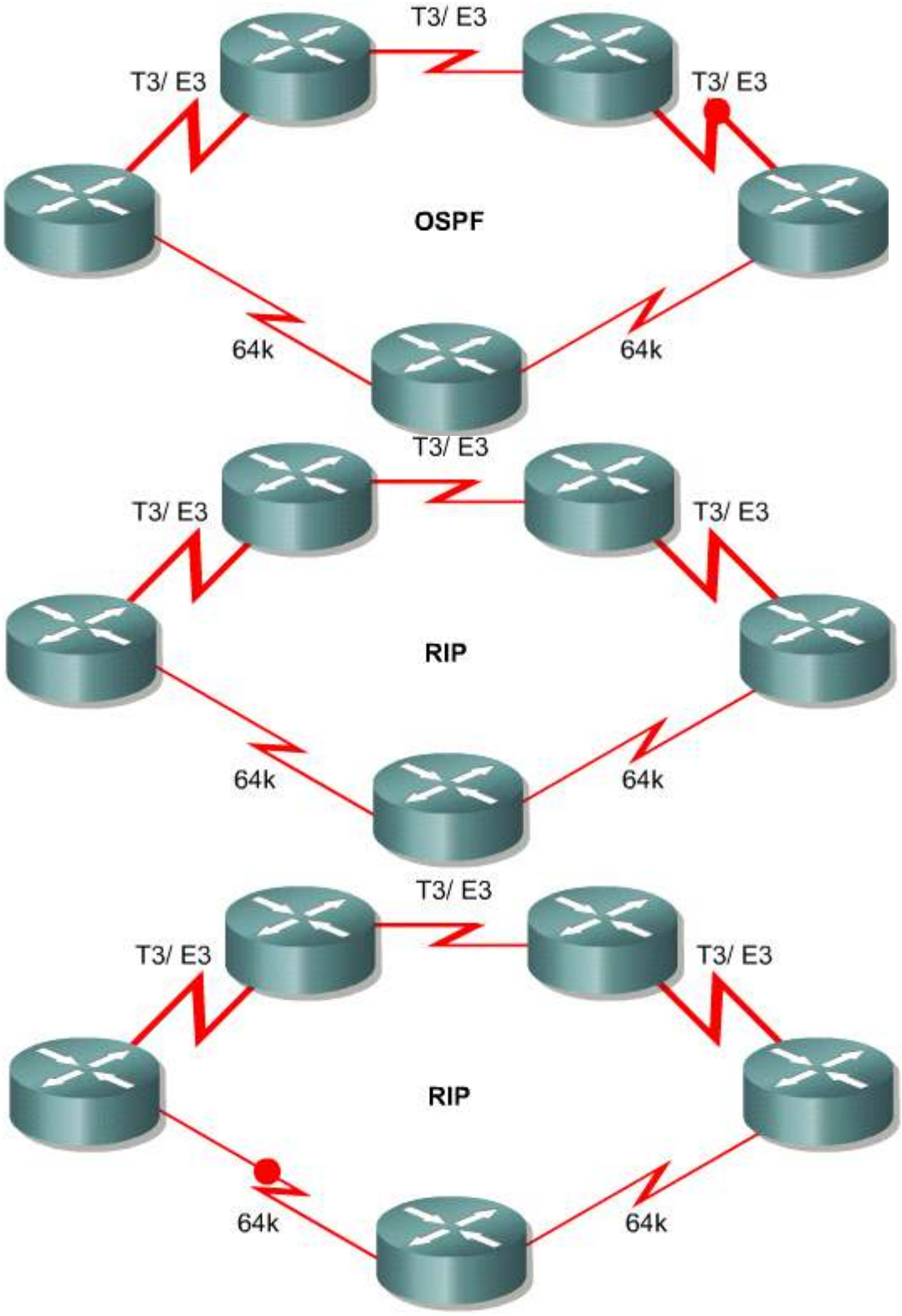
Les protocoles à état de liens offrent une convergence plus rapide et une meilleure utilisation de la bande passante. Ils prennent en charge le routage CIDR (classless interdomain routing) et la technique VLSM (variable-length subnet mask). Ils sont ainsi adaptés pour les réseaux complexes et évolutifs. En fait, les protocoles à état de liens offrent généralement des performances supérieures à celles des protocoles à vecteur de distance, et ceci quelle que soit la taille du réseau. Les protocoles à état de liens ne sont pas mis en œuvre sur tous les réseaux, car ils nécessitent plus de mémoire et de puissance de traitement que les protocoles à vecteur de distance et peuvent dépasser les capacités des équipements lents. Leur relative complexité constitue également un frein à leur adoption généralisée. Seuls des administrateurs suffisamment formés peuvent les configurer et les gérer correctement.

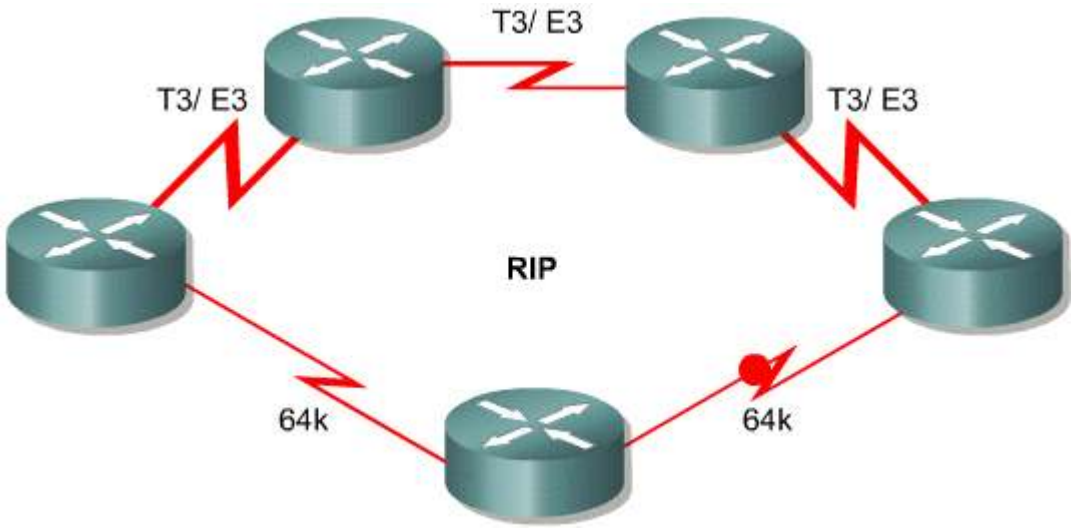
2.2 Concepts de zone unique OSPF

2.2.1 Vue d'ensemble de l'OSPF

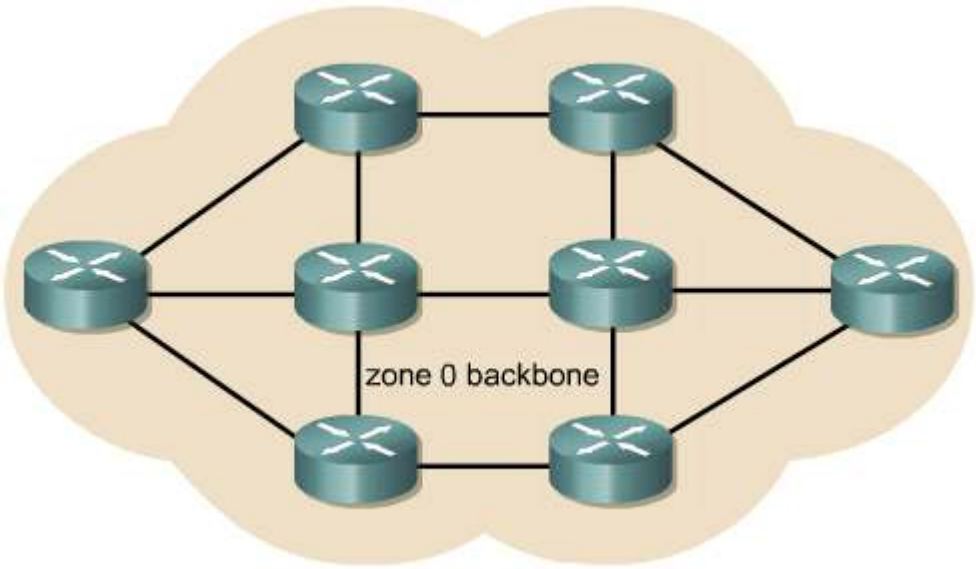
Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens basé sur des normes ouvertes. Il est spécifié dans différentes normes du groupe IETF (Internet Engineering Task Force). Le terme «Open» de OSPF signifie qu'il s'agit d'une norme ouverte au public et non-propriétaire.


T3/ E3
T3/ E3
T3/ E3
OSPF
64k
64k
T3/ E3
T3/ E3
T3/ E3
OSPF
64k
64k
T3/ E3
T3/ E3
T3/ E3
OSPF
64k
64k

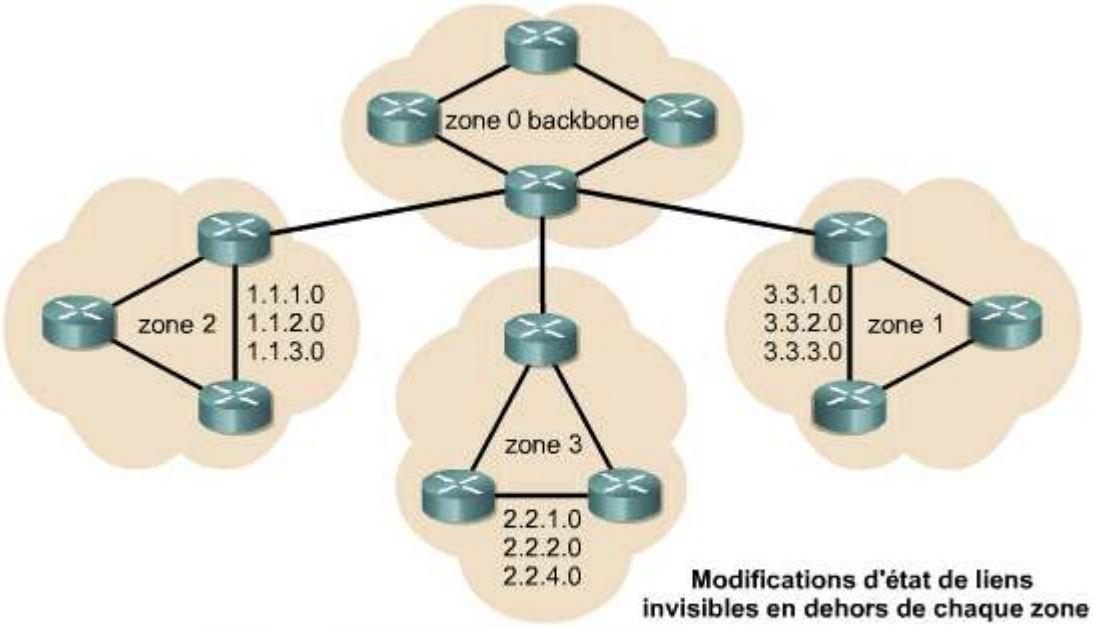

T3/ E3
T3/ E3
T3/ E3
OSPF
64k
64k
T3/ E3
T3/ E3
T3/ E3
RIP
64k
64k
T3/ E3
T3/ E3
T3/ E3
RIP
64k
64k



L'OSPF est en train de s'imposer comme protocole IGP de prédilection par rapport à RIP v1 et RIP v2, car il est évolutif. Le RIP est limité à 15 sauts ; il converge lentement et il choisit parfois des routes lentes parce qu'il fait l'impasse sur des facteurs critiques, tels que la bande passante, dans la détermination de la route. Un désavantage d'OSPF est qu'il ne supporte que la pile de protocoles TCP/IP. [1] [2] L'OSPF surmonte ces limitations et s'avère un protocole de routage robuste et évolutif adapté aux réseaux d'aujourd'hui. L'OSPF peut être utilisé et configuré en tant que zone unique pour les petits réseaux. [3]



Il peut également être utilisé pour les grands réseaux. Le routage OSPF peut évoluer vers les grands réseaux si les principes de conception de réseau hiérarchique sont appliqués. [4]



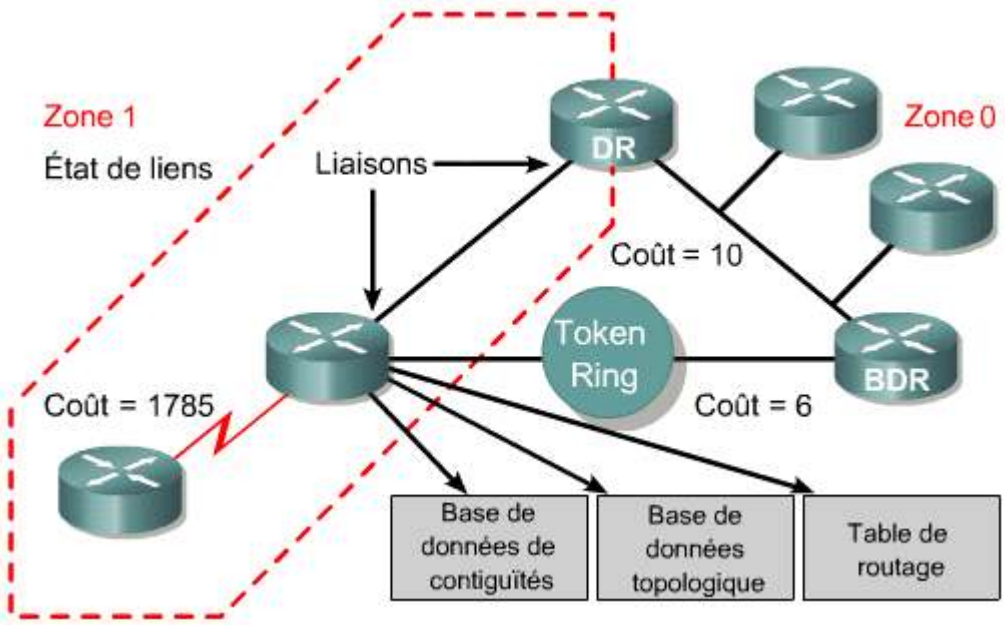
Les grands réseaux OSPF sont hiérarchiques et divisés en plusieurs zones.

Les grands réseaux OSPF utilisent une conception hiérarchique. Plusieurs zones se connectent à une zone de distribution, la zone 0, également appelée backbone. Cette approche de conception permet d'exercer un contrôle étendu sur les mises à jour de routage. La définition de zones réduit la charge de routage, accélère la convergence, isole l'instabilité du réseau à zone unique et améliore les performances.

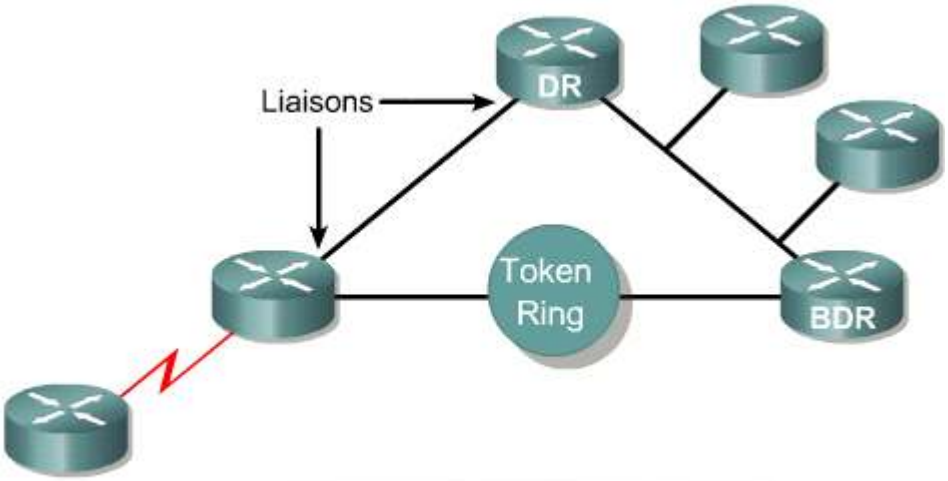
2.2 Concepts de zone unique OSPF

2.2.2 Terminologie OSPF

L'OSPF fonctionne différemment des protocoles de routage à vecteur de distance. Les routeurs à état de liens identifient les routeurs voisins puis communiquent avec les voisins identifiés. L'OSPF a sa terminologie propre. Les nouveaux termes sont présentés à la figure 1.

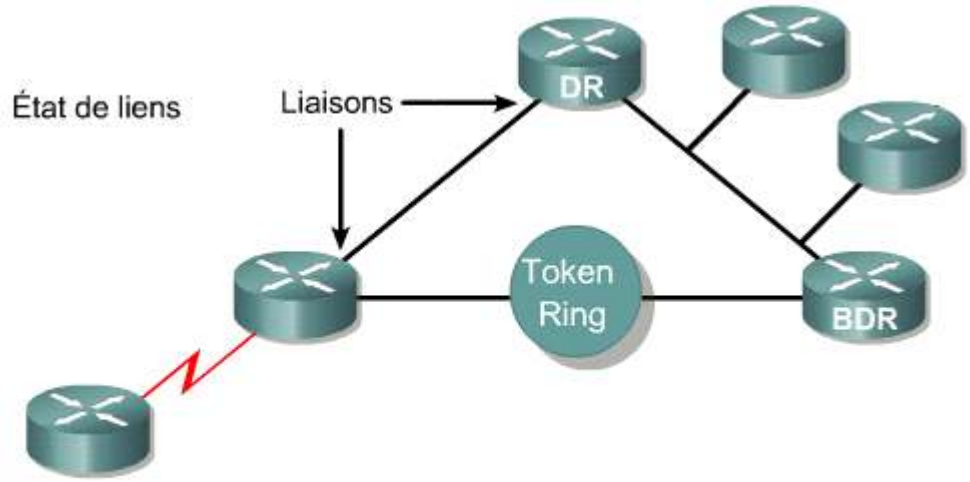


Des informations sur l'état ou les liens de chaque routeur OSPF sont recueillies auprès des voisins OSPF. 2



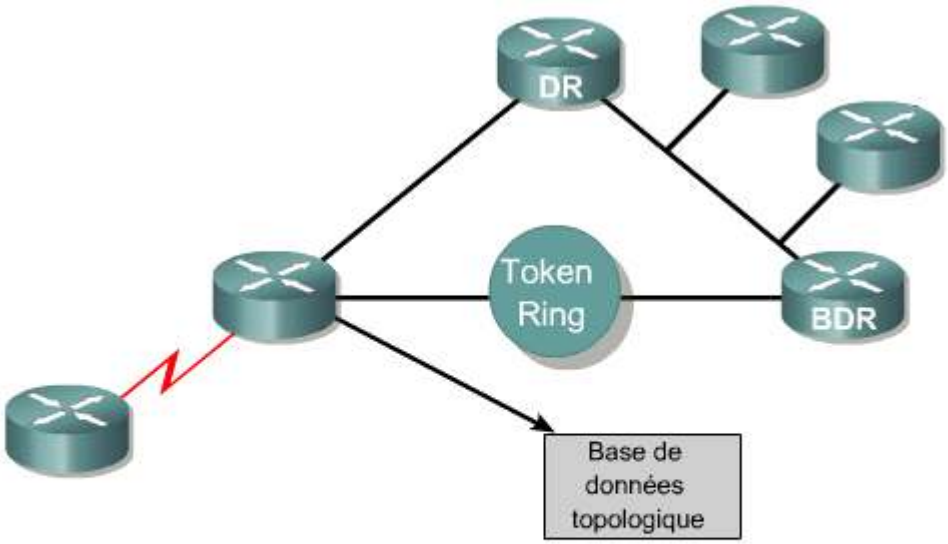
Liaison : interface sur un routeur.

Ces informations sont diffusées à tous ses voisins. Le terme diffusion désigne le processus d'envoi d'informations par tous les ports, à l'exception du port qui a servi à les recevoir. Un routeur OSPF annonce ses propres états de liens et transmet ceux qu'il reçoit. 3



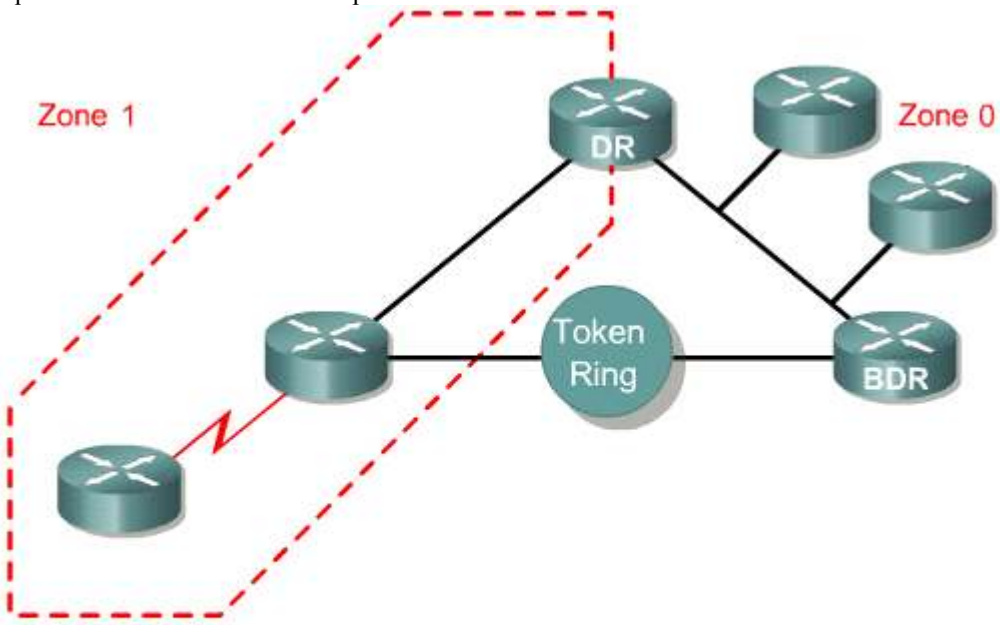
État de lien : état d'une liaison entre deux routeurs. Désigne également une interface de routeur et sa relation avec les routeurs

Les routeurs traitent les informations sur les états de liens et construisent une base de données d'état de liens. 4



Base de données d'état de liens (ou base de données topologique) : liste d'informations relatives aux autres routeurs de l'interréseau. Indique la topologie de l'interréseau.

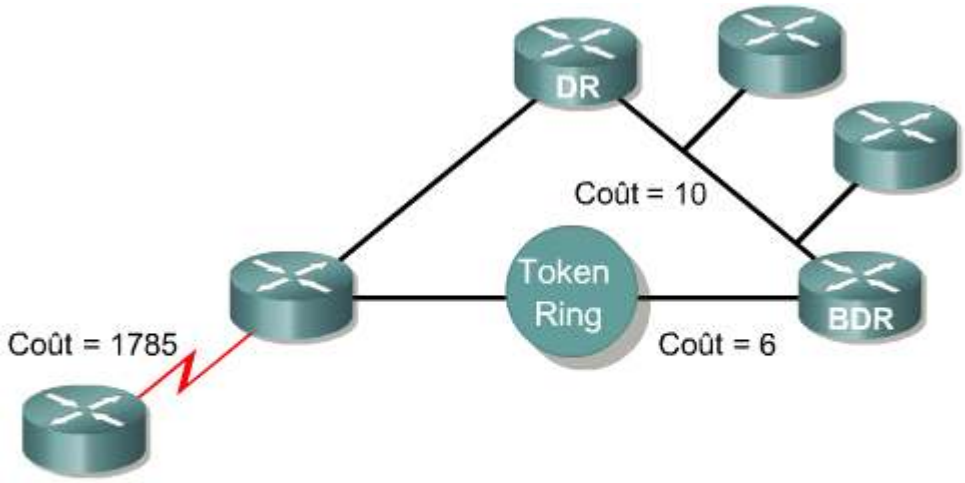
Chaque routeur de la zone OSPF dispose de la même base de données de liens. 5



Zone : ensemble des réseaux et des routeurs ayant la même identification de zone. Chaque routeur d'une zone a les mêmes informations d'état de liens. Un routeur dans une zone est appelé routeur interne.

Chaque routeur dispose des mêmes informations sur l'état des liens et sur les voisins de chaque autre routeur.

Chaque routeur exécute ensuite l'algorithme SPF sur sa propre copie de la base de données. Ce calcul détermine le meilleur chemin vers une destination. L'algorithme SPF cumule le coût, qui est la valeur habituellement basée sur la bande passante. 6



Coût : valeur affectée à une liaison. Plutôt que d'utiliser le nombre de sauts, les protocoles à état de liens affectent un coût à une liaison, qui est basé sur sa bande passante (vitesse de transmission).

Le chemin de moindre coût est ajouté à la table de routage, également appelée base de données d'acheminement.

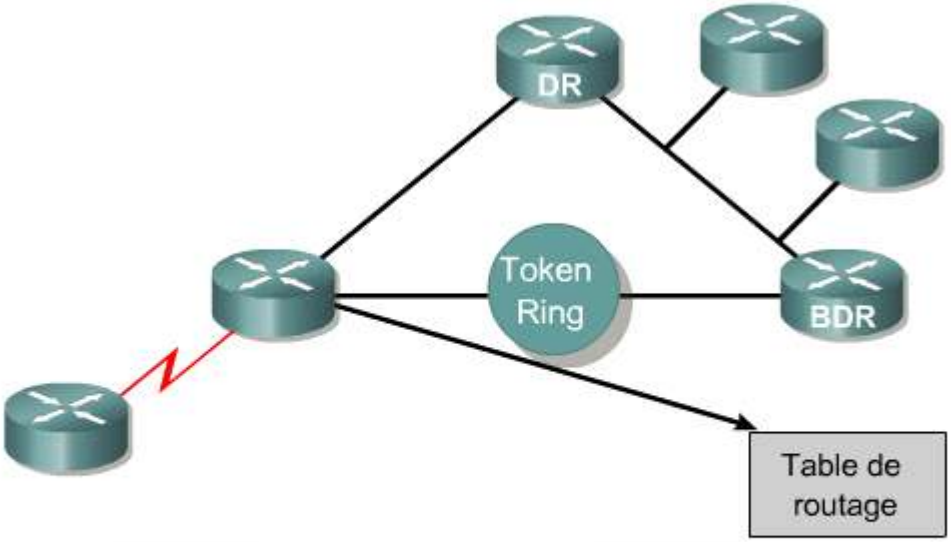
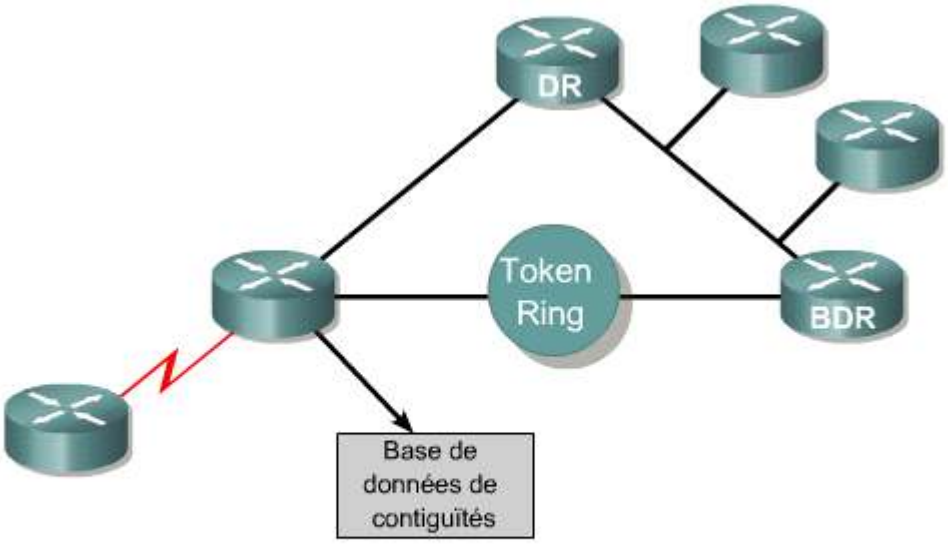


Table de routage : parfois appelée base de données de transmission, elle est générée lors de l'exécution d'un algorithme sur la base de données d'état de liens. La table de routage de chaque routeur est unique.

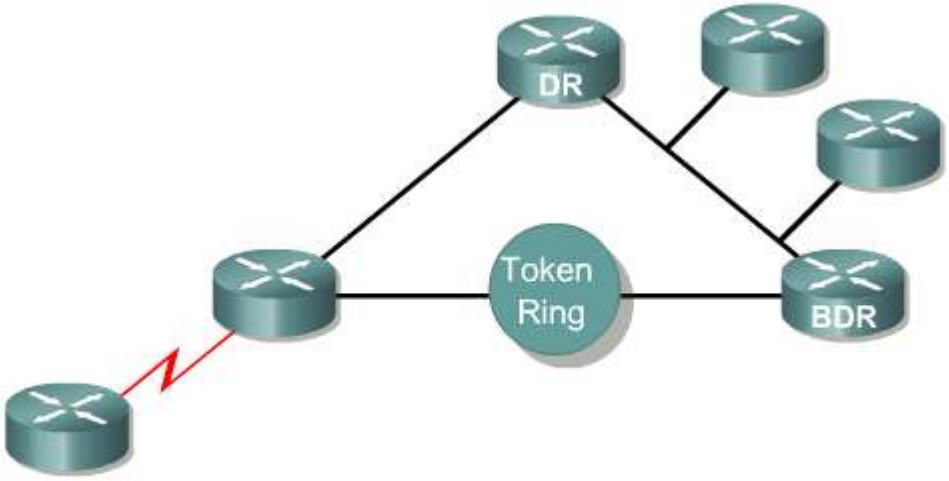
Chaque routeur conserve une liste de voisins adjacents, appelée base de données d'adjacence. La base de données d'adjacence est une liste de tous les routeurs voisins avec lesquels le routeur a établi des communications bidirectionnelles. Cette liste est

propre à chaque routeur.



Base de données de contiguïtés : Une liste de tous les routeurs voisins avec lesquels le routeur a établi des communications bidirectionnelles. Cette liste est propre à chaque routeur.

Afin de réduire le nombre d'échanges d'informations de routage entre plusieurs voisins sur le même réseau, les routeurs OSPF choisissent un routeur désigné (DR) et un routeur désigné de secours (BDR) qui servent de points focaux pour l'échange des informations de routage.



Routeur désigné (DR) et routeur désigné de secours (BDR) : routeur choisi par tous les autres routeurs du même réseau LAN pour les représenter tous. Outre les réseaux point à point, chaque réseau dispose d'un DR et d'un BDR.

Activité de média interactive

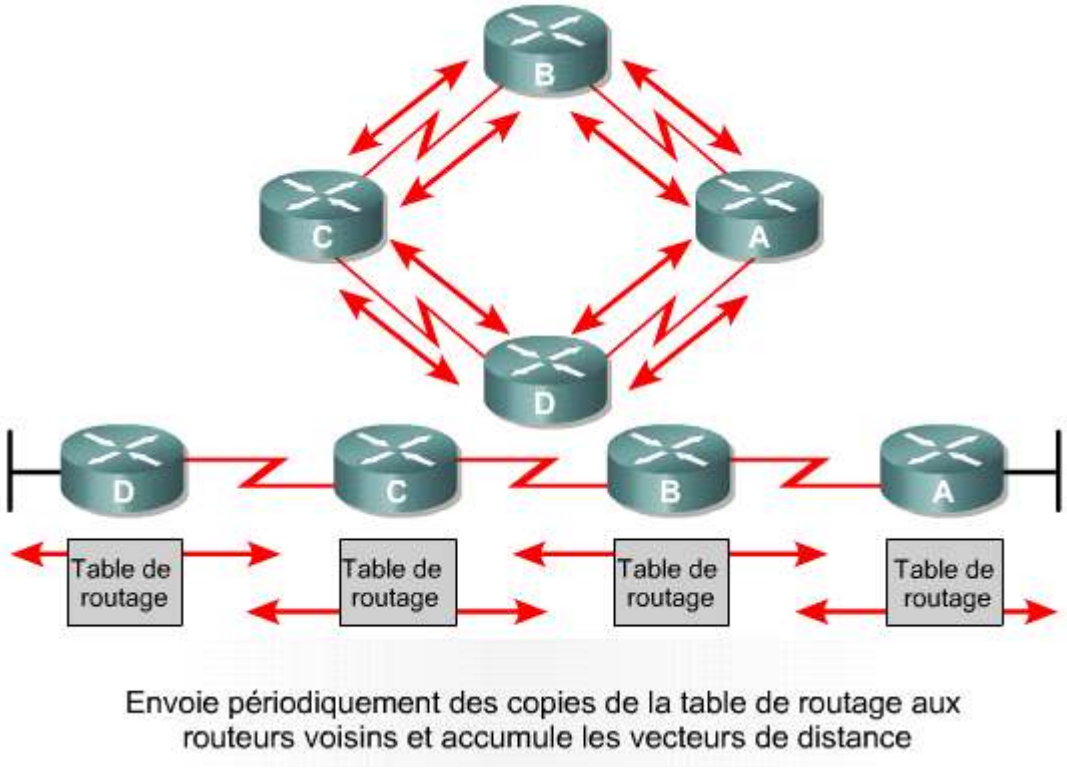
Mots croisés: Terminologie OSPF

À la fin de cette activité, l'étudiant sera en mesure de comprendre les différents termes de l'OSPF.

2.2 Concepts de zone unique OSPF

2.2.3 Comparaison de l'OSPF avec les protocoles de routage à vecteur de distance

L'OSPF utilise la technologie d'état de liens plutôt que la technologie de vecteur de distance (RIP). Les routeurs à état de liens actualisent une image commune du réseau et échangent des informations de lien lors de la découverte initiale des changements survenus sur le réseau. Les routeurs à état de liens ne diffusent pas régulièrement leurs tables de routage comme le font les protocoles à vecteur de distance. 1Ils utilisent ainsi moins de bande passante pour la gestion des tables de routage.

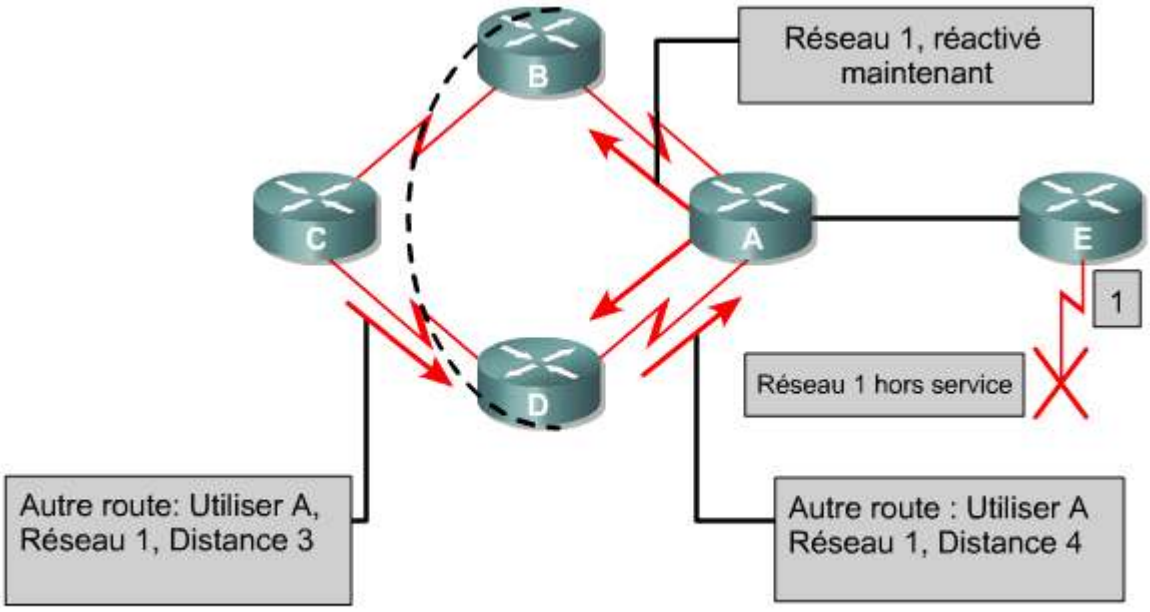


Le RIP est approprié pour les petits réseaux, et le meilleur chemin est basé sur le nombre de sauts le plus bas. L'OSPF est approprié pour les besoins des grands interréseaux évolutifs, et le meilleur chemin est déterminé par la vitesse. Le RIP et les autres protocoles à vecteur de distance utilisent des algorithmes simples pour calculer les meilleurs chemins. L'algorithme SPF est complexe. Les routeurs qui implémentent le routage à vecteur de distance peuvent nécessiter moins de mémoire et des processeurs moins rapides que ceux qui exécutent l'OSPF.

L'OSPF sélectionne les routes en fonction du coût, qui est lié à la vitesse. Plus la vitesse est élevée, et plus le coût OSPF du lien est faible.

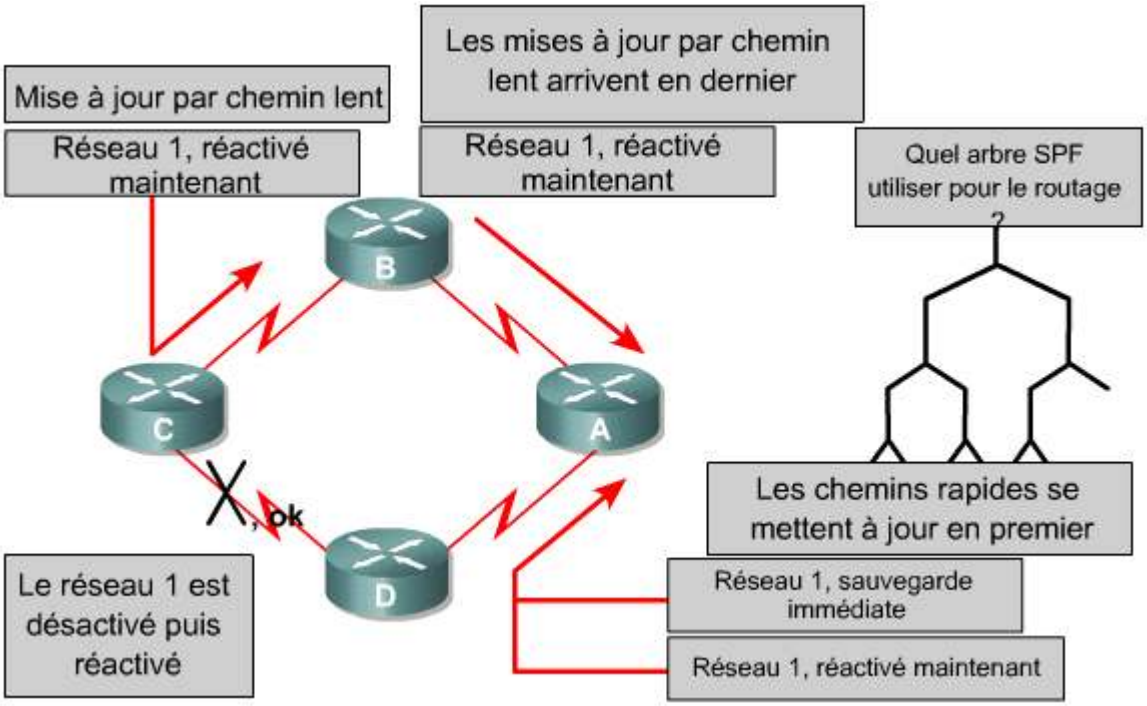
L'OSPF sélectionne le chemin exempt de boucles le plus rapide dans l'arbre du chemin le plus court d'abord comme meilleur chemin du réseau.

L'OSPF garantit un routage exempt de boucles. Les protocoles à vecteur de distance peuvent générer des boucles de routage. 2



Autres routes, convergence lente, routage incohérent

Si des liens sont instables, la diffusion des informations sur l'état des liens peut désynchroniser les annonces d'état de liens et rendre les décisions incohérentes. 3



L'OSPF résout les problèmes suivants:

- vitesse de convergence,
- prise en charge de masque de sous-réseau de longueur variable (VLSM)
- taille du réseau,
- sélection du chemin,
- regroupement des membres.

Dans les grands réseaux, la convergence RIP peut prendre plusieurs minutes puisque la table de routage de chaque routeur est copiée et partagée avec des routeurs directement connectés. Après la convergence OSPF initiale, le maintien d'un état convergé est plus rapide car seules les modifications au sein du réseau sont diffusées aux autres routeurs d'une zone.

L'OSPF prend en charge les VLSM et est donc appelé protocole sans classe. Le RIP v1 ne prend pas en charge les VLSM, contrairement au RIP v2.

Le RIP considère comme inaccessible tout réseau qui se trouve à une distance supérieure à 15 routeurs, car le nombre de sauts est limité à 15. De ce fait, le RIP ne convient qu'aux petites topologies. L'OSPF n'a pas de limite de taille et il est adapté aux réseaux de taille intermédiaire à grande.

Le RIP sélectionne un chemin vers un réseau en ajoutant l'un des nombres de sauts indiqués par un voisin. Il compare les nombres de sauts pour atteindre une destination et sélectionne le chemin de plus petite distance ou nombre de sauts. Cet algorithme est simple, et il ne requiert ni un routeur puissant ni beaucoup de mémoire. Le RIP ne prend pas en compte la bande passante disponible dans la détermination du meilleur chemin.

L'OSPF sélectionne un chemin à l'aide du coût, une métrique basée sur la bande passante. Tous les routeurs OSPF doivent obtenir des informations complètes sur les réseaux de chaque routeur pour calculer le plus court chemin. C'est un algorithme complexe. Par conséquent, l'OSPF requiert des routeurs plus puissants et davantage de mémoire que le RIP.

Le RIP utilise une topologie linéaire. Les routeurs d'une région RIP échangent des informations avec tous les routeurs. L'OSPF fait appel à la notion de zone. Un réseau peut être subdivisé en groupes de routeurs. De cette façon, l'OSPF peut limiter le trafic vers ces zones. Les changements au sein d'une zone n'affectent pas les performances des autres zones. Cette approche hiérarchique permet à un réseau d'évoluer de façon efficace. 4

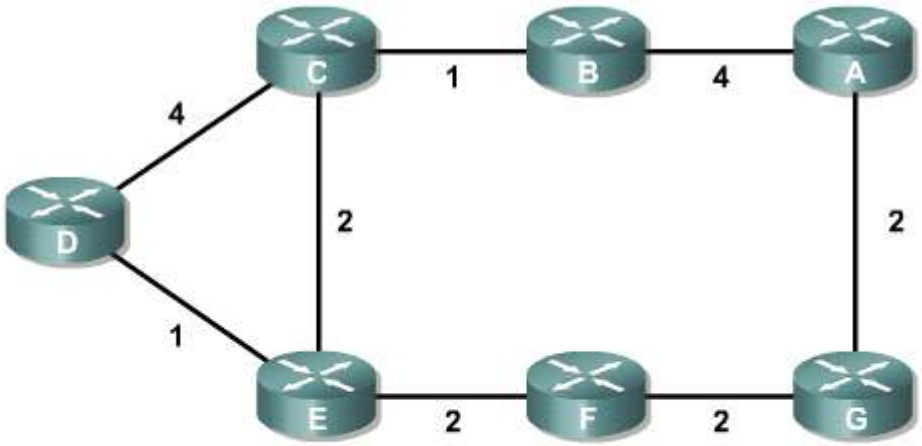
Vecteur de distance	État de lien
• Visualise la topologie du réseau du point de vue des voisins • Ajoute des vecteurs de distance d'un routeur à l'autre • Mises à jour périodiques fréquentes : convergence lente • Passe des copies des tables de routage aux routeurs voisins • Utilise une topologie linéaire	• Dispose d'une vue commune de la topologie du réseau • Calcule le plus court chemin vers les autres routeurs • Mises à jour déclenchées par événement et convergence plus rapide • Passe les mises à jour du routage à état de liens aux autres routeurs • Permet une structure hiérarchique pour les grands interréseaux

Activité de média interactive

Case à cocher: Protocoles de routage à état de liens et à vecteur de distance

Quand il aura achevé cette activité, l'étudiant sera capable d'identifier les différents protocoles de routage que ce soit les protocoles à état de liens ou à vecteur de distance.

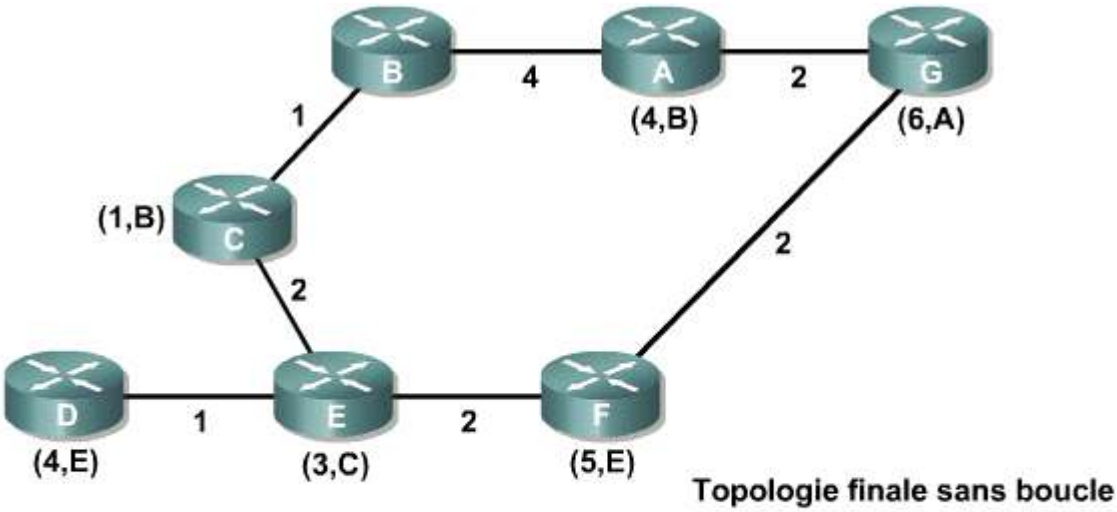
L'OSPF utilise l'algorithme du plus court chemin d'abord pour déterminer le meilleur chemin vers une destination.



A	B	C	D	E	F	G
B/4	A/4	B/1	C/4	C/2	E/2	A/2
G/2	C/1	D/4	E/1	D/1	G/2	F/2
		E/2		F/2		

En vertu de cet algorithme, le meilleur chemin est celui de moindre coût. L'algorithme du plus court chemin (shortest path-algorithm) a été formulé par Edsger Wybe Dijkstra, un scientifique informaticien Hollandais. Cet algorithme est aussi connu sous le nom d'algorithme de Dijkstra. Selon cet algorithme, un réseau est un ensemble de nœuds connectés par des liaisons point-à-point. 1Chaque lien a un coût. Chaque nœud a un nom. Chaque nœud dispose d'une base de données complète de tous les liens, ce qui fait que des informations complètes sur la topologie physique sont connues. Les bases de données d'état de liens de tous les routeurs d'une même zone sont identiques. Le tableau de la figure 1montre les informations que le nœud D a reçues. Par exemple, D a été informé qu'il est connecté au nœud C avec un coût de liaison de 4 et avec le nœud E avec un coût de liaison de 1.

L'algorithme du plus court chemin d'abord calcule ensuite une topologie exempte de boucles en utilisant le nœud comme point de départ et en examinant en temps voulu les informations dont il dispose sur les nœuds adjacents. Dans la figure 2, le nœud a calculé le meilleur chemin vers D. Le meilleur chemin vers D passe par le nœud E, qui a un coût de 4. Ces informations sont converties en une entrée de route dans B qui transmettra le trafic à C. Les paquets destinés à D à partir de B, passeront de B à C à E, puis à D dans ce réseau OSPF.



Topologie finale sans boucle

A	B	C	D	E	F	G
B/4	A/4	B/1	C/4	C/2	E/2	A/2
G/2	C/1	D/4	E/1	D/1	G/2	F/2
		E/2		F/2		

Dans l'exemple, le noeud B a déterminé que pour aller au noeud F le chemin le plus court, passant par le nœud C, a un coût de 5. Toutes les autres topologies possibles comporteront des boucles ou emprunteront des chemins plus coûteux.

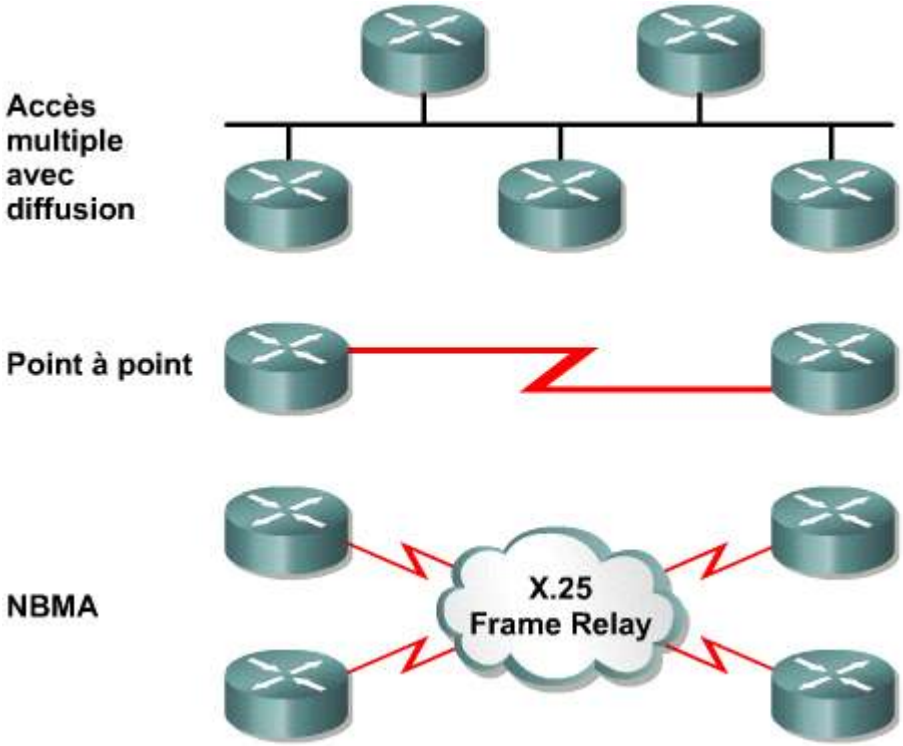
2.2 Concepts de zone unique OSPF

2.2.5 Types de réseau OSPF

Une relation de voisinage est nécessaire pour que les routeurs OSPF se partagent des informations de routage. Un routeur essaiera de devenir adjacent, ou voisin d'au moins un autre routeur sur chaque réseau IP auquel il est connecté. Certains routeurs peuvent tenter de devenir adjacents à tous leurs routeurs voisins. D'autres peuvent tenter de devenir adjacents à seulement un ou deux routeurs voisins. Les routeurs OSPF déterminent avec quel routeur ils doivent devenir adjacents en fonction du type de réseau auquel ils sont connectés. Une fois qu'une adjacence (contiguïté) a été formée entre voisins, les informations d'état de liens sont échangées.

Les interfaces OSPF reconnaissent automatiquement trois types de réseaux:

- les réseaux à accès multiple avec diffusion, comme Ethernet,
- les réseaux point à point,
- les réseaux à accès multiple sans diffusion (Nonbroadcast multi-access - NBMA) comme le Frame Relay [1].

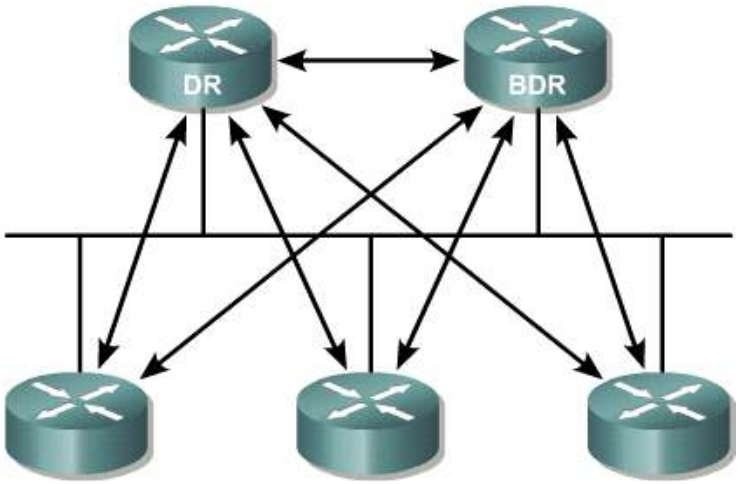


Un quatrième type, point à multipoint, peut être configuré manuellement sur une interface par un administrateur. 2

Type de réseau	Caractéristiques	Sélection DR ?
Accès multiple avec diffusion	Ethernet, Token Ring ou FDDI	Oui
Accès multiple sans diffusion	Frame Relay, X.25, SMDS	Oui
Point à point	PPP, HDLC	Non
Point-à-multipoint	Configuré par un administrateur	Non

Dans un réseau à accès multiples, il est impossible de savoir à l'avance combien de routeurs seront connectés. Dans les réseaux point-à-point, seulement deux routeurs peuvent être connectés.

Dans un réseau broadcast à accès multiple avec diffusion, plusieurs routeurs peuvent être connectés. Si chaque routeur devait établir une contiguïté (adjacence) complète avec chaque autre routeur et échanger des informations d'état de liens avec chaque voisin, la charge serait excessive. Avec 5 routeurs, 10 relations de contiguïté seraient nécessaires et 10 états de liens seraient envoyés. Avec 10 routeurs, 45 contiguïtés seraient nécessaires. En général, pour n routers, n*(n-1)/2 contiguïtés devraient être formées. 3



La solution à cette surcharge consiste à opérer une sélection de routeur désigné (DR). Ce routeur devient adjacent à tous les autres routeurs du segment de broadcast. Tous les autres routeurs sur le segment envoient leurs informations d'état de liens au routeur désigné. Ce dernier agit alors comme porte-parole pour le segment. Le routeur désigné envoie des informations d'état de liens à tous les autres routeurs sur le segment en utilisant l'adresse multicast 224.0.0.5 pour tous les routeurs OSPF.

Malgré le gain d'efficacité que permet de réaliser un routeur désigné, il y a un inconvénient. Le routeur désigné constitue un point de défaillance unique. Un deuxième routeur est sélectionné comme routeur désigné de secours (BDR) pour prendre le relais du routeur désigné au cas où ce dernier tomberait en panne. 3 Afin d'avoir la certitude que le routeur désigné et le routeur désigné de secours voient les états de liens que tous les routeurs envoient sur le segment, l'adresse multicast pour tous les routeurs désignés, 224.0.0.6, est utilisée.

Sur les réseaux point-à-point qui ne comportent que deux nœuds, aucun routeur désigné ou routeur désigné de secours n'est sélectionné. Les deux routeurs deviennent totalement adjacents l'un par rapport à l'autre.

Activité interactive

Glisser-Positionner: Types de réseaux OSPF

À la fin de cette activité, l'étudiant sera en mesure d'identifier la fonction des différents types de réseaux OSPF.

2.2 Concepts de zone unique OSPF

2.2.6 Protocole HELLO de l'OSPF

Lorsqu'un routeur lance un processus de routage OSPF sur une interface, il envoie un paquet HELLO et continue d'envoyer des HELLO à intervalle régulier. Les règles qui régissent l'échange des paquets HELLO OSPF sont appelées protocole HELLO.

Au niveau de la couche 3 du modèle OSI, des paquets HELLO sont adressés à l'adresse multicast 224.0.0.5. Cette adresse correspond à «tous les routeurs OSPF». Les routeurs OSPF utilisent des paquets HELLO pour initier de nouvelles contiguïtés et pour s'assurer que les routeurs voisins fonctionnent encore. Des HELLO sont envoyés toutes les 10 secondes par défaut sur les réseaux broadcast à accès multiple et sur les réseaux point-à-point. Sur les interfaces qui se connectent aux réseaux NBMA, telles que le Frame Relay, le délai par défaut est de 30 secondes.

Sur les réseaux à accès multiple, le protocole Hello sélectionne un routeur désigné (DR) et un routeur désigné de secours (BDR).

Bien que le paquet hello soit de petite taille, il est constitué de l'en-tête de paquet OSPF. 1

Version	Type	Longueur du paquet
ID du routeur		
ID de zone		
Somme de contrôle		Type d'authentification
Données d'authentification		

Le champ Type est paramétré sur 1 pour indiquer que le paquet contient des informations HELLO.

Le champ type est défini à 1 pour le paquet hello.

Le contenu transporté dans le paquet HELLO doit avoir fait l'objet d'un accord entre tous les voisins pour qu'une contiguïté soit formée et que les informations d'état de liens soient échangées. 2

Masque de réseau
Intervalle HELLO | Options | Priorité du routeur
Intervalle d'arrêt
Routeur désigné
Routeur désigné de secours
ID du routeur voisin
ID du routeur voisin
(Des champs ID du routeur voisin peuvent être ajoutés à la fin de l'en-tête, si nécessaire.)

Les paquets HELLO transportent des informations sur les intervalles d'arrêt et de HELLO, ainsi que sur les identifiants des routeurs. Les routeurs doivent se mettre d'accord sur ces paramètres pour former des

Activité interactive

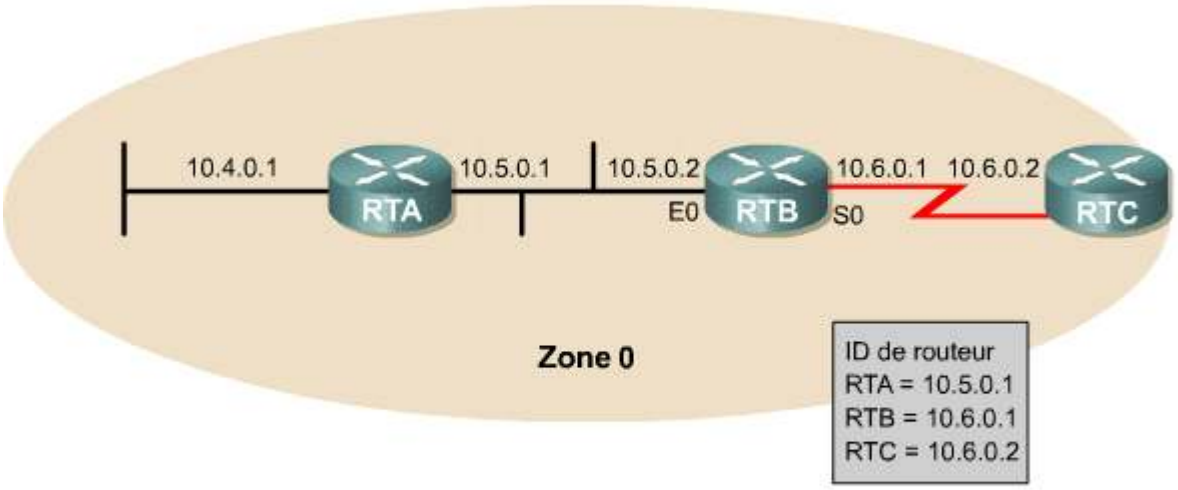
Glisser-Positionner: En-tête de paquet OSPF

À la fin de cette activité, l'étudiant sera en mesure d'identifier les différents champs de l'en-tête de paquet OSPF.

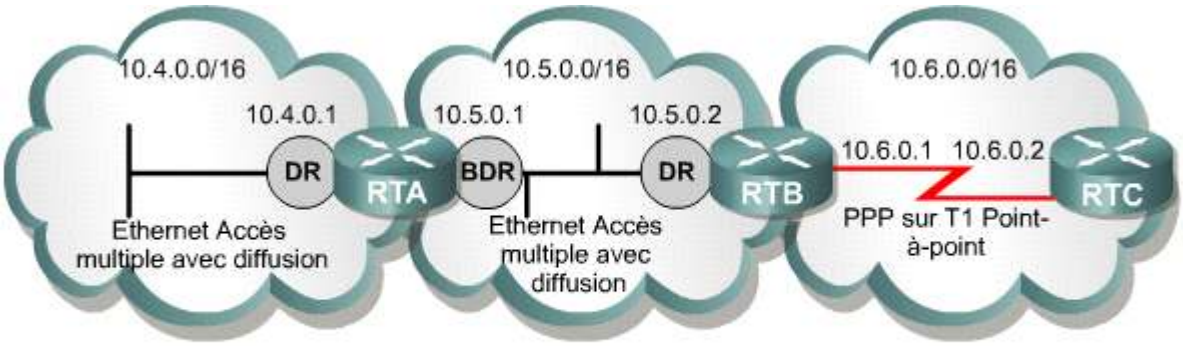
2.2 Concepts de zone unique OSPF

2.2.7 Étapes du fonctionnement de l'OSPF

Quand un routeur démarre un processus de routage OSPF sur une interface, il envoie un paquet d'invite "Hello" et continue d'envoyer ces invites à intervalles réguliers. L'ensemble des règles qui gouvernent cet échange de paquets d'invite OSPF est appelé le protocole «Hello». Dans les réseaux à accès multiples, le protocole «Hello» élit un routeur désigné (DR acronyme de «Designated Router») et un routeur désigné de secours (BDR acronyme de Backup DR). Le protocole «Hello» transporte les informations de ceux des voisins qui acceptent de former une adjacence et d'échanger leurs informations d'état de liens. Dans un réseau à accès multiples le DR et le BDR maintiennent les relations d'adjacence avec tous les autres routeurs OSPF du réseau. [1] [2]



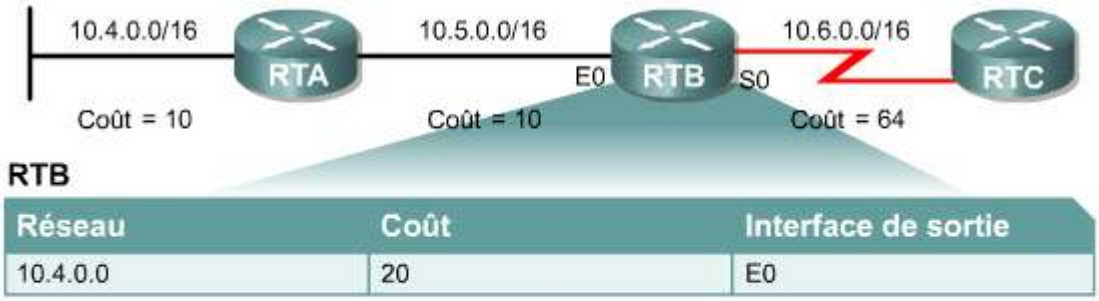
Un routeur OSPF tente de former une contiguïté avec au moins un voisin pour chaque réseau IP auquel il est connecté.



Les routeurs OSPF sélectionnent les DR et BDR uniquement sur les réseaux IP à accès multiple.

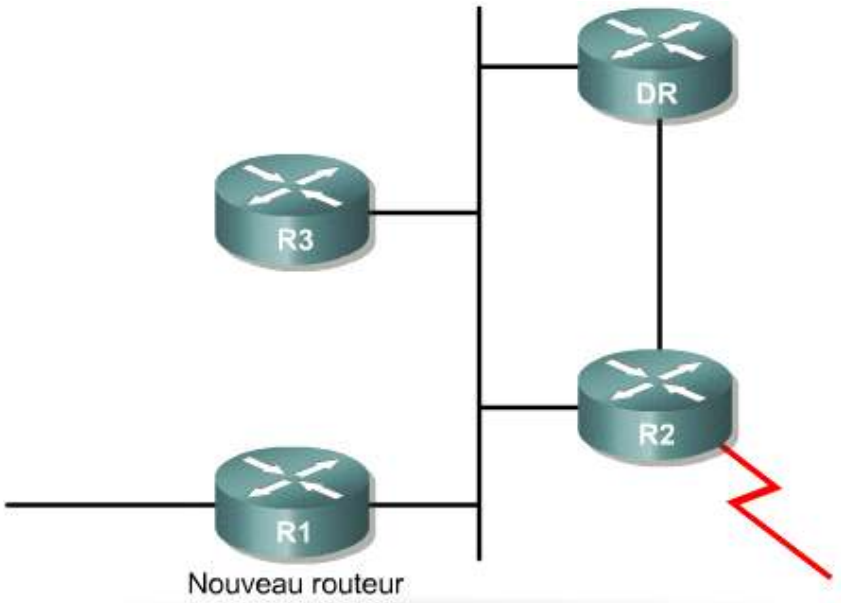
Les routeurs adjacents traversent une série d'états. Ils doivent être à l'état complet pour que les tables de routage soient créées et le trafic acheminé. Chaque routeur envoie des mises à jour de routage à état de liens (LSA) dans des paquets de mise à jour d'état de liens (LSU). Ces LSA décrivent toutes les liaisons du routeur. Chaque routeur qui reçoit une LSA de ses voisins l'enregistre dans la base de données d'état de liens. Ce processus est répété pour tous les routeurs du réseau OSPF.

Lorsque les bases de données sont complètes, chaque routeur utilise l'algorithme SPF pour calculer une topologie logique exempte de boucles vers chaque réseau connu. Le chemin le plus court au coût le plus bas est utilisé dans la construction de cette topologie, ce qui fait que la meilleur route est sélectionnée. 3

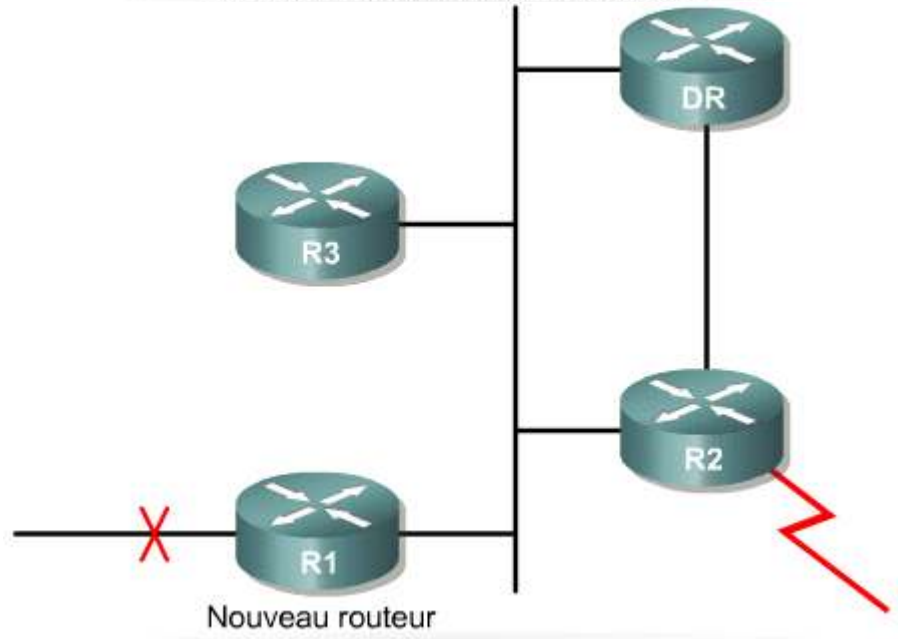


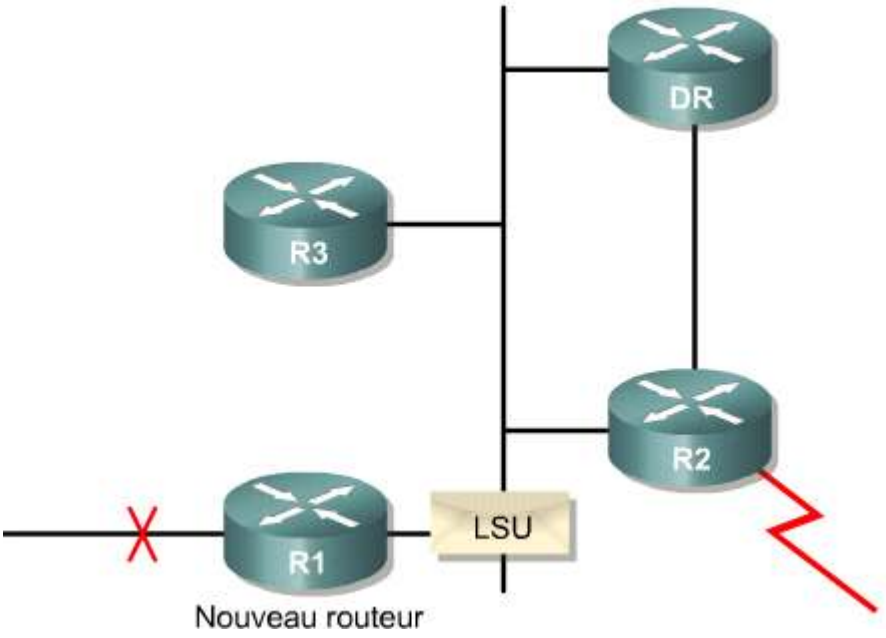
La base de données d'état de liens est traitée par l'algorithme du plus court chemin d'abord et les meilleurs chemins sont sélectionnés.

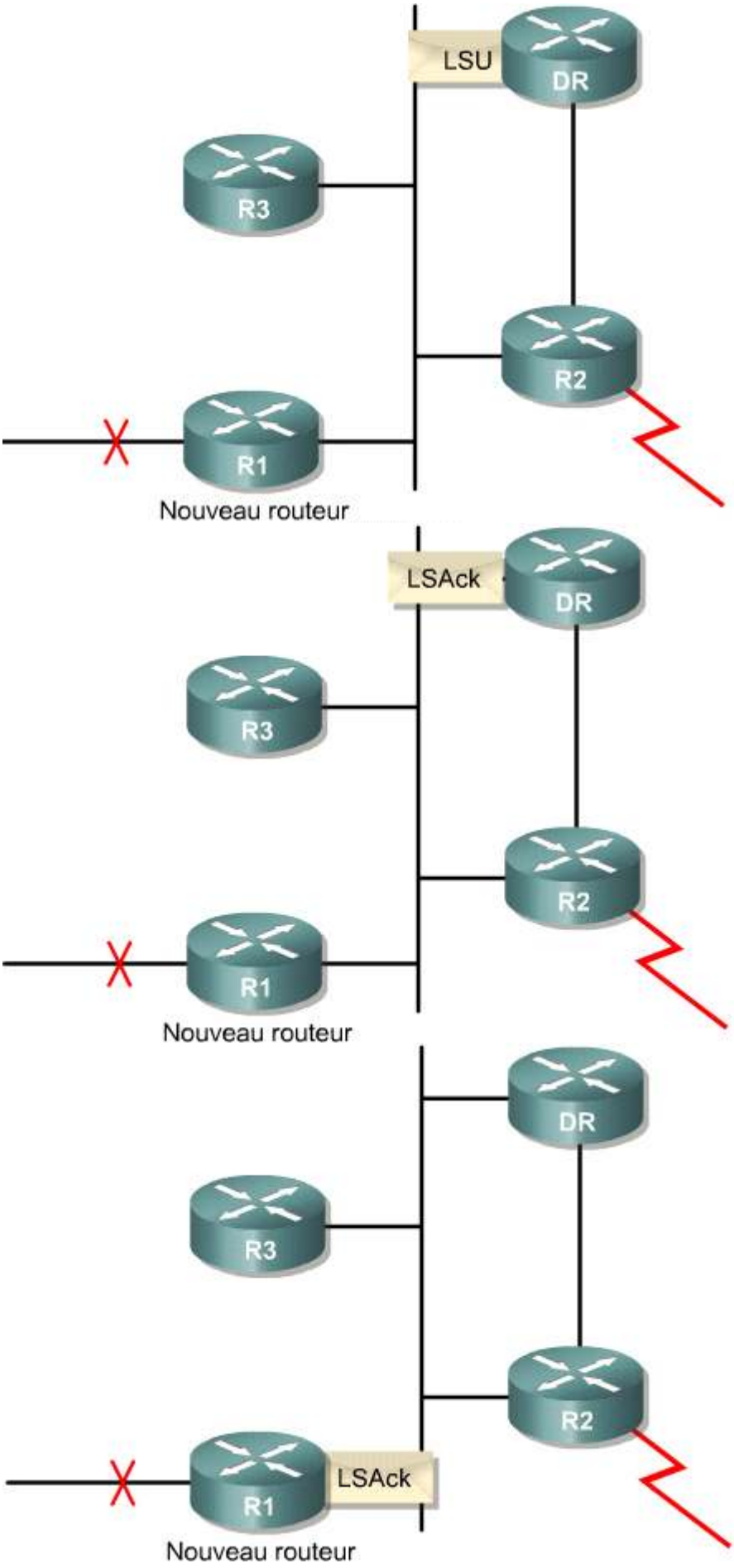
Les informations de routage sont alors mises à jour. En cas de changement de l'état de lien, les routeurs utilisent un processus de diffusion pour avertir tous les autres routeurs du réseau du changement qui est survenu. L'intervalle d'arrêt du protocole HELLO constitue une mécanisme qui permet de déterminer qu'un voisin adjacent est défaillant. 4 – 7



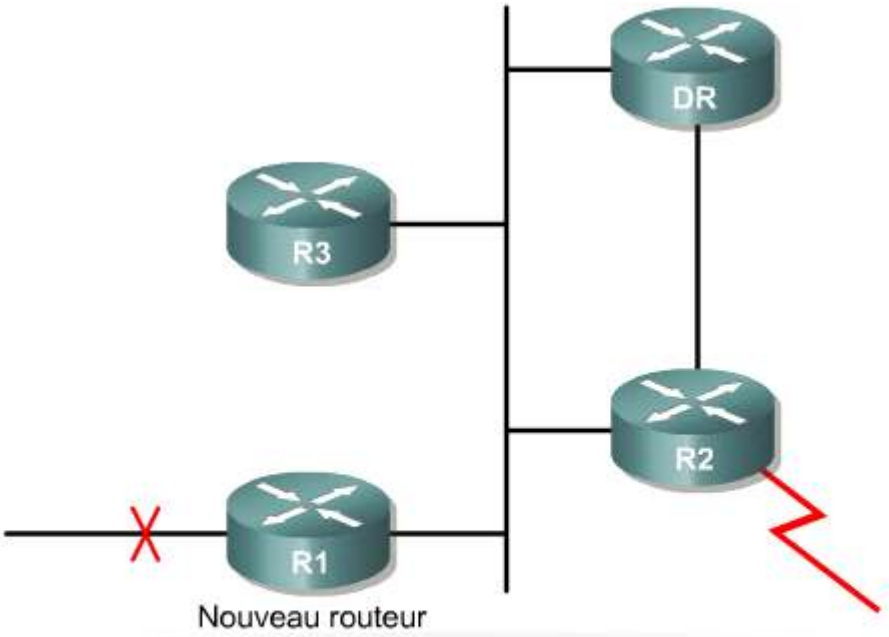
R1 détecte qu'un lien est coupé et envoie un LSU au DR. Le DR accuse réception du LSU.



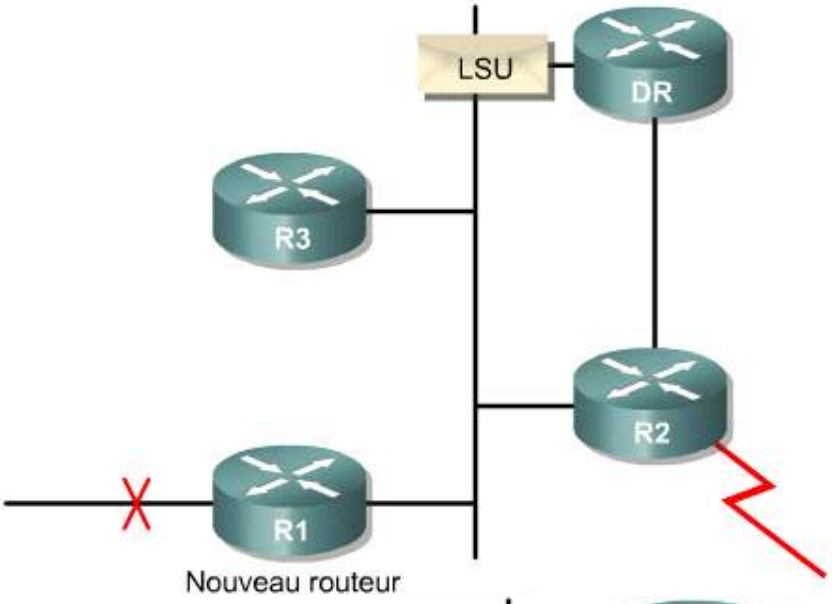


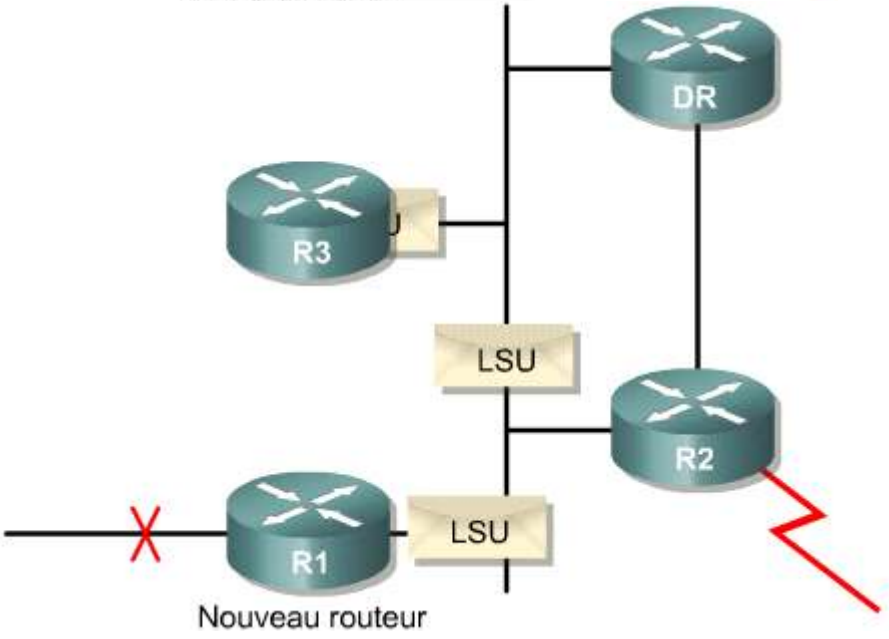

LSU
DR
R3
R2
R1
Nouveau routeur
LSAck
DR
R3
R2
R1
Nouveau routeur
DR
R3
R2
LSAck
R1
Nouveau routeur

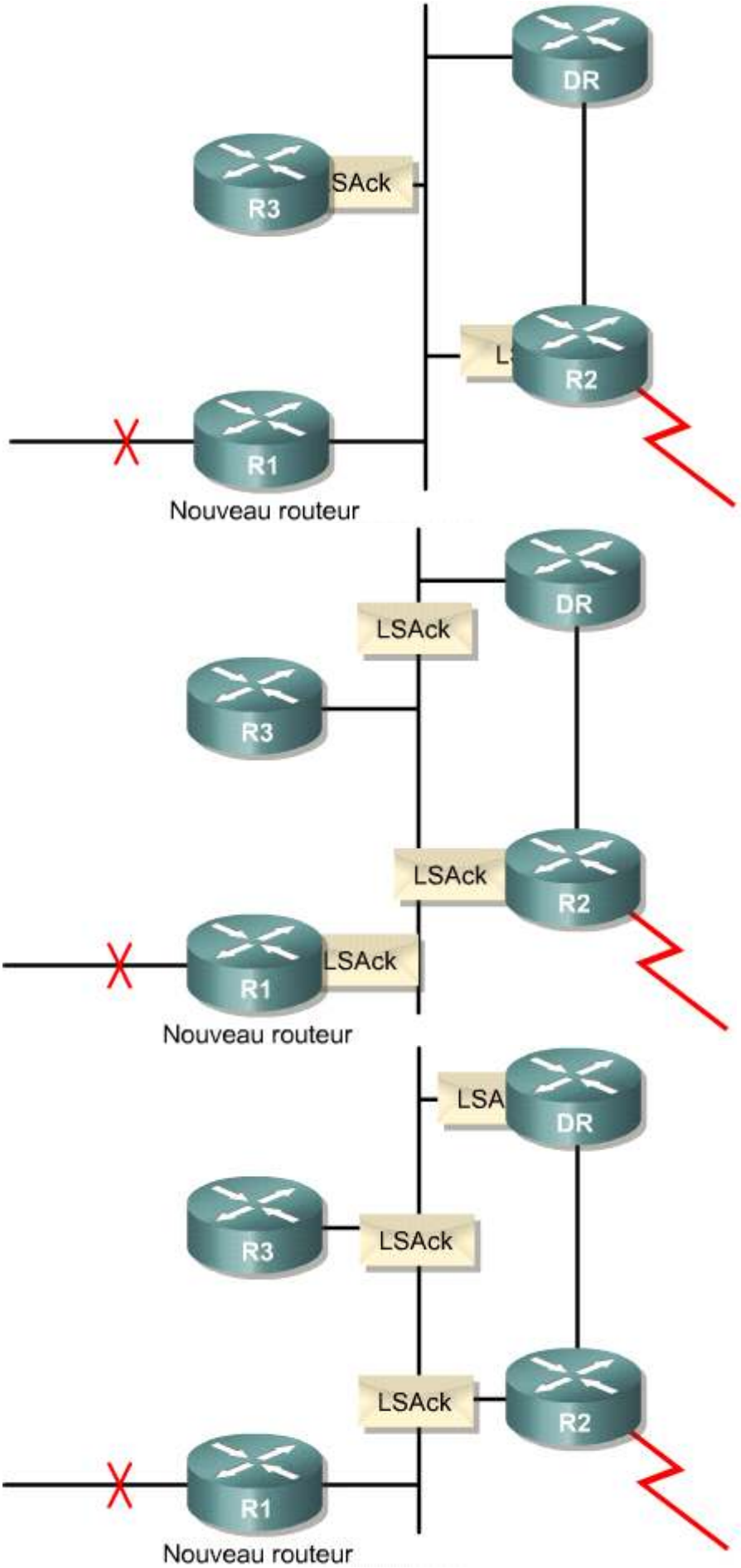
5-

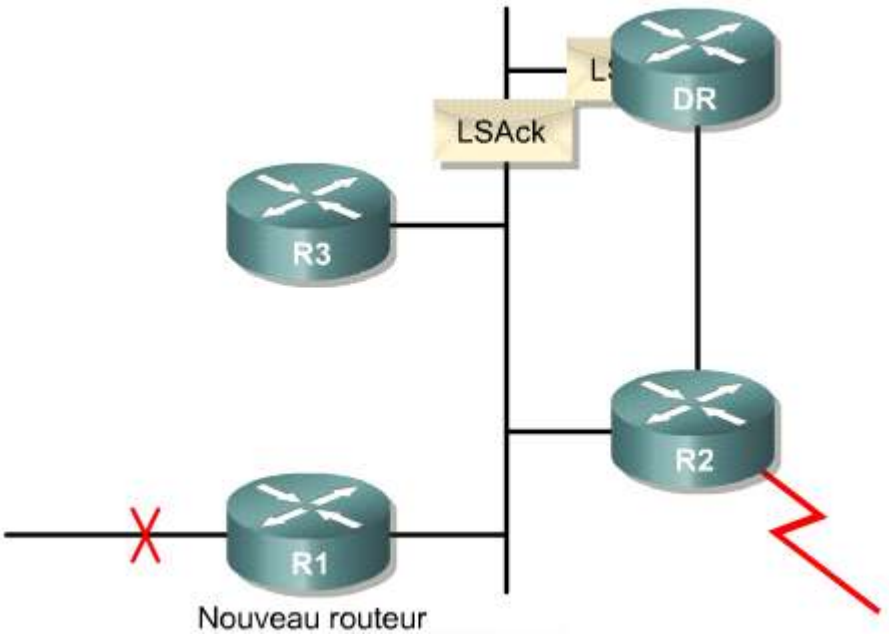


Quand le DR reçoit le LSU et en accuse réception, il diffuse ce LSU à tous les routeurs OSPF du réseau à l'adresse multicast 224.0.0.5. Chaque routeur va accuser réception du LSU avec un LSAck.

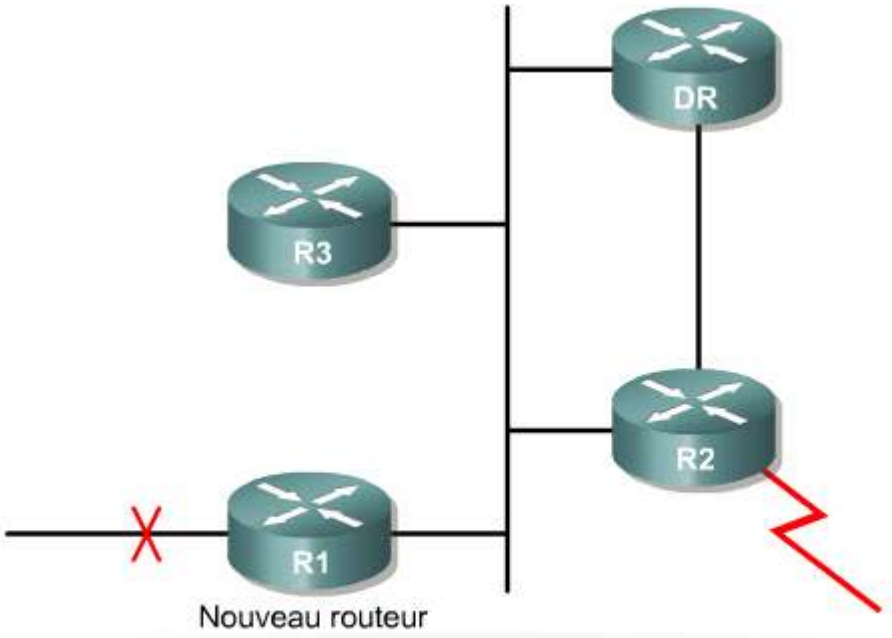




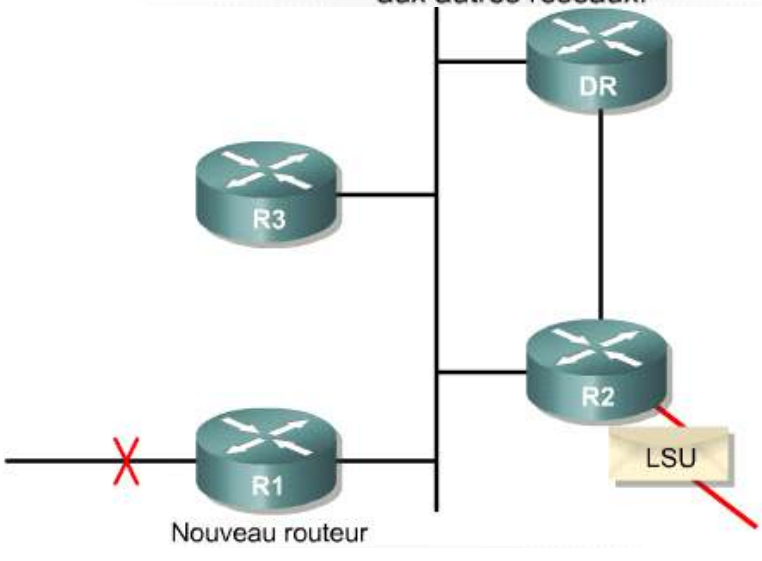

DR
SAck
R3
R2
R1
Nouveau routeur
DR
LSAck
R3
LSAck
R2
R1
LSAck
Nouveau routeur
LSA
DR
R3
LSAck
LSAck
R2
R1
Nouveau routeur

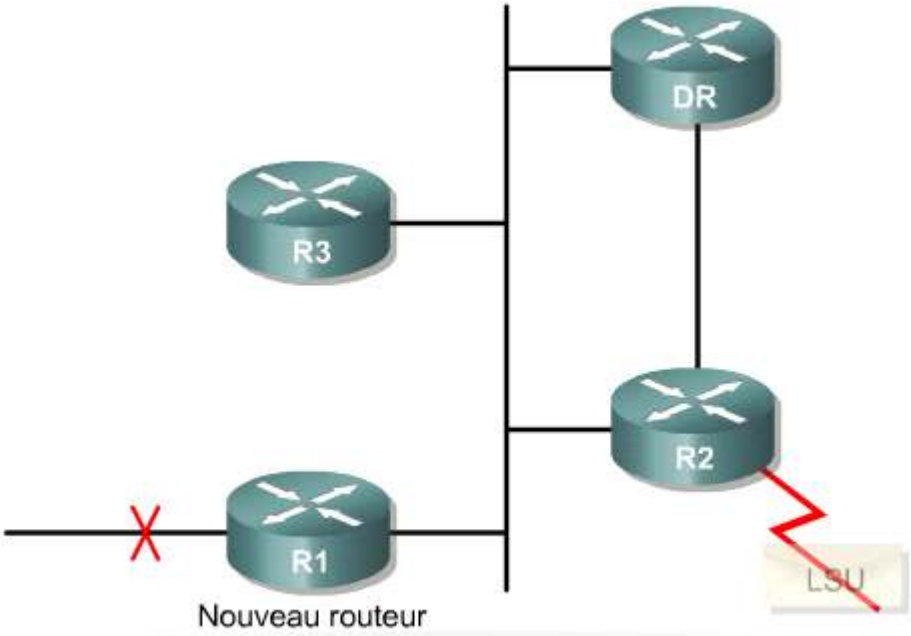


6-

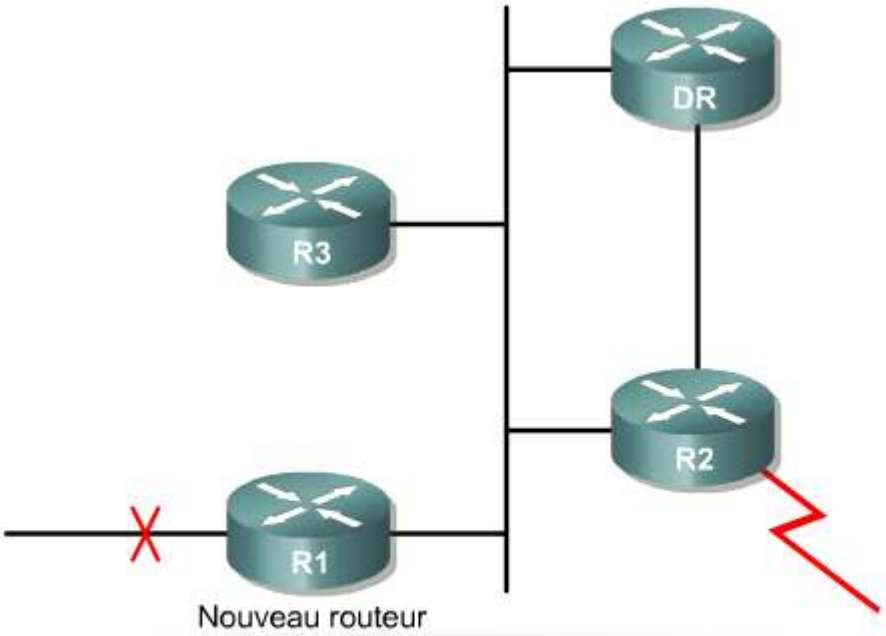


Si un routeur OSPF est connecté à d'autres réseaux, il diffuse le LSU aux autres réseaux.

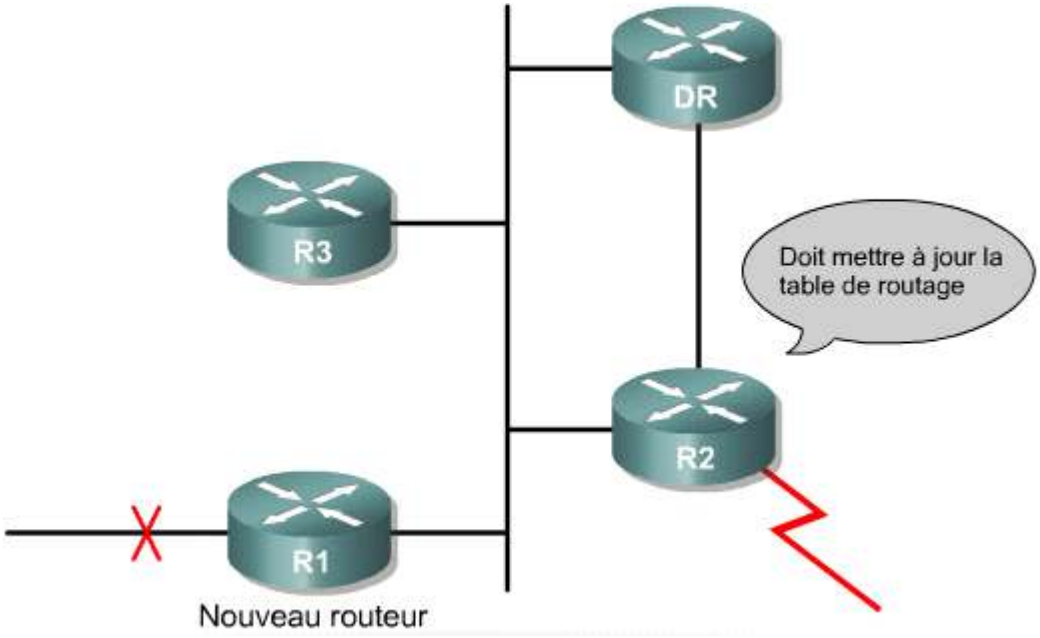




7-



Après avoir reçu un LSU qui comporte de nouvelles informations, le routeur OSPF met à jour sa base de données d'état de liens. Ensuite, il active l'algorithme SPF qui utilise cette nouvelle information pour recalculer la table de routage.

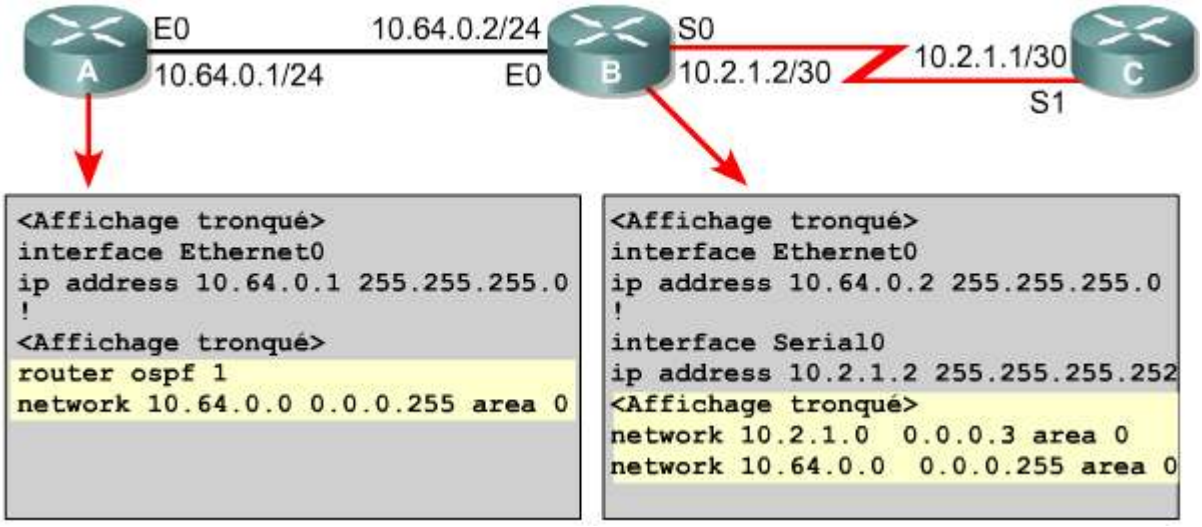


2.3 Configuration d'une zone unique OSPF

2.3.1 Configuration du protocole de routage OSPF

Le routage OSPF est fondé sur la notion de zone. Chaque routeur contient une base de données complète des états de liens en vigueur dans une zone spécifique. Tout nombre entre 0 et 4294967295 peut être affecté à une zone d'un réseau OSPF. Cependant, le numéro 0 est affecté à une zone unique, qui est identifiée en tant que zone 0. Dans les réseaux OSPF à zones multiples, toutes les zones doivent se connecter à la zone 0. Cette zone est également appelée zone de backbone.

La configuration d'OSPF demande que le processus de routage OSPF soit activé sur le routeur en spécifiant les adresses de réseau et les informations qui définissent la zone OSPF. 1



Les adresses de réseau sont configurées avec un masque générique, et non pas avec un masque de sous-réseau. Le masque générique représente les liens ou les adresses hôtes qui peuvent se trouver dans ce segment. Les ID de zone peuvent être saisies sous forme de numéro complet ou de notation décimale (semblable à une adresse IP A.B.C.D). 2

Commande network area	Description
adresse	Peut être l'adresse du réseau, du sous-réseau ou de l'interface. Invite le routeur à déterminer les liaisons à annoncer, les liaisons sur lesquelles écouter des annonces et les réseaux auxquels annoncer les routes.
masque-génériqu	Masque inverse utilisé pour déterminer le mode de lecture de l'adresse. Le masque contient des bits génériques où 0 équivaut à une correspondance et 1 à " ne sais pas " ; par exemple, 0.0.255.255 indique une correspondance dans les deux premiers octets. (Le masque de sous-réseau NORMAL équivalent serait le masque de 16 bits 255.255.0.0.) Si vous indiquez l'adresse d'interface, utilisez le masque 0.0.0.0.
id-zone	Indique la zone à associer à l'adresse. Peut être un numéro ou ressembler à une adresse IP A.B.C.D. Pour une zone de backbone, l'ID doit être égal à 0.

Pour activer le routage OSPF, utilisez la syntaxe de commande de configuration globale:

```
Router(config)#router ospf id-processus
```

L'ID de processus est un numéro qui permet d'identifier un processus de routage OSPF sur le routeur. Plusieurs processus OSPF peuvent être démarrés sur un même routeur. Ce numéro peut être n'importe quelle valeur comprise entre 1 et 65535. La plupart des administrateurs réseau conservent le même ID de processus à travers un système autonome, mais cela n'est pas obligatoire. Il est rarement nécessaire d'exécuter plus d'un processus OSPF sur un routeur. Les réseaux IP sont annoncés de la façon suivante dans OSPF:

```
Router(config-router)#network adresse masque-générique  area id-zone
```

Chaque réseau doit pouvoir être identifié par la zone auquel il appartient. L'adresse réseau peut être celle d'un réseau entier, d'un sous-réseau ou l'adresse de l'interface. Le masque générique représente l'ensemble d'adresses hôtes que le segment prend en charge. Il est différent d'un masque de sous-réseau, utilisé lors de la configuration des adresses IP sur les interfaces.

Activité de TP

Exercice: Configuration du processus de routage OSPF

Dans ce TP, les étudiants vont configurer un système d'adressage IP pour la zone OSPF 0, puis de configurer et de vérifier le routage OSPF.

Activité de TP

Activité en ligne: Configuration du routage OSPF

Au cours de ce TP, les étudiants vont configurer et contrôler le routage OSPF.

2.3 Configuration d'une zone unique OSPF

2.3.2 Configuration d'une adresse d'essai en mode bouclé OSPF et de la priorité des routeurs

Lorsque le processus OSPF démarre, la plate-forme logicielle Cisco IOS utilise l'adresse IP active locale la plus élevée comme ID de routeur OSPF. En l'absence d'interface active, le processus OSPF ne démarre pas. En cas de défaillance de l'interface active, le processus OSPF est privé d'ID de routeur et cesse par conséquent de fonctionner jusqu'à ce que l'interface soit rétablie.

Pour garantir la stabilité de l'OSPF, une interface doit être active en permanence pour le processus. Vous pouvez configurer à cet effet une interface en mode bouclé (c'est-à-dire une interface logique). L'OSPF utilise alors cette adresse comme ID de

routeur, quelle que soit sa valeur. Sur un routeur possédant plusieurs interfaces en mode bouclé, l'OSPF choisit l'adresse IP en mode bouclé la plus élevée comme ID de routeur.

Pour créer et affecter une adresse IP à une interface en mode bouclé, utilisez les commandes suivantes:

```
Router(config)#interface loopback numéro
Router(config-if)#ip addressadresse-ip masque-sous-réseau
```

Il est recommandé d'utiliser les interfaces en mode bouclé pour tous les routeurs qui exécutent le protocole OSPF. Cette interface en mode bouclé doit être configurée avec une adresse utilisant un masque de sous réseau 32 bits de 255.255.255.255. Ce type de masque est appelé masque d'hôte, car le masque de sous-réseau spécifie un réseau pour un hôte. Lorsqu'il est demandé à l'OSPF d'annoncer un réseau en mode bouclé, ce dernier annonce toujours la boucle locale comme une route hôte avec un masque 32 bits. [1]

```
! Create the loopback 0 interface
Sydney3(config)#interface loopback 0
Sydney3(config-if)#ip address 192.168.31.33
255.255.255.255
Sydney3(config-if)#exit
! Remove loopback 0 interface
Sydney3(config)#no interface loopback 0
Sydney3(config)#
01:47:27: %LINK-5-CHANGED: Interface Loopback0, changed
state to administratively down
```

Une interface en mode bouclé est une interface uniquement logicielle. Pour supprimer une interface en mode bouclé, entrez la commande **no interface loopback**.

Il peut y avoir plus de deux routeurs dans les réseaux broadcast à accès multiple. L'OSPF sélectionne un routeur désigné (DR) pour en faire le point focal de toutes les mises à jour et annonces d'état de liens. Le rôle du routeur désigné étant critique, un routeur désigné de secours (BDR) est sélectionné pour prendre le relais en cas de défaillance du routeur désigné.

Si le type de réseau d'une interface est broadcast, la priorité par défaut de l'OSPF est 1. Lorsque des priorités OSPF sont identiques, la sélection du routeur désigné par l'OSPF se fait sur la base de l'ID du routeur. L'ID de routeur la plus élevée est sélectionnée.

Le résultat de la sélection peut être déterminé en vérifiant que les bulletins (les paquets hello 6) comportent une priorité pour cette interface de routeur. L'interface qui signale la priorité la plus élevée pour un routeur s'assure que ce dernier devienne le routeur désigné. [2]

Masque de réseau		
Intervalle HELLO	Options	Priorité du routeur
Intervalle d'arrêt		
Routeur désigné		
Routeur désigné de secours		
ID du routeur voisin		
ID du routeur voisin		
(Des champs ID du routeur voisin peuvent être ajoutés à la fin de l'en-tête, si nécessaire.)		

Les paquets HELLO transportent des informations sur les intervalles d'arrêt et de HELLO, ainsi que sur les identifiants des routeurs. Les routeurs doivent accepter ces informations pour former des contiguïtés.

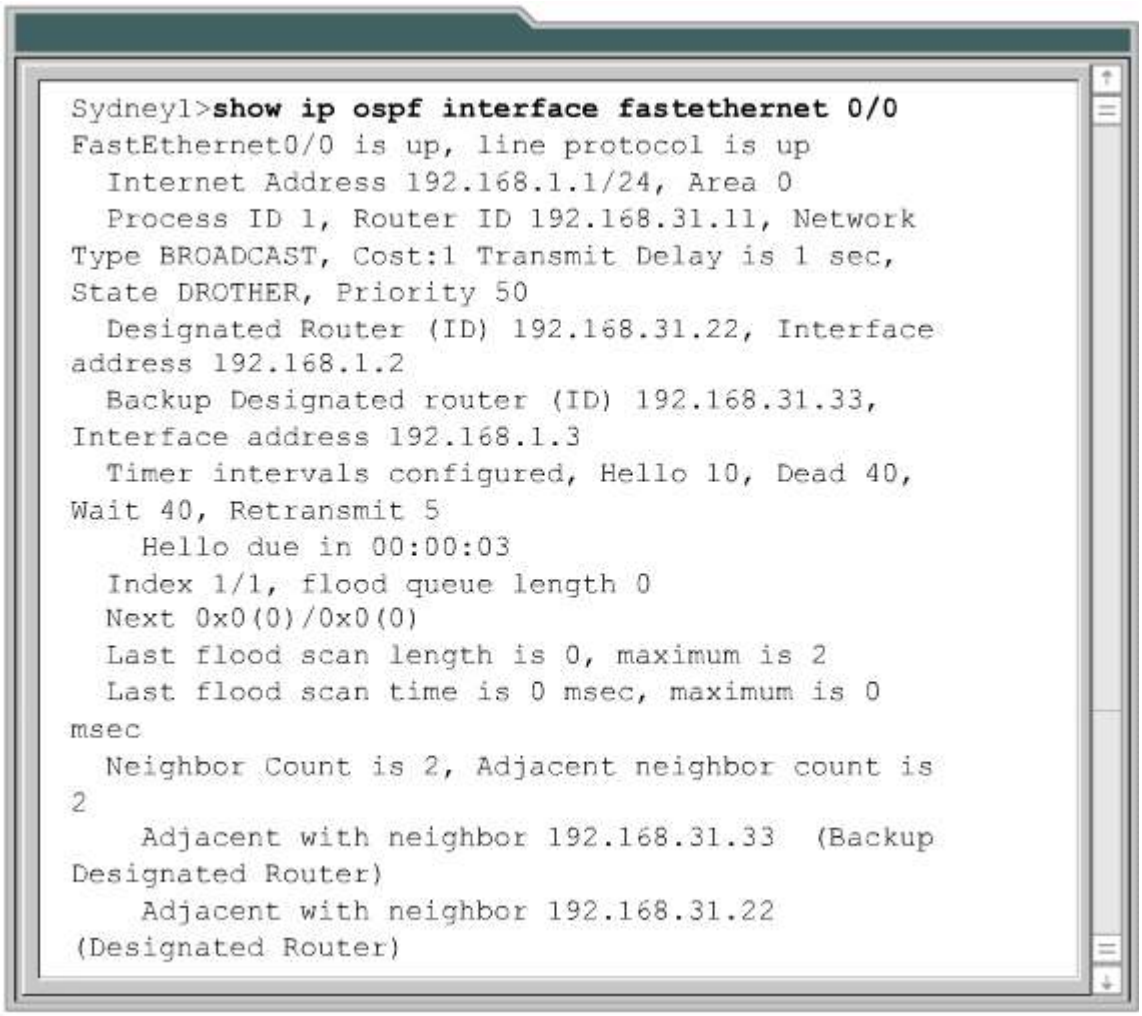
Les priorités peuvent être définies à n'importe quelle valeur comprise entre 0 et 255. Une valeur égale à 0 empêche la sélection du routeur. Le routeur dont la priorité OSPF est la plus élevée sera sélectionné comme routeur désigné. Le routeur dont la priorité est immédiatement inférieure sera le routeur désigné de secours. Après le processus de sélection, le routeur désigné et le routeur désigné de secours conservent leur rôle, même si des routeurs aux valeurs de priorité OSPF plus élevées sont ajoutés au réseau.

Modifiez la priorité OSPF en entrant la commande de configuration d'interface globale **`ip ospf priority`** sur une interface qui participe à l'OSPF. 3

```
Sydney1(config)#interface fastethernet 0/0
Sydney1(config-if)#ip ospf priority 50
Sydney1(config-if)#end
Sydney1#
00:21:57: %SYS-5-CONFIG_I: Configured from console
by console
```

Le champ Priorité du routeur du paquet HELLO envoyé sur l'interface Fast Ethernet est paramétré sur 50.

La commande **`show ip ospf interface`** affichera la valeur de priorité d'interface ainsi que d'autre informations clés. 4



```
Sydney1>show ip ospf interface fastethernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0
  Process ID 1, Router ID 192.168.31.11, Network
Type BROADCAST, Cost:1 Transmit Delay is 1 sec,
State DROTHER, Priority 50
  Designated Router (ID) 192.168.31.22, Interface
address 192.168.1.2
  Backup Designated router (ID) 192.168.31.33,
Interface address 192.168.1.3
  Timer intervals configured, Hello 10, Dead 40,
Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 2
  Last flood scan time is 0 msec, maximum is 0
msec
  Neighbor Count is 2, Adjacent neighbor count is
2
    Adjacent with neighbor 192.168.31.33  (Backup
Designated Router)
    Adjacent with neighbor 192.168.31.22
(Designated Router)
```

```
Router(config-if)#ip ospfpriority numéro
Router#show ip ospf interfacenuméro de type
```

Activité de TP

Exercice: Configuration d'OSPF avec des adresses d'essai en mode bouclé

Dans ce TP, les étudiants vont configurer OSPF avec des adresses d'essai en mode bouclé.

Activité de TP

Activité en ligne: Configuration d'OSPF avec des adresses d'essai en mode bouclé

Au cours de ce TP, l'étudiant va observer le processus de sélection des routeurs désignés DR et BDR.

2.3 Configuration d'une zone unique OSPF

2.3.3 Modification de la métrique de coût OSPF

OSPF utilise le coût comme la mesure de détermination de la meilleure route. Un coût est associé au coté sortant de chaque interface de routeur. Des coûts sont aussi associés à des données de routage définies extérieurement. En général, le coût d'un chemin est calculé d'après la formule 10^8/bande passante, où la bande passante est exprimée en bits/s. L'administrateur système peut aussi configurer les coûts par d'autres méthodes. Plus le coût est faible, plus l'interface sera susceptible d'être choisie pour transmettre le trafic de données. L'IOS Cisco détermine automatiquement un coût basé sur la bande passante de l'interface. 1

Type de lien et bande passante	Coût
Liaison série - 56 kbits/s	1785
Liaison série T1 - 1,544 Mbits/s	64
Liaison série E1 - 2,048 Mbits/s	48
Token Ring - 4 Mbits/s	25
Ethernet - 10 Mbits/s	10
Token Ring - 16 Mbits/s	6
Fast Ethernet / FDDI - 100 Mbits/s	1

Pour que l'OSPF fonctionne de manière appropriée, il est essentiel de définir la bande passante d'interface correcte.

```
Router(config)#interface serial 0/0
Router(config-if)#bandwidth 56
```

Le coût peut être modifié pour influer sur le résultat du calcul de coût OSPF. La modification de coût s'effectue couramment dans un environnement de routage multifournisseurs. Elle permet de faire correspondre la valeur de coût des différents fournisseurs. Le Gigabit Ethernet est une autre cas. Le coût par défaut affecte la valeur de coût le plus faible de 1 à une liaison à 100 Mbits/s. Dans le cas de liaisons à 100 Mbits/s et Gigabit Ethernet, les valeurs de coût par défaut pourraient déterminer un chemin inapproprié si elles n'étaient pas ajustées. Le numéro de coût peut être compris entre 1 et 65535. 2

Cisco

```
Sydney2(config-if)#ip ospf cost ?
  <1-65535>  Cost
Sydney2(config-if)#ip ospf cost 1
```

Utilisez les commandes de configuration d'interface suivante pour définir le coût de la liaison:

```
Router(config-if)#ip ospfcost numéro
```

Activité de TP

Exercice: Modification de la métrique de coût OSPF

Dans ce TP, les étudiants vont modifier la métrique de coût d'OSPF (Open Shortest Path First).

Activité de TP

Activité en ligne: Modification de la métrique de coût OSPF

Au cours de ce TP, l'étudiant va modifier la métrique de coût OSPF.

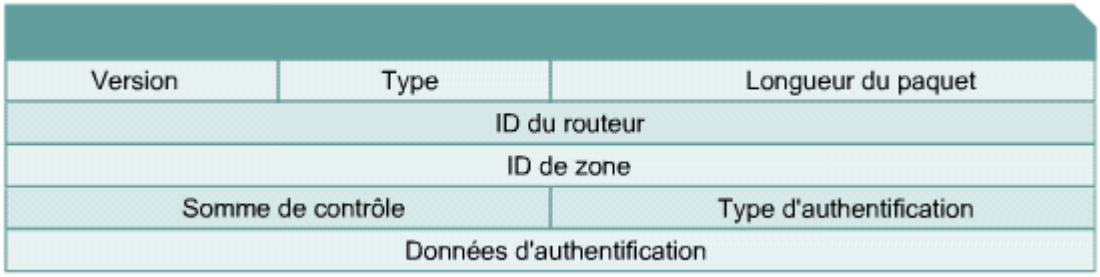
2.3 Configuration d'une zone unique OSPF

2.3.4 Configuration de l'authentification OSPF

Par défaut, un routeur s'attend à recevoir les informations de routage d'un autre routeur qui doit les lui envoyer. Il s'attend également à ce que ces informations ne soient pas altérées en chemin.

Pour sécuriser cet échange, les routeurs d'une zone spécifique peuvent être configurés pour s'authentifier mutuellement.

Chaque interface OSPF peut présenter une clé d'authentification à l'usage des routeurs qui envoient des informations OSPF aux autres routeurs du segment. La clé d'authentification, ou mot de passe, est une secret partagé entre les routeurs. Elle permet de générer les données d'authentification dans l'en-tête de paquet OSPF. 1



Le mot de passe peut comporter jusqu'à huit caractères. Utilisez la syntaxe de commande suivante pour configurer l'authentification OSPF:

```
Router(config-if)#ip ospf authentication-keymot de passe
```

Une fois le mot de passe configuré, l'authentification doit être activée:

```
Router(config-router)#areanuméro-de-zoneauthentication
```

Si vous configurez une authentification simple, le mot de passe est envoyé sous forme de texte en clair. Cela veut dire qu'il peut être facilement décodé si un analyseur de paquets capture un paquet OSPF.

Il est recommandé de crypter les informations d'authentification. Pour envoyer des informations d'authentification cryptées et pour renforcer la sécurité, le mot-clé MD5 (Message Digest 5) est utilisé. Le mot-clé MD5 spécifie le type d'algorithme de hachage (MD) à utiliser, et le champ de type de cryptage correspond au type de cryptage, où 0 signifie aucun et où 7 signifie propriétaire.

Utilisez la syntaxe de commande de configuration d'interface suivante:

```
Router(config-if)#ip ospf message-digest-key identificateur-de-clé type-d-encryption md5 clé
```

L'identificateur-de-clé est un identifiant dont la valeur est comprise entre 1 et 255. La clé est un mot de passe alphanumérique qui comporte jusqu'à seize caractères. Les routeurs voisins doivent utiliser le même identifiant de clé et la même valeur de clé.

La commande suivante est configurée en mode de configuration de routeur: 2

Cisco

```
Sydney1(config-if)#ip ospf message-digest-key 1 md5 7
unsecret
Sydney1(config-if)#exit
Sydney1(config)#router ospf 1
Sydney1(config-router)#area 0 authentication message-
digest
Sydney1(config-router)#end
Sydney1#
```

La configuration de l'interface et du routeur est nécessaire.

```
Router(config-router)#areaid-de-zoneauthentication message-digest
```

L'authentification MD5 crée un condensé de message. Ce dernier est composé de données brouillées qui sont basées sur le mot de passe et sur le contenu du paquet. Le routeur récepteur utilise le mot de passe partagé et le paquet pour recalculer le condensé de message via l'algorithme MD5. Si les résultats (condensés de message) de l'application des algorithmes MD5 correspondent, le routeur détermine que la source et le contenu du paquet n'ont pas été altérés. L'authentification, si elle est utilisée, est identifiée par un champ type. Dans le cas de l'authentification par algorithme MD5, le champ de données d'authentification contient l'id de clé et la longueur du condensé de message qui est ajouté au paquet. L'algorithme MD5 est comme un filigrane infalsifiable.

Activité de TP

Exercice: Configuration de l'authentification OSPF

Dans ce TP, les étudiants vont configurer l'authentification sous OSPF (Open Shortest Path First).

Activité de TP

Activité en ligne: Configuration de l'authentification OSPF

Au cours de ce TP, l'étudiant va configurer un système d'adressage IP pour une zone OSPF, configurer et vérifier le routage OSPF, puis instaurer l'authentification OSPF dans la zone.

2.3 Configuration d'une zone unique OSPF

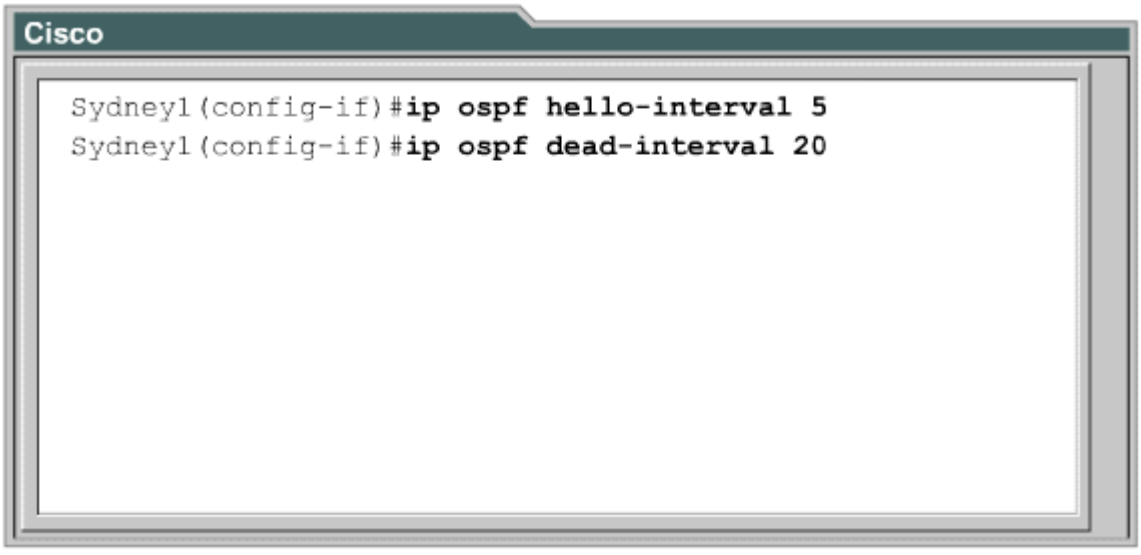
2.3.5 Configuration des compteurs OSPF

Les routeurs OSPF doivent disposer des mêmes intervalles HELLO et des mêmes intervalles d'arrêt (dead) pour échanger des informations. Par défaut, l'intervalle d'arrêt est quatre fois plus long que l'intervalle HELLO. Cela signifie que le routeur aurait l'opportunité d'effectuer quatre envois de paquet HELLO avant d'être déclaré arrêté.

Sur les réseaux OSPF avec diffusion, l'intervalle HELLO par défaut est de 10 secondes et l'intervalle d'arrêt par défaut de 40 secondes. Sur les réseaux sans diffusion, l'intervalle HELLO par défaut est de 30 secondes et l'intervalle d'arrêt par défaut de 120 secondes. Ces valeurs par défaut garantissent un bon fonctionnement de l'OSPF et ont rarement besoin d'être modifiées.

L'administrateur réseau est autorisé à choisir ces valeurs de compteur. Leur modification doit être justifiée par une amélioration des performances du réseau OSPF ou encore, afin de permettre l'interopérabilité d'équipement provenant de plusieurs manufacturiers différents. Ces compteurs doivent être synchronisés avec ceux des routeurs voisins.

Pour configurer les intervalles HELLO et les intervalles d'arrêt sur une interface, utilisez les commandes suivantes: 1



Les compteurs OSPF sont configurés sur l'interface.

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

Activité de TP

Exercice: Configuration des compteurs OSPF

L'objectif de ce TP est de configurer les compteurs OSPF.

Activité de TP

Activité en ligne: Configuration des compteurs OSPF

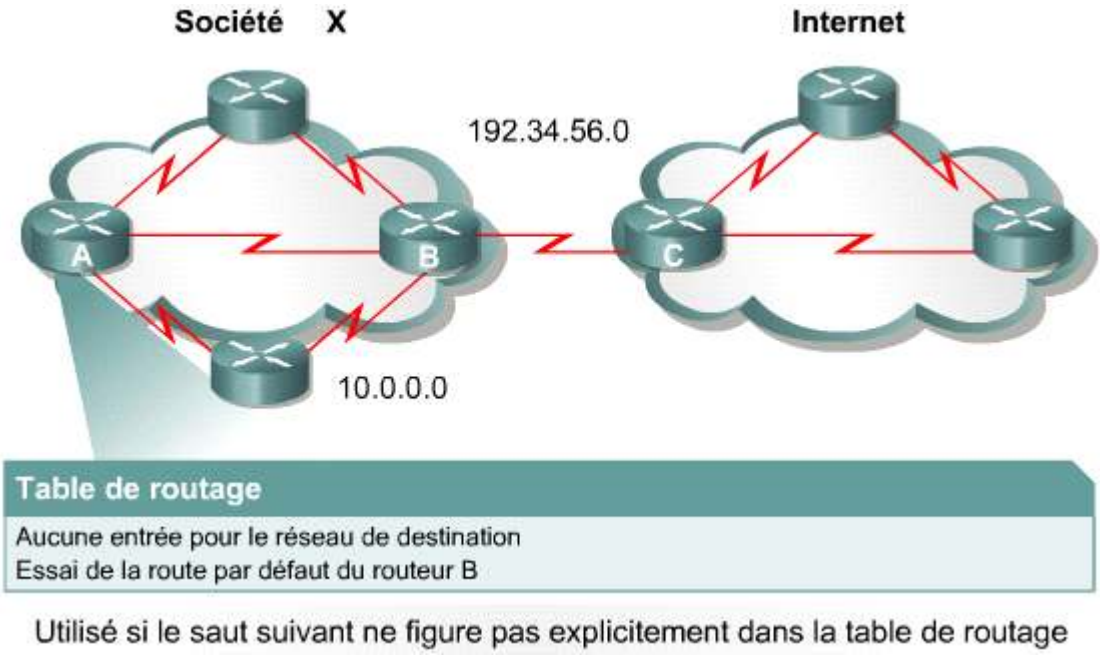
Au cours de ce TP, l'étudiant va régler les compteurs OSPF pour maximiser l'efficacité du réseau.

2.3 Configuration d'une zone unique OSPF

2.3.6 OSPF, propagation d'une route par défaut

Le routage OSPF garantit des chemins exempts de boucles vers chaque réseau du domaine. Pour atteindre des réseaux à l'extérieur du domaine, l'OSPF doit connaître le réseau ou posséder une route par défaut. Pour inclure une entrée pour chaque réseau existant dans le monde, un routeur devrait disposer de ressources énormes.

Il existe heureusement un alternative pratique qui consiste à ajouter une route par défaut au routeur OSPF connecté au réseau extérieur. Cette route peut être redistribuée à chaque routeur du système autonome au travers de mises à niveau OSPF normales. [1]



Une route par défaut configurée est utilisée par un routeur pour générer une passerelle de dernier recours. La syntaxe de configuration de route statique par défaut utilise l'adresse 0.0.0.0 de réseau et un masque de sous-réseau 0.0.0.0:

```
Router(config)#ip route 0.0.0.0 0.0.0.0 [interface | adresse-du-saut-suivant]
```

C'est ce que l'on appelle une route à quatre zéros. Elle peut mapper n'importe quelle adresse de réseau en utilisant la règle suivante. La passerelle de réseau est déterminée en effectuant une opération ET logique sur la destination du paquet avec le masque de sous-réseau.

L'instruction de configuration suivante propagera cette route à tous les routeurs situés dans une zone OSPF normale:

```
Router(config-router)#default-information originate
```

Tous les routeurs de la zone OSPF prendraient connaissance d'une route par défaut à condition que l'interface du routeur périphérique à la passerelle par défaut soit active.

Activité de TP

Exercice: Propagation de routes par défaut dans un domaine OSPF

L'objectif de ce TP est de configurer un système d'adressage IP pour une zone OSPF.

Activité de TP

Activité en ligne: Propager des informations de route par défaut dans un domaine OSPF

Au cours de ce TP, l'étudiant va configurer le réseau OSPF pour que tous les hôtes de la zone OSPF puissent se connecter à des réseaux extérieurs.

2.3 Configuration d'une zone unique OSPF

2.3.7 Problèmes de configuration OSPF fréquents

Pour pouvoir échanger des informations de routage, un routeur OSPF doit établir une relation de voisinage ou de contiguïté avec un autre routeur OSPF. L'incapacité à établir une relation de voisinage peut être due à l'une des raisons suivantes: 1

- Les HELLO ne sont pas envoyés par les deux voisins.
- Les compteurs d'intervalles HELLO et d'intervalles d'arrêt ne sont synchronisés.
- Les interfaces se trouvent sur des types de réseau différents.
- Les mots de passe ou les clés d'authentification sont différents.

Dans le routage OSPF, il est également important de vérifier les points suivants:

- Toutes les interfaces ont une adresse et un masque de sous-réseau corrects.
- Les instructions **`network area`** ont des masques génériques appropriés.
- Les instructions **`network area`** placent les interfaces dans la zone correcte.

Absence de voisin	Routes OSPF non affichées
Les interfaces ont-elles les mêmes compteurs OSPF ?	L'adresse IP et le masque de sous-réseau des interfaces sont-ils corrects ?
Les interfaces connectées ont-elles le même type de réseau ?	Les instructions réseau ont-elles des masques génériques corrects ?
Les clés d'authentification et les mots de passe sont-ils identiques sur les interfaces ?	Les instructions réseau placent-elles les liaisons dans la zone appropriée ?
Les routeurs voisins ont-ils des adresses IP en double ?	
L'interface du routeur est-elle activée ?	

2.3 Configuration d'une zone unique OSPF

2.3.8 Vérification de la configuration OSPF

Un certain nombre de commandes show sont disponibles pour vérifier la configuration OSPF. La figure 1

Commande	Description
`show ip protocol`	Affiche des paramètres sur les compteurs, les filtres, les métriques, les réseaux et d'autres informations sur le routeur dans sa globalité.
`show ip route`	Affiche les routes connues du routeur et la manière dont elles ont été apprises. Il s'agit d'une des meilleures méthodes de détermination de la connectivité entre le routeur local et le reste de l'interréseau.
`show ip ospf interface`	Vérifie que les interfaces ont été configurées dans les zones appropriées. Si aucune adresse d'essai en mode bouclé n'est spécifiée, l'interface dont l'adresse est la première dans la hiérarchie est utilisée comme ID de routeur. Indique également les intervalles de compteur, y compris l'intervalle HELLO, et précise les contiguïtés.
`show ip ospf`	Indique le nombre d'exécutions de l'algorithme du plus court chemin d'abord (SPF). Indique également l'intervalle de mise à jour des états de liens, en supposant qu'aucun changement de topologie ne survienne.
`show ip ospf neighbor detail`	Affiche la liste détaillée des équipements voisins, leur priorité et leur état (par exemple : init, exstart ou full).
`show ip ospf database`	Affiche le contenu de la base de données topologique mise à jour par le routeur. Cette commande indique également l'ID du routeur et l'ID du processus OSPF. Un certain nombre de types de base de données peut être affiché avec cette commande par le biais de mots-clés. Reportez-vous à www.cisco.com pour plus de détails sur les mots-clés.

répertorie ces commandes. La figure 2

Commande	Description
`clear ip route *`	Efface toutes les routes de la table de routage
`clear ip route a.b.c.d`	Efface toutes les routes vers a.b.c.d dans la table de routage
`debug ip ospf events`	Signale tous les événements OSPF
`debug ip ospf adj`	Signale tous les événements de contiguïté OSPF

présente les commandes utiles pour le dépannage de l'OSPF.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Les caractéristiques du routage à état de liens
- Comment les informations de routage à état de liens sont mises à jour
- L'algorithme de routage à état de liens
- Les avantages et les inconvénients du protocole à état de liens
- Le routage à état de liens comparé au routage à vecteur de distance
- La terminologie de l'OSPF
- Les différences entre les protocoles de routage à vecteur de distance et à état de liens
- Les différents types de réseau OSPF
- Le fonctionnement de l'algorithme du plus court chemin d'abord (SPF)
- Le protocole HELLO de l'OSPF
- Les étapes de base du fonctionnement de l'OSPF
- L'activation de l'OSPF sur un routeur
- La configuration d'une adresse en mode bouclé pour définir la priorité d'un routeur
- Le paramétrage de la préférence de route OSPF par modification de la métrique de coût

- La configuration de l'authentification OSPF
- La modification des compteurs OSPF
- La création et la propagation d'une route par défaut
- L'utilisation des commandes **show** pour vérifier le fonctionnement de l'OSPF

Résumé

• Les protocoles de routage à état de liens collectent les informations de routage de tous les autres routeurs du réseau ou d'une zone définie du réseau.
- Les protocoles de routage à état de liens effectuent les opérations suivantes :
- Ils répondent rapidement aux changements du réseau.
- Ils envoient des mises à jour déclenchées uniquement par les modifications de réseau.
- Ils envoient des mises à jour périodiques appelées actualisations d'état de liens.
- Ils utilisent un mécanisme HELLO pour déterminer l'accessibilité des voisins.

• Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens basé sur des normes ouvertes.

• Le routage OSPF fait appel à la notion de zone. Chaque routeur contient une base de données complète des états de liens dans une zone spécifique.

Vue d'ensemble

Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) est un protocole de routage propriétaire développé par Cisco qui est basé sur le protocole IGRP (Interior Gateway Routing Protocol).

Contrairement à l'IGRP, qui est un protocole de routage par classes, l'EIGRP prend en charge le routage CIDR (classless interdomain routing), permettant ainsi aux concepteurs de réseaux de maximiser l'espace d'adressage en utilisant cette technique ainsi que le VLSM (masque de sous-réseau de longueur variable). Par rapport à l'IGRP, l'EIGRP offre une convergence plus rapide, une évolutivité améliorée et un traitement plus efficace des boucles de routage.

De plus, l'EIGRP peut remplacer le protocole RIP (Routing Information Protocol) de Novell et RTMP (AppleTalk Routing Table Maintenance Protocol), procurant ainsi aux réseaux IPX et AppleTalk une efficacité élevée.

L'EIGRP est souvent décrit comme un protocole de routage hybride, offrant le meilleur des algorithmes à vecteur de distance et à état de liens.

C'est un protocole de routage avancé qui repose sur des fonctions couramment associées aux protocoles de routage à état de liens. Certaines des meilleures fonctions de l'OSPF, telles que les mises à jour partielles et la découverte du voisinage réseau, sont également mises à profit dans l'EIGRP. Cependant, ce dernier est plus rapide à configurer que l'OSPF.

L'EIGRP est un choix idéal pour les grands réseaux multiprotocoles construits principalement à base de routeurs Cisco.

Le présent module décrit les tâches de configuration courantes du protocole EIGRP. Il met particulièrement l'accent sur la façon dont l'EIGRP établit des relations avec des routeurs adjacents, calcule des routes principales et des routes de secours et réagit aux éventuelles défaillances sur les routes connues vers une destination donnée.

Un réseau est constitué de nombreux équipements, protocoles et médias qui permettent à la communication de données de s'effectuer. Lorsqu'un élément du réseau ne fonctionne pas correctement, un ou deux utilisateurs peuvent être dans l'impossibilité de communiquer, ou le réseau tout entier peut tomber en panne. Dans un cas comme dans l'autre, l'administrateur réseau doit identifier et dépanner rapidement les problèmes lorsqu'ils surviennent. Les problèmes réseau proviennent souvent des facteurs suivants:

- Commandes incorrectement tapées
- Listes de contrôle d'accès incorrectement construites ou incorrectement placées
- Routeurs, commutateurs ou autres équipements de réseau mal configurés
- Mauvaises connexions physiques

L'administrateur réseau doit aborder le dépannage de manière méthodique, en utilisant un modèle de résolution de problèmes général. Il est souvent utile de vérifier en premier lieu les problèmes de la couche physique, avant de remonter les couches de

façon organisée. Bien que ce module se concentre sur le dépannage des protocoles de routage qui fonctionnent au niveau de la couche 3, il est important d'éliminer tout problème pouvant exister au niveau des couches inférieures.

À la fin de ce module, les étudiants doivent être en mesure de:

- Décrire les différences entre les protocoles EIGRP et IGRP
- Décrire les concepts clés, les technologies et les structures de données de l'EIGRP
- Comprendre la convergence EIGRP et le fonctionnement de base de l'algorithme DUAL (Diffusing Update Algorithm)
- Effectuer une configuration EIGRP de base
- Configurer le résumé de routes EIGRP
- Décrire les processus utilisés par l'EIGRP pour construire et mettre à jour des tables de routage
- Vérifier les opérations EIGRP
- Décrire les huit étapes du processus de dépannage général
- Appliquer un processus logique au dépannage du routage
- Dépanner un processus de routage RIP à l'aide des commandes **show** et **debug**
- Dépanner un processus de routage IGRP à l'aide des commandes **show** et **debug**
- Dépanner un processus de routage EIGRP à l'aide des commandes **show** et **debug**
- Dépanner un processus de routage OSPF à l'aide des commandes **show** et **debug**

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
3.1	Concepts EIGRP
3.2	Configuration EIGRP
3.3	Dépannage des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des • Configuration d'un routeur en vue de fonctionnalités d'administration supplémentaires • Création d'une configuration initiale sur un routeur	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
• Sélection d'un protocole de routage approprié d'après les besoins des utilisateurs	• Configuration de protocoles de routage d'après les besoins des • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes • Configuration d'un routeur en vue de fonctionnalités d'administration supplémentaires	• Dépannage de protocoles de routage	• Évaluation des caractéristiques des protocoles de routage

3.1 Protocole EIGRP

3.1.1 Comparaison entre les protocoles EIGRP et IGRP

En 1994, Cisco a lancé l'EIGRP, une version évolutive et améliorée de son protocole de routage à vecteur de distance propriétaire, l'IGRP. La technologie à vecteur de distance utilisée pour le protocole IGRP est la même que celle du protocole EIGRP ; les données de distance sous-jacentes restent inchangées.

L'EIGRP améliore considérablement les propriétés de convergence et l'efficacité d'exploitation par rapport à l'IGRP. Cela permet de bénéficier d'une architecture améliorée tout en conservant l'investissement existant en IGRP.

La comparaison des protocoles EIGRP et IGRP se fonde sur les catégories majeures suivantes:

- le mode de compatibilité,
- le calcul de métrique,
- le nombre de sauts,
- la redistribution automatique de protocole,
- l'étiquetage de route.

L'IGRP et l'EIGRP sont compatibles entre eux. Cette compatibilité fournit une interopérabilité transparente avec les routeurs IGRP. Elle permet aux utilisateurs de tirer parti des avantages des deux protocoles. À la différence de l'IGRP, L'EIGRP offre la prise en charge multiprotocoles.

Les deux protocoles utilisent des calculs de métrique différents. Du fait qu'il utilise une métrique de 32 bits de longueur, et non de 24 bits comme l'IGRP, L'EIGRP multiplie la valeur de la métrique de l'IGRP par 256. En multipliant ou en divisant par 256, l'EIGRP peut facilement échanger des informations avec l'IGRP. 1

Les protocoles EIGRP et IGRP utilisent la formule de calcul de métrique suivante :
- métrique = [K1 * bande passante + (K2 * bande passante) / 256 - charge) + (K3 * délai)] * [K5/(fiabilité + K4)]

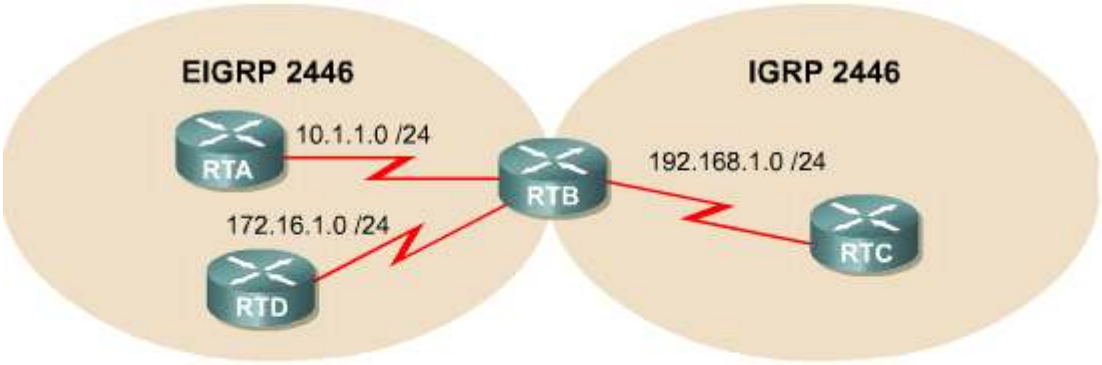
Les valeurs constantes par défaut sont les suivantes :
- K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0
- métrique = bande passante + délai

Lorsque K4 et K5 = 0, la partie [K5/(fiabilité+ K4)] de l'équation n'est pas prise en compte dans la métrique. Ainsi, avec les valeurs constantes par défaut, l'équation de la métrique est : Bande passante + Délai.

IGRP et EIGRP utilisent les équations suivantes pour déterminer les valeurs utilisées dans le calcul de la métrique (notez que pour EIGRP, la valeur est multipliée par 256) :
- bande passante pour IGRP = (10000000/bande passante)
- bande passante pour EIGRP = (10000000/bande passante) * 256
- délai pour IGRP = délai/10
- délai pour EIGRP = (délai/10) * 256

L'IGRP prend en un charge un nombre maximum de sauts de 255. L'EIGRP se limite à 224 sauts, mais cela est plus que suffisant pour les interréseaux les plus vastes correctement conçus.

Pour faire partager l'information à des protocoles de routage aussi différents que l'OSPF et le RIP, il faut une configuration avancée. Des fonctions telles que la redistribution et le partage des routes, s'effectuent automatiquement entre l'IGRP et l'EIGRP tant que les deux processus utilisent le même numéro de système autonome (AS). Dans la figure 2, RTB redistribue automatiquement les routes acquises par l'EIGRP au système autonome IGRP, et vice versa.




```
RTB(config)#router igrp 2446
RTB(config-router)#network 192.168.1.0
RTB(config)#router eigrp 2446
RTB(config-router)#network 10.1.1.0
RTB(config-router)#network 172.16.1.0
```

Les protocoles EIGRP et IGRP redistribuent automatiquement les routes entre les systèmes autonomes qui portent le même numéro.

L'EIGRP étiquettera comme externes les routes acquises auprès d'IGRP ou d'une autre source extérieure, car elles ne proviennent pas de routeurs EIGRP. L'IGRP ne peut faire la différence entre les routes internes et les routes externes.

Notez que dans les informations affichées par la commande **`show ip route`** pour les routeurs de la figure 3, les routes EIGRP sont étiquetées «D», et les routes externes «EX». RTA fait la différence entre le réseau acquis via l'EIGRP (172.16.0.0) et le réseau qui a été redistribué à partir de l'IGRP (192.168.1.0). Dans la table RTC, le protocole IGRP ne fait pas cette distinction. RTC, qui exécute uniquement l'IGRP, voit uniquement les routes IGRP, malgré le fait que 10.1.1.0 et 172.16.0.0 ont été redistribués à partir de l'EIGRP.

```
RTA#show ip route
<Affichage tronqué>
C    10.1.1.0 is directly connected, Serial0
D    172.16.1.0 [90/2681856] via 10.1.1.1, Serial0
D EX 192.168.1.0 [170/2681856] via 10.1.1.1,
00:00:04, Serial0
```

```
RTC#show ip route
<Affichage tronqué>
C    192.168.1.0 is directly connected, Serial0
I    10.0.0.0 [100/10476] via 192.168.1.1,
00:00:04, Serial0
I    172.16.0.0 [100/10476] via 192.168.1.1,
00:00:04, Serial0
```

Activité de média interactive

Case à cocher: Protocoles de routage IGRP et EIGRP

À la fin de cette activité, l'étudiant sera en mesure de différencier les protocoles IGRP et EIGRP.

3.1 Protocole EIGRP

3.1.2 Concepts et terminologie de l'EIGRP

Afin de pouvoir réagir rapidement aux changements, les routeurs EIGRP stockent les informations de topologie et de route en mémoire RAM. À l'instar de l'OSPF, l'EIGRP enregistre ces informations dans diverses tables et bases de données.

Il enregistre les routes apprises de manière spécifique. Chaque route reçoit un état particulier et peut être étiquetée pour fournir des informations utiles supplémentaires.

L'EIGRP met à jour trois tables:

- la table de voisinage,
- la table topologique,
- la table de routage.

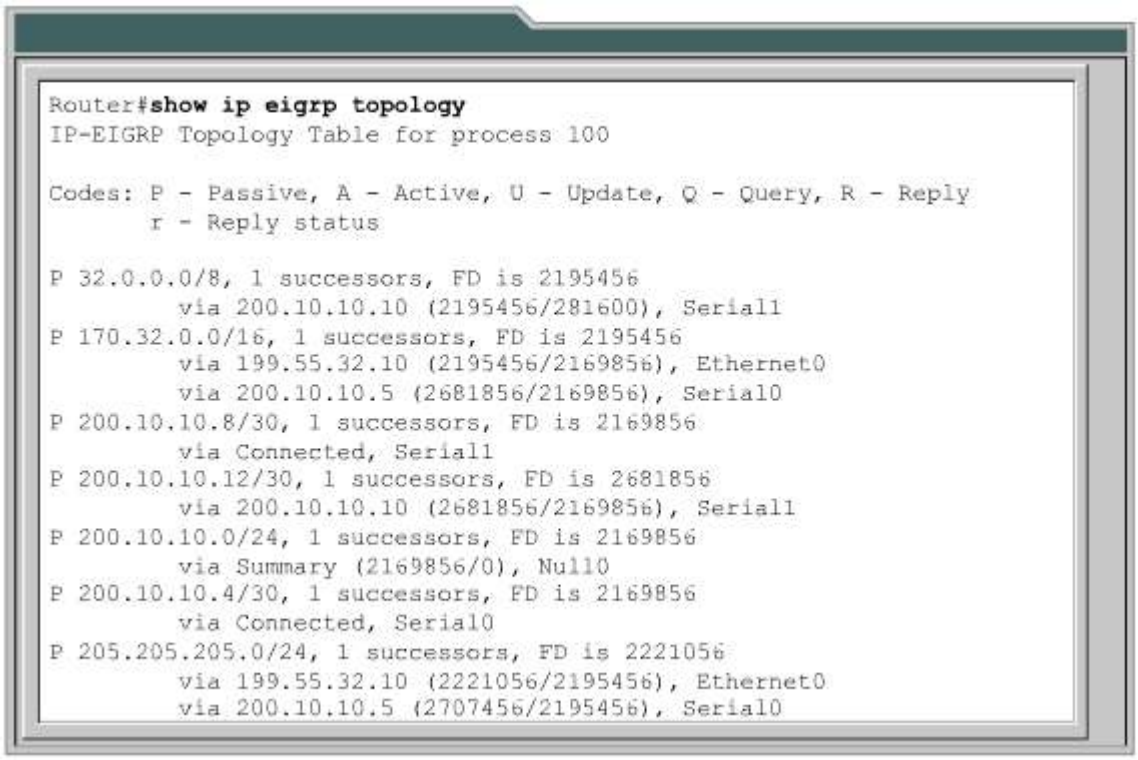
La table de voisinage est la table la plus importante de l'EIGRP. Chaque routeur EIGRP tient à jour une table de voisinage qui répertorie les routeurs adjacents. Cette table est comparable à la base de données de contiguïté utilisée par l'OSPF. Il y a une table de voisinage pour chaque protocole pris en charge par l'EIGRP. 1

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
M   Address         Interface Hold Uptime  SRTT  RTO  Q   SEQ
                              (sec)        (ms)      CNT NUM
2   200.10.10.10    Se1       13 00:19:09  26   200  0   10
1   200.10.10.5     Se0       12 03:31:36  50   300  0   39
0   199.55.32.10    Et0       11 03:31:40  10   200  0   40
```

Lorsque des voisins nouvellement découverts sont acquis, l'adresse et l'interface du voisin sont enregistrées. Ces informations sont stockées dans la structure de données de voisinage. Lorsqu'un voisin envoie un paquet HELLO, il annonce un délai de conservation. Ce délai et le laps de temps pendant lequel un routeur considère son voisin accessible et opérationnel. Autrement dit, si un paquet HELLO n'est pas détecté pendant le délai de conservation, celui-ci expire. Au moment de l'expiration, le DUAL (Diffusing Update Algorithm), algorithme à vecteur de distance de l'EIGRP, est informé du changement de topologie et doit recalculer la nouvelle topologie.

La table topologique est constituée de toutes les tables de routage EIGRP du système autonome. L'algorithme DUAL extrait les informations fournies dans la table de voisinage et dans la table topologique et calcule les routes de moindre coût vers chaque destination. 2 En analysant ces informations, les routeurs EIGRP peuvent identifier rapidement d'autres routes et les emprunter. Les informations que l'algorithme DUAL fournit au routeur sont utilisées pour déterminer la route successeur, c'est-à-dire la route principale ou la meilleure route. Une copie est également insérée dans la table topologique.

Chaque routeur EIGRP tient à jour une table topologique pour chaque protocole réseau configuré. Toutes les routes apprises jusqu'à une destination sont conservées dans la table topologique. 2

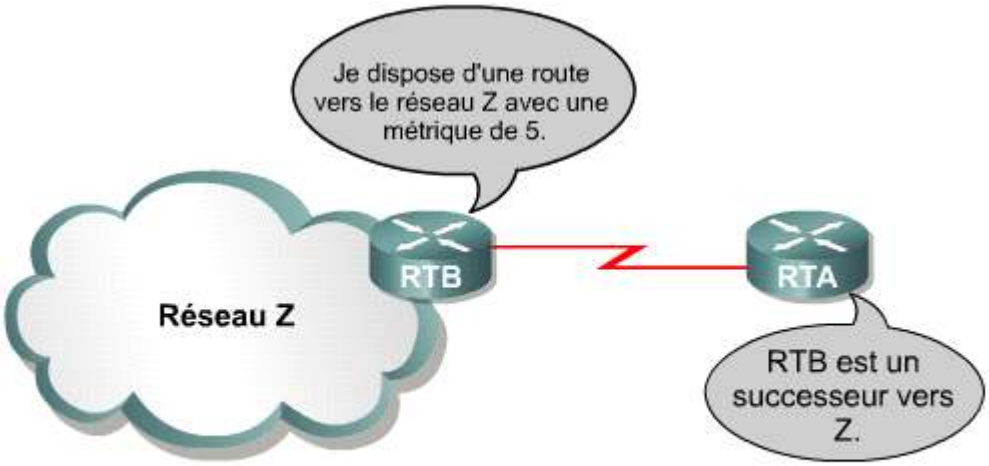


```
Router#show ip eigrp topology
IP-EIGRP Topology Table for process 100

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply
       r - Reply status

P 32.0.0.0/8, 1 successors, FD is 2195456
         via 200.10.10.10 (2195456/281600), Serial1
P 170.32.0.0/16, 1 successors, FD is 2195456
         via 199.55.32.10 (2195456/2169856), Ethernet0
         via 200.10.10.5 (2681856/2169856), Serial0
P 200.10.10.8/30, 1 successors, FD is 2169856
         via Connected, Serial1
P 200.10.10.12/30, 1 successors, FD is 2681856
         via 200.10.10.10 (2681856/2169856), Serial1
P 200.10.10.0/24, 1 successors, FD is 2169856
         via Summary (2169856/0), Null0
P 200.10.10.4/30, 1 successors, FD is 2169856
         via Connected, Serial0
P 205.205.205.0/24, 1 successors, FD is 2221056
         via 199.55.32.10 (2221056/2195456), Ethernet0
         via 200.10.10.5 (2707456/2195456), Serial0
```

La table topologique inclut les champs suivants:

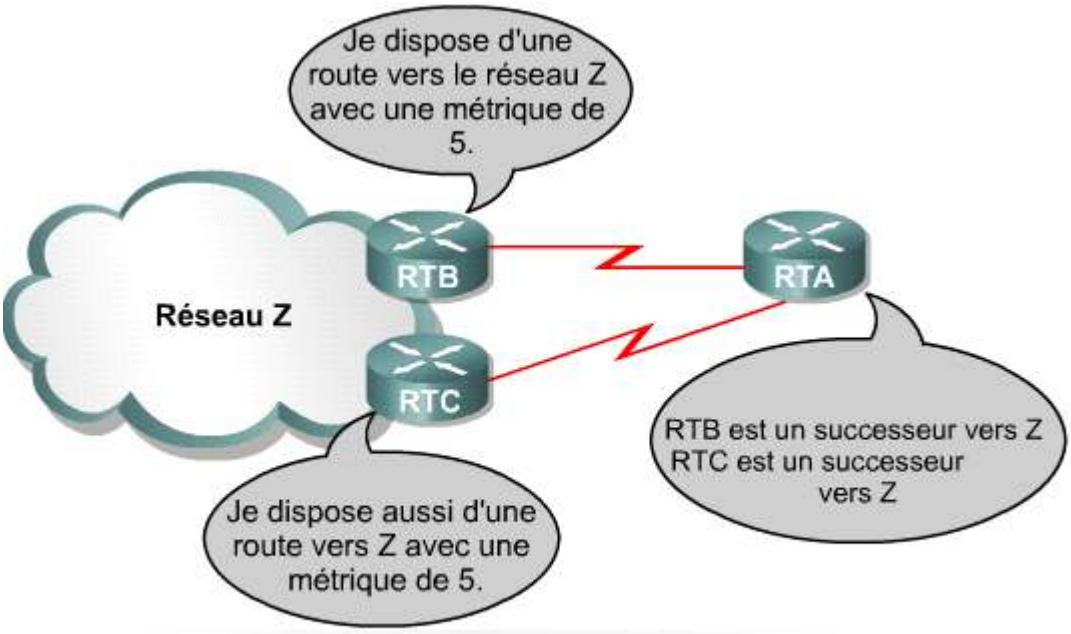
- **Distance possible (FD)** – La distance possible (FD, acronyme de Feasible Distance) est la métrique calculée la plus faible vers chaque destination. Par exemple, la distance possible jusqu'à 32.0.0.0 est 2195456**.**.
- **Source de la route (via 200.10.10.10)** – La source de la route est le numéro d'identification du routeur qui a initialement annoncé cette route. Ce champ est uniquement renseigné pour les routes apprises en externe auprès du réseau EIGRP. L'étiquetage de route peut se révéler particulièrement utile avec un routage basé sur des politiques. Par exemple la source de la route qui mène à 32.0.0.0 est 200.10.10.10 via 200.10.10.10.
- **Distance annoncée (RD)** – La distance annoncée (RD, acronyme de Reported Distance) du chemin est celle annoncée par un voisin adjacent jusqu'à une destination spécifique. Par exemple, la distance annoncée jusqu'à 32.0.0.0 est /281600 comme l'indique (2195456/281600).
- **Informations d'interface** – L'interface permettant d'atteindre la destination
- **État de la route** – Une route est identifiée comme étant soit passive (P), c'est-à-dire stables et prêtes à l'utilisation, soit active (A), ce qui signifie qu'elle va être recalculée par l'algorithme DUAL.

La table de routage EIGRP contient les meilleures routes vers une destination donnée. Ces informations sont extraites de la table topologique. Chaque routeur EIGRP tient à jour une table de routage pour chaque protocole de réseau.



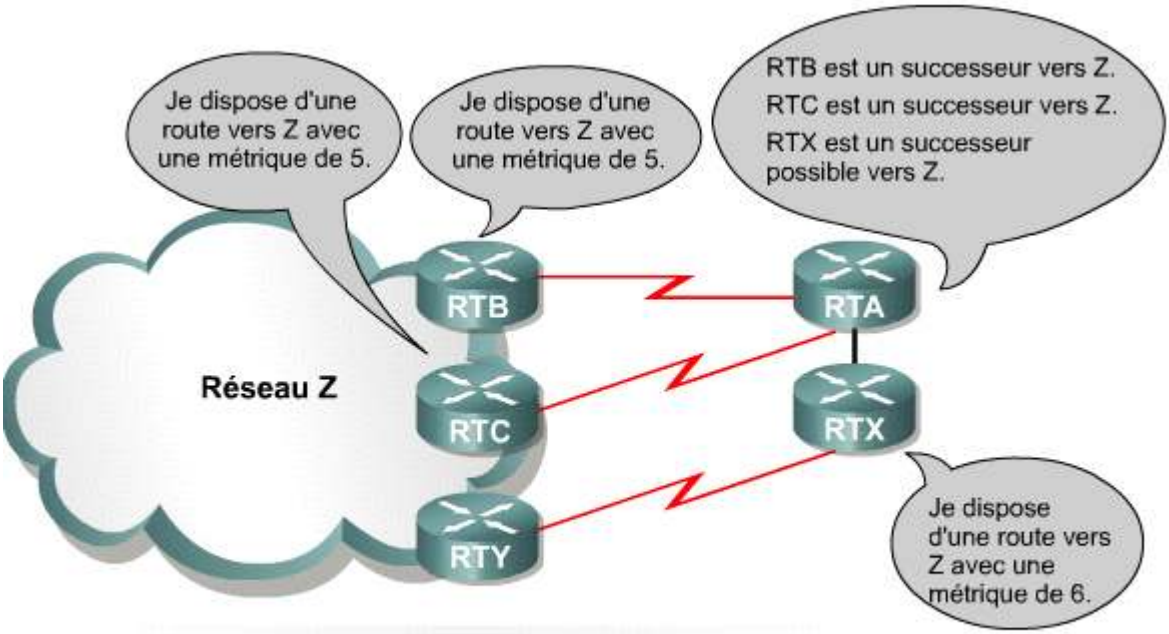
Un successeur est un routeur voisin qui représente l'étape suivante vers une destination donnée en utilisant un chemin sans boucle au coût minimal.

Une route successeur est une route sélectionnée comme route principale à utiliser pour atteindre une destination. 3 À l'aide des informations contenues dans la table de voisinage et la table topologique, l'algorithme DUAL identifie cette route puis l'insère dans la table de routage. Il peut y avoir jusqu'à quatre routes successeur pour une route particulière. Ces routes peuvent être de coût égal ou différent et elles sont identifiées comme les meilleurs chemins exempts de boucles vers une destination donnée. Une copie des routes successeur est également insérée dans la table topologique.



RTA peut installer plusieurs successeurs si ces voisins annoncent des routes avec la même métrique.

Une route successeur possible (FS) est une route de secours. 4 Ces routes sont identifiées en même temps que les routes successeur, mais elles ne sont conservées que dans la table topologique. Bien que cela ne soit pas obligatoire, il est possible de conserver plusieurs routes successeur dans la table topologique. 5



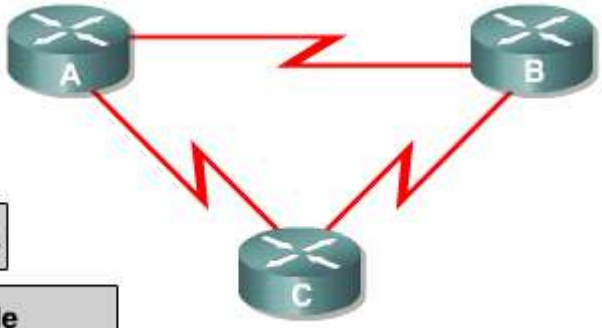
En identifiant des successeurs possibles, les routeurs EIGRP peuvent installer immédiatement d'autres routes en cas d'échec d'un successeur.

Un routeur voit ses routes successeur possibles comme des voisins en aval, c'est-à-dire plus proches que lui de la destination. Le coût de la route successeur possible se calcule sur la base du coût annoncé du routeur voisin vers la destination. Si une route successeur est interrompue, le routeur cherchera une route successeur possible identifiée. Cette route sera promue à l'état de successeur. Une route successeur possible doit avoir un coût annoncé inférieur à celui de la route successeur existante vers la destination. S'il n'est pas possible d'identifier une route successeur possible avec les informations existantes, le routeur place un état Actif sur une route et envoie des paquets de requête à tous les voisins afin de recalculer la topologie actuelle. Le routeur peut identifier toute route successeur ou route successeur possible à l'aide des nouvelles données reçues dans les paquets de réponse. Le routeur place alors un état Passif sur la route.

La table topologique peut enregistrer des informations supplémentaires sur chaque route. L'EIGRP classifie les routes comme internes ou externes. Il ajoute une étiquette de route à chaque route pour déterminer cette classification. Les routes internes partent de l'intérieur du système autonome EIGRP.

Les routes externes partent de l'extérieur du système autonome EIGRP. Les routes apprises ou redistribuées des autres protocoles de routage, tels que le RIP (Routing Information Protocol), l'OSPF et l'IGRP sont externes. Les routes statiques qui proviennent de l'extérieur du système autonome EIGRP sont externes. L'étiquette peut être configurée avec un numéro compris entre 0 et 255. 6 7

```
RTX#show ip eigrp topology 204.100.50.0
IP-EIGRP topology entry for 204.100.50.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s),
FD is 2297856
  Routing Descriptor Blocks:
  10.1.0.1 (Serial0), from 10.1.0.1, Send flag is 0x0
      Composite metric is (2297856/128256), Route is External
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 25000 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
      External data:
        Originating router is 192.168.1.1
        AS number of route is 0
        External protocol is Connected, external metric is 0
        Administrator tag is 0 (0x00000000)
```



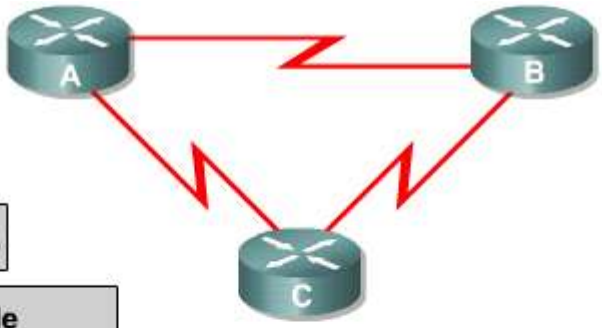
Protocole A

Routeur A Table de voisinage

Routeur A Table topologique

Fenêtre contextuelle (pop up)

Étape 1 - Le routeur A génère des informations sur le protocole A des voisins.



Protocole A

Routeur A Table de voisinage

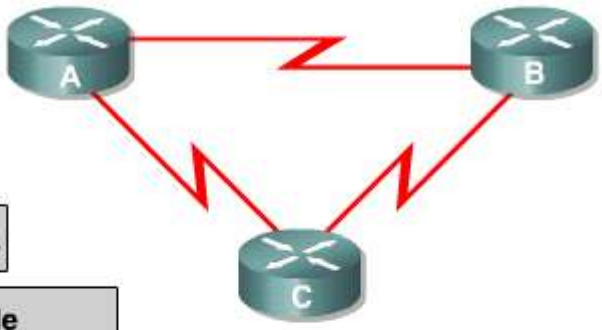
Informations du routeur B

Routeur A Table topologique

Informations du routeur B

Fenêtre contextuelle (pop up)

Étape 1 - Le routeur A génère des informations sur le protocole A des voisins.



Protocole A

Routeur A Table de voisinage

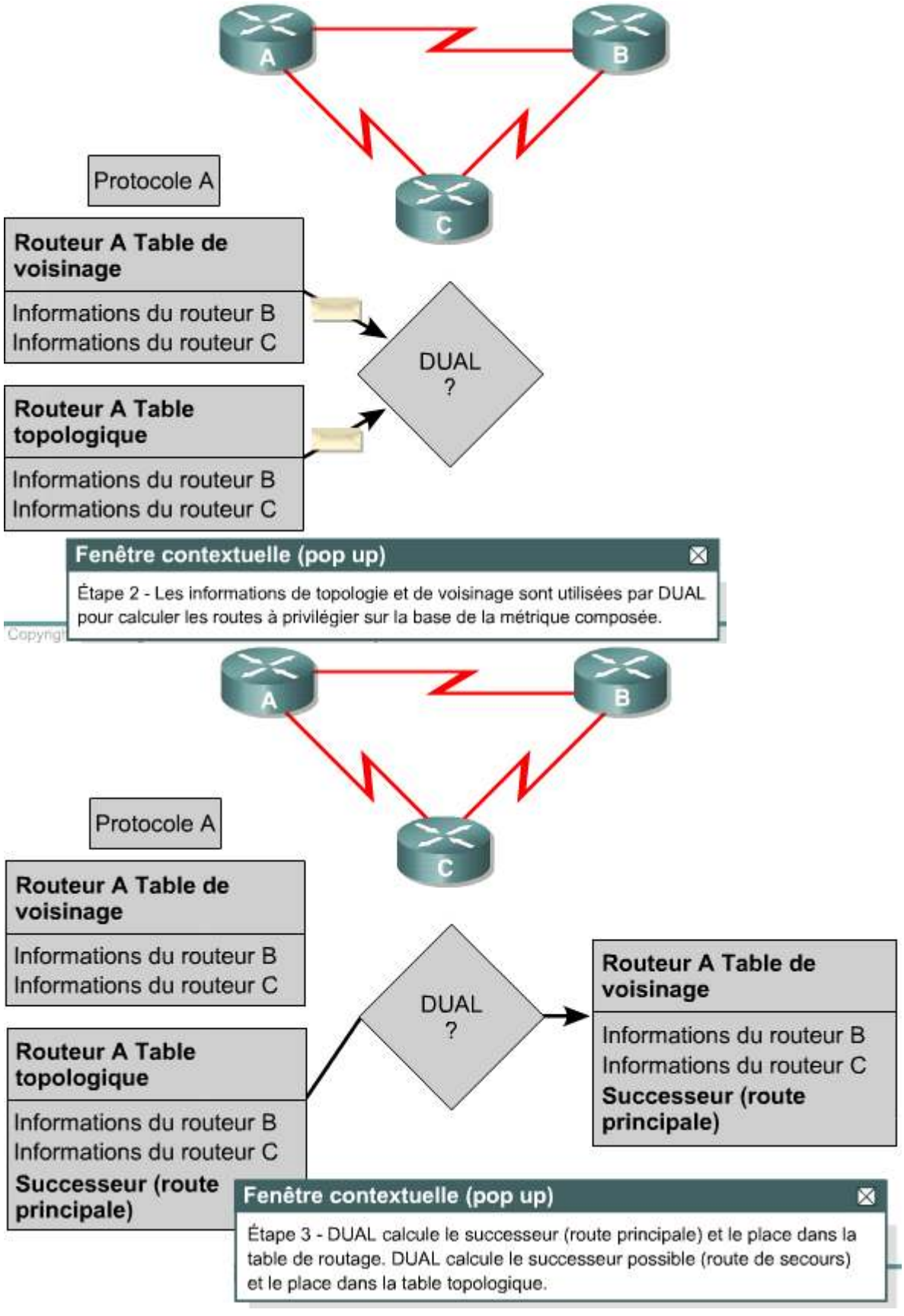
Informations du routeur B
Informations du routeur C

Routeur A Table topologique

Informations du routeur B
Informations du routeur C

Fenêtre contextuelle (pop up)

Étape 1 - Le routeur A génère des informations sur le protocole A des voisins.



3.1 Protocole EIGRP

3.1.3 Caractéristiques de conception du protocole EIGRP

L'EIGRP fonctionne assez différemment de l'IGRP. L'EIGRP est un protocole de routage à vecteur de distance avancé qui joue le rôle d'un protocole à état de liens lors de la mise à jour des voisins et de la gestion des informations de routage. Par rapport aux protocoles à vecteur de distance simples, l'EIGRP offre notamment les avantages suivants: [1]

- une convergence rapide,
- une utilisation efficace de la bande passante,
- la prise en charge de la technique VLSM (variable-length subnet) et du routage CIDR (classless interdomain routing). Contrairement à l'IGRP, l'EIGRP offre la prise en charge totale d'IP sans classe en échangeant les masques de sous-réseau dans les mises à jour de routage.
- la prise en charge multiple de la couche réseau,
- l'indépendance vis à vis des protocoles routés Des modules dépendant des protocoles (PDM) protègent l'EIGRP des longues révisions. Les protocoles routés évolutifs, tels qu'IP, peuvent requérir un nouveau module de protocole, mais pas nécessairement une refonte de l'EIGRP proprement dit.

Les routeurs EIGRP convergent rapidement car ils reposent sur l'algorithme DUAL. Cet algorithme garantit à tout instant un fonctionnement exempt de boucles grâce à un calcul de route qui permet à tous les routeurs concernés par le changement topologique de se synchroniser de façon simultanée.

L'EIGRP utilise la bande passante de façon rationnelle en envoyant des mises à jour partielles et limitées, et sa consommation est minime lorsque le réseau est stable. Les routeurs EIGRP effectuent des mises à jour partielles et incrémentielles, plutôt que d'envoyer leurs tables en entier. C'est un fonctionnement similaire à celui de l'OSPF, mais contrairement aux routeurs OSPF, les routeurs EIGRP envoient ces mises à jour partielles uniquement aux routeurs qui ont besoin de l'information, et pas à tous les routeurs d'une zone. C'est pour cela que l'on utilise le terme de mises à jour limitées. Plutôt que d'utiliser des mises à jour de routage temporisées, les EIGRP gardent le contact à l'aide de petits paquets HELLO. Bien qu'ils soient échangés régulièrement, les paquets HELLO consomment une part négligeable de la bande passante.

L'EIGRP prend en charge IP, IPX et AppleTalk à travers des modules dépendant des protocoles (PDM). L'EIGRP peut redistribuer les informations IPX, Novell RIP et SAP pour améliorer les performances globales. En effet, il peut relayer ces trois protocoles. En effet, il peut relayer ces deux protocoles. Un routeur EIGRP recevra des mises à jour de routage et de service, ne mettant à jour les autres routeurs que lors de changements dans les SAP ou les tables de routage. Les mises à jour de routage se produisent comme dans n'importe quel réseau EIGRP, en utilisant des mises à jour partielles.

L'EIGRP peut également remplacer le protocole RTMP (AppleTalk Routing Table Maintenance Protocol). En tant que protocole de routage à vecteur de distance, le RTMP repose sur des échanges périodiques et complets des informations de routage. Pour réduire la charge, l'EIGRP redistribue les informations de routage AppleTalk à l'aide de mises à jour pilotées par événement. L'EIGRP utilise également une métrique composée configurable afin de déterminer la meilleure route vers un réseau AppleTalk. Le RTMP utilise le nombre de sauts, ce qui peut rendre le routage inefficace. Étant donné que les clients AppleTalk attendent des informations RTMP des routeurs locaux, l'EIGRP pour AppleTalk ne devrait être exécuté que sur un réseau sans client, comme une liaison WAN (wide-area network).

3.1 Protocole EIGRP

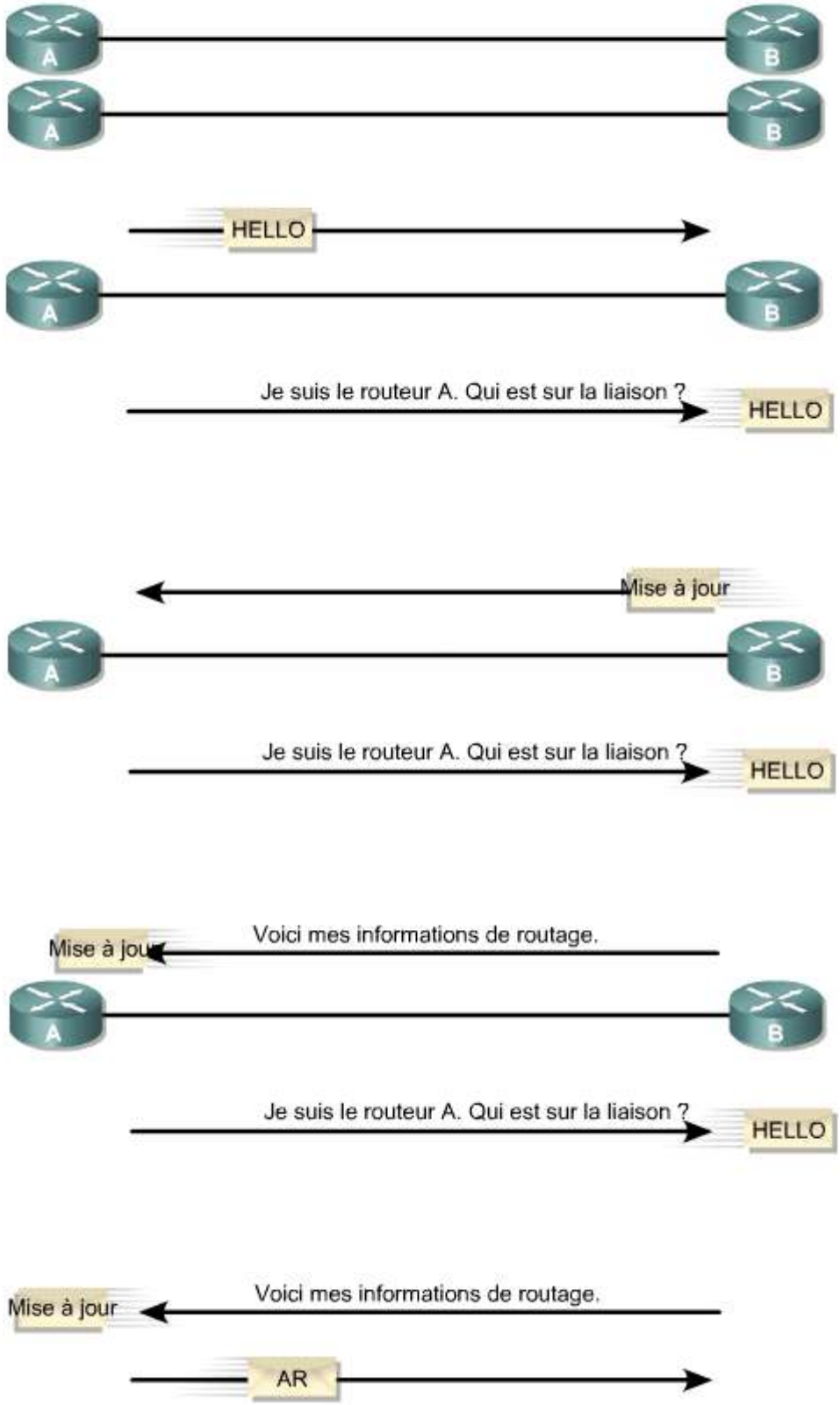
3.1.4 Technologies EIGRP

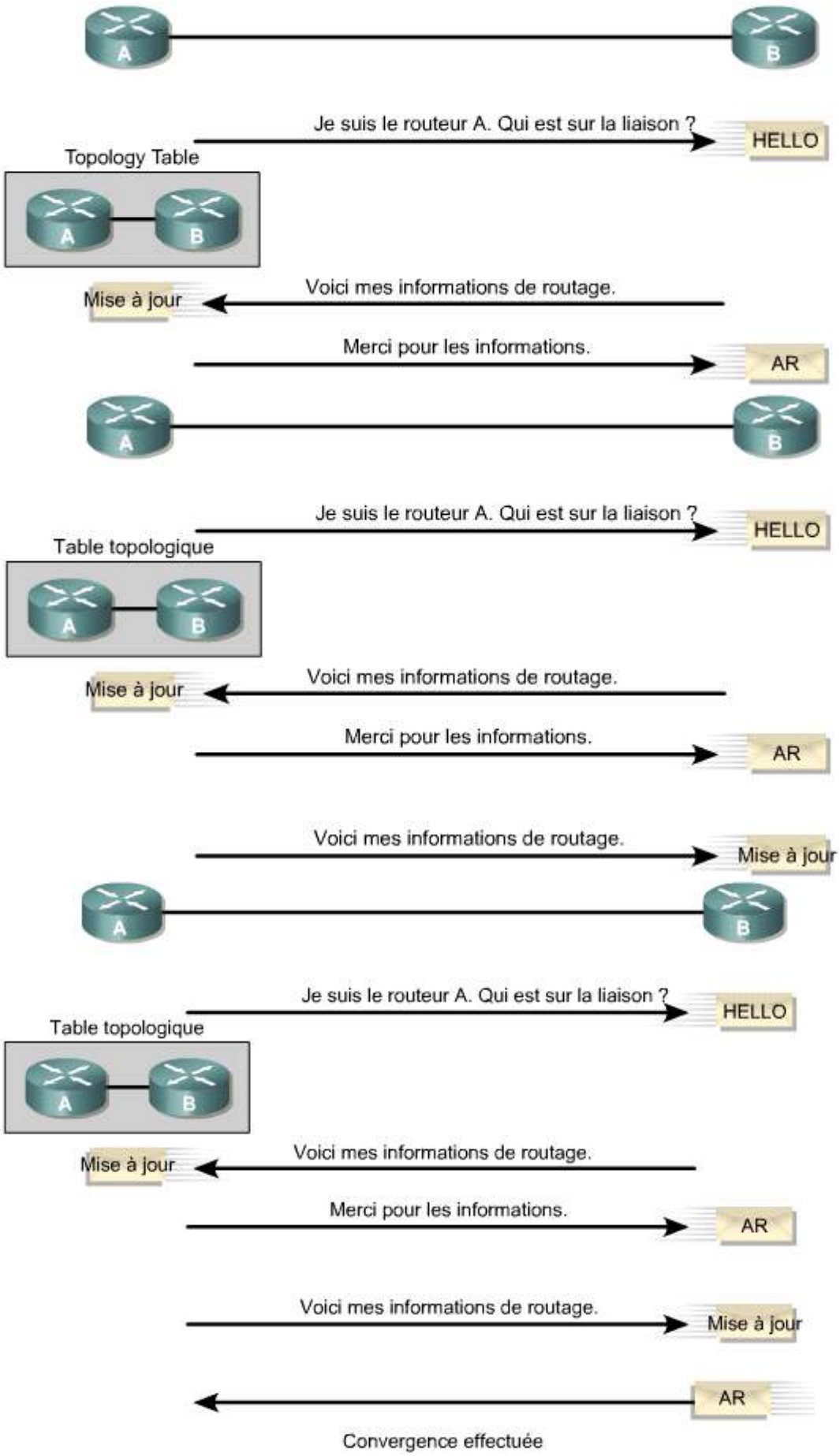
L'EIGRP inclut un bon nombre de nouvelles technologies, chacune représentant une amélioration sur le plan de l'efficacité d'exploitation, de la vitesse de convergence ou de la fonctionnalité par rapport à l'IGRP et aux autres protocoles de routage. Ces technologies peuvent être classées dans l'une des catégories suivantes:

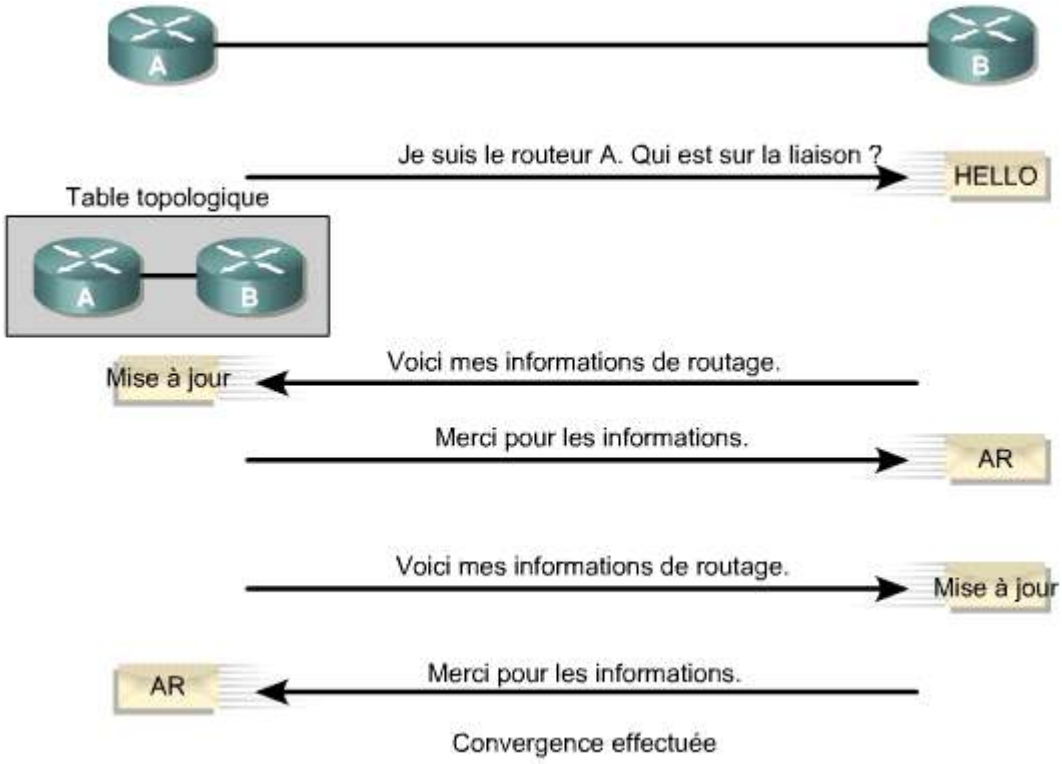
- Découverte et récupération de voisinage
- Protocole de transport fiable
- Algorithme de machine à états finis DUAL
- Modules dépendant du protocole

Les routeurs à vecteur de distance simples n'établissent aucune relation avec leurs voisins. Les routeurs RIP et IGRP effectuent seulement une diffusion de broadcast ou de multicast des mises à jour sur les interfaces configurées. En revanche, les routeurs EIGRP établissent de façon active des relations avec leurs voisins, d'une façon très similaire aux routeurs OSPF.

Les routeurs EIGRP établissent des contiguïtés comme l'illustre la figure 1.


A
B
A
B
HELLO
A
B
Je suis le routeur A. Qui est sur la liaison ?
HELLO
Mise à jour
A
B
Je suis le routeur A. Qui est sur la liaison ?
HELLO
Voici mes informations de routage.
Mise à jou
A
B
Je suis le routeur A. Qui est sur la liaison ?
HELLO
Voici mes informations de routage.
Mise à jour
AR


A
B
Je suis le routeur A. Qui est sur la liaison ?
HELLO
Topology Table
A
B
Mise à jour
Voici mes informations de routage.
Merci pour les informations.
AR
A
B
Je suis le routeur A. Qui est sur la liaison ?
HELLO
Table topologique
A
B
Mise à jour
Voici mes informations de routage.
Merci pour les informations.
AR
Voici mes informations de routage.
Mise à jour
A
B
Je suis le routeur A. Qui est sur la liaison ?
HELLO
Table topologique
A
B
Mise à jour
Voici mes informations de routage.
Merci pour les informations.
AR
Voici mes informations de routage.
Mise à jour
AR
Convergence effectuée



Les routeurs EIGRP établissent des contiguïtés avec des routeurs voisins en utilisant des petits paquets HELLO. Ces paquets sont envoyés par défaut toutes les cinq secondes. Un routeur EIGRP suppose que tant qu'il reçoit des paquets HELLO des voisins connus, ces derniers et leurs routes restent praticables ou passifs. Pour former des contiguïtés, les routeurs EIGRP procèdent comme suit:

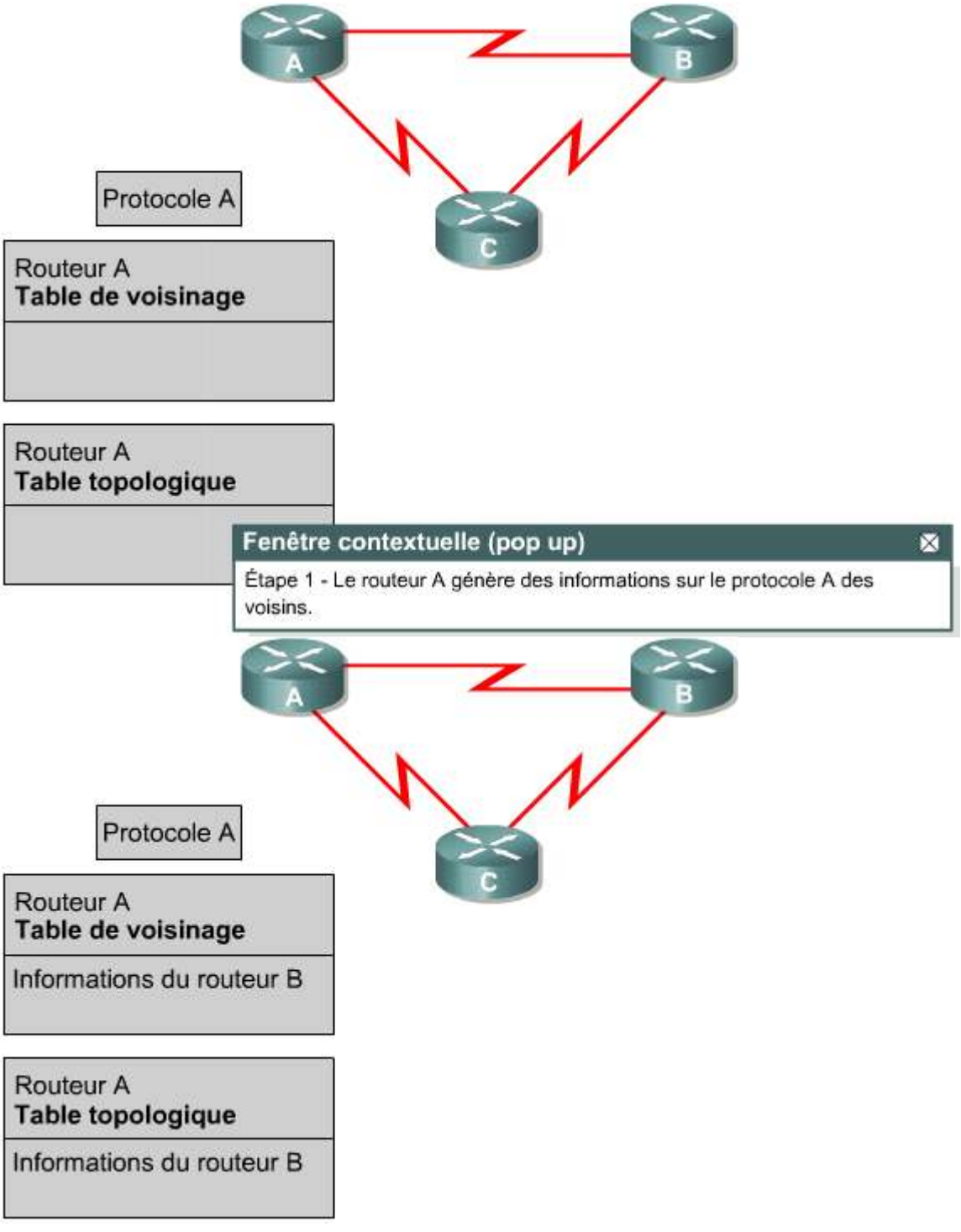
- Ils prennent connaissance de façon dynamique des nouvelles routes qui relient leur réseau
- Ils identifient les routeurs qui deviennent inaccessibles ou inutilisables
- Ils redécouvrent les routeurs qui étaient précédemment inaccessibles

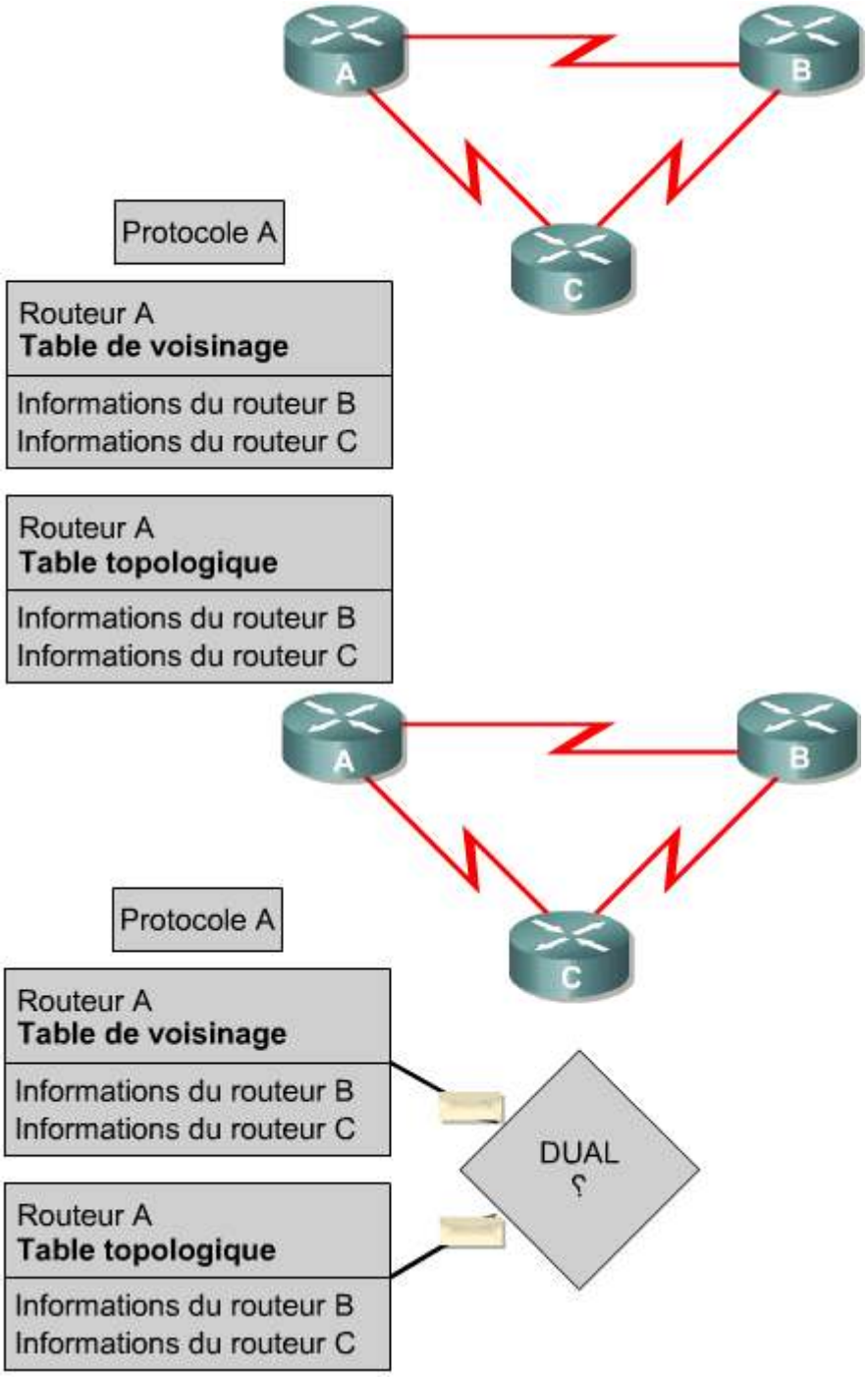
Le RTP (Reliable Transport Protocol) est un protocole de la couche transport qui peut garantir la livraison ordonnée des paquets EIGRP à tous les voisins. Sur un réseau IP, les hôtes utilisent TCP pour séquencer les paquets et garantir leur livraison en temps voulu. Cependant, l'EIGRP est indépendant des protocoles. Cela signifie qu'il ne dépend pas du TCP/IP pour échanger des informations de routage comme le font les protocoles RIP, IGRP et OSPP. Pour rester indépendant d'IP, l'EIGRP utilise RTP comme son propre protocole de couche de transport propriétaire pour assurer la livraison des informations de routage.

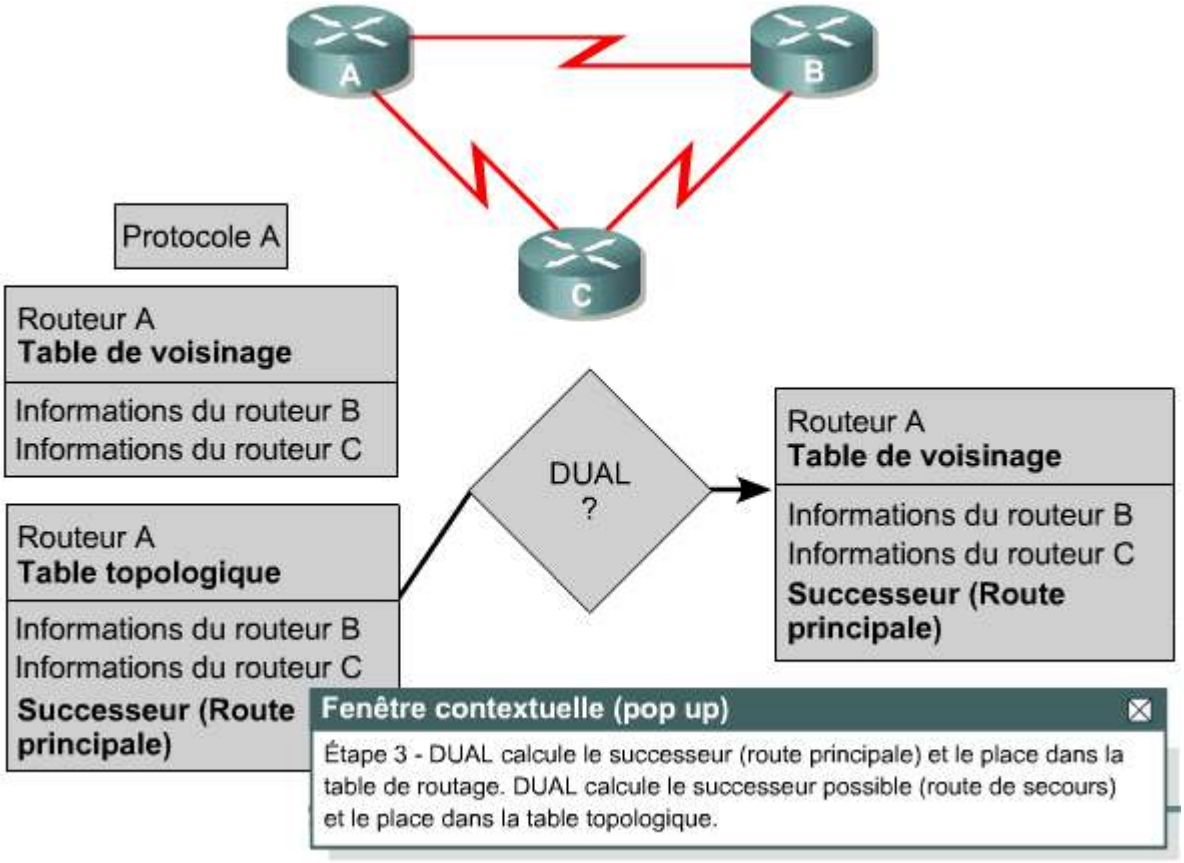
L'EIGRP peut faire appel à RTP pour fournir un service fiable ou non fiable selon la situation. Par exemple, les paquets HELLO ne nécessitent pas la surcharge de la livraison fiable car ils sont envoyés fréquemment et sont de taille limitée. Toutefois, la livraison fiable des autres informations de routage peut accélérer la convergence, parce que les routeurs EIGRP n'attendent pas l'expiration d'un compteur pour retransmettre.

Avec RTP, l'EIGRP peut diffuser un multicast et un unicast à différents homologues de façon simultanée, d'où une efficacité maximale.

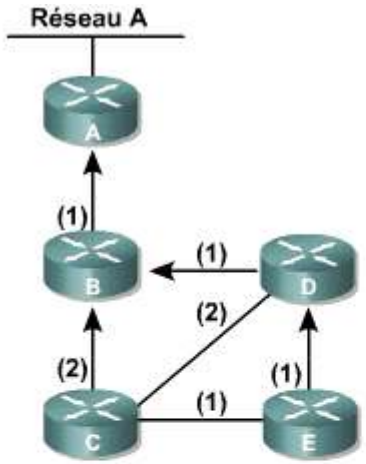
La pièce maîtresse de l'EIGRP est l'algorithme DUAL (Diffusing Update Algorithm), qui est le moteur de calcul de route de ce protocole. Le nom entier de cette technologie est «DUAL finite-state machine» (FSM). Un FSM est un système algorithmique non lié au matériel. Les FSM définissent un ensemble d'états possibles que peut prendre un objet, les événements à l'origine de ces états et les événements résultant de ces états. Les concepteurs utilisent des FSM pour décrire comment un matériel, un programme informatique ou un algorithme de routage vont réagir à un ensemble d'événements donnés. Le système DUAL FSM contient toute la logique permettant de calculer et comparer des routes dans un réseau EIGRP.


A
B
C
Protocole A
Routeur A
Table de voisinage
Routeur A
Table topologique
Fenêtre contextuelle (pop up)
Étape 1 - Le routeur A génère des informations sur le protocole A des voisins.
A
B
C
Protocole A
Routeur A
Table de voisinage
Informations du routeur B
Routeur A
Table topologique
Informations du routeur B


A
B
C
Protocole A
Routeur A
Table de voisinage
Informations du routeur B
Informations du routeur C
Routeur A
Table topologique
Informations du routeur B
Informations du routeur C
A
B
C
Protocole A
Routeur A
Table de voisinage
Informations du routeur B
Informations du routeur C
Routeur A
Table topologique
Informations du routeur B
Informations du routeur C
DUAL



L'algorithme DUAL analyse toutes les routes annoncées par les voisins. Les métriques composées de chaque route sont utilisées pour les comparer. 2 3 Il garantit également que chaque chemin est exempt de boucles. Il insère des chemins de moindre coût dans la table de routage. Ces routes principales sont appelées routes successeur. Une copie des routes successeur est également insérée dans la table topologique.



Numéros entre () = métrique

C EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via B	3	1	(Successor)
via D	4	2	(FS)
via E	4	3	

D EIGRP	FD	RD	Topologie
Réseau A	2		(FD)
via B	2	1	(Successor)
via C	5	3	

E EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via D	3	2	(Successor)
via C	4	3	

Légende	
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

L'EIGRP conserve les informations importantes sur les routes et la topologie dans un table de voisinage ou une table topologique. Ces tables fournissent à l'algorithme DUAL des informations de route complètes en cas d'interruption du

réseau. L'algorithme sélectionne rapidement d'autres routes en se basant sur les informations de ces tables. Si un lien est interrompu, DUAL recherche un autre chemin, ou route successeur possible, dans la table topologique.

L'une des caractéristiques les plus intéressantes de l'EIGRP est sa conception modulaire. Ce type de conception en couches s'avère être des plus évolutives et des plus adaptables. Grâce aux PDM, la prise en charge des protocoles routés, comme IP, IPX et AppleTalk est incluse dans l'EIGRP. Théoriquement, l'EIGRP peut s'adapter facilement aux protocoles routés nouveaux ou révisés, tels que IPv6, par simple ajout de modules dépendant des protocoles.

Chaque PDM se charge de toutes les fonctions liées à son protocole routé spécifique. Le module IP-EIGRP assure les fonctions suivantes:

- Envoi et réception des paquets EIGRP qui transportent les données IP
- Notification à l'algorithme DUAL des nouvelles informations de routage IP reçues
- Actualisation des résultats des décisions de routage DUAL dans la table de routage IP
- Redistribution des informations de routage qui ont été apprises par d'autres protocoles de routage compatibles IP

3.1 Protocole EIGRP

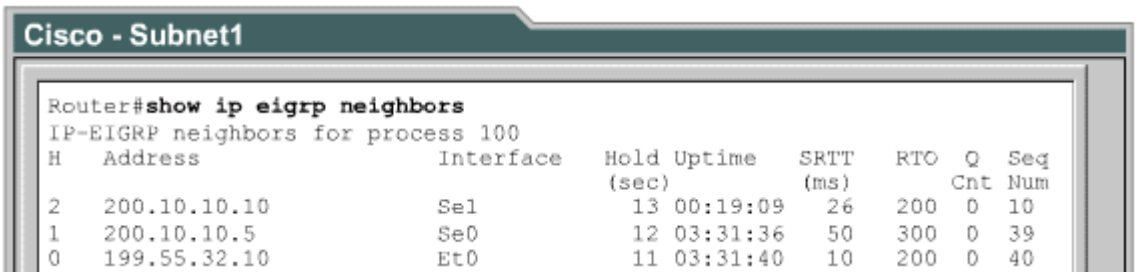
3.1.5 Structure de données EIGRP

Comme l'OSPF, l'EIGRP recourt à différents types de paquets pour mettre à jour ses différentes tables et établir des relations complexes avec les routeurs voisins.

Les cinq types de paquets EIGRP sont les suivants: 1

- HELLO
- Accusé de réception
- Mise à jour
- Requête
- Réponse

EIGRP recourt aux paquets HELLO pour découvrir, vérifier et redécouvrir les routeurs voisins. La redécouverte a lieu si des routeurs EIGRP ne reçoivent aucun HELLO de leur homologue pendant un intervalle de délai de conservation mais rétablissent ensuite la communication. 2



Les routeurs EIGRP envoient des HELLO selon un intervalle fixe mais configurable, appelé intervalle HELLO. L'intervalle HELLO par défaut est fonction de la bande passante de l'interface. 3 Sur les réseaux IP, les routeurs EIGRP envoient des HELLO à l'adresse IP multicast 224.0.0.10.

Bande passante	Exemple de liaison	Intervalle HELLO par défaut	Délai de conservation par défaut
1,544 Mbits/s ou moins	Frame Relay	60 secondes	180 secondes
Supérieure à 1,544 Mbits/s	T1, Ethernet	5 secondes	15 secondes

Un routeur EIGRP stocke des informations sur les voisins dans la table de voisinage. La table de voisinage inclut le champ de numéro de séquence (Seq No) où est enregistré le numéro du dernier paquet EIGRP reçu que chaque voisin a envoyé. La table de voisinage inclut également un champ de délai de conservation qui enregistre l'heure à laquelle le dernier paquet a été reçu. Pour que l'état Passif soit maintenu, les paquets doivent être reçus dans l'intervalle du délai de conservation. L'état Passif est un état accessible et opérationnel.

Si un voisin ne se manifeste pas pendant la durée du délai de conservation, l'EIGRP considère qu'il est défaillant, et l'algorithme DUAL doit alors intervenir pour réévaluer la table de routage. Par défaut, le délai de conservation est de trois fois l'intervalle HELLO, mais l'administrateur peut configurer les deux compteurs selon ses besoins.

L'OSPF requiert que les routeurs voisins possèdent les mêmes intervalles HELLO et d'arrêt pour communiquer. L'EIGRP n'a pas cette restriction. Les routeurs voisins prennent connaissance de chaque compteur respectif en échangeant des paquets HELLO. Ils utilisent ensuite ces informations pour nouer une relation stable en dépit de leurs compteurs différents.

Les paquets HELLO sont toujours envoyés de manière fiable. Cela veut dire qu'aucun accusé de réception n'est transmis.

Un routeur EIGRP utilise des paquets d'accusé de réception pour indiquer la réception de n'importe quel paquet EIGRP au cours d'un échange fiable. Le RTP (Reliable Transport Protocol) peut assurer une communication fiable entre des hôtes EIGRP. Pour être fiable, le message d'un émetteur doit faire l'objet d'un accusé de réception. Les paquets d'accusé de réception, qui sont des paquets HELLO sans données, sont utilisés à cette fin. Contrairement aux HELLO multicast, les paquets d'accusé de réception sont unicast. Il est possible d'envoyer des accusés de réception en les joignant à d'autres types de paquets EIGRP, comme les paquets de réponse.

Les paquets de mise à jour sont utilisés lorsqu'un routeur découvre un nouveau voisin. Un routeur EIGRP envoie des paquets de mise à jour unicast à ce nouveau voisin afin de pouvoir l'ajouter à sa table topologique. Plusieurs paquets de mise à jour peuvent s'avérer nécessaires pour transmettre la totalité des informations topologiques à un voisin nouvellement découvert.

Les paquets de mise à jour sont également utilisés lorsqu'un routeur détecte un changement topologique. Dans ce cas, le routeur EIGRP envoie un paquet de mise à jour multicast à tous les voisins, qui leur signale le changement. Tous les paquets de mise à jour sont envoyés de manière fiable.

Un routeur EIGRP utilise des paquets de requête chaque fois qu'il a besoin d'informations spécifiques sur un ou plusieurs de ses voisins. Un paquet de réponse est utilisé pour répondre à une requête.

Si un routeur EIGRP perd sa route successeur et ne peut pas trouver de route successeur possible pour une route, l'algorithme DUAL place la route à l'état Actif. Une requête est alors envoyée en multicast à tous les voisins afin de tenter de trouver une route successeur vers le réseau de destination. Les voisins doivent répondre en envoyant des informations sur les routes successeur ou indiquer qu'aucune information n'est disponible. Les requêtes peuvent être multicast ou unicast, tandis que les réponses sont toujours unicast. Les deux types de paquets sont envoyés de manière fiable.

3.1 Protocole EIGRP

3.1.6 Algorithme EIGRP

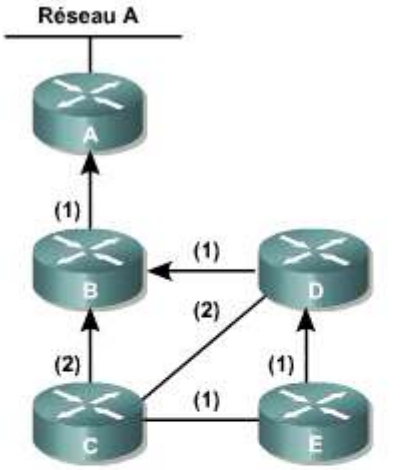
L'algorithme DUAL sophistiqué assure une convergence exceptionnellement rapide de l'EIGRP. Afin de mieux comprendre la convergence avec DUAL, étudiez l'exemple de la figure 1. Chaque routeur a construit une table topologique qui contient des informations sur la manière d'atteindre le réseau de destination A.

Chaque table topologique contient les informations suivantes:

- Le protocole de routage ou EIGRP
- Le coût le plus bas de la route, ou distance possible (FD)
- Le coût de la route tel qu'annoncé par le routeur voisin, ou distance annoncée (RD)

Le titre Topologie indique la route principale préférée, ou route successeur (Successor) et, lorsqu'elle est identifiée, la route de secours, ou route successeur possible (FS). Notez qu'il n'est pas nécessaire d'avoir une route successeur possible identifiée.

Le réseau EIGRP exécute une série d'actions pour faire converger les routeurs, qui disposent actuellement des informations topologiques suivantes: 1



Numéros entre () = métrique

C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D	4	2	(FS)
	via E	4	3	

D	EIGRP	FD	RD	Topologie
Réseau A		2		(FD)
	via B	2	1	(Successeur)
	via C	5	3	

E	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via D	3	2	(Successeur)
	via C	4	3	

Légende	
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

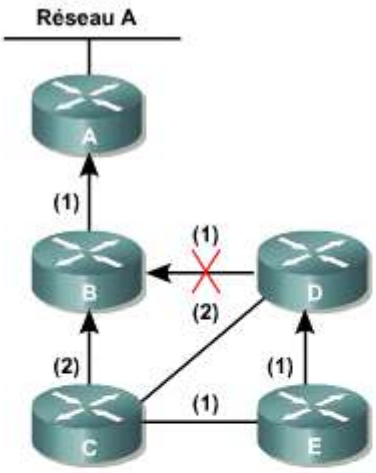
- Le routeur C a une route successeur en passant par le routeur B.
- Le routeur C a une route successeur possible en passant par le routeur D.
- Le routeur D a une route successeur en passant par le routeur B.
- Le routeur D n'a pas de route successeur possible.
- Le routeur E a une route successeur en passant par le routeur D.
- Le routeur E n'a pas de route successeur possible.

Les règles de sélection des routes successeur sont spécifiées à la figure 2.

1. La route successeur possible est une route de secours utilisable en cas de défaillance de la route successeur.
2. La distance RD (distance annoncée) vers la destination, telle qu'elle est annoncée par le routeur voisin, doit être inférieure à la distance FD (distance possible) de la route du successeur principal.
3. Si ce critère est satisfait et s'il n'existe pas de boucle de routage, la route peut être sélectionnée comme route successeur possible.
4. La route successeur possible peut alors être promue au rang de route successeur.
5. Si la distance RD (distance annoncée) de la route alternative est égale ou supérieure à la distance FD (distance possible) du successeur d'origine, la route est rejetée comme route successeur possible.
6. Le routeur doit recalculer la topologie du réseau en collectant des informations pour tous les voisins.
7. Le routeur envoie un paquet de type requête à tous les voisins pour connaître les chemins de routage disponibles et le coût de métrique associé pour le réseau de destination.
8. Tous les routeurs voisins doivent envoyer un paquet en réponse à la requête.
9. Les données reçues sont écrites dans la table topologique du routeur émetteur.
10. DUAL peut alors identifier les routes du nouveau successeur et, le cas échéant, les routes du nouveau successeur possible sur la base de ces nouvelles informations.

L'exemple suivant démontre comment chaque routeur de la topologie appliquera les règles de route successeur possible lorsque la route reliant le routeur D au routeur B sera interrompue:

Dans le routeur D: 3



C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D	4	2	(FS)
	via E	4	3	

D	EIGRP	FD	RD	Topologie
Réseau A		2		(FD)
	~~via B~~	~~2~~	~~1~~	~~(Successeur)~~
	via C	5	3	

E	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via D	3	2	(Successeur)
	via C	4	3	

Légende	
C	Destination
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

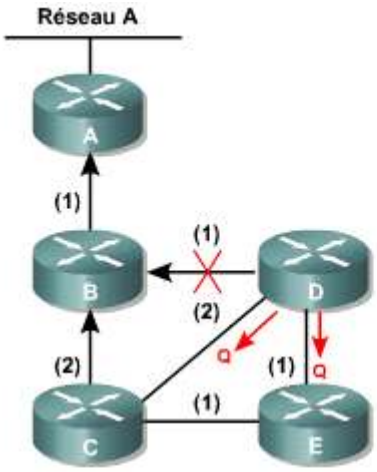
- La route passant par le routeur B est supprimée de la table topologique.
- C'est la route successeur. Le routeur D n'a pas de route successeur possible identifiée.
- Le routeur D doit effectuer un nouveau calcul de route.

Dans le Routeur C:

- La route vers le routeur A passant par le routeur D est interrompue.

- La route passant par le routeur D est supprimée de la table.
- C'est une route successeur possible pour le routeur C.

Dans le routeur D: 4



C EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via B	3	1	(Successeur)
via D			
via E	4	3	

D EIGRP		FD	R	Topologie
Réseau A	**ACTIF**	-1	2	(FD)
via B				(q)
via C		5	3	(q)

E EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
~~via D~~	~~3~~	~~2~~	(Successeur)
via C	4	3	

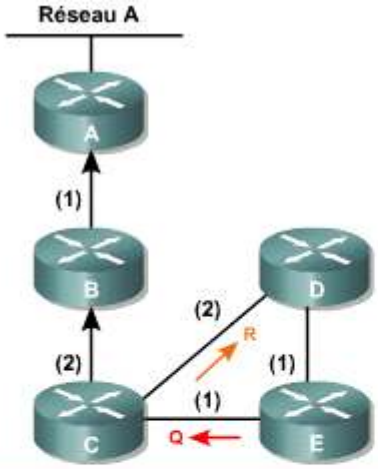
Légende	
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

- Le routeur D n'a pas de route successeur possible. Il ne peut commuter vers une route de secours identifiée.
- Le routeur D doit recalculer la topologie du réseau. Le chemin vers le réseau de destination A est défini à l'état Actif.
- Le routeur D envoie un paquet de requête à tous les voisins connectés, le routeur C et le routeur E, pour leur demander des informations topologiques.
- Le routeur C n'a pas une entrée précédente pour le routeur D.
- Le routeur D n'a pas une entrée précédente pour le routeur E.

Dans le Routeur E:

- La route vers le réseau A passant par le routeur D est interrompue.
- La route passant par le routeur D est mise hors fonction.
- C'est la route successeur pour le routeur E.
- Le routeur E n'a pas de route possible identifiée.
- Notez que le coût de la distance annoncée du routage via le routeur C est 3, soit le même coût que la route successeur passant par le routeur D.

Dans le Routeur C: 5



C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D			
	via E			

D	EIGRP		FD	R	Topologie
Réseau A	**ACTIF**	-1			(FD)
	via B				(q)
	via C		5	3	(q)

E	EIGRP		FD	R	Topologie
Réseau A	**ACTIF**	-1			(FD)
	via D				
	via C		4	3	(q)

Légende	
C	Destination
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

- Le routeur E envoie un paquet de requête au routeur C.
- Le routeur C supprime le routeur E de la table.
- Le routeur C répond au routeur D avec une nouvelle route vers le réseau A.

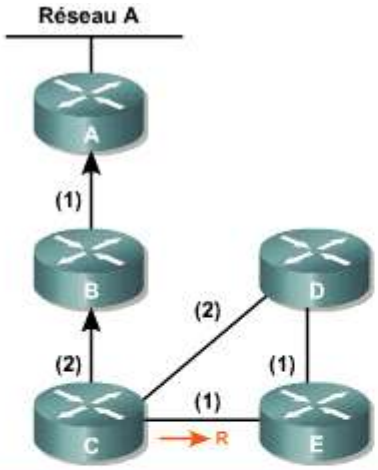
Dans le routeur D:

- L'état de la route vers le réseau de destination A est toujours marqué comme Actif. Le calcul n'est pas encore terminé.
- Le routeur C a répondu au routeur D pour confirmer qu'une route vers le réseau de destination A est disponible au coût de 5.
- Le routeur D attend toujours une réponse du routeur E.

Dans le Routeur E:

- Le routeur E n'a pas de route successeur possible pour atteindre le réseau de destination A.
- Le routeur E, par conséquent, étiquette l'état de la route vers le réseau de destination comme étant Actif.
- Le routeur E devra recalculer la topologie du réseau.
- Le routeur E supprime de la table la route qui passe par le routeur D.
- Le routeur E envoie un requête au routeur C, lui demandant des informations topologiques.
- Le routeur E a déjà une entrée via le routeur C. Son coût de 3 est identique à celui de la route successeur.

Dans le Routeur E: 6



C EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via B	3	1	(Successeur)
via D			
via E			

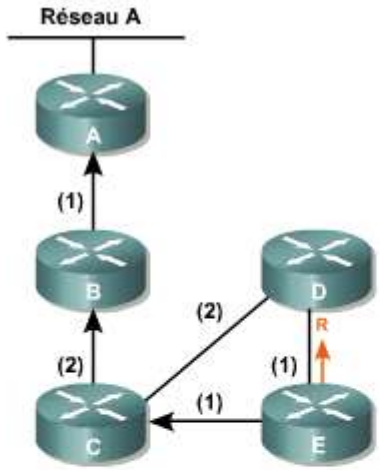
D EIGRP	FD	RD	Topologie
Réseau A **ACTIF**	-1		(FD)
via B			(q)
via C	5	3	

E EIGRP	FD	RD	Topologie
Réseau A **ACTIF**	4		(FD)
via C	4	3	(Successeur)
via D			

Légende	
C	Destination
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

- Le routeur C répond avec une distance signalée de 3.
- Le routeur E peut à présent définir la route passant par le routeur C comme nouvelle route successeur avec une distance possible de 4 et une distance signalée de 3.
- Le routeur E remplace l'état « Actif » de la route vers le réseau de destination A par un état « Passif ». Notez qu'un routeur a un état « Passif » par défaut tant que des paquets HELLO sont reçus. Dans cet exemple, seules les routes dont l'état est «Actif» sont étiquetées.

Dans le Routeur E:



C EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via B	3	1	(Successeur)
via D			
via E			

D EIGRP	FD	RD	Topologie
Réseau A	5		(FD)
via C	5	3	(Successeur)
via E	5	4	

E EIGRP	FD	RD	Topologie
Réseau A	4		(FD)
via C	4	3	(Successeur)
via D			

Légende	
C	Destination
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

- Le routeur E envoie une réponse au routeur D, lui indiquant les informations topologiques du routeur E.

Dans le routeur D:

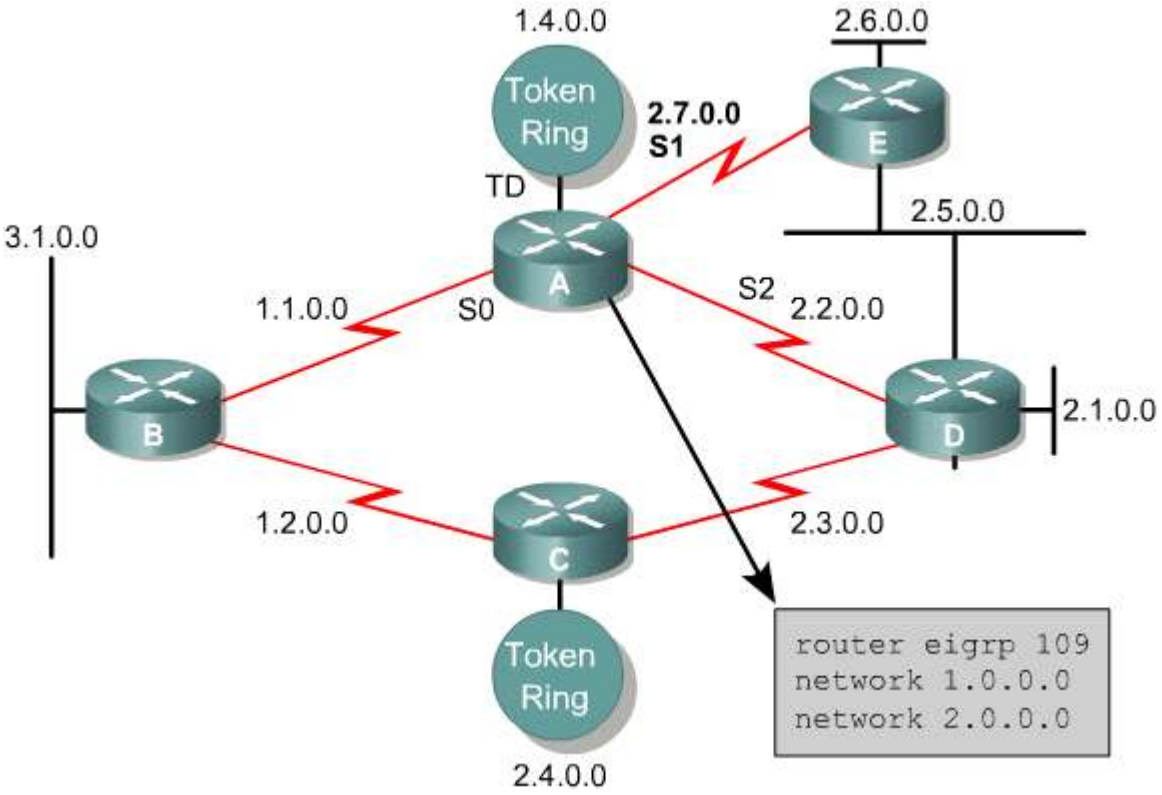
- Le routeur D reçoit le paquet de réponse du routeur E lui indiquant les informations topologiques du routeur E.
- Le Routeur D entre ces données pour la route vers le réseau de destination A passant par le routeur E.
- Cette route devient une route successeur supplémentaire étant donné que son coût est identique au routage passant par le routeur C et que la distance signalée est inférieure au coût de distance possible de 5.

La convergence a été atteinte entre tous les routeurs EIGRP à l'aide de l'algorithme DUAL.

3.2 Configuration EIGRP

3.2.1 Configuration EIGRP

Malgré la complexité de l'algorithme DUAL, la configuration de l'EIGRP peut être relativement simple. Les commandes de configuration EIGRP varient en fonction du protocole qui doit être routé. Il peut s'agir notamment des protocoles IP, IPX et AppleTalk. Cette section présente la configuration d'EIGRP pour le protocole IP. 1



Pour configurer l'EIGRP pour IP, procédez comme suit:

1. Utilisez la commande suivante pour activer EIGRP et définir le système autonome:

   `router(config)#`**`router eigrp`***`numéro-du-système-autonome`*

   Le numéro de système autonome suivant est utilisé pour identifier tous les routeurs qui font partie de l'interréseau. Cette valeur doit correspondre à tous les routeurs au sein de l'interréseau.

2. Spécifiez les réseaux qui appartiennent au système autonome EIGRP sur le routeur local en utilisant la commande suivante:

   `router(config-router)#`**`network`***`numéro-réseau`*

   Le numéro du réseau qui détermine quelles interfaces du routeur participent à l'EIGRP et quels réseaux sont annoncés par le routeur.

La commande **network** configure uniquement des réseaux connectés. Par exemple, le réseau 3.1.0.0, qui se trouve à l'extrémité droite de la figure principale, n'est pas directement connecté au routeur A. Par conséquent, ce réseau ne fait pas partie de la configuration du routeur A.

3. Lors de la configuration de liaisons série à l'aide d'EIGRP, il est important de configurer le paramètre de bande passante sur l'interface. Si la bande passante de ces interfaces n'est pas modifiée, l'EIGRP sélectionne la bande passante par défaut sur la liaison plutôt que la bande passante réelle. Si la liaison est plus lente, le routeur risque de ne pas converger, les mises à jour de routage peuvent de ne pas aboutir et la sélection de chemin peut s'avérer inefficace. Pour définir la bande passante de l'interface, utilisez la syntaxe suivante:

   ```
   router(config-if)#bandwidth kbits/s
   ```

   La commande **bandwidth** est uniquement utilisée par le processus de routage. Vous devez l'utiliser pour définir une vitesse identique à celle de la ligne de l'interface.

4. Cisco recommande également l'ajout des commandes suivantes à toutes les configurations EIGRP:

   ```
   router(config-if)#eigrp log-neighbor-changes
   ```

   Cette commande active la journalisation des changements de contiguïté de voisins pour surveiller la stabilité du système de routage et pour mieux détecter les problèmes.

Activité de TP

Exercice: Configuration du routage EIGRP

Dans ce TP, les étudiants vont configurer le routage EIGRP.

Activité de TP

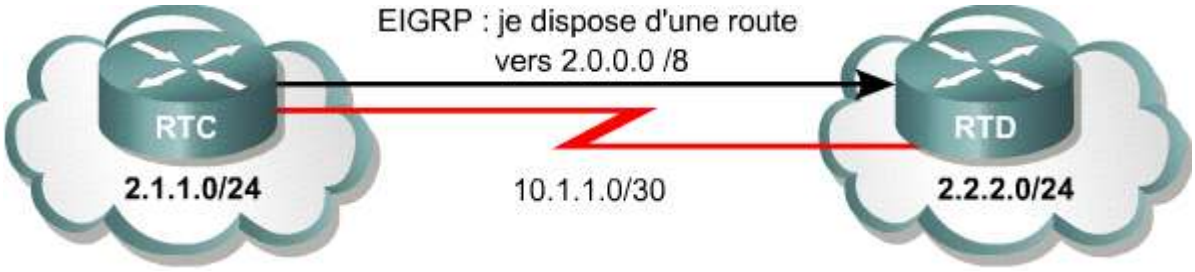
Activité en ligne: Configuration EIGRP

Au cours de ce TP, l'étudiant va configurer le routage EIGRP.

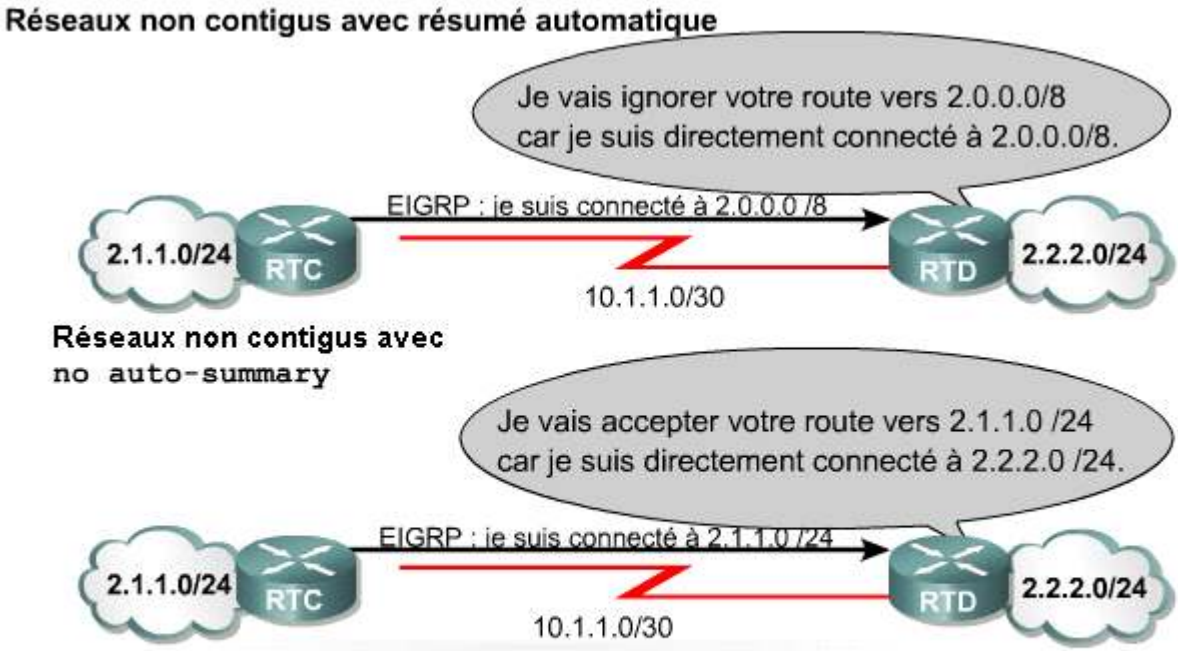
3.2 Configuration EIGRP

3.2.2 Configuration des résumés EIGRP

L'EIGRP résume automatiquement les routes aux frontières de classes. Il s'agit de la frontière où se termine l'adresse réseau, comme défini par l'adressage à base de classes. Cela signifie que même si le RTC est connecté uniquement au sous-réseau 2.1.1.0, il annoncera qu'il est connecté au réseau de Classe A entier, 2.0.0.0. Dans la plupart des cas, la fonction de résumé automatique est avantageuse car elle permet de conserver des tables de routage aussi compactes que possible. 1



Cependant, ce n'est pas toujours la meilleure option. Par exemple, avec certains sous-réseaux non contigus, le résumé automatique doit être désactivé pour que le routage fonctionne correctement. 2



La fonction de résumé automatique empêche les routeurs d'apprendre des informations à propos des sous-réseaux non contigus. Lorsque la fonction de résumé est désactivée, les routeurs EIGRP annoncent des routes aux sous-réseaux.

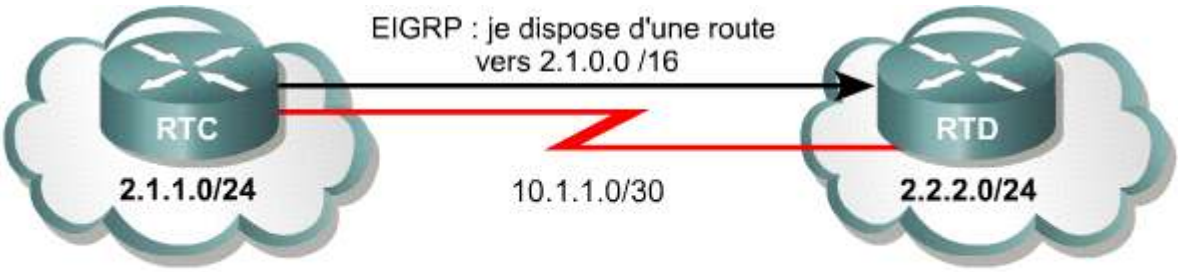
Pour désactiver la fonction de résumé automatique, utilisez la commande suivante:

```
router(config-router)#no auto-summary
```

Avec l'EIGRP, vous pouvez configurer manuellement une adresse résumée en configurant un préfixe. Les routes résumées manuelles sont configurées interface par interface. L'interface qui propagera le résumé de route doit donc être sélectionnée en premier. L'adresse résumée peut ensuite être définie avec la commande **ip summary-address eigrp**:

```
router(config-if)#ip summary-address eigrp numéro-système-autonome masque adresse-ip [distance-administrative]
```

Les routes résumées EIGRP ont par défaut une distance administrative de 5. Il est également possible de les configurer pour une valeur comprise entre 1 et 255.



Les adresses résumées peuvent être configurées manuellement par interface

Dans la figure 3, RTC peut être configuré à l'aide des commandes illustrées ci-dessous:

```
RTC(config)#router eigrp 2446
RTC(config-router)#no auto-summary
RTC(config-router)#exit
RTC(config)#interface serial 0/0
RTC(config-if)#ip summary-address eigrp 2446 2.1.0.0 255.255.0.0
```

Par conséquent, RTC ajoutera une route à sa table, comme suit:

```
D 2.1.0.0/16 is a summary, 00:00:22, Null0
```

Notez que la route résumée provient de Null0 et pas d'une interface réelle. Cela est dû au fait que cette route est utilisée à des fins d'annonce et qu'elle ne représente pas un chemin que RTC peut emprunter pour atteindre ce réseau. Sur RTC, cette route a une distance administrative de 5.

RTD n'est pas conscient du résumé mais il accepte la route. Il est affecté à cette route la distance administrative d'une route EIGRP normale, c'est-à-dire 90 par défaut.

Dans la configuration de RTC, la fonction de résumé automatique est désactivée à l'aide de la commande **no auto-summary**. Si la fonction n'était pas désactivée, RTD recevrait deux routes, l'adresse résumée manuelle, qui est 2.1.0.0 /16, et l'adresse résumée par classes automatique qui est 2.0.0.0 /8.

Dans la plupart des cas, vous devez lancer la commande **no auto-summary** lors du résumé manuel.

3.2 Configuration EIGRP

3.2.3 Vérification de l'EIGRP de base

La vérification du fonctionnement de l'EIGRP s'effectue à l'aide de diverses commandes **show**. La figure 1 répertorie les principales commandes **show** EIGRP et décrit brièvement leurs fonctions.

Commande	Description
show ip eigrp neighbors *[type number]* **[details]**	Affiche la table de voisinage EIGRP. Utilisez les options " type " et " numéro " pour indiquer une interface. Le mot-clé " details " étend le résultat.
show ip eigrp interfaces *[type number]* *[as-number]* **[details]**	Affiche des informations EIGRP pour chaque interface. Les mots-clés facultatifs limitent l'affichage des informations à une interface ou à un système autonome spécifique. Le mot-clé " details " entraîne l'affichage d'informations détaillées.
show ip eigrp topology *[as-number | [[ip-address] mask]]*	Affiche tous les successeurs possibles dans la table topologique EIGRP. Les mots-clés facultatifs peuvent filtrer les informations affichées sur la base du numéro de système autonome ou d'une adresse réseau spécifique.
show ip eigrp topology [active | pending | zero-successors]	Selon le mot-clé utilisé, affiche toutes les routes de la table topologique qui sont actives, en attente ou sans successeurs.
show ip eigrp topology all-links	Affiche toutes les routes, et non simplement les successeurs possibles, dans la topologie EIGRP.
show ip eigrp traffic *[as-number]*	Affiche le nombre de paquets Enhanced IGRP envoyés et reçus. Les informations affichées par la commande peuvent être filtrées à l'aide d'un numéro de système autonome facultatif.

La fonction **debug** de l'IOS fournit également des commandes de surveillance EIGRP utiles. 2

Commande	Description
debug eigrp fsm	Cette commande indique l'activité des successeurs possibles EIGRP permettant de déterminer si des mises à jour de routage sont en cours d'installation et de suppression par le processus de routage.
debug eigrp packet	Les informations affichées par cette commande reflètent l'envoi et la réception de paquets EIGRP. Ces paquets peuvent être de type HELLO, mise à jour, requête ou réponse. Les numéros de séquence et d'accusé de réception utilisés par l'algorithme de transport fiable EIGRP sont indiqués dans les informations affichées.

Activité de TP

Exercice: Vérification de la configuration EIGRP de base

Dans ce TP, les étudiants vont configurer un système d'adressage IP pour le réseau et vérifier la configuration EIGRP.

Activité de TP

Activité en ligne: Vérification de l'EIGRP de base

Au cours de ce TP, l'étudiant va configurer et vérifier le routage EIGRP.

3.2 Configuration EIGRP

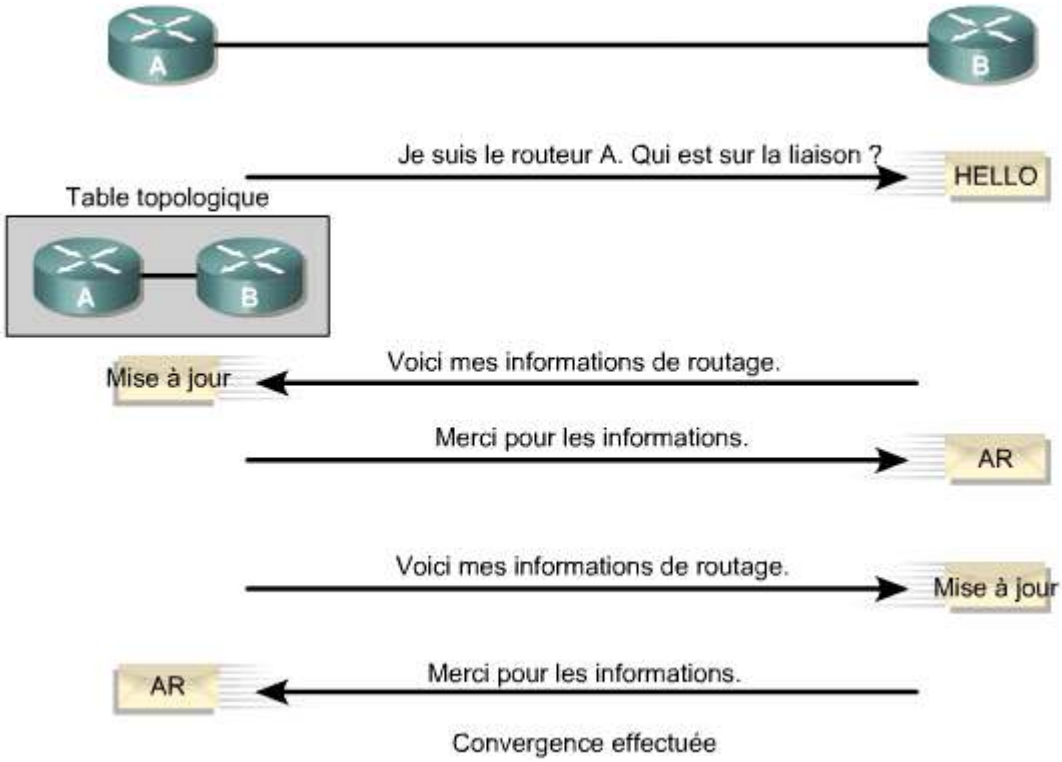
3.2.4 Construction de tables de voisinage

Les routeurs à vecteur de distance simples n'établissent aucune relation avec leurs voisins. Les routeurs RIP et IGRP effectuent seulement une diffusion de broadcast ou de multicast des mises à jour sur les interfaces configurées. En revanche, les routeurs EIGRP établissent de façon active des relations avec leurs voisins, d'une façon très similaire aux routeurs OSPF. 1

Cisco - Router

```
Router#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime    SRTT   RTO  Q   Seq
                                            (sec)          (ms)       Cnt Num
2   200.10.10.10            Se1               13 00:19:09  26   200  0   10
1   200.10.10.5             Se0               12 03:31:36  50   300  0   39
0   199.55.32.10            Et0               11 03:31:40  10   200  0   40
```

La table de voisinage est la table la plus importante de l'EIGRP. Chaque routeur EIGRP tient à jour une table de voisinage qui répertorie les routeurs adjacents. Cette table est comparable à la base de données de contiguïté utilisée par l'OSPF. Il y a une table de voisinage pour chaque protocole pris en charge par l'EIGRP.



Les routeurs EIGRP établissent des contiguïtés avec des routeurs voisins en utilisant des petits paquets HELLO. Ces paquets sont envoyés par défaut toutes les cinq secondes. 2 Un routeur EIGRP suppose que tant qu'il reçoit des paquets HELLO des voisins connus, ces derniers et leurs routes restent praticables ou passifs. Pour former des contiguïtés, les routeurs EIGRP procèdent comme suit:

- Ils prennent connaissance de façon dynamique des nouvelles routes qui relient leur réseau
- Ils identifient les routeurs qui deviennent inaccessibles ou inutilisables
- Ils redécouvrent les routeurs qui étaient précédemment inaccessibles

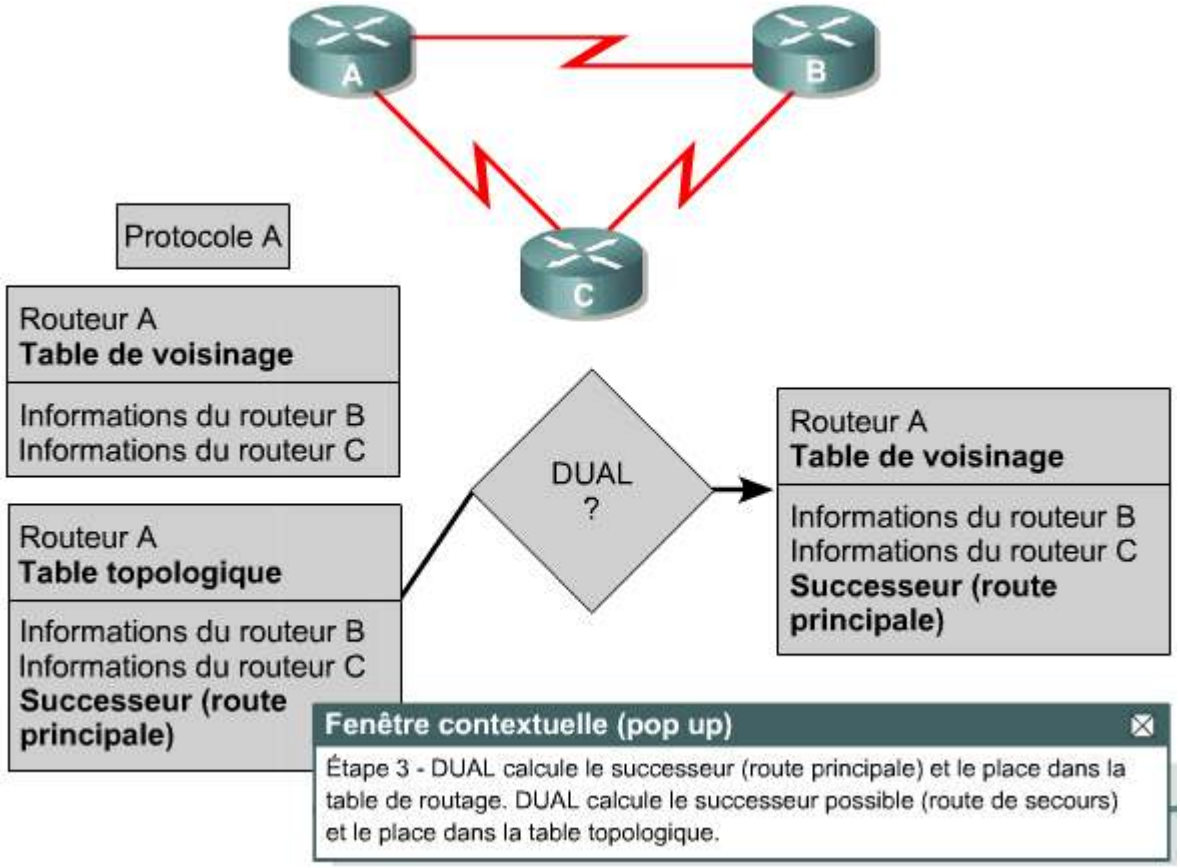
La table de voisinage comporte les champs suivants:

- **Adresse du voisin** – Il s'agit de l'adresse de couche réseau du routeur voisin.
- **Délai de conservation** – Intervalle à l'issue duquel la liaison est considérée comme indisponible si aucun signal n'a été reçu du voisin. À l'origine, le paquet attendu était un paquet HELLO, mais dans les versions actuelles de la plate-forme logicielle Cisco IOS, tout paquet EIGRP reçu après le premier HELLO réinitialise le compteur.
- **Smooth Round-Trip Timer (SRTT)** – C'est le temps moyen nécessaire pour envoyer et recevoir des paquets d'un voisin. Ce compteur permet de déterminer l'intervalle de transmission (RTO).
- **Queue count (Q Cnt)** – Il s'agit du nombre de paquets en attente d'envoi dans une file d'attente. Si cette valeur est constamment supérieure à zéro, il peut y avoir un problème de congestion au niveau du routeur. Un zéro signifie qu'il n'y a aucun paquet EIGRP dans la file d'attente.
- **Sequence Number (Seq No)** – C'est le numéro du dernier paquet reçu de ce voisin. L'EIGRP utilise ce champ pour accuser réception de la transmission d'un voisin et pour identifier les paquets hors séquence. La table de voisinage permet de prendre en charge une livraison fiable et ordonnée des paquets et peut être considérée comme analogue au protocole TCP utilisé dans la livraison fiable de paquets IP.

3.2 Configuration EIGRP

3.2.5 Découverte des routes

Les routeurs EIGRP stockent les informations de topologie et de route en mémoire RAM, afin de pouvoir réagir rapidement aux changements. Comme l'OSPF, l'EIGRP enregistre ces informations dans diverses tables ou bases de données. 1



L'algorithme de vecteur de distance EIGRP, DUAL, utilise les informations collectées dans les tables de voisinage et les tables topologiques et calcule la route de moindre coût jusqu'à la destination. La route principale est appelée route successeur. Lorsqu'elle est calculée, DUAL insère la route successeur dans la table de routage et une copie dans la table topologique.

L'algorithme DUAL tente également de calculer une route de secours en cas de défaillance de la route successeur. C'est ce que l'on appelle la route successeur possible. Une fois calculée, DUAL place la route possible dans la table topologique. Cette route peut être appelée si la route successeur vers une destination devient inaccessible ou non fiable.

Activité de média interactive

Mots croisés: Concepts et terminologie EIGRP

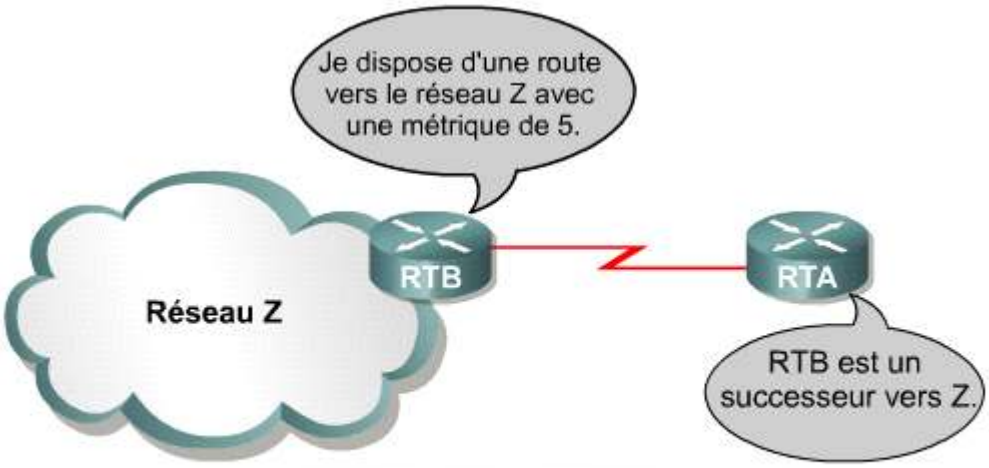
À la fin de cette activité, l'étudiant sera en mesure de comprendre les différents concepts et termes de l'EIGRP.

3.2 Configuration EIGRP

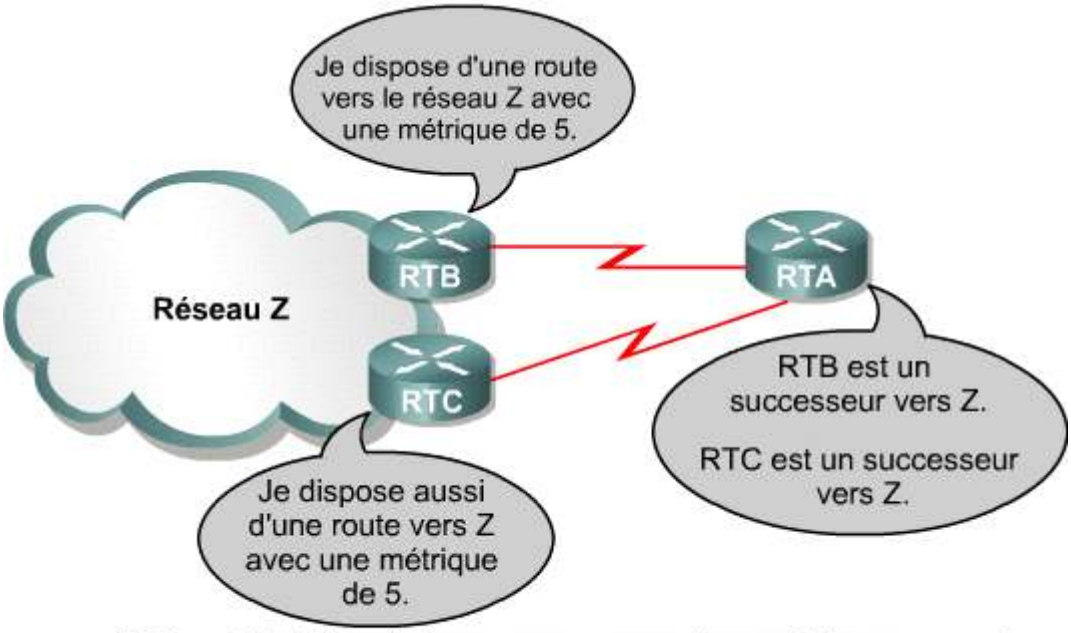
3.2.6 Sélection de routes

Si un lien est interrompu, DUAL recherche un autre chemin, ou successeur possible, dans la table topologique. 1 2 3 S'il est impossible de trouver une route successeur possible, la route est étiquetée à l'état Actif, ou inutilisable pour l'instant. Des paquets de requête sont envoyés aux routeurs voisins pour demander des informations topologiques. DUAL utilise ces informations pour recalculer les routes successeur et successeur possible jusqu'à destination.

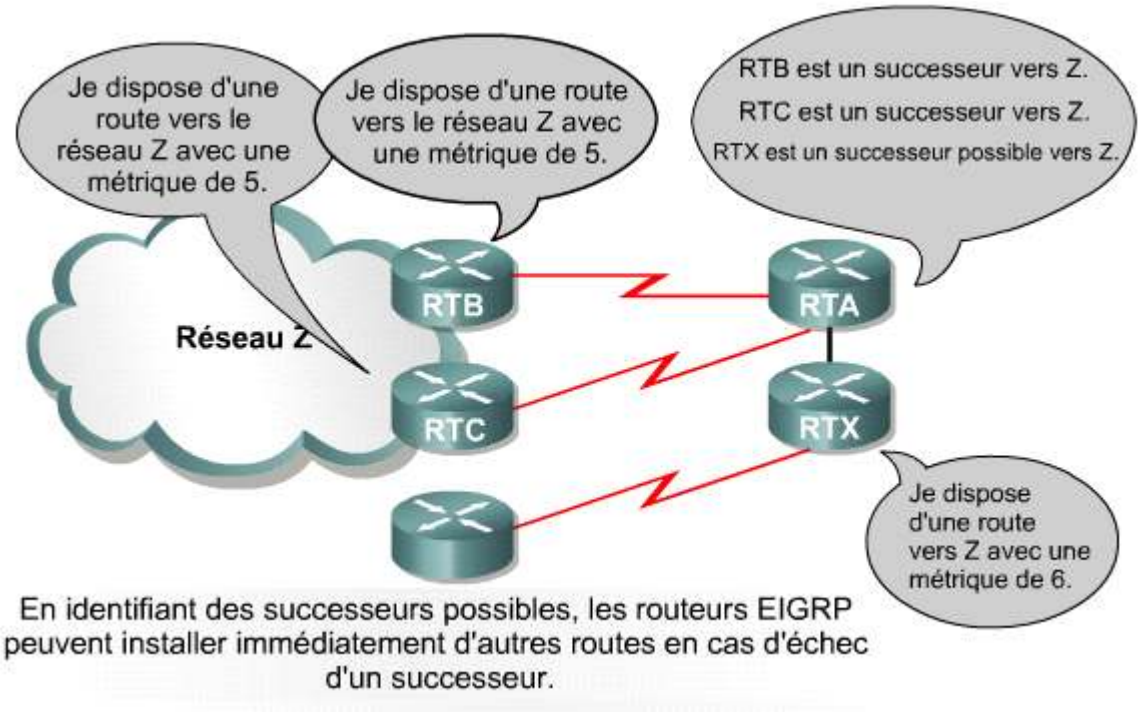
Lorsque l'algorithme DUAL a terminé ses calculs, la route successeur est placée dans la table de routage. Ensuite, la route successeur et la route successeur possible sont placées dans la table topologique. La route jusqu'à la destination finale passe alors de l'état Actif à l'état Passif. Cela veut dire que la route est maintenant opérationnelle et fiable.



Un successeur est un routeur voisin qui représente l'étape suivante vers une destination donnée en utilisant un chemin sans boucle au coût minimal.



RTA peut installer plusieurs successeurs si ces voisins annoncent des routes avec la même métrique.



L'algorithme DUAL sophistiqué assure une convergence exceptionnellement rapide de l'EIGRP. Afin de mieux comprendre la convergence avec DUAL, considérez l'exemple de la figure 1. Chaque routeur a construit une table topologique qui contient des informations sur la manière d'atteindre le réseau de destination Z.

Chaque table contient les informations suivantes:

- Le protocole de routage ou EIGRP
- Le coût le plus bas de la route, ou distance possible (FD)
- Le coût de la route tel qu'annoncé par le routeur voisin, ou distance annoncée (RD)

DUAL identifie la route principale préférée, ou route successeur (Successor). Si elle est identifiée, DUAL identifie également les routes de secours, ou successeurs possibles (FS). Notez qu'il n'est pas nécessaire d'avoir un successeur possible identifié. Notez qu'il n'est pas nécessaire d'avoir un successeur possible identifié. 4

1. La route successeur possible est une route de secours utilisable en cas de défaillance de la route successeur.
2. La distance RD (distance annoncée) vers la destination, telle qu'elle est annoncée par le routeur voisin, doit être inférieure à la distance FD (distance possible) de la route du successeur principal.
3. Si ce critère est satisfait et s'il n'existe pas de boucle de routage, la route peut être sélectionnée comme route possible.
4. La route successeur possible peut alors être promue au rang de route successeur.
5. Si la distance RD (distance annoncée) de la route alternative est égale ou supérieure à la distance FD (distance possible) du successeur d'origine, la route est rejetée comme route successeur possible.
6. Le routeur doit recalculer la topologie du réseau en collectant des informations pour tous les voisins.
7. Le routeur envoie un paquet de type requête à tous les voisins pour connaître les chemins de routage disponibles et le coût de métrique associé pour le réseau de destination.
8. Tous les routeurs voisins doivent envoyer un paquet en réponse à la requête. Les données reçues sont écrites dans la table topologique du routeur émetteur. DUAL peut alors identifier les routes du nouveau successeur et, le cas échéant, les routes du nouveau successeur possible sur la base de ces nouvelles informations.

3.2 Configuration EIGRP

3.2.7 Mise à jour des tables de routage

L'algorithme DUAL analyse toutes les routes annoncées par les voisins en utilisant la métrique composée de chaque route pour les comparer. Il s'assure également que chaque chemin est exempt de boucles.

Des chemins de moindre coût sont alors insérés par l'algorithme DUAL dans la table de routage. Ces routes principales sont appelées routes successeur. Une copie des chemins successeur est insérée dans la table topologique.

L'EIGRP conserve les informations importantes sur les routes et la topologie dans un table de voisinage ou une table topologique. Ces tables fournissent à DUAL des informations de route complètes en cas d'interruption du réseau. DUAL sélectionne rapidement d'autres routes en se basant sur les informations de ces tables.

Si un lien est interrompu, DUAL recherche un autre chemin, ou successeur possible, dans la table topologique. S'il est impossible de trouver une route successeur possible, la route est étiquetée à l'état Actif, ou inutilisable pour l'instant. Des paquets de requête sont envoyés aux routeurs voisins pour demander des informations topologiques. DUAL utilise ces informations pour recalculer les routes successeur et successeur possible jusqu'à destination.

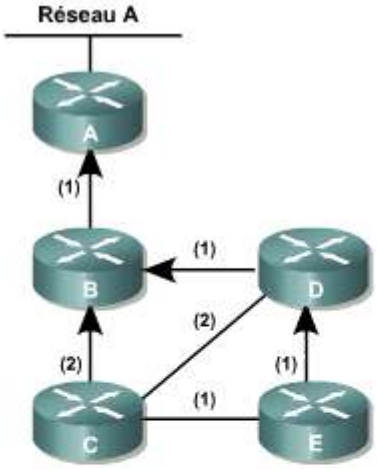
Lorsque l'algorithme DUAL a terminé ses calculs, la route successeur est placée dans la table de routage. Ensuite, la route successeur et la route successeur possible sont placées dans la table topologique. La route jusqu'à la destination finale passe alors de l'état Actif à l'état Passif. Cela veut dire que la route est maintenant opérationnelle et fiable.

Les routeurs EIGRP établissent et maintiennent des contiguïtés avec des routeurs voisins en utilisant des petits paquets HELLO. Ces paquets sont envoyés par défaut toutes les cinq secondes. Un routeur EIGRP suppose que tant qu'il reçoit des paquets HELLO des voisins connus, ces derniers et leurs routes restent praticables ou passives.

Lorsque des voisins nouvellement découverts sont appris, l'adresse et l'interface du voisin sont enregistrées. Ces informations sont stockées dans la structure de données de voisinage. Lorsqu'un voisin envoie un paquet HELLO, il annonce un délai de conservation. Ce délai et le laps de temps pendant lequel un routeur considère son voisin accessible et opérationnel. Autrement dit, si un paquet HELLO n'est pas détecté pendant le délai de conservation, celui-ci expire. Au moment de l'expiration, le DUAL est informé du changement de topologie et doit recalculer la nouvelle topologie.

Dans l'exemple des figures 1 à 3, DUAL doit reconstruire la topologie à la suite de la découverte d'une liaison rompue entre le routeur D et le routeur B.

Les nouvelles routes successeur seront placées dans la table de routage mise à jour.

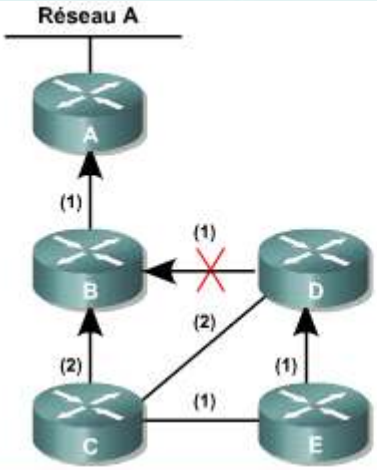


C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D	4	2	(FS)
	via E	4	3	

D	EIGRP	FD	RD	Topologie
Réseau A		2		(FD)
	via B	2	1	Successeur)
	via C	5	3	

E	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via D	3	2	(Successeur)
	via C	4	3	

Légende	
C	Destination
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

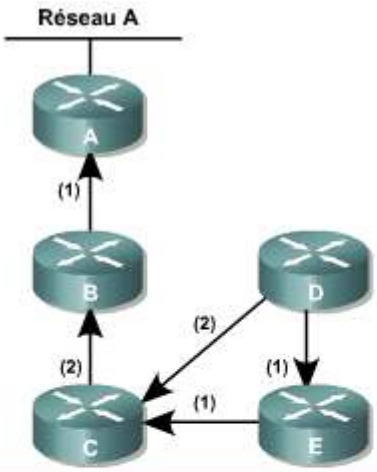


C	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via B	3	1	(Successeur)
	via D	4	2	(FS)
	via E	4	3	

D	EIGRP	FD	RD	Topologie
Réseau A		2		(FD)
	~~via B~~	~~2~~	~~1~~	~~(Successeur)~~
	via C	5	3	

E	EIGRP	FD	RD	Topologie
Réseau A		3		(FD)
	via D	3	2	(Successeur)
	via C	4	3	

Légende	
C	Destination
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination



C EIGRP	FD	RD	Topologie
Réseau A	3		(FD)
via B	3	1	(Successeur)
via D			
via E			

D EIGRP	FD	RD	Topologie
Réseau A	5		(FD)
via C	5	3	(Successeur)
via E	5	4	(Successeur)

E EIGRP	FD	RD	Topologie
Réseau A	4		(FD)
via C	4	3	(Successeur)
via D			

Légende	
C	Destination
EIGRP	Type de protocole
FD	Feasible Distance - distance possible
RD	Reported Distance - distance annoncée par le routeur voisin
Successor	Route principale vers la destination
FS	Feasible Successor (successeur possible) - Route de secours vers la destination

3.3 Dépannage des protocoles de routage

3.3.1 Processus de dépannage de protocole de routage

Tout dépannage de protocole de routage doit commencer par une séquence logique ou diagramme fonctionnel. Ce diagramme fonctionnel n'est pas un cadre rigide de dépannage d'un interréseau Cependant, c'est une fondation qui permet à l'administrateur réseau d'élaborer un processus de résolution de problèmes adapté à un environnement particulier.

1. Lorsque vous analysez une panne de réseau, faites un énoncé clair du problème. 1

Étape 1. Lors de l'analyse d'une panne de réseau, énoncez clairement le problème.

- Définissez le problème en termes de symptômes et de causes possibles.
- Pour analyser correctement le problème, identifiez les symptômes généraux, puis déterminez les catégories de problèmes ou les causes susceptibles de générer ces symptômes. Par exemple, le fait que des hôtes ne répondent pas aux demandes de services de clients est un symptôme.
- Parmi les causes possibles, il se peut que l'hôte soit mal configuré, que les cartes d'interface soient défectueuses ou que des commandes de configuration du routeur soient manquantes.

2. Rassemblez les faits nécessaires pour mieux isoler les causes possibles. 2

Étape 2. Définissez le problème en termes de symptômes et de causes possibles.

- Recueillez des faits susceptibles de vous aider à identifier les causes possibles. Interrogez les personnes concernées (utilisateurs, administrateurs réseau, directeurs, etc.).
- Collectez des informations issues des systèmes d'administration de réseaux, des résultats d'analyse des protocoles, des résultats des commandes de diagnostic du routeur ou des notes de version de logiciels.

3. Examinez les problèmes possibles relativement aux faits recueillis. 3

Étape 3. Envisagez les problèmes possibles sur la base des faits collectés.
- À l'aide de ces faits, vous pouvez éliminer certains problèmes potentiels de la liste.
- Selon les données, vous pouvez être amené à éliminer les problèmes matériels et vous concentrer sur les problèmes logiciels.
- À chaque occasion, essayez de limiter le nombre de problèmes potentiels afin de créer un plan d'action efficace.

4. Créez un plan d'action basé sur les problèmes potentiels restants. 4

Étape 4. Créez un plan d'action sur la base des problèmes potentiels restants.
- Commencez par le problème le plus probable et établissez un plan dans lequel une seule variable est modifiée.
- Le fait de changer une seule variable à la fois aide à reproduire une solution donnée pour un problème spécifique. N'essayez pas de modifier plusieurs variables en même temps. Une telle action peut résoudre le problème. Toutefois, l'identification du changement ayant permis d'éliminer le symptôme devient plus difficile et ne facilite pas la résolution d'un problème identique survenant ultérieurement.

5. Mettez en œuvre le plan d'action, en exécutant chaque étape soigneusement tout vérifiant si le symptôme disparaît. 5

Étape 5. Mettez en œuvre le plan d'action, en suivant chaque étape tout en vérifiant si le symptôme disparaît.

6. Analysez les résultats afin de déterminer si le problème a été résolu. Si c'est le cas, alors le processus est terminé. 6

Étape 6. Analysez les résultats pour déterminer si le problème a été résolu. Le cas échéant, le processus est terminé.

7. Si le problème n'a pas été résolu, élaborez un plan d'action basé sur le problème suivant le plus probable de la liste. Retournez à l'étape 4, modifiez une variable à la fois, et répétez le processus jusqu'à ce que le problème soit résolu. 7

Étape 7. Si le problème n'a pas été résolu, créez un plan d'action sur la base du problème potentiel suivant dans la liste. Revenez à l'étape 4, changez une variable à la fois et répétez le processus jusqu'à ce que le problème soit résolu.

8. Une fois la cause réelle du problème identifiée, essayez de le résoudre. 8

Étape 8. Une fois la cause réelle du problème identifiée, essayez d'apporter une solution.
- À ce stade, il est important d'expliquer en détail le problème et la solution pour pouvoir s'y reporter ultérieurement.
- Si toutes les tentatives entreprises jusqu'à présent ont échoué, vous pouvez faire appel au support technique du fabricant de l'équipement suspect.
- Vous pouvez également consulter des experts ou des ingénieurs techniques pour vous aider à réaliser le processus de dépannage.

Les routeurs Cisco fournissent diverses commandes intégrées pour vous aider à surveiller et à dépanner un interrréseau:

- Les commandes **show** permettent de surveiller le comportement à l'installation et le comportement normal du réseau, ainsi que d'isoler des zones problématiques 9

Utilisez les commandes show Cisco IOS pour les activités suivantes :
- Surveillance du comportement du routeur pendant l'installation initiale
- Surveillance du fonctionnement normal du réseau
- Identification d'interfaces, de nœuds, de médias ou d'applications problématiques
- Détermination des périodes de congestion d'un réseau
- Détermination de l'état de serveurs, de clients ou d'autres équipements voisins

- Les commandes **debug** permettent d'identifier précisément les problèmes de protocole et de configuration.
- Les outils de réseau TCP/IP tels que ping, traceroute et telnet 10

Outils réseau TCP/IP :
- La commande **ping** étendue permet un contrôle plus précis que la commande **ping** de base.
- La commande **ping** permet de tester rapidement la connectivité réseau de bout en bout.
- La commande **traceroute** est utilisée pour identifier les goulots d'étranglement ou localiser des connexions réseau rompus.
- La commande **telnet** peut être utilisée pour tester la connectivité réseau de bout en bout.

Les commandes **show** de la plate-forme logicielle Cisco IOS sont des outils indispensables pour comprendre l'état d'un routeur, détecter les routeurs voisins, surveiller le réseau en général et isoler les problèmes du réseau.

Les commandes EXEC **debug** peuvent fournir une foule d'informations sur le trafic d'interface, les messages d'erreur internes, les paquets de diagnostics spécifiques au protocole et d'autres données de dépannage utiles. Utilisez les commandes **debug** pour isoler les problèmes, pas pour surveiller le fonctionnement normal du réseau. N'utilisez les commandes **debug** que pour rechercher des types spécifiques de trafic ou de problèmes. Avant d'utiliser la commande **debug**, limitez le problème à un sous-ensemble de causes probables. Utilisez la commande **show debugging** pour voir quelle fonction de déboguage est activée.

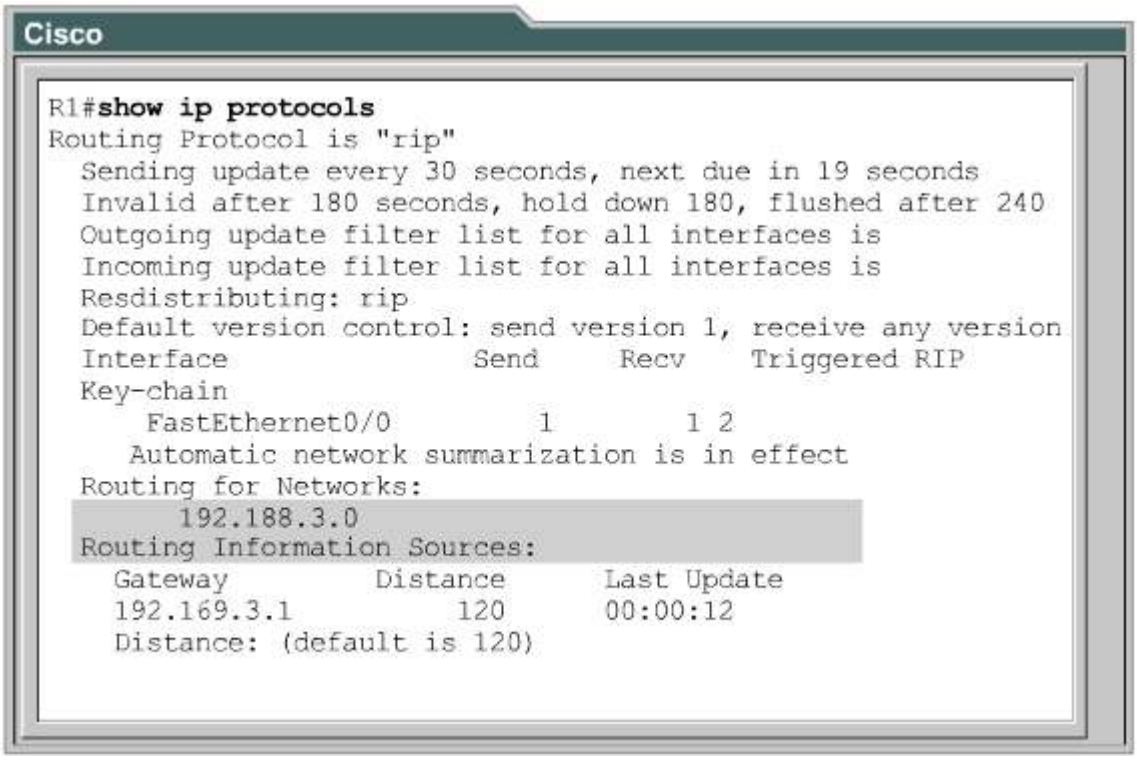
3.3 Dépannage des protocoles de routage

3.3.2 Dépannage de la configuration RIP

Le problème le plus couramment rencontré dans le protocole RIP (Routing Information Protocol) et qui empêche les routes RIP d'être annoncées est le masque de sous-réseau de longueur variable (VLSM). Cela est dû au fait que la RIP Version 1 ne prend pas en charge VLSM. Si les routes RIP ne sont pas annoncées, vous devez vérifier:

- Les problèmes éventuels de connectivité au niveau de la couche 1 ou de la couche 2.

- La division en sous-réseaux VLSM est configurée. La subdivision en sous-réseaux VLSM ne peut pas être utilisée avec RIP v1.
- La non-concordance entre les configurations de routage RIP v1 et RIP v2.
- Les instructions réseau manquantes ou incorrectement assignées.
- L'interface sortante est interrompue.
- L'interface réseau annoncée est interrompue.



La commande **show ip protocols** fournit des informations sur les paramètres et sur l'état courant du processus de protocole de routage actif. Le protocole RIP envoie des mises à jour aux interfaces des réseaux spécifiés. 1 Si l'interface FastEthernet 0/1 a été configurée mais que le réseau n'a pas été ajouté au routage RIP, aucune mise à jour ne sera envoyée ou reçue via l'interface.

Utilisez la commande EXEC **debug ip rip** pour afficher des informations sur les transactions de routage RIP. Les commandes **no debug ip rip**, **no debug all** ou **undebug all** permettent de désactiver toutes les opérations de déboguage.

La figure 2 montre que le routeur en cours de déboguage a reçu une mise à jour d'un autre routeur à l'adresse source 192.168.3.1. Ce routeur a envoyé des informations sur deux destinations dans la mise à jour de table de routage. Le routeur en cours de déboguage a également envoyé des mises à jour. Les deux routeurs ont diffusé l'adresse 255.255.255.255 comme destination. Le nombre entre parenthèses représente l'adresse source encapsulée dans l'en-tête IP.

Cisco

```
R1#debug ip rip
R1#clear ip route *
3d08h: RIP: sending request on FastEthernet0/0 to
255.255.255.255
R1#
3d08h:  RIP: sending v1 flash update to
255.255.255.255 via FastEthernet0/0 (192.168.3.2)
3d08h:  RIP: build flash update entries
3d08h:   network 172.31.0.0 metric 1
R1#
3d08h:  RIP: received v1 update from 192.168.3.1 on
FastEthernet0/0
3d08h:       172.30.0.0 in 1 hops
3d08h:       172.16.0.0 in 2 hops

R1#
```

Si vous obtenez le message suivant, il est probable que l'émetteur a envoyé un paquet mal formé:

```
RIP: bad version 128 from 160.89.80.43
```

3.3 Dépannage des protocoles de routage

3.3.3 Dépannage de la configuration IGRP

Le protocole IGRP (Interior Gateway Routing Protocol) est un protocole de routage à vecteur de distance avancé que Cisco a développé au milieu des années 80. L'IGRP possède diverses caractéristiques qui le différencient des autres protocoles de routage à vecteur de distance comme le RIP. 1

Caractéristiques	Explication
Évolutivité accrue	Le protocole de routage IGRP est utilisé dans des réseaux de plus grande taille que ceux qui utilisent le protocole RIP.
Métrique sophistiquée	IGRP utilise une métrique composée qui apporte une flexibilité significative lors la sélection de la route. La sélection de la route repose sur plusieurs facteurs : le délai interréseau, la bande passante par défaut, la charge et éventuellement la fiabilité. IGRP peut être utilisé pour surmonter la limite RIP de 15 sauts. Par défaut, IGRP propose une valeur maximum de 100 sauts, qui peut être étendue à un maximum de 255 sauts.
Chemins multiples	IGRP peut maintenir jusqu'à six chemins distincts entre un réseau source et une destination. Les chemins ne doivent pas correspondre aux coûts comme avec RIP. Des chemins multiples peuvent être utilisés pour augmenter la bande passante disponible ou pour la redondance de route.

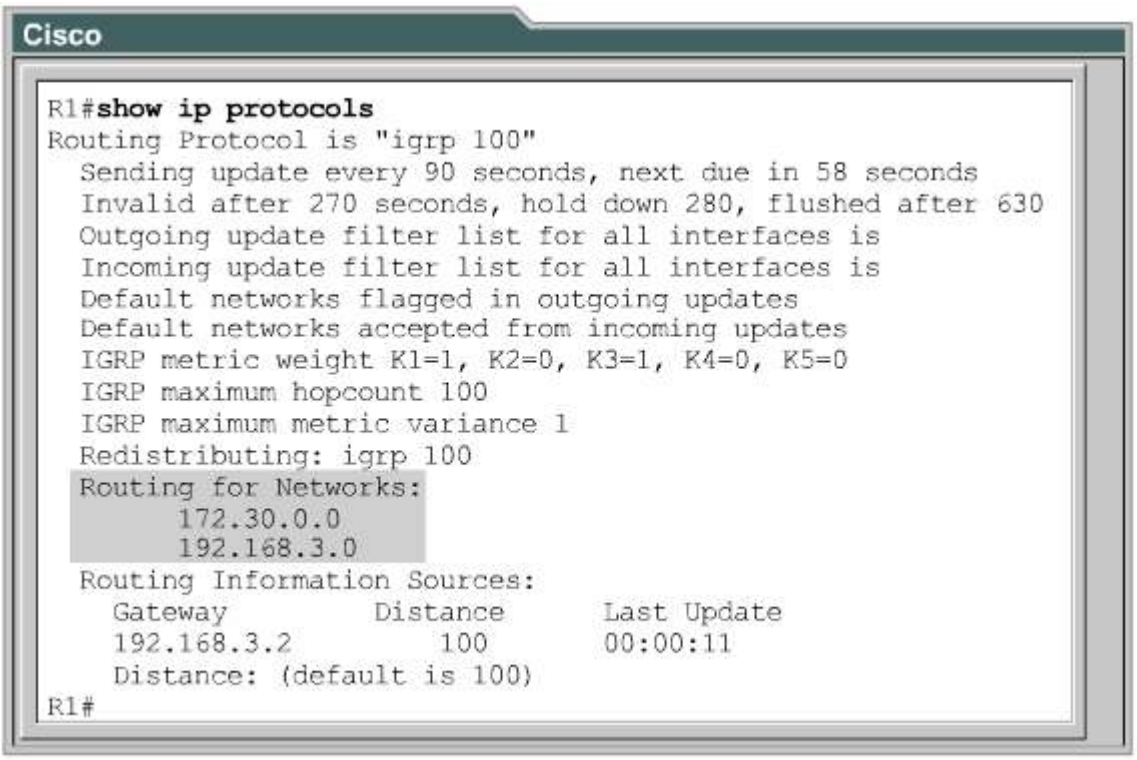
Utilisez la commande **router igrp***système-autonome* pour activer le processus de routage IGRP:

```
R1(config)#router igrp 100
```

Utilisez la commande de configuration de routeur **network***numéro-réseau* pour permettre aux interfaces de participer au processus de mise à jour IGRP:

```
R1(config-router)#network 172.30.0.0
R1(config-router)#network 192.168.3.0
```

Vérifiez la configuration IGRP à l'aide des commandes **show running-configuration** et **show ip protocols**:



2

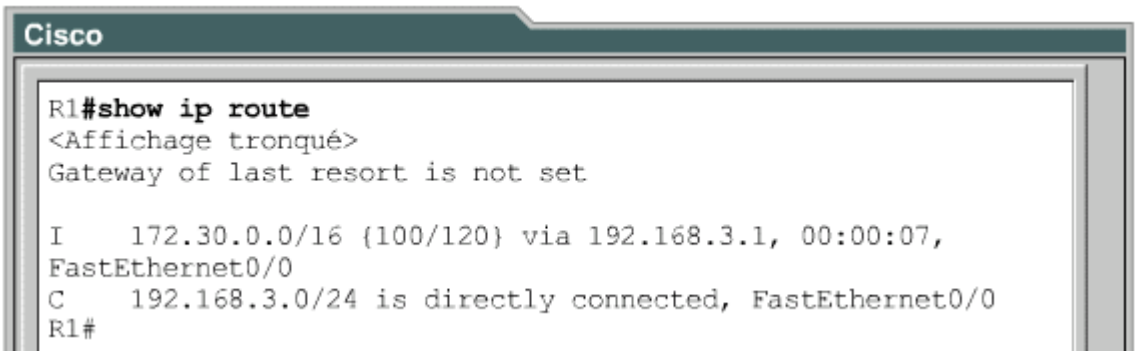
```
R1#show ip protocols
```

Vérifiez le fonctionnement de l'IGRP à l'aide de la commande **show ip route**: **[3]**

```
R1#show ip route
```

Si l'IGRP ne vous semble pas fonctionner de manière correcte, vérifiez les points suivants:

- Problèmes éventuels de connectivité au niveau de la couche 1 ou de la couche 2.
- Non-concordance des numéros de système autonome sur les routeurs IGRP.
- Instructions réseau manquantes ou incorrectement assignées.
- L'interface sortante est interrompue.
- L'interface réseau annoncée est interrompue.



Pour visualiser les informations de débogage IGRP, utilisez les commandes suivantes:

- **debug ip igrp transactions [host ip address]** pour visualiser les informations de transaction IGRP
- **debug ip igrp events [host ip address]** pour visualiser les informations de mise à jour de routage

Pour désactiver le débogage, utilisez la commande **no debug ip igrp**.

Si un réseau devient inaccessible, les routeurs qui exécutent IGRP envoient des mises à jour déclenchées aux voisins pour les en informer. Un routeur voisin répond alors avec des mises à jour en mode «poison reverse» et maintient le réseau suspect à l'état de retenue pendant 280 secondes.

3.3.4 Dépannage de la configuration EIGRP

3.3.4 Dépannage de la configuration EIGRP

Le fonctionnement normal de l'EIGRP est stable, efficace en termes d'utilisation de la bande passante et relativement simple à surveiller et à dépanner.

Utilisez la commande **router eigrp***système-autonome* pour activer le processus de routage EIGRP:

```
R1(config)#router eigrp 100
```

Pour échanger des mises à jour de routage, chaque routeur du réseau EIGRP doit être configuré avec le même numéro de système autonome.

Utilisez la commande de configuration de routeur **network***numéro-réseau* pour permettre aux interfaces de participer au processus de mise à jour EIGRP:

```
R1(config-router)#network 172.30.0.0
R1(config-router)#network 192.168.3.0
```

Vérifiez la configuration EIGRP à l'aide des commandes **show running-configuration** et **show ip protocols**: 1

Cisco

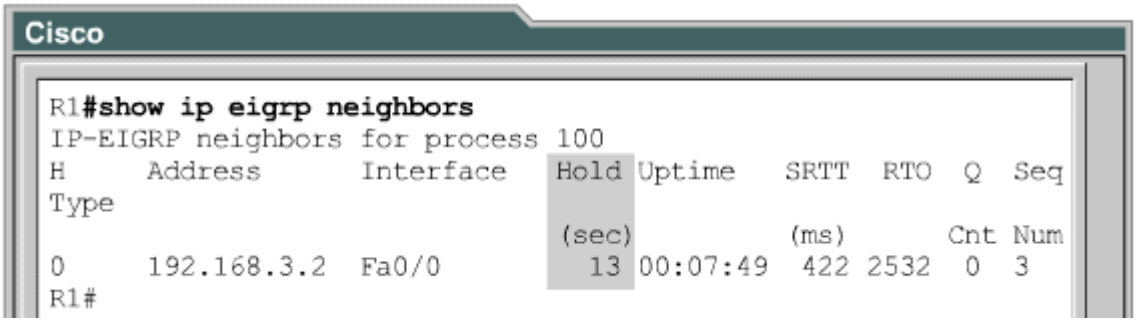
```
R1#show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  Automatic network summarization is in effect
  Routing for Networks:
        172.30.0.0
        192.168.3.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:07:40
    192.168.3.2          100      00:03:44
    Distance: internal 90 external 170
R1#
```

```
R1#show ip protocols
```

Voici quelques raisons possible du dysfonctionnement de l'EIGRP:

- Problèmes éventuels de connectivité au niveau de la couche 1 ou de la couche 2.
- Non-concordance des numéros de système autonome sur les routeurs EIGRP.
- La liaison est congestionnée ou interrompue.
- L'interface sortante est interrompue.
- L'interface réseau annoncée est interrompue.
- La fonction de résumé automatique est activée sur les routeurs sur des sous-réseaux non contigus. Utilisez la commande **`no auto-summary`** pour désactiver le résumé automatique du réseau.

L'une des raisons les plus courantes d'un voisin manquant est la panne de la liaison proprement dite. Ce peut être également l'expiration d'un compteur de retenue. Puisque des HELLO sont envoyés toutes les 5 secondes sur la plupart des réseaux, la valeur de délai de conservation des informations affichées par une commande **`show ip eigrp neighbors`** doit normalement être comprise entre 10 et 15. 2



Pour surveiller et dépanner efficacement un réseau EIGRP, utilisez les commandes décrites dans les figures 3 – 4.

Commande	Utilisation
`Router#show ip eigrp neighbors`	Affiche les voisins découverts par EIGRP et identifie la date de la dernière réinitialisation d'un voisin.
`Router#show ip eigrp topology`	Cette commande affiche la table topologique, l'état (actif ou inactif) des routes, le nombre de successeurs et la distance possible vers la destination.
`Router#show ip route eigrp`	Affiche les entrées EIGRP actuelles de la table de routage.
`Router#show ip protocols`	Affiche les paramètres et l'état actuel du processus de protocole de routage actif. Cette commande indique le numéro du système autonome EIGRP. Elle indique également les numéros de filtrage et de redistribution, ainsi que des informations relatives à la distance et aux voisins.
`Router#show ip eigrp traffic`	Affiche le nombre de paquets EIGRP envoyés et reçus. Cette commande affiche des statistiques sur les paquets de type HELLO, mise à jour, requête, réponse et accusé de réception.
`Router(config-router)#eigrp log-neighbor-changes`	Fournit un historique indiquant la date de réinitialisation des voisins et la raison de cette réinitialisation.

Commande	Description
debug eigrp fsm	Affiche des informations sur les paquets de protocole Enhanced IGRP. Cette commande permet d'analyser les paquets envoyés et reçus sur une interface. Étant donné que la commande debug ip eigrp génère une grande quantité de données, utilisez-la uniquement lorsque le trafic réseau est peu important.

3.3 Dépannage des protocoles de routage

3.3.5 Dépannage de la configuration OSPF

Le protocole OSPF (Open Shortest Path First) est un protocole de routage à état de liens. Un lien est une interface sur un routeur. L'état d'un lien est une description de cette interface et de sa relation avec les routeurs voisins. Par exemple, une description de l'interface inclurait l'adresse IP de l'interface, le masque de sous-réseau, le type de réseau auquel elle est connectée, les routeurs connectés à ce réseau, etc. Ces informations forment une base de données d'état de liens.

La majorité des problèmes rencontrés avec OSPF sont liés à la formation des contiguïtés et à la synchronisation des bases de données d'état de liens. La commande **show ip ospf neighbor** est utile pour dépanner la formation des contiguïtés. Les commandes pouvant être utilisées pour dépanner OSPF sont indiquées dans la figure 1

Commande	Utilisation
show ip protocols	Affiche des paramètres sur les compteurs, les filtres, les métriques, les réseaux et d'autres informations pour le processus de routage OSPF.
show ip ospf interface	Utilisez cette commande pour : • afficher les intervalles de compteur et les contiguïtés ; • déterminer si OSPF est activé sur l'interface ; vérifier si les interfaces entre des routeurs OSPF sont situées dans la même zone OSPF.
show ip ospf neighbor	Affiche des informations de voisinage OSPF pour chaque interface.
show ip route	Affiche les routes connues du routeur et la manière dont elles ont été apprises. Cette commande est l'une des meilleures méthodes de détermination de la connectivité entre le routeur local et le reste de l'interréseau.

.

Utilisez la commande du mode privilégié **debug ip ospf events** pour afficher les informations suivantes sur les événements liés à l'OSPF:

- Contiguïtés
- Diffusion des informations
- Sélection du routeur désigné
- Calcul du plus court chemin d'abord (SPF)

Si un routeur configuré pour le routage OSPF ne voit pas un voisin OSPF sur un réseau attaché, procédez comme suit:

- Vérifiez que les deux routeurs ont été configurés avec le même masque IP, le même intervalle HELLO OSPF et le même intervalle d'arrêt OSPF.
- Vérifiez que les deux voisins font partie de la même zone.

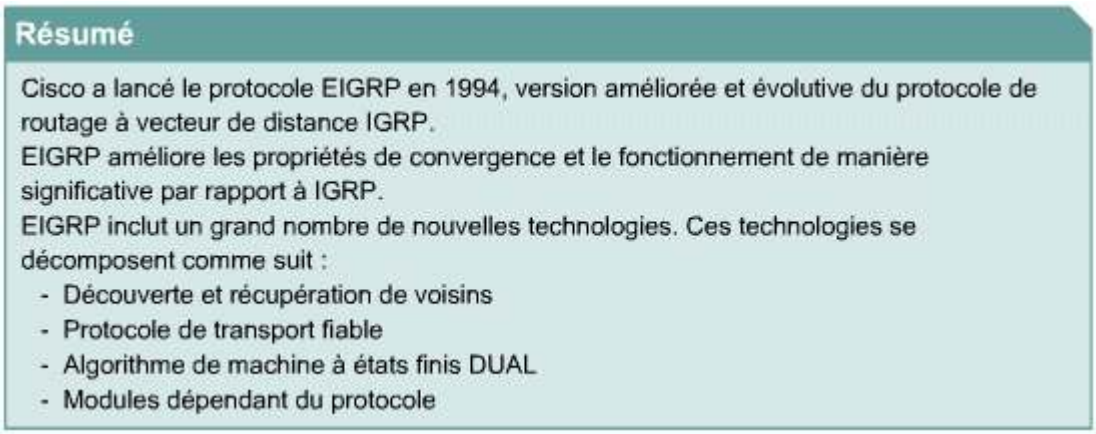
Pour afficher des informations sur chaque paquet OSPF reçu, utilisez la commande du mode privilégié **debug ip ospf packet**. La forme **no** de cette commande désactive l'affichage du message de débogage.

La commande **debug ip ospf packet** produit un ensemble d'informations pour chaque paquet reçu. Les informations affichées varient légèrement, selon l'authentification utilisée.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Différences entre l'EIGRP et l'IGRP
- Concepts clés, technologies et structures de données de l'EIGRP
- Convergence EIGRP et le fonctionnement de base de l'algorithme DUAL (Diffusing Update Algorithm)
- Configuration EIGRP de base
- Configuration du résumé de routes EIGRP
- Processus utilisés par l'EIGRP pour construire et mettre à jour des tables de routage
- Vérification des opérations EIGRP
- Huit étapes du processus de dépannage général
- Application d'un processus logique au dépannage du routage
- Dépannage d'un processus de routage RIP à l'aide des commandes **show** et **debug**
- Dépannage d'un processus de routage IGRP à l'aide des commandes **show** et **debug**
- Dépannage d'un processus de routage EIGRP à l'aide des commandes **show** et **debug**
- Dépannage d'un processus de routage OSPF à l'aide des commandes **show** et **debug**



Vue d'ensemble

La conception de réseaux LAN s'est généralisée et a évolué au fil du temps. Il n'y a pas si longtemps, les concepteurs utilisaient encore des concentrateurs et des ponts pour construire des réseaux. Aujourd'hui, les commutateurs et les routeurs constituent les composants essentiels d'une conception LAN et leurs fonctions et performances sont en constante amélioration.

Ce module renvoie à certaines origines des LAN Ethernet modernes en décrivant l'évolution d'Ethernet/802.3, l'architecture LAN la plus fréquemment déployée. Un rappel du contexte historique du développement des réseaux LAN et des diverses unités pouvant être utilisées au niveau des couches 1, 2 et 3 du modèle OSI aidera à mieux comprendre les raisons de l'évolution des équipements.

Auparavant, la plupart des réseaux Ethernet étaient construits à l'aide de répéteurs. Lorsque leurs performances ont commencé à se dégrader en raison du nombre excessif d'équipements qui se partageaient le même segment, les ingénieurs ont ajouté des ponts pour créer plusieurs domaines de collision. À mesure que les réseaux croissaient en taille et en complexité, les ponts évoluaient vers la commutation moderne avec la microsegmentation des réseaux. Aujourd'hui, les réseaux comprennent généralement des commutateurs et des routeurs, avec la fonction de routage et de commutation souvent assurée par le même équipement.

Les commutateurs modernes sont capables d'exécuter des tâches complexes et variées au sein d'un réseau. Ce module présente la technique de segmentation et décrit les principes de base de la commutation.

Les commutateurs et les ponts se partagent les tâches les plus lourdes d'un réseau LAN et les décisions qu'ils prennent lors de la réception des trames sont presque instantanées. Le présent module décrit en détail la façon dont les trames sont transmises et filtrées par les commutateurs et explique comment ces derniers apprennent les adresses physiques de tous les nœuds de réseau. Il traite également des principes de la segmentation LAN et des domaines de collision à titre d'introduction à l'utilisation de ponts et de commutateurs dans une conception LAN.

Les commutateurs sont des équipements de couche 2 qui permettent d'accroître la bande passante disponible et de réduire la congestion des réseaux. Un commutateur peut diviser un LAN en microsegments, qui sont des segments à hôte unique. La microsegmentation crée de multiples domaines sans collision à partir d'un grand domaine de collision. En tant qu'équipement de couche 2, un commutateur LAN augmente le nombre de domaines de collision, mais tous les hôtes connectés au commutateur appartiennent toujours au même domaine de broadcast.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Décrire l'historique et la fonction de Ethernet half-duplex à média partagé
- Définir le principe de collision dans le contexte de réseau Ethernet
- Définir la microsegmentation
- Définir la détection de signal avec accès multiple et détection de collision (CSMA/CD)
- Décrire quelques éléments clés pouvant affecter la performance des réseaux
- Décrire la fonction des répéteurs/concentrateurs
- Définir la latence d'un réseau
- Définir le temps de transmission
- Définir la segmentation réseau avec des routeurs, des commutateurs et des ponts
- Définir la latence d'un commutateur Ethernet
- Expliquer les différences entre la commutation de couche 2 et de couche 3
- Définir la commutation symétrique et asymétrique
- Définir la mise en mémoire tampon
- Comparer et différencier les mode de commutation "store-and-forward" et "cut-through"
- Comprendre les différences entre les concentrateurs, les ponts et les commutateurs
- Décrire les fonctions principales des commutateurs
- Énumérer les principaux modes d'acheminement des trames des commutateurs
- Décrire le processus par lequel les commutateurs apprennent les adresses MAC
- Identifier et définir les modes d'acheminement
- Définir la segmentation LAN
- Définir la microsegmentation en utilisant le commutateur
- Décrire le processus de filtrage de trame
- Comparer et différencier les domaines de collision des domaines de broadcast
- Identifier les câbles nécessaires à l'interconnexion des commutateurs et des stations de travail
- Identifier les câbles nécessaires à l'interconnexion des commutateurs entre eux

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Personnalisation de la configuration d'un commutateur pour répondre aux exigences du réseau		• Comparaison des principales caractéristiques des environnements LAN

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Personnalisation de la configuration d'un commutateur pour répondre aux exigences du réseau		• Comparaison des principales caractéristiques des environnements LAN

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Personnalisation de la configuration d'un commutateur pour répondre aux exigences du réseau		• Évaluation des caractéristiques des environnements LAN

4.1 Présentation des réseaux LAN Ethernet/802.3

4.1.1 Développement des réseaux LAN Ethernet/802.3

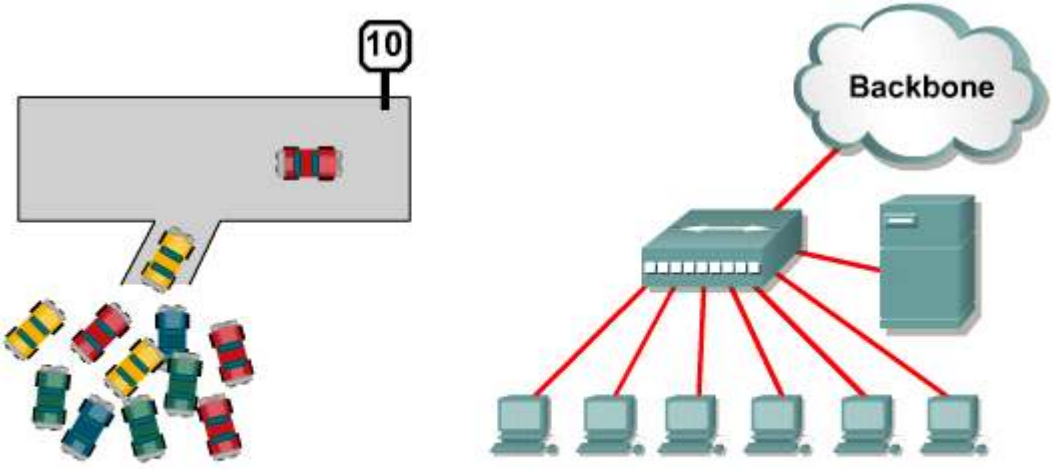
Les anciennes technologies LAN utilisaient généralement des infrastructures Ethernet à câble épais ou fin. 1 Il est important de comprendre certaines limites de ces infrastructures pour connaître l'impact des commutateurs actuels.

L'ajout de concentrateurs (aussi appelé hub) dans les réseaux a contribué à améliorer la technologie Ethernet à câble épais ou fin. Un concentrateur est un équipement de couche 1 parfois appelé concentrateur Ethernet ou répéteur multiport. L'introduction de concentrateurs dans un réseau a permis d'élargir l'accès de ce dernier à un nombre plus élevé d'utilisateurs. En outre, les concentrateurs actifs ont permis aux réseaux de couvrir de plus grandes distances. Pour ce faire, un concentrateur régénère le signal de données. Il ne prend aucune décision lorsqu'il reçoit des signaux de données. Il regénère et amplifie le signal reçu avant de le transmettre à toutes les unités connectées à l'exception de celle d'où origine le signal.

Ethernet à câble épais
- Limité à 500 mètres avant une dégradation des signaux
- Répéteurs nécessaires tous les 500 mètres
- Limitations liées au nombre de stations et à leur emplacement
- Mise en place difficile et onéreuse dans les bâtiments
- Ajout d'utilisateurs relativement simple
- Bande passante partagée de 10 Mbits/s

Ethernet à câble fin
- Un segment Ethernet à câble fin (10Base-2) peut parcourir une distance maximale de 185 mètres.
- Répéteurs nécessaires tous les 185 mètres
- Moins onéreux et nécessite moins d'espace que les réseaux Ethernet à câble épais
- Mise en place toujours difficile dans les bâtiments
- Interruptions réseau nécessaires pour l'ajout d'utilisateurs

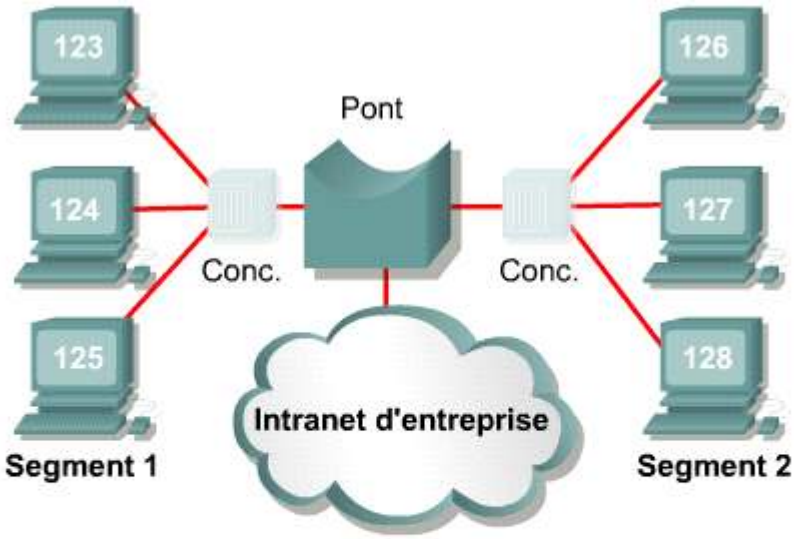
Ethernet est essentiellement une technologie partagée où tous les utilisateurs d'un segment LAN donné convoitent la même bande passante disponible. Cette situation est comparable plusieurs véhicules qui tentent d'accéder en même temps à une route à une voie. Comme la route n'a qu'une voie, un seul véhicule à la fois peut y accéder. Les concentrateurs ont donc augmenté le nombre d'utilisateurs d'un réseau en quête de la même bande passante. 2



Les collisions sont dérivées des réseaux Ethernet. Si deux ou plusieurs équipements tentent de transmettre simultanément, il se produit une collision, tout comme deux véhicules s'engageant en même temps sur la même voie. Le trafic est refoulé jusqu'à ce que la voie soit dégagée. Un nombre excessif de collisions sur un réseau entraîne un ralentissement des temps de réponse. Il en résulte un encombrement du réseau ou une augmentation des tentatives d'accès simultanées.

Les équipements de couche 2 sont plus intelligents que ceux de la couche 1. Ils prennent des décisions de transmission sur la base des adresses MAC *(Media Access Control)* contenues dans les en-têtes des trames de données acheminées.

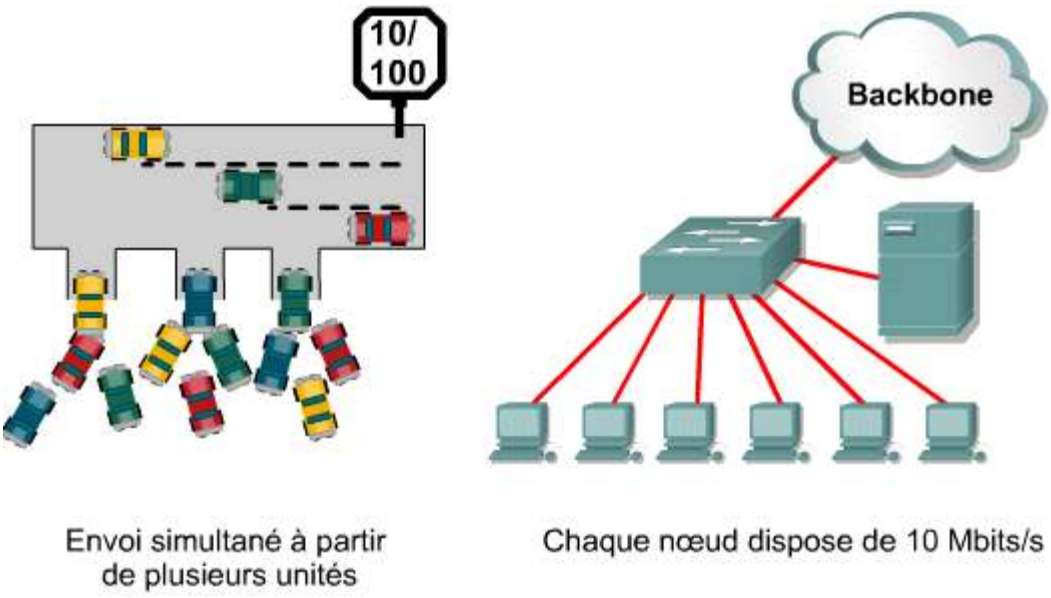
Un pont est un équipement de couche 2 qui permet de diviser ou de segmenter un réseau. Il est capable de collecter et de transmettre des trames de données de façon sélective entre deux segments de réseau. Pour ce faire, il apprend l'adresse MAC de tous les équipements de chaque segment connecté. À l'aide de cette information, il crée une table de pontage et achemine ou bloque le trafic en se basant sur cette table. Il en résulte des domaines de collision de plus petite taille et une efficacité accrue du réseau. 3 Les ponts ne limitent pas le trafic de broadcast. Ils renforcent néanmoins le contrôle du trafic au sein d'un réseau.



- Les ponts sont plus intelligents que les concentrateurs.
- Les ponts " écoutent " les conversations pour apprendre des informations et mettre à jour les tables d'adressage.
- Les ponts recueillent et passent des trames entre deux segments du réseau.
- Les ponts contrôlent le trafic vers le réseau.

Un commutateur est également un équipement de couche 2 parfois appelé pont multiport. Il prend des décisions de transmission en se basant sur les adresses MAC contenues dans les trames de données acheminées. De plus, il apprend les adresses MAC des équipements connectés à chaque port et insère ces informations dans une table de commutation.

Les commutateurs créent un circuit virtuel entre deux unités connectées qui souhaitent communiquer. Une fois ce circuit créé, un chemin de communication dédié est établi entre les deux unités. La mise en œuvre d'un commutateur introduit la microsegmentation sur un réseau. En théorie, il crée un environnement exempt de collisions entre la source et la destination, ce qui permet d'optimiser l'utilisation de la bande passante disponible. Il facilite également la création de multiples connexions simultanées de circuits virtuels, à la manière d'une autoroute divisée en plusieurs voies où chaque véhicule dispose de sa propre voie. [4]



Cependant, les équipements de couche 2 présentent l'inconvénient de transmettre des trames de broadcast à tous les équipements connectés au réseau. Un nombre excessif de broadcasts sur un réseau entraîne un ralentissement des temps de réponse.

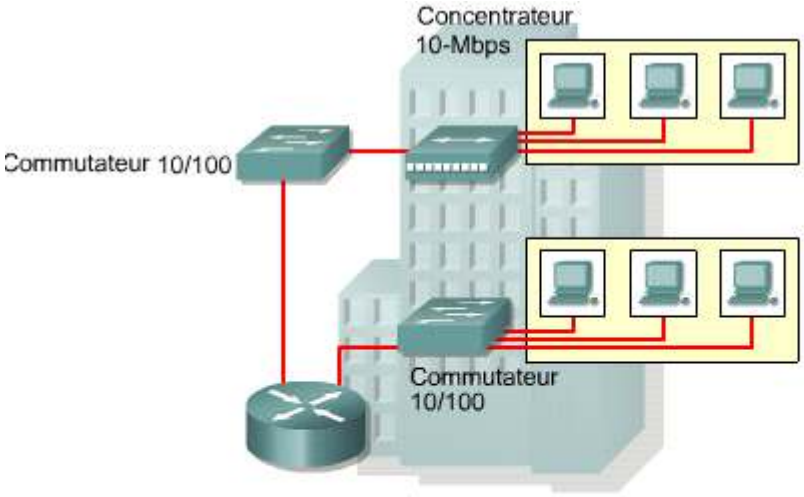
Un routeur est un équipement de couche 3. Il prend des décisions en se basant sur les groupes d'adresses réseau, ou classes, et non sur les adresses MAC individuelles de couche 2. Les routeurs utilisent des tables de routage pour enregistrer les adresses de couche 3 des réseaux directement connectés aux interfaces locales et aux chemins de réseau appris par les routeurs voisins.

Un routeur assure toutes les fonctions suivantes:

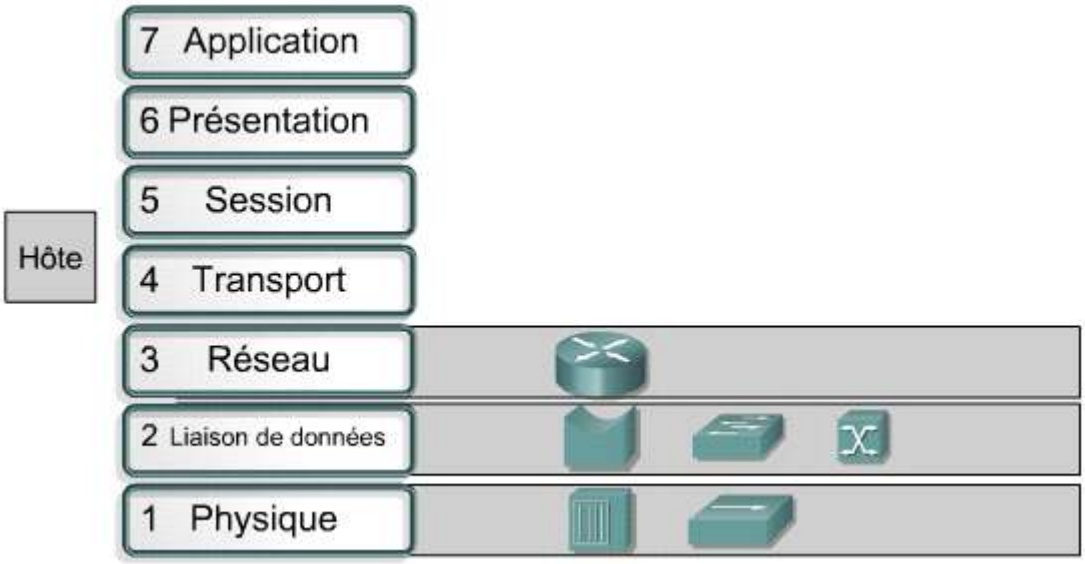
- il examine les paquets de données entrants de couche 3;
- il sélectionne le meilleur chemin pour ces paquets sur le réseau;
- il les commute vers le port de sortie approprié.

Les routeurs n'acheminent pas par défaut les paquets broadcast à moins d'être configurés explicitement pour le faire. Par conséquent, ils réduisent la taille des domaines de collision et de broadcast. Sur les grands réseaux, ils constituent les équipements de régulation du trafic les plus importants. Ils permettent à la plupart des ordinateurs de communiquer entre eux, quels que soient leur type et leur emplacement.

En général, les réseaux LAN se composent d'une combinaison d'équipements de couche 1, 2 et 3. La mise en œuvre de ces équipements dépend de facteurs propres aux besoins de l'organisation. [5] [6]



- Les routeurs permettent une évolutivité.
- Les ressources sont pour la plupart commutées, mis à part certaines qui sont partagées.
- Les groupes d'utilisateurs sont déterminés d'après leur emplacement physique.



Activité de média interactive

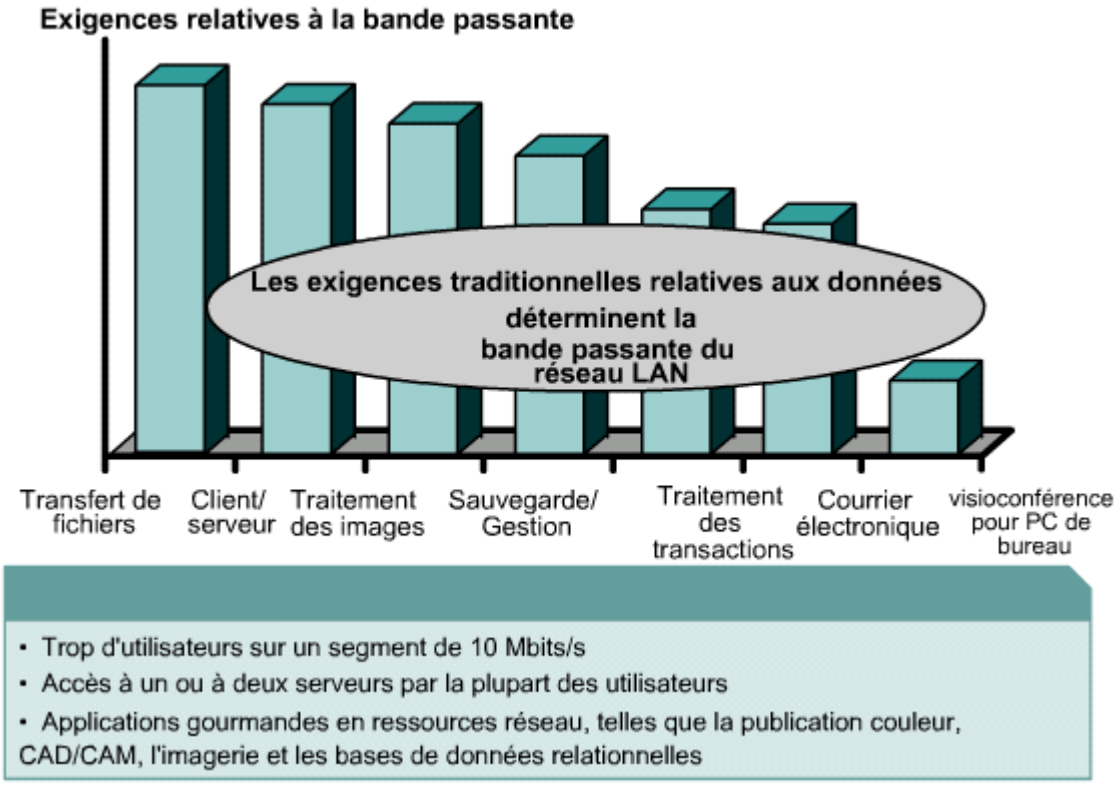
Glisser-Positionner: Fonction du matériel au niveau des couches

À la fin de cette activité, les étudiants seront en mesure d'identifier les différentes couches OSI dans le cadre du fonctionnement des activités réseau.

4.1 Présentation des réseaux LAN Ethernet/802.3

4.1.2 Facteurs ayant une incidence sur les performances du réseau

Les LAN modernes sont de plus en plus congestionnés et surchargés. Outre le nombre croissant d'utilisateurs, un ensemble de plusieurs facteurs a contribué à démontrer les limites des capacités des LAN traditionnels. 1

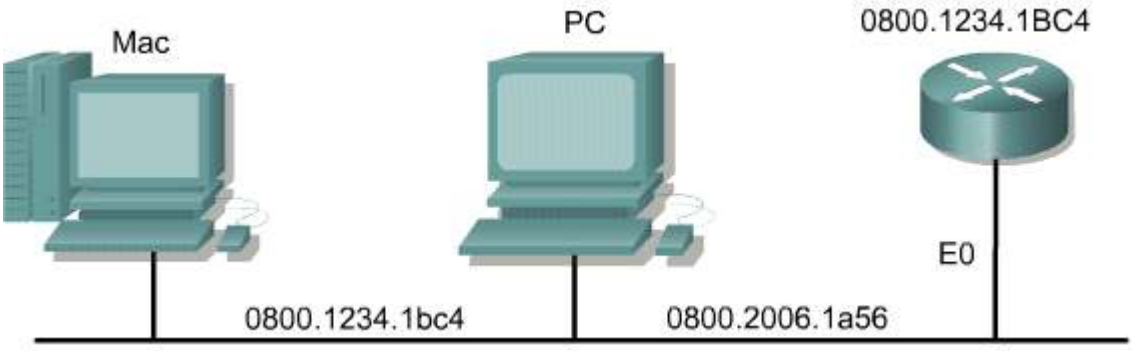


- L'environnement multitâche des systèmes d'exploitation actuels pour ordinateur de bureau tels que Windows, Unix/Linux et Mac OS X permet d'effectuer des transactions réseau simultanées. Cette capacité accrue a entraîné une augmentation de la demande en ressources réseau.
- L'utilisation d'applications fortement consommatrices de ressources réseau telles qu'Internet ne cesse de croître. Les applications client-serveur permettent aux administrateurs de centraliser les informations, ce qui facilite la gestion et la protection de celles-ci.
- Les applications client-serveur libèrent les stations de travail locales de la gestion des informations et des coûts inhérents à la fourniture de l'espace disque nécessaire à leur stockage. Étant donné l'avantage économique que présentent les applications client-serveur, elles sont appelées à se généraliser dans le futur.

4.1 Présentation des réseaux LAN Ethernet/802.3

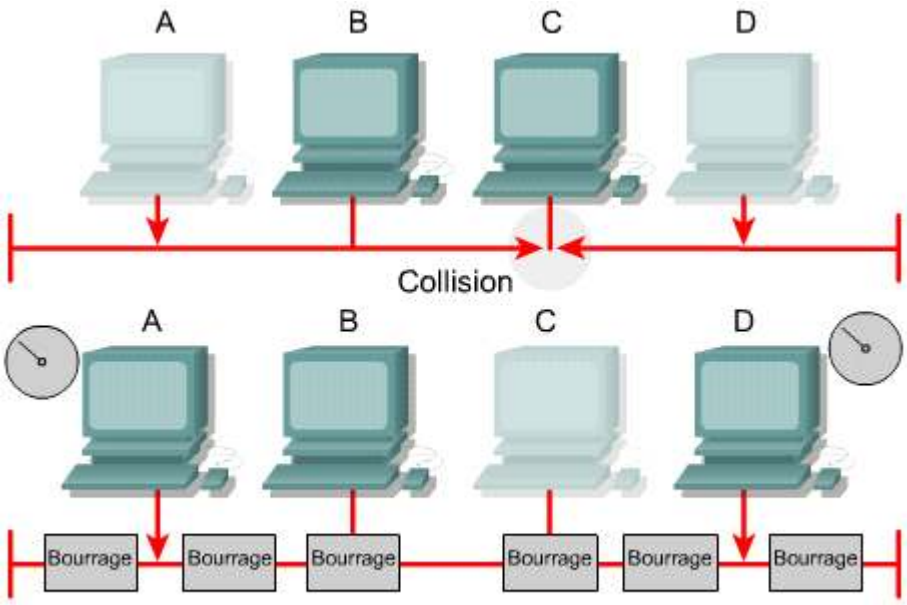
4.1.3 Éléments d'un réseau Ethernet/802.3

Ethernet est une technologie de transmission broadcast. Ainsi, les unités d'un réseau tels que des ordinateurs, des imprimantes et des serveurs de fichiers communiquent entre eux par l'entremise d'un média partagé. Plusieurs facteurs peuvent avoir un effet négatif sur la performance d'un LAN Ethernet/802.3 à média partagé :1



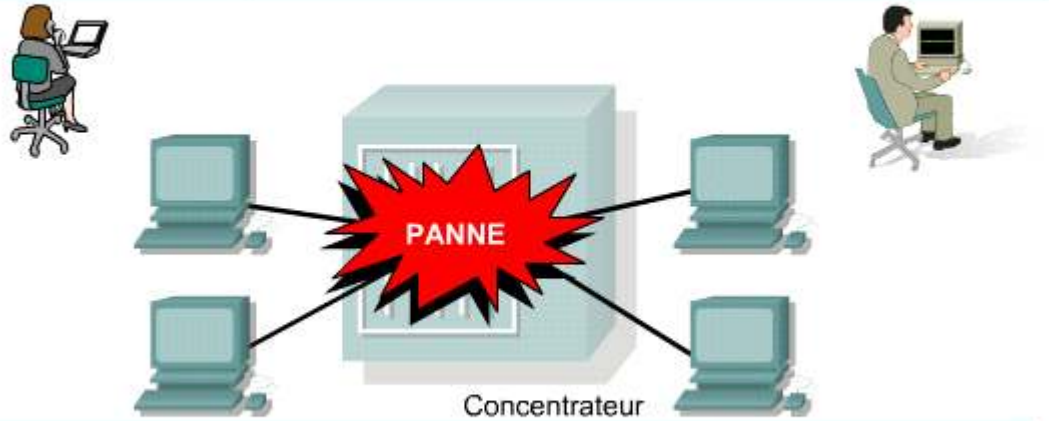
- L'acheminement des trames de données des LAN Ethernet/802.3 est de type broadcast.
- Le mode de détection de porteuse avec accès multiple et détection de collision (CSMA/CD) ne permet qu'à une seule station à la fois de transmettre.
- Les applications multimédia fortement consommatrices de bande passante, comme les applications vidéo et Internet, conjuguées à la nature broadcast d'Ethernet, peuvent entraîner des problèmes de congestion sur le réseau.
- Une latence normale se produit lorsque des trames se déplacent sur le média partagé et à travers les unités réseau.

Ethernet utilise la détection de signal avec accès multiple et détection de collision (CSMA/CD) et peut supporter des vitesses de transmission très élevées. La technologie Fast Ethernet, ou 100Base-TX permet d'atteindre des vitesses allant jusqu'à 100 Mbits/s. La technologie Gigabit Ethernet supporte jusqu'à 1000 Mbits/s et la technologie Ethernet 10-Gigabit jusqu'à 10 000 Mbits/s. L'objectif d'Ethernet est de fournir un service d'acheminement au mieux et d'offrir les mêmes possibilités de transmission à toutes les unités partageant le média. Le phénomène de collisions est normal dans des réseaux de type Ethernet mais il peut toutefois devenir un problème majeur. [2] [3]



Détection de porteuse avec accès multiple (CSMA/CD)

- " J'aurais déjà pu me rendre jusqu'au service des finances. "
- " Je savais que j'aurais dû rester à la maison. "
- " Les transferts de fichiers prennent un temps fou. "
- " J'attends tout le temps. "



- Lenteur de réponse du réseau
- Augmentation du nombre de plaintes de la part des utilisateurs

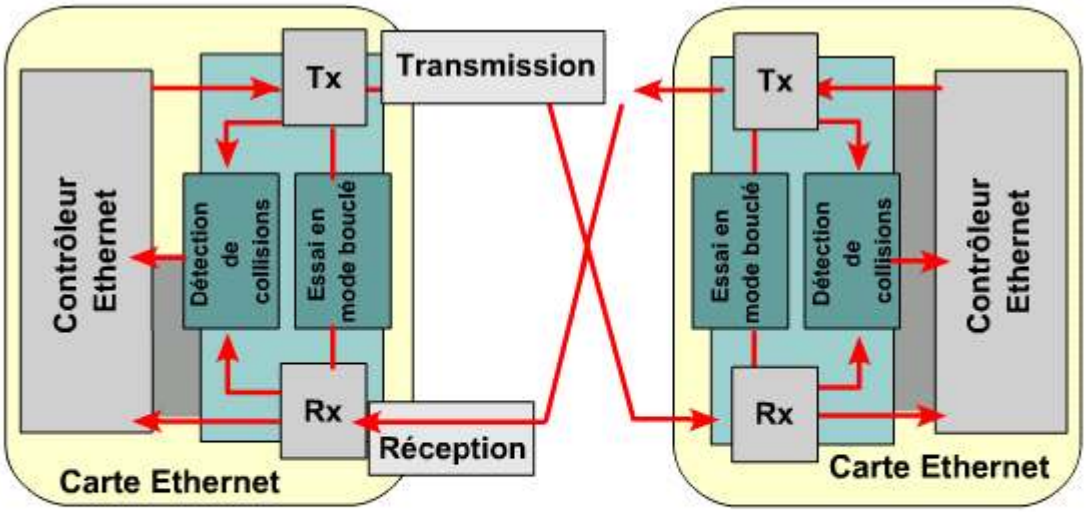
4.1 Présentation des réseaux LAN Ethernet/802.3

4.1.4 Réseaux half-duplex

Ethernet était initialement une technologie half-duplex : un hôte pouvait soit transmettre, soit recevoir, mais ne pouvait pas transmettre et recevoir simultanément. Chaque hôte Ethernet vérifie si des données sont en cours de transmission sur le réseau avant de transmettre d'autres données. Si le réseau est en cours d'utilisation, la transmission est retardée. Malgré le report de transmission, plusieurs hôtes Ethernet peuvent transmettre simultanément, ce qui engendre une collision. Lorsqu'une collision se produit, l'hôte qui détecte la collision en premier envoie aux autres hôtes un signal de bourrage. Dès

réception de ce signal, chaque hôte arrête de transmettre, puis attend une période aléatoire avant d'essayer de retransmettre. L'algorithme de temporisation génère ce délai aléatoire. Plus le nombre d'hôtes transmettant sur un réseau augmente, plus le risque de collision est élevé.

L'exécution de logiciels gourmands en ressources réseau, comme les applications client-serveur qui incitent les hôtes à transmettre plus souvent et plus longtemps, entraîne la saturation des LAN Ethernet. La carte réseau dont sont dotées les unités LAN fournit plusieurs circuits de façon à favoriser la communication entre ces unités. 1

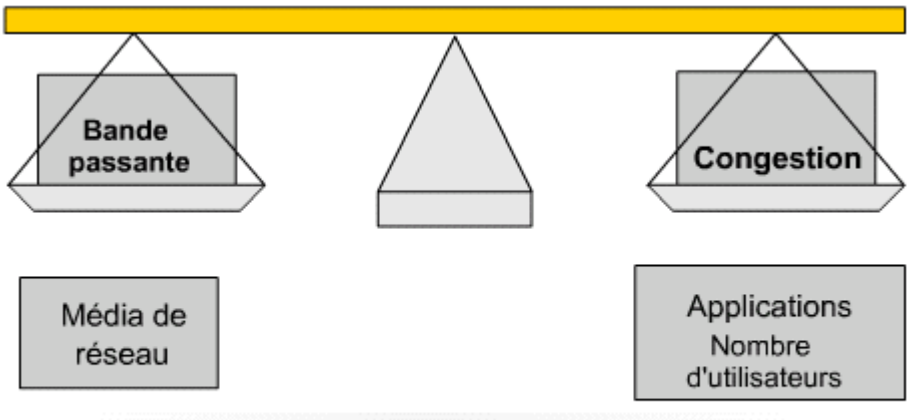


- Les fonctions les plus importantes sont la réception (Rx), la transmission (Tx) et la détection de collisions.
- Le connecteur physique Ethernet fournit plusieurs circuits.

4.1 Présentation des réseaux LAN Ethernet/802.3

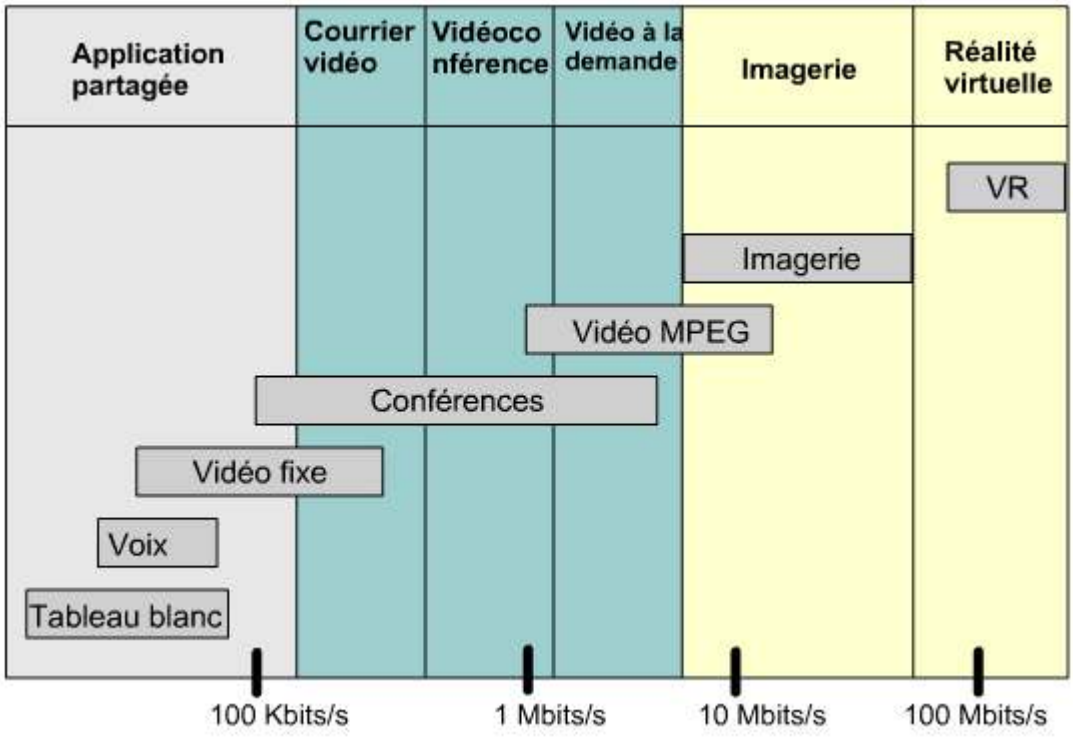
4.1.5 Congestion d'un réseau

Les progrès technologiques permettent de fabriquer des stations de travail et des ordinateurs de bureau de plus en plus rapides et intelligents. La combinaison de stations de travail de plus en plus puissantes à des applications fortement consommatrices de ressources réseau exige une capacité réseau ou une bande passante plus importante. 1



L'équilibre repose sur une bande passante suffisante pour répondre aux besoins des utilisateurs et des applications.

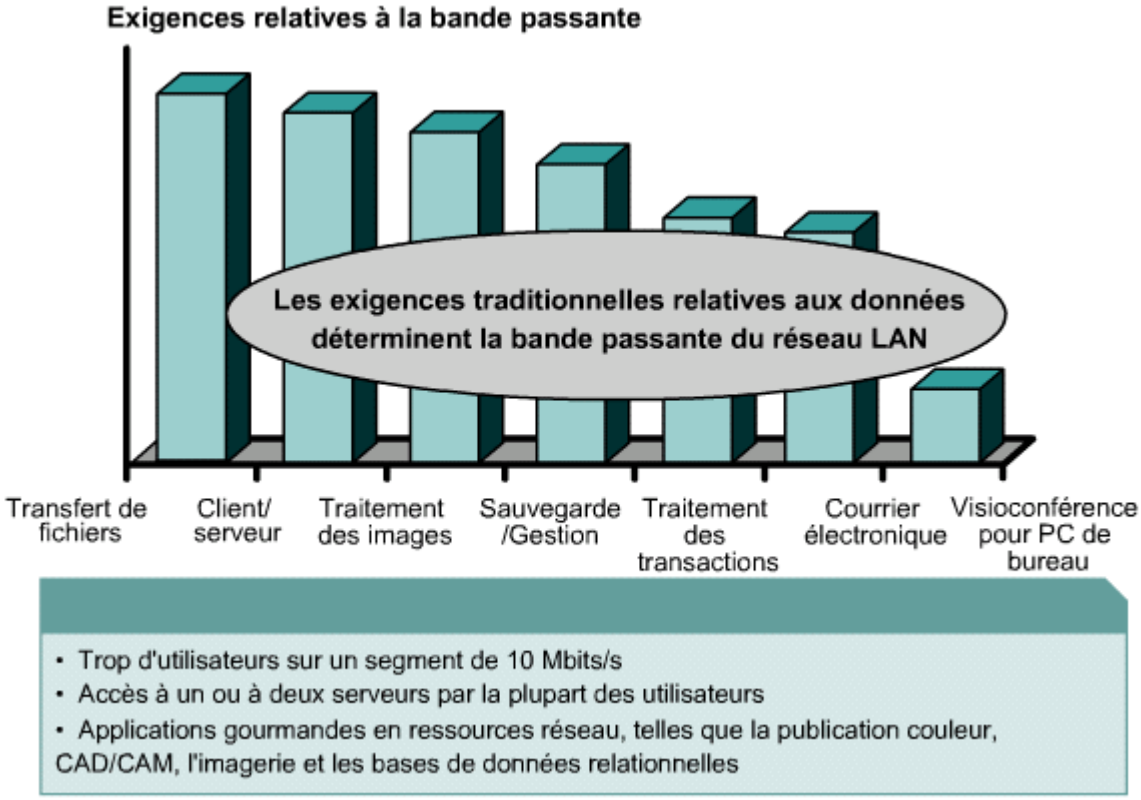
Les besoins excèdent dorénavant les 10 Mbits/s et plusieurs organisations doivent maintenant supporter une bande passante de 100 Mbits/s sur leur réseau. Tous ces facteurs contribuent à placer davantage de contraintes sur les réseaux n'offrant qu'une bande passante limitée à 10 Mbits/s. 2



Les réseaux actuels doivent transmettre un nombre accru de médias de divers formats:

- fichiers graphiques de grande taille,
- images,
- animations vidéo,
- applications multimédias.

Le nombre d'utilisateurs est également en constante augmentation. Tous ces facteurs sollicitent davantage la bande passante disponible. L'augmentation du nombre d'utilisateurs qui partagent de gros fichiers, accèdent à des serveurs de fichiers et se connectent à Internet entraîne des congestions de réseau. Cela se traduit par un ralentissement des temps de réponse et des transferts de fichiers, ainsi que par une diminution de la productivité des utilisateurs du réseau. Pour décongestionner un réseau, il convient d'accroître la bande passante ou d'utiliser plus efficacement la bande passante disponible. 3



4.1 Présentation des réseaux LAN Ethernet/802.3

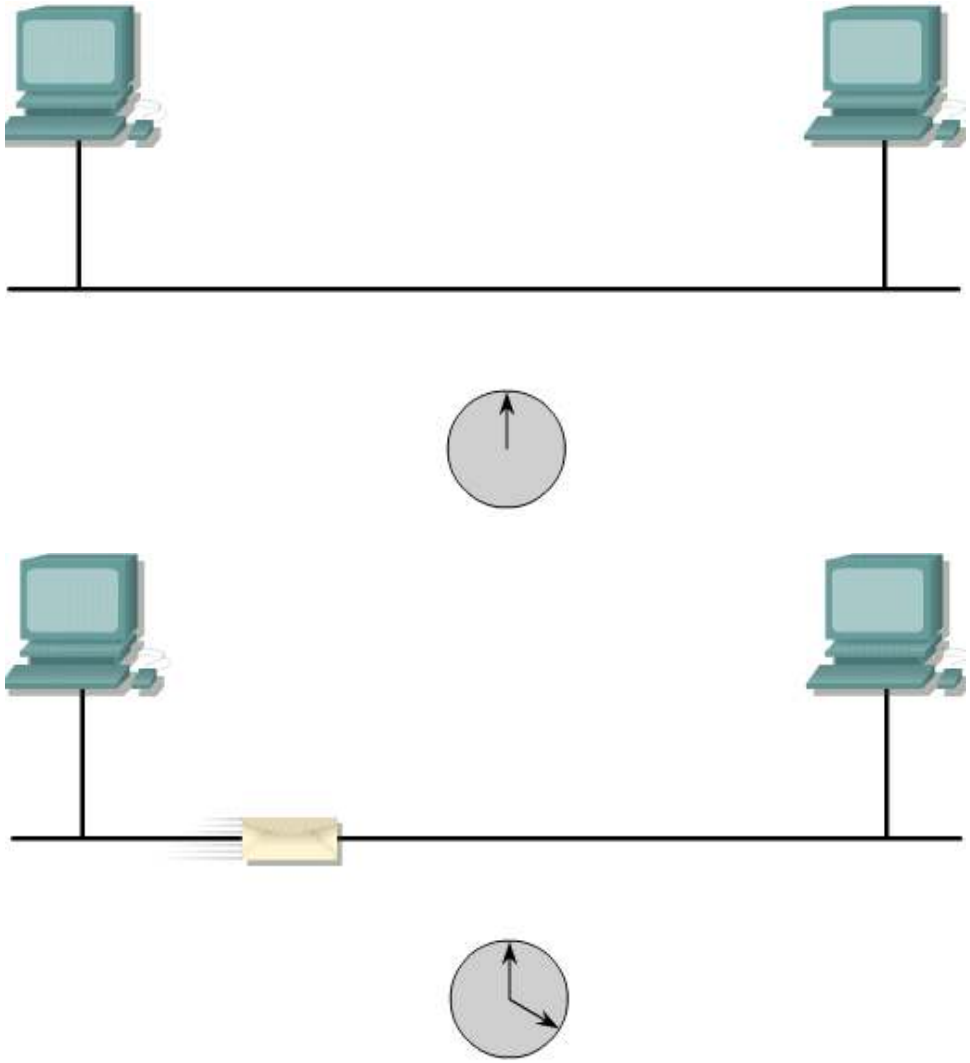
4.1.6 Latence d'un réseau

La latence, parfois appelée délai, est le temps nécessaire à une trame ou à un paquet pour circuler entre sa station d'origine et sa destination finale. Il est important d'évaluer la latence totale du chemin entre l'origine et la destination pour les LAN et les WAN. Dans le cas d'un LAN Ethernet, il est vital de bien comprendre le concept de latence et ses effets sur la synchronisation réseau, afin de déterminer si la détection de porteuse avec accès multiple et détection de collision (CSMA/CD) fonctionnera correctement pour détecter les collisions et négocier les transmissions.

Il existe au moins trois causes de latence:

- Premièrement, le temps nécessaire à la carte réseau d'origine pour placer des impulsions électriques sur le fil, plus le temps nécessaire à la carte réseau réceptrice pour interpréter ces impulsions. Cette cause est parfois appelée délai de carte réseau, qui est généralement de 1 microseconde pour les cartes réseau 10BaseT).
- Deuxièmement, le délai de propagation réel du signal traversant le câble. En général, ce délai est d'environ 0,556 microseconde par 100 m de câble à paires torsadées non blindées (UTP) de catégorie 5. Des câbles plus longs et une vitesse de propagation nominale (NVP) plus lente augmentent ce délai.
- Enfin, le temps de latence dépendant des unités réseau de couche 1, 2 ou 3 ajoutées sur le chemin entre les deux ordinateurs qui communiquent.

La latence ne dépend pas uniquement de la distance et du nombre d'unités. Par exemple, si trois commutateurs correctement configurés séparent deux stations de travail, ces dernières subiront moins de latence que si elles étaient séparées par deux routeurs correctement configurés car les routeurs gèrent des fonctions plus longues et plus complexes. En effet, un routeur doit analyser des données de couche 3. 1



4.1 Présentation des réseaux LAN Ethernet/802.3

4.1.7 Temps de transmission Ethernet 10BaseT

Tous les réseaux connaissent ce que les spécialistes appellent la « durée d'un bit » ou une « tranche de temps ». De nombreuses technologies LAN, dont Ethernet, définissent la durée d'un bit comme l'unité de base au cours de laquelle UN bit est envoyé. Pour que les équipements électroniques ou optiques soient en mesure de reconnaître un 1 ou un 0 binaire, il doit exister une période minimale durent laquelle le bit est actif ou non.

Le temps de transmission est égal au nombre de bits envoyés multiplié par la durée d'un bit d'une technologie donnée. Une autre manière de visualiser le temps de transmission est de considérer l'intervalle de temps entre le début et la fin d'une transmission ou encore, l'intervalle entre le début de transmission d'une trame et une collision. Le temps de transmission des trames de petite taille est plus court que celui des trames de grande taille. 1

Taille de trame en octets	Durée de transmission en microsecondes
64	51.2
512	410
1000	800
1518	1214

Chaque bit Ethernet 10 Mbits/s dispose d'une fenêtre de transmission de 100 ns. Il s'agit de la durée du bit. Comme un octet équivaut à 8 bits, la transmission d'un octet nécessite au moins 800 ns. Une trame de 64 octets, la plus petite trame 10BaseT admise par un réseau CSMA/CD pour garantir un bon fonctionnement, nécessite 51 200 ns (51,2 microsecondes). La transmission de l'intégralité d'une trame de 1 000 octets à partir de la station d'origine nécessite seulement 800 microsecondes. Le moment auquel la trame arrive réellement sur la station de destination dépend de la latence supplémentaire induite par le réseau. Cette latence peut être due à divers délais, notamment aux suivants :

- délais de la carte réseau,
- délais de propagation,
- délais des couches 1, 2 et 3.

Activité de média interactive

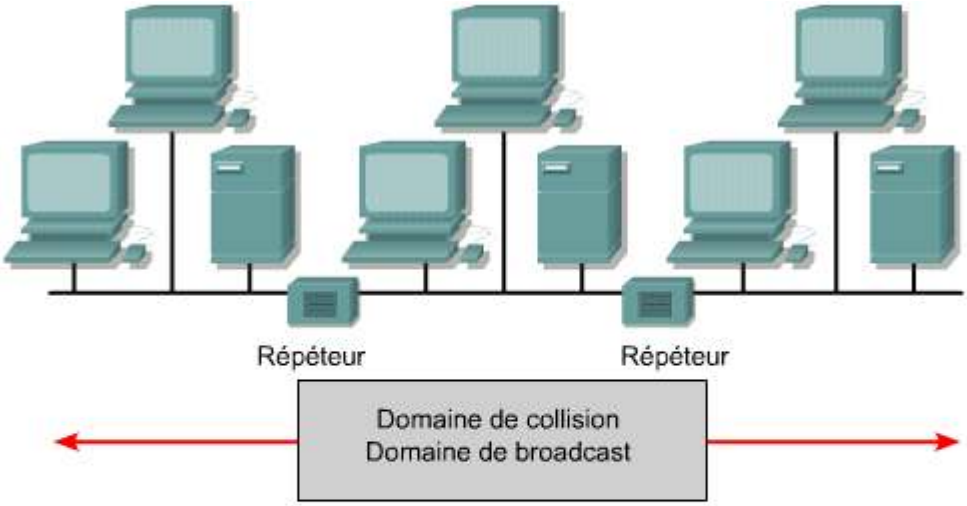
Glisser-Positionner: Temps de transmission 10BaseT

À la fin de cette activité, les étudiants seront en mesure d'identifier les temps de transmission 10BaseT.

4.1 Présentation des réseaux LAN Ethernet/802.3

4.1.8 Avantages des répéteurs

La distance pouvant être couverte par un réseau LAN est limitée en raison de l'atténuation. Ce terme désigne l'affaiblissement du signal qui circule sur le réseau. La résistance du câble ou du média à travers lequel passe le signal est à l'origine de la perte de puissance du signal. Un répéteur Ethernet est une unité réseau de couche physique qui amplifie ou régénère le signal sur un LAN Ethernet. Lorsqu'un répéteur est utilisé pour prolonger la distance d'un LAN, il permet à un réseau de couvrir une plus grande distance et d'être partagé par un plus grand nombre d'utilisateurs. Cependant, l'utilisation de répéteurs et de concentrateurs complique les problèmes liés aux broadcasts et aux collisions. Elle a aussi un effet négatif sur les performances globales d'un LAN à média partagé. [1] [2]



- Les répéteurs sont des équipements de couche 1 qui régénèrent le signal avant de le transmettre.
- Les répéteurs autorisent des distances de bout en bout supérieures.
- Les répéteurs augmentent la taille du domaine de collision.
- Les répéteurs augmentent la taille du domaine de broadcast.

Activité de média interactive

Agrandissement: Microconcentrateur Cisco 1503

Dans cette vue agrandie, l'étudiant peut voir un microconcentrateur Cisco 1503.

4.1 Présentation des réseaux LAN Ethernet/802.3

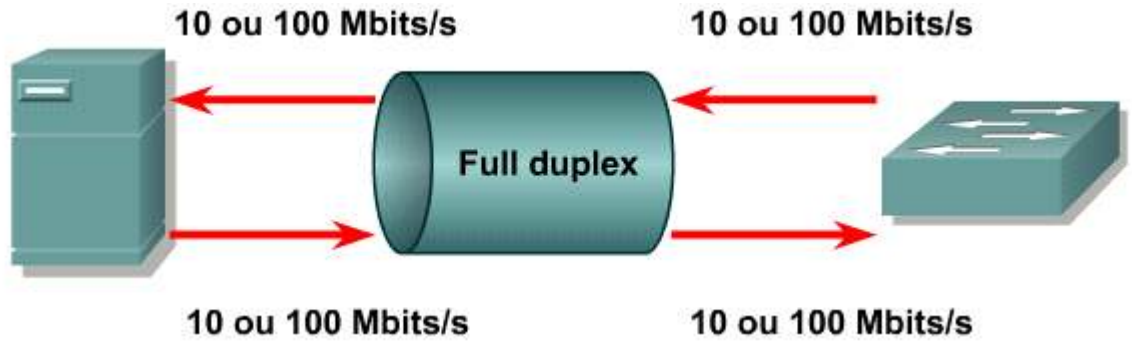
4.1.9 Transmission full duplex

Le mode Ethernet full duplex permet de transmettre un paquet et d'en recevoir un autre simultanément. Les transmissions et réceptions simultanées nécessitent l'utilisation d'un câble à deux paires de fils et d'une connexion commutée entre chaque nœud. Cette connexion est considérée comme une connexion point à point et s'effectue sans collision. Comme les deux nœuds peuvent transmettre et recevoir en même temps, la bande passante n'est pas négociée. Les réseaux Ethernet full duplex peuvent utiliser une infrastructure de câblage existante pour autant que le média réponde aux normes Ethernet minimales.

Pour transmettre et recevoir simultanément, un port de commutateur dédié est nécessaire pour chaque nœud. Les connexions en mode full duplex peuvent utiliser un média 10BaseT, 100BaseTX ou 100BaseFX pour créer des connexions point-à-point. Les cartes réseau de tous les équipements connectés doivent être dotées des caractéristiques full duplex.

Un commutateur Ethernet full duplex exploite les avantages des deux paires de fils du câble en créant une connexion directe entre la transmission (TX) à une extrémité du circuit et la réception (RX) à l'autre extrémité. Lorsque deux stations sont ainsi connectées, un environnement exempt de domaine de collision est créé, car la transmission et la réception des données s'effectuent sur deux circuits non concurrents.

En règle générale, Ethernet utilise seulement de 50 à 60 % des 10 Mbits/s de bande passante disponible en raison des collisions et de la latence. Le mode Ethernet full duplex offre 100 % de la bande passante dans les deux directions, ce qui produit un débit potentiel de 20 Mbits/s, c'est-à-dire 10 Mbits/s en transmission et 10 Mbits/s en réception. 1



- Double la bande passante entre des nœuds (par exemple, un commutateur et un serveur)
- Transmission sans collision
- Deux chemins de données de 10 ou 100 Mbits/s

Activité de média interactive

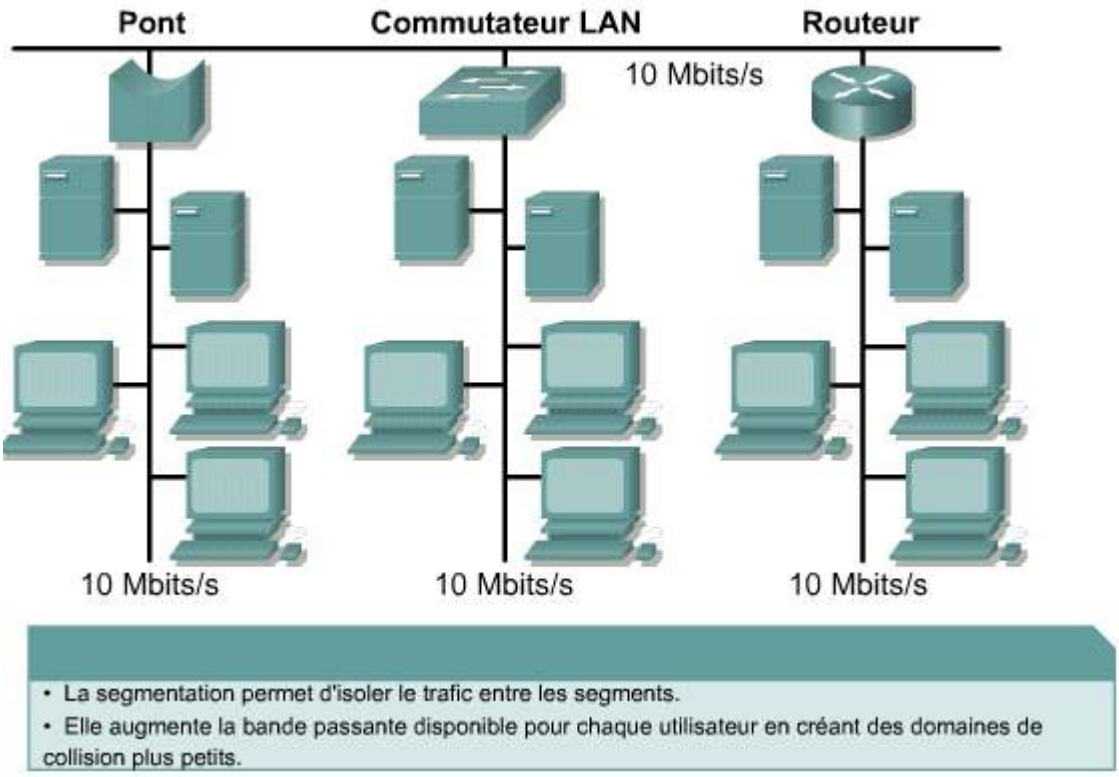
Glisser-Positionner: Ethernet full duplex

À la fin de cette activité, les étudiants seront en mesure d'identifier les exigences du mode Ethernet full duplex.

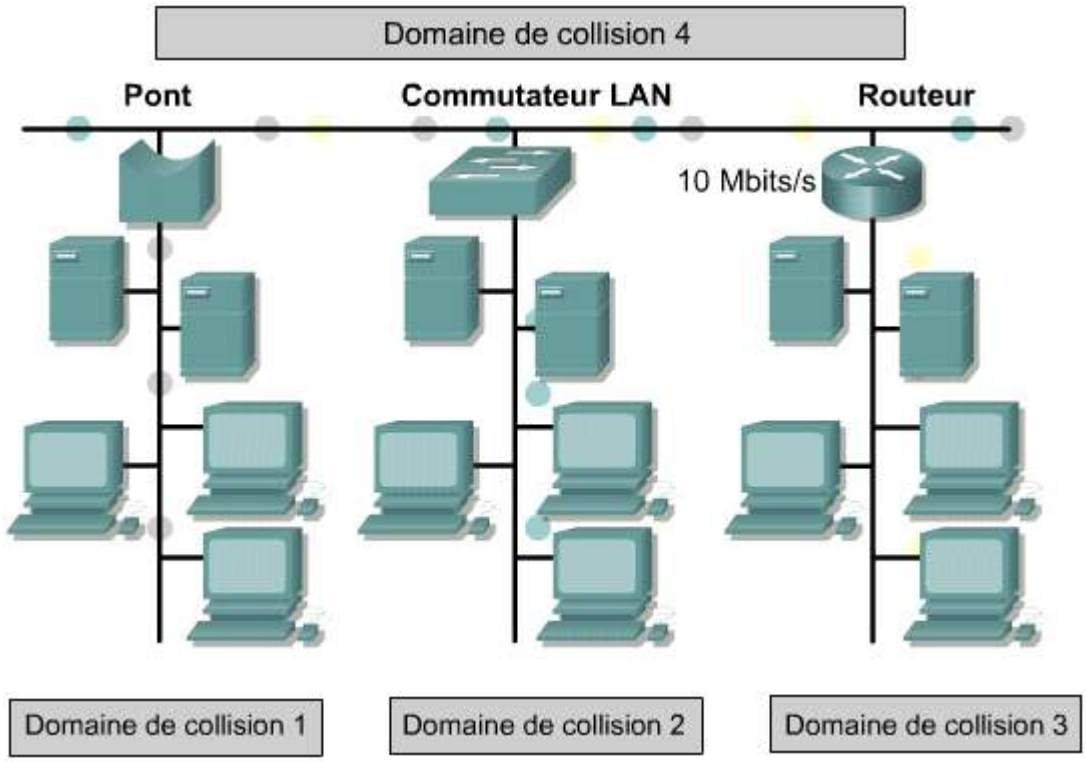
4.2 Introduction à la commutation LAN

4.2.1 Segmentation LAN

Un réseau peut être divisé en unités plus petites appelées segments. La figure 1



illustre un exemple de réseau Ethernet segmenté. Le réseau comprend quinze ordinateurs. Sur ces quinze ordinateurs, six sont des serveurs et neuf des stations de travail. Chaque segment utilise le mode d'accès CSMA/CD et assure le trafic entre les utilisateurs sur le segment. Chaque segment constitue son propre domaine de collision. 2

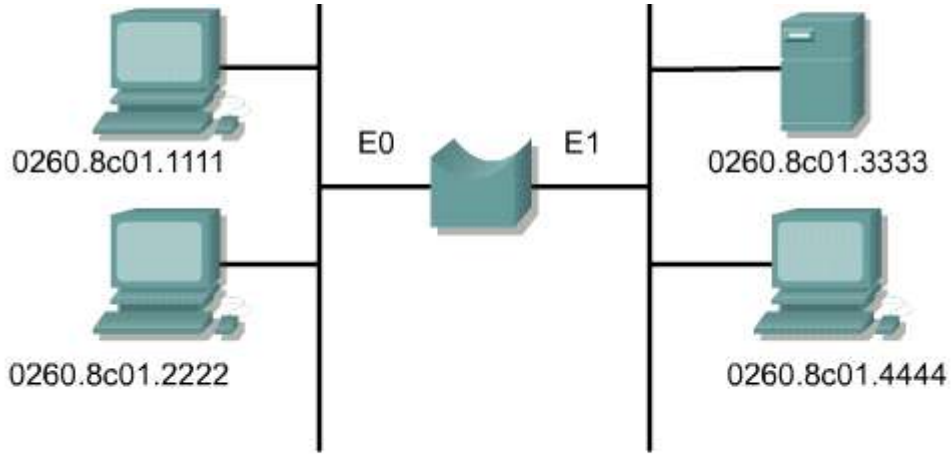


La segmentation permet de réduire significativement la congestion du réseau au sein de chaque segment. Lors de la transmission des données dans un segment, les équipements du segment se partagent la totalité de la bande passante disponible. Les données échangées entre les segments sont transmises au backbone du réseau via un pont, un routeur ou un commutateur.

4.2 Introduction à la commutation LAN

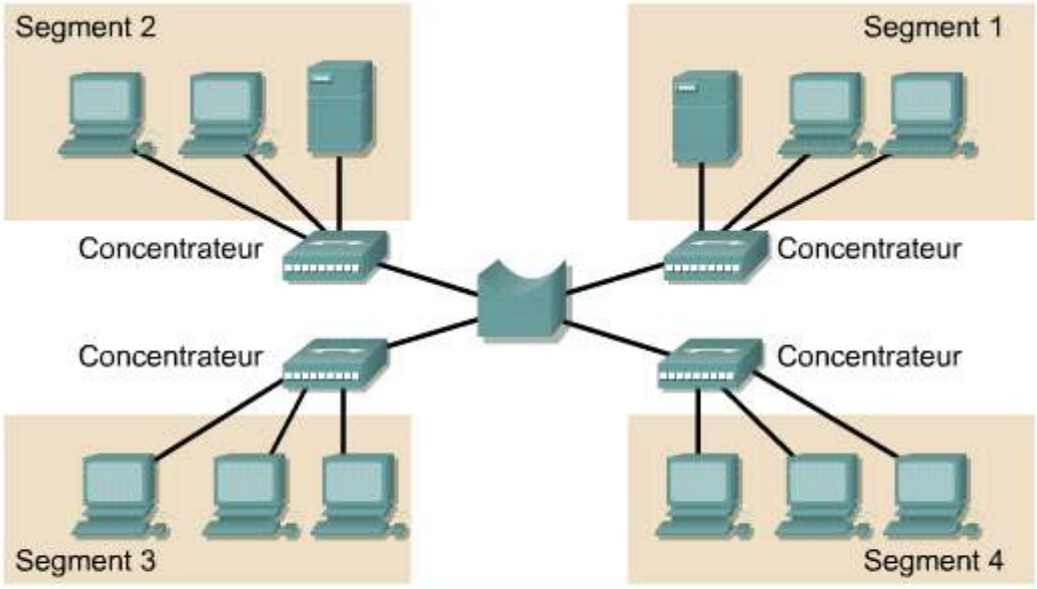
4.2.2 Segmentation LAN à l'aide de ponts

Les ponts sont des équipements de couche 2 qui transmettent des trames de données en fonction de l'adresse MAC. Les ponts lisent l'adresse MAC de l'émetteur des paquets de données reçus sur les ports entrants pour découvrir les équipements de chaque segment. Les adresses MAC sont ensuite utilisées pour créer une table de commutation qui permet au pont de bloquer les paquets qu'il n'est pas nécessaire de transmettre à partir du segment local. 1

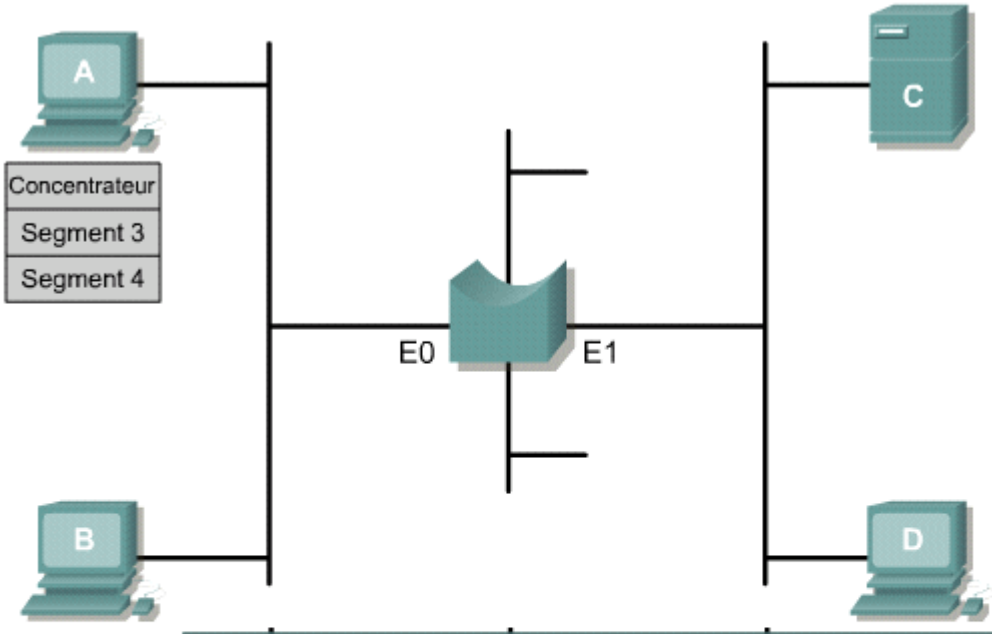


Interface	Adresse MAC
E0	0260.8c01.1111
E0	0260.8c01.2222
E1	0260.8c01.3333
E1	0260.8c01.4444

Bien que le fonctionnement d'un pont soit transparent pour les autres équipements, l'utilisation d'un pont augmente de dix à trente pour cent la latence d'un réseau. Cette latence résulte du processus de prise de décision qui a lieu avant l'envoi d'un paquet. Un pont est considéré comme un équipement de type Store-and-Forward, car il doit examiner le champ d'adresse de destination et calculer le code de redondance cyclique (CRC) dans le champ de séquence de contrôle de trame avant l'envoi d'une trame. Si le port de destination est occupé, le pont peut stocker temporairement la trame jusqu'à ce que le port soit de nouveau disponible. 2

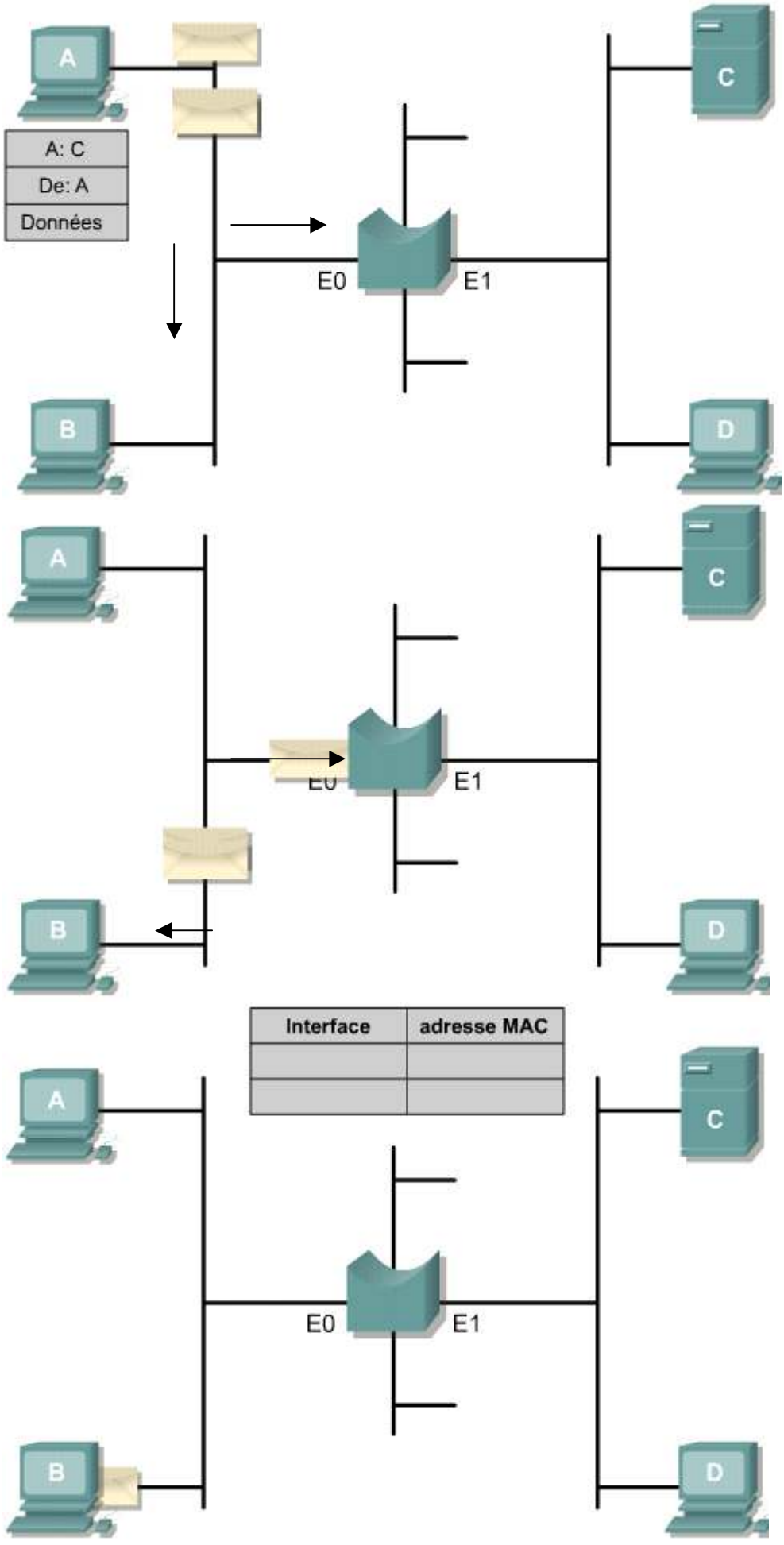


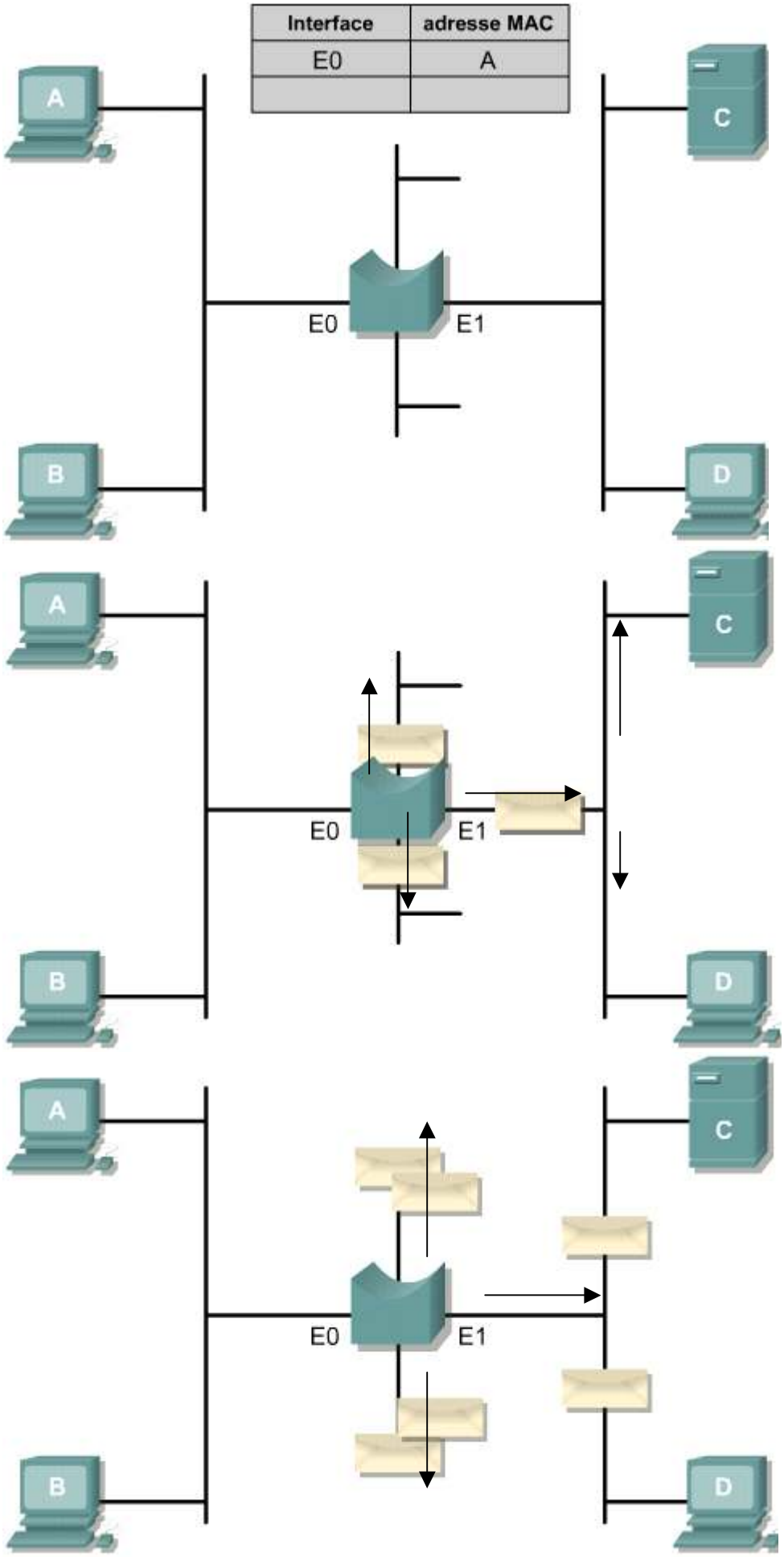
- La segmentation permet d'avoir moins d'utilisateurs par segment
- Le pont stocke et achemine les trames en fonction des adresses de couche 2.
- Indépendant du protocole de couche 3
- Augmentation de la latence sur le réseau

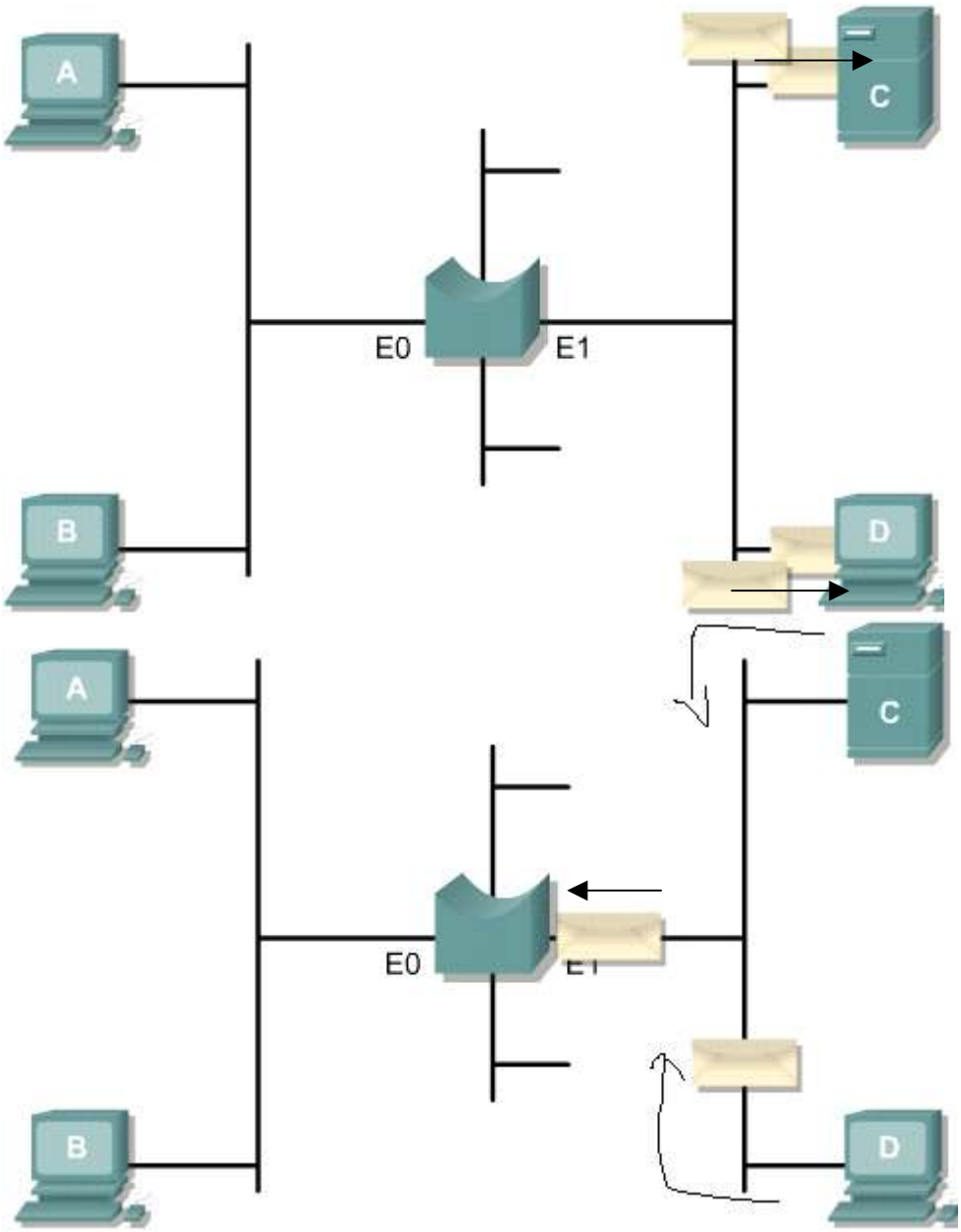


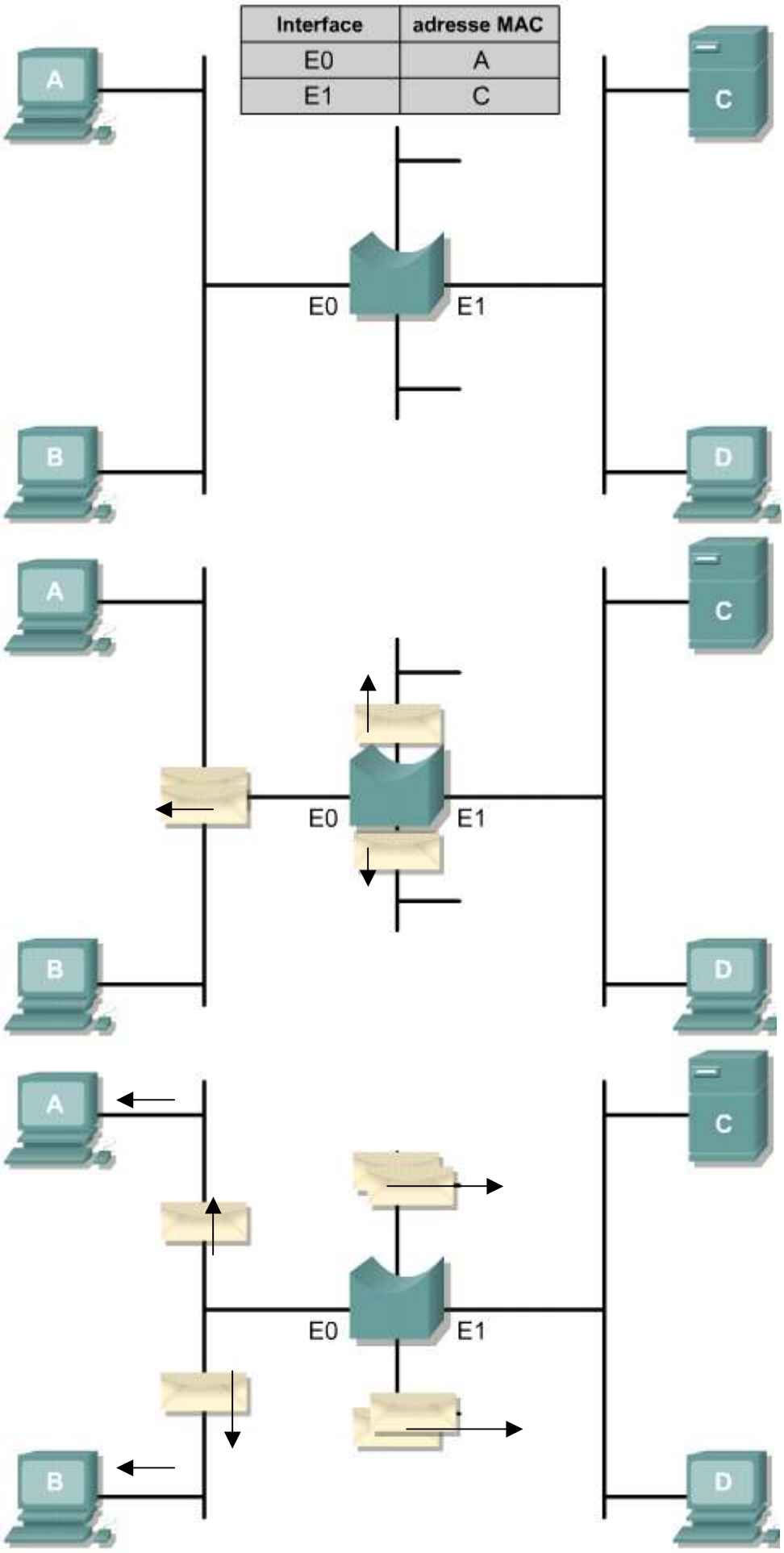
Fenêtre contextuelle (pop up)

Un pont apprend la location des stations de travail en examinant l'adresse MAC de la source. Si le pont détecte une trame et ne reconnaît pas l'adresse de la source ou de la destination, le pont ajoute l'adresse de la source à sa table. Ensuite, le pont diffuse cette trame sur toutes les interfaces, sauf sur celle par laquelle il l'a reçue. Quand la réponse arrive, le pont examine l'adresse de la source et l'ajoute à sa table de pontage. Après cet échange initial, le pont est capable de gérer la communication entre ces deux équipements.


A
A: C
De: A
Données
C
E0
E1
B
D
A
C
E0
E1
B
D
Interface
adresse MAC
A
C
E0
E1
B
D


Interface
adresse MAC
E0
A
A
C
E0
E1
B
D
A
C
E0
E1
B
D
A
C
E0
E1
B
D


A
C
E0
E1
B
D
A
C
E0
B
D

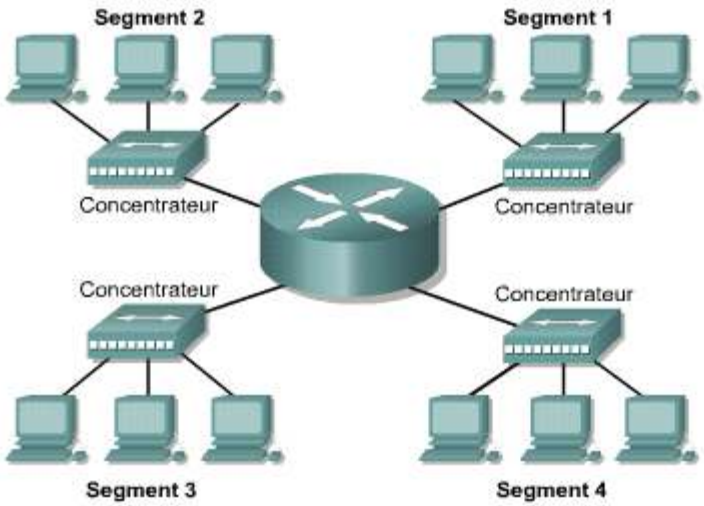

Interface
adresse MAC
E0
A
E1
C
A
C
E0
E1
B
D
A
C
E0
E1
B
D
A
C
E0
E1
B
D

4.2 Introduction à la commutation LAN
4.2.3 Segmentation LAN à l'aide de routeurs

Les routeurs assurent la segmentation des réseaux en ajoutant un coefficient de latence de 20 à 30 % sur un réseau commuté. Cette latence accrue est due au fonctionnement d'un routeur au niveau de la couche réseau qui utilise l'adresse IP pour déterminer le meilleur chemin vers le nœud de destination; La figure 1 représente un routeur Cisco.

Les ponts et les réseaux assurent la segmentation au sein d'un réseau ou d'un sous-réseau. Les routeurs assurent la connectivité entre les réseaux et les sous-réseaux.

En outre, les routeurs n'envoient pas de broadcasts, tandis que les commutateurs et les ponts doivent transmettre des trames de broadcast. 2



- Elle est plus facile à gérer. Elle est caractérisée par une fonctionnalité accrue. Il existe de multiples chemins actifs.
- Domaines de broadcast plus petits
- Fonctionne au niveau de la couche 3

Activité de média interactive

Agrandissement: Routeur Cisco 2621

Dans cette vue agrandie, l'étudiant peut voir un routeur Cisco 2621.

Activité de média interactive

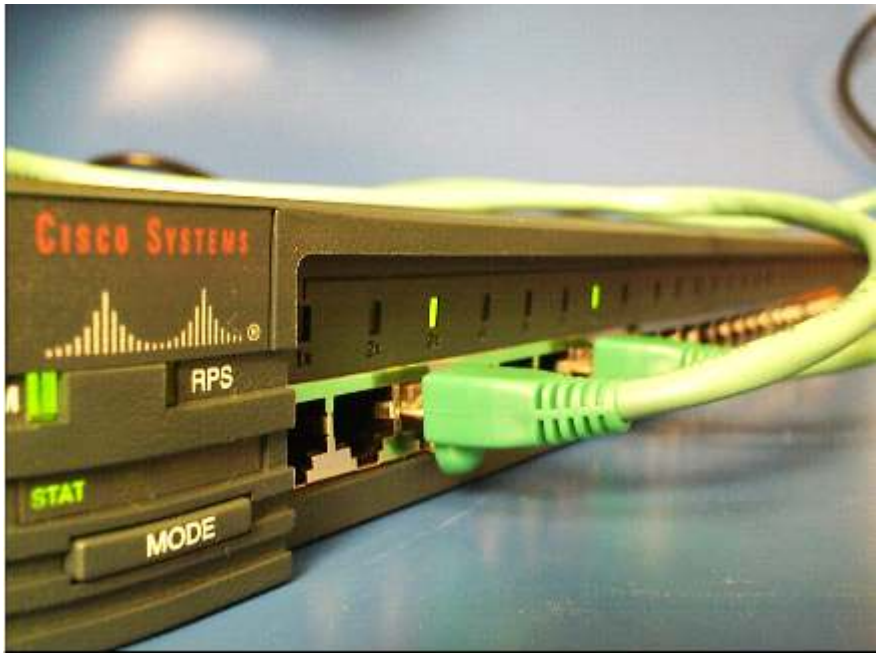
Agrandissement: Routeur Cisco 3640

Dans cette vue agrandie, l'étudiant peut voir un routeur Cisco 3640.

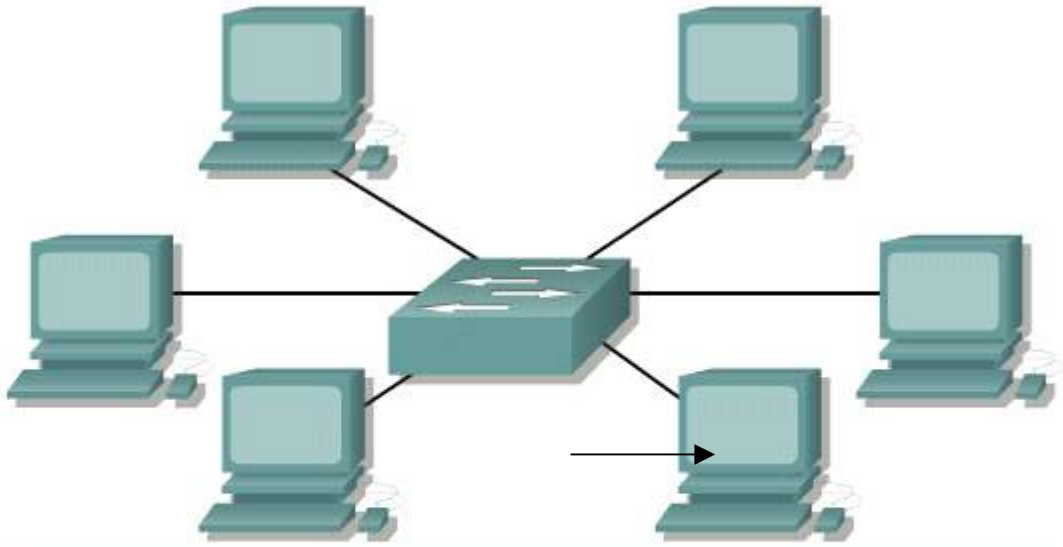
4.2 Introduction à la commutation LAN

4.2.4 Segmentation LAN à l'aide de commutateurs

La commutation LAN réduit les pénuries de bande passante et les goulots d'étranglement sur le réseau, comme ceux qui se produisent entre plusieurs stations de travail et un serveur de fichiers distant. La figure 1

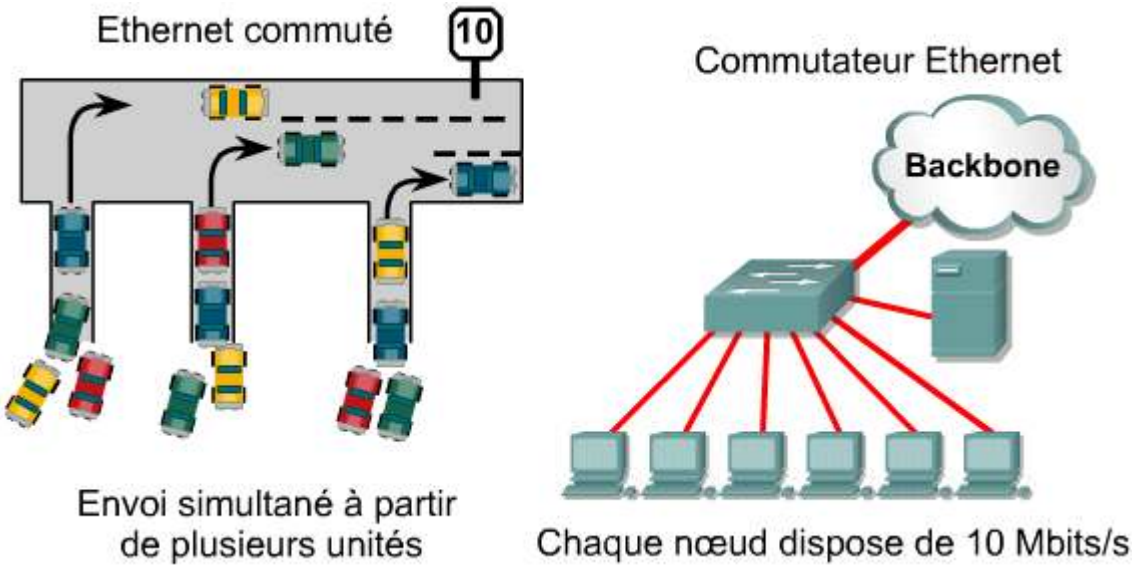


représente un commutateur Cisco. Un commutateur divise un réseau LAN en microsegments afin de réduire la taille des domaines de collision. Cependant, tous les hôtes connectés au commutateur restent dans le même domaine de broadcast. 2



- Élimination de l'effet des collisions grâce à la microsegmentation
- Latence faible et hauts débits d'acheminement des trames au niveau de chaque port d'interface
- Compatible avec le câblage et les cartes réseau conformes à la norme 802.3 (CSMA/CD)

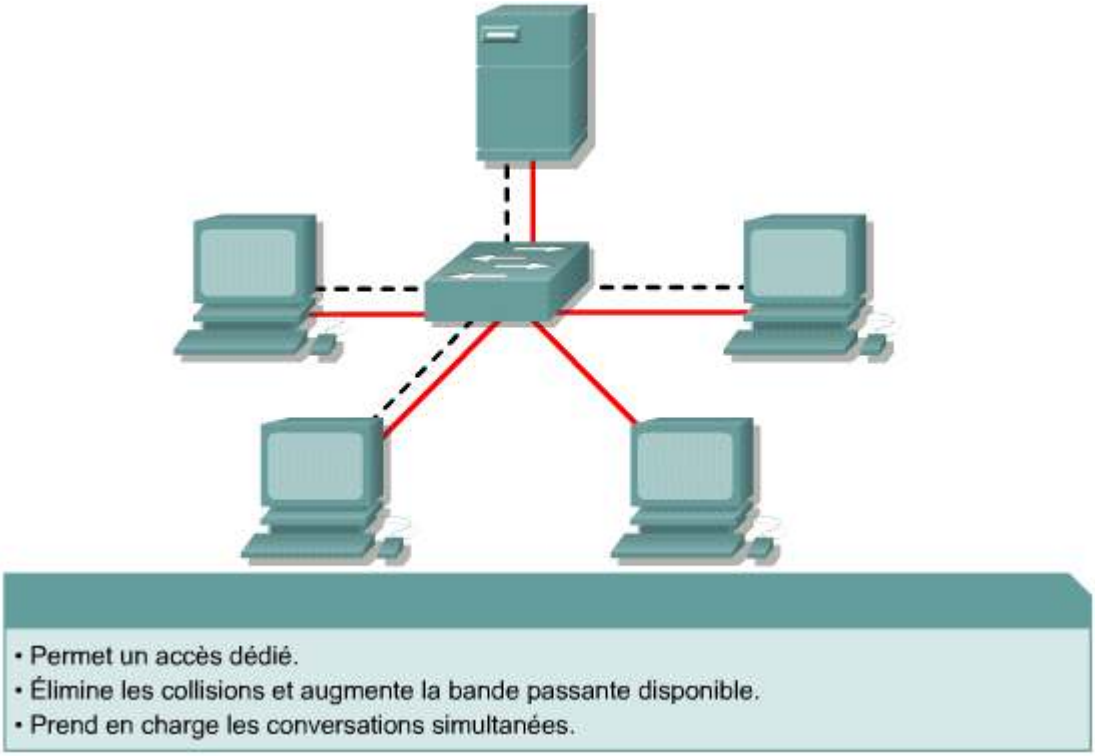
Dans un LAN Ethernet commuté parfait, les nœuds d'émission et de réception opèrent comme s'ils étaient les seuls nœuds du réseau. Lorsque ces deux nœuds établissent une liaison, ou circuit virtuel, ils accèdent au maximum de bande passante disponible. Ces liaisons offrent un débit plus important que les LAN Ethernet connectés via des ponts ou des concentrateurs. 3 Le circuit de réseau virtuel est établi au sein du commutateur et n'existe que lorsque les noeuds ont besoin de communiquer.



4.2 Introduction à la commutation LAN

4.2.5 Fonctionnement de base d'un commutateur

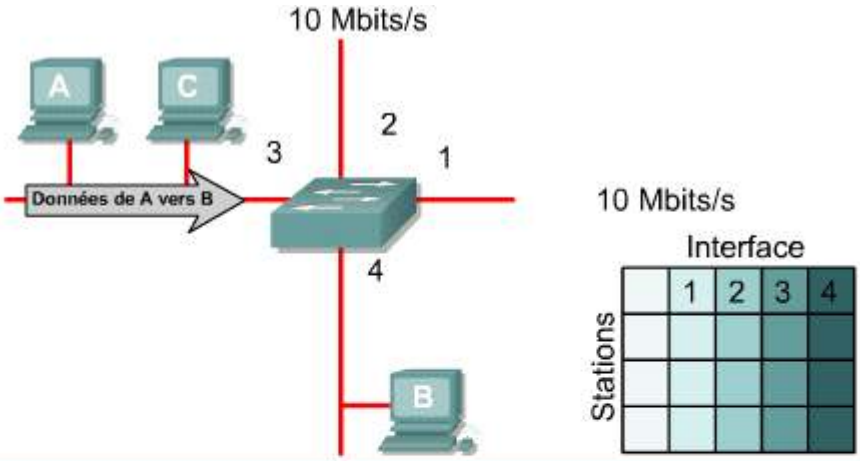
La commutation est une technologie qui permet de réduire la congestion des réseaux LAN Ethernet, Token Ring et FDDI *(Fiber Distributed Data Interface)*. Les commutateurs utilisent la microsegmentation afin de réduire les domaines de collisions et le trafic réseau. Cette réduction engendre un utilisation plus efficace de la bande passante et augmente ainsi le débit. Les commutateurs LAN sont souvent utilisés pour remplacer des concentrateurs partagés et sont conçus pour fonctionner avec les infrastructures de câblage existantes. 1



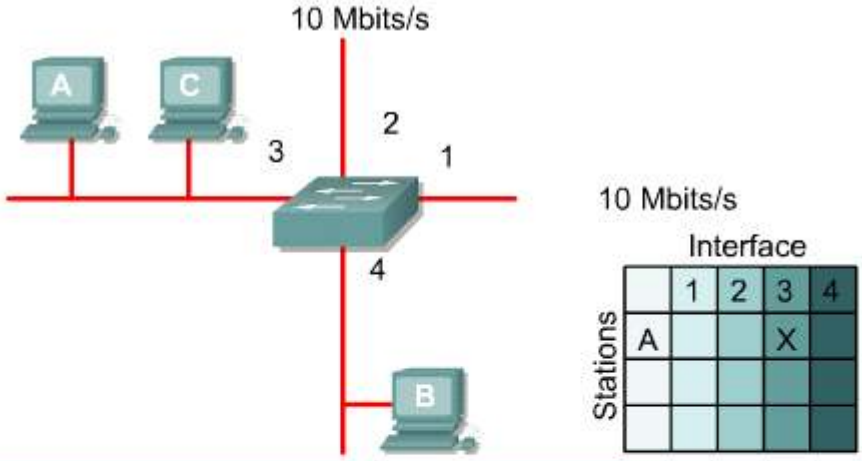
Une unité de commutation exécute deux fonctions de base:

- La commutation de trames de données – Opération qui consiste à recevoir une trame sur une interface du commutateur, de sélectionner la(les) interface(s) de sortie et de finalement transmettre la trame.
- Gestion des tables de commutation – Les commutateurs créent et gèrent des tables de commutation. Les commutateurs construisent aussi sur chaque LAN des topologies réseau exempts de boucles.

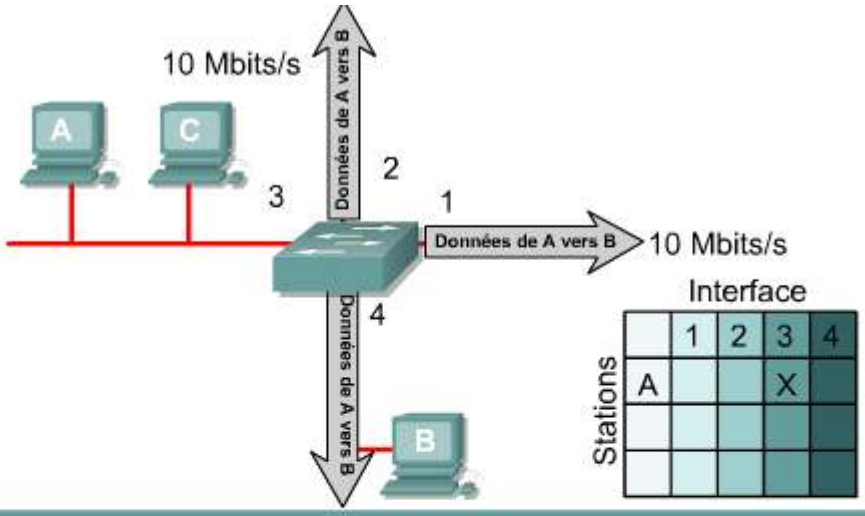
Les figures 2 à 6 illustrent le fonctionnement de base d'un commutateur.



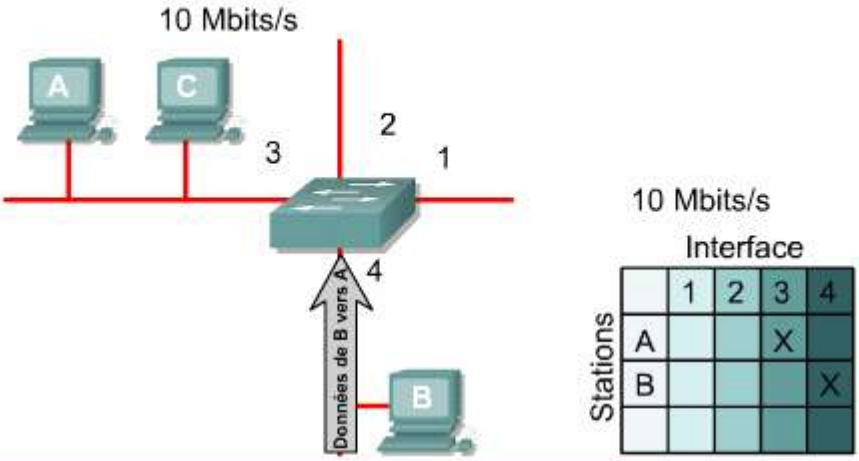
- Il achemine les paquets selon une table de transmission.
  - Il achemine les trames en fonction de l'adresse MAC (couche 2).
- Il fonctionne au niveau de la couche 2 du modèle OSI.
- Il apprend l'emplacement d'une station en examinant l'adresse d'origine.
  - Il envoie les trames sur tous les ports lorsque l'adresse de destination est de type broadcast, multicast ou inconnu.
  - Il achemine les données lorsque la destination est située sur une interface différente.



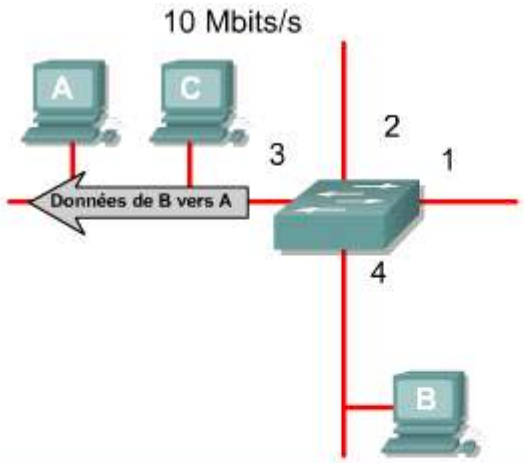
- Il achemine les paquets selon une table de transmission.
  - Il achemine les trames en fonction de l'adresse MAC (couche 2).
- Il fonctionne au niveau de la couche 2 du modèle OSI.
- Il apprend l'emplacement d'une station en examinant l'adresse d'origine.
  - Il envoie les trames sur tous les ports lorsque l'adresse de destination est de type broadcast, multicast ou inconnu.
  - Il achemine les données lorsque la destination est située sur une interface différente.

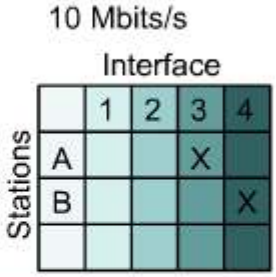


- Il achemine les paquets selon une table de transmission.
  - Il achemine les trames en fonction de l'adresse MAC (couche 2).
- Il fonctionne au niveau de la couche 2 du modèle OSI.
- Il apprend l'emplacement d'une station en examinant l'adresse d'origine.
  - Il envoie les trames sur tous les ports lorsque l'adresse de destination est de type broadcast, multicast ou inconnu.
  - Il achemine les données lorsque la destination est située sur une interface différente.



- Il achemine les paquets selon une table de transmission.
  - Il achemine les trames en fonction de l'adresse MAC (couche 2).
- Il fonctionne au niveau de la couche 2 du modèle OSI.
- Il apprend l'emplacement d'une station en examinant l'adresse d'origine.
  - Il envoie les trames sur tous les ports lorsque l'adresse de destination est de type broadcast, multicast ou inconnu.
  - Il achemine les données lorsque la destination est située sur une interface différente.



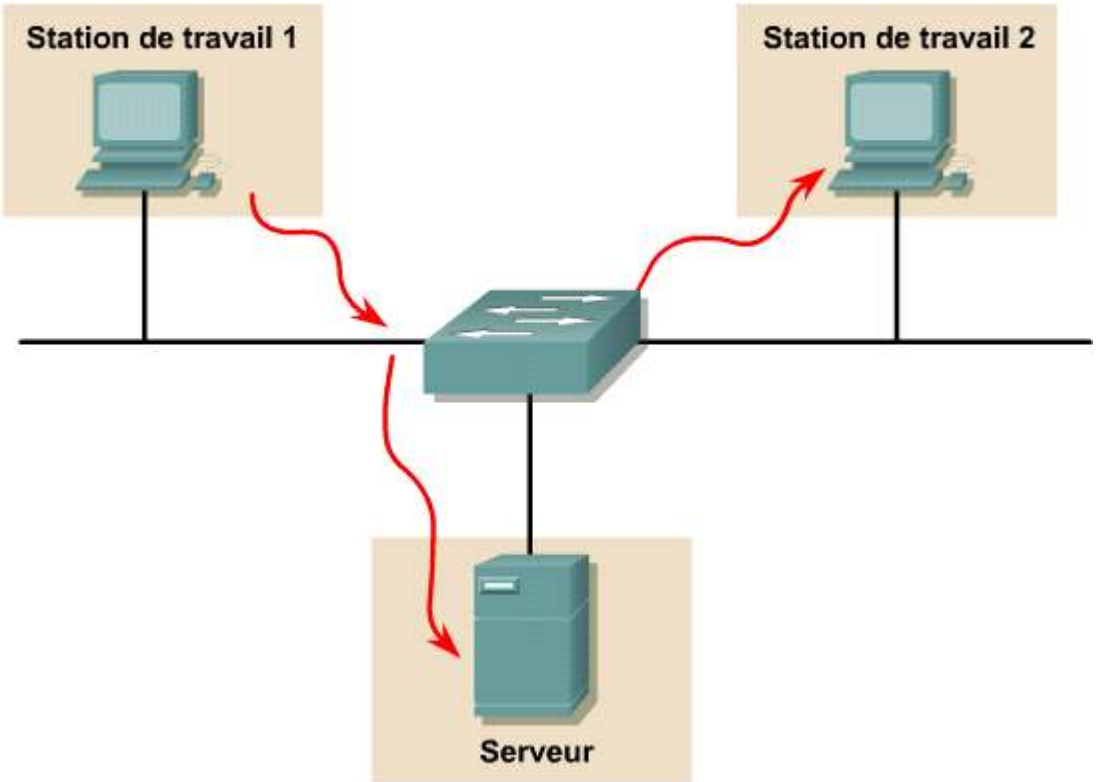


- Il achemine les paquets selon une table de transmission.
  - Il achemine les trames en fonction de l'adresse MAC (couche 2).
- Il fonctionne au niveau de la couche 2 du modèle OSI.
- Il apprend l'emplacement d'une station en examinant l'adresse d'origine.
  - Il envoie les trames sur tous les ports lorsque l'adresse de destination est de type broadcast, multicast ou inconnu.
  - Il achemine les données lorsque la destination est située sur une interface différente.

4.2 Introduction à la commutation LAN

4.2.6 Latence des commutateurs Ethernet

La latence d'un commutateur est l'intervalle de temps à partir de l'entrée du début d'une trame dans le commutateur jusqu'à la sortie de la fin de la trame correspondante. Cette période est directement liée au processus de commutation configuré et au volume du trafic. 1



La latence est mesurée en fractions de seconde. Avec des équipements de réseau opérant à des débits extrêmement élevés, chaque nanoseconde de latence supplémentaire contribue à dégrader les performances réseau.

4.2 Introduction à la commutation LAN

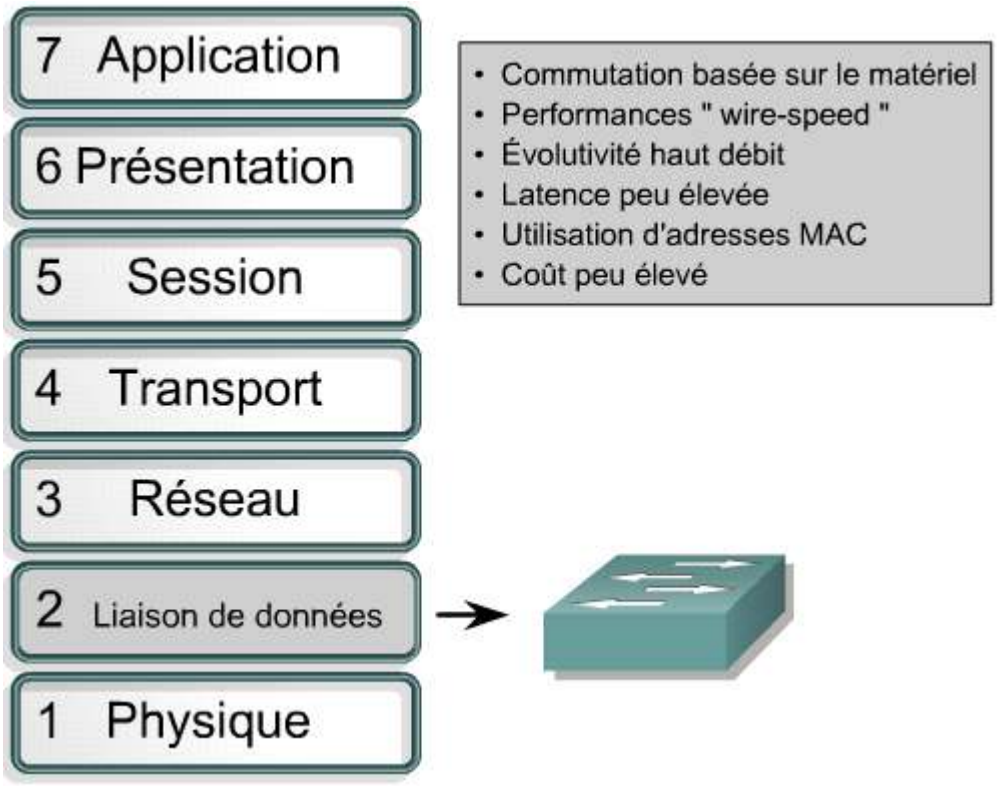
4.2.7 Commutation des couches 2 et 3

Il existe deux méthodes pour effectuer la commutation des trames de données: la commutation de couche 2 et la commutation de couche 3. Les routeurs et les commutateurs de couche 3 utilisent la commutation de couche 3 pour commuter les paquets. Les commutateurs de couche 2 ainsi que les ponts utilisent quant à eux la commutation de couche 2 pour acheminer les trames.

Les commutateurs de couche 3 incluent une technologie de routage et performent habituellement mieux que les commutateurs de couche 2. Les commutateurs de couche 3 sont plus difficiles à configurer que les commutateurs de couche 2 si toutes les fonctionnalités de couche 3 sont désirées. Dans la plupart des commutateurs de couche 3, une adresse IP est assignée à chaque port. D'autres modèles de commutateurs de couche 3 ne nécessitent qu'une adresse IP soit assignée au VLAN par défaut, ce qui rend le commutateur adressable de chaque port. Les options de configuration et les fonctionnalités des commutateurs de couche 3 et des routeurs comportent de nombreuses similarités. La principale différence entre le processus de commutation de paquet d'un routeur et d'un commutateur de couche 3 se situe au niveau de l'implémentation physique. Dans la plupart des routeurs, la commutation de paquet s'effectue au niveau logiciel par l'entremise d'un microprocesseur. Un commutateur de couche 3 effectue la commutation de paquet directement au niveau matériel en ayant recourt à des circuits intégrés spécialisés (ASIC) pour cette application spécifique.

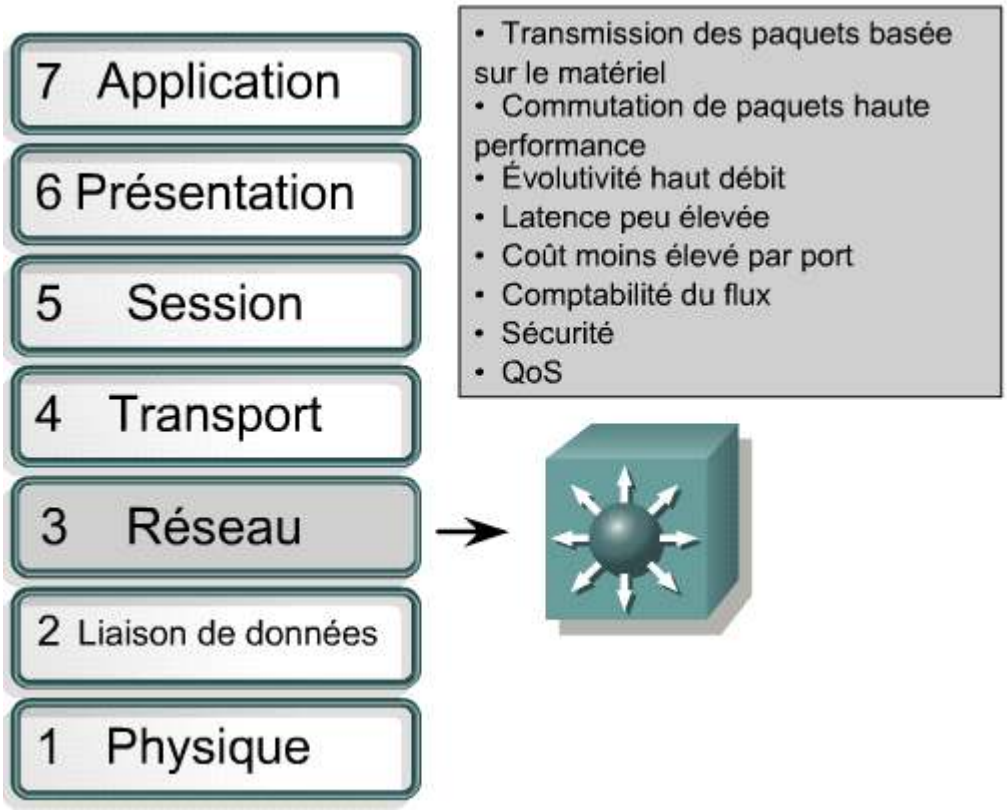
La différence entre la commutation de couche 2 et la commutation de couche 3 réside au niveau du type d'information utilisé dans la trame pour déterminer l'interface de sortie appropriée. La commutation de couche 2 se base sur les informations des adresses MAC, alors que la commutation de couche 3 se base sur les adresses de la couche réseau, ou adresses IP.

La commutation de couche 2 recherche une adresse MAC de destination dans l'en-tête de la trame, puis transmet cette dernière à l'interface ou au port approprié en se basant sur l'adresse MAC de la table de commutation. 1



La table de commutation se trouve dans la mémoire associative (CAM). Si le commutateur de couche 2 ne sait pas où envoyer la trame, il la diffuse à tous les ports du réseau. Si une réponse est renvoyée, le commutateur enregistre la nouvelle adresse dans la mémoire associative.

La commutation de couche 3 est une fonction de la couche réseau. Les informations d'en-tête de couche 3 sont examinées et le paquet est acheminé sur la base de l'adresse IP. 2

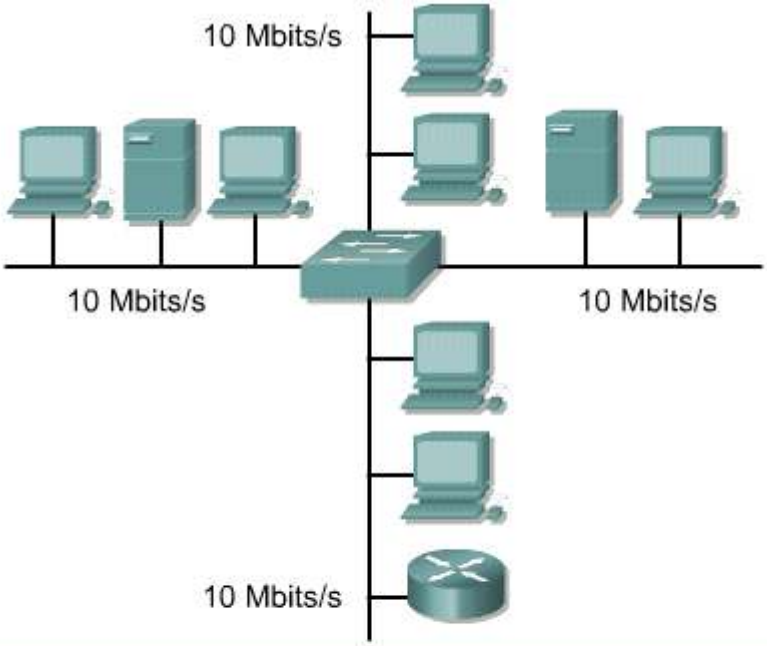


Le flux du trafic des réseaux commutés ou non hiérarchiques est intrinsèquement différent du celui des réseaux routés ou hiérarchiques. Ces derniers offrent un flux de trafic plus souple.

4.2.8	Commutation symétrique et asymétrique	

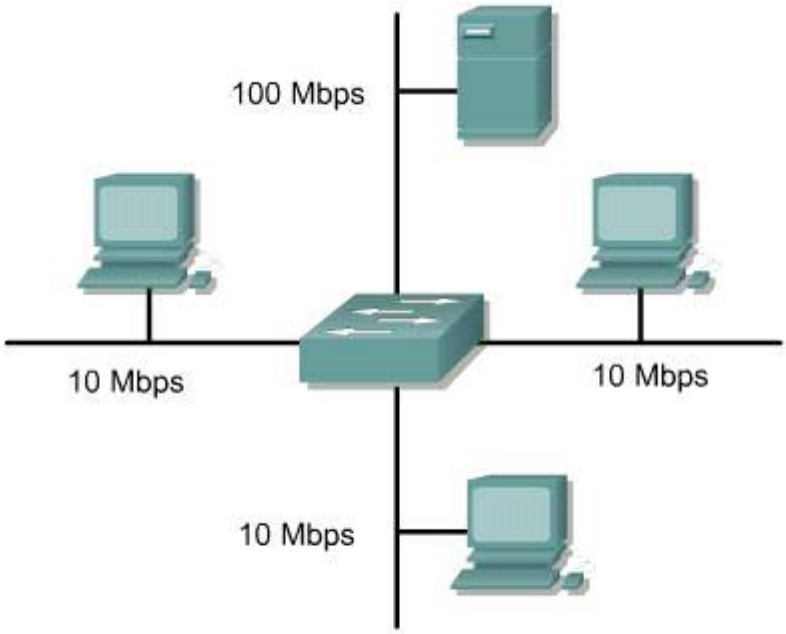
4.2.8	Commutation symétrique et asymétrique	

La commutation symétrique ou asymétrique d'un réseau LAN dépend de la façon dont la bande passante est allouée aux ports de commutateur. La commutation symétrique fournit des connexions commutées entre des ports de même débit. 1



• Assure la commutation entre des bandes passantes similaires (10/10 ou 100/100 Mbits/s)
• Plusieurs communications simultanées augmentent le débit.

Un commutateur LAN asymétrique fournit des connexions commutées entre des ports de débit différent, par exemple entre une combinaison de ports de 10 Mbits/s et de 100 Mbits/s. 2



- Assure la commutation entre des bandes passantes différentes (10/100 Mbits/s).
- Le commutateur doit recourir à la mise en mémoire tampon.

La commutation asymétrique permet d'attribuer davantage de bande passante au port de commutateur du serveur afin d'éviter les goulots d'étranglement. Le trafic devient ainsi plus fluide lorsque plusieurs clients communiquent simultanément avec le même serveur. La commutation asymétrique nécessite l'utilisation de la mémoire tampon pour conserver les trames contiguës entre les ports de débit différent.

4.2 Introduction à la commutation LAN

4.2.9 Mise en mémoire tampon

Un commutateur Ethernet peut utiliser une technique de mise en mémoire tampon pour stocker et transmettre des trames. Il est également possible de recourir à la mise en mémoire tampon lorsque le port de destination est occupé. La zone de mémoire dans laquelle le commutateur stocke les données s'appelle la mémoire tampon. Cette mémoire peut utiliser deux méthodes pour acheminer les trames : la mise en mémoire tampon axée sur les ports et la mise en mémoire tampon partagée. 1

- Dans le cas de la mise en mémoire tampon axée sur les ports, les trames sont placées dans des files d'attente liées à des ports entrants spécifiques.
- La mise en mémoire partagée stocke toutes les trames dans une mémoire tampon commune que partagent tous les ports du commutateur.

Dans le cas de la mise en mémoire tampon axée sur les ports, les trames sont placées dans des files d'attente liées à des ports entrants spécifiques. Une trame n'est transmise au port sortant que si toutes les trames qui la précèdent dans la file d'attente ont été correctement transmises. Une seule trame peut retarder la transmission de toutes les trames en mémoire en raison d'un port de destination occupé. Ce retard se produit même si les autres trames peuvent être transmises à des ports de destination libres.

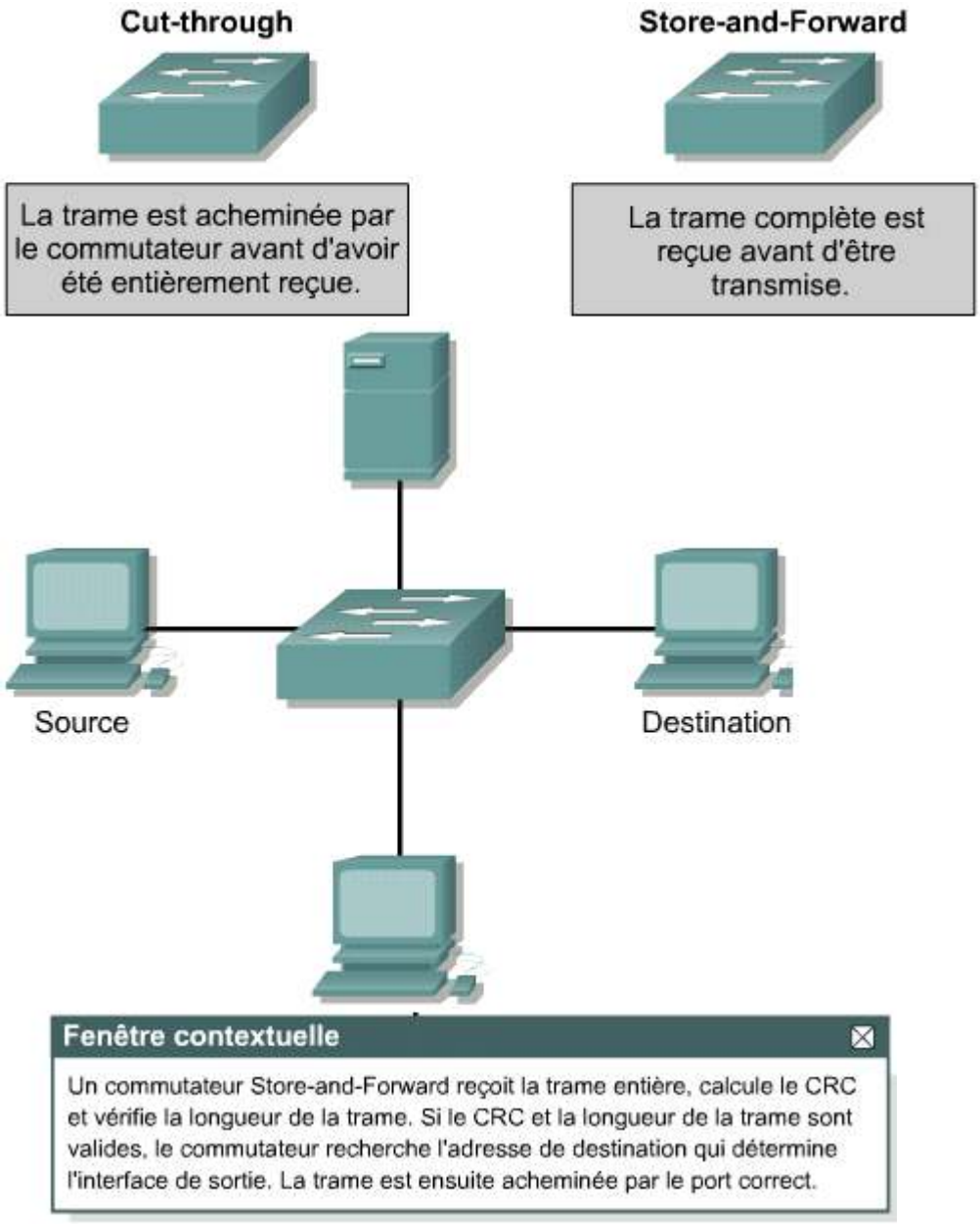
La mise en mémoire partagée stocke toutes les trames dans une mémoire tampon commune à tous les ports du commutateur. La capacité de mémoire tampon nécessaire à un port est allouée dynamiquement. Les trames se trouvant dans la mémoire tampon sont ensuite liées dynamiquement au port destination, ce qui permet de recevoir le paquet par un port et de le transmettre par un autre, sans avoir à le déplacer vers une autre file d'attente.

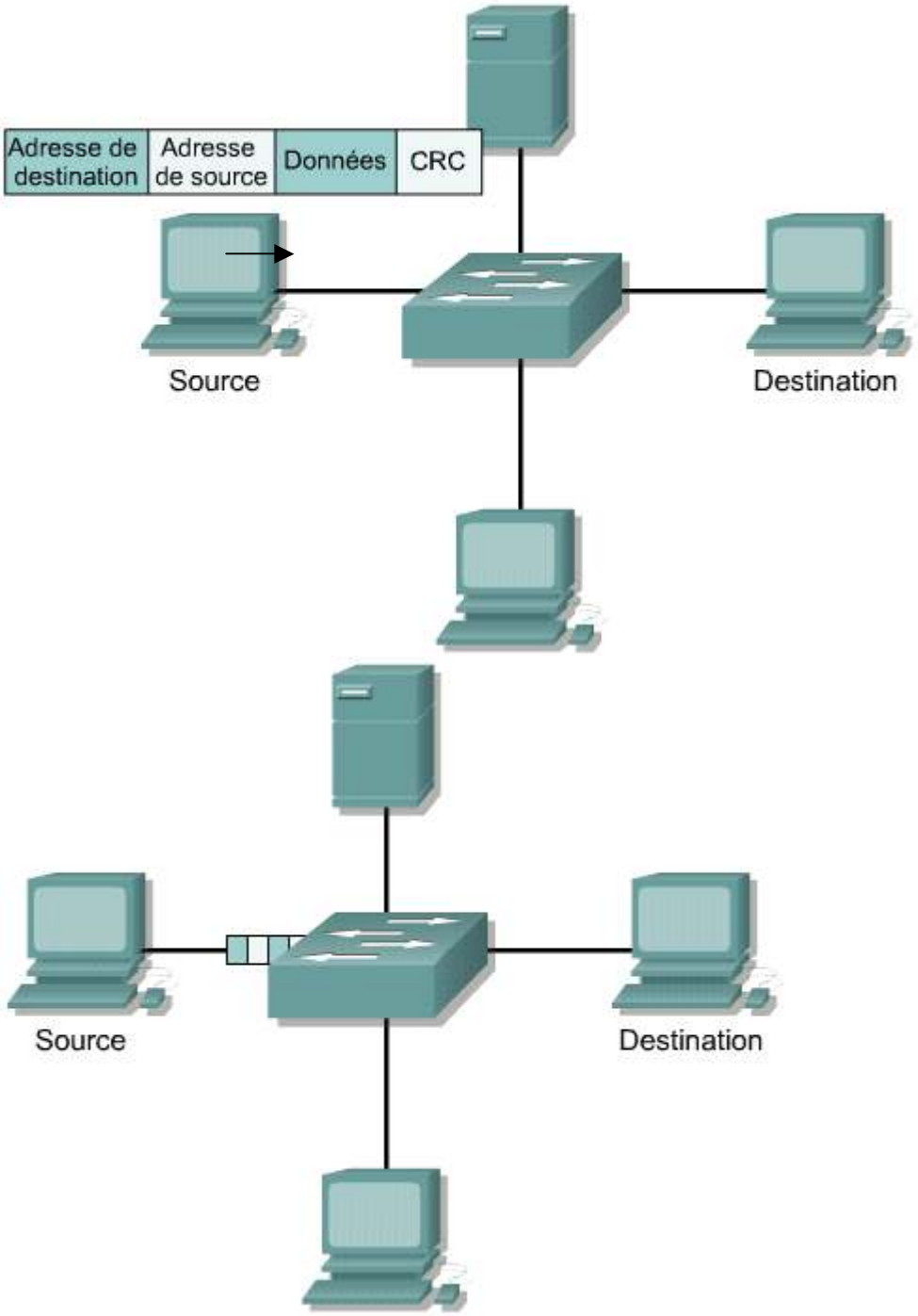
Le commutateur tient à jour une carte de liaisons entre une trame et un port, indiquant l'emplacement vers lequel un paquet doit être acheminé. Cette carte est effacée dès que la trame a été transmise correctement. La mémoire tampon est partagée. Le nombre de trames stockées dans la mémoire tampon est limité par la taille totale de cette mémoire, mais n'est pas limité à un seul tampon du port, ce qui permet de transmettre les grandes trames en en supprimant un minimum. Cela se révèle particulièrement important dans le cadre de la commutation asymétrique pour laquelle les trames sont échangées entre des interfaces de différentes vitesses.

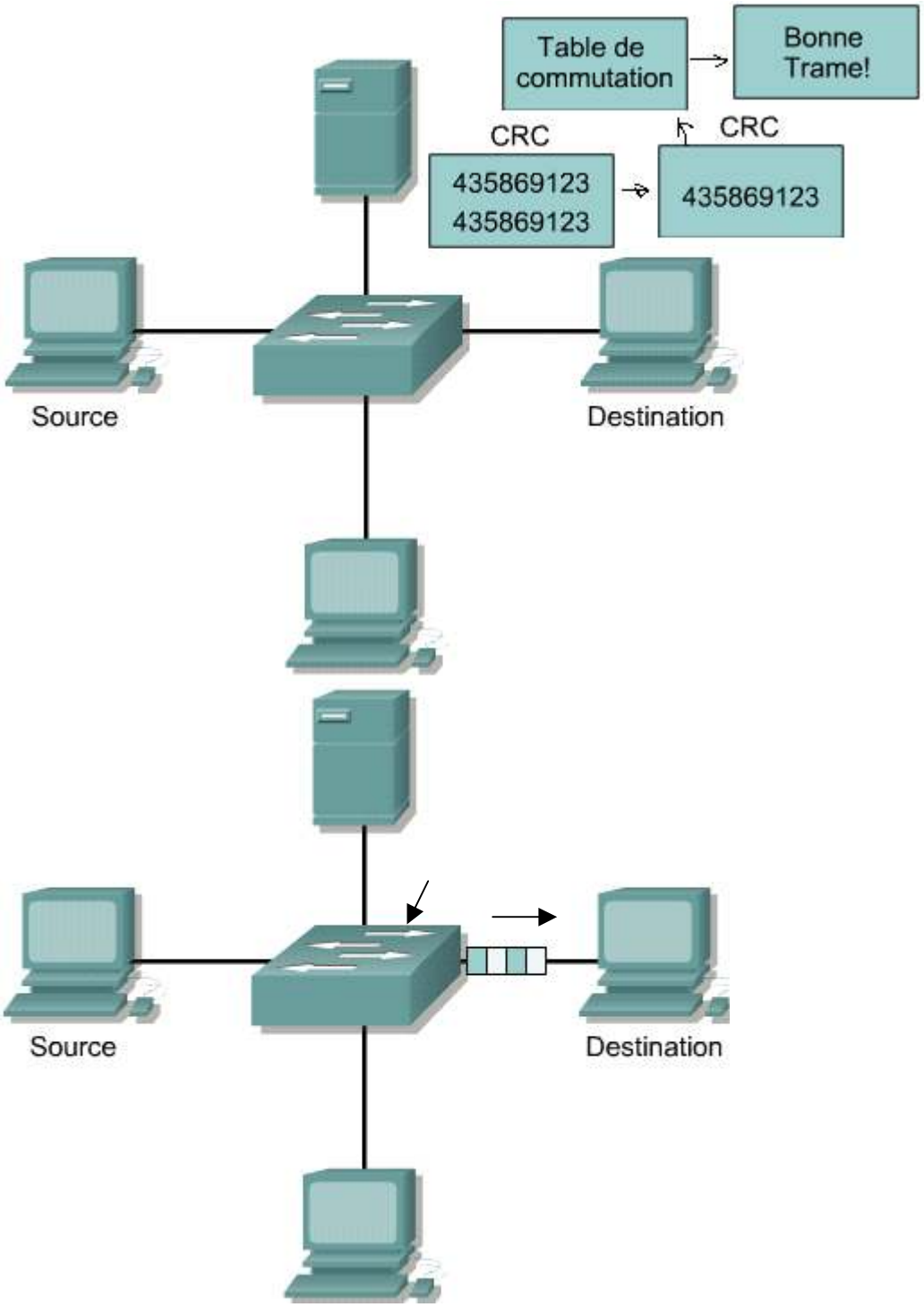
4.2 Introduction à la commutation LAN

4.2.10 Deux modes de commutation

La transmission de trames recourt aux deux modes de commutation suivants: 1 2

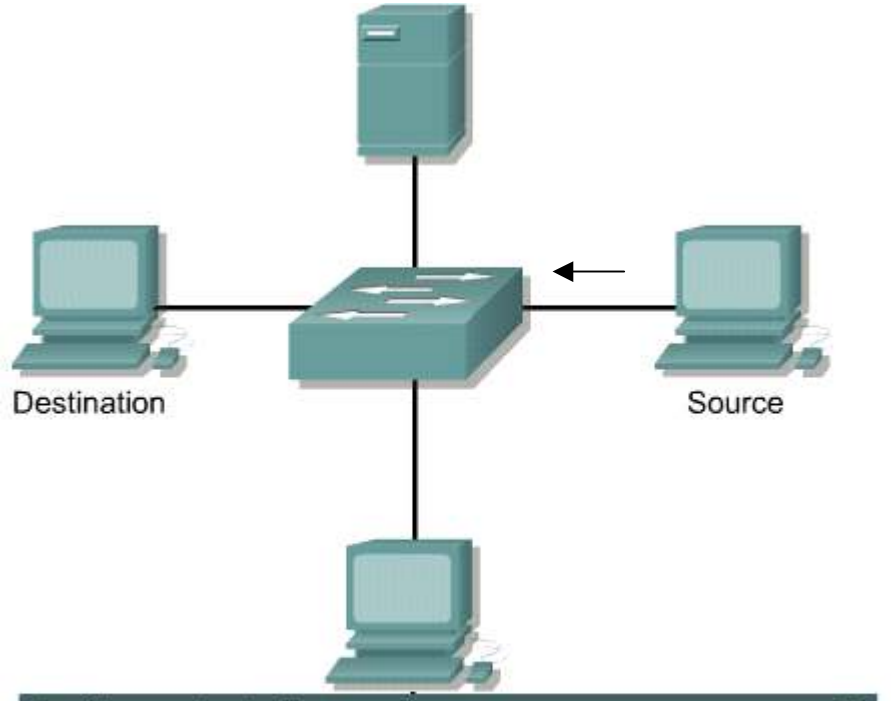



Adresse de destination
Adresse de source
Données
CRC
Source
Destination
Source
Destination



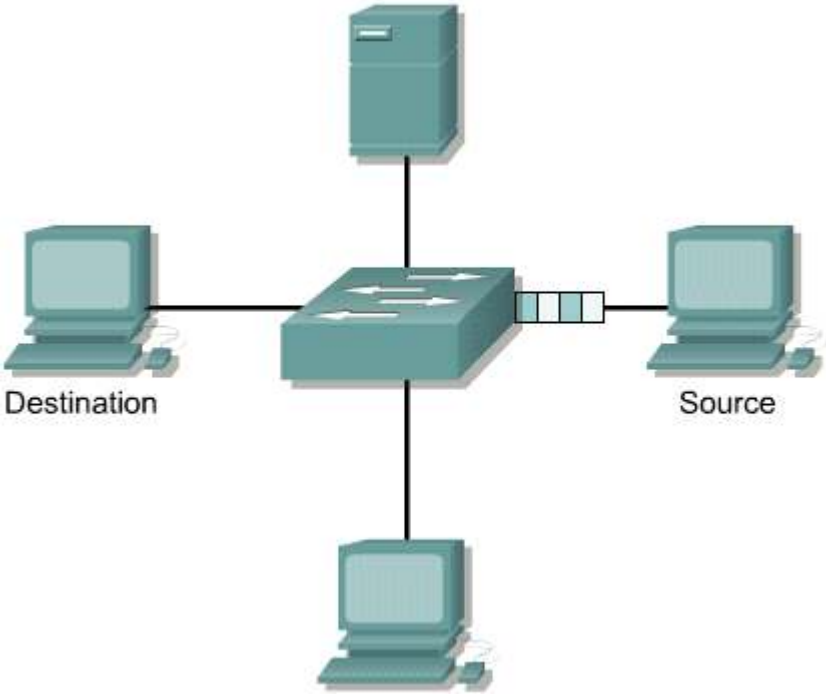
- **Commutation Store-and-Forward** – La trame entière doit être reçue pour pouvoir l'acheminer. Les adresses d'origine et de destination sont lues et des filtres sont appliqués avant l'acheminement de la trame. Une latence est générée pendant la réception de la trame. Elle est élevée s'il s'agit d'une grande trame, car l'intégralité d'une trame doit être reçue pour que le processus de commutation puisse démarrer. Le commutateur est en mesure de vérifier les erreurs dans toute la trame, ce qui améliore la détection des erreurs.
- **Commutation Cut-through** – La trame est envoyée via le commutateur avant la réception intégrale de la trame. L'adresse de destination de la trame doit être au moins lue avant la transmission de la trame. Ce mode réduit à la fois la latence de la transmission et la détection des erreurs.

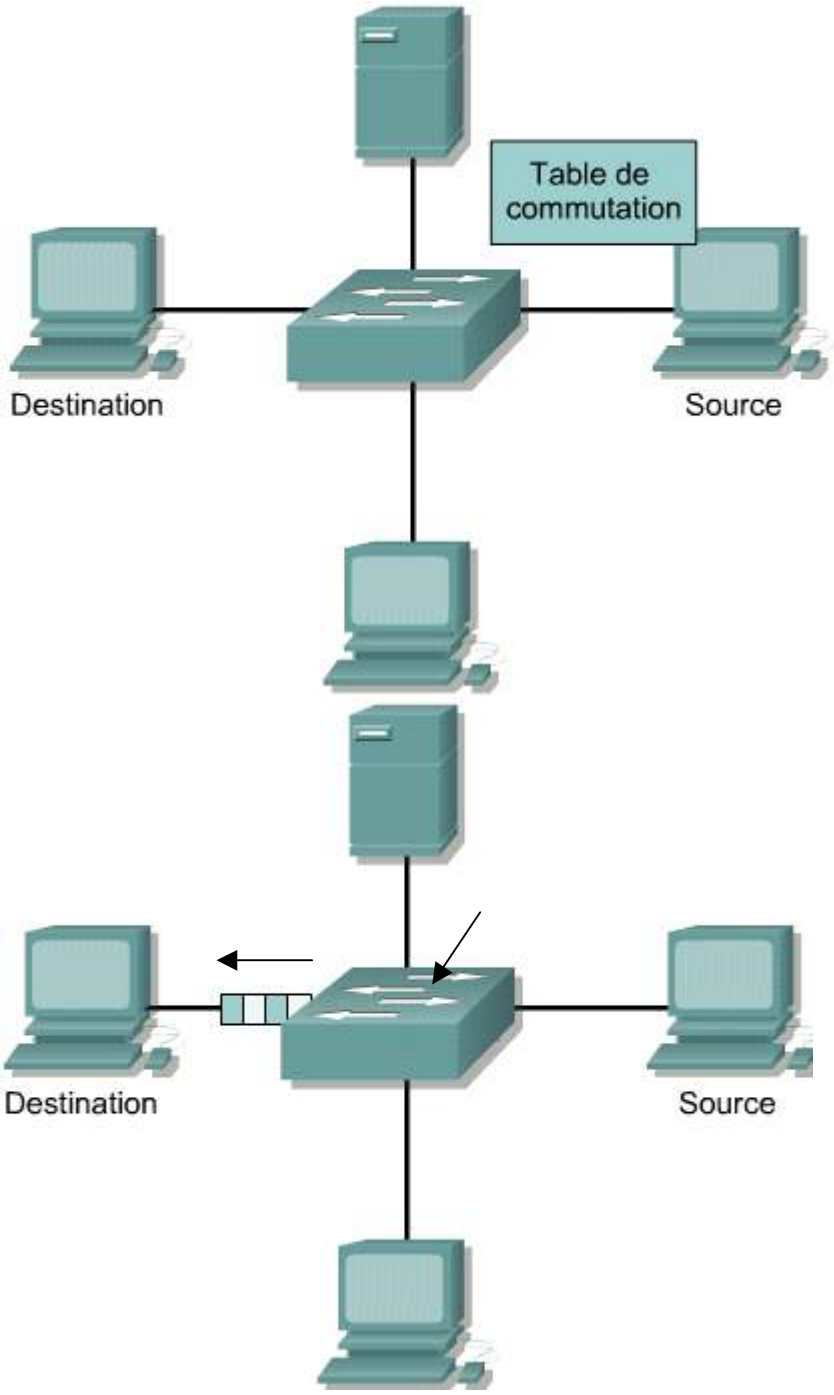
Il existe deux types de commutation Cut-through: 3



Fenêtre contextuelle

Un commutateur Cut-through achemine la trame avant qu'elle ne soit entièrement reçue. Au minimum, l'adresse de destination de la trame doit être lue avant que celle-ci ne soit acheminée.





- **Fast-Forward** – Ce type de commutation offre le niveau de latence le plus faible. La commutation Fast-Forward transmet une trame immédiatement après la lecture de l'adresse de destination. Comme le mode de commutation Fast-Forward commence l'acheminement avant la réception du trame entier, il peut arriver que des trames relayés comportent des erreurs. Bien que cela ne se produise qu'occasionnellement, la carte réseau de destination rejette la trame défectueux lors de sa réception. En mode Fast-Forward, la latence est mesurée à partir du premier bit reçu jusqu'au premier bit transmis.
- **Fragment-Free** – Ce mode de commutation filtre les fragments de collision avant de commencer la transmission. Les fragments de collision constituent la majorité des erreurs de trame. Dans un réseau fonctionnant correctement, la taille des fragments de collision doit être inférieure à 64 octets. Tout fragment d'une taille supérieure à 64 octets constitue une trame valide et est habituellement reçu sans erreur. En mode de commutation Fragment-Free, la trame doit être considéré comme n'étant pas un fragment de collision pour être acheminé. La latence est mesurée à partir du premier bit reçu jusqu'au premier bit transmis.

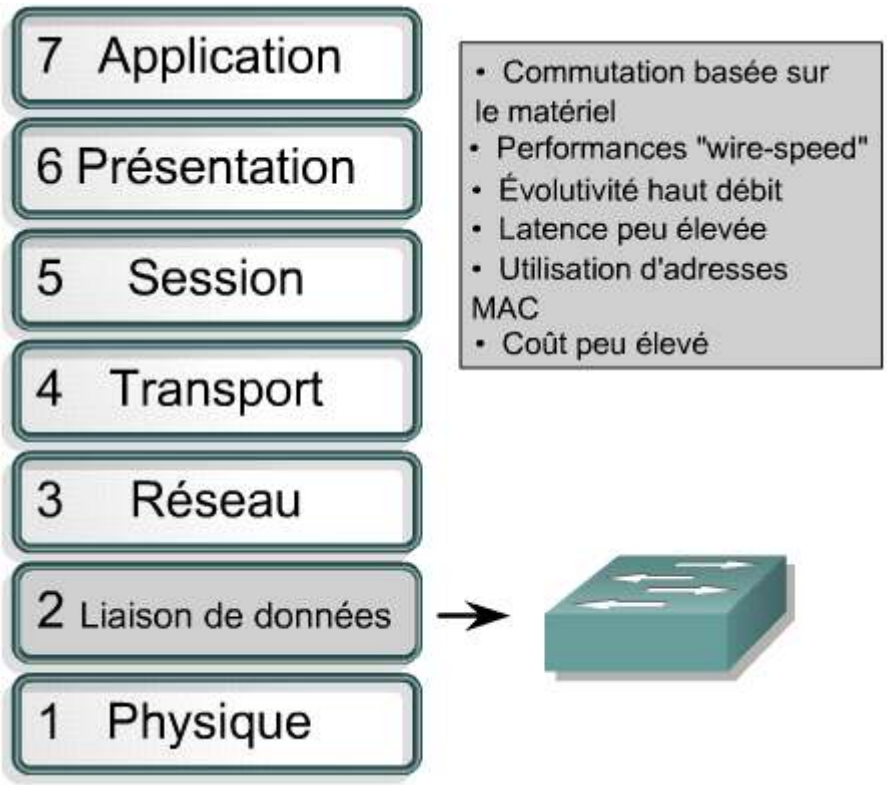
La latence de chaque mode de commutation dépend de la façon dont le commutateur achemine les trames. Pour accélérer l'acheminement des trames, le commutateur réduit le temps de vérification des erreurs, ce qui risque d'augmenter le nombre de retransmissions.

4.3 Fonctionnement d'un commutateur

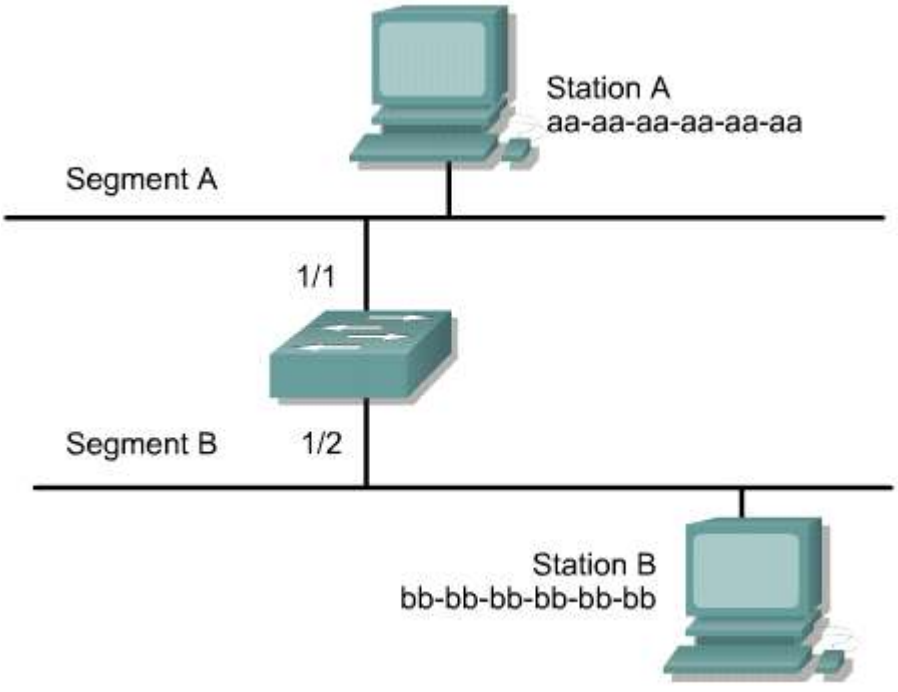
4.3.1 Fonctions des commutateurs Ethernet

Cette page passe en revue les fonctions d'un commutateur de niveau 2.

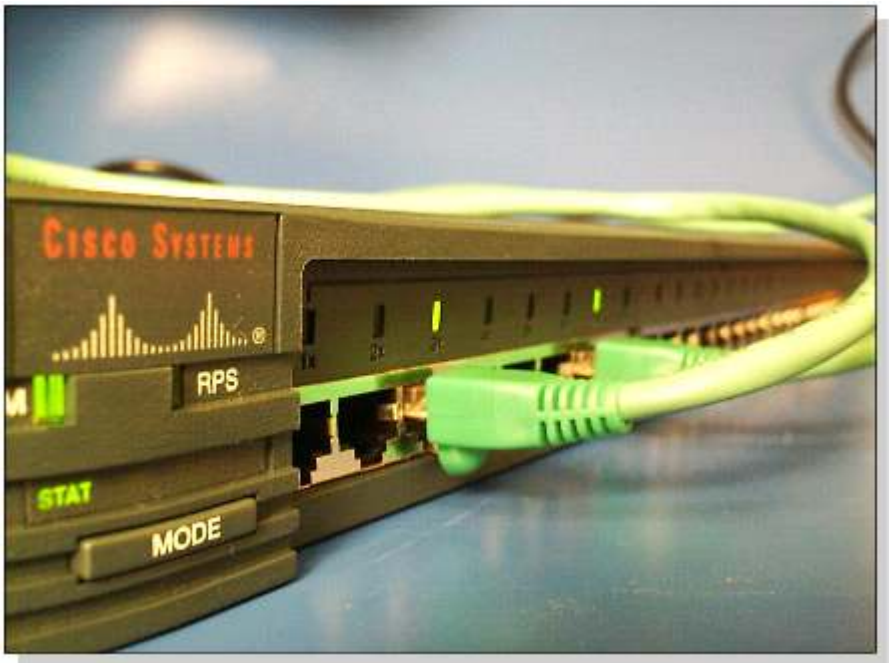
Un commutateur est un dispositif qui interconnecte des segments réseau et qui utilise une table d'adresses MAC afin de déterminer le segment sur lequel chaque trame doit être acheminée. Les commutateurs et les ponts fonctionnent ainsi au niveau de la couche 2 du modèle de référence OSI. Les commutateurs et les ponts fonctionnent au niveau de la couche 2 du modèle OSI. 1

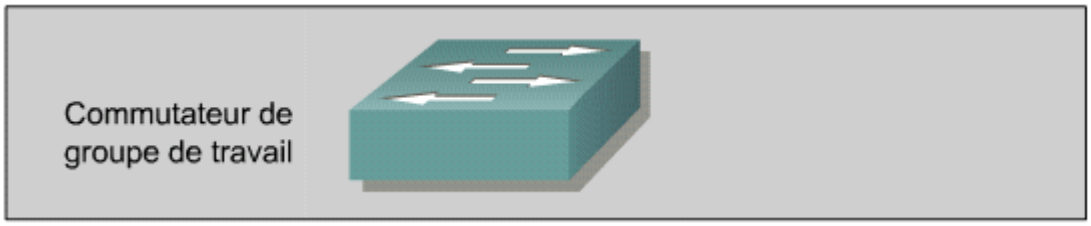


Les commutateurs sont parfois appelés ponts multiports ou concentrateurs de commutation. Ce sont des équipements de couche 2, puisqu'ils prennent des décisions en se basant sur les adresses MAC. 2

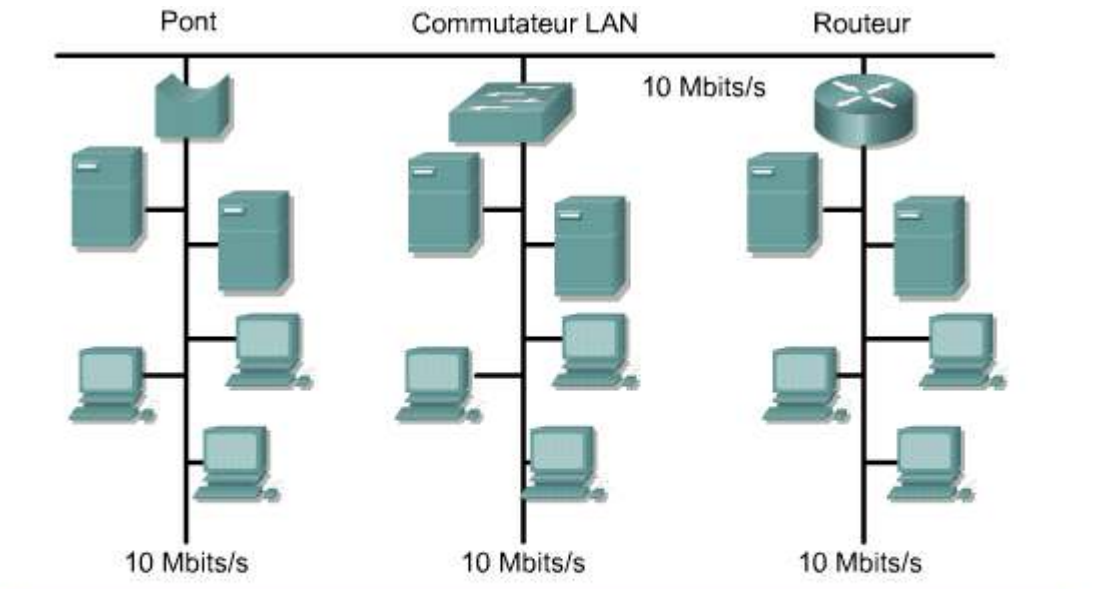


En revanche, les concentrateurs régénèrent les signaux de couche 1 à destination de tous les ports sans prendre de décisions. Comme un commutateur est capable de prendre des décisions relatives à la sélection du chemin, le réseau LAN devient plus efficace. En général, les stations de travail d'un réseau Ethernet sont connectées directement au commutateur. Un commutateur apprend les hôtes qui sont connectés à un port en lisant l'adresse MAC comprise dans les trames. Il ouvre un circuit virtuel uniquement entre les nœuds d'origine et de destination, ce qui limite la communication à ces deux ports sans affecter le trafic des autres ports. En revanche, un concentrateur achemine les données vers tous leurs ports de façon à ce que tous les hôtes voient les données et les traitent, même si elles ne leur sont pas destinées. [3] [4]





Les réseaux LAN hautes performances sont généralement entièrement commutés: [5]



- La segmentation permet d'isoler le trafic entre les segments.
- Elle augmente la bande passante disponible pour chaque utilisateur en créant des domaines de collision plus petits.

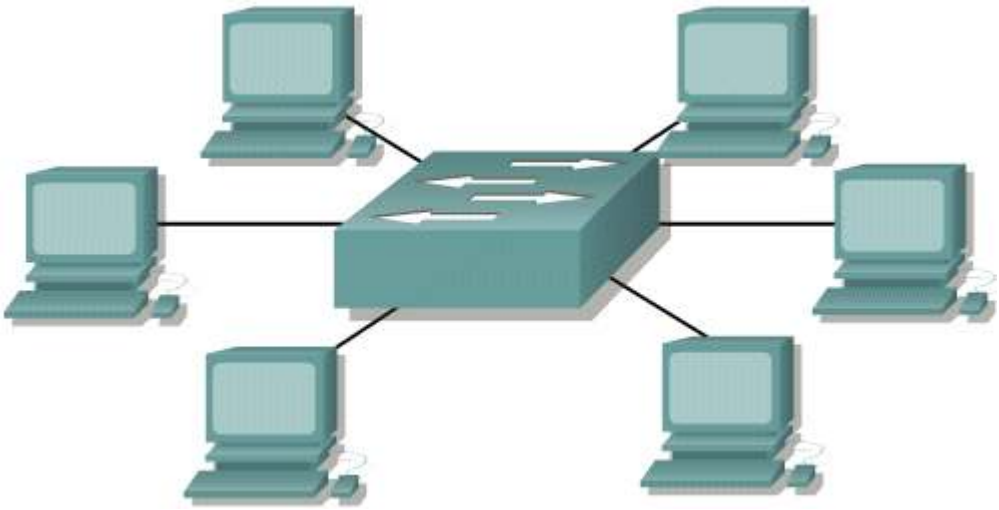
- Un commutateur concentre la connectivité, ce qui rend la transmission de données plus efficace. Les trames sont commutées à partir des ports entrants vers les ports sortants. Chaque port ou interface peut fournir à chaque hôte l'intégralité de la bande passante de la connexion.
- Dans un concentrateur Ethernet standard, tous les ports se connectent à un fond de panier ou à une connexion physique du concentrateur, et tous les équipements reliés au concentrateur partagent la bande passante du réseau. Si deux stations établissent une session qui utilise un niveau de bande passante important, les performances de toutes les autres stations reliées au commutateur se dégradent.
- Pour réduire cette dégradation, le commutateur traite chaque interface comme un segment individuel. Lorsque les stations des différentes interfaces doivent communiquer, le commutateur achemine les trames à la vitesse du câble d'une interface à l'autre pour garantir que chaque session reçoive l'intégralité de la bande passante.

Pour commuter efficacement les trames entre les interfaces, le commutateur tient à jour sa table d'adresses. Lorsqu'une trame entre dans le commutateur, l'adresse MAC de la station émettrice est associée à l'interface réceptrice.

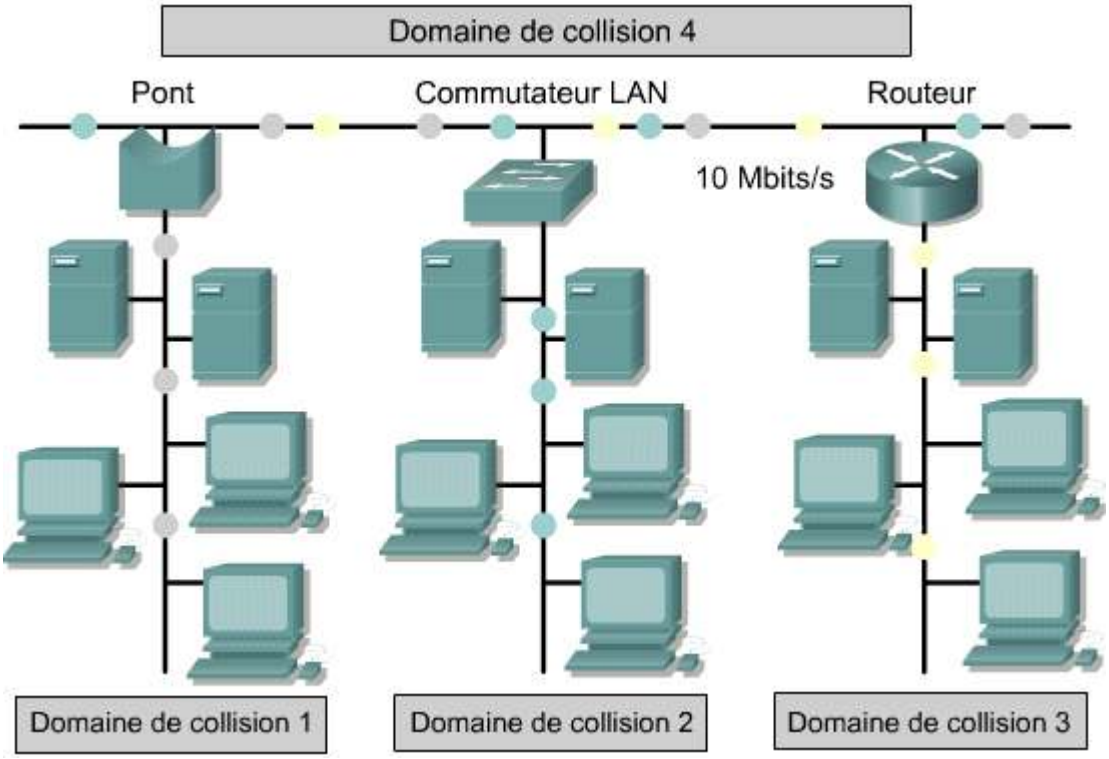
Les principales fonctions d'un commutateur Ethernet sont les suivantes:

- Il isole le trafic entre des segments.
- Il augmente la bande passante pour chaque utilisateur en créant des domaines de collision plus petits.

La première propriété, isoler le trafic entre les segments, permet une sécurité accrue pour les hôtes sur le réseau. Chaque segment utilise le mode d'accès CSMA/CD pour gérer le trafic des données entre les utilisateurs sur le segment. Cette segmentation permet à plusieurs utilisateurs d'envoyer simultanément des informations sur les différents segments sans provoquer le ralentissement du réseau. 6

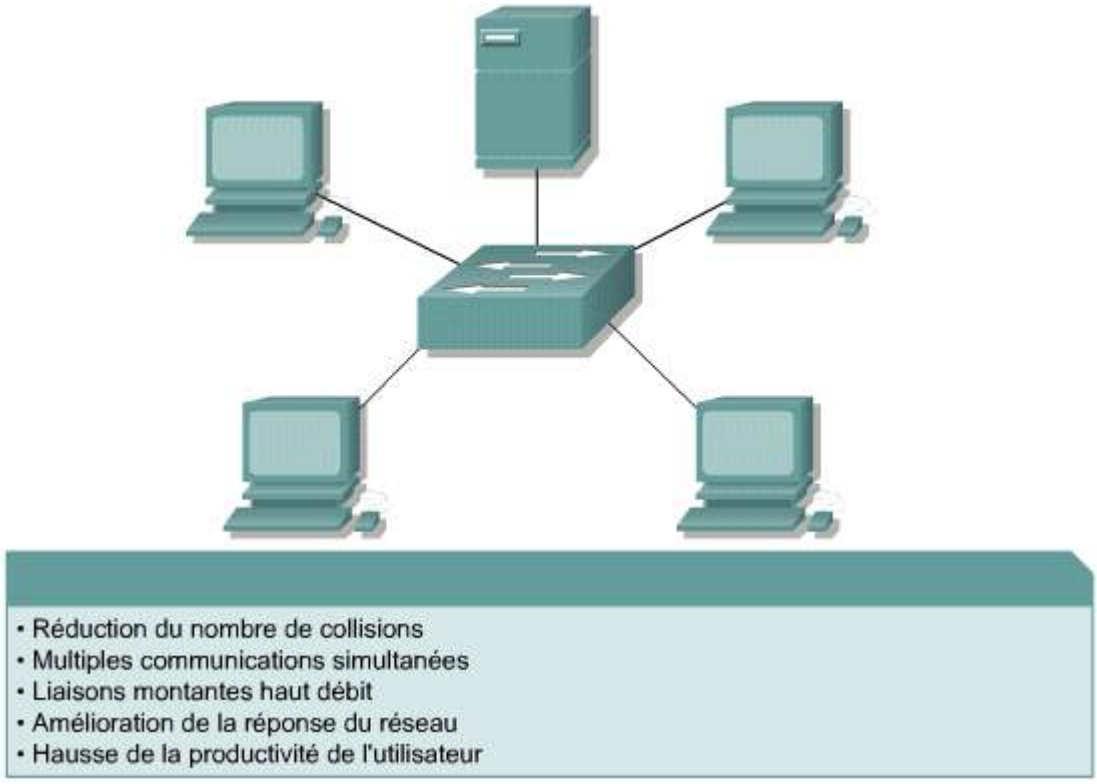


L'utilisation de segments sur un réseau diminue le nombre d'utilisateurs et, le cas échéant, le nombre d'équipements partageant la même bande passante lorsqu'ils communiquent entre eux. Chaque segment dispose de son propre domaine de collision. 7



Les commutateurs Ethernet filtrent le trafic en redirigeant vers le ou les ports appropriés les datagrammes qui sont basés sur les adresses MAC de couche 2.

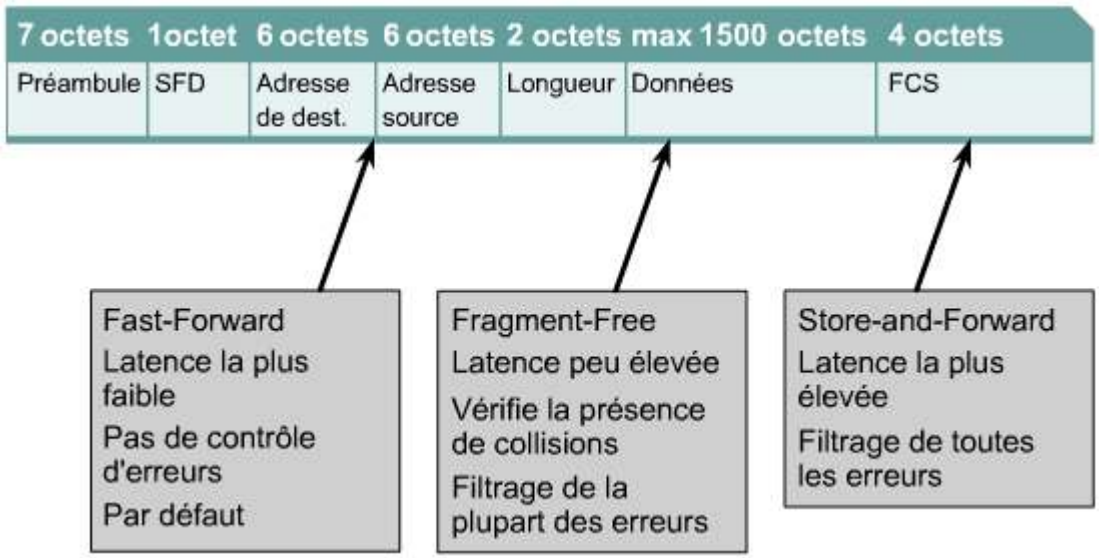
La deuxième propriété est appelée microsegmentation. La microsegmentation permet la création de segments réseau dédiés comportant un seul hôte par segment. Chaque hôte reçoit ainsi toute la bande passante du lien sans pour autant avoir à compétitionner avec d'autres hôtes pour obtenir de la disponibilité de bande passante. Les serveurs les plus utilisés peuvent être placés sur des liaisons individuelles de 100 Mbits/s. Dans les réseaux actuels, un commutateur Fast Ethernet se comporte souvent comme le backbone du LAN, avec des concentrateurs et des commutateurs Ethernet ou des concentrateurs Fast Ethernet assurant les connexions des ordinateurs de bureau dans les groupes de travail. À mesure que l'utilisation des nouvelles applications exigeantes se généralisera, comme les applications multimédia ou la vidéoconférence, certains ordinateurs de bureau disposeront de liaisons dédiées de 100 Mbits/s au réseau. 8



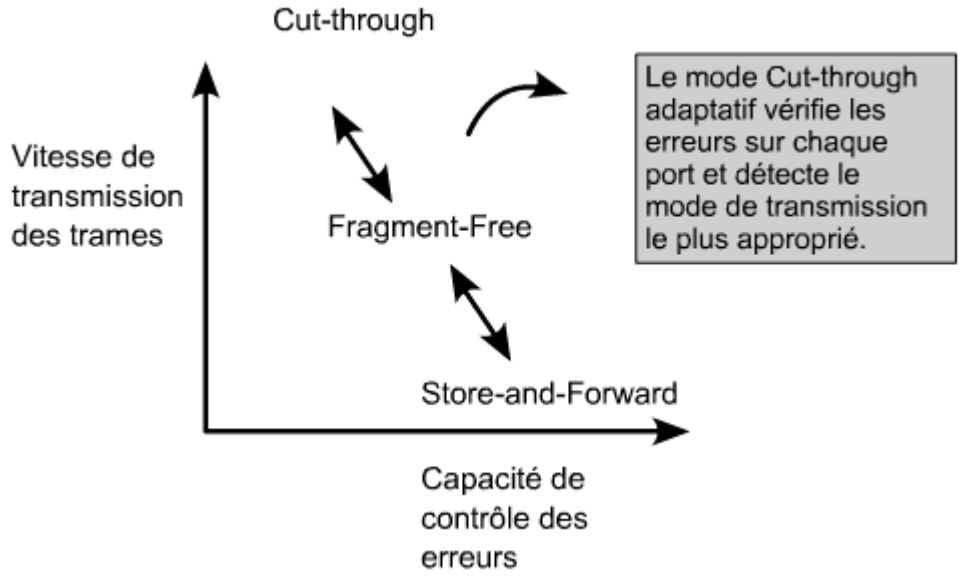
4.3 Fonctionnement d'un commutateur

4.3.2 Modes de transmission de trame

Il existe trois types de transmission de trame: 1



- **Commutation Cut-through –** Un commutateur qui effectue la commutation "cut-through" lit uniquement l'adresse MAC de destination lors de la réception d'une trame. La trame est ensuite acheminée avant d'avoir été entièrement reçue. Ce mode réduit la latence de la transmission mais diminue aussi le potentiel de détection d'erreurs de commutation. Il y a deux types de commutation "cut-through":
  - **Commutation "Fast-forward"** – Ce mode de commutation offre le plus faible niveau de latence en acheminant une trame dès la réception de l'adresse MAC de destination. Dans ce mode, la latence est mesurée à partir du premier bit reçu jusqu'au premier bit transmis (c'est la méthode du premier entré, premier sortie ou "FIFO"). Ce mode offre un faible potentiel de détection d'erreurs de commutation de réseau LAN.
  - **Commutation "Fragment-free"** – Ce mode de commutation filtre les fragments de collision, qui constituent la majorité des erreurs de trames, avant que l'acheminement ne puisse commencer. Habituellement, les fragments de collision ont une taille inférieure à 64 octets. Dans le mode "Fragment-free", la trame reçue doit être jugée comme n'étant pas un fragment de collision pour être acheminée. Selon ce mode, la latence est aussi mesurée en regard du premier reçu, premier transmis (FIFO).
- **Store-and-Forward** – Dans ce mode, la trame doit être reçue entièrement pour qu'elle puisse être acheminée. Les adresses d'origine et de destination sont lues et des filtres sont appliqués avant l'acheminement de la trame. Une latence est générée pendant la réception de la trame. Elle est élevée s'il s'agit d'une grande trame, car l'intégralité d'une trame doit être reçue pour que le processus de commutation puisse démarrer. Le commutateur dispose du temps nécessaire pour vérifier les erreurs, ce qui améliore la détection des erreurs.
- **Adaptive Cut-through** – Il existe un autre mode de commutation hybride, appelé Cut-through adaptatif, qui combine les modes Store-and-Forward et Cut-through. Dans ce mode, le commutateur utilise le mode Cut-through jusqu'à ce qu'il détecte un nombre d'erreurs donné. Une fois le seuil d'erreurs atteint, il passe en mode Store-and-Forward. 2



Activité de média interactive

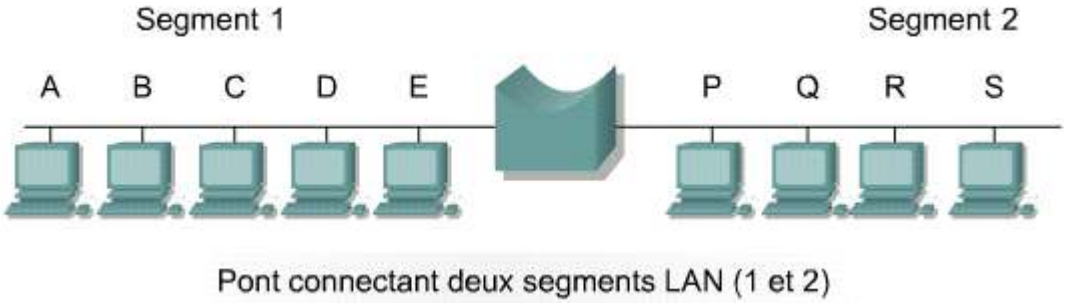
Glisser-Positionner: Points de déclenchement des modes de commutation

À la fin de cette activité, l'étudiant sera en mesure de comprendre les différents modes de commutation.

4.3 Fonctionnement d'un commutateur

4.3.3 Apprentissage des adresses par les commutateurs et les ponts

Les ponts et les commutateurs ne transmettent que les trames devant être acheminées d'un segment LAN à l'autre. Pour ce faire, ils doivent connaître les équipements qui sont connectés à chaque segment LAN. 1



Pont connectant deux segments LAN (1 et 2)

Un pont est considéré comme un équipement intelligent car il prend des décisions en se basant sur les adresses MAC. Pour ce faire, il se réfère à une table d'adresses. Lorsqu'un pont est activé, des messages de broadcast sont transmis pour demander à toutes les stations du segment local du réseau de répondre. Lorsque les stations renvoient le message de broadcast, le pont crée une table d'adresses locales. Ce processus est appelé apprentissage.

Pour apprendre des adresses, les ponts et les commutateurs procèdent comme suit:

- Ils lisent l'adresse MAC d'origine de chaque trame ou datagramme reçu.
- Ils enregistrent le port qui a reçu l'adresse MAC.

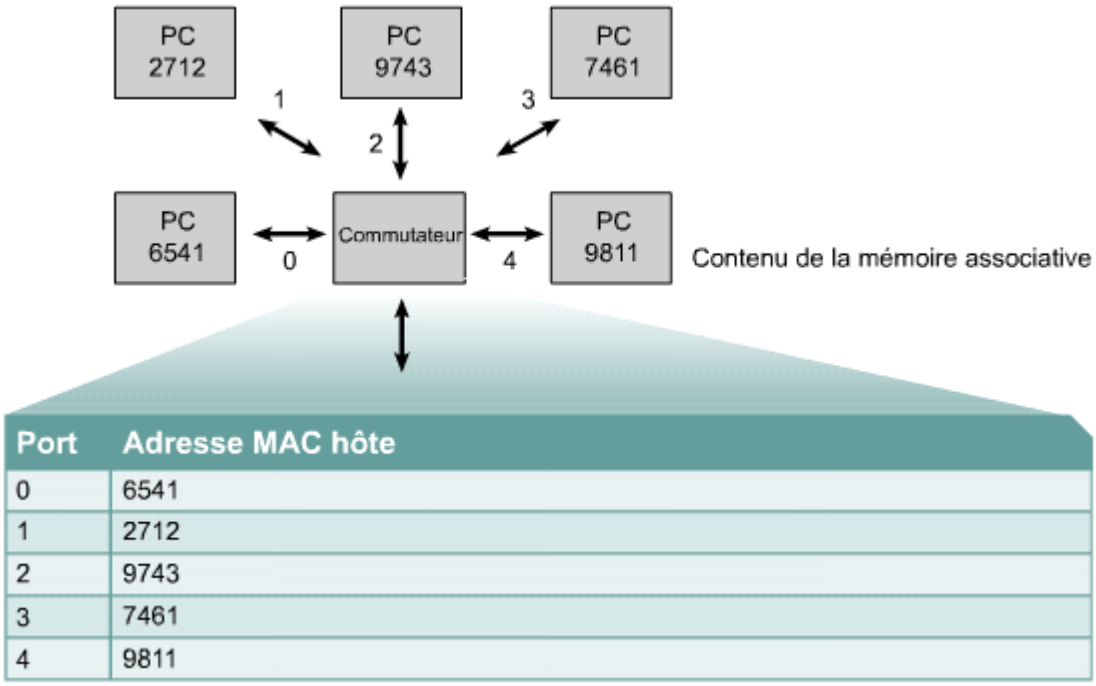
Ainsi, un pont ou un commutateur apprend les adresses appartenant aux équipements connectés à chaque port.

Les adresses apprises et l'interface ou le port associé sont stockés dans la table d'adressage. Le pont examine l'adresse de destination de toutes les trames reçues. Il balaie ensuite la table pour rechercher l'adresse de destination appropriée.

La table de commutation est enregistrée dans une mémoire associative (Content Addressable Memory – CAM). Cette mémoire associative est mise à profit pour les travaux de commutation afin de réaliser les fonctions suivantes:

- Elle extrait et traite les informations relatives aux adresses de paquets de données entrants.
- Elle compare l'adresse de destination à une de ses tables d'adresses.

La mémoire associative stocke les adresses MAC et les numéros de port associés. Elle compare l'adresse MAC de destination reçue au contenu de la table CAM. S'il existe une correspondance, le port est fourni et le contrôle de routage achemine la trame vers l'adresse et le port en question.



Port	Adresse MAC hôte
0	6541
1	2712
2	9743
3	7461
4	9811

Un commutateur Ethernet peut apprendre l'adresse de chaque unité du réseau en lisant l'adresse d'origine de chaque trame transmise et en enregistrant le port par lequel la trame est entrée dans le commutateur. Le commutateur ajoute ensuite ces informations à sa base de données de transmission. Les adresses sont apprises dynamiquement. Autrement dit, les adresses sont apprises et enregistrées dans une mémoire associative au fur et à mesure qu'elles sont lues. Si une adresse d'origine ne se trouve pas dans la mémoire associative, elle est apprise et enregistrée afin qu'elle puisse être utilisée ultérieurement.

Une adresse est horodatée chaque fois qu'elle est enregistrée. Cela permet de stocker les adresses pendant une période déterminée. Chaque fois qu'une adresse est référencée ou trouvée dans la mémoire associative, elle est de nouveau horodatée. Les adresses qui ne sont pas consultées pendant une période déterminée sont éliminées de la liste. L'élimination des adresses obsolètes permet à la mémoire associative de conserver une base de données de transmission précise et fonctionnelle.

Le processus suivi par la mémoire associative (CAM) est le suivant:

1. Si l'adresse n'est pas trouvée, le pont achemine la trame sur chaque interface à l'exception de l'interface sur laquelle la trame a été reçue.Ce processus est appelé inondation. L'adresse en question peut avoir été effacée par le pont à cause d'un redémarrage récent ou encore, parce que la capacité maximale de la table d'adresse a été atteinte, ou simplement parce que périmée. Étant donné que le pont ignore sur quelle interface acheminer la trame, elle sera transmise sur toutes les interfaces à l'exception de celle sur laquelle elle a initialement été reçue. Il est absolument inutile de renvoyer la trame sur le segment de réception car tous les ordinateurs ou les ponts sur ce segment doivent nécessairement avoir reçu la trame en question préalablement.
2. Si l'adresse est trouvée dans la table d'adresses et que l'adresse est associée à l'interface de réception, la trame est rejetée. Elle doit nécessairement avoir déjà été reçue par la destination.
3. Si l'adresse est trouvée dans la table d'adresses et que l'adresse est associée à une interface autre que celle de réception, le pont l'achemine sur l'interface en question.

Si l'adresse se trouve dans une table d'adresses mais qu'elle n'est pas associée au port qui a reçu la trame, le pont envoie celle-ci au port associé à l'adresse.

4.3 Fonctionnement d'un commutateur
4.3.4 Filtrage des trames par les commutateurs et les ponts

La plupart des ponts et des commutateurs ont maintenant la capacité de filtrer des trames selon des critères visant presque n'importe quel champ de la couche 2. Par exemple, un pont peut être programmé pour refuser, et non transmettre, toutes les trames provenant d'un réseau donné. Comme les informations de la couche liaison comprennent souvent une référence à un protocole de couche supérieure, les ponts peuvent généralement filtrer sur la base de ce paramètre. En outre, les filtres peuvent s'avérer très utiles pour traiter les paquets de broadcast et de multicast inutiles.

Une fois qu'il a créé la table d'adresses locales , un pont est prêt à fonctionner. Lorsqu'il reçoit une trame, il examine l'adresse de destination. Si l'adresse de la trame est locale, le pont l'ignore. Si la trame est destinée à un autre segment LAN, le pont la copie sur le second segment.

- Une trame est dite filtrée lorsqu'elle est ignorée.
- Une trame est dite transmise lorsqu'elle est copiée.

Le filtrage de base conserve les trames locales et envoie les trames distantes à un autre segment LAN.

Le filtrage d'adresses d'origine et de destination spécifiques comprend les actions suivantes:

- Le non acheminement des trames émises par une station en dehors de son segment LAN local.
- L'arrêt de toutes les trames « externes » destinées à une station donnée limite les autres stations avec lesquelles elle peut communiquer.

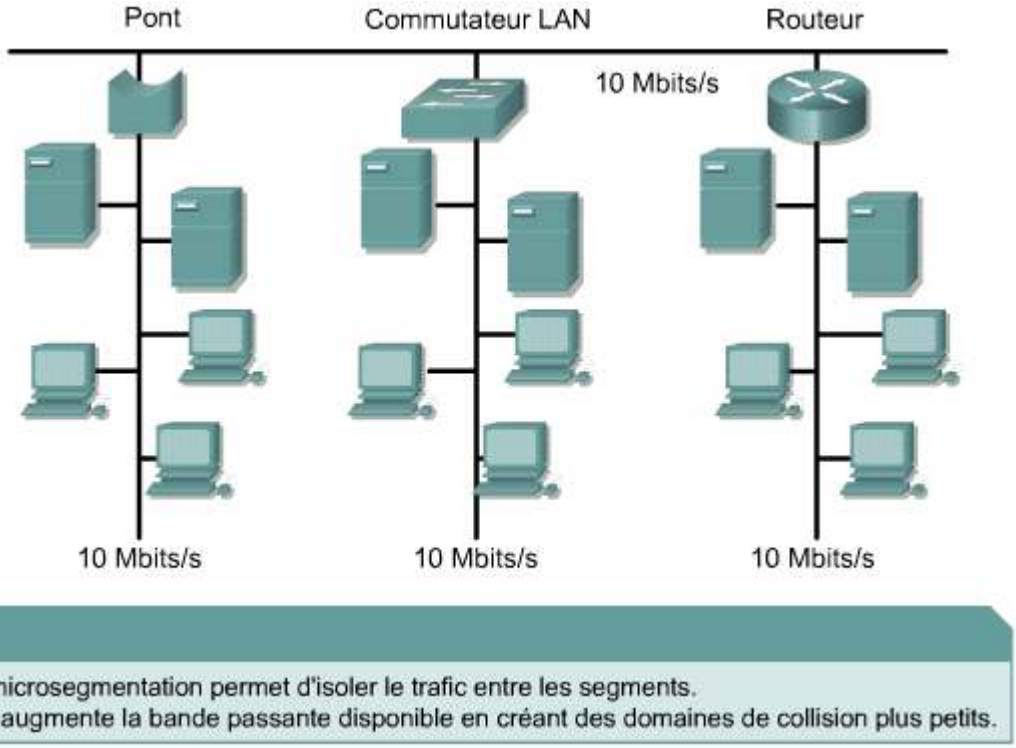
Ces deux types de filtrage permettent de contrôler le trafic interréseau et améliorent, par conséquent, la sécurité.

La plupart des commutateurs Ethernet peuvent filtrer les trames broadcast et multicast. Les ponts et les commutateurs qui peuvent filtrer les trames sous la base des adresses MAC peuvent aussi filtrer les trames Ethernet selon qu'il s'agisse d'une adresse broadcast ou multicast. Ce filtrage est accompli par la mise en œuvre de LAN virtuels (VLAN). Ceci permet aux administrateurs réseau de prévenir la transmission de messages multicast et broadcast inutiles sur le réseau. De manière occasionnelle, une unité en dysfonctionnement peut émettre continuellement des trames broadcast qui seront ensuite retransmises sur le réseau. Ce phénomène qui porte le nom de tempête de broadcast (broadcast storm) peut réduire considérablement la performance du réseau. Un commutateur ayant la capacité de filtrer les trames broadcast peut donc rendre les tempêtes de broadcast moins dangereuse.

Les commutateurs actuels sont également capables de filtrer en fonction du protocole de couche réseau, ce qui estompe la démarcation entre les ponts et les routeurs. Un routeur opère au niveau de la couche réseau à l'aide d'un protocole de routage pour acheminer le trafic directement sur le réseau. Un commutateur qui met en œuvre les techniques de filtrage avancées est généralement appelé un pont-routeur. Les ponts-routeurs filtrent en examinant les informations de la couche réseau mais n'utilisent pas de protocole de routage. [1]

4.3 Fonctionnement d'un commutateur
4.3.5 Pourquoi segmenter les réseaux LAN ?

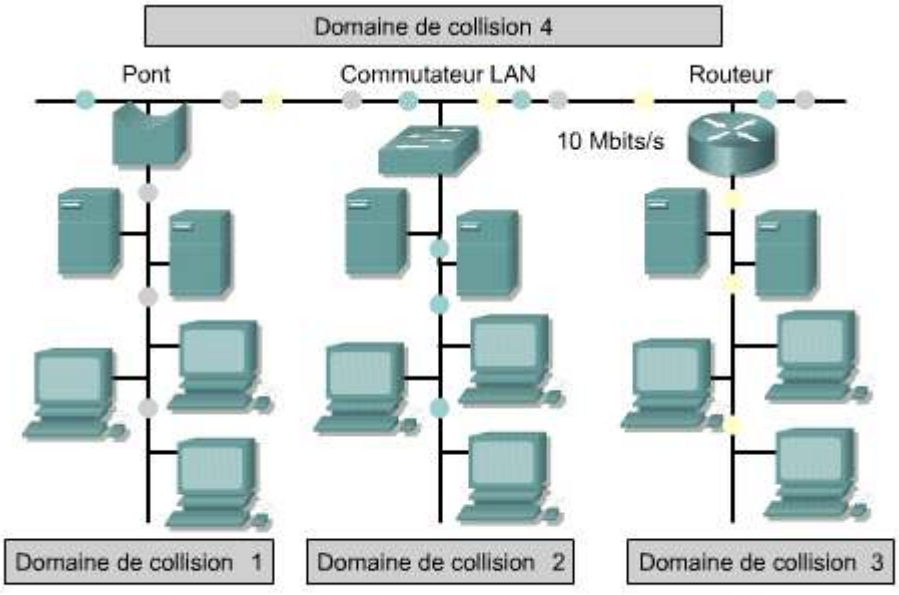
Deux raisons principales sont à la base de la segmentation d'un LAN. La première a pour but d'isoler le trafic entre les segments. La seconde a pour but de fournir davantage de bande passante par utilisateur par la création de domaines de collision de petite taille. [1]



Sans la segmentation, les LAN d'une taille supérieure à un petit groupe de travail seraient rapidement encombrés par le trafic et les collisions.

La segmentation LAN peut être mise en œuvre à l'aide de ponts, de commutateurs et de routeurs. Chacun de ces équipements présente des avantages et des inconvénients.

L'ajout de ponts, de commutateurs et de routeurs segmente un LAN en un certain nombre de domaines de collision de petite taille. Dans l'exemple représenté sur la figure, quatre domaines de collision ont été créés. 2



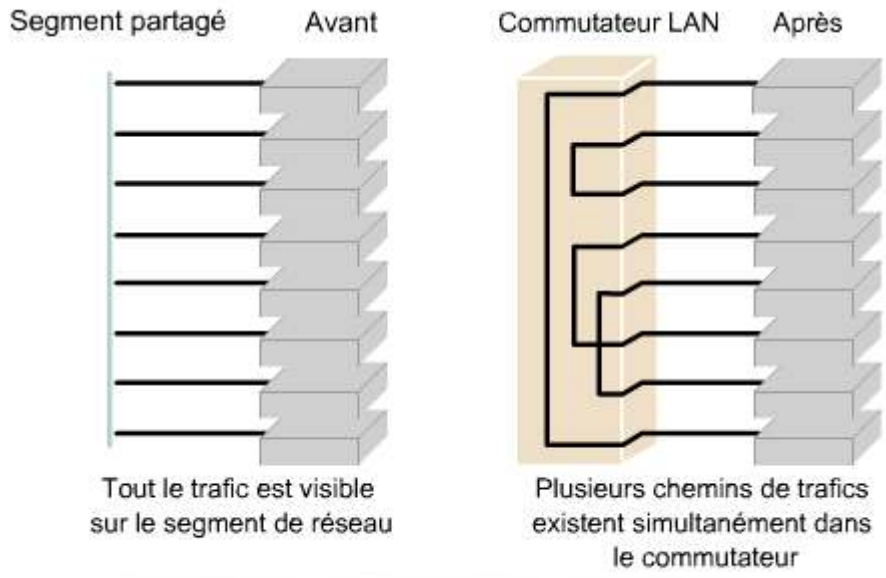
Les ponts, les commutateurs et les routeurs divisent les domaines de collision.

En divisant les grands réseaux en unités autonomes, les ponts et les commutateurs offrent plusieurs avantages. Les ponts et les commutateurs diminuent le trafic reçu par les unités de tous les segments connectés, parce qu'un certain pourcentage du trafic seulement est acheminé. Ils réduisent le domaine de collision mais pas le domaine de broadcast.

Chaque interface du routeur se connecte à un réseau distinct. Par conséquent, l'insertion du routeur dans un LAN créera de petits domaines de collision et de broadcast car les routeurs n'acheminent pas de messages de broadcast, sauf s'ils sont programmés à cet effet.

Un commutateur recourt à la microsegmentation pour réduire le domaine de collision d'un LAN. Pour ce faire, il crée des segments de réseau dédiés ou des connexions point-à-point, puis il connecte ces segments à son réseau virtuel.

Ce circuit de réseau virtuel n'existe que lorsque deux nœuds doivent communiquer. Ce composant est appelé circuit virtuel car il n'existe que s'il est nécessaire et il est créé à l'intérieur du commutateur. 3

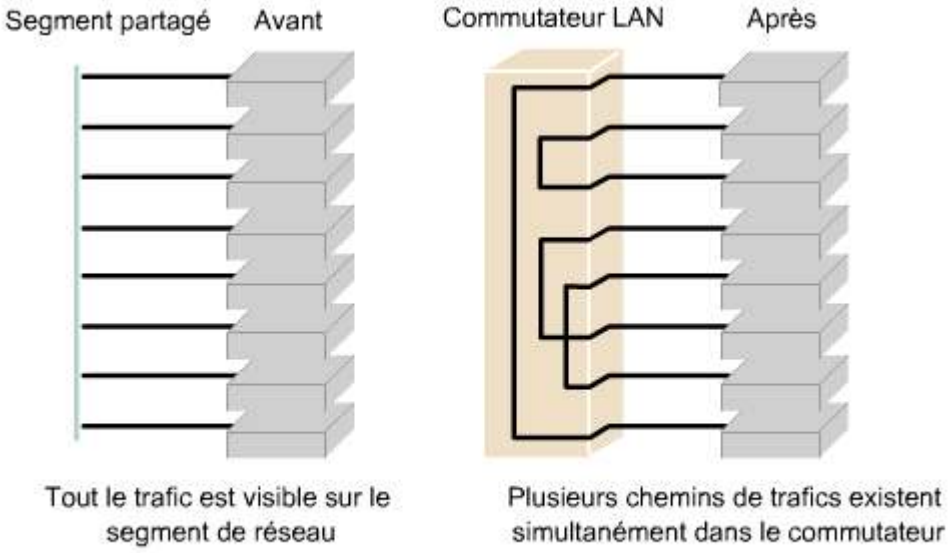


Un commutateur crée des chemins dédiés entre les hôtes émetteur et récepteur.

4.3 Fonctionnement d'un commutateur

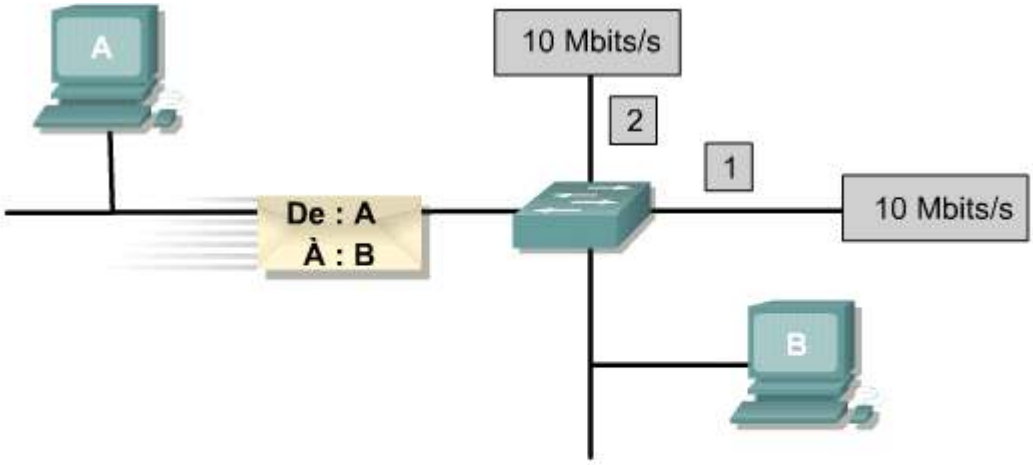
4.3.6 Mise en œuvre de la microsegmentation

Les commutateurs d'un LAN sont considérés comme des ponts multiports sans domaine de collision en raison de la microsegmentation. 1

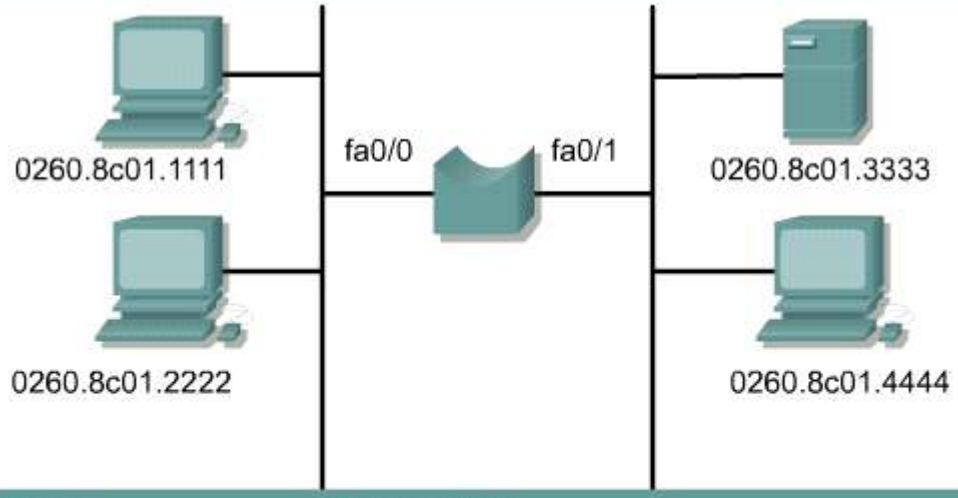


Un commutateur crée des chemins dédiés entre les hôtes émetteur et récepteur.

L'échange des données s'effectue à haut débit en commutant la trame vers sa destination. En lisant les informations de l'adresse MAC de destination de la couche 2, les commutateurs peuvent atteindre de hauts débits de transfert de données, à l'instar des ponts. Ce procédé entraîne de faibles niveaux de latence et un débit de transmission élevé. 2 3



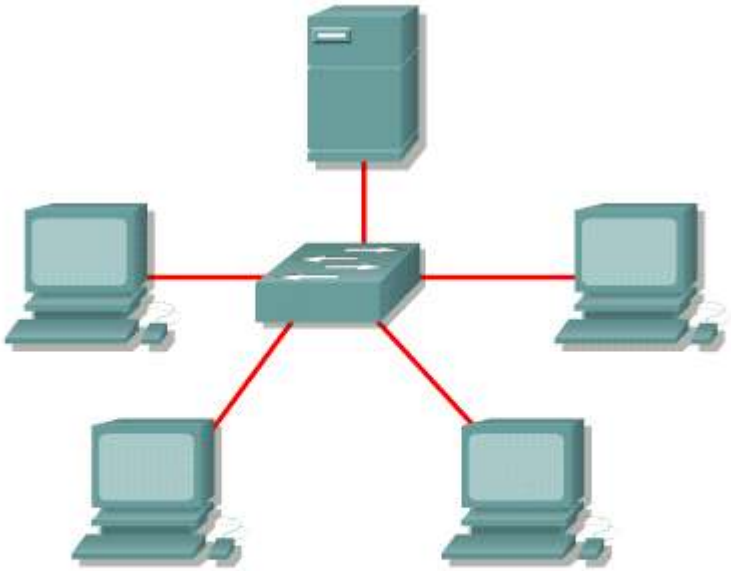
- Il achemine les trames selon une table de transmission.
- Il fonctionne au niveau de la couche 2 du modèle OSI.
- Il achemine les trames en fonction de l'adresse MAC (couche 2).



Interface	Adresse MAC
Fa0/0	0260.8c01.1111
Fa0/0	0260.8c01.2222
Fa0/1	0260.8c01.3333
Fa0/1	0260.8c01.4444

La commutation Ethernet augmente la bande passante disponible sur un réseau. Pour ce faire, elle crée des segments réseau dédiés ou des connexions point-à-point et connecte ces segments en un réseau virtuel au niveau du commutateur. Ce circuit de réseau virtuel n'existe que lorsque deux nœuds doivent communiquer. Ce composant est appelé circuit virtuel car il n'existe que s'il est nécessaire et il est créé à l'intérieur du commutateur.

Bien qu'un commutateur LAN réduise la taille des domaines de collision, tous les hôtes qui y sont connectés continuent d'appartenir au même domaine de broadcast. Par conséquent, un broadcast provenant d'un nœud continuera d'être vu par tous les autres nœuds connectés via le commutateur LAN. [4]



- Permet un accès dédié.
- Élimine les collisions et accroît la capacité.
- Supporte plusieurs conversations simultanées

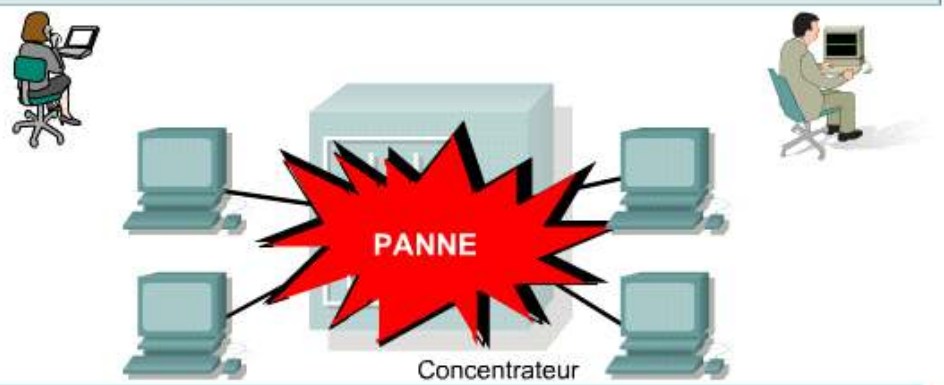
Les commutateurs sont des unités de la couche liaison de données qui, comme les ponts, permettent à plusieurs segments physiques d'un LAN de s'interconnecter en un seul réseau de plus grande taille. À l'instar des ponts, les commutateurs transmettent et diffusent le trafic en fonction des adresses MAC. Comme la commutation s'effectue au niveau matériel et non au niveau logiciel, la transmission est considérablement plus rapide. Chaque port de commutateur peut être considéré comme un micropont qui se comporte comme un pont à part entière et fournit à chaque hôte la totalité de la bande passante du média.

4.3 Fonctionnement d'un commutateur

4.3.7 Commutateurs et domaines de collision

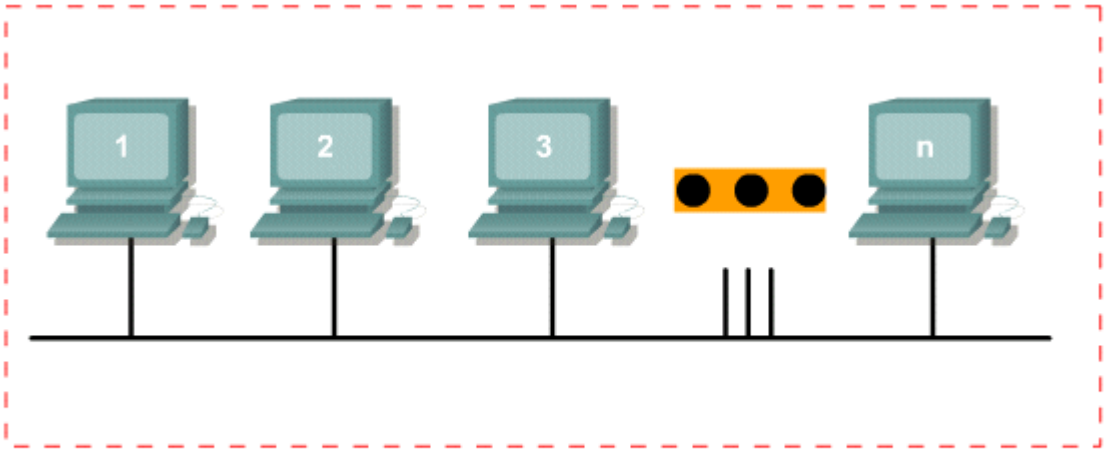
Les collisions constituent l'inconvénient majeur des réseaux Ethernet 802.3. Une collision se produit lorsque deux hôtes transmettent des trames simultanément. Les trames transmises au cours d'une collision sont altérées ou détruites. Les hôtes émetteurs arrêtent la transmission pendant une période de temps aléatoire basée sur les règles Ethernet 802.3 du mode d'accès CSMA/CD. Un nombre excessif de collisions peut nuire à la productivité d'un réseau. [1]

- " J'aurais déjà pu me rendre jusqu'au service des finances. "
- " Je savais que j'aurais dû rester à la maison. "
- " Les transferts de fichiers prennent un temps fou. "
- " J'attends tout le temps. "

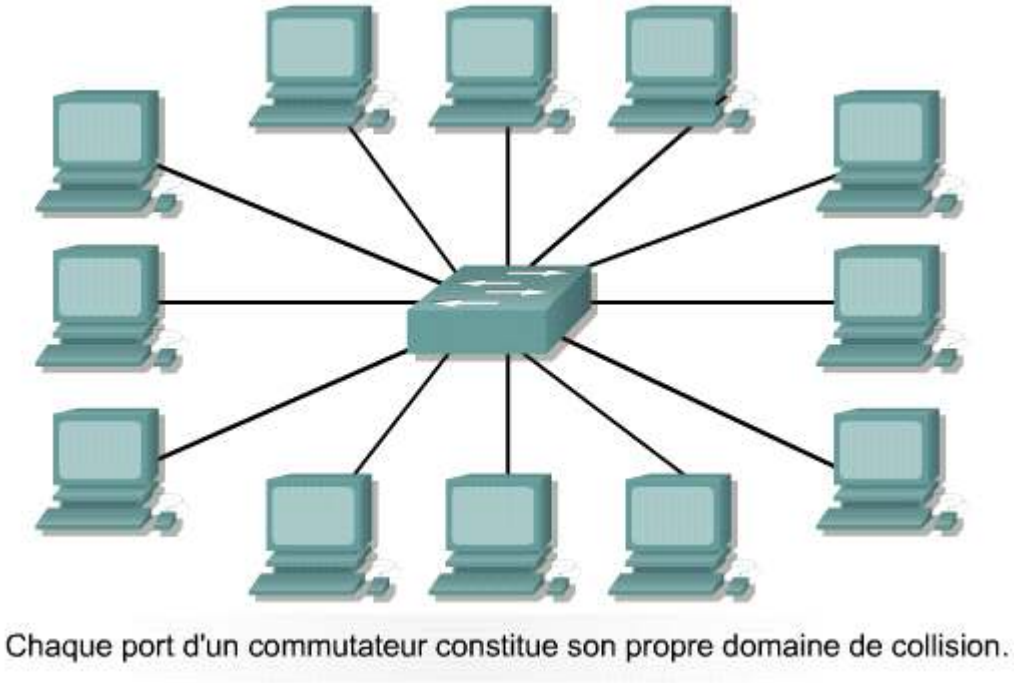


- Lenteur de réponse du réseau
- Augmentation du nombre de plaintes de la part des utilisateurs

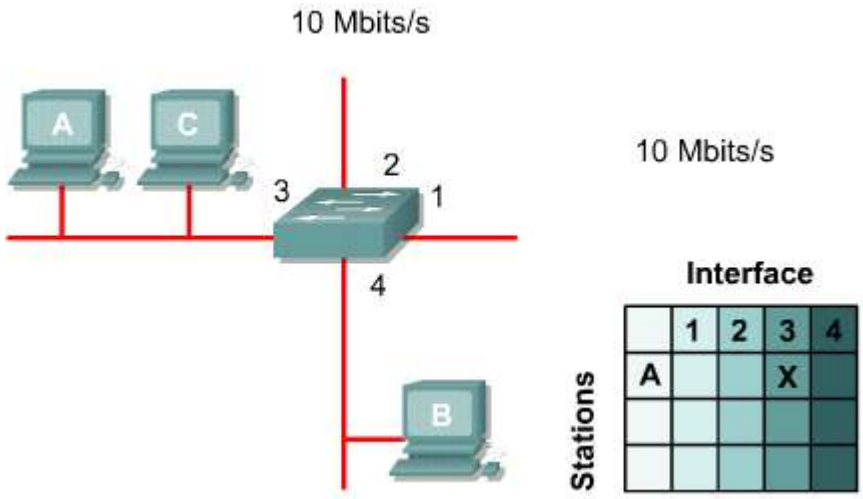
La zone du réseau d'où proviennent les trames qui entrent en collision est appelée domaine de collision. Tous les environnements à média partagé sont des domaines de collision. 2



Quand un hôte est connecté à une interface d'un commutateur, le commutateur crée alors une connexion dédiée. Cette connexion est considérée comme un domaine de collision individuel. Par exemple, si un commutateur à douze ports comprend une unité connectée à chaque port, douze domaines de collision sont créés. 3

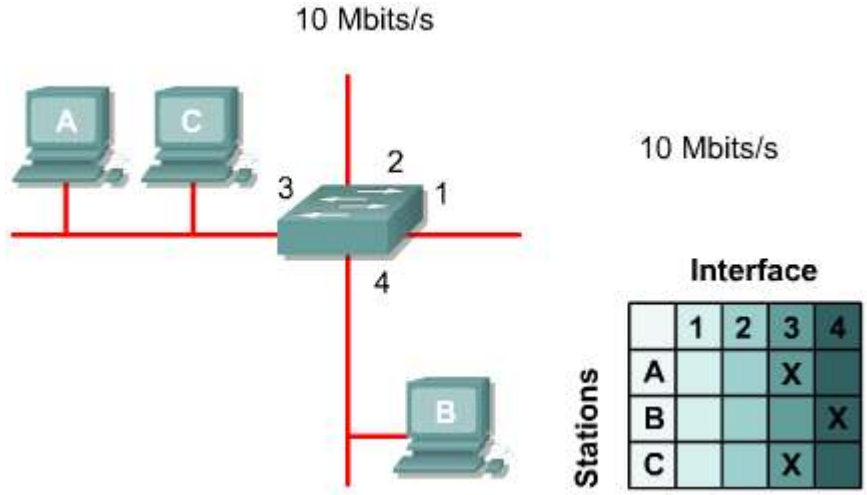


Un commutateur crée une table de commutation en apprenant les adresses MAC des hôtes connectés à chaque port du commutateur. 4



Lorsque deux hôtes connectés veulent communiquer, le commutateur consulte la table de commutation et établit une connexion virtuelle entre les deux ports. Le circuit virtuel est maintenu jusqu'à ce que la session soit terminée.

Dans la figure 5, les hôtes B et C veulent communiquer entre eux. Le commutateur crée une connexion virtuelle appelée microsegment. Ce microsegment se comporte comme si le réseau ne comprenait que deux hôtes, un hôte émetteur et un hôte récepteur fournissant le taux d'utilisation maximal de bande passante.



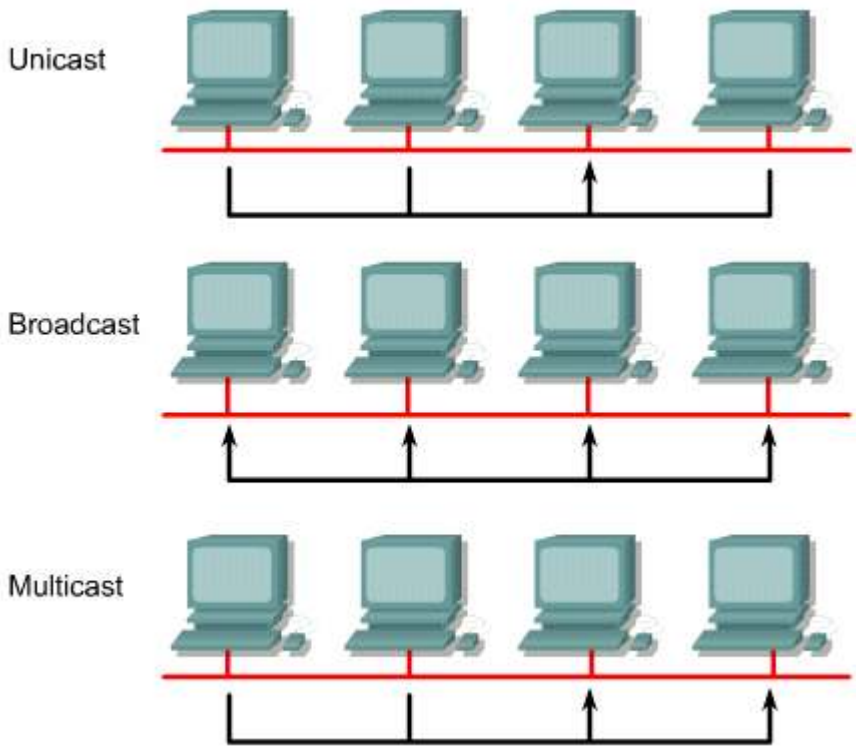
Les commutateurs réduisent le nombre de collisions et augmentent la bande passante sur les segments réseau parce qu'ils offrent une bande passante réservée à chacun de ces segments.

4.3 Fonctionnement d'un commutateur

4.3.8 Commutateurs et domaines de broadcast

Il existe trois modes de transmission sur un réseau. Le mode le plus fréquent est la transmission unicast. Dans ce mode, un émetteur tente d'atteindre un récepteur.

La transmission multicast est le deuxième mode de transmission. Dans ce mode, un émetteur tente d'atteindre un sous-ensemble, un groupe ou un segment entier. 1

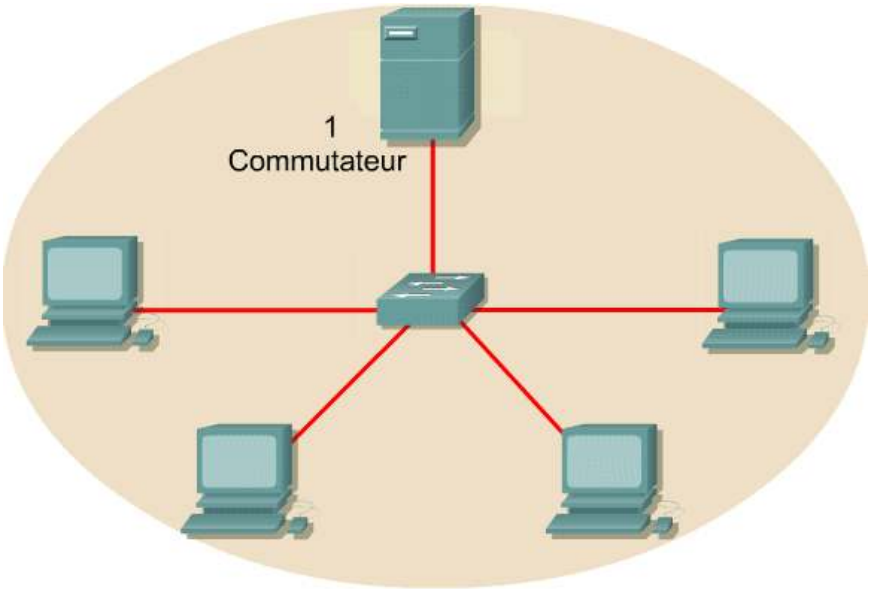


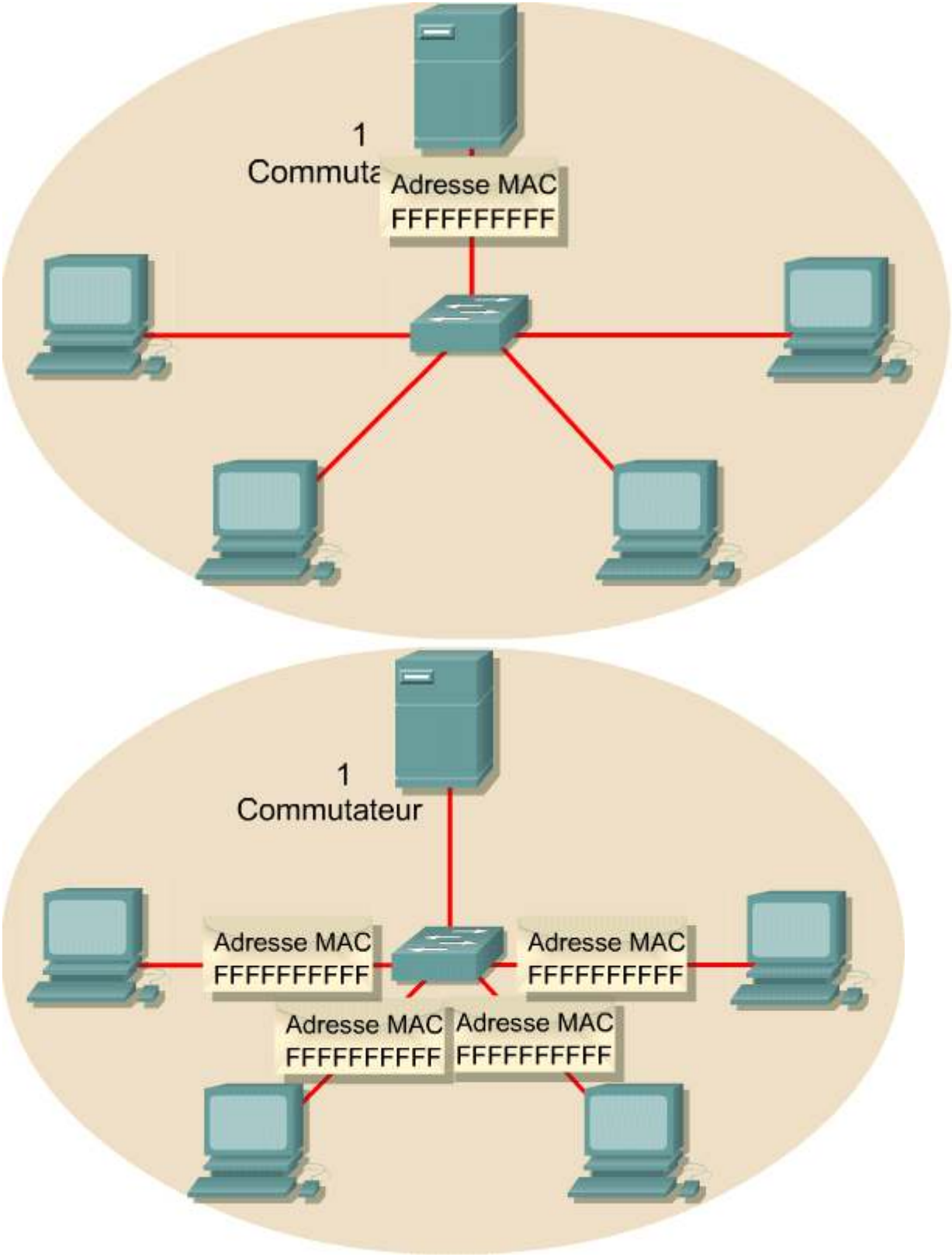
La diffusion de broadcasts constitue le troisième mode de transmission. Dans ce mode, un émetteur tente d'atteindre tous les récepteurs du réseau. Le serveur envoie un message et toutes les unités du segment le reçoivent.

Lorsqu'une unité souhaite envoyer un broadcast de couche 2, l'adresse MAC de destination de la trame contient uniquement des 1. Une adresse MAC ne contenant que des 1 correspond à l'adresse hexadécimale FF:FF:FF:FF:FF:FF. En attribuant cette valeur à la destination, toutes les unités accepteront et traiteront la trame de broadcast.

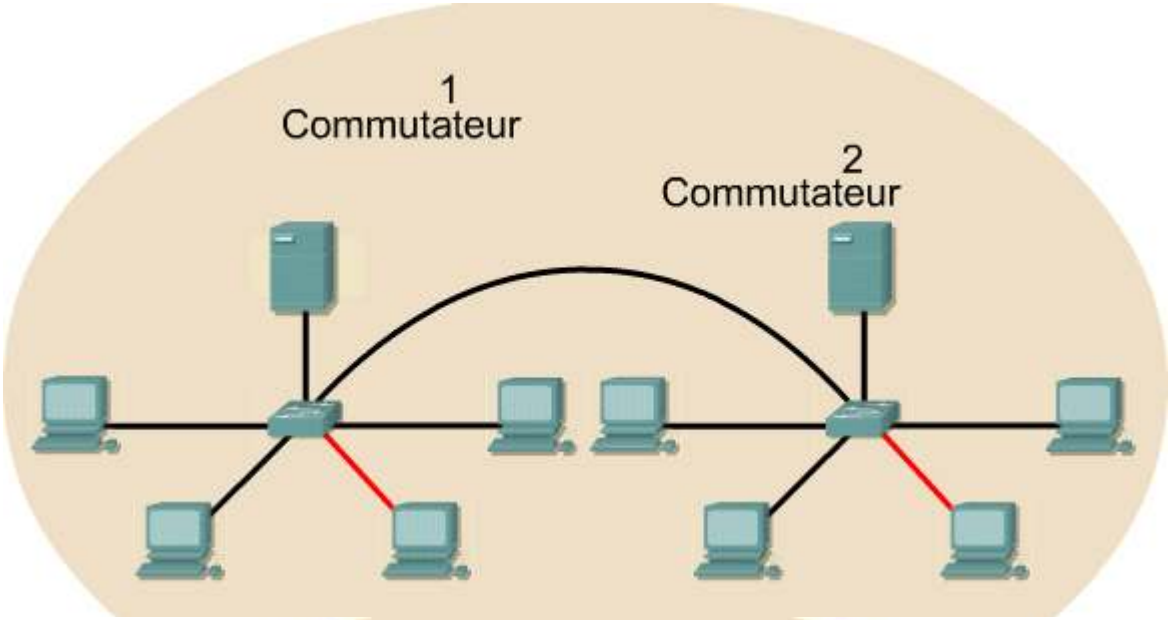
Le domaine de broadcast de couche 2 est appelé domaine de broadcast MAC. Ce domaine comprend toutes les unités du LAN qui reçoivent d'un hôte les trames de broadcast destinées à toutes les autres machines du LAN.

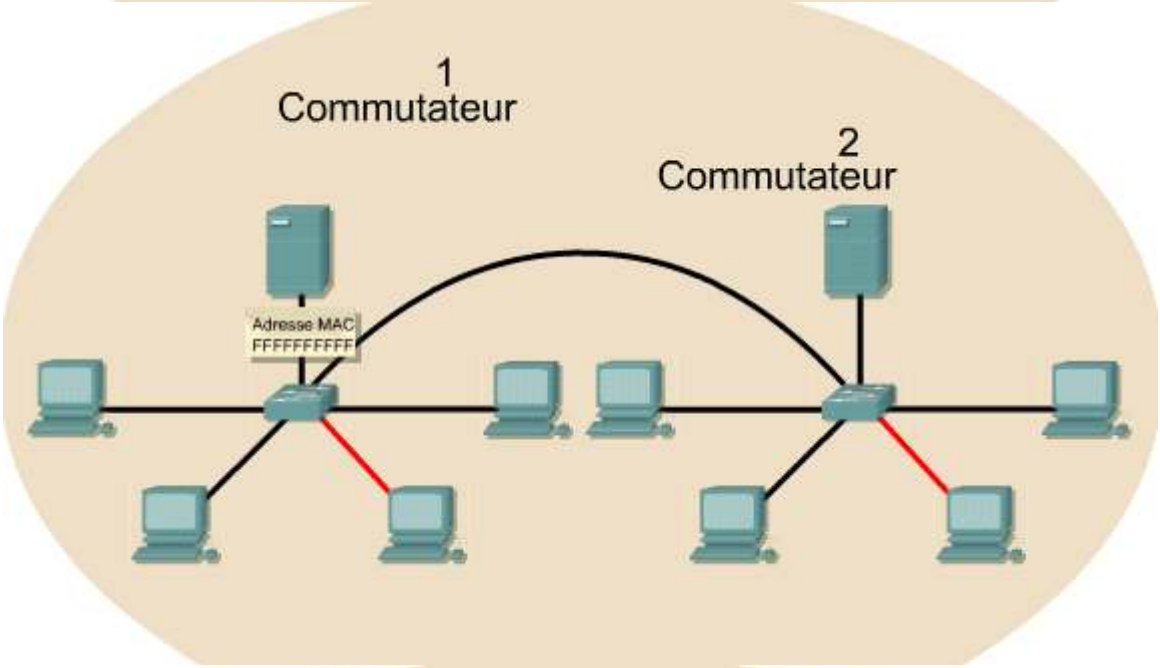
Un commutateur est un équipement de couche 2. Lorsqu'un commutateur reçoit un broadcast, il l'envoie à chacun de ses ports excepté, au port d'entrée. Chaque unité connectée doit traiter la trame de broadcast, ce qui réduit l'efficacité du trafic en raison de la bande passante disponible utilisée pour diffuser les broadcasts. 2

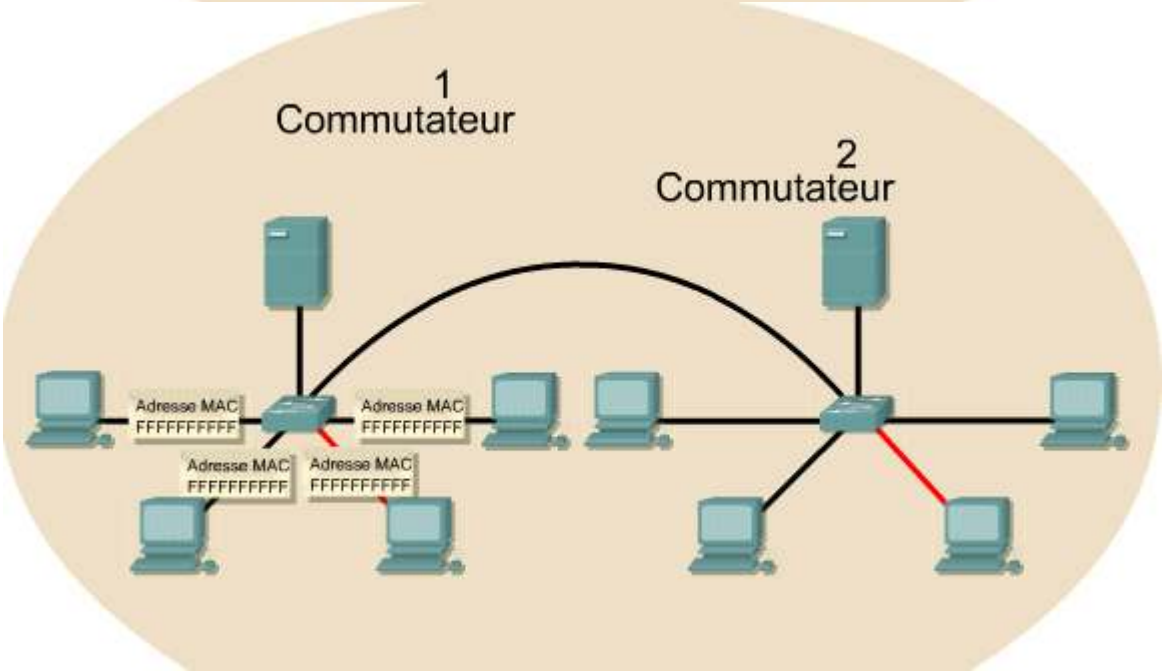


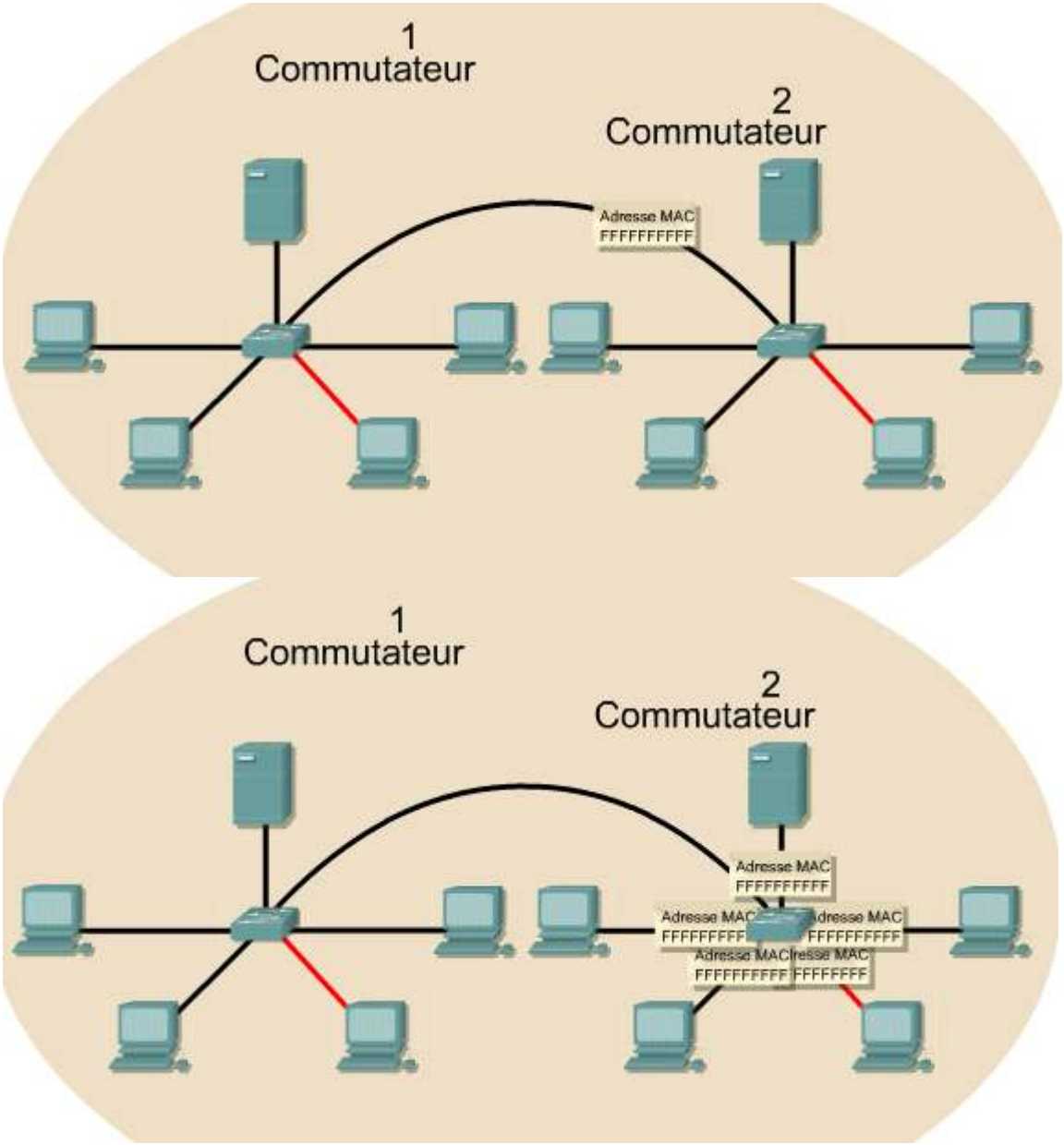


Lorsque deux commutateurs sont connectés, le domaine de broadcast augmente. Dans cet exemple, une trame de broadcast est envoyée à tous les ports connectés au commutateur 1 qui est relié au commutateur 2. La trame est diffusée à toutes les unités connectées au commutateur 2. 3


1
Commutateur
2
Commutateur


1
Commutateur
2
Commutateur
Adresse MAC
FFFFFFFFFF


1
Commutateur
2
Commutateur
Adresse MAC
FFFFFFFFFF
Adresse MAC
FFFFFFFFFF
Adresse MAC
FFFFFFFFFF
Adresse MAC
FFFFFFFFFF



Le résultat global se traduit par une réduction de la bande passante disponible, car toutes les unités du domaine de broadcast doivent recevoir et traiter la trame de broadcast.

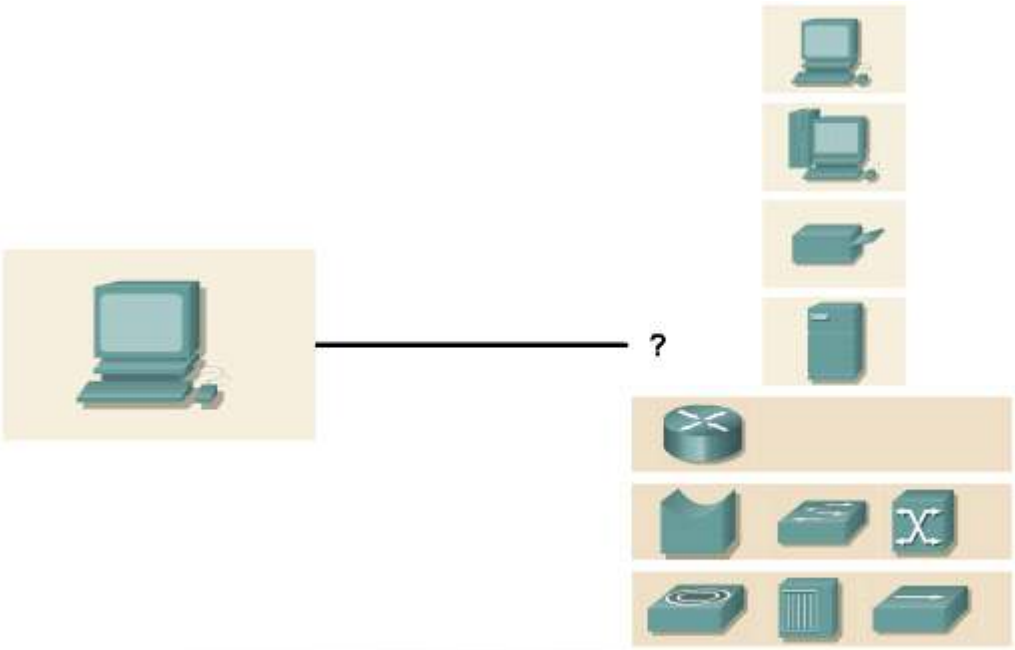
Les routeurs sont des équipements de couche 3. Ils ne diffusent pas de broadcasts et sont utilisés pour segmenter les domaines de collision et de broadcast.

4.3 Fonctionnement d'un commutateur

4.3.9 Communication entre des commutateurs et une station de travail

Lorsqu'une station de travail se connecte à un réseau LAN, elle ne se préoccupe pas des autres unités connectées au média du LAN. Elle se contente de transmettre les trames de données au média, via une carte réseau.

La station de travail pourrait être reliée directement à une autre station de travail en utilisant un câble croisé. Les câbles croisés sont utilisés afin d'interconnecter les unités suivantes: 1



Les stations de travail ne se préoccupent que de transmettre des trames de données au média.

- Station de travail à station de travail
- Commutateur à commutateur
- Commutateur à concentrateur
- Concentrateur à concentrateur
- Routeur à routeur
- Routeur à PC

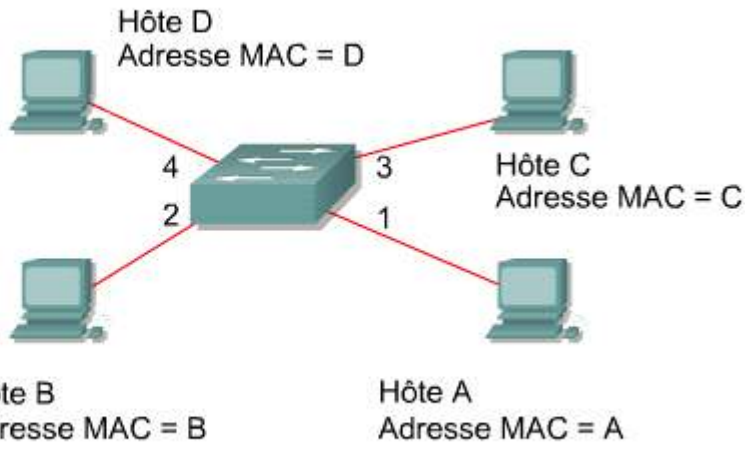
Les câbles droits sont quant à eux utilisés pour interconnecter les unités suivantes:

- Commutateur à routeur
- Commutateur à station de travail ou serveur
- Concentrateur à station de travail ou serveur

Les commutateurs sont des unités de couche 2 intelligentes qui apprennent les adresses MAC des unités reliées aux ports du commutateur. Les informations relatives aux adresses sont entrées dans une table de commutation. Une fois la table créée, le commutateur peut lire l'adresse MAC de destination d'une trame de données entrant sur un port et la transmettre immédiatement. 2

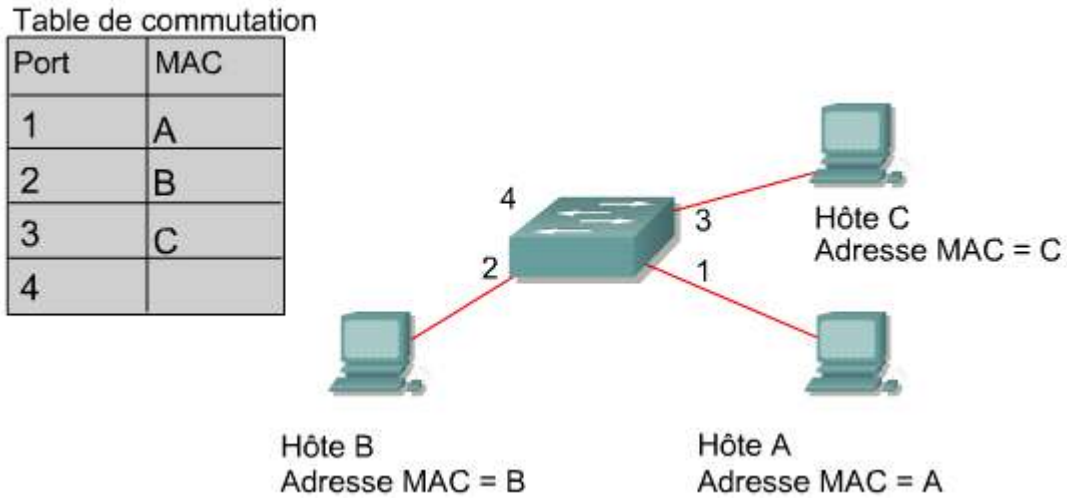
Table de commutation

Port	MAC
1	A
2	B
3	C
4	D

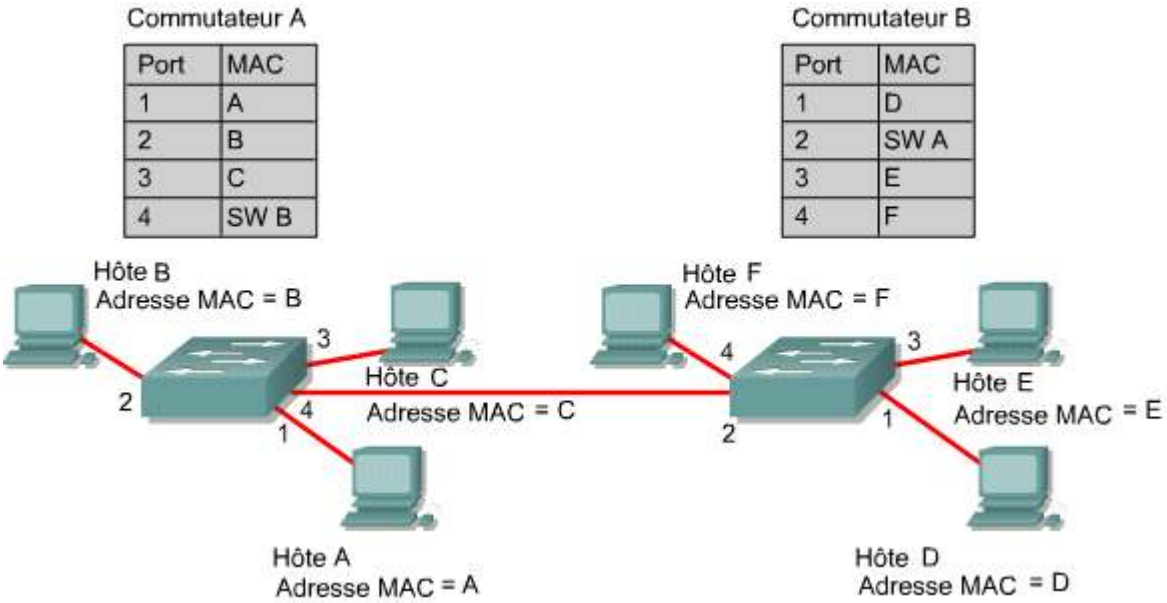


Les commutateurs prennent des décisions intelligentes d'acheminement.

Le commutateur ne connaît pas l'adresse MAC d'une unité tant que celle-ci n'a pas effectué de transmission. 3



Les commutateurs améliorent considérablement l'évolutivité du réseau et peuvent être directement connectés. La figure 4 illustre un exemple de transmission de trame utilisant un réseau multicommutateur.



Résumé

La compréhension des points clés suivants devrait être acquise :

- Historique et fonctionnement Ethernet partagé en mode half-duplex
- Collisions dans un réseau Ethernet
- Microsegmentation
- Mode d'accès CSMA/CD
- Éléments affectant les performances réseau
- Fonction des répéteurs
- Latence d'un réseau
- Temps de transmission
- Fonctionnement de base de la technologie Fast Ethernet
- Segmentation d'un réseau à l'aide de routeurs, de commutateurs et de ponts
- Fonctionnement de base d'un commutateur
- Latence des commutateurs Ethernet
- Différences entre la commutation de couche 2 et la commutation de couche 3
- Commutation symétrique et asymétrique
- Mise en mémoire tampon

- Commutation Store-and-Forward et Cut-through
- Différences entre les concentrateurs, les ponts et les commutateurs
- Principales fonctions d'un commutateur
- Principaux modes de transmission de trames de commutateur
- Apprentissage d'adresses par les commutateurs
- Filtrage de trames
- Segmentation LAN
- Microsegmentation à l'aide de la commutation
- Modes de transmission
- Domaines de collision et de broadcast

Résumé

• Les premières technologies LAN utilisaient des infrastructures Ethernet à câble épais ou fin.
• Ethernet est l'architecture LAN la plus répandue. Le réseau Ethernet est utilisé pour transporter des données entre les unités d'un réseau. Ces unités peuvent être des ordinateurs, des imprimantes ou des serveurs de fichiers.
• Un réseau peut être divisé en unités plus petites appelées segments.
• La segmentation permet de réduire efficacement la congestion de réseau au sein de chaque segment.
• La commutation LAN diminue les contraintes de bande passante et les goulots d'étranglement sur le réseau, tels que ceux qui se produisent entre des stations de travail et un serveur de fichiers distant.
• Les deux modes de commutation sont : Store-and-Forward et Cut-through.
• Les deux types de commutation Cut-through sont : Fast-Forward et Fragment-Free.
• Un commutateur est une unité réseau qui sélectionne un chemin ou un circuit pour l'envoi d'une trame vers sa destination. Les commutateurs et les ponts fonctionnent au niveau de la couche 2 du modèle OSI.

Vue d'ensemble

La conception d'un réseau constitue un défi important, qui va bien au-delà de la simple interconnexion des ordinateurs. Pour être fiable, évolutif et facile à gérer, un réseau doit posséder un grand nombre de caractéristiques évoluées. Afin de concevoir des réseaux fiables, gérables et évolutifs, les concepteurs doivent connaître les caractéristiques particulières des principaux composants.

La conception d'un réseau devient de plus en plus difficile malgré les améliorations des performances des équipements et des capacités des médias. L'utilisation de plusieurs types de médias et l'interconnexion de réseaux locaux à d'autres réseaux externes complique l'environnement de réseau. C'est pourquoi une bonne conception de réseau améliorera les performances et réduira les difficultés inhérentes à la croissance et à l'évolution du réseau.

Un réseau LAN peut s'étendre à une seule pièce, à un bâtiment ou à un ensemble de bâtiments proches les uns des autres. On appelle campus un groupe de bâtiments situés sur un même site et appartenant à une organisation unique. La conception de grands réseaux locaux inclut l'identification des éléments suivants:

- Une couche accès qui interconnecte les utilisateurs finaux au sein du réseau LAN
- Une couche distribution qui assure, entre les réseaux LAN des utilisateurs finaux, une connectivité basée sur les politiques d'administration et de sécurité
- Une couche principale qui assure la connexion la plus rapide entre les points de distribution

Chacune de ces couches de conception de réseau LAN nécessite des commutateurs adaptés à des tâches spécifiques. Les caractéristiques, fonctions et spécifications techniques de chaque commutateur varient en fonction de la couche conception du réseau LAN à laquelle le commutateur est destiné. Afin de garantir aux utilisateurs les meilleures performances de réseau, il convient de comprendre le rôle de chaque couche, puis de choisir les commutateurs les mieux adaptés pour cette couche.

À la fin de ce module, les étudiants doivent être en mesure de:

- Décrire les quatre objectifs majeurs de la conception de réseau LAN
- Lister les considérations clés de la conception de réseau LAN

- Comprendre les différentes étapes d'une conception méthodique de réseau LAN
- Comprendre les problèmes de conception associés avec la structure LAN des couches 1, 2 et 3 ou de la topologie
- Décrire le modèle de conception à trois couches
- Identifier les fonctions de chaque couche du modèle à trois couches
- Répertorier les commutateurs Cisco de la couche accès et leurs caractéristiques
- Répertorier les commutateurs Cisco de la couche distribution et leurs caractéristiques
- Répertorier les commutateurs Cisco de la couche principale et leurs caractéristiques

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
5.1	Conception LAN
5.2	Commutateurs LAN

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
• Conception d'un LAN simple à l'aide de la technologie • Conception d'un interréseau simple à l'aide de la technologie Cisco	• Mise en œuvre d'un LAN • Personnalisation de la configuration d'un commutateur pour répondre aux exigences du réseau		• Comparaison des principales caractéristiques des environnements LAN

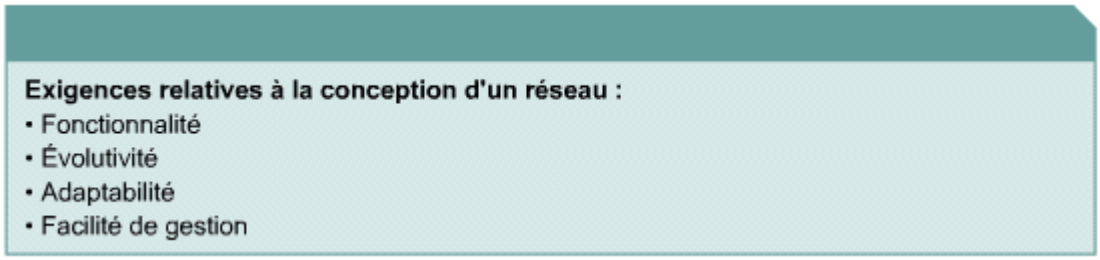
Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
• Conception d'un LAN simple à l'aide de la technologie • Conception d'un interréseau simple à l'aide de la technologie Cisco	• Mise en œuvre d'un LAN • Personnalisation de la configuration d'un commutateur pour répondre aux exigences du réseau		• Évaluation des caractéristiques des environnements LAN

5.1 Conception LAN

5.1.1 Objectifs de la conception LAN

La première étape de conception d'un réseau local consiste à définir les objectifs et à les expliquer par écrit. Ces objectifs sont propres à chaque organisation ou situation. Les exigences suivantes sont habituellement rencontrées dans la plupart des conceptions réseau: 1



- **Fonctionnalité** – Le réseau doit être fonctionnel. Il doit permettre aux utilisateurs de répondre à leurs besoins professionnels. Il doit fournir une connectivité fiable entre les utilisateurs ainsi qu'entre les utilisateurs et les applications, avec un débit raisonnable.
- **Évolutivité** – Le réseau doit présenter une capacité d'extension. La conception initiale doit pouvoir s'étendre sans qu'il soit nécessaire d'apporter des modifications importantes à la conception globale.
- **Adaptabilité** – Le réseau doit être conçu de façon à s'adapter aux futures technologies. Il ne doit inclure aucun élément susceptible de limiter la mise en œuvre de nouvelles technologies au fur et à mesure qu'elles deviennent disponibles.
- **Facilité de gestion** – Un réseau doit être conçu pour faciliter la surveillance et la gestion du réseau afin d'en garantir la stabilité permanente.

Activité de média interactive

Associer: Objectifs de conception d'un réseau local

À la fin de ce TP, l'étudiant sera en mesure de comprendre les termes, les définitions et les objectifs de la conception LAN.

5.1 Conception LAN

5.1.2 Choix de conception LAN

Beaucoup d'organisations mettent à niveau des réseaux LAN existants ou planifient, conçoivent et mettent en œuvre de nouveaux LAN. Cette extension de la conception LAN découle du développement des technologies de haut débit telles que l'ATM (Asynchronous Transfer Mode). Elle est également due aux architectures LAN complexes qui utilisent la commutation LAN et les LAN virtuels (VLAN).

Afin de maximiser la bande passante et les performances LAN, il faut prendre en compte les aspects de conception LAN suivants:

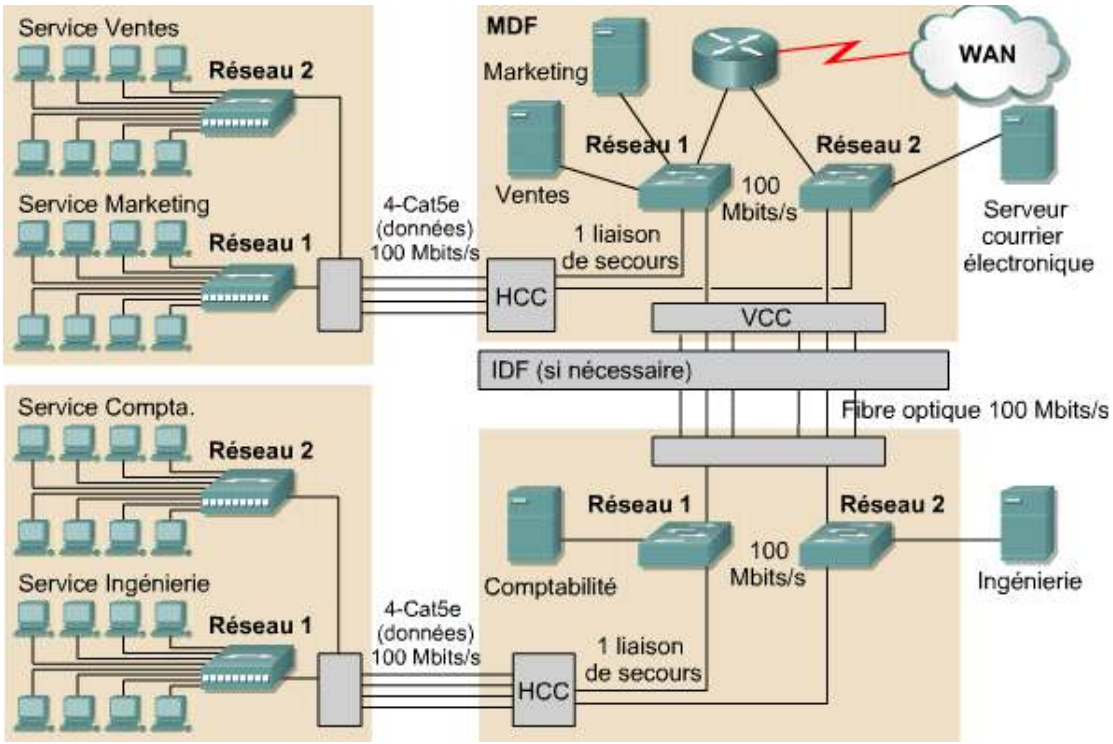
- la fonction et l'emplacement des serveurs,
- Problématique des domaines de collision,
- les problèmes de segmentation,
- les problèmes de domaine de broadcast.

Les serveurs fournissent des services de partage de fichiers, d'impression, de communication et d'application. Ils ne fonctionnent généralement pas comme des stations de travail. Ils exécutent des systèmes d'exploitation spécialisés, comme NetWare, Windows Server, UNIX et Linux. Chaque serveur est habituellement dédié à une seule fonction, par exemple au courrier électronique ou au partage de fichiers.

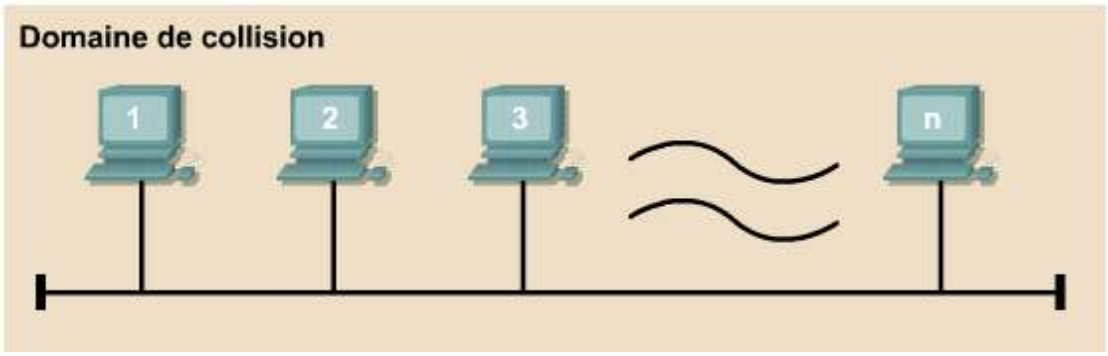
On peut distinguer deux catégories de serveurs : les serveurs d'entreprise et les serveurs de groupe de travail. Un serveur d'entreprise prend en charge tous les utilisateurs du réseau en leur offrant des services tels que le courrier électronique ou le système de noms de domaine (DNS), dont tous les membres d'une organisation ont besoin, car il s'agit de fonctions centralisées. En revanche, un serveur de groupe de travail prend en charge un ensemble spécifique d'utilisateurs et offre des services tels que le traitement de texte et le partage de fichiers.

Les serveurs d'entreprise doivent être installés dans le répartiteur principal MDF. 1 Règle générale, le trafic à destination des serveurs d'entreprise devrait voyager seulement vers le MDF et ne pas être transmis sur d'autres réseaux. Cependant, certains réseaux utilisent un routage central ou encore, peuvent avoir une batterie de serveurs à titre de serveurs d'entreprise. Idéalement, les serveurs de groupe de travail doivent être installés dans des répartiteurs intermédiaires IDF, le plus près possible des utilisateurs qui accèdent aux applications de ces serveurs. En installant les serveurs de groupe de travail près des utilisateurs, le trafic circule uniquement dans l'infrastructure réseau menant au répartiteur intermédiaire IDF et n'a aucune

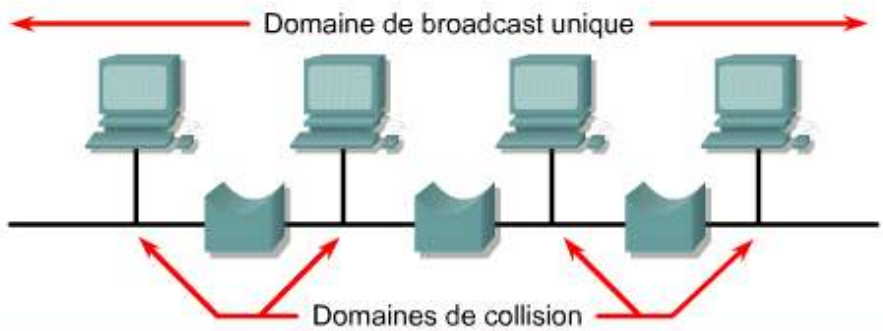
incidence sur les autres utilisateurs de ce segment de réseau. Dans le répartiteur principal MDF et les répartiteurs intermédiaires IDF, les commutateurs LAN de couche 2 liés à ces serveurs doivent avoir un débit minimal de 100 Mbits/s.



Les nœuds Ethernet utilisent CSMA/CD. Chaque nœud doit rivaliser avec tous les autres nœuds pour accéder au média partagé, ou domaine de collision. Si deux nœuds transmettent simultanément, une collision se produit. Dans ce cas, la trame transmise est détruite, et un signal de bourrage est envoyé à tous les nœuds sur le segment. Les nœuds émetteurs attendent une période aléatoire, puis renvoient les données. Un nombre excessif de collisions peut réduire la bande passante disponible d'un segment de réseau jusqu'à 35 % ou 40 % de la bande passante disponible. 2



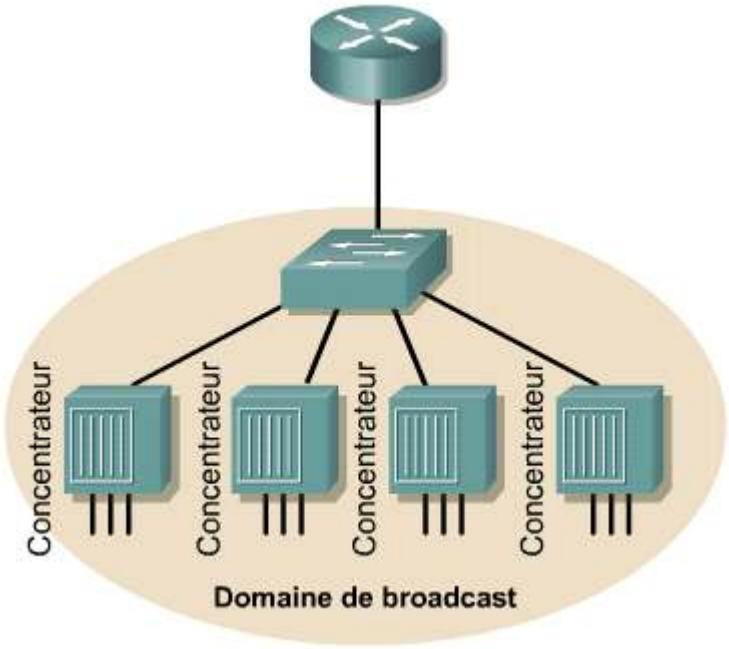
La segmentation consiste à diviser un domaine de collision en domaines de collision plus petits. 3La création de domaines de collision plus petits réduit le nombre de collisions sur un segment LAN, et permet d'utiliser plus largement la bande passante. Les équipements de couche 2 tels que les ponts et les commutateurs peuvent être utilisés pour segmenter un LAN en domaines de collision plus petits. C'est ce que peuvent faire les routeurs au niveau de la couche 3.



Le pontage et la commutation sont utilisés pour la segmentation :

- Il en résulte plusieurs domaines de collision.
- Il y a toujours un seul domaine de broadcast.
- Il est possible de réserver de la bande passante pour les stations de travail.

Un broadcast se produit lorsque l'adresse MAC (media access control) de destination de la trame de données est définie à FF-FF-FF-FF-FF-FF. Un domaine de broadcast désigne un ensemble d'unités qui reçoivent une trame de données de broadcast provenant de n'importe lequel des équipements faisant partie de cet ensemble. Tous les hôtes qui reçoivent une trame de broadcast doivent la traiter. Le traitement des données de broadcast consomme les ressources et la bande passante disponible de l'hôte. Les équipements de couche 2 tels que les ponts et les commutateurs réduisent la taille d'un domaine de collision. Ils ne réduisent pas la taille du domaine de broadcast. Parce qu'ils agissent à la couche 3, les routeurs réduisent la taille du domaine de collision et aussi celle du domaine de broadcast. 4



5.1 Conception LAN

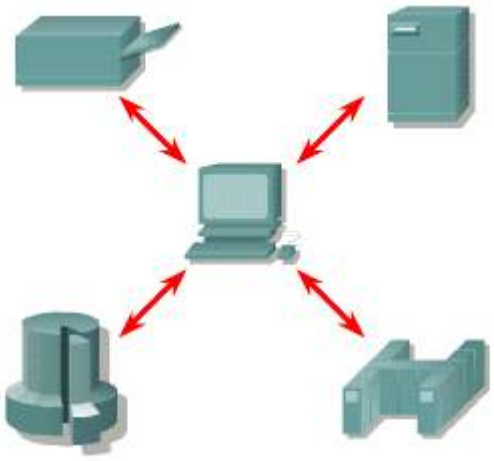
5.1.3 Méthodologie de conception de réseau LAN

Pour qu'un réseau local soit efficace et réponde aux besoins des utilisateurs, il doit être mis en œuvre en respectant une série d'étapes systématiquement planifiées. Ces étapes sont les suivantes:

- recueillir les impératifs et les attentes,
- analyser les besoins et les données,
- concevoir la structure LAN des couches 1, 2 et 3 (c'est-à-dire la topologie),
- créer des documents sur la mise en œuvre logique et physique du réseau.

Le processus de recueil de l'information permet de clarifier et d'identifier tout problème de réseau actuel. Ces informations comprennent l'historique et l'état en cours de l'organisation, la croissance prévue, les politiques d'exploitation et les

procédures de gestion, les procédures et les systèmes administratifs ainsi que les points de vue des futurs utilisateurs du réseau local. 1

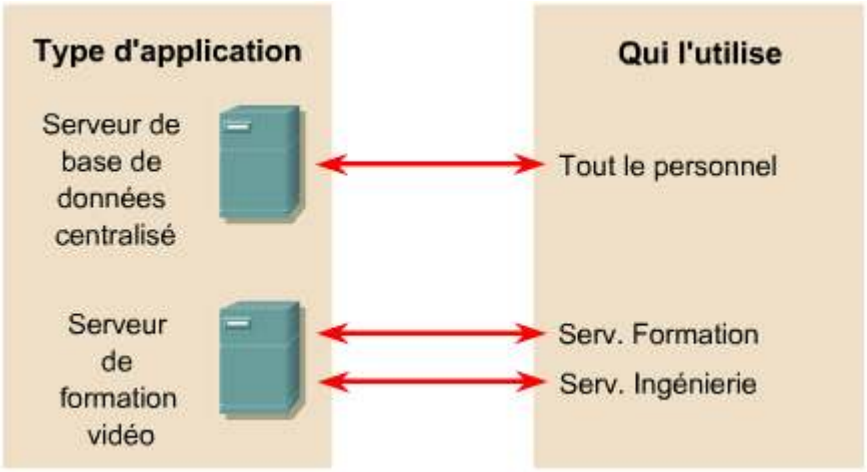


- Structure d'entreprise
- Flux d'informations commerciales
- Applications utilisées
- Topologie actuelle
- Caractéristiques du réseau actuel en matière de performance

Lors du recueil des informations, vous devez vous poser les questions suivantes:

- Qui seront les futurs utilisateurs du réseau local?
- Quel est leur niveau de compétence?
- Comment se comportent-ils vis-à-vis des ordinateurs et des applications informatiques?
- Quel est le stade de développement des règles organisationnelles documentées?
- Certaines données sont-elles d'une importance vitale?
- Certaines opérations sont-elles d'une importance vitale?
- Quels sont les protocoles autorisés sur le réseau?
- Certains types d'ordinateur de bureau sont-ils les seuls hôtes supportés par le réseau?
- Qui est responsable de l'adressage, de l'attribution de noms, de la conception de la topologie et de la configuration du réseau LAN?
- Quelles sont les ressources matérielles et logicielles ainsi que les ressources humaines?
- Quel est le lien entre ces ressources et de quelle façon sont-elles partagées?
- Quelles sont les ressources financières de l'organisation?

La constitution de documentation sur les exigences suivantes permet d'établir une estimation de coûts et des délais pour la mise en œuvre de la conception LAN projetée. Il est important de comprendre les problèmes de performance du réseau existant. 2



Un réseau n'est utile que dans la mesure où il est disponible. De nombreux éléments peuvent affecter la disponibilité, notamment les suivants:

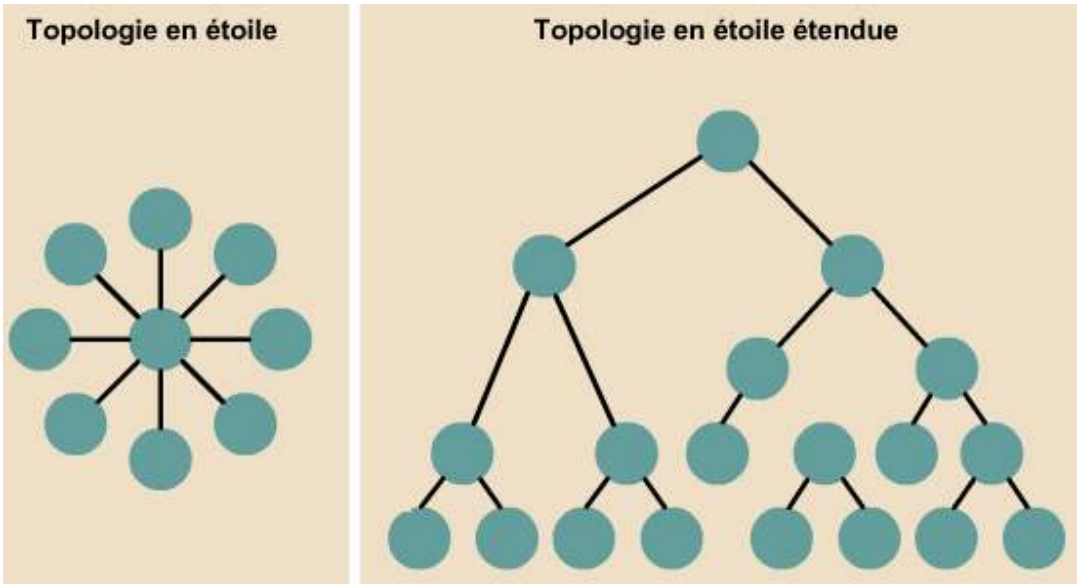
- le débit,
- le temps de réponse,
- l'accès aux ressources.

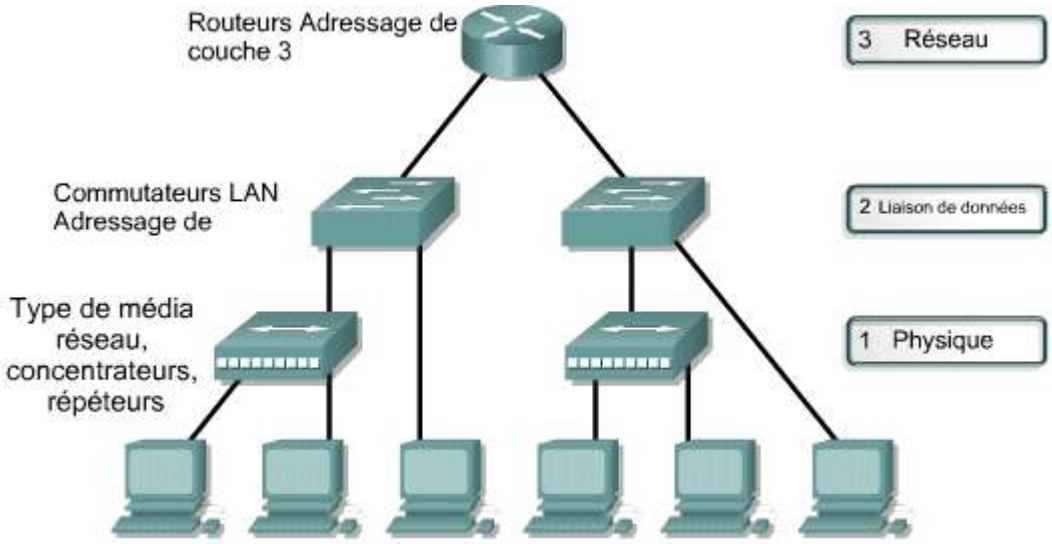
Chaque client a sa propre définition de la disponibilité. Par exemple, un client peut avoir des besoins spécifiques en matière de transmission de voix et de vidéo sur le réseau. Ces services peuvent nécessiter une bande passante beaucoup plus large que celle disponible sur le réseau ou le backbone. Il est possible d'ajouter des ressources pour augmenter la disponibilité, mais cela augmente alors le coût du réseau. La conception d'un réseau vise à fournir une disponibilité maximale au moindre coût.

L'étape suivante consiste à analyser les besoins du réseau et de ses utilisateurs. Les besoins des utilisateurs d'un réseau varient constamment. Par exemple, à mesure que le nombre d'applications vocales et vidéo augmente, la demande de bande passante s'accroît également.

L'évaluation des besoins de l'utilisateur constitue un autre élément de la phase d'analyse. Un réseau local incapable de fournir rapidement aux utilisateurs un accès à des informations précises ne sert à rien. Par conséquent, vous devez prendre les mesures nécessaires pour répondre aux besoins de l'organisation en matière d'accès aux informations.

L'étape suivante consiste à choisir une topologie LAN globale capable de répondre aux besoins des utilisateurs. 3 4



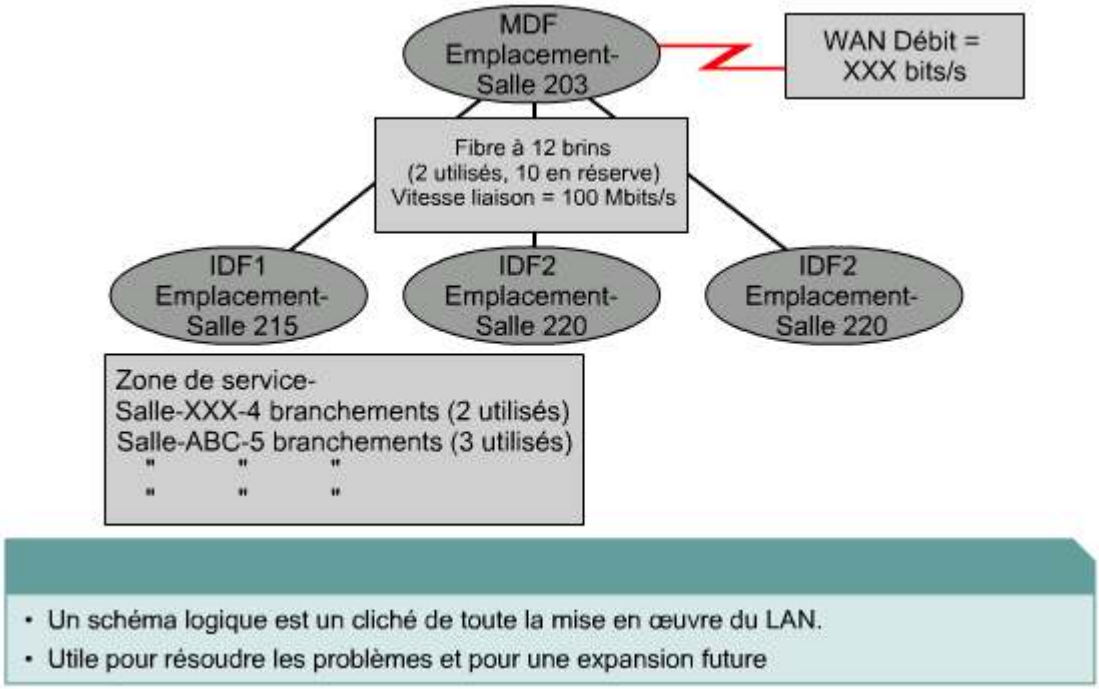


Ce cursus est axé sur la topologie en étoile et la topologie en étoile étendue. Ces topologies utilisent la technologie Ethernet 802.3 CSMA/CD. La topologie CSMA/CD en étoile est la configuration dominante dans l'industrie.

La conception d'une topologie LAN peut être divisée en trois catégories uniques du modèle de référence OSI:

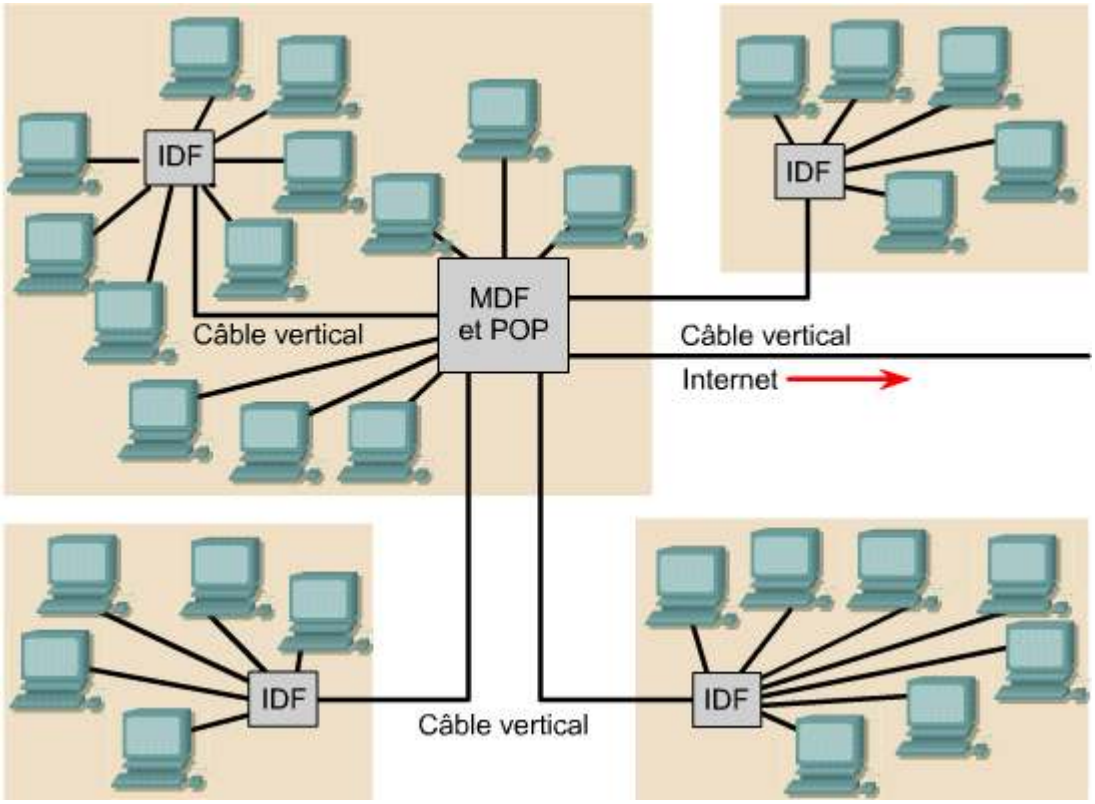
- la couche réseau,
- la couche liaison de données
- la couche physique.

L'étape suivante de la méthodologie de conception de réseau local consiste à constituer la documentation de la topologie physique et logique du réseau. La topologie physique du réseau se rapporte à la façon dont les divers composants LAN sont connectés ensemble. La conception logique du réseau fait référence au flux de données dans un réseau. Ce terme fait également référence aux systèmes d'attribution de noms et d'adressage utilisés dans la mise en œuvre de la solution de conception LAN. [5]



La documentation d'une conception LAN importante inclut les éléments suivants:

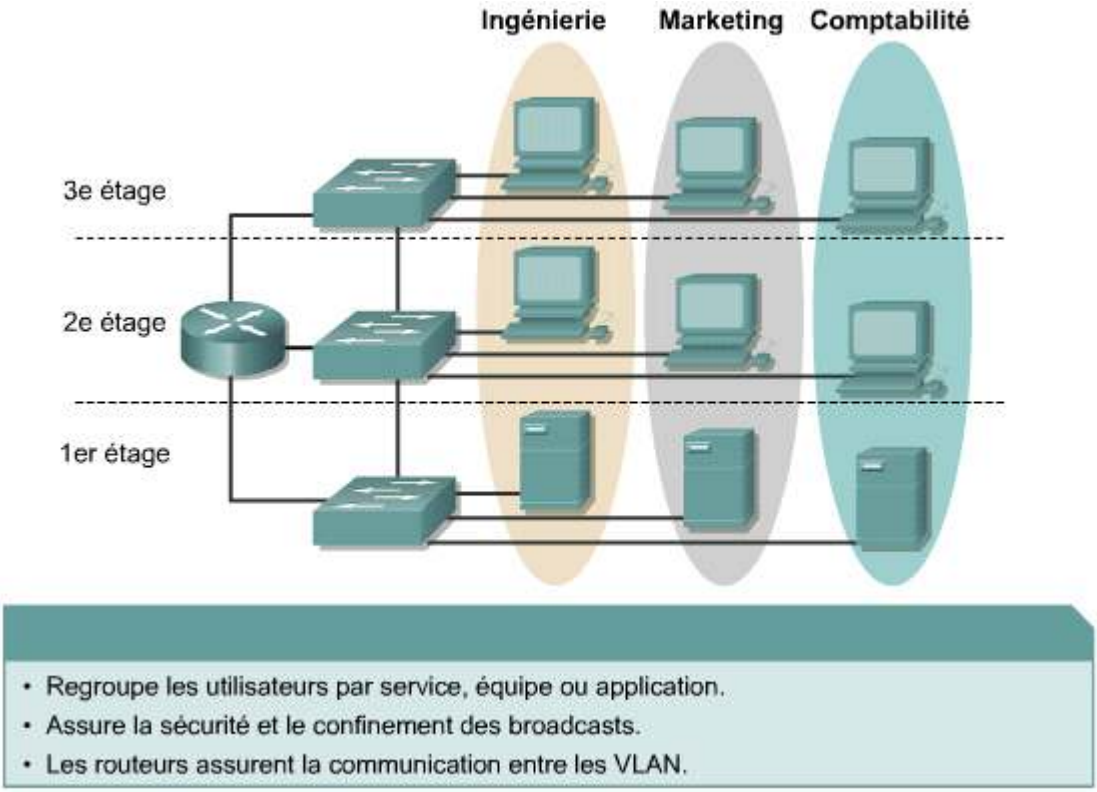
- la carte topologique de la couche OSI [6],



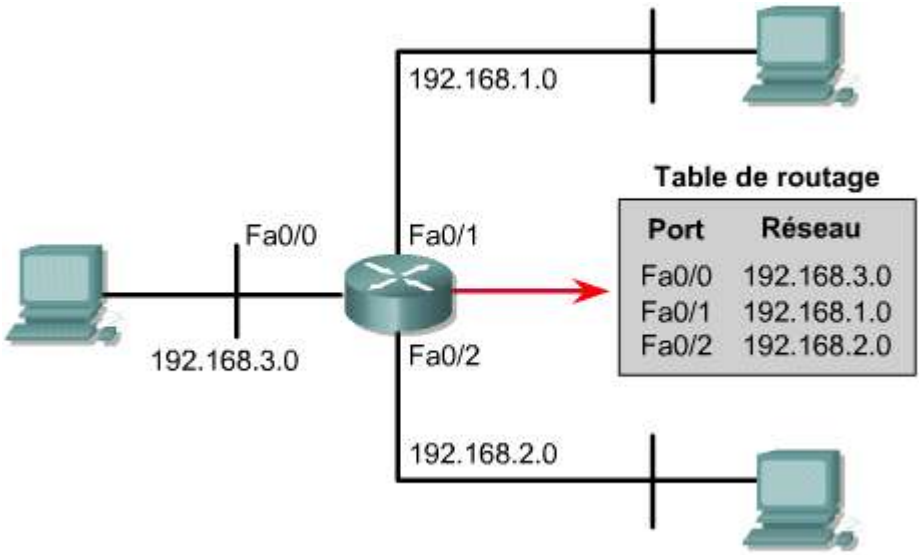
- la carte logique du réseau LAN,
- la carte physique du réseau LAN,
- les feuilles d'identification des câbles 7,

Connexion	ID câble	Interconnexion Raccord/Port	Type de câble	État
IDF1 à salle 203	203-1	HCC1/Port 13	UTP cat. 5	Utilisé
IDF1 à salle 203	203-2	HCC1/Port 14	UTP cat. 5	Non utilisé
IDF1 à salle 203	203-3	HCC2/Port 3	UTP cat. 5	Non utilisé
IDF1 à MDF	IDF1-1	VCC1/Port 1	Fibre multimode	Utilisé
IDF1 à MDF	IDF1-2	VCC1/Port 2	Fibre multimode	Utilisé

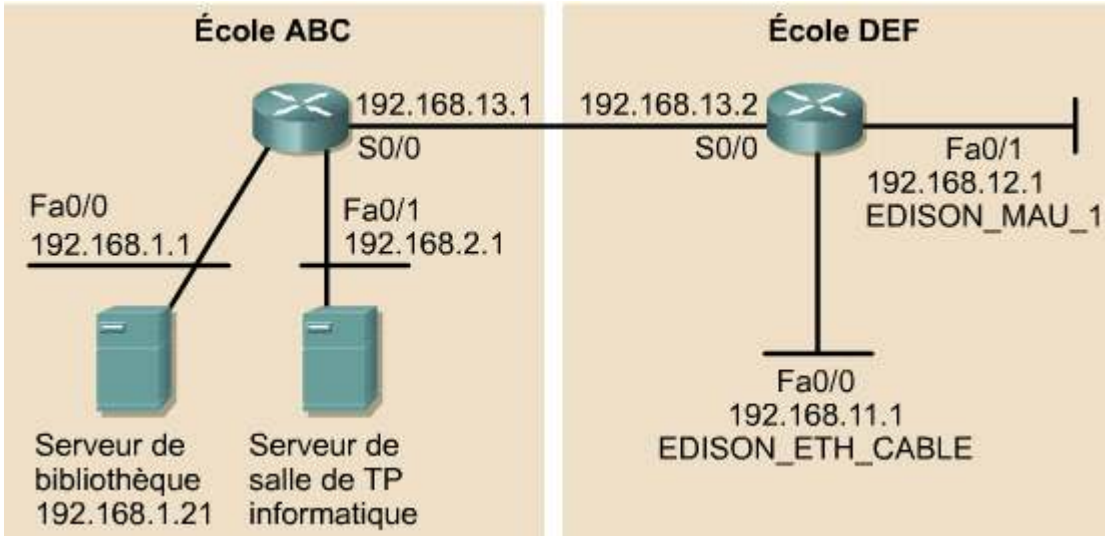
- la carte logique du VLAN 8,



- la carte logique de la couche 3 9,



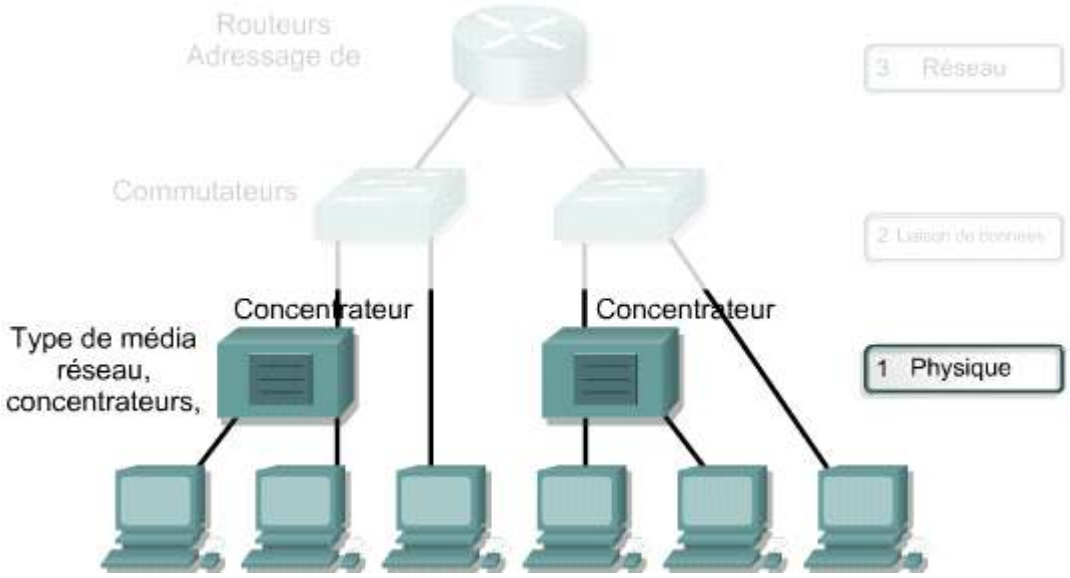
- les cartes d'adressage 10



5.1 Conception LAN

5.1.4 Conception de la couche 1

Le câblage physique est l'un des éléments les plus importants à prendre en considération lors de la conception d'un réseau. [1]



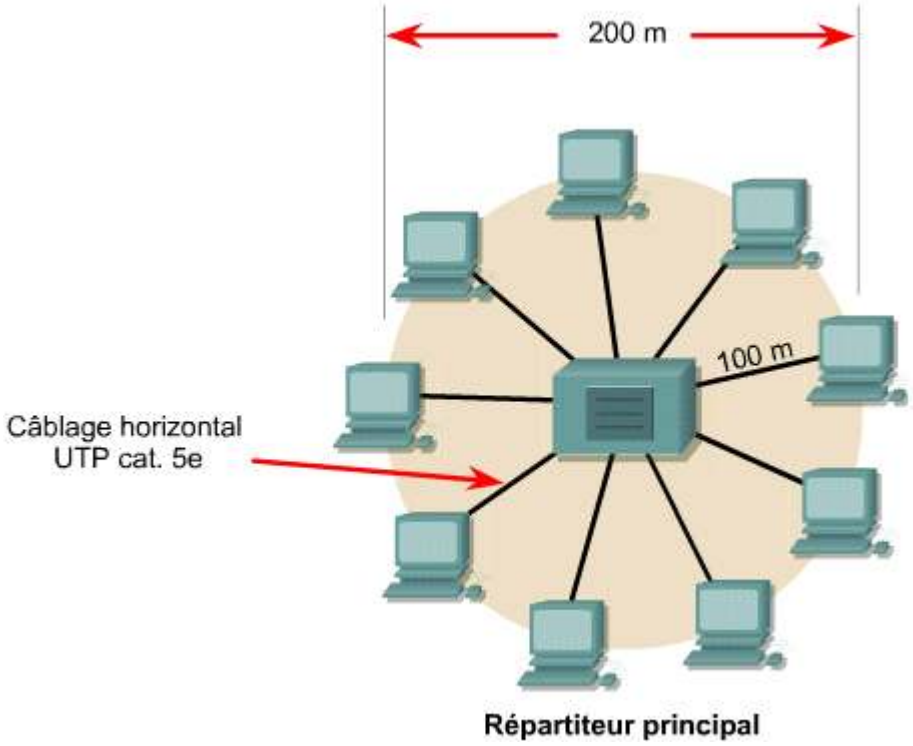
Aujourd'hui, le câblage de la plupart des réseaux LAN est basé sur la technologie Fast Ethernet. Fast Ethernet est une évolution d'Ethernet passant de 10 Mbits/s à 100 Mbits/s et capable d'utiliser la fonction full-duplex. Fast Ethernet utilise la topologie Ethernet 10BaseT en bus logique orienté broadcast, avec la méthode CSMA/CD pour l'adressage MAC.

Les questions relatives à la conception au niveau de la couche 1 comprennent le type de câble à utiliser (généralement, des câbles de cuivre ou à fibre optique) ainsi que la structure globale du câblage. [2]

	Débit de données	Méthode de signalisation	Type de média	Longueur maximale
10BaseT	10 Mbits/s	Bande de base	UTP cat. 5e	100 m
10BaseFL	10 Mbits/s	Bande de base	Fibre optique	2000 m
100BaseTX	100Mbits/s	Bande de base	UTP cat. 5e	100 m
100BaseFX	100 Mbits/s	Bande de base	Fibre multimode (deux brins)	2000 m

Les médias de câblage de couche 1 incluent des câbles à paires torsadées non blindées (UTP) ou blindées (STP) 10/100BASE-TX de catégorie 5, 5e ou 6 et des câbles à fibre optique 100BaseFX, avec la norme TIA/EIA-568-B pour la disposition et la connexion des méthodes de câblage.

Vous devez évaluer avec soin les points forts et les faiblesses des diverses topologies. L'efficacité d'un réseau est en effet directement liée au câblage sous-jacent. 3

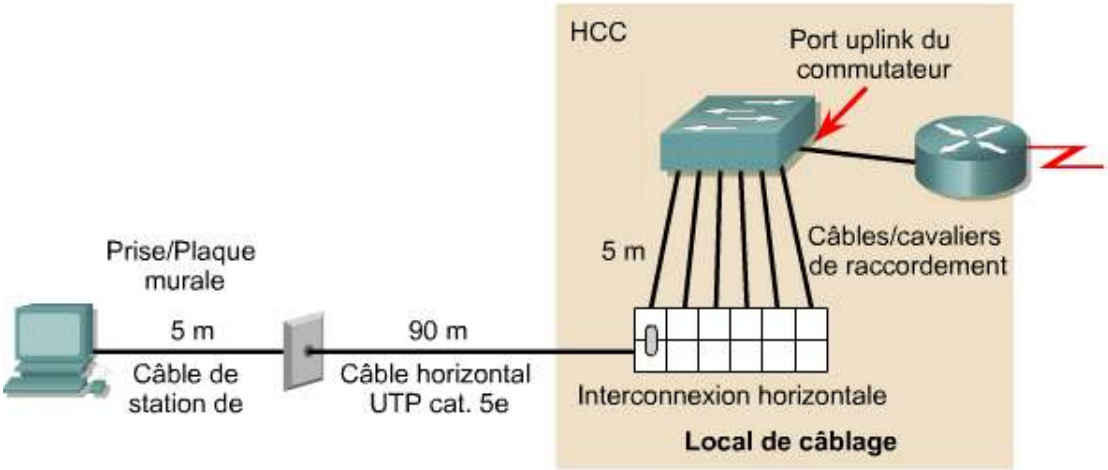


La plupart des problèmes qui se produisent sur un réseau proviennent de la couche 1. Si vous prévoyez d'apporter des modifications importantes à un réseau, il est essentiel d'effectuer une vérification complète des câbles pour identifier les zones qui nécessitent une mise à niveau ou une réinstallation.

Vous devez utiliser des câbles à fibre optique dans le réseau de backbone et le câblage vertical. Des câbles à paires torsadées non blindées de catégorie 5e doivent être utilisés pour le câblage horizontal. La mise à niveau du câblage doit être prioritaire sur tout autre changement. Les entreprises doivent également s'assurer que ces systèmes sont conformes aux normes de l'industrie, telles que la norme TIA/EIA-568-B.

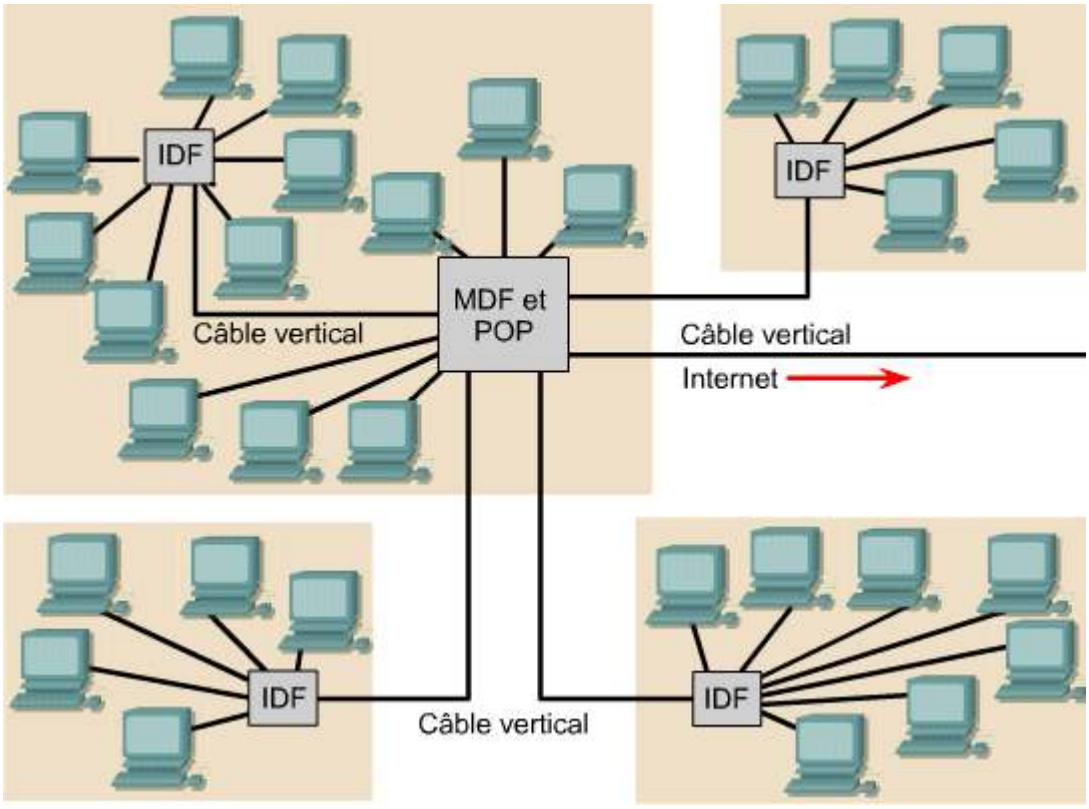
Cette norme stipule que chaque équipement connecté au réseau doit être relié à un emplacement central par des câbles horizontaux. Cela s'applique si tous les hôtes qui doivent accéder au réseau se trouvent à une distance inférieure ou égale à 100 mètres pour le câble à paires torsadées non blindées Ethernet de catégorie 5.

Dans une topologie en étoile simple comportant un seul local technique, le répartiteur principal MDF comprend un ou plusieurs tableaux d'interconnexions horizontales (horizontal cross-connect ou HCC). 4

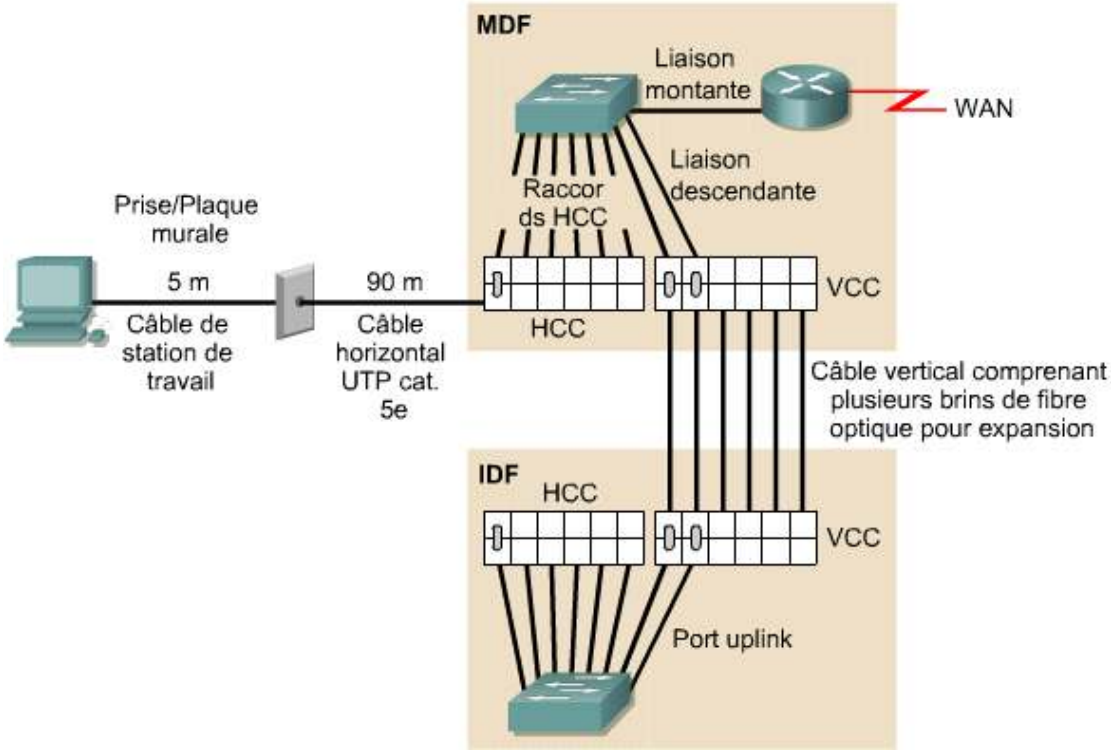


Les câbles d'interconnexion horizontale servent à relier le câblage horizontal de la couche 1 aux ports du commutateur LAN de la couche 2. Selon le modèle, le port « uplink » du commutateur LAN est connecté au port Ethernet du routeur de la couche 3 via un câble de raccordement. À ce stade, l'hôte d'extrémité est doté d'une connexion physique complète au port du routeur.

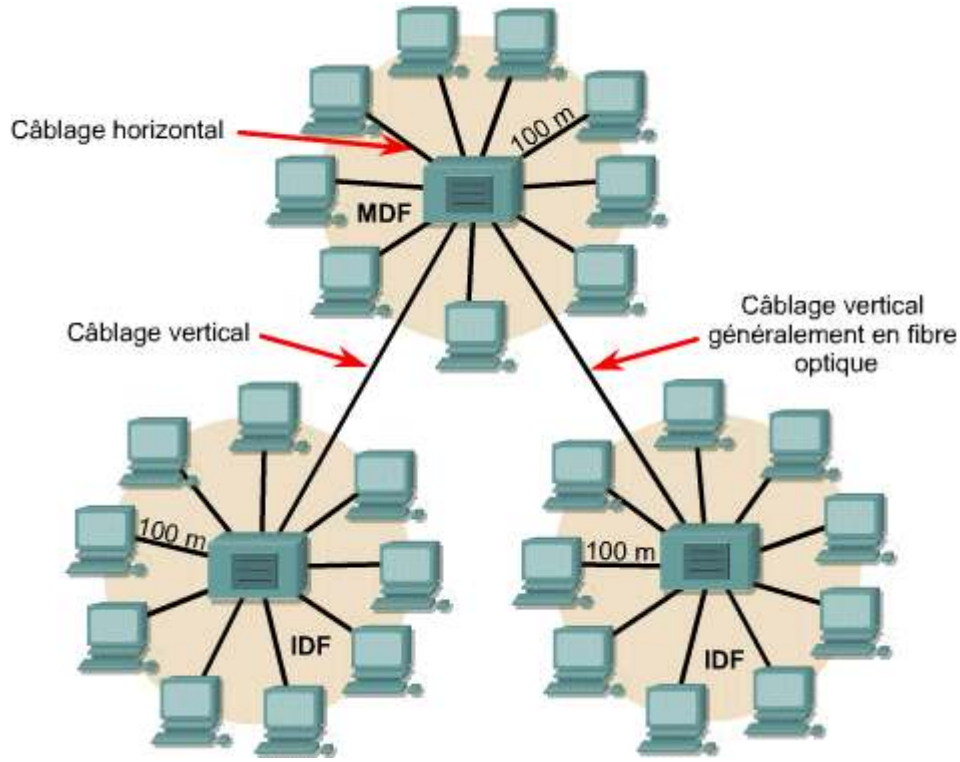
Lorsque des hôtes de grands réseaux dépassent la limite des 100 mètres fixée pour le câble à paires torsadées non blindées de catégorie 5e, plusieurs locaux techniques sont nécessaires. La création de plusieurs locaux techniques entraîne la création de plusieurs zones d'interconnexion de réseaux. Les locaux techniques secondaires sont appelés des répartiteurs intermédiaires (IDF). 5



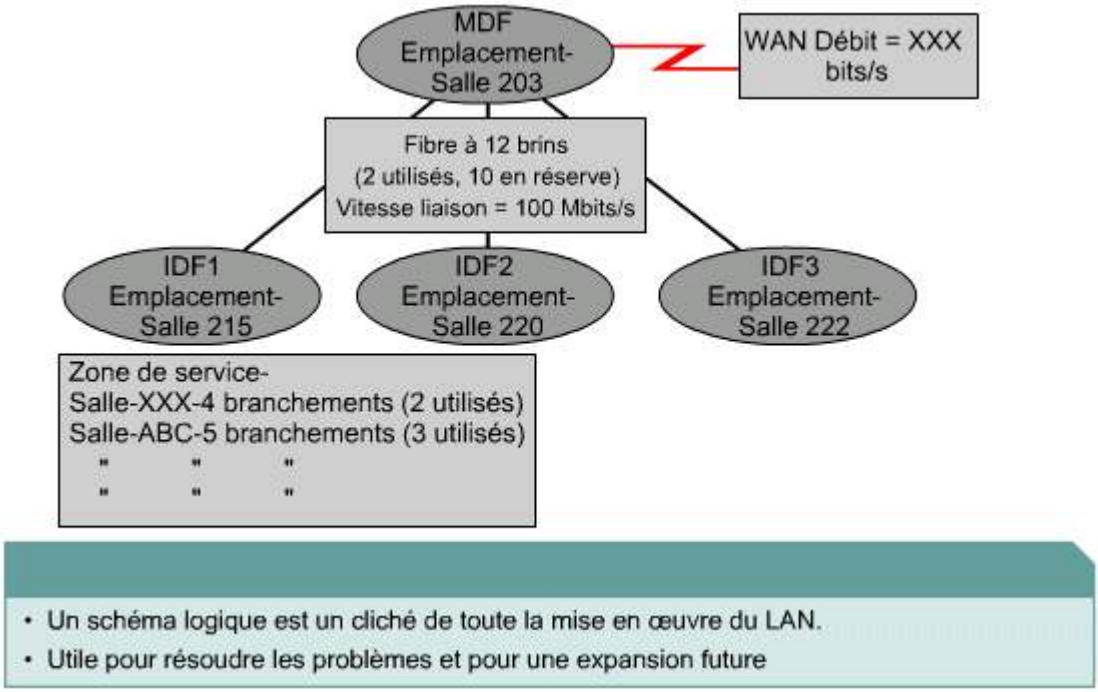
Les normes TIA/EIA568-B précisent que les répartiteurs intermédiaires IDF doivent être connectés au répartiteur principal MDF par le biais d'un câblage vertical appelé câblage de backbone. 6



Une interconnexion verticale (vertical cross-connect ou VCC) permet d'interconnecter les divers répartiteurs intermédiaires IDF au répartiteur principal MDF. Un câblage en fibre optique est généralement utilisé car les câbles verticaux dépassent souvent la limite des 100 mètres imposée pour les câbles à paires torsadées non blindées de catégorie 5e.



Le schéma logique représente le modèle de la topologie du réseau sans les détails relatifs au parcours d'installation précis des câbles. Le schéma logique est le plan de base du réseau local, qui inclut les éléments suivants:



- L'emplacement exact et l'identification des locaux techniques du répartiteur principal MDF et des répartiteurs intermédiaires IDF.
- Le type et le nombre de câbles utilisés pour interconnecter le répartiteur principal MDF et les répartiteurs intermédiaires IDF.
- Le nombre de câbles de réserve disponibles pour accroître la bande passante entre les locaux techniques. Par exemple, si le câblage vertical entre le répartiteur intermédiaire 1 et le répartiteur principal est utilisé à 80 %, vous pouvez ajouter deux paires supplémentaires pour doubler la capacité.

- Une documentation détaillée de tous les parcours de câbles, les numéros d'identification et le port de l'interconnexion horizontale ou verticale auquel aboutissent les câbles. 9

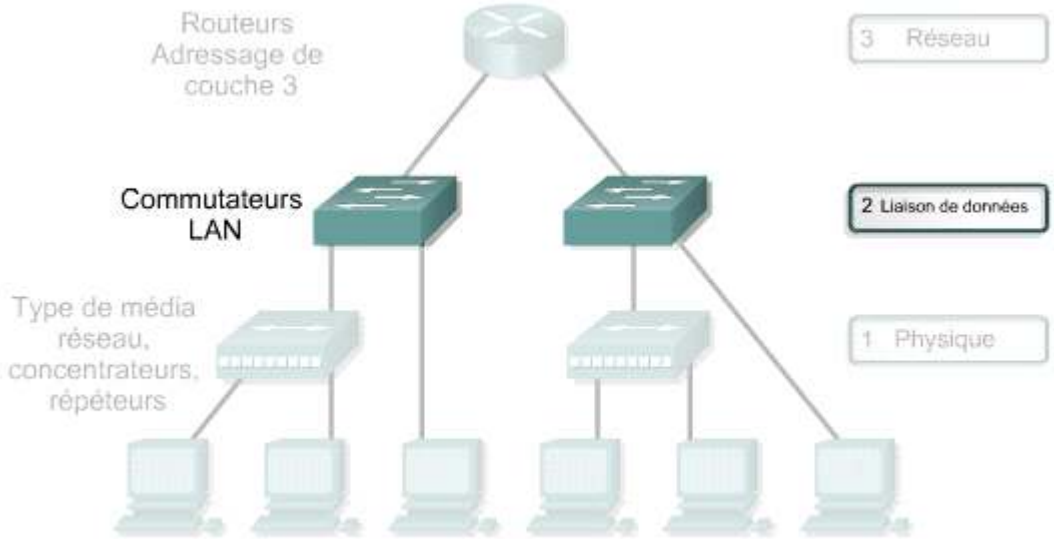
Connexion	ID câble	Interconnexion Raccord/Port	Type de câble	État
IDF1 à salle 203	203-1	HCC1/Port 13	UTP cat. 5e	Utilisé
IDF1 à salle 203	203-2	HCC1/Port 14	UTP cat. 5e	Non utilisé
IDF1 à salle 203	203-3	HCC2/Port 3	UTP cat. 5e	Non utilisé
IDF1 à MDF	IDF1-1	VCC1/Port 1	Fibre multimode	Utilisé
IDF1 à MDF	IDF1-2	VCC1/Port 2	Fibre multimode	Utilisé

Le schéma logique est essentiel pour le dépannage des problèmes de connectivité réseau. Si par exemple la salle 203 perd sa connectivité au réseau, en examinant la feuille d'identification des câbles, vous pouvez constater que la salle 203 est reliée au câble 203-1 qui aboutit au port 13 de l'interconnexion horizontale 1. Vous pouvez tester cette section de câble à l'aide d'un testeur de câble pour savoir s'il s'agit d'une défaillance de la couche 1. Si tel est le cas, vous pouvez utiliser l'un des deux autres parcours de câble pour rétablir la connectivité et avoir le temps de dépanner le câble 203-1.

5.1 Conception LAN

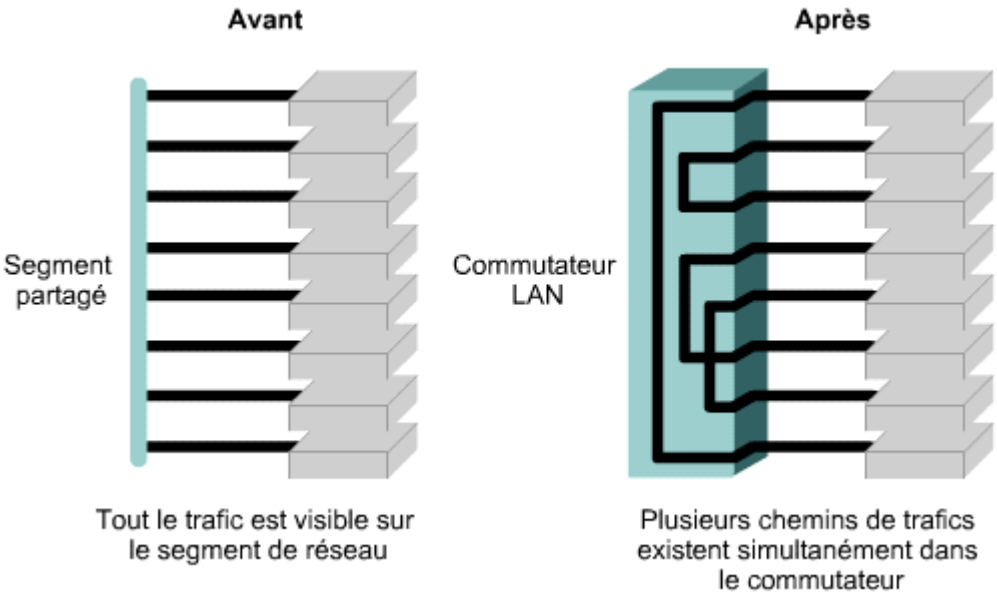
5.1.5 Conception de la couche 2

Les objectifs des unités de couche 2 dans le réseau sont de commuter des trames à l'aide des adresses MAC de destination, de permettre la détection d'erreurs et de réduire la congestion dans le réseau. 1



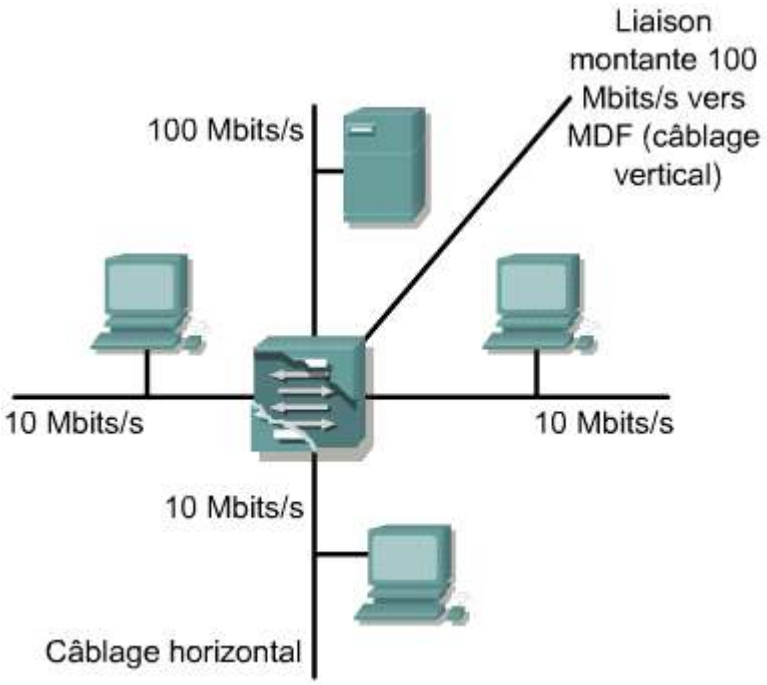
Les ponts et les commutateurs de réseau LAN sont les deux principales unités réseau de couche 2. Les unités réseau de couche 2 déterminent la dimension des domaines de collision.

Les collisions et la taille du domaine de collision sont deux facteurs qui nuisent aux performances d'un réseau. 2



La micro-segmentation du réseau réduit la taille des domaines de collision et réduit les collisions. Elle est mise en œuvre par l'utilisation de ponts et de commutateurs. L'objectif est d'augmenter les performances d'un groupe de travail ou d'un backbone. Vous pouvez utiliser des commutateurs avec des concentrateurs pour fournir aux utilisateurs et aux serveurs le niveau de performances approprié.

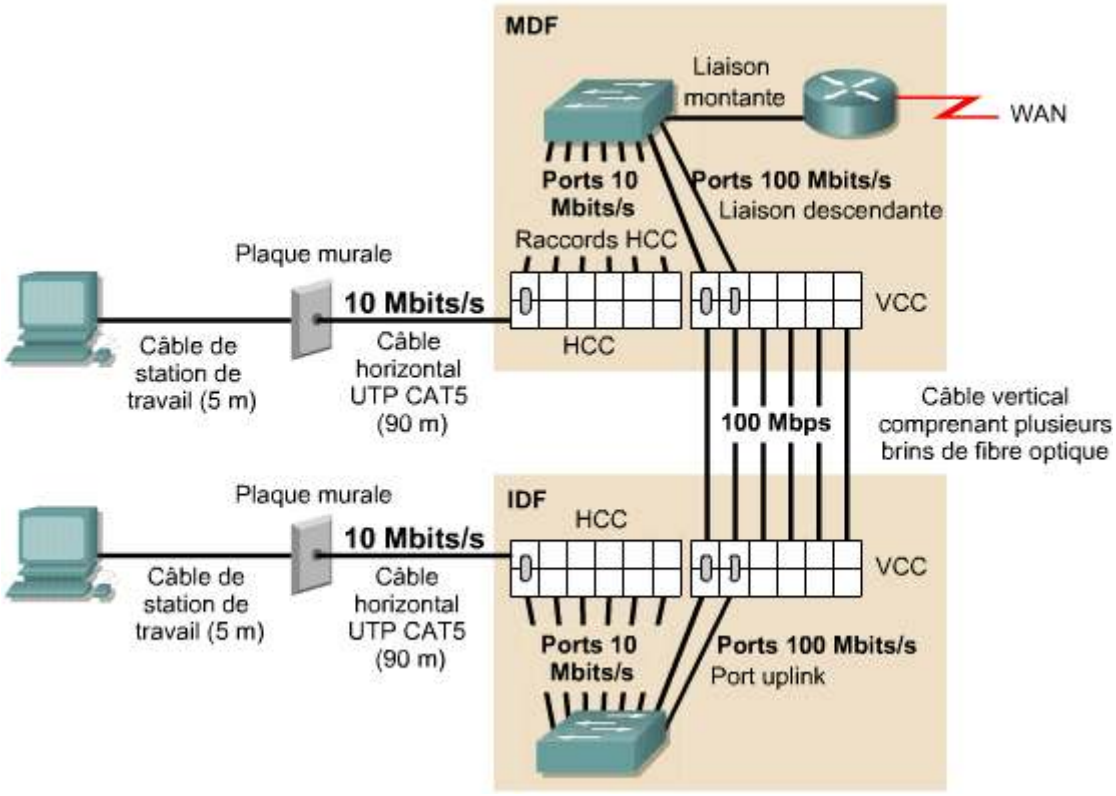
Grâce à une autre caractéristique importante, un commutateur LAN peut attribuer la bande passante par port, ce qui laisse davantage de bande passante aux câbles verticaux, aux liaisons montantes (uplinks) et aux serveurs. 3



Ce type de commutation est appelé commutation asymétrique. La commutation asymétrique permet des connexions commutées entre des ports de différentes bande passante comme la combinaison de ports à 10-Mbits/s et 100-Mbits/s. La commutation symétrique permet la connexion entre des ports de même bande passante.

La capacité souhaitée d'un câble vertical est supérieure à celle d'un câble horizontal. Si vous installez un commutateur LAN au niveau du répartiteur principal MDF et du répartiteur intermédiaire IDF, le câble vertical acheminera tout le trafic de

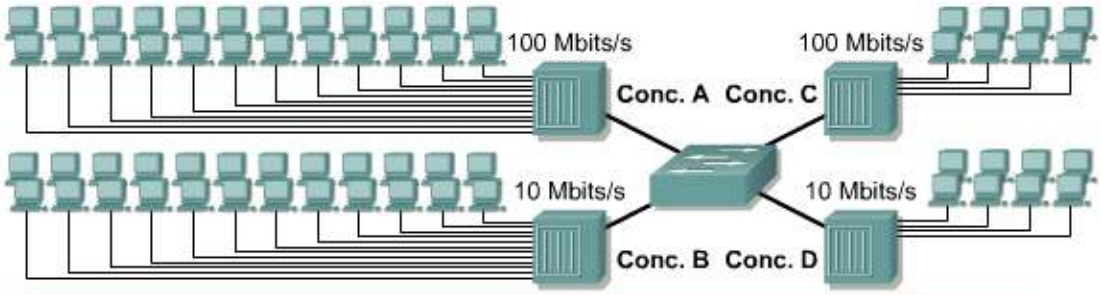
données entre le répartiteur principal et le répartiteur intermédiaire. 4



Les câbles horizontaux entre le répartiteur intermédiaire et les stations de travail sont constitués de paires torsadées non blindées de catégorie 5e. Aucun branchement de câble ne doit dépasser 100 mètres de longueur. Dans un environnement normal, un débit de 10 Mbits/s convient pour le câble de branchement horizontal. Utilisez des commutateurs LAN asymétriques pour combiner des ports à 10 Mbits/s et à 100 Mbits/s sur un même commutateur.

L'étape suivante consiste à déterminer le nombre de ports à 10 Mbits/s et à 100 Mbits/s nécessaires pour le répartiteur principal MDF et pour chacun des répartiteurs intermédiaires IDF. Vous pouvez déterminer ce nombre en examinant les besoins des utilisateurs en ce qui concerne le nombre de câbles de branchement horizontaux par salle dans chaque zone d'interconnexion de réseaux. Cela inclut le nombre de câbles verticaux. Par exemple, supposons que les besoins des utilisateurs spécifient l'installation de quatre câbles horizontaux dans chaque salle. Le répartiteur intermédiaire IDF desservant la zone d'interconnexion de réseaux couvre 18 salles. Par conséquent, quatre câbles de branchement dans chacune des 18 salles équivalent à 72 ports du commutateur LAN. (4 x 18 = 72)

Pour déterminer la taille d'un domaine de collision, vous devez déterminer le nombre d'hôtes physiquement connectés à un port du commutateur. Cela affecte également la disponibilité de la bande passante pour les hôtes. Idéalement, un seul hôte doit être connecté à un port de commutateur LAN. Le domaine de collision comprendrait alors uniquement l'hôte source et l'hôte de destination. La taille du domaine de collision serait de deux. En raison de la petite taille de ce domaine de collision, il n'y aurait pratiquement aucune collision lorsque deux hôtes communiqueraient entre eux. L'autre méthode permettant de mettre en œuvre une commutation LAN consiste à installer des concentrateurs LAN partagés sur les ports du commutateur et de connecter plusieurs hôtes à un seul port du commutateur. 5



Concentrateur A:
- Domaine de collision = 24 hôtes
- Bande passante moyenne = 100 Mbits/s/24 hôtes = 4,167 Mbits/s par hôte

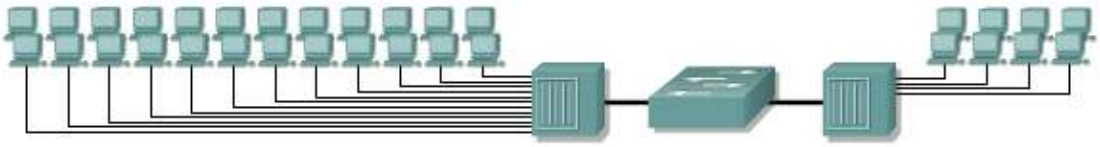
Concentrateur B:
- Domaine de collision = 24 hôtes
- Bande passante moyenne = 10 Mbits/s/24 hôtes = 0,4167 Mbits/s par hôte

Concentrateur C:
- Domaine de collision = 8 hôtes
- Bande passante moyenne = 100 Mbits/s/8 hôtes = 12,5 Mbits/s par hôte

Concentrateur D:
- Domaine de collision = 8 hôtes
- Bande passante moyenne = 10 Mbits/s/8 hôtes = 1,25 Mbits/s par hôte

Tous les hôtes connectés au concentrateur LAN partagé partagent le même domaine de collision et la même bande passante. Les collisions se produiraient plus fréquemment.

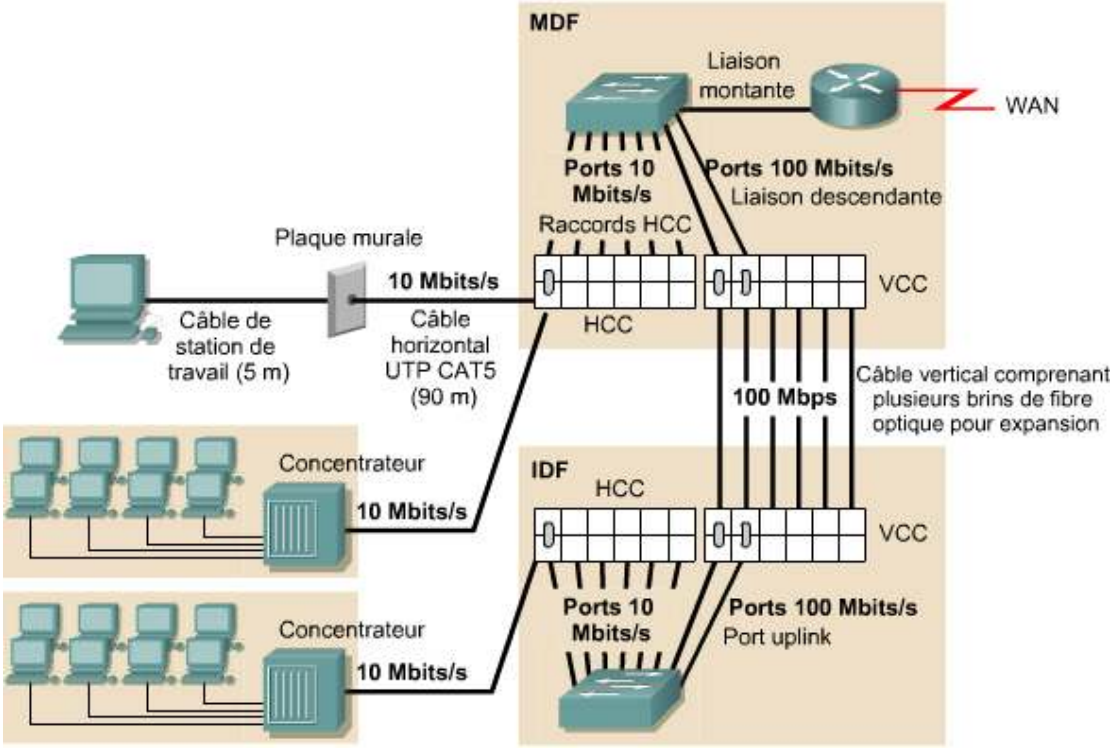
LAN commuté



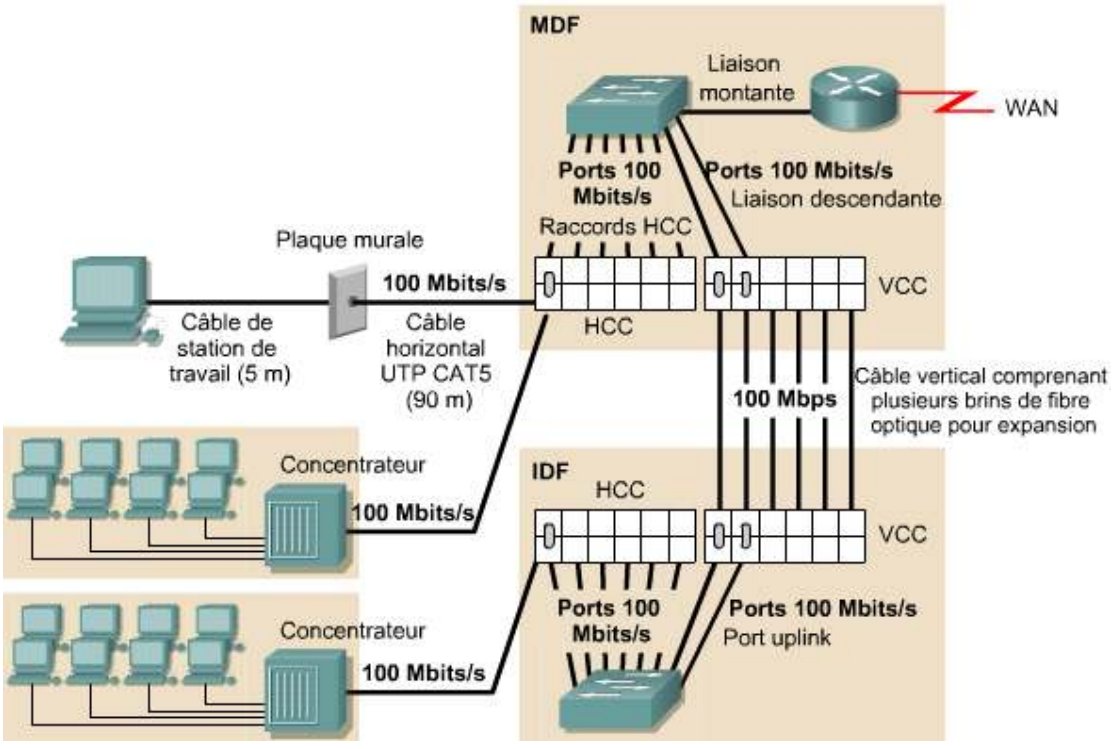
LAN avec concentrateurs

- Dans un LAN purement commuté, la taille du domaine de collision est de 2 hôtes.
- Avec des concentrateurs, la taille du domaine de collision augmente et la bande passante est partagée.

Les concentrateurs à média partagé sont généralement utilisés dans un environnement de commutateurs LAN pour créer davantage de points de connexion à l'extrémité des câbles horizontaux. 7



C'est une solution acceptable, mais vous devez toutefois faire attention. La taille des domaines de collision ne doit pas augmenter et les besoins des hôtes en matière de bande passante doivent être respectés conformément aux spécifications définies à l'étape d'estimation des besoins du processus de conception du réseau. 8

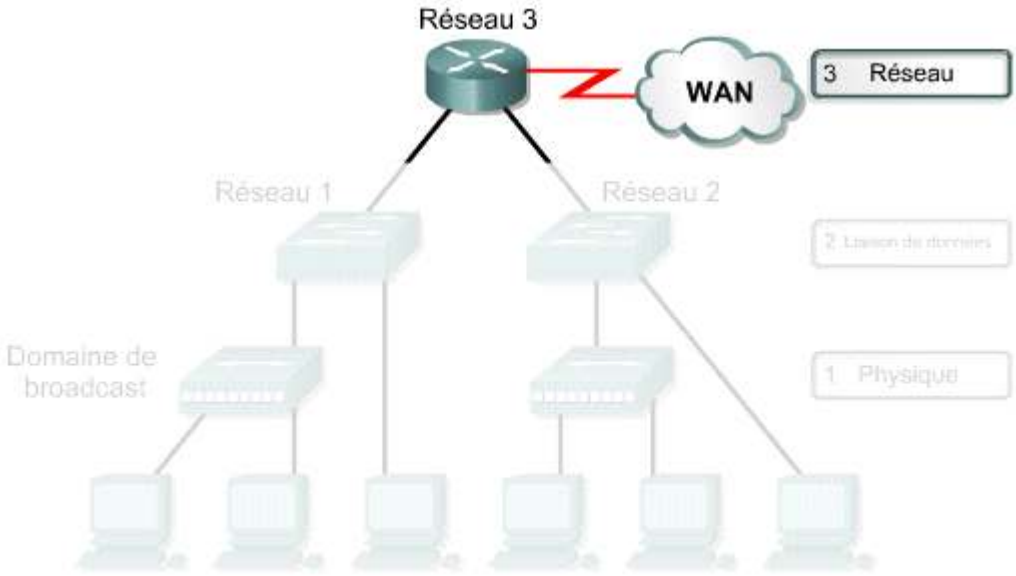


5.1 Conception LAN

5.1.6 Conception de la couche 3

Un routeur est un équipement de couche 3. Il est considéré comme l'un des équipements les plus puissants d'une topologie de réseau.

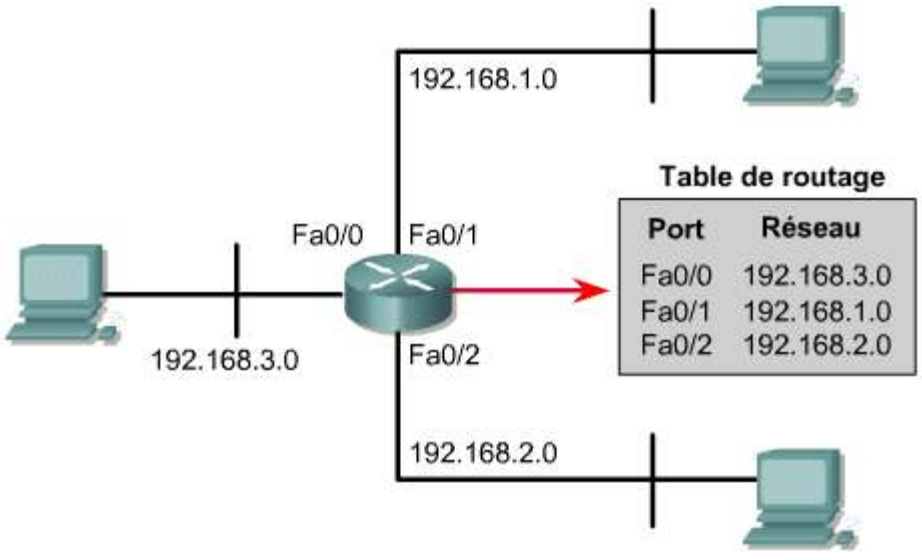
Les équipements de couche 3 peuvent être utilisés pour créer des segments LAN distincts. Ils permettent la communication entre les segments sur la base de l'adressage de couche 3, tel que l'adressage IP. La mise en œuvre des équipements de couche 3 permet de segmenter le réseau local en réseaux physiques et logiques uniques. Les routeurs fournissent également la connectivité aux réseaux WAN tels qu'Internet. 1



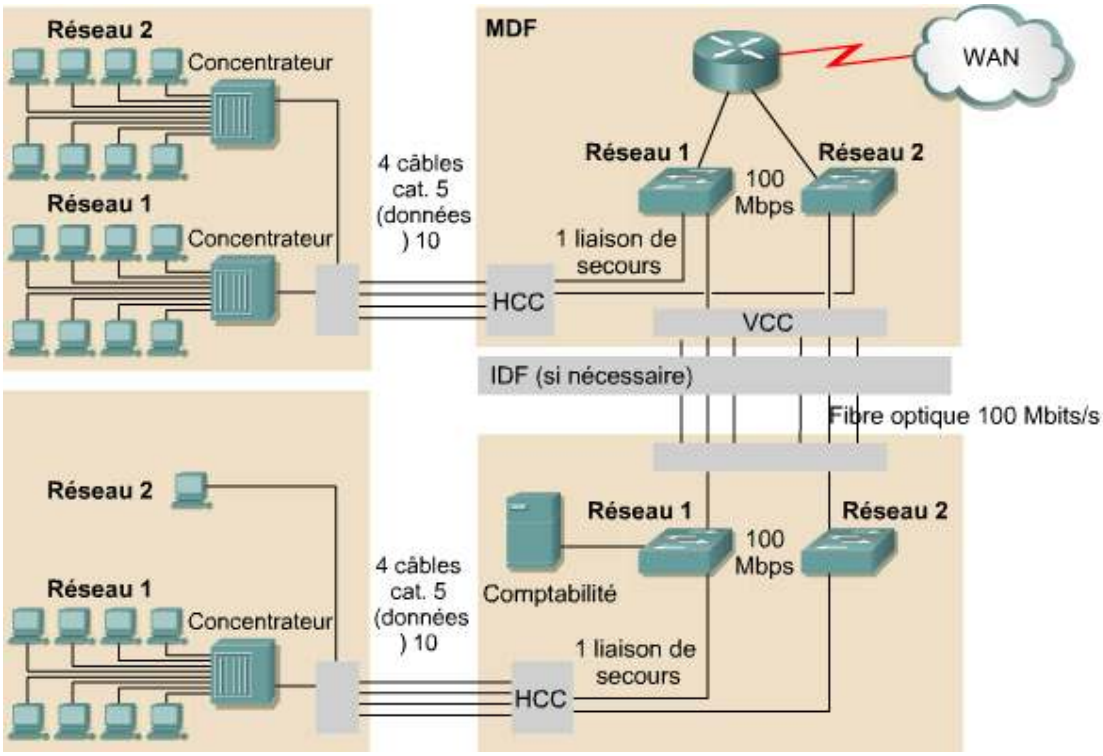
Les routeurs sont utilisés comme pare-feu contre les broadcasts.

Le routage de couche 3 détermine le flux du trafic entre des segments physiques bien distincts du réseau en fonction de l'adressage de couche 3. Un routeur achemine des paquets de données en se basant sur les adresses de destination. Il ne transmet pas les messages de broadcast LAN tels que les requêtes ARP. Par conséquent, l'interface du routeur est considérée comme le point d'entrée et de sortie d'un domaine de broadcast; elle empêche les messages de broadcast d'atteindre d'autres segments LAN.

Les routeurs fournissent une évolutivité au réseau parce qu'ils servent de pare-feu vis-à-vis des broadcasts. Ils peuvent également favoriser l'évolutivité en divisant les réseaux en sous-réseaux, sur la base des adresses de couche 3. 2



Lorsque vous devez prendre la décision d'utiliser des routeurs ou des commutateurs, posez-vous toujours la question: «Quel est le problème à résoudre?». Si le problème est lié au protocole plutôt qu'aux collisions, choisissez les routeurs. Les routeurs résolvent les problèmes liés au nombre excessif de broadcasts, aux protocoles qui n'évoluent pas correctement, à la sécurité et à l'adressage de la couche réseau. Toutefois, ils sont plus coûteux et plus difficiles à configurer que les commutateurs.

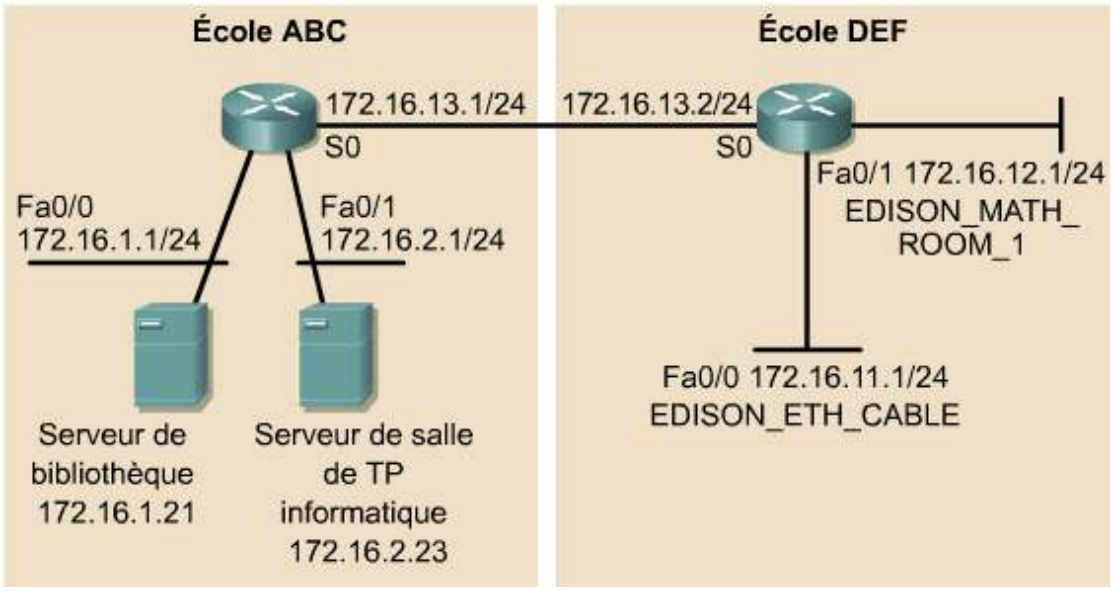


La figure 3 illustre un exemple de mise en œuvre comportant plusieurs réseaux physiques. Tout le trafic de données du réseau 1 à destination du réseau 2 doit passer par le routeur. Cette mise en œuvre comprend deux domaines de broadcast : les deux réseaux comportent des systèmes distincts d'adressage IP de réseau/sous-réseau de couche 3. Dans un modèle de câblage structuré de couche 1, il est facile de créer plusieurs réseaux physiques en reliant les câblages horizontal et vertical au commutateur approprié de couche 2. Cela à l'aide de câbles de raccordement. Cette mise en œuvre assure un haut niveau de sécurité, car l'ensemble du trafic entrant et sortant du réseau LAN doit passer par le routeur.

Une fois qu'un modèle d'adressage IP a été développé pour un client, il doit faire l'objet d'une documentation claire et précise. Une convention standard doit être définie pour l'adressage des hôtes importants du réseau. 4

Adresse logique	Unités du réseau physique
x.x.x.1-x.x.x.10	Ports de routeur, LAN et WAN
x.x.x.11-x.x.x.20	Commutateurs LAN
x.x.x.21-x.x.x.30	Serveurs d'entreprise
x.x.x.31-x.x.x.80	Serveurs de groupe de travail
x.x.x.81-x.x.x.254	Hôtes

Ce système d'adressage doit être cohérent pour l'ensemble du réseau. Les cartes d'adressage fournissent un cliché du réseau. 5 6



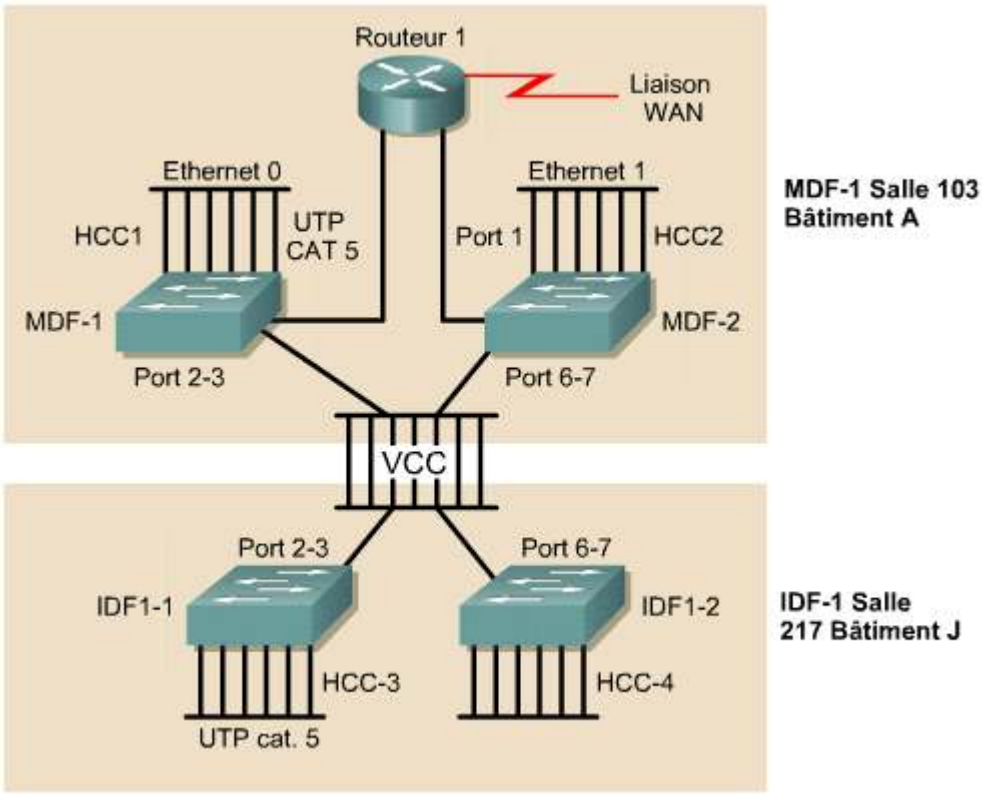
Adresse IP réseau 172.16.0.0

Masque de sous-réseau = 255.255.255.0

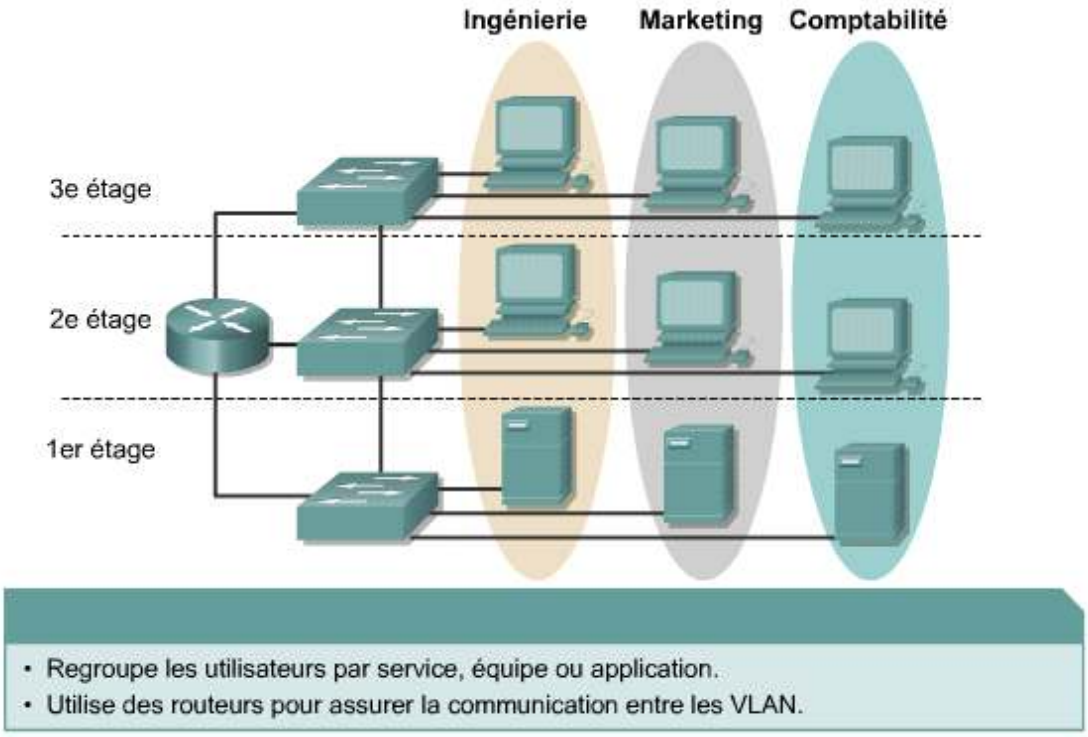
Rectorat XYZ

École ABC	École DEF
172.16.1.0 à 172.16.10.0	172.16.11.0 à 172.16.21.0
Masque de sous-réseau = 255.255.255.0	Masque de sous-réseau = 255.255.255.0
Nom du routeur = Routeur ABC	Nom du routeur = Routeur DEF
Fa0/0 = 172.16.1.1	Fa0/0 = 172.16.11.1
Fa0/1 = 172.16.2.1	Fa0/1 = 172.16.12.1

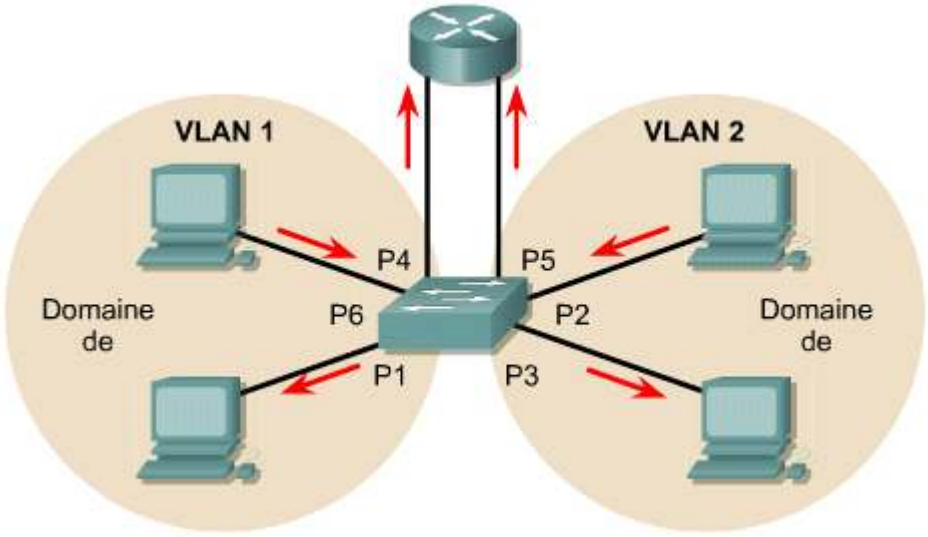
La création de cartes physiques vous aide à dépanner le réseau.



La mise en œuvre de VLAN (Virtual Local Area Network), c'est-à-dire de réseau local virtuel, combine la commutation de couche 2 et les technologies de routage de couche 3 pour limiter à la fois les domaines de collision et les domaines de broadcast. Les VLAN permettent également de sécuriser le réseau en créant des groupes de VLAN selon leur fonction et en utilisant des routeurs pour communiquer entre eux. 8



Une association à un port physique est utilisée pour mettre en œuvre l'attribution de VLAN. Les ports P0, P4 et P6 sont attribués au VLAN 1, tandis que les ports P2, P3 et P5 le sont au VLAN 2. Les réseaux VLAN 1 et VLAN 2 ne communiquent que par le biais du routeur. Cela limite la taille des domaines de broadcast et le routeur est utilisé pour déterminer si le réseau VLAN 1 peut communiquer avec le réseau VLAN 2. 9



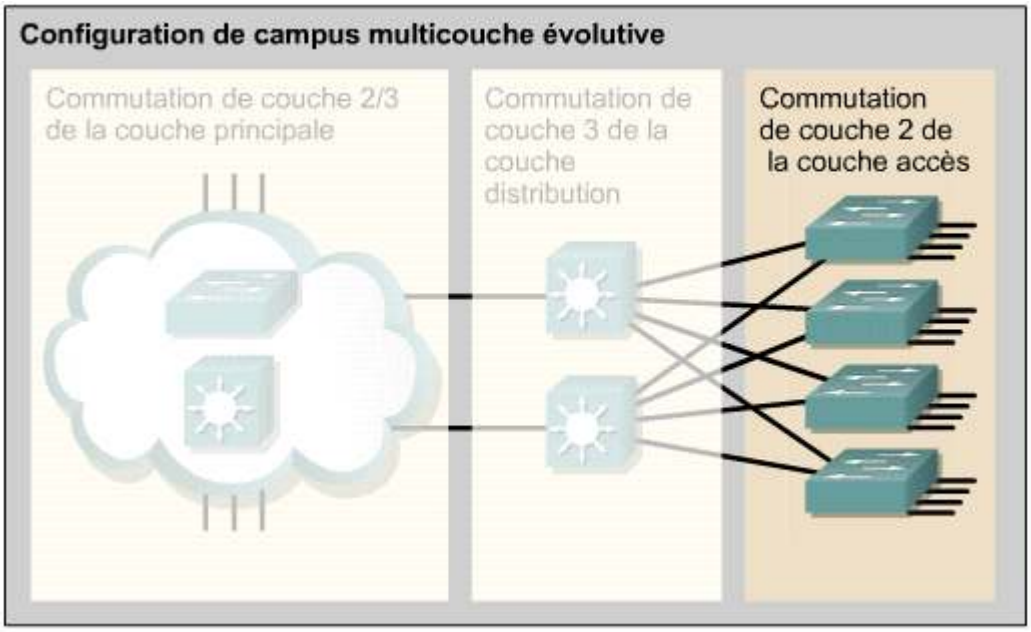
5.2 Commutateurs LAN

5.2.1 LAN commutés, vue d'ensemble de la couche accès

La construction d'un LAN capable de satisfaire les besoins des moyennes et grandes entreprise a davantage de chances de réussir si un modèle de conception hiérarchique est utilisé. L'utilisation d'un modèle de conception hiérarchique permettra d'apporter plus facilement des modifications au réseau au fur et à mesure de la croissance de l'organisation. Le modèle de conception hiérarchique comprend les trois couches suivantes:

- La couche accès permet aux utilisateurs répartis dans les groupes de travail d'accéder au réseau.
- La couche distribution assure une connectivité basée sur les politiques d'administration et de sécurité.

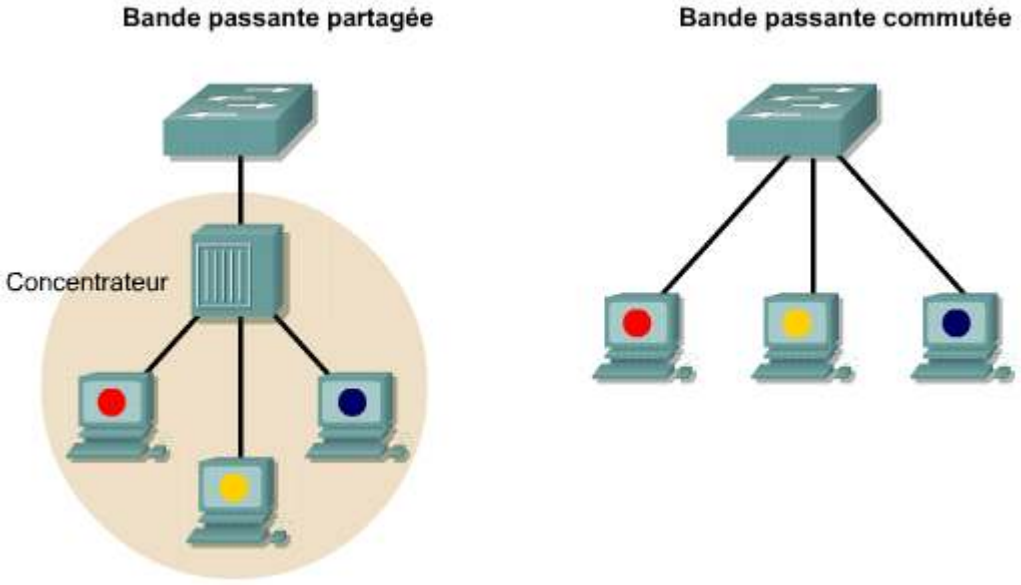
- La couche principale assure l'optimisation du transport entre les sites. La couche principale est souvent appelée backbone. 1



Ce modèle hiérarchique s'applique à n'importe quelle conception de réseau. Il est important de réaliser que ces trois couches peuvent exister en entités physiques distinctes. Mais ce n'est pas une obligation. Ces couches sont définies pour mener à bien la conception du réseau et pour constituer des fonctionnalités qui doivent exister dans un réseau.

La couche accès est le point d'entrée au réseau pour les stations de travail utilisateur et les serveurs. Dans un réseau LAN de campus, l'équipement utilisé au niveau de la couche accès peut être un commutateur ou un concentrateur.

Si un concentrateur est utilisé, la bande passante est partagée. Si un commutateur est utilisé, alors la bande passante est réservée. Si une station de travail ou un serveur est directement connecté à un port du commutateur, alors l'ordinateur connecté dispose de toute la bande passante de la connexion du commutateur. Si un concentrateur est connecté à un port de commutateur, la bande passante est partagée entre tous les équipements connectés au concentrateur. 2



Les fonctions de la couche accès comprennent également le filtrage de la couche MAC et la micro-segmentation. Le filtrage de la couche MAC permet aux commutateurs de diriger uniquement les trames vers le port du commutateur qui est connecté à l'équipement de destination. Le commutateur crée de petits segments de couche 2 appelés microsegments. Le domaine de collision peut ne comporter que deux équipements. Les commutateurs de couche 2 sont utilisés dans la couche accès. 3

- Bande passante partagée
- Bande passante réservée
- Filtrage de la couche MAC
- Microsegmentation

5.2 Commutateurs LAN

5.2.2 Commutateurs de la couche accès

Les commutateurs de la couche accès fonctionnent au niveau de la couche 2 du modèle OSI et fournissent des services tels que l'appartenance au VLAN. Le commutateur de couche accès a pour principal objectif d'autoriser l'accès des utilisateurs finaux sur le réseau. Un commutateur de la couche accès devrait fournir cette fonctionnalité à faible coût et avec une densité de port élevée.

Les commutateurs Cisco suivants sont couramment utilisés au niveau de la couche accès: 1

- Gamme Catalyst 1900
- Gamme Catalyst 2820
- Gamme Catalyst 2950
- Gamme Catalyst 4000
- Gamme Catalyst 5000

Catalyst	Type	Couches OSI prises en charge	Ports Ethernet	Ports Fast Ethernet	Gigabit Ethernet	Taille d'entreprise
Série 1900	Configuration fixe	Couche 2	12 ou 24	2	0	Petite à moyenne
Série 2820	Configuration fixe avec emplacements d'extension modulaires	Couche 2	24	2	0	Petite à moyenne
Série 2950	Configuration fixe	Couche 2	0	12 ou 24 (vitesse configurable)	0 ou 2	Petite à moyenne
Série 4000	Modulaire - plusieurs emplacements par châssis	Couches 2 et 3	Ports configurables - jusqu'à 240	Ports configurables - jusqu'à 240	Ports configurables jusqu'à 240	Varie selon les options choisies
Série 5000	Modulaire - plusieurs emplacements par châssis	Couches 2 et 3	Ports configurables - jusqu'à 528	Ports configurables - jusqu'à 266	Ports configurables - jusqu'à 38	Varie selon les options choisies

Le commutateur de la gamme Catalyst 1900 ou 2820 est un équipement d'accès efficace pour les réseaux de campus petits et moyens. Le commutateur de la gamme Catalyst 2950 fournit un accès efficace pour les serveurs et les utilisateurs qui requièrent une bande passante plus large. Cela est possible à l'aide de ports de commutateur à capacité Fast Ethernet et, pour certains modèles, à aussi des ports Gigabit Ethernet. Les commutateurs de la gamme Catalyst 4000 et 5000 incluent des ports Gigabit Ethernet et sont des équipements d'accès efficaces pour un grand nombre d'utilisateurs dans les grands réseaux de campus. 2

Activité de média interactive

Agrandissement: Cisco Catalyst 1912

Dans cette vue agrandie, l'étudiant peut voir un commutateur Cisco Catalyst 1912

Activité de média interactive

Agrandissement: Cisco Catalyst 2950

Dans cette vue agrandie, l'étudiant peut voir un commutateur Cisco Catalyst 2950

Activité de média interactive

Agrandissement: Cisco Catalyst 4006

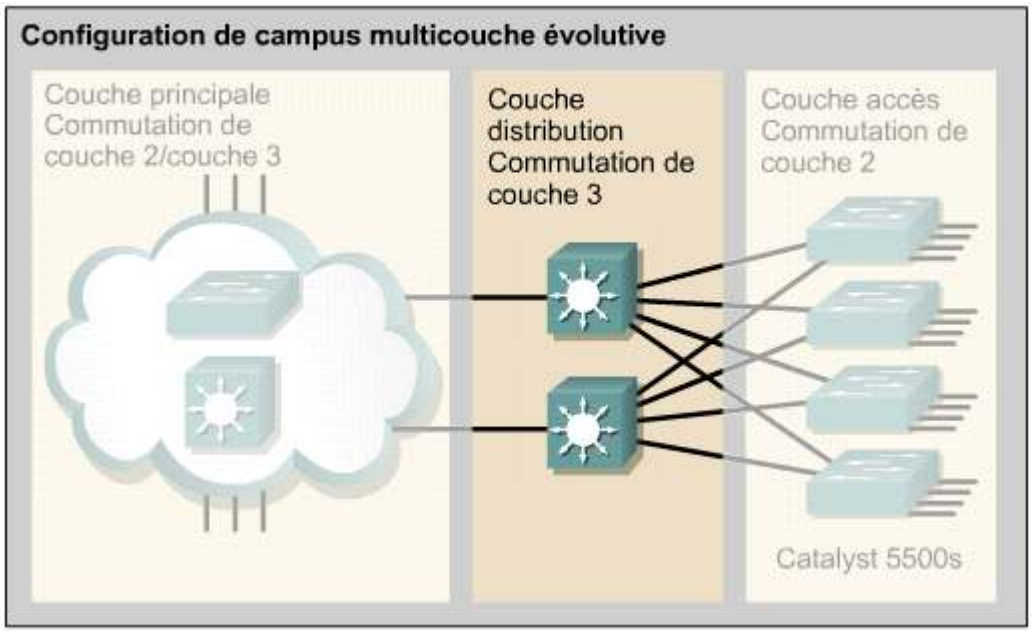
Dans cette vue agrandie, l'étudiant peut voir un commutateur Cisco Catalyst 4006.

5.2 Commutateurs LAN

5.2.3 Vue d'ensemble de la couche distribution

La couche distribution du réseau se situe entre la couche accès et la couche principale. Elle aide à définir et à distinguer la couche principale. Elle a pour rôle de définir les limites à l'intérieur desquelles le traitement des paquets peut avoir lieu. Elle segmente également les réseaux en domaines de broadcast. Des politiques de traitement peuvent être appliquées et des listes de contrôle d'accès peuvent filtrer les paquets. La couche distribution circonscrit les problèmes réseaux aux groupes de travail dans lesquels ils se produisent. La couche distribution empêche également ces problèmes d'affecter la couche principale. Les commutateurs de cette couche fonctionnent au niveau de la couche 2 et de la couche 3. Dans un réseau commuté, la couche distribution comprend plusieurs fonctions, notamment: 1

- le regroupement des connexions du local technique,
- la définition des domaines de broadcast et de diffusion multipoint (multicast),
- le routage des LAN virtuels (VLAN),
- le changement de média, si nécessaire,
- la sécurité.



5.2 Commutateurs LAN

5.2.4 Commutateurs de la couche distribution

Les commutateurs de la couche distribution sont les points de regroupement de plusieurs commutateurs de la couche accès. Le commutateur doit être en mesure de supporter la totalité du trafic des équipements de la couche accès.

La couche distribution doit avoir des performances élevées. Le commutateur de couche distribution est un point auquel est délimité un domaine de broadcast. La couche distribution combine le trafic VLAN et constitue un point qui focalise les décisions de la politique d'administration et de sécurité appliquées au flux du trafic. C'est pour cela que les commutateurs de la couche distribution fonctionnent au niveau de la couche 2 et de la couche 3 du modèle OSI. On appelle les commutateurs de cette couche «commutateurs multicouches». Ces derniers combinent en un seul équipement les fonctions d'un routeur et d'un commutateur. Ils sont conçus pour commuter le trafic de façon à obtenir des performances supérieures à celles d'un routeur standard. S'ils ne possèdent pas de module de routeur associé, un routeur externe est utilisé pour la fonction de couche 3.

Les commutateurs Cisco suivants sont adaptés pour la couche distribution:

- Catalyst 2926G 1

Cisco Catalyst 2926G

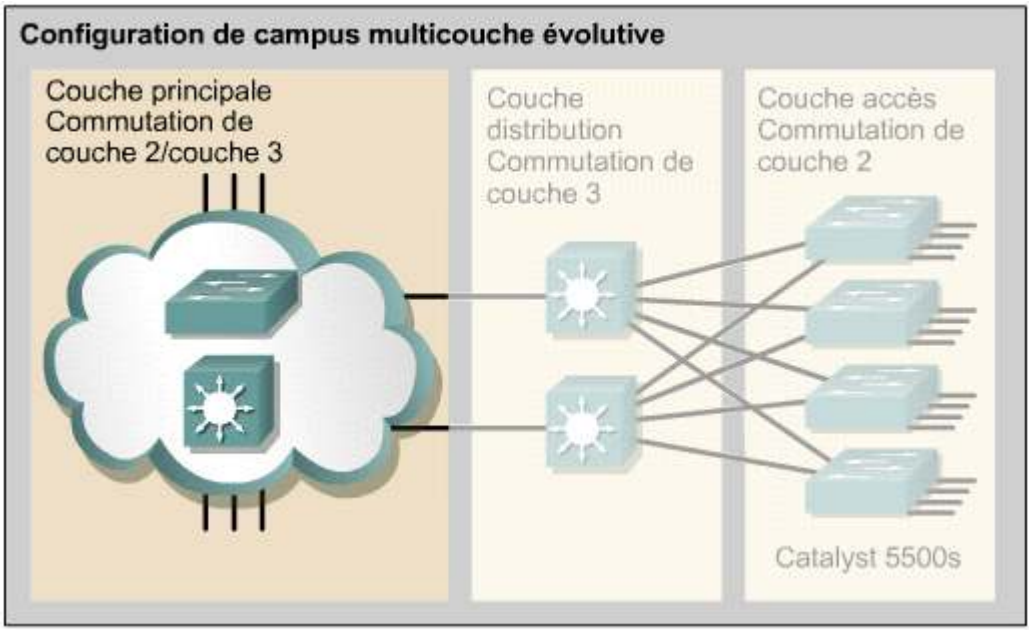
- Catalyst 3550
- Gamme Catalyst 5000
- Gamme Catalyst 6000 [2] [3]

Famille Cisco Catalyst 6000

5.2 Commutateurs LAN

5.2.5 Vue d'ensemble de la couche principale

La couche principale est un backbone de commutation à haut débit. S'ils ne possèdent pas de module de routeur associé, un routeur externe est utilisé pour la fonction de couche 3. Cette couche du réseau ne doit pas effectuer de tâches liées au traitement de paquets. Le traitement de paquets, comme le filtrage de liste de contrôle d'accès, pourrait en effet ralentir la commutation des paquets. L'établissement d'une infrastructure principale avec des routes redondantes procure de la stabilité au réseau pour pallier une éventuelle défaillance d'un équipement. [1]



La couche principale peut être conçue pour utiliser la commutation de couche 2 ou de couche 3. Des commutateurs ATM (Asynchronous Transfer Mode) ou Ethernet peuvent être utilisés.

Activité de média interactive

Pointer-cliquer: Le modèle de conception à trois couches

À la fin de cette activité, les étudiants seront en mesure d'identifier la fonction clé de la couche principale dans le modèle de conception à trois couches.

5.2 Commutateurs LAN

5.2.6 Commutateurs de la couche principale

La couche principale est le backbone du réseau commuté de campus. Les commutateurs de cette couche intègrent diverses technologies de couche 2. À condition que la distance entre les commutateurs de la couche principale ne soit pas trop grande, les commutateurs peuvent utiliser la technologie Ethernet. D'autres technologies de couche 2, telles que la commutation de cellules ATM (Asynchronous Transfer Mode), peuvent également être utilisées. Dans une conception de réseau, la couche principale peut être une couche principale routée ou de couche 3. Les commutateurs de couche principale sont conçus pour fournir en cas de besoin une fonctionnalité de couche 3 efficace. Des facteurs tels que le besoin, le coût et la performance doivent être pris en compte avant d'opérer un choix.

Les commutateurs Cisco suivants sont adaptés pour la couche principale: 1 2 3

- Gamme Catalyst 6500
- Gamme Catalyst 8500
- Gamme IGX 8400
- Lightstream 1010

Résumé

La compréhension des points clés suivants devrait être acquise:

- Les quatre objectifs majeurs de la conception de réseau LAN
- Les aspects principaux de la conception de réseau LAN
- Les différentes étapes d'une conception de réseau LAN systématique
- Les problèmes de conception associés aux couches 1, 2 et 3
- Le modèle de conception à trois couches
- Les fonctions de chaque couche du modèle à trois couches
- Les commutateurs Cisco de la couche accès et leurs caractéristiques
- Les commutateurs Cisco de la couche distribution et leurs caractéristiques
- Les commutateurs Cisco de la couche principale et leurs caractéristiques

Résumé

• La première étape de conception d'un réseau local consiste à définir les objectifs de la conception et à les expliquer par écrit.
• L'utilisation d'un modèle de conception hiérarchique permettra d'apporter plus facilement des modifications au réseau au fur et à mesure de la croissance de l'organisation. Le modèle de conception hiérarchique comprend les trois couches suivantes :
- La couche accès permet aux utilisateurs et aux groupes de travail d'accéder au réseau.
- La couche distribution assure une connectivité fondée sur les politiques.
- La couche principale assure l'optimisation du transport entre les sites. La couche principale est souvent appelée le backbone.

Vue d'ensemble

Un commutateur est une unité réseau de couche 2 qui agit comme point de concentration pour le raccordement de stations de travail, de serveurs, de concentrateurs et d'autres commutateurs.

Un concentrateur est un des premiers types d'unité de concentration mis sur le marché, il fournit également des ports multiples. Il est cependant moins performant qu'un commutateur car toutes les unités connectées à un concentrateur occupent le même domaine de bande passante ce qui entraîne des collisions. L'utilisation des concentrateurs comporte un autre inconvénient : ils fonctionnent en mode half-duplex. En mode half-duplex, les concentrateurs peuvent envoyer ou recevoir des données à n'importe quel moment, mais pas les deux en même temps. En revanche, les commutateurs peuvent fonctionner en mode full-duplex ce qui signifie qu'ils peuvent envoyer et recevoir des données simultanément.

Les commutateurs sont des ponts multiport. Il s'agit de la technologie standard actuelle pour les réseaux LAN Ethernet qui utilisent une topologie en étoile. Un commutateur fournit de nombreux circuits virtuels point à point, dédiés, si bien que les collisions sont pratiquement impossibles.

Étant donné le rôle dominant des commutateurs dans les réseaux modernes, il convient de bien en comprendre le fonctionnement et d'être en mesure de configurer ce type d'unité pour assurer la maintenance des réseaux.

La configuration d'un nouveau commutateur est prédéfinie avec des valeurs par défaut. Il est rare que cette configuration réponde entièrement aux besoins d'un administrateur réseau, c'est pourquoi il est possible de configurer et de gérer les commutateurs à partir d'une interface de commande en ligne (CLI). Il est de plus en plus fréquent de configurer et de gérer les unités réseau à partir d'une interface et d'un navigateur Web.

Un administrateur réseau doit connaître l'ensemble des tâches permettant de gérer un réseau à base de commutateurs. Certaines de ces tâches sont liées à la gestion du commutateur et de son IOS (Internetworking Operating System). D'autres permettent de gérer les interfaces et les tables pour garantir un fonctionnement optimal, fiable et sécurisé. La configuration de base des commutateurs, la mise à niveau de l'IOS et la récupération des mots de passe sont les compétences essentielles que doit posséder l'administrateur réseau.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Identification des principaux composants d'un commutateur Catalyst
- Surveillance de l'activité des commutateurs et de leur état à l'aide des indicateurs LED
- Observation, avec HyperTerminal, des informations affichées lors du démarrage d'un commutateur
- Utilisation des fonctions d'aide de l'interface de commande en ligne
- Liste des principaux modes de commande des commutateurs
- Vérification des paramètres par défaut d'un commutateur Catalyst
- Définition d'une adresse IP et d'une passerelle par défaut pour le commutateur afin de pouvoir s'y connecter à travers un réseau et le gérer ainsi à distance
- Affichage des paramètres du commutateur avec un navigateur Web
- Configuration de la vitesse et du mode de transfert (half ou full duplex) des interfaces
- Examen et gestion de la table d'adresses MAC des commutateurs
- Configuration de la sécurité des ports
- Gestion des fichiers de configuration et des images IOS
- Exécution de la procédure de récupération de mots de passe sur un commutateur
- Mise à niveau de l'IOS d'un commutateur

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
6.1	Démarrage du commutateur
6.2	Configuration du commutateur

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
	• Personnalisation de la configuration d'un commutateur pour répondre aux exigences du réseau • Création d'une configuration initiale sur un commutateur		

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Personnalisation de la configuration d'un commutateur pour répondre aux exigences du réseau • Création d'une configuration initiale sur un commutateur		

6.1 Démarrage du commutateur

6.1.1 Démarrage physique du commutateur Catalyst

Les commutateurs sont des ordinateurs dédiés et spécialisés qui contiennent une unité centrale de traitement (central processing unit - CPU), une mémoire à accès aléatoire (random access memory – RAM) et un système d'exploitation. Comme l'illustre la figure 1, les commutateurs comportent généralement plusieurs ports qui servent à connecter des hôtes ainsi que des ports spécialisés pour la gestion de ces équipements. Un commutateur peut être géré par le biais d'une connexion au port console qui vous permet de consulter et de modifier la configuration.

En règle générale, les commutateurs n'ont pas d'interrupteur d'alimentation permettant de les mettre sous tension ou hors tension. Ils se connectent ou se déconnectent simplement d'une source d'alimentation.

Plusieurs commutateurs de la série Cisco Catalyst 2950 apparaissent à la figure 1. Il y a des modèles avec 12, 24 et 48 ports. Les deux commutateurs du dessus à la figure 1sont des commutateurs symétriques à configuration fixes dont tous les ports sont de technologie FastEthernet ou 10/100. Les trois modèles suivants sont asymétriques et comportent deux ports Gigabit Ethernet fixes pour les médias de fibre ou de cuivre. Les quatre modèles du bas sont des commutateurs asymétriques comportant des emplacements pour interfaces modulaires GBIC (Gigabit Interface Converter) qui peut accomoder une variété d'options pour les médias de fibre ou de cuivre.

6.1 Démarrage du commutateur

6.1.2 Indicateurs LED de commutateur

Le panneau avant d'un commutateur comporte différents voyants permettant de surveiller les activités et les performances du système. On appelle ces voyants des diodes électroluminescentes (LED). Le panneau avant du commutateur comporte les LED suivantes:

- LED système
- LED RPS (Remote Power Supply)
- LED pour le mode des ports
- LED pour l'état des ports

La LED système indique si le système est bien alimenté et s'il fonctionne correctement.

La LED RPS indique si une source de téléalimentation est utilisée.

La LED Mode indique l'état actuel du bouton Mode. Les modes permettent de déterminer comment sont interprétés les LED d'état des ports. Pour sélectionner ou modifier le mode du port, appuyez plusieurs fois sur le bouton Mode jusqu'à ce que le LED Mode affiche le mode souhaité.

La signification des LED correspondant à l'état des ports varie en fonction de la valeur courante du LED Mode. 1

Led Mode	Couleur	Description
STAT	Désactivé	Aucune liaison
	Vert fixe	Liaison opérationnelle
	Vert clignotant	Le port est en train d'envoyer ou de recevoir des données.
	Alternativement vert/orange	Liaison défectueuse
	Orange fixe	Le port ne transmet pas de données car il a été désactivé par un administrateur ou une violation d'adresse, ou bloqué par le protocole Spanning Tree.
UTIL	Désactivé	Chaque LED éteinte indique une réduction de moitié de la bande passante totale. Les LED sont éteintes de droite à gauche. Si le LED le plus à droite est éteint, le commutateur utilise moins de 50 % de la bande passante totale. Si les deux LED les plus à droite sont éteintes, le commutateur utilise moins de 25 % de la bande passante totale.
	Vert	Si toutes les LED sont vertes, le commutateur utilise au moins 50 % de la bande passante totale.
DUPLX	Désactivé	Le port fonctionne en mode half-duplex.
	Vert	Le port fonctionne en mode full duplex.
SPEED	Désactivé	Le port fonctionne à 10 Mbits/s.
	Vert	Le port fonctionne à 100 Mbits/s.
	Vert clignotant	Le port opère à 1000 Mbits/s

6.1 Démarrage du commutateur

6.1.3 Vérification des LED au cours du test automatique de mise sous tension (POST)

Une fois que le câble d'alimentation est connecté, le commutateur lance une série de tests intitulée test automatique de mise sous tension (Power-On Self Test – POST). Le POST est un test qui s'exécute automatiquement et vérifie si le commutateur fonctionne correctement. La LED système indique le succès ou l'échec du test automatique de mise sous tension. Lorsque la LED système est éteinte mais que le commutateur est connecté, le test automatique de mise sous tension est en cours d'exécution. Lorsque la LED système est verte, cela signifie que le test automatique de mise sous tension a réussi. Lorsque la LED système est orange, cela signifie que le test automatique de mise sous tension a échoué. L'échec de ce test est considéré comme une erreur fatale. En cas d'échec, le fonctionnement du commutateur ne sera pas fiable.

Les LED d'état des ports peuvent également changer de couleur pendant le test automatique de mise sous tension du commutateur. Elles peuvent devenir orange pendant 30 secondes, juste le temps pour le commutateur de découvrir la topologie du réseau et de rechercher d'éventuelles boucles. Si les LED d'état des ports deviennent vertes, cela signifie que le commutateur a établi un lien entre le port et une cible telle qu'un ordinateur. Si elles s'éteignent, cela signifie que le commutateur a déterminé que rien n'est connecté au port. [1]

LED système

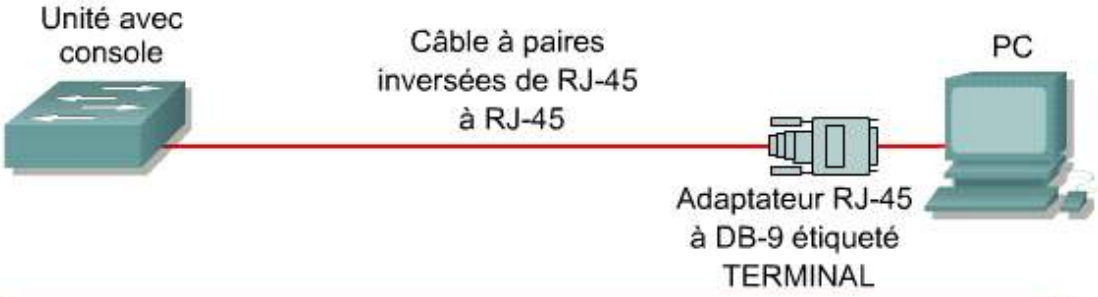
La LED système indique le succès ou l'échec de POST.

- Si la LED système est éteinte alors que le commutateur est connecté, le test POST est en cours.
- Si la LED système est verte, le test POST a réussi.
- Si la LED système est orange, le test POST a échoué.

6.1 Démarrage du commutateur

6.1.4 Affichage des informations après démarrage initial du commutateur

Pour configurer ou vérifier l'état d'un commutateur, connectez un ordinateur à ce commutateur afin d'établir une session de communication. Utilisez un câble à paires inversées pour connecter le port console situé à l'arrière du commutateur à un port COM situé à l'arrière de l'ordinateur. 1



- Les PC nécessitent un adaptateur RJ-45 à DB-9 ou RJ-45 à DB-25.
- Les propriétés du port COM sont: 9600 bits/s, 8 bits de données, aucune parité, 1 bit d'arrêt et contrôle de flux matériel
- Un accès hors bande à la console est fourni.
- Le port AUX du commutateur peut être utilisé pour une console connectée par modem.

Lancez HyperTerminal sur l'ordinateur. Une fenêtre de dialogue s'affiche. 2

La connexion doit d'abord être nommée lors de la configuration initiale de la communication HyperTerminal avec le commutateur. Sélectionnez le port COM auquel le commutateur est connecté via le menu déroulant, puis cliquez sur le bouton OK. Une deuxième fenêtre de dialogue s'affiche. 3

Définissez les paramètres comme indiqué, puis cliquez sur le bouton OK.

Branchez le commutateur à une prise murale. Les informations délivrées après le démarrage initial du commutateur devraient s'afficher sur l'écran HyperTerminal. Cet affichage présente des informations sur le commutateur, des détails sur l'état du POST et des données sur le matériel du commutateur.

Lorsque le commutateur a démarré et que le test automatique de mise sous tension a été réalisé, les invites du dialogue de configuration système s'affichent. Il est possible de configurer le commutateur manuellement avec ou sans l'assistance du dialogue de configuration système. Le dialogue de configuration système du commutateur est plus simple que celui du routeur.

Cisco C2950

```
C2950 Boot Loader (CALHOUN-HBOOT-M) Version
12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
Compiled Mon 30-Apr-01 07:56 by devgoyal
WS-C2950-24 starting...
Base ethernet MAC Address: 00:08:e3:2e:e6:00
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 162 files, 3 directories
flashfs[0]: 0 orphaned files, 0 orphaned
directories
flashfs[0]: Total bytes: 7741440
flashfs[0]: Bytes used: 2961920
flashfs[0]: Bytes available: 4779520
flashfs[0]: flashfs fsck took 6 seconds.
...done initializing flash.
Boot Sector Filesystem (bs:) installed, fsid: 3
Parameter Block Filesystem (pb:) installed, fsid:
4
Loading "flash:c2950-c3h2s-mz.120-
5.3.WC.1.bin"...##################################
################################################
########################################
File "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin"
uncompressed and installed, entry point:
0x80010000
executing...

Initializing flashfs...
flashfs[1]: 162 files, 3 directories
flashfs[1]: 0 orphaned files, 0 orphaned
directories
flashfs[1]: Total bytes: 7741440
flashfs[1]: Bytes used: 2961920
flashfs[1]: Bytes available: 4779520
flashfs[1]: flashfs fsck took 6 seconds.
flashfs[1]: Initialization complete.
Done initializing flashfs.
C2950 POST: System Board Test : Passed
C2950 POST: Ethernet Controller Test : Passed
C2950 POST: MII TEST : Passed

cisco WS-C2950-12 (RC32300) processor (revision
B0) with 22260K bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)
32K bytes of flash-simulated non-volatile
configuration memory.
Base ethernet MAC Address: 00:08:E3:2E:E6:00
Motherboard assembly number: 73-5782-08
Power supply part number: 34-0965-01
Motherboard serial number: FOC060502HP
Power supply serial number: PHI05500C5D
Model revision number: B0
Motherboard revision number: B0
Model number: WS-C2950-12
System serial number: FOC0605W0BH

Press RETURN to get started!
C2950 INIT: Complete

IOS (tm) C2950 Software (C2900XL-C3H2S-M), Version
12.0(5)XU,
RELEASE SOFTWARE
(fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Mon 03-Apr-00 16:37 by swati
--- System Configuration Dialog ---
At any point you may enter a question mark '?' for
help.
Use ctrl-c to abort configuration dialog at any
prompt.
Default settings are in square brackets '[]'.
Continue with configuration dialog? [yes/no]:
```

6.1 Démarrage du commutateur

6.1.5 Aperçu de l’aide de l’interface de commande en ligne du commutateur

L’interface de commande en ligne (CLI) des commutateurs Cisco ressemble beaucoup à celle des routeurs Cisco.

Pour utiliser le système d'aide, il suffit d'entrer un point d'interrogation (**?**). Lorsque cette commande est entrée à l'invite du système, la liste des commandes disponibles pour le mode de commande actuel s'affiche. 1

Le système d'aide est très flexible. Pour obtenir la liste des commandes qui commencent par une séquence de caractères particulière, entrez ces caractères suivis immédiatement d’un point d’interrogation (**?**). N’entrez pas d’espace avant le point d’interrogation. Cette forme d’aide s’appelle l’aide sur les termes car elle permet de compléter un terme.

Pour obtenir la liste des mots clés ou des arguments associés à une commande particulière, entrez un ou plusieurs termes associés à la commande, suivis d’un espace et d’un point d’interrogation (**?**). Cette forme d’aide est appelée aide à la syntaxe des commandes car elle fournit des mots clés ou des arguments en fonction d’une commande partielle.

Cisco

```
Switch>?

Exec commands:

access-enable     Create a temporary Access-List entry

clear             Reset functions

connect           Open a terminal connection

disable           Turn off privileged commands

disconnect        Disconnect an existing network
                  connection

enable            Turn on privileged commands
exit              Exit from the EXEC

help              Description of the interactive help
                  system

lock              Lock the terminal

login             Log in as a particular user

logout            Exit from the EXEC

name-connection   Name an existing network connection

ping              Send echo messages

rcommand          Run command on remote switch
resume            Resume an active network connection

show              Show running system information

systat            Display information about terminal
                  lines

telnet            Open a telnet connection

terminal          Set terminal line parameters

traceroute        Trace route to destination

tunnel            Open a tunnel connection

where             List active connections
```

Activité de média interactive

Compléter les zones vides : Commutateurs et domaines de collision

À la fin de cette activité, les étudiants doivent être en mesure d'identifier le rôle d'un commutateur dans la prévention et la réduction des domaines de collision.

6.1 Démarrage du commutateur

6.1.6 Modes de commande des commutateurs

Les commutateurs disposent de plusieurs modes de commande. Le mode par défaut est le mode utilisateur (User EXEC mode). L'invite permettant de reconnaître le mode utilisateur est le signe «supérieur à» (>). Les commandes disponibles en mode utilisateur sont celles qui permettent de modifier les paramètres du terminal, de réaliser des tests de base et d'afficher les informations système. La figure 1 décrit les commandes **show** disponibles en mode utilisateur.

Commandes	Description
`show version`	Affiche les informations de version du logiciel et du matériel. Utilisé afin de déterminer exactement le logiciel et les modules en cours d'utilisation.
`show flash:`	Affiche l'information à propros du système de fichiers flash: .
`show mac-address-table`	Affiche les adresses MAC contenues dans la table de con
`show controllers ethernet-controller`	Indique les trames abandonnées ou différées, les erreurs d'alignement, les collisions, etc.

La commande **enable** est utilisée pour passer du mode utilisateur au mode privilégié. L'invite permettant de reconnaître le mode privilégié (Privileged EXEC mode) est le signe «dièse» (#). Parmi les commandes du mode privilégié, on retrouve celles du mode utilisateur, plus la commande **configure**. La commande **configure** permet d'accéder aux autres modes de commande. Comme ces modes sont utilisés pour configurer le commutateur, l'accès au mode privilégié devrait être protégé par un mot de passe pour empêcher les accès non autorisés. Si l'administrateur a défini un mot de passe, le système demande aux utilisateurs d'entrer ce mot de passe pour pouvoir accéder au mode privilégié. Le mot de passe tient compte des majuscules et ne s'affiche pas à l'écran.

Commandes	Description
`show running-config`	Affiche le fichier de configuration courant du commutateur.
`show post`	Indique si commutateur a réussi son test automatique de mise sous tension (POST)
`show vlan`	Vérifie la configuration VLAN.
`show interfaces`	Affiche la configuration et l'état d'une interface.

6.2 Configuration du commutateur

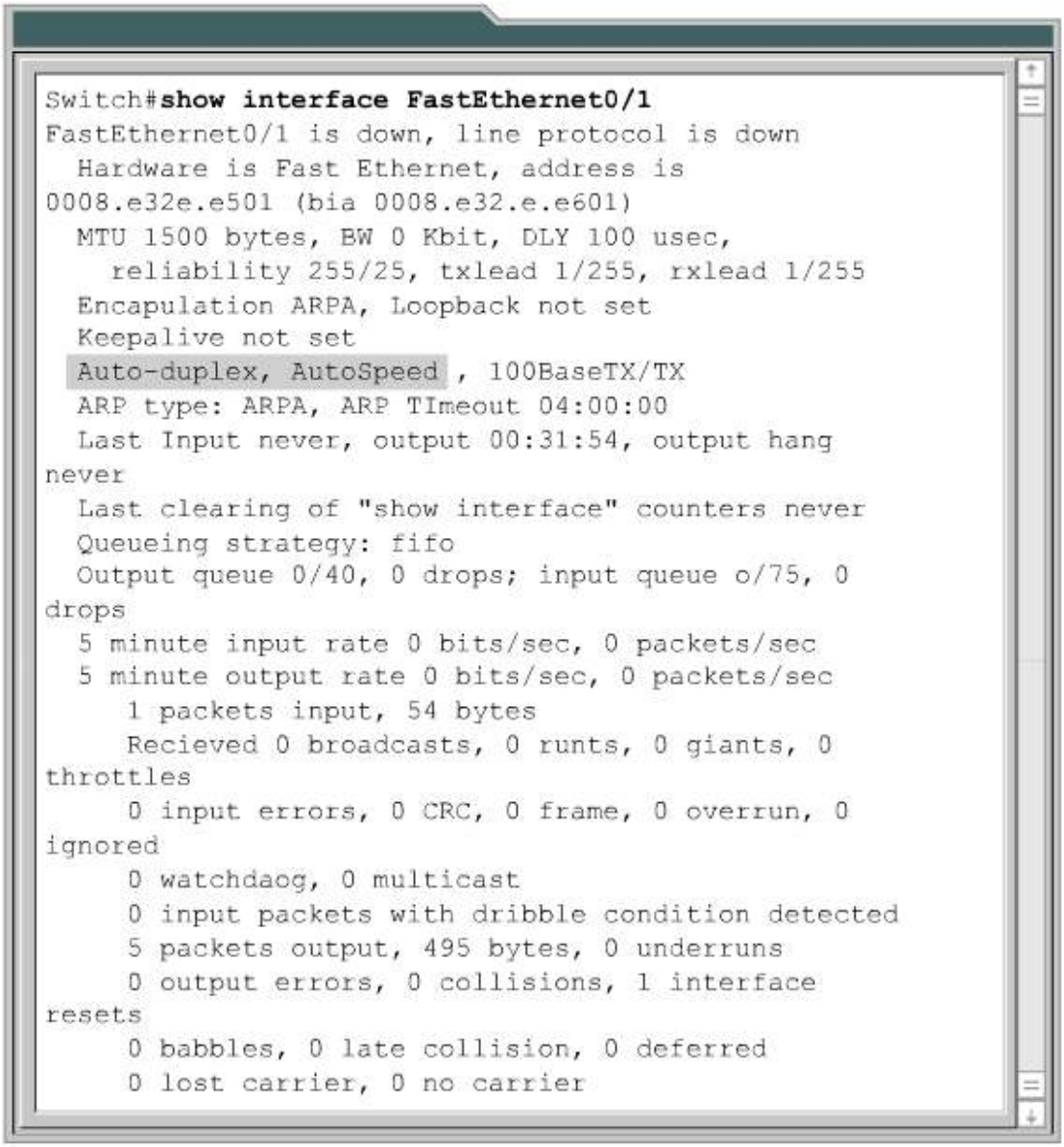
6.2.1 Vérification de la configuration par défaut du commutateur Catalyst

La première fois qu'un commutateur est mis sous tension, il comporte des données par défaut dans le fichier de la configuration courante. Le nom d'hôte par défaut est Switch. Aucun mot de passe n'est défini sur les lignes de console ou de terminal virtuel (vty). 1

Il est possible de donner une adresse IP à un commutateur pour des raisons d'administration. Il faut configurer cette adresse au niveau de l'interface virtuelle, VLAN 1. Par défaut, le commutateur n'a pas d'adresse IP. 1

```
Switch#show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!<Affichage tronqué>
!
interface VLAN1
 no ip directed-broadcast
 no ip route-cache
!
!
!<Affichage tronqué>
!
line con 0
 transport input none
 stopbits 1
line vty 5 15
!
end
```

Les ports ou interfaces du commutateur sont définis sur le mode automatique et tous les ports du commutateur se trouvent dans le VLAN 1.



```
Switch#show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
  Hardware is Fast Ethernet, address is
0008.e32e.e501 (bia 0008.e32.e.e601)
  MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
    reliability 255/25, txlead 1/255, rxlead 1/255
  Encapulation ARPA, Loopback not set
  Keepalive not set
  Auto-duplex, AutoSpeed , 100BaseTX/TX
  ARP type: ARPA, ARP TImeout 04:00:00
  Last Input never, output 00:31:54, output hang
never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/40, 0 drops; input queue o/75, 0
drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1 packets input, 54 bytes
     Recieved 0 broadcasts, 0 runts, 0 giants, 0
throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0
ignored
     0 watchdaog, 0 multicast
     0 input packets with dribble condition detected
     5 packets output, 495 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface
resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
```

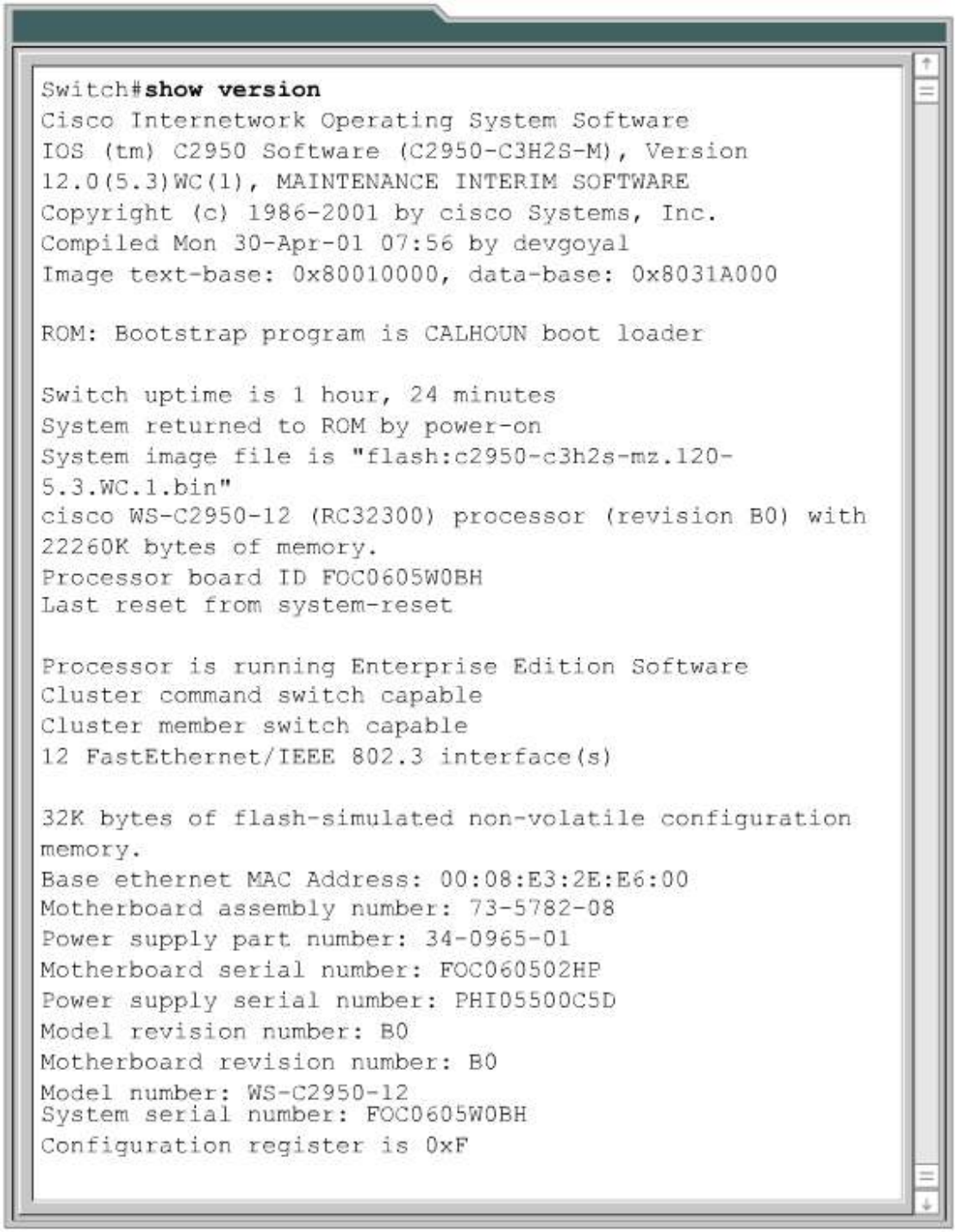
3 VLAN 1 est le VLAN d'administration par défaut.

```
Switch#show vlan
VLAN Name                Status Ports
---- ------------------- ------ -------------------------
1    default             active Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                                Fa0/5, Fa0/6, Fa0/7, Fa0/8,
                                Fa0/9, Fa0/10,Fa0/11,Fa0/12
1002 fddi-default        active
1003 token-ring-default active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type  SAID    MTU   Parent RingNo BridgeNo
---- ----- ------  ----- ------ ------ --------
1    enet  100001  1500  -      -      -
1002 fddi  101002  1500  -      -      -
1003 tr    101003  1500  1005   0      -
1004 fdnet 101004  1500  -      -      1
1005 trnet 101005  1500  -      -      1

Stp BrdgMode Trans1 Trans2
--- -------- ------ ------
-   -        1002   1003
-   -        1      1003
-   srb      1      1002
ibm -        0      0
ibm -        0      0
```

Le répertoire flash par défaut comporte un fichier qui contient l'image IOS, un fichier nommé env_vars et un sous-répertoire nommé html. Une fois que le commutateur est configuré, ce répertoire peut également contenir un fichier config.text et une base de données VLAN. Le répertoire flash ne contient ni fichier de base de données, vlan.dat, ni fichier de configuration stocké, config.text. 4

```
Switch#show flash ou Switch#dir flash:
Directory of flash:/

  2  -rwx     1674921   Apr 30 2001 15:09:51  c2950-
c3h2s-mz.120-5.3.WC.1.bin
  3  -rwx         269   Jan 01 1970 00:00:57
env_vars
  4  drwx       10240   Apr 30 2001 15:09:52  html

7741440 bytes total (4780544 bytes free)
```

Il est possible de vérifier les paramètres de version IOS et du registre de configuration en utilisant la commande **`show version`**. 5



```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-C3H2S-M), Version
12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:56 by devgoyal
Image text-base: 0x80010000, data-base: 0x8031A000

ROM: Bootstrap program is CALHOUN boot loader

Switch uptime is 1 hour, 24 minutes
System returned to ROM by power-on
System image file is "flash:c2950-c3h2s-mz.120-
5.3.WC.1.bin"
cisco WS-C2950-12 (RC32300) processor (revision B0) with
22260K bytes of memory.
Processor board ID FOC0605W0BH
Last reset from system-reset

Processor is running Enterprise Edition Software
Cluster command switch capable
Cluster member switch capable
12 FastEthernet/IEEE 802.3 interface(s)

32K bytes of flash-simulated non-volatile configuration
memory.
Base ethernet MAC Address: 00:08:E3:2E:E6:00
Motherboard assembly number: 73-5782-08
Power supply part number: 34-0965-01
Motherboard serial number: FOC060502HP
Power supply serial number: PHI05500C5D
Model revision number: B0
Motherboard revision number: B0
Model number: WS-C2950-12
System serial number: FOC0605W0BH
Configuration register is 0xF
```

Dans cet état par défaut, le commutateur a un domaine de broadcast et peut être géré ou configuré via le port console en utilisant l'interface de commande en ligne (CLI). Le protocole d'acheminement STP (Spanning-Tree Protocol) est également activé et permet au pont d'élaborer une topologie exempte de boucles de couche 2 dans un réseau local étendu.

La configuration par défaut convient pour les petits réseaux. Les avantages de la microsegmentation sur le plan des performances sont immédiatement visibles.

Activité de TP

Exercice : Vérification de la configuration par défaut du commutateur

Au cours de ce TP, les étudiants vont étudier la configuration par défaut d'un commutateur de la gamme 2900.

Activité de TP

Activité en ligne : Fonctionnement de base du commutateur

Au cours de ce TP, les étudiants vont examiner la configuration d'un commutateur 2950.

6.2 Configuration du commutateur

6.2.2 Configuration du commutateur catalyst

Un commutateur peut déjà avoir été préconfiguré et nécessiter uniquement l'entrée des mots de passe pour accéder au mode utilisateur ou privilégié. Vous pouvez accéder au mode de configuration des commutateurs à partir du mode privilégié.

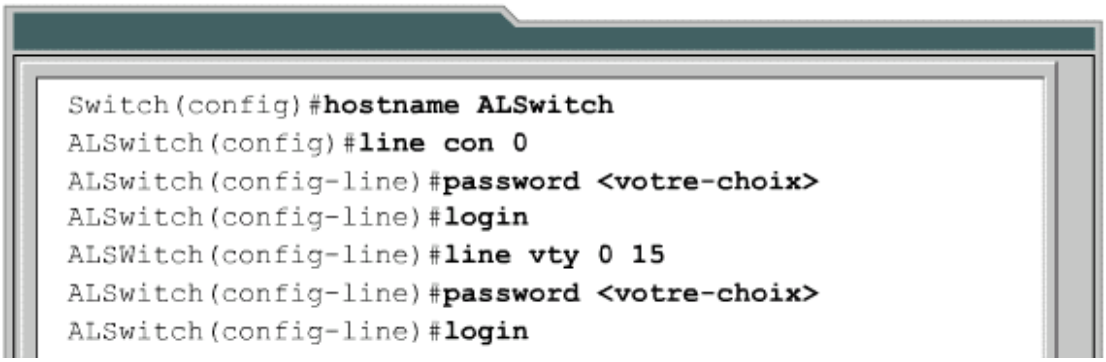
Dans le mode d'interface de commande en ligne (CLI – command line interface), l'invite de commande par défaut du mode privilégié est Switch#. L'invite du mode utilisateur sera Switch>.

Suivez les étapes suivantes pour être sûr que la nouvelle configuration remplace la configuration existante:

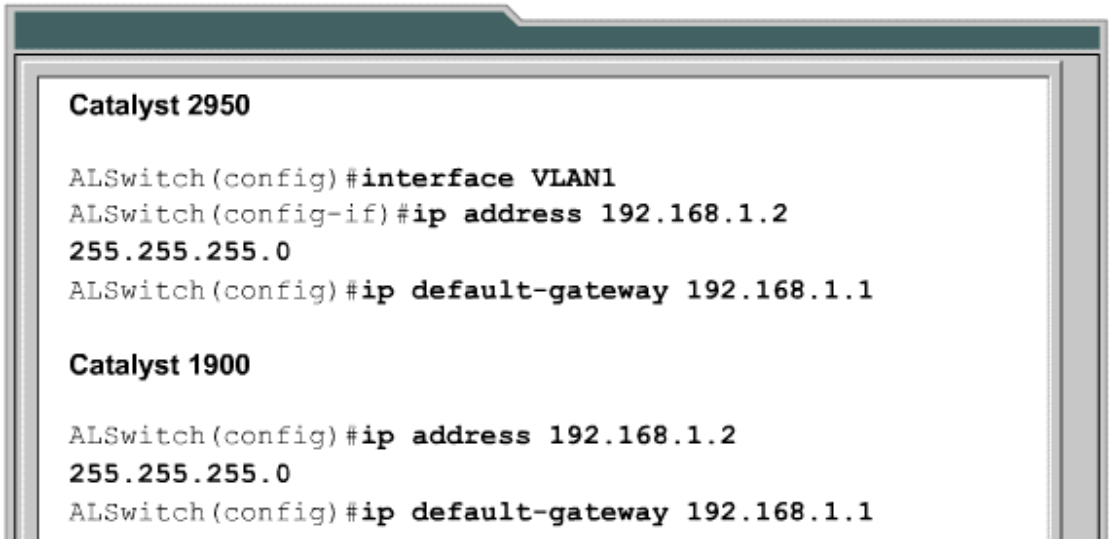
- Supprimez toutes les informations VLAN existantes en supprimant le fichier de base de données VLAN (vlan.dat) de la mémoire flash.
- Supprimez le fichier de configuration sauvegardé startup-config.
- Rechargez le commutateur 1.

Tous les aspects liés à la sécurité, à la documentation et à la gestion d'un équipement réseau sont extrêmement importants.

Il est possible de donner un nom d'hôte à un commutateur. Les mots de passe doivent être définis au niveau des lignes de console et des lignes vty. 2



Si vous voulez que le commutateur soit accessible via Telnet et d'autres applications TCP/IP, il faut définir des adresses IP et une passerelle par défaut. 3



Catalyst 2950

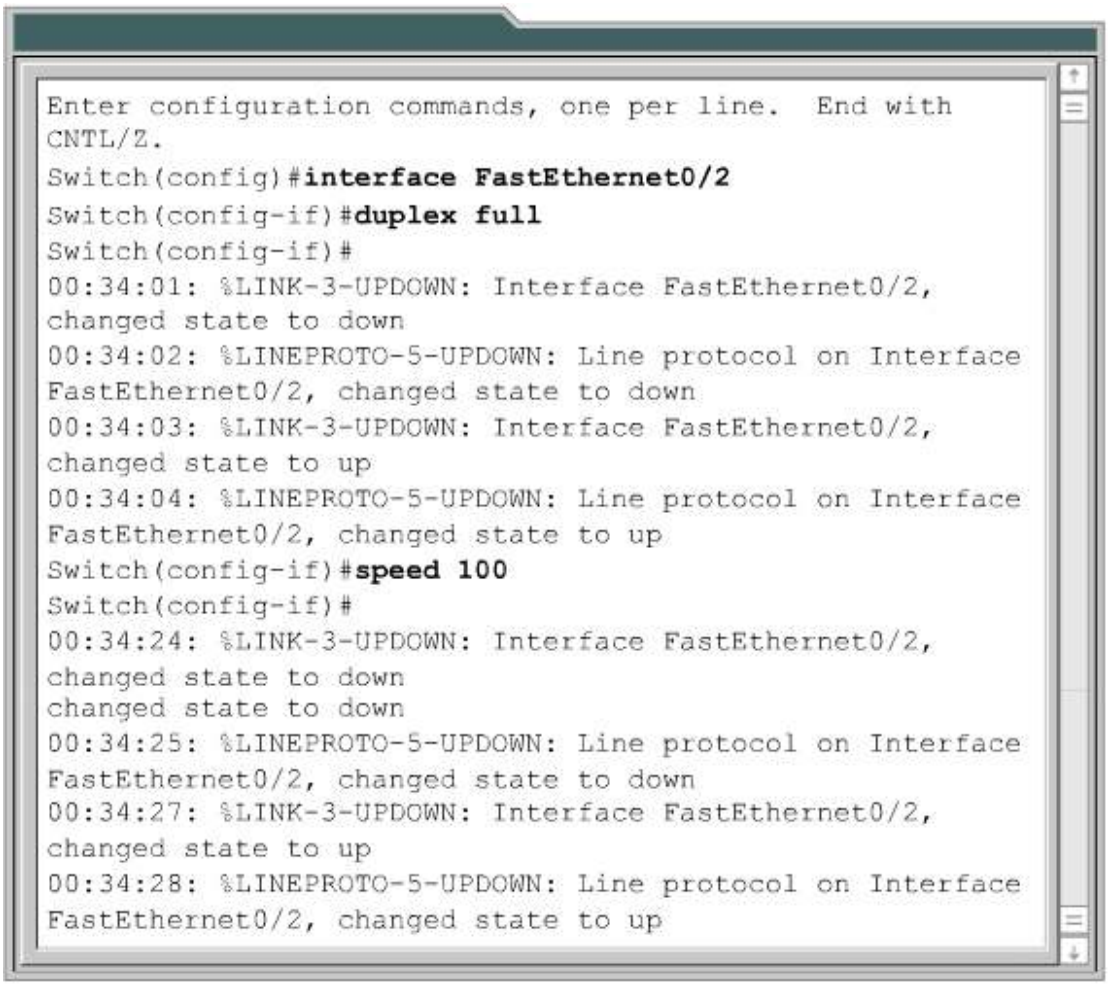
```
ALSwitch(config)#interface VLAN1
ALSwitch(config-if)#ip address 192.168.1.2
255.255.255.0
ALSwitch(config)#ip default-gateway 192.168.1.1
```

Catalyst 1900

```
ALSwitch(config)#ip address 192.168.1.2
255.255.255.0
ALSwitch(config)#ip default-gateway 192.168.1.1
```

VLAN 1 est le VLAN de gestion par défaut. Les VLAN de gestion est utilisé pour gérer tous les équipements sur le réseau. Dans un réseau commuté, tous les équipements du réseau doivent être inclus dans le VLAN de gestion. Tous les ports appartiennent au VLAN 1 par défaut. Une pratique recommandée est d'enlever tous les ports d'accès de VLAN 1 et de les placer dans un autre réseau. Ceci permet la gestion des équipements tout en gardant le trafic en provenance et à destination des hôtes en dehors du VLAN de gestion.

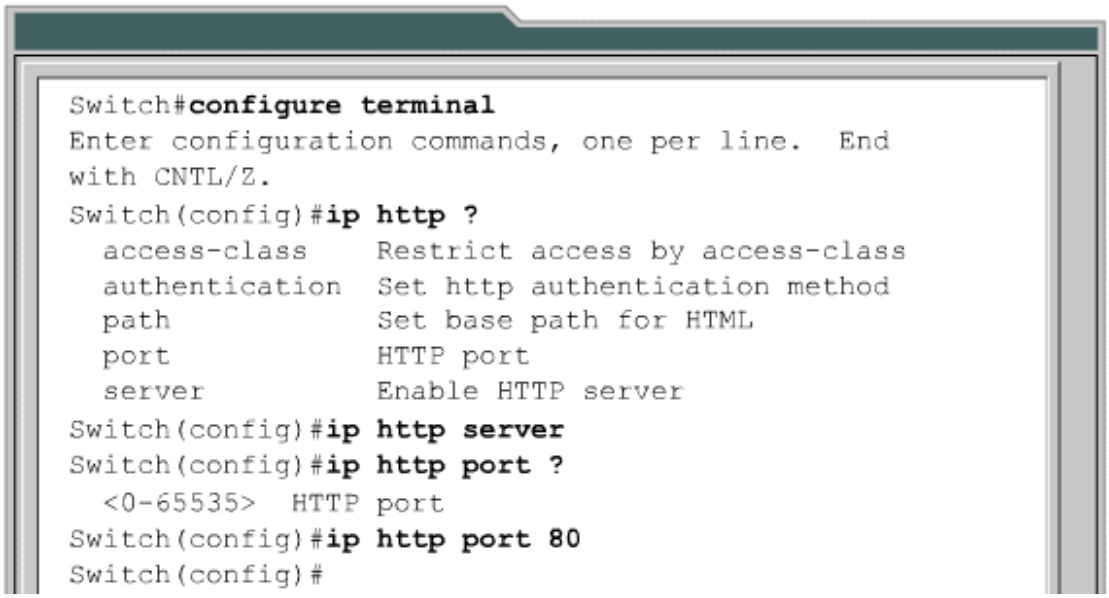
Par défaut, la vitesse et le mode duplex des ports de commutation Fast Ethernet sont définis automatiquement. Les interfaces peuvent ainsi négocier ces paramètres. Lorsqu'un administrateur réseau tient absolument à fixer lui-même la vitesse et le mode duplex d'une interface, il peut définir ces valeurs manuellement. 4



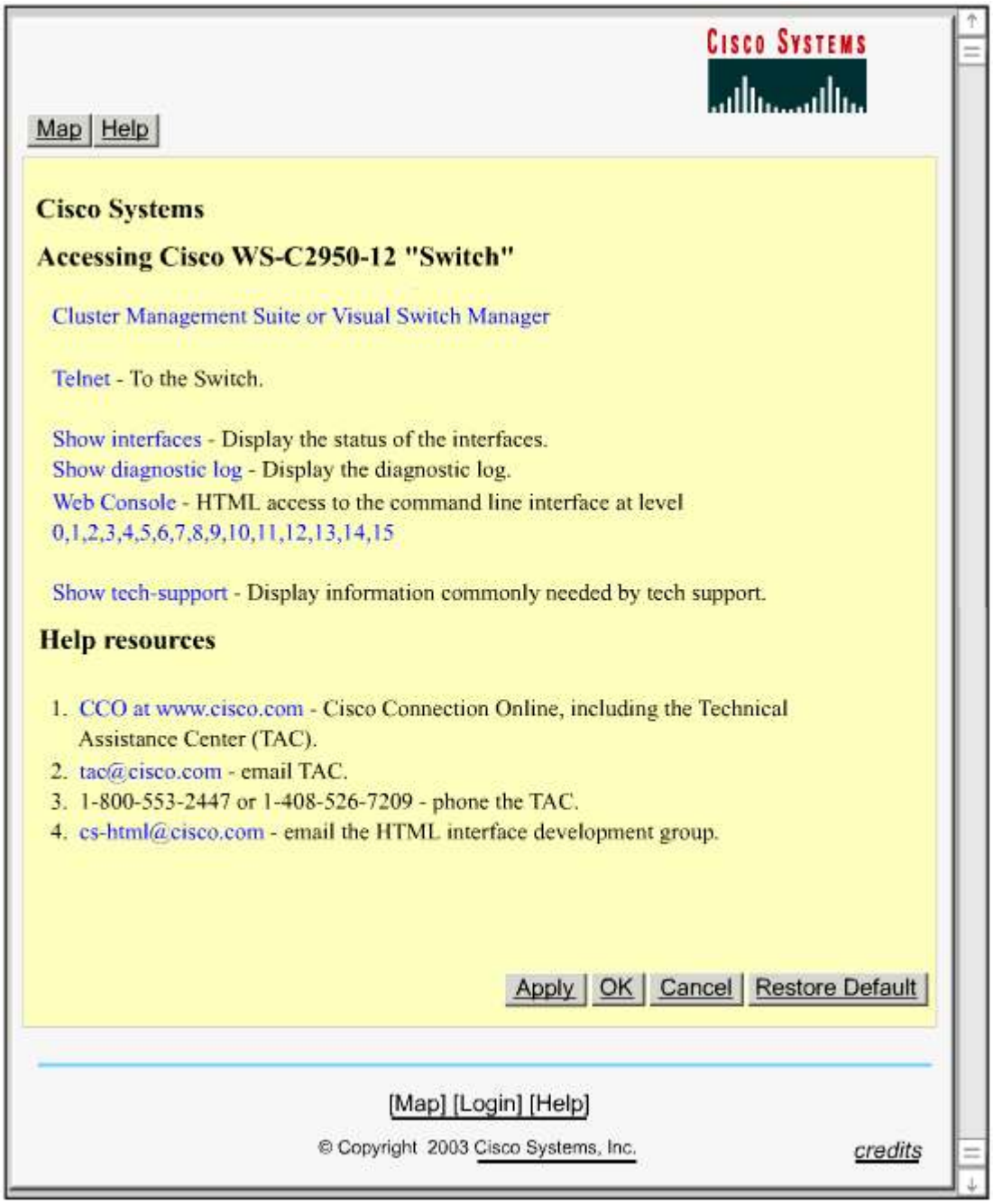
```
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#
00:34:01: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to down
00:34:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to down
00:34:03: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to up
00:34:04: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up
Switch(config-if)#speed 100
Switch(config-if)#
00:34:24: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to down
changed state to down
00:34:25: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to down
00:34:27: %LINK-3-UPDOWN: Interface FastEthernet0/2,
changed state to up
00:34:28: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/2, changed state to up
```

Des équipements de réseau intelligents peuvent offrir une interface Web à des fins de configuration et de gestion. Une fois qu'un commutateur est configuré avec une adresse IP et une passerelle, il est possible d'y accéder de cette façon. Un

navigateur Web peut accéder à ce service en utilisant l'adresse IP et le port 80, port par défaut pour http. Il est possible d'activer ou de désactiver le service HTTP et de choisir l'adresse du port pour le service. 5



Un composant logiciel supplémentaire tel qu'un applet peut être téléchargé vers le navigateur à partir du commutateur. En outre, les équipements réseaux peuvent être gérés par une interface graphique (GUI) de type navigateur. 6 7


Cisco Systems
Map
Help
Cisco Systems
Accessing Cisco WS-C2950-12 "Switch"
Cluster Management Suite or Visual Switch Manager
Telnet - To the Switch.
Show interfaces - Display the status of the interfaces.
Show diagnostic log - Display the diagnostic log.
Web Console - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15
Show tech-support - Display information commonly needed by tech support.
Help resources
1. CCO at www.cisco.com - Cisco Connection Online, including the Technical Assistance Center (TAC).
2. tac@cisco.com - email TAC.
3. 1-800-553-2447 or 1-408-526-7209 - phone the TAC.
4. cs-html@cisco.com - email the HTML interface development group.
Apply
OK
Cancel
Restore Default
[Map] [Login] [Help]
© Copyright 2003 Cisco Systems, Inc.
credits

Activité de TP

Exercice : Configuration de base d'un commutateur

Au cours de ce TP, les étudiants vont configurer un commutateur avec un nom et une adresse IP.

Activité de TP

Activité en ligne : Configuration de base d'un commutateur

Au cours de ce TP, les étudiants vont configurer un commutateur 2950.

6.2.3 Gestion de la table d'adresses MAC

6.2.3 Gestion de la table d'adresses MAC

Les commutateurs apprennent les adresses MAC des PC ou des stations de travail connectés à un de leurs ports de commutation en examinant l'adresse source des trames reçues sur ce port. Les adresses MAC ainsi apprises sont ensuite enregistrées dans une table d'adresses MAC. Les trames ayant une adresse MAC de destination enregistrée dans la table peuvent être commutées vers l'interface appropriée.

Pour afficher les adresses apprises par un commutateur, entrez la commande **`show mac-address-table`** en mode privilégié. 1

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

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000d.6562.f240    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    00b0.d0cb.8e1c    DYNAMIC     Fa0/3
   1    00b0.d0cb.8e75    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 6
Switch#
```

Un commutateur est capable d'apprendre et de gérer de façon dynamique des milliers d'adresses MAC. Pour ne pas surcharger la mémoire et optimiser le fonctionnement du commutateur, les adresses apprises peuvent être supprimées de la table d'adresses MAC. Les machines ont peut-être été supprimées d'un port, mises hors tensions ou connectées à un autre port sur le même commutateur ou sur un commutateur différent. Ceci peut engendrer une certaine confusion dans le transfert des trames. Par conséquent, si aucune trame n'est interceptée avec l'adresse apprise précédemment, l'entrée correspondante est automatiquement supprimée dans la table d'adresses MAC ou expire au bout de 300 secondes.

Au lieu d'attendre l'expiration d'une entrée dynamique, l'administrateur a la possibilité d'utiliser la commande **`clear mac-address-table`** en mode privilégié. 2

```
Switch#clear mac-address-table dynamic
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000d.6562.f240    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
Total Mac Addresses for this criterion: 4
Switch#
```

Cette commande permet également de supprimer les adresses MAC qu'un administrateur a configurées. Cette méthode permet de s'assurer que les adresses invalides sont automatiquement supprimées.

Activité de TP

Exercice : Gestion de la table d'adresses MAC

Au cours de ce TP, les étudiants vont créer une configuration de commutateur de base et gérer la table MAC.

Activité de TP

Activité en ligne : Gestion des tables d'adresses MAC. Au cours de ce TP, les étudiants vont observer et supprimer les entrées de la table d'adresses MAC.

6.2 Configuration du commutateur

6.2.4 Configuration d'adresses MAC statiques

Vous pouvez décider d'affecter une adresse MAC de façon permanente à une interface pour différentes raisons. Voici certaines de ces raisons:

- L'adresse MAC ne doit jamais être supprimée automatiquement par le commutateur.
- Un serveur ou une station de travail spécifique doit être attachée au port et l'adresse MAC est connue.
- Améliorer la sécurité.

Utilisez cette commande pour définir une entrée d'adresse MAC statique pour un commutateur:

```
Switch(config)#mac-address-table static <adresse-mac de l'hôte> interface
FastEthernet <numéro Ethernet> vlan <nom vlan>
```

Pour supprimer cette entrée, utilisez la forme **no** de cette commande:

```
Switch(config)#no mac-address-table static <adresse-mac de l'hôte> interface
FastEthernet <numéro Ethernet>vlan <nom vlan> 1
```

```
Switch(config)#mac-address-table ?
  aging-time    Set MAC address table entry maximum age
  notification  Enable/Disable MAC Notification on the
switch
  static        static keyword

Switch(config)#mac-address-table static 00b0.d0cd.8e1d
               vlan 1 interface FastEthernet 0/5
Switch(config)#exit
Switch#
00:30:01: %SYS-5-CONFIG_I: Configured from console by
console
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000d.6562.f240    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    00b0.d0cb.8e1c    DYNAMIC     Fa0/3
   1    00b0.d0cb.8e75    DYNAMIC     Fa0/2
   1    00b0.d0cd.8e1d    STATIC      Fa0/5
Total Mac Addresses for this criterion: 7

Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#no mac-address-table static 00b0.d0cd.8e1d
               vlan 1
Switch(config)#end
Switch#sh
00:31:46: %SYS-5-CONFIG_I: Configured from console by
console
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000d.6562.f240    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    00b0.d0cb.8e1c    DYNAMIC     Fa0/3
   1    00b0.d0cb.8e75    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 6
Switch#
```

Activité de TP

Exercice : Configuration d'adresses MAC statiques

Dans ce TP, les étudiants vont créer une entrée statique dans la table des adresses MAC.

Activité de TP

Activité en ligne : Configuration d'adresses MAC statiques

Dans ce TP, l'étudiant vont configurer des adresses MAC statiques.

6.2 Configuration du commutateur

6.2.5 Configuration de la sécurité des ports

Une des grandes responsabilités de l'administrateur réseau est de sécuriser le réseau. Les ports de commutation de la couche d'accès sont accessibles via le câblage structuré au niveau des prises murales disponibles dans les bureaux et les salles. N'importe qui peut brancher un PC ou un ordinateur portable à une de ces prises. Ceci représente donc un accès possible au réseau pour les utilisateurs non autorisés. Les commutateurs offrent une fonction appelée « sécurité des ports ». Il est possible de limiter le nombre d'adresses qu'une interface peut apprendre. Le commutateur peut être configuré pour entreprendre une action dans le cas où cette limite serait dépassée. 1 Des adresses MAC sécurisées peuvent être définies de façon statique. La sécurisation statique des adresses MAC peut toutefois s'avérer une tâche complexe et source d'erreurs.

```
Switch(config)#interface FastEthernet 0/2
Switch(config-if)#switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addrs
  violation     Security Violation Mode
  <cr>
```

Une autre approche consiste à définir la sécurité des ports sur une interface du commutateur. Le nombre d'adresses MAC par port peut être limité à 1. La première adresse apprise par le commutateur de façon dynamique devient l'adresse sécurisée.

Pour annuler la sécurité des ports sur une interface, utilisez la forme **no** de la commande.

Utilisez la commande **show port security** pour vérifier l'état de sécurité du port.

Activité de TP

Exercice : Configuration de la sécurité des ports

Dans ce TP, les étudiants vont apprendre à configurer l'option de sécurité "port security" sur des ports FastEthernet individuels.

Activité de TP

Activité en ligne : Configuration de la sécurité des ports

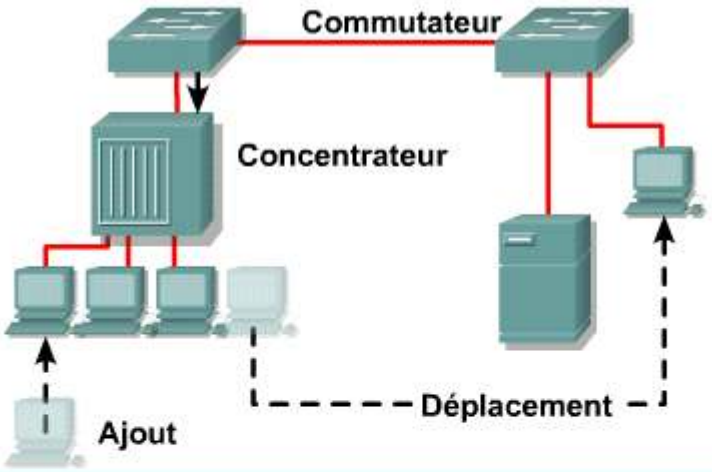
Au cours de ce TP, les étudiants vont définir la sécurité des ports du commutateur.

6.2 Configuration du commutateur

6.2.6 Exécution d'ajouts, de déplacements et de modifications

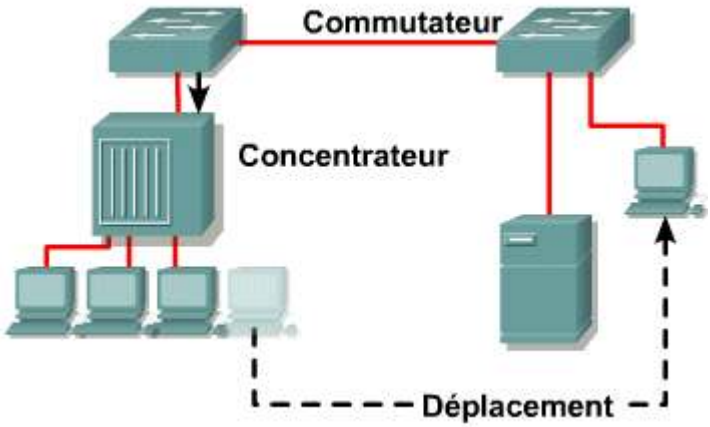
Lorsqu'un nouveau commutateur est ajouté à un réseau, configurez les éléments suivants:

- Le nom du commutateur
- L'adresse IP du commutateur dans le VLAN d'administration
- Une passerelle par défaut
- Les mots de passe de ligne 1



- Configurez le nom du commutateur.
- Déterminez et configurez l'adresse IP à des fins de gestion.
- Configurez une passerelle par défaut.
- Configurez un accès administratif pour les interfaces en mode console, auxiliaire et de terminal virtuel (VTY).
- Configurez la sécurité de l'équipement.
- Configurez les ports d'accès du commutateur si nécessaire.

Lorsqu'un hôte passe d'un port ou d'un commutateur à un autre, il est préférable de supprimer les configurations pouvant entraîner un comportement inattendu. La configuration requise peut ensuite être ajoutée. 2



Ajout d'une adresse MAC
1. Configurez la sécurité des ports.
2. Configurez l'adresse MAC.

Modification d'une adresse MAC
1. Supprimez les restrictions d'adresse MAC.

Déplacement d'une adresse MAC
1. Ajoutez l'adresse à un nouveau port.
2. Configurez la sécurité des ports sur le nouveau commutateur.
3. Configurez l'adresse MAC du port alloué pour le nouvel utilisateur.
4. Supprimez la configuration de l'ancien port.

Activité de TP

Exercice : Ajout, suppression et modification d'adresses MAC

Au cours de ce TP, les étudiants vont créer et vérifier une configuration de commutateur de base.

Activité de TP

Activité en ligne : Ajout, suppression et modification d'adresses MAC sur le commutateur

Au cours de ce TP, les étudiants vont ajouter une adresse MAC au commutateur, puis déplacer cette adresse et la modifier.

6.2 Configuration du commutateur

6.2.7 Gestion du fichier de système d'exploitation du commutateur

Un administrateur devrait documenter et gérer les fichiers de configuration opérationnels des équipements réseau. Le fichier de la configuration courante le plus récent devrait être sauvegardé sur un serveur ou un disque. Il s'agit non seulement d'un élément documentaire essentiel, mais cette sauvegarde pourrait s'avérer extrêmement utile le jour où une configuration doit être restaurée. 1

Un administrateur doit :
- documenter et mettre à jour les fichiers de configuration opérationnels des unités réseau ;
- sauvegarder des copies du fichier de la configuration courante sur un serveur ou un disque.

L'IOS devrait également être sauvegardée sur un serveur local. Il est alors possible, le cas échéant, de recharger l'IOS en mémoire flash.

Activité de TP

Exercice : Gestion des fichiers du système d'exploitation du commutateur

Au cours de ce TP, les étudiants vont créer et vérifier une configuration de commutateur de base, sauvegarder l'IOS du commutateur sur un serveur TFTP, puis la restaurer.

Activité de TP

Exercice : Gestion des fichiers de configuration de démarrage du commutateur.Au cours de ce TP, les étudiants vont

créer et vérifier une configuration de commutateur de base, sauvegarder la configuration de démarrage du commutateur sur un serveur TFTP, puis la restaurer.

Activité de TP

Activité en ligne : Gestion des fichiers du système d'exploitation du commutateur

Au cours de ce TP, les étudiants vont déplacer les fichiers vers et depuis le commutateur en utilisant un serveur TFTP.

Activité de TP

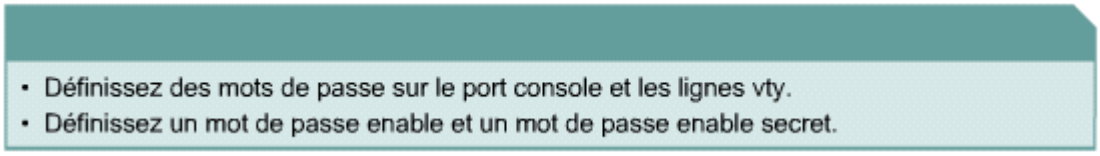
Activité en ligne : Gestion des fichiers de configuration de démarrage

Au cours de ce TP, les étudiants vont déplacer les fichiers vers et depuis le commutateur en utilisant un serveur TFTP.

6.2 Configuration du commutateur
6.2.8 Procédure de récupération de mots de passe 1900/2950

Pour des raisons de sécurité et de gestion, les mots de passe doivent être définis au niveau des lignes de console et des lignes vty. Il faut également définir un mot de passe « enable » et un mot de passe «enable secret». Cette procédure permet de garantir que seuls les utilisateurs autorisés ont accès aux modes utilisateur et privilégié du commutateur.

Dans certains cas, l'accès physique au commutateur est possible mais il n'est pas possible d'accéder au mode utilisateur ou privilégié car l'utilisateur ne connaît pas le mot de passe correspondant ou l'a oublié. 1



Il faut alors suivre une procédure de récupération de mots de passe.

Activité de TP

Activité en ligne : Procédure de récupération de mots de passe sur un commutateur de la gamme 2900

Au cours de ce TP, les étudiants vont apprendre à utiliser la procédure de récupération de mots de passe.

Activité de TP

Activité en ligne : Procédure de récupération de mots de passe sur un commutateur de la gamme 2900

Au cours de ce TP, les étudiants vont apprendre à utiliser la procédure de récupération de mots de passe.

6.2 Configuration du commutateur
6.2.9 Mise à jour du firmware 1900/2950

De nouvelles versions des images IOS et firmware sortent régulièrement avec des correctifs, de nouvelles fonctions et de meilleures performances. Si la sécurité du réseau peut être améliorée ou si ce même réseau peut mieux fonctionner grâce à une nouvelle version de l'IOS, il faut alors changer de version. 1

- Les images de l'IOS et du firmware sont mises à jour périodiquement avec correction des erreurs, introduction de nouvelles fonctions et amélioration des performances.
- La sécurité du réseau peut être améliorée, de même que son fonctionnement, avec une nouvelle version de l'IOS.

Pour mettre à niveau l'IOS, récupérez la nouvelle image sur un serveur local à partir de Cisco Connection Online (CCO) Software Center.

Activité de TP

Exercice : Mise à jour du firmware d'un commutateur de la gamme Catalyst 2950

Au cours de ce TP, les étudiants vont créer et vérifier une configuration de commutateur de base, puis mettre à niveau l'IOS et les fichiers HTML à partir d'un fichier fourni par le professeur.

Activité de TP

Activité en ligne : Mise à jour du firmware d'un commutateur de la gamme Catalyst 2950

Au cours de ce TP, les étudiants vont mettre à jour le firmware du commutateur.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Identification des principaux composants d'un commutateur Catalyst
- Surveillance de l'activité des commutateurs et de leur état à l'aide des indicateurs LED
- Examen des informations affichées, avec HyperTerminal, durant le démarrage du commutateur
- Utilisation des fonctions d'aide de l'interface de commande en ligne
- Liste des principaux modes de commande des commutateurs
- Connaissance des paramètres par défaut d'un commutateur Catalyst
- Définition d'une adresse IP et d'une passerelle par défaut pour le commutateur afin de pouvoir s'y connecter à travers un réseau et le gérer ainsi à distance
- Affichage des paramètres du commutateur avec un navigateur Web
- Configuration de la vitesse et du mode de transfert (half ou full duplex) des interfaces
- Examen et gestion de la table d'adresses MAC des commutateurs
- Configuration de la sécurité des ports
- Gestion des fichiers de configuration et des images IOS
- Exécution de la procédure de récupération de mots de passe sur un commutateur
- Mise à niveau de l'IOS d'un commutateur

Résumé

- Les commutateurs sont des ordinateurs dédiés et spécialisés qui contiennent une unité centrale de traitement (central processing unit - CPU), une mémoire à accès aléatoire (random access memory - RAM) et un système d'exploitation.
- Le panneau avant d'un commutateur comporte des témoins lumineux permettant de surveiller l'activité et les performances du système. Ces témoins sont des diodes électroluminescentes (LED).
- Les commutateurs ont plusieurs modes de commande. Le mode par défaut est le mode utilisateur (User EXEC mode).
- Lors de la première mise sous tension du commutateur, le fichier de configuration courante contient des données par défaut. Le commutateur a un nom par défaut : Switch. Aucun mot de passe n'est défini sur le port console ou les lignes de terminal virtuel (vty).
- Les commutateurs apprennent les adresses MAC des PC ou des stations de travail qui sont connectés à leurs ports de commutation en examinant l'adresse source des trames qui sont reçues sur ce port.

Vue d'ensemble

La notion de redondance dans un réseau est extrêmement importante, car elle permet aux réseaux de tolérer les pannes. Les topologies redondantes constituent une protection contre les temps d'arrêt dus à une panne au niveau d'une liaison, d'un port ou d'une unité du réseau. Les ingénieurs réseau sont souvent obligés de prendre des décisions difficiles qui nécessitent de comparer le coût de la redondance avec le besoin de disponibilité du réseau.

Les topologies redondantes basées sur des commutateurs et des ponts sont sensibles aux tempêtes de broadcast, aux transmissions de trames multiples et à l'instabilité de la base de données des adresses MAC. Par conséquent, la redondance d'un réseau nécessite une planification et une surveillance particulières pour fonctionner correctement.

Les avantages des réseaux commutés concernent les domaines de collision plus petits, la microsegmentation et le fonctionnement en mode full duplex. Les réseaux commutés offrent de meilleures performances.

La redondance dans un réseau est nécessaire car elle offre une protection contre les pertes de connectivité liées à la défaillance d'un composant individuel. Toutefois, pour obtenir cette redondance, des topologies physiques contenant des boucles sont souvent nécessaires. Les boucles de couche physique peuvent être à l'origine de problèmes sérieux dans les réseaux commutés. Les tempêtes de broadcast, les transmissions de trames multiples et l'instabilité de la base de données MAC (Media Access Control) peuvent rendre ces réseaux inutilisables.

Le protocole Spanning Tree est utilisé dans les réseaux commutés pour créer une topologie logique sans boucle à partir d'une topologie physique qui en comporte. Les liaisons, les ports et les commutateurs qui ne font pas partie de la topologie sans boucle active ne participent pas à l'acheminement des trames de données. Le protocole Spanning Tree est un outil efficace qui offre aux administrateurs réseau la sécurité d'une topologie redondante tout en éliminant le risque lié aux boucles de commutation.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Définir la redondance et son importance dans les réseaux
- Décrire les principaux composants d'une topologie réseau redondante
- Définir les tempêtes de broadcast et décrire leur impact sur les réseaux commutés
- Définir les transmissions de trames multiples et décrire leur impact sur les réseaux commutés
- Identifier les causes et les effets de l'instabilité de la base de données des adresses MAC
- Identifier les avantages et les risques d'une topologie redondante
- Décrire le rôle du Spanning Tree dans un réseau commuté à chemins redondants
- Identifier les principaux éléments du fonctionnement du Spanning Tree
- Décrire le processus de sélection du pont racine

- Énumérer les états Spanning Tree dans l'ordre
- Comparer le protocole Spanning Tree et le protocole Spanning Tree rapide

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
7.1	Topologies redondantes
7.2	Protocole Spanning Tree (STP)

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et	Dépannage	Technologie
			• Description du processus "spanning tree"

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
			• Description du processus "spanning tree"

7.1 Topologies redondantes

7.1.1 Redondance

La plupart des entreprises et des organismes comptent de plus en plus sur les réseaux informatiques pour gérer leur fonctionnement. L'accès aux serveurs de fichiers, aux bases de données, à l'Internet, aux intranets et aux extranets est essentiel au succès des entreprises. En cas de panne du réseau, la productivité est perdue et les clients ne sont pas satisfaits.

De plus en plus, les entreprises recherchent un temps de fonctionnement 24 heures sur 24 et 7 jours sur 7 pour leurs réseaux informatiques. Une fiabilité de 100 pour cent est peut être impossible à obtenir, mais beaucoup d'organisations se fixent un objectif de 99,99 pour cent. Ceci signifie qu'en moyenne le réseau n'est pas disponible pour une heure tous les 4000 jours, ou aproximativement 5,25 minutes par an.

Atteindre un tel objectif nécessite l'utilisation de réseaux extrêmement fiables. La fiabilité dans un réseau est obtenue par l'utilisation d'un équipement fiable et par la conception d'un réseau qui tolère les pannes et les défaillances. Le réseau est conçu pour reconverger rapidement, de sorte que la panne soit ignorée.

La tolérance aux pannes est obtenue par la redondance. La redondance est synonyme d'excès par rapport à ce qui est habituel et naturel. Comment la redondance contribue-t-elle à la fiabilité?

Supposez que votre voiture soit votre seul moyen de vous rendre au travail. Si cette voiture tombe en panne, il vous est impossible de vous rendre au travail jusqu'à ce qu'elle soit réparée et restituée.

Si votre voiture est en panne et n'est plus disponible en moyenne un jour sur dix, elle est utilisée à 90 % du temps. Vous pouvez vous rendre au travail pendant neuf jours sur dix. La fiabilité est donc de 90 %.

Acheter une autre voiture est un moyen d'améliorer les choses. Vous n'avez pas besoin de deux voitures pour vous rendre au travail. Toutefois, en cas de panne du premier véhicule, vous disposez d'une solution de secours du fait de la redondance. La possibilité d'aller au travail ne dépend plus d'un seul véhicule.

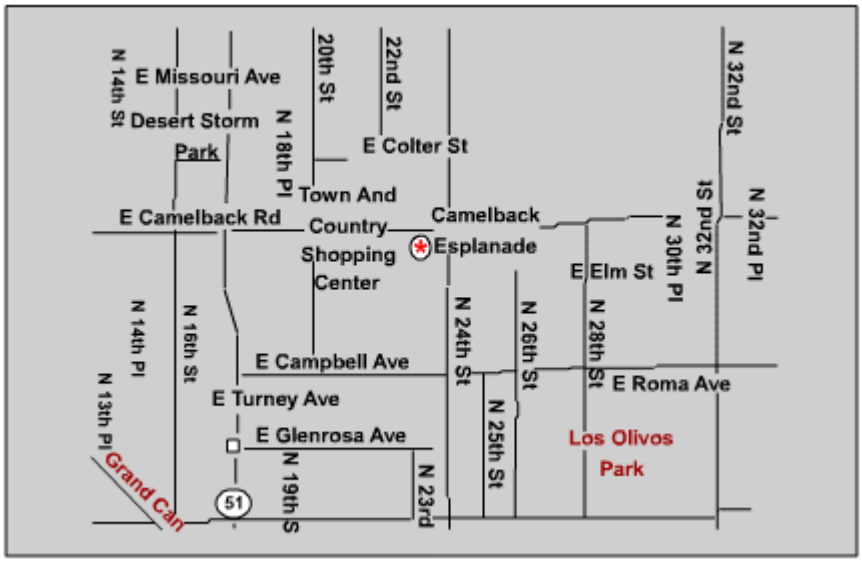
Les deux voitures peuvent devenir inutilisables en même temps, 1 jour sur 100. L'achat d'un deuxième véhicule a amélioré la fiabilité qui est passée à 99 %. 1

7.1 Topologies redondantes

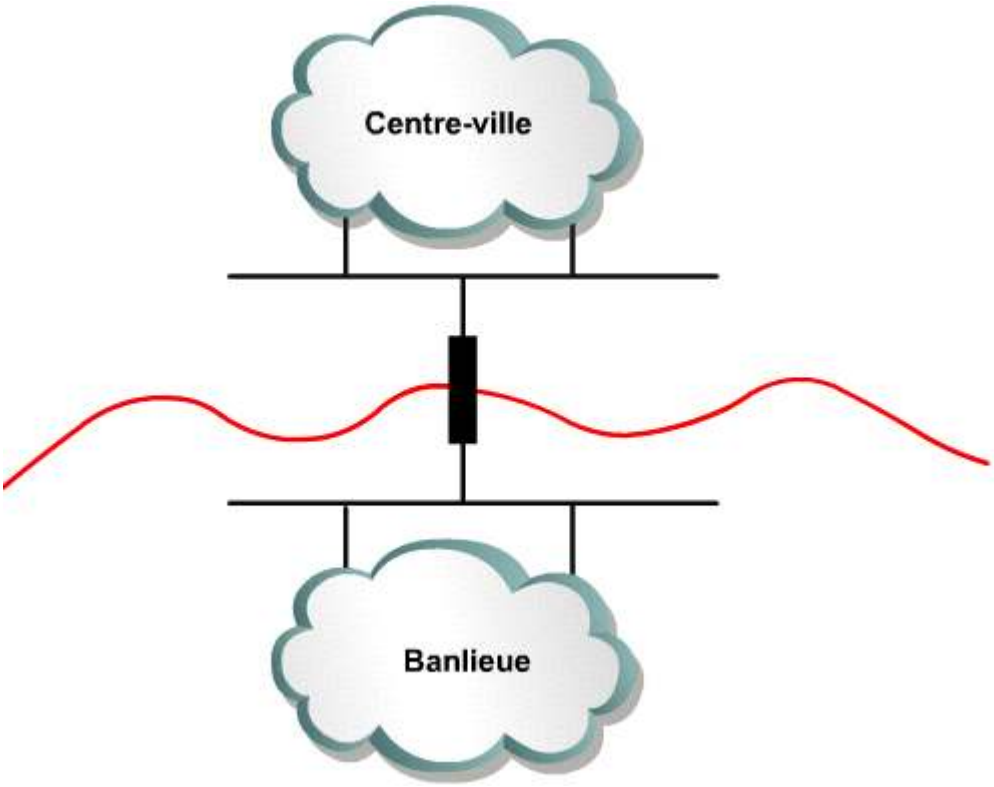
7.1.2 Topologies redondantes

L'un des objectifs des topologies redondantes est d'éliminer les risques de pannes du réseau provoquées par un composant unique. Pour améliorer leur fiabilité, tous les réseaux ont besoin de redondance.

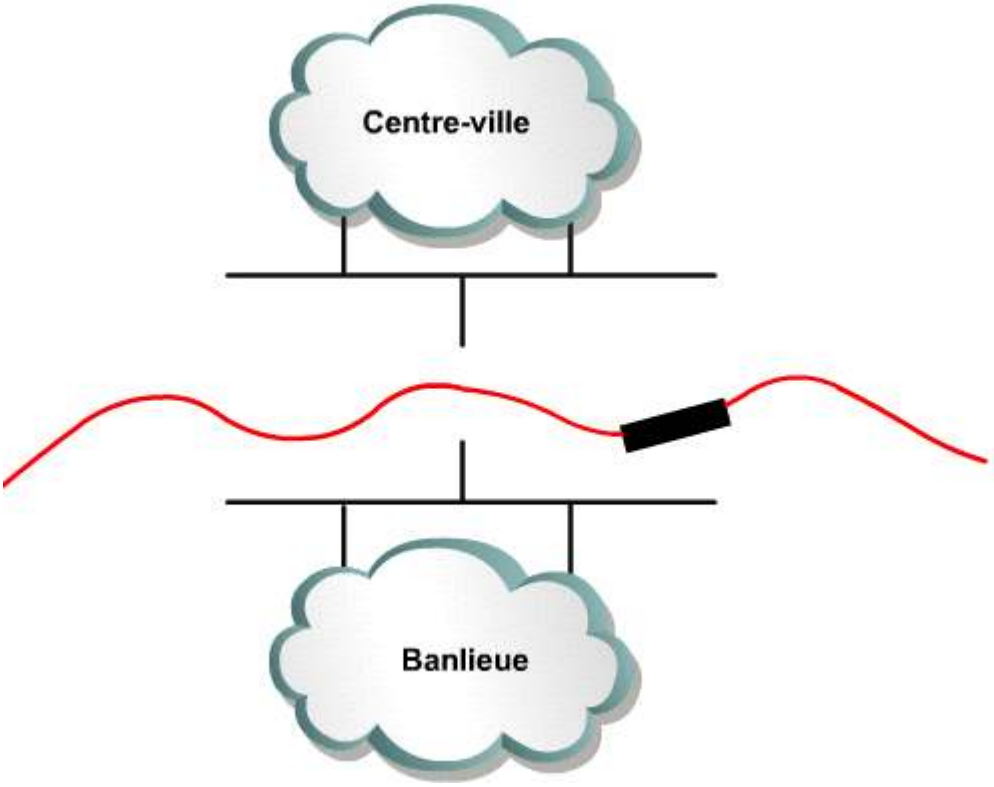
Un réseau de routes est un bon exemple de topologie redondante. Lorsqu'une route est fermée pour cause de travaux, il y a des chances pour qu'une autre route conduise à la même destination. 1



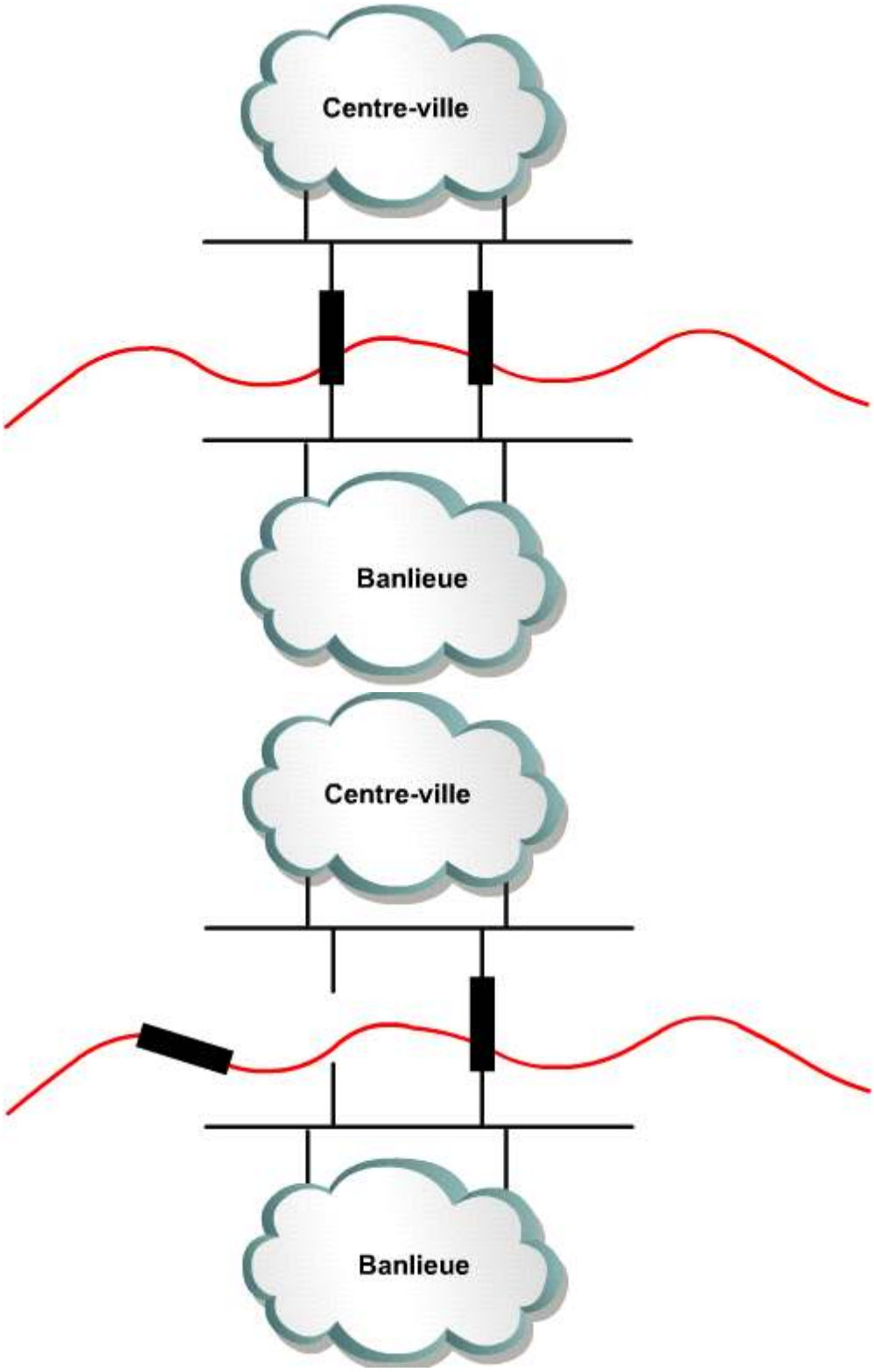
Prenons l'exemple d'une communauté de banlieu séparée du centre de la ville par une rivière. S'il n'existe qu'un seul pont pour traverser la rivière, un seul itinéraire permet d'accéder à la ville. La topologie n'a pas de redondance. 2



Si le pont est inondé ou endommagé à la suite d'un accident, il devient impossible de se rendre dans le centre de la ville par ce pont. 3



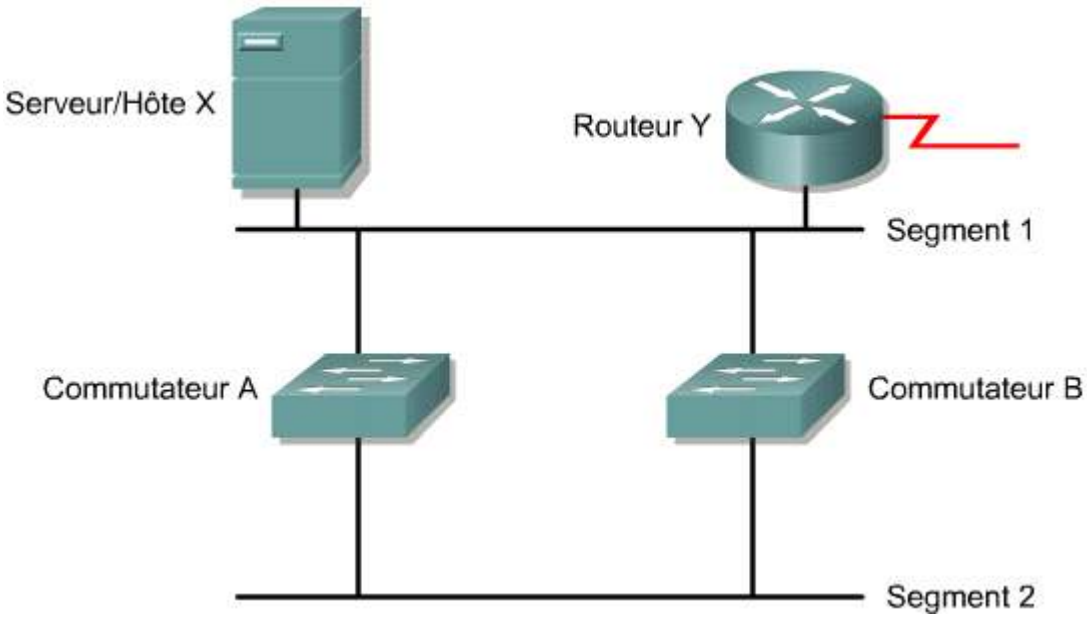
La construction d'un second pont sur la rivière crée une topologie redondante. La banlieue n'est plus coupée du centre de la ville si l'un des ponts devient infranchissable. 4 5



7.1 Topologies redondantes

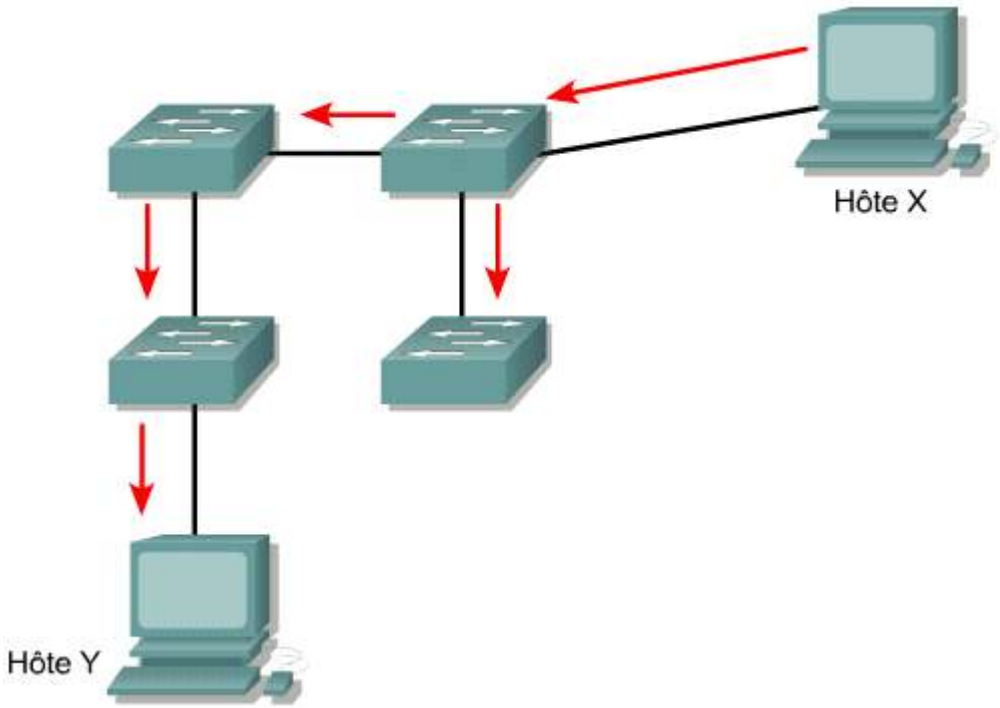
7.1.3 Topologies commutées redondantes

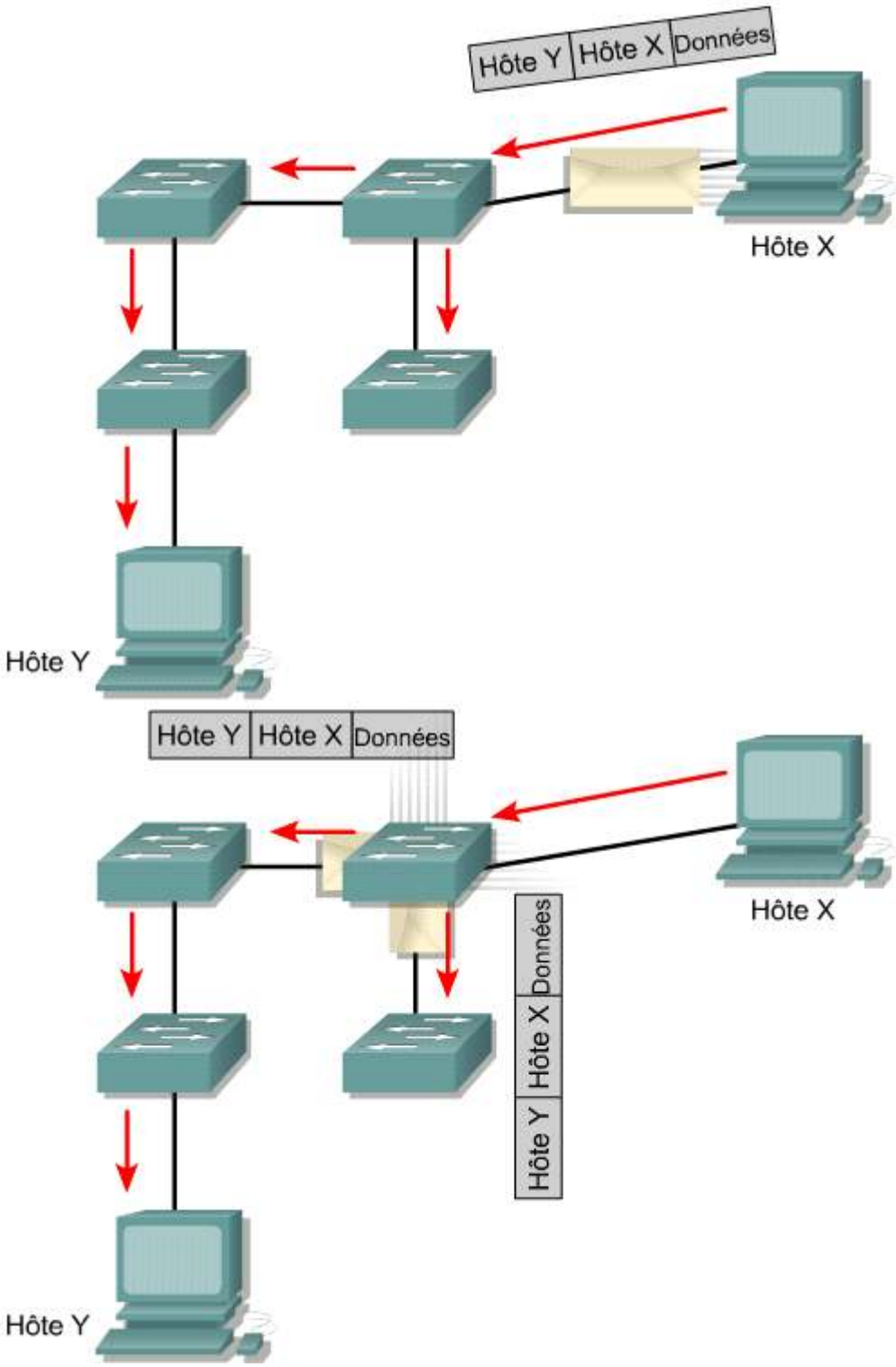
Les réseaux possédant des routes et des équipements redondants permettent un temps de fonctionnement supérieur. Les topologies redondantes éliminent les points de panne isolés. Si une panne survient sur une route ou une unité, la route ou l'unité redondante peut prendre le relais pour les travaux en cours. 1

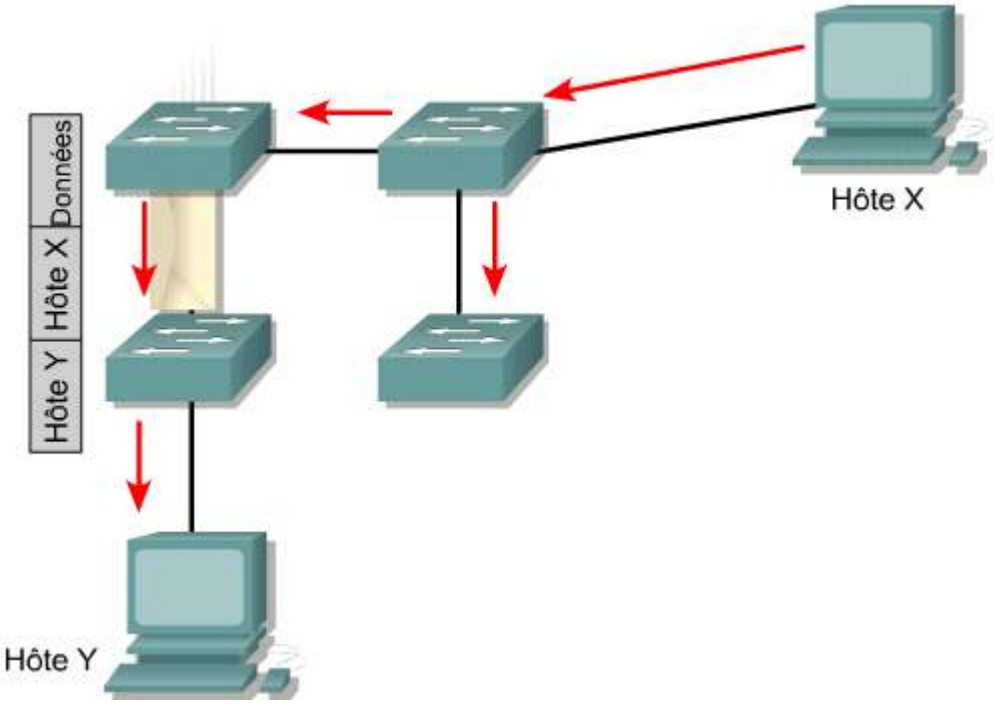


Si le commutateur A tombe en panne, le trafic peut quand même être acheminé du segment 2 au segment 1 jusqu'au routeur par le commutateur B.

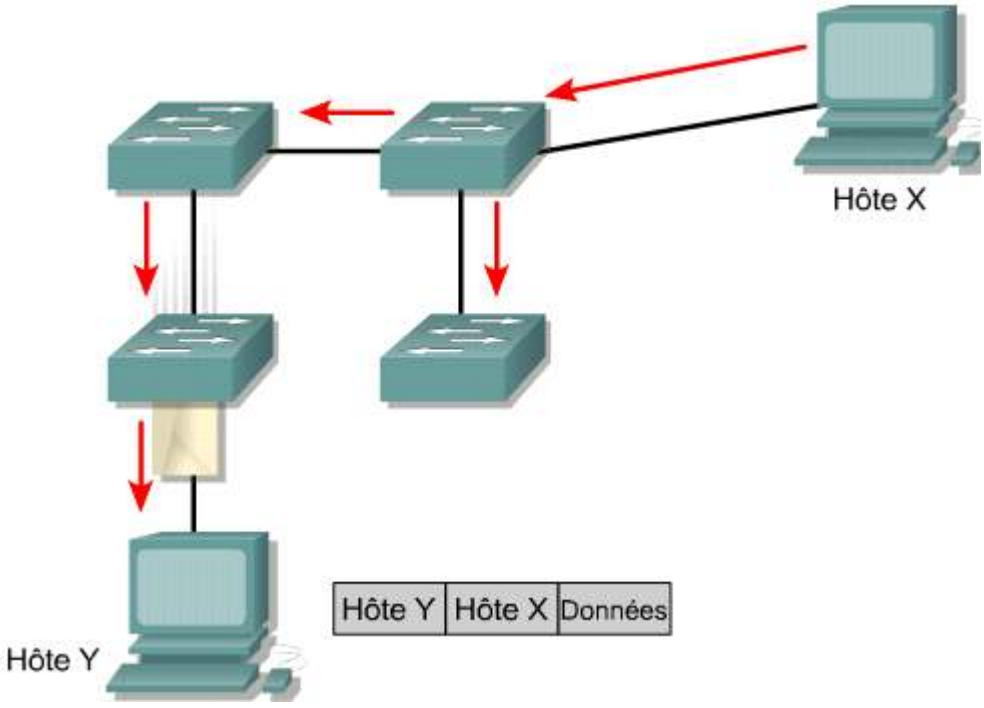
Les commutateurs apprennent les adresses MAC des équipements du réseau, ainsi que les ports sur lesquels ils sont connectés, de sorte que les données puissent être correctement acheminées vers leur destination. Les commutateurs vont diffuser, à tous leurs ports, les trames à destination d'équipements inconnus, jusqu'à ce qu'ils apprennent les adresses MAC et le port d'accès de ces équipements. 2



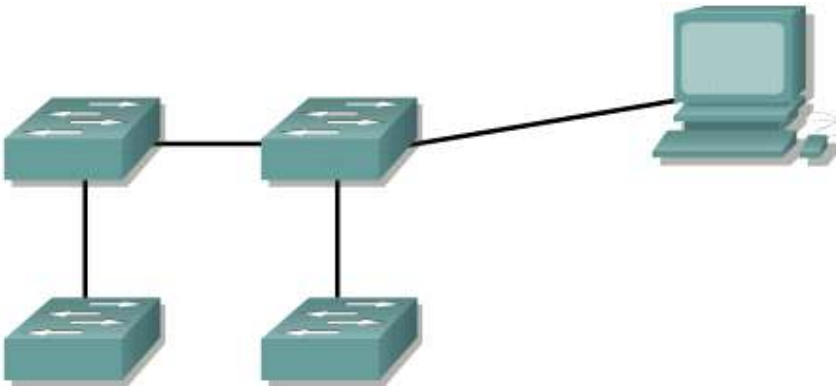

Hôte Y
Hôte X
Données
Hôte X
Hôte Y
Hôte Y
Hôte X
Données
Hôte X
Hôte Y
Hôte Y
Hôte X
Données

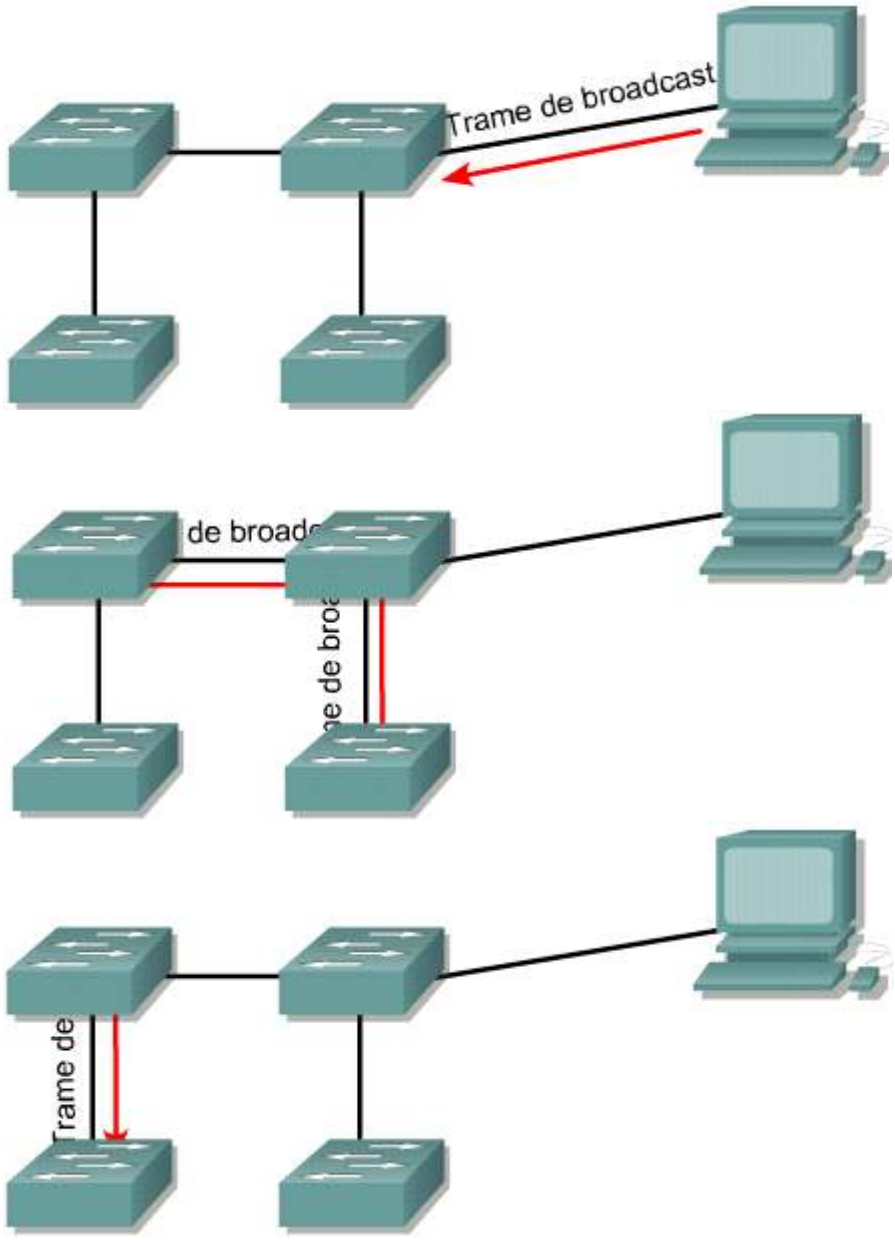


f



Les broadcasts et les multicasts sont aussi diffusés sur tous les ports. 3





Une topologie commutée redondante peut provoquer des tempêtes de broadcast, des copies de trames multiples et des problèmes d'instabilité dans la table des adresses MAC.

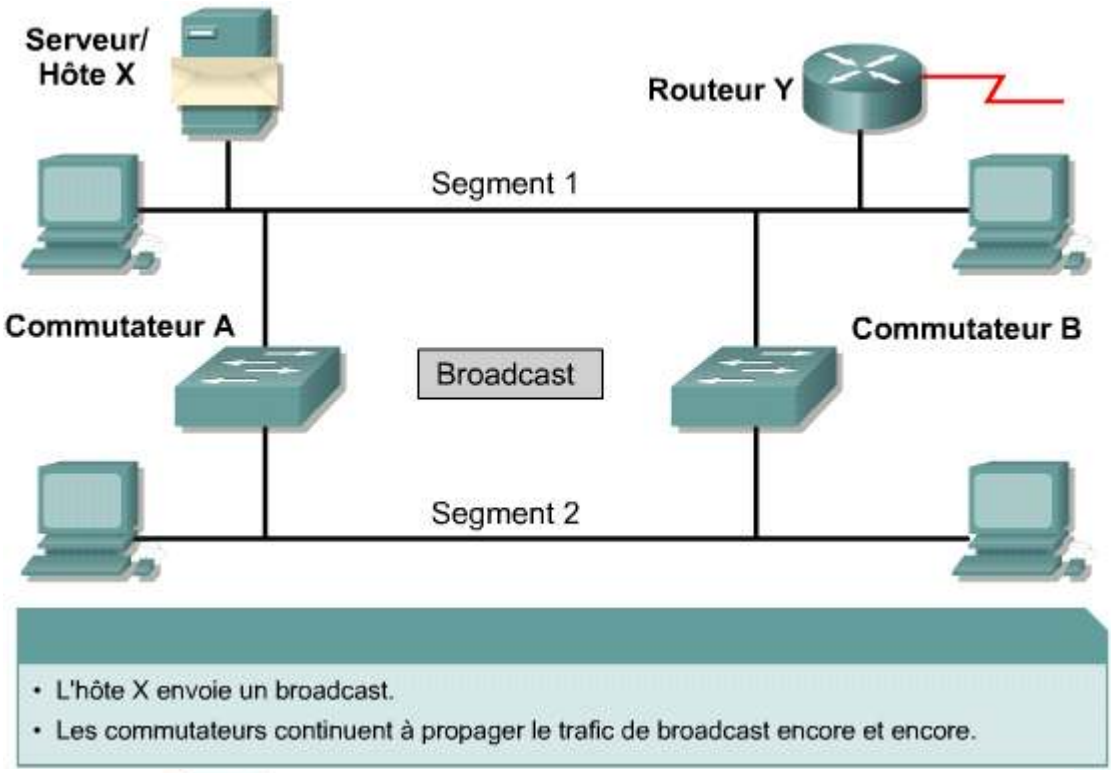
7.1 Topologies redondantes

7.1.4 Tempêtes de broadcast

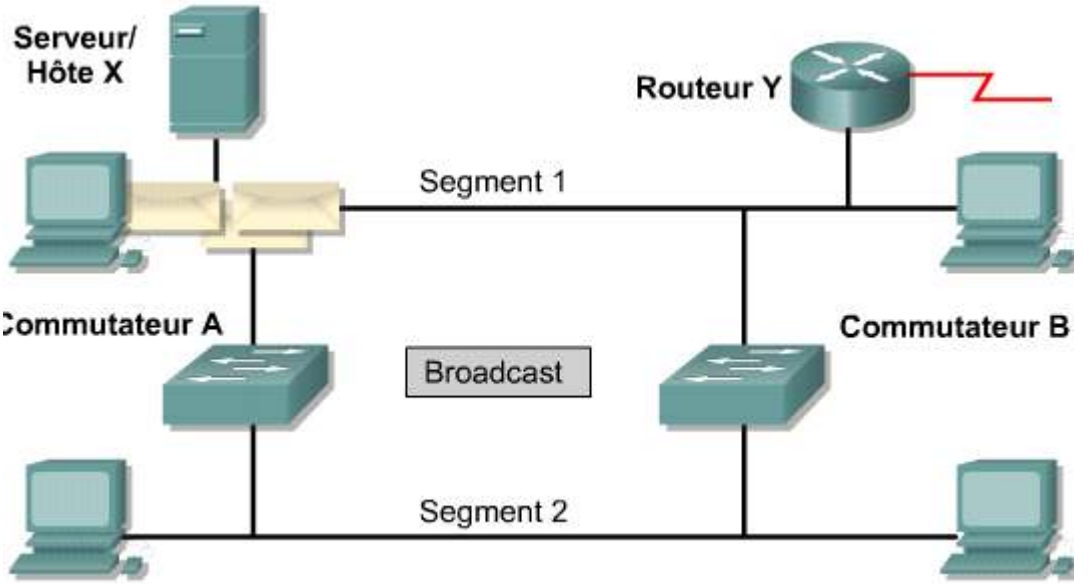
Les messages de diffusion broadcast et multicast peuvent engendrer des problèmes dans un réseau commuté.

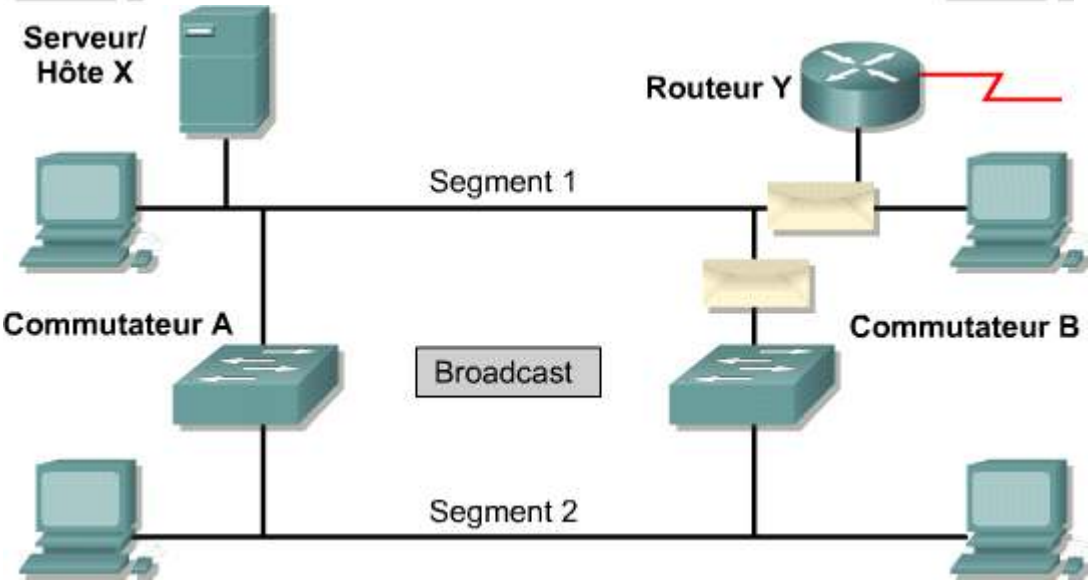
Les messages multicast sont traités comme les messages broadcast par les commutateurs. Les trames de broadcast et de multicast sont diffusées sur tous les ports, à l'exception du port sur lequel elles ont été reçues.

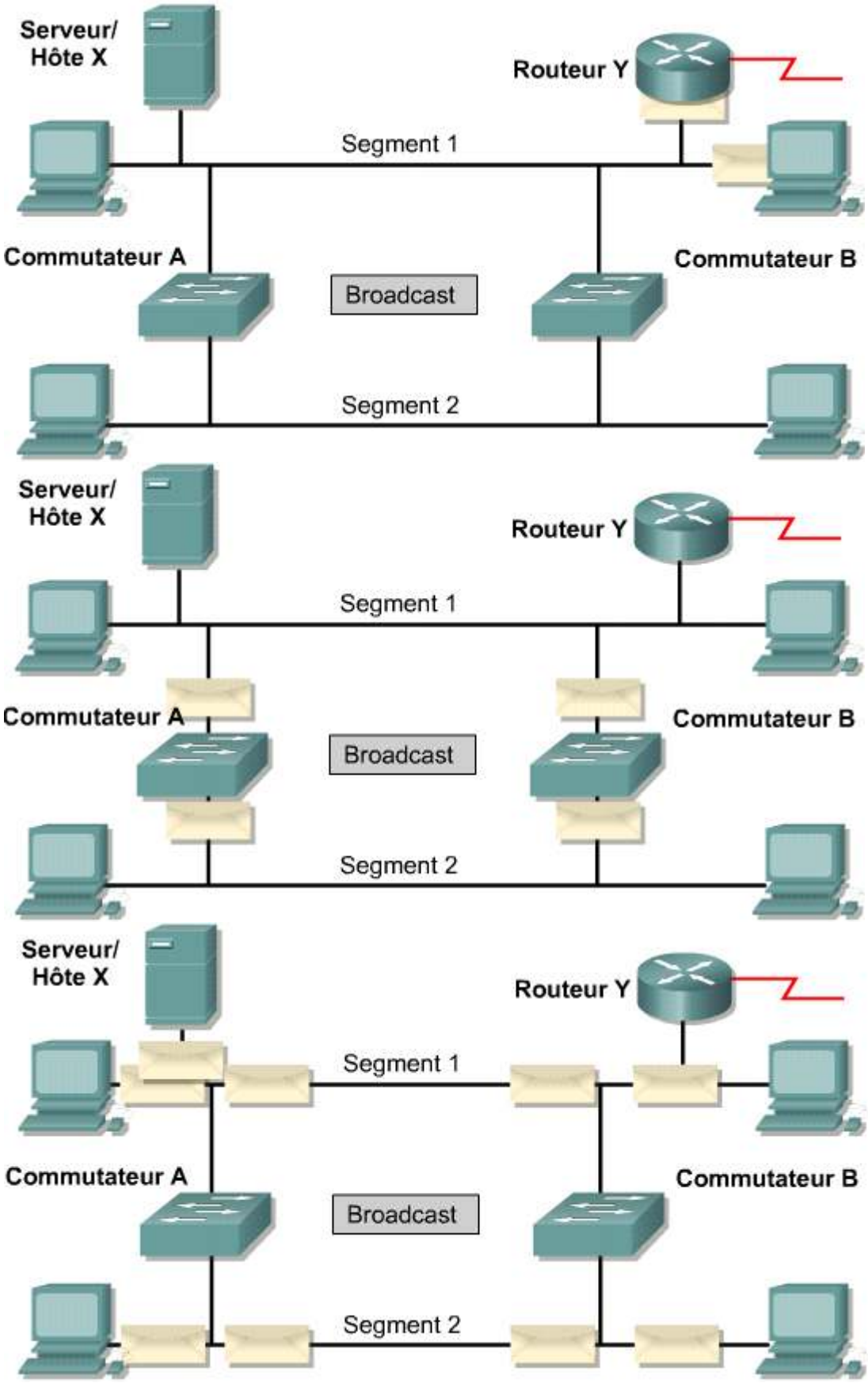
Si l'hôte X envoie un message de broadcast, comme une requête ARP pour l'adresse de couche 2 du routeur, le commutateur A transmet ce message de broadcast sur tous les ports. Le commutateur B, placé sur le même segment, transmet également tous les messages de broadcast. Le commutateur B voit tous les messages de broadcast transmis par le commutateur A, et réciproquement. Le commutateur A voit les messages de broadcast et les fait suivre. Le commutateur B voit les messages de broadcast et les fait suivre. 1

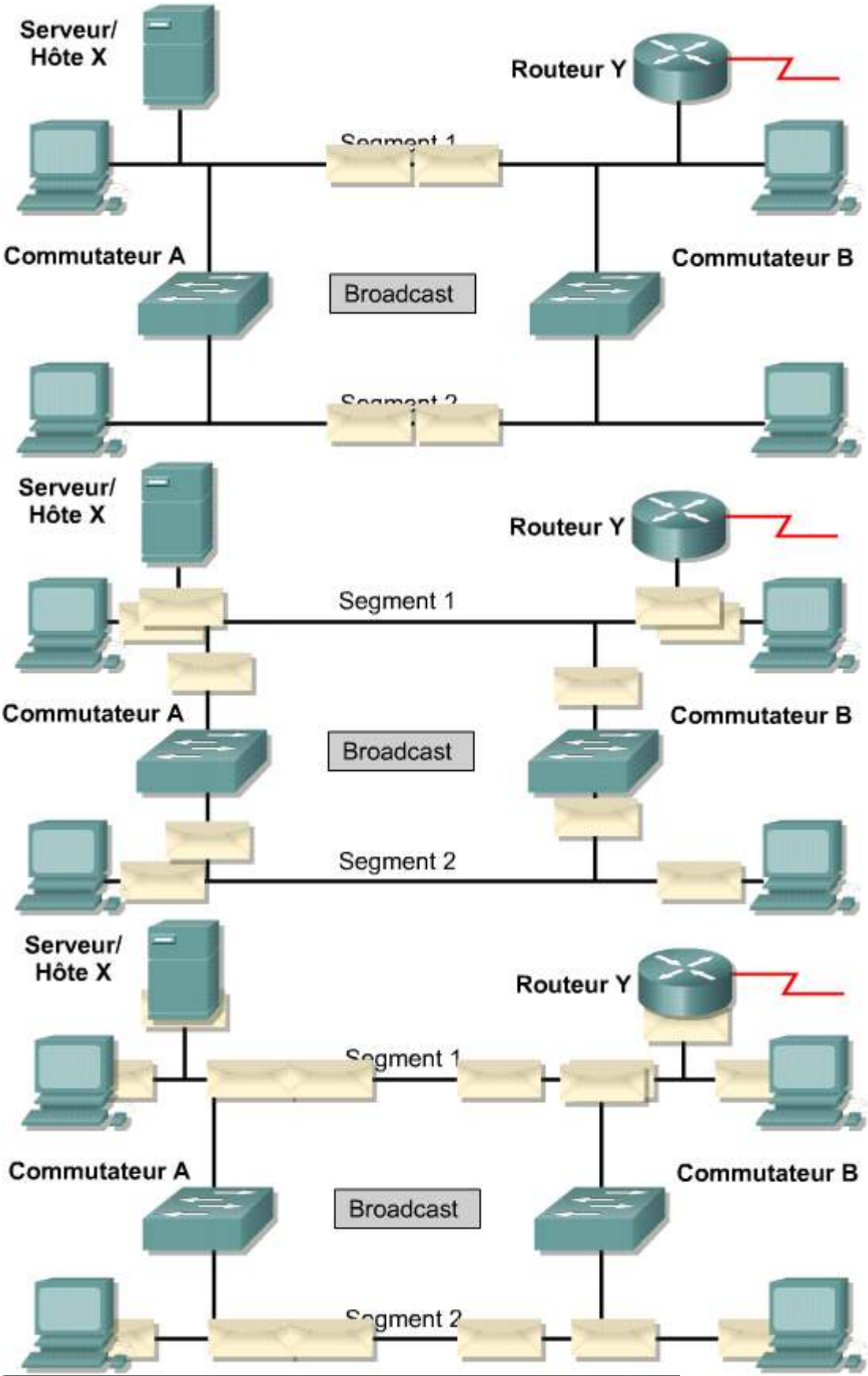


- L'hôte X envoie un broadcast.
- Les commutateurs continuent à propager le trafic de broadcast encore et encore.






Serveur/
Hôte X
Routeur Y
Segment 1
Commutateur A
Commutateur B
Broadcast
Segment 2
Serveur/
Hôte X
Routeur Y
Segment 1
Commutateur A
Commutateur B
Broadcast
Segment 2
Serveur/
Hôte X
Routeur Y
Segment 1
Commutateur A
Commutateur B
Broadcast
Segment 2



Fenêtre contextuelle

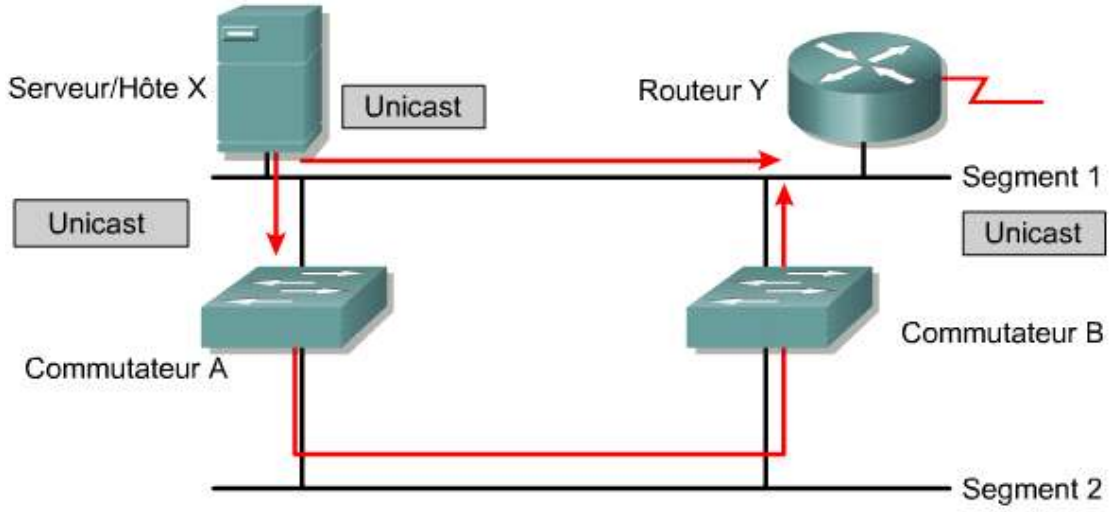
Cet exemple représente uniquement des trames de broadcast qui sont transmises en continu à l'aide de commutateurs. Cela provoque une tempête de broadcast, car les trames continueront d'être acheminées tant que le commutateur disposera d'un endroit vers lequel les transmettre. Toutes les autres trames ne sont pas représentées pour simplifier l'exemple.

Les commutateurs continuent à propager le trafic de broadcast encore et encore. C'est ce que l'on appelle une tempête de broadcast. Cette tempête de broadcast se poursuit jusqu'à ce que l'un des commutateurs soit déconnecté. Les commutateurs et les unités d'extrémité sont tellement occupés à traiter les messages de broadcast que le trafic utilisateur ne peut pas être acheminé. Le réseau semble être en panne ou extrêmement ralenti.

7.1 Topologies redondantes

7.1.5 Transmissions de trames multiples

Dans un réseau commuté redondant, il est possible pour une unité d'extrémité de recevoir plusieurs trames. 1



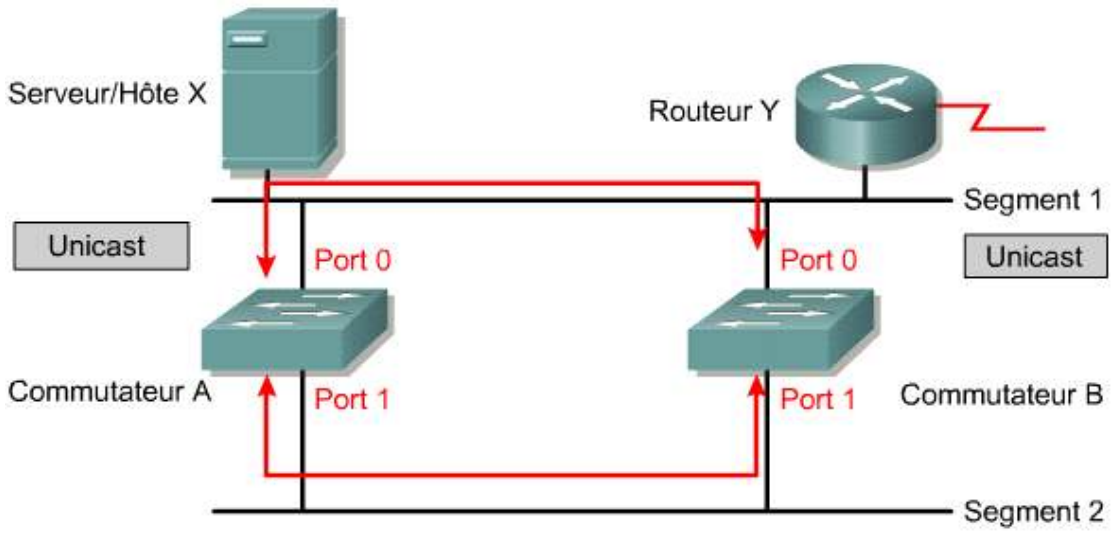
Supposez que l'adresse MAC du routeur Y ait été supprimée par les deux commutateurs, à cause d'un dépassement du temps de rafraîchissement. Supposez également que l'hôte X dispose encore de l'adresse MAC du routeur Y dans sa mémoire cache ARP et envoie une trame unicast au routeur Y. Le routeur reçoit la trame, car il figure sur le même segment que l'hôte X.

Le commutateur A ne dispose pas de l'adresse MAC du routeur Y et diffuse donc la trame sur ses ports. Le commutateur B ne connaît pas non plus le port du routeur Y. Il diffuse la trame qu'il a reçue et le routeur Y reçoit donc plusieurs copies de la même trame. Cela est le résultat d'opérations inutiles sur toutes les unités.

7.1 Topologies redondantes

7.1.6 Instabilité de la base de données MAC (Media Access Control)

Dans un réseau commuté redondant, il est possible pour les commutateurs d'apprendre des informations erronées. Un commutateur peut apprendre qu'une adresse MAC est associée à un certain port alors qu'elle correspond en fait à un autre port. 1



Dans cet exemple, l'adresse MAC du routeur Y ne figure pas dans la table d'adresses MAC des commutateurs.

L'hôte X envoie une trame au routeur Y. Les commutateurs A et B apprennent l'adresse MAC de l'hôte X sur le port 0.

La trame destinée au routeur Y est diffusée sur le port 1 des deux commutateurs. Les commutateurs A et B voient cette information sur le port 1 et considèrent à tort que l'adresse MAC de l'hôte X est associée au port 1. Lorsque le routeur Y envoie une trame à l'hôte X, les commutateurs A et B reçoivent également la trame et l'envoient sur le port 1. Cela est inutile, mais les commutateurs ont reçu une mauvaise information, à savoir que l'hôte X était sur le port 1.

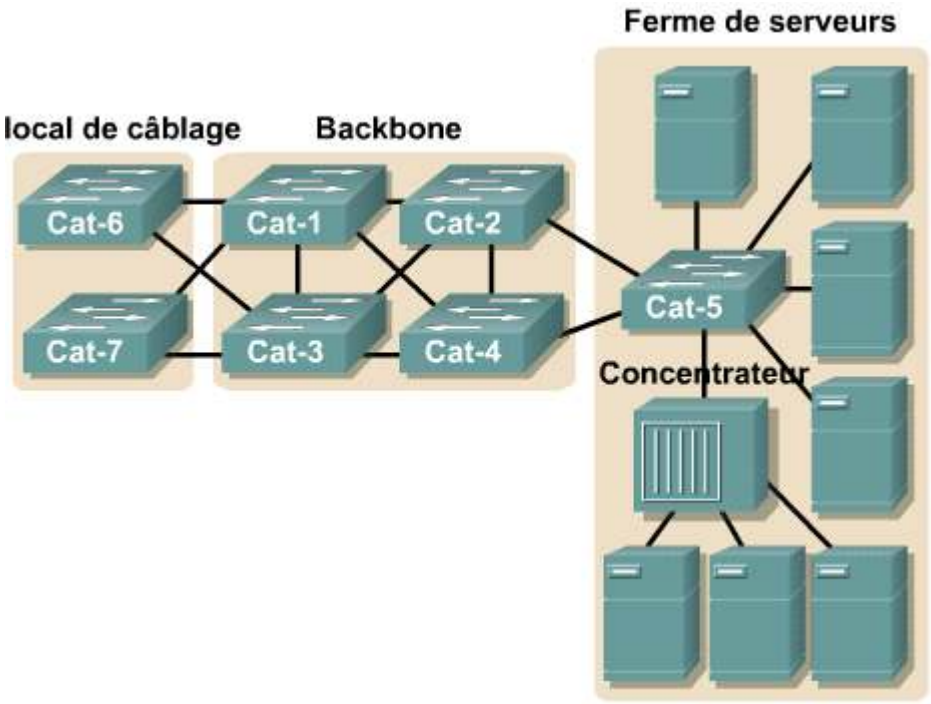
Dans cet exemple, la trame unicast du routeur Y vers l'hôte X est emprisonnée dans une boucle.

7.2 Protocole Spanning Tree (STP)

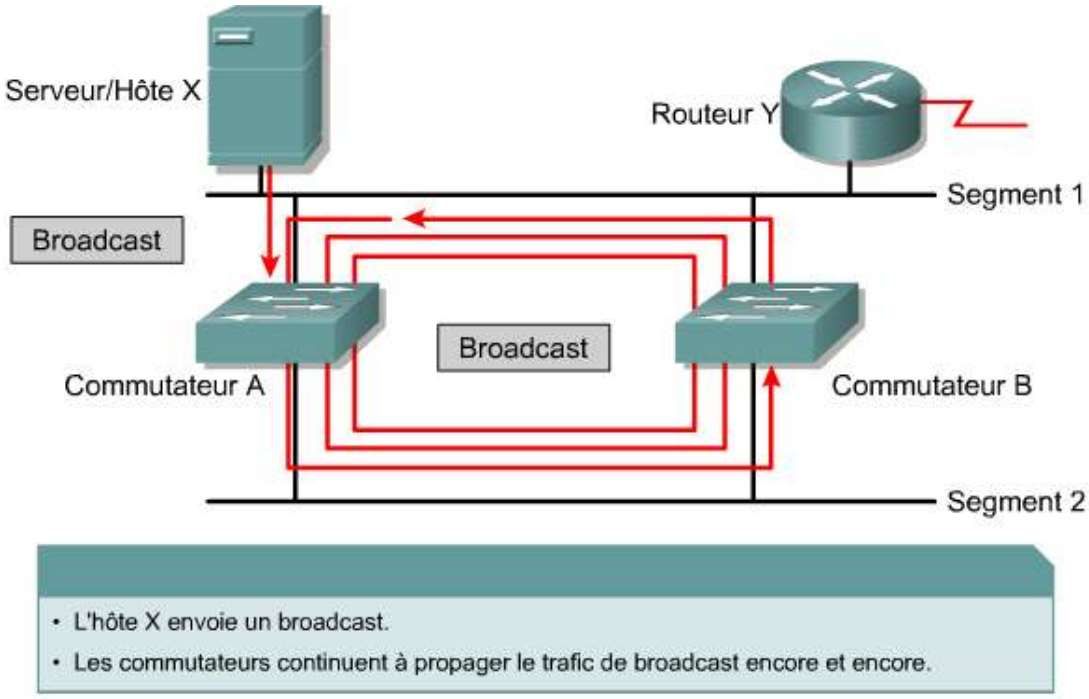
7.2.1 Topologie redondante et Spanning Tree

Les topologies réseau redondantes sont conçues pour garantir le fonctionnement continu des réseaux en cas de défaillance d'un composant unique. Le risque d'interruption du travail est diminué pour les utilisateurs, car le réseau continue à fonctionner. Toute interruption provoquée par une panne doit être aussi courte que possible.

La fiabilité est accrue par la redondance. Un réseau qui est basé sur des commutateurs ou des ponts introduit des liaisons redondantes entre ces commutateurs ou ces ponts pour surmonter la panne d'une liaison unique. Ces connexions introduisent des boucles physiques dans le réseau. 1 Ces boucles de pontage sont créées de sorte qu'en cas d'échec d'une liaison, une autre liaison puisse prendre le relais et acheminer le trafic.



Les commutateurs diffusent le trafic sur tous les ports lorsque celui-ci est pour une destination encore inconnue. Le trafic broadcast et multicast est aussi transmis sur tous les ports, à l'exception du port sur lequel il est arrivé. 2



L'en-tête de couche 2 ne comporte pas de durée de vie. Si une trame est envoyée dans une topologie de commutateurs en boucle de couche 2, elle peut tourner indéfiniment. La bande passante est gaspillée et le réseau est inutilisable.

Au niveau de la couche 3, la durée de vie est décrémentée et le paquet est supprimé lorsque la valeur de durée de vie atteint 0. Cela crée un dilemme. Une topologie physique qui contient des boucles de pontage ou de commutation est nécessaire sur le plan de la fiabilité, mais un réseau commuté ne peut pas avoir de boucles.

La solution consiste à autoriser les boucles physiques et à créer une topologie logique sans boucle. [3] Pour cette topologie logique, le trafic destiné à la ferme de serveurs connectée à Cat-5 à partir de toute station de travail utilisateur reliée à Cat-4 est acheminé par Cat-1 et Cat-2, et ce même s'il existe une connexion physique directe entre Cat-5 et Cat-4.

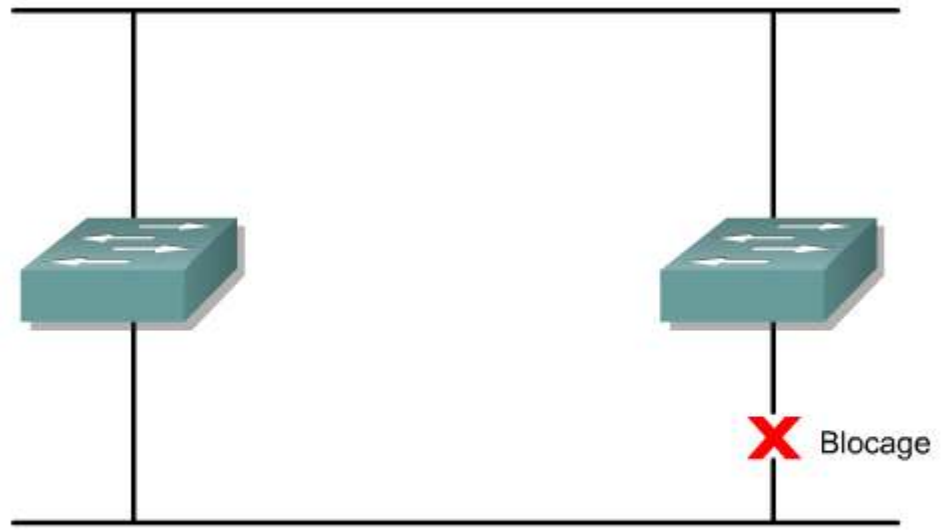
La topologie logique sans boucle créée est appelée un arbre. Cette topologie logique, en étoile étendue ou non, correspond donc à l'arbre de recouvrement (Spanning Tree) du réseau. Il s'agit d'un arbre de recouvrement car toutes les unités du réseau sont accessibles ou «recouvertes».

L'algorithme utilisé pour créer cette topologie logique sans boucle est l'algorithme «spanning tree». La convergence de cet algorithme peut prendre du temps. Un nouvel algorithme appelé algorithme spanning tree «rapide» (RSTP) est introduit pour réduire la durée de calcul d'une topologie logique sans boucle par un réseau.

7.2 Protocole Spanning Tree (STP)

7.2.2 Protocole Spanning Tree

Les ponts et les commutateurs Ethernet peuvent utiliser le protocole Spanning Tree IEEE 802.1d et utiliser l'algorithme «spanning tree» pour développer un réseau de couche 2 sans boucle utilisant le plus court chemin. [1]



Fournit une topologie réseau redondante sans boucle en plaçant certains ports en état bloqué.

Le plus court chemin est basé sur les coûts de liaison cumulés. Les coûts de liaison sont basés sur la vitesse de la liaison. 2

Vitesse de liaison	Coût (spéc. IEEE révisée)	Coût (spéc. IEEE précédente)
10 Gbits/s	2	1
1 Gbits/s	4	1
100 Mbits/s	19	10
10 Mbits/s	100	100

Le protocole Spanning Tree établit un nœud racine, appelé pont racine. Il crée une topologie comportant un chemin vers chaque nœud du réseau. L'arbre obtenu part du pont racine. Les liaisons redondantes qui ne font pas partie de l'arbre du plus court chemin sont bloquées.

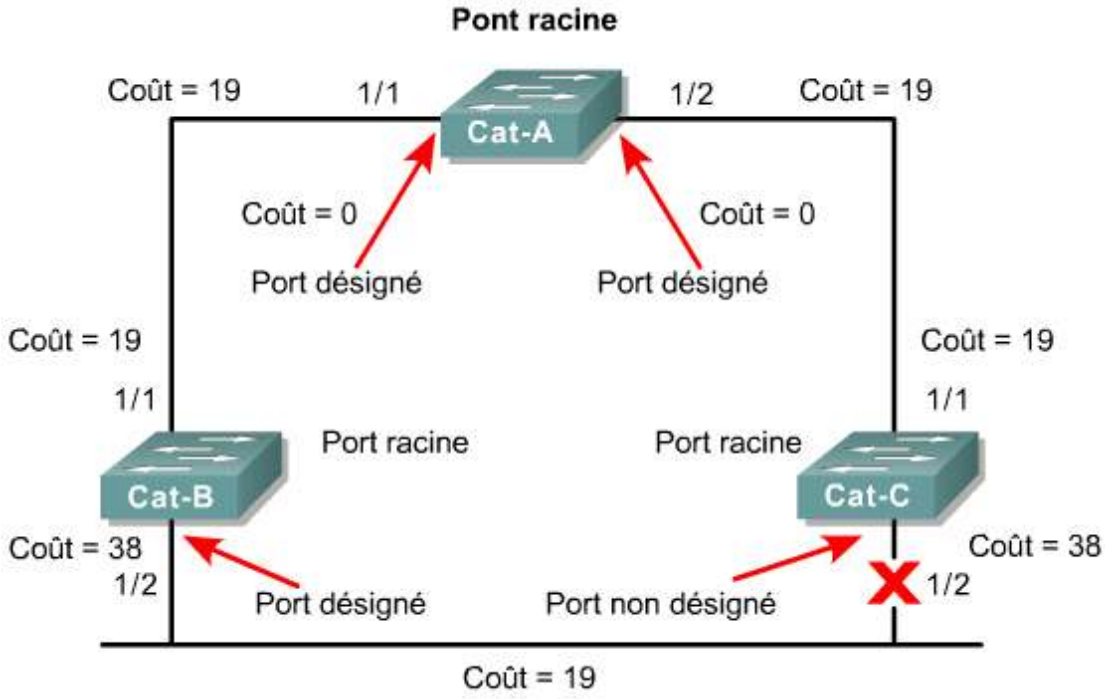
C'est le blocage de certains chemins qui permet la création d'une topologie de couche 2 sans boucle. Les trames de données reçues sur les liaisons bloquées sont abandonnées.

Le protocole Spanning Tree requiert des unités réseau qu'elles échangent des messages pour détecter les boucles de pontage. Les liaisons qui génèrent une boucle sont bloquées.

Le message qu'un commutateur envoie, permettant la formation d'une topologie logique sans boucle, est appelé unité BPDU (Bridge Protocol Data Unit). Les unités BPDU continuent d'être reçues sur les ports bloqués. Ainsi, si une panne survient sur un chemin ou un équipement actif, un nouveau Spanning Tree peut être calculé.

Les unités BPDU contiennent suffisamment d'informations pour que tous les commutateurs puissent effectuer les opérations suivantes:

- Sélectionner un commutateur devant servir de racine pour le Spanning Tree
- Calculer le chemin le plus court entre lui-même et le commutateur racine
- Désigner un des commutateurs comme étant le plus proche de la racine, pour chaque segment LAN. Ce pont est appelé «commutateur désigné». Le commutateur désigné gère toutes les communications émises sur le réseau LAN en direction du pont racine.
- Choisir un de ses ports comme port racine pour chacun des commutateurs non racine. Il s'agit de l'interface qui fournit le meilleur chemin vers le commutateur racine.
- Sélectionner des ports appartenant au Spanning Tree: les ports désignés. Les ports non désignés sont bloqués. 3



-

Activité de média interactive

Pointer-cliquer: Protocole STP (Spanning Tree Protocol)

À la fin de cette activité, l'étudiant en saura plus sur le concept de protocole Spanning Tree.

7.2 Protocole Spanning Tree (STP)

7.2.3 Fonctionnement du Spanning Tree

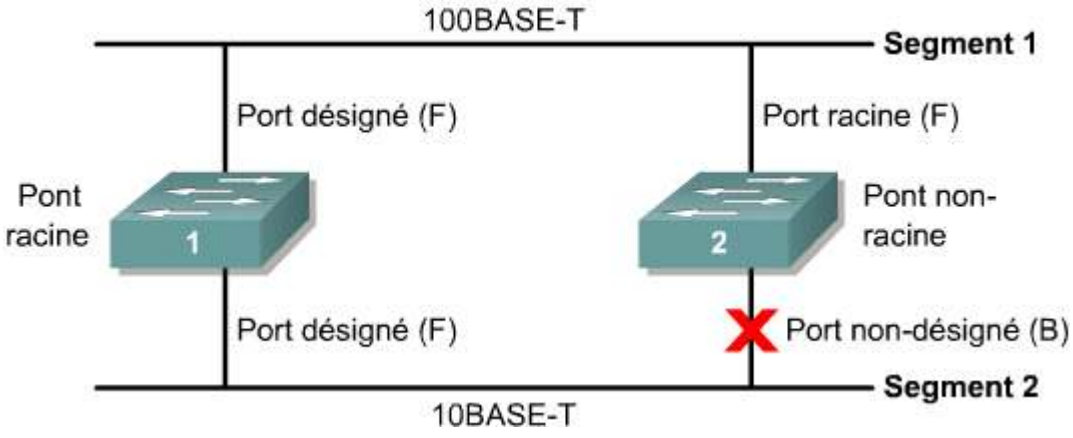
Lorsque le réseau a été stabilisé, il a convergé et il existe un Spanning Tree par réseau.

En conséquence, chaque réseau commuté contient les éléments suivants:

- Un pont racine par réseau
- Un port racine par pont non racine
- Un port désigné par segment
- Des ports non désignés inutilisés

Les ports racine et les ports désignés sont utilisés pour la transmission (F) du trafic de données.

Les ports non désignés suppriment le trafic de données. Ces ports sont appelés ports de blocage (B) ou de suppression. [1]

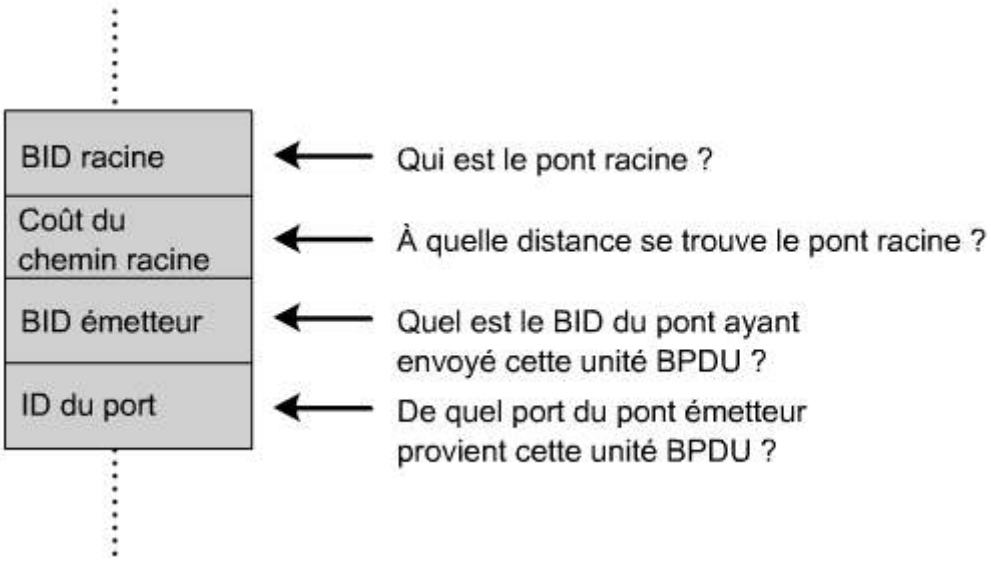


7.2 Protocole Spanning Tree (STP)

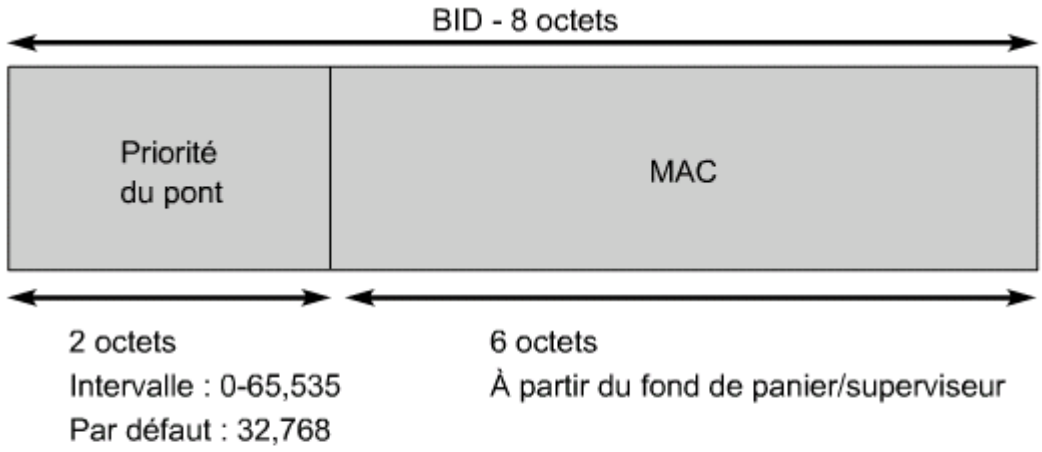
7.2.4 Sélection du pont racine

La première décision que tous les commutateurs du réseau doivent prendre est d'identifier le pont racine. La position du pont racine dans un réseau a un impact sur le flux du trafic.

Lorqu'un commutateur est activé, l'algorithme « spanning tree » est utilisé pour identifier le pont racine. Des unités BPDU sont envoyées avec l'ID de pont (BID). 1



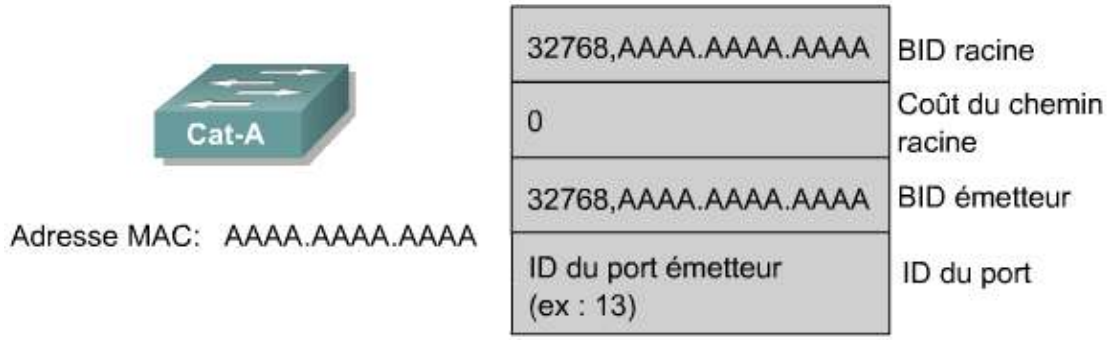
Le BID est constitué d'une priorité de pont égale à 32768 par défaut ainsi que de l'adresse MAC du commutateur. 2



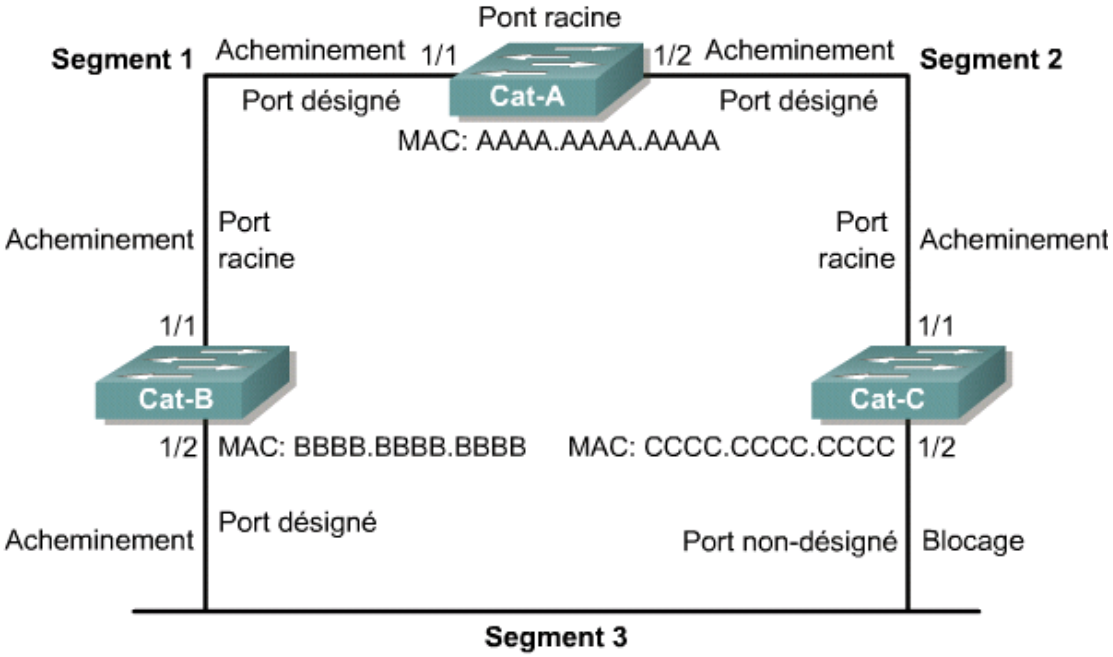
- L'ID du pont (BID) est utilisé pour identifier chaque pont/commutateur.
- Le BID est utilisé pour déterminer le centre du réseau, par rapport à STP, à savoir le pont racine.

Par défaut, les unités BPDU sont envoyées toutes les deux secondes.

Quand un commutateur démarre, il assume qu'il est le commutateur racine et envoie les BPDU contenant l'adresse Mac du commutateur à la fois dans les champs racine et BID de l'expéditeur. Ces BPDU sont considérées inférieures car elles sont générées par un commutateur ayant perdu sa connexion au pont racine. Le commutateur en question transmet les BPDU contenant l'information qu'il est maintenant le pont racine ainsi que le pont désigné. 3



Tous les commutateurs voient les BID envoyés. Lorsqu'un commutateur reçoit une unité BPDU avec un BID de racine inférieur, il le remplace dans les unités BPDU envoyées. Tous les ponts voient cela et désignent le pont dont la valeur BID est la plus petite comme pont racine. 4



Un administrateur réseau peut avoir une influence sur cette décision s'il paramètre une valeur de priorité de commutateur inférieure à la valeur par défaut, ce qui diminue la valeur BID. Mais un tel paramétrage nécessite une bonne compréhension du flux de trafic sur le réseau.

Activité de TP

Exercice: Sélection du pont racine

Au cours de ce TP, l'étudiant va créer une configuration de commutateur de base et la vérifier. Il va également déterminer le commutateur sélectionné comme commutateur racine avec les paramètres d'usine par défaut.

Activité de TP

Activité en ligne: Sélection du pont racine

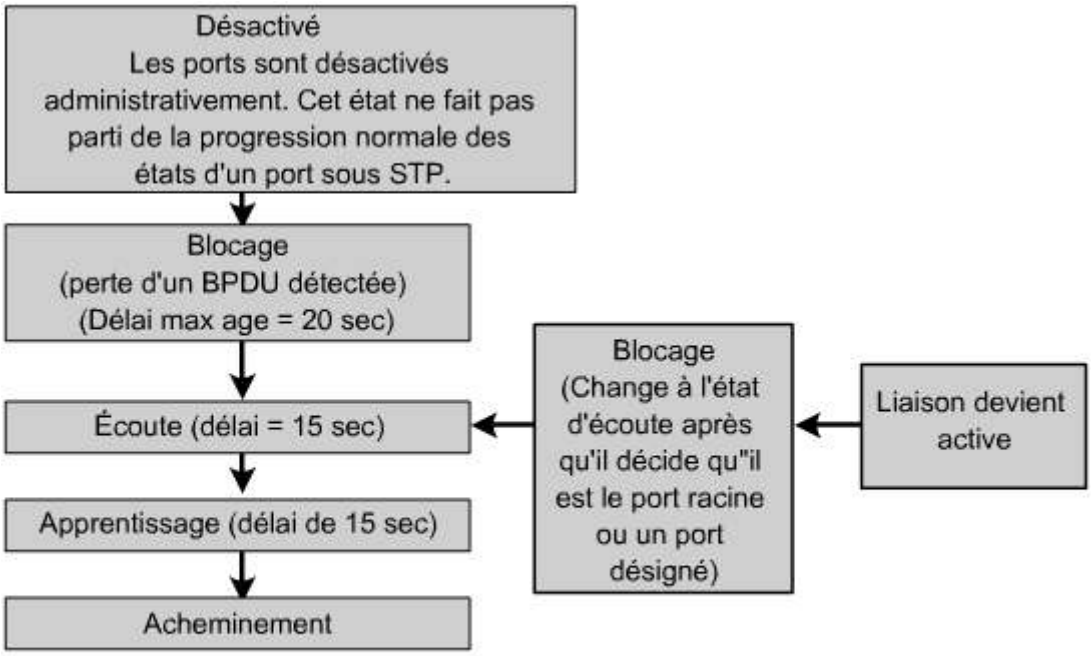
Au cours de ce TP, les étudiants vont exécuter les opérations suivantes: vérifier la configuration des hôtes et des commutateurs en testant la connectivité.

7.2 Protocole Spanning Tree (STP)

7.2.5 Étapes des états des ports Spanning Tree

Il est nécessaire de propager les informations de protocole sur l'ensemble d'un réseau commuté. Les changements topologiques survenant dans une partie du réseau ne sont pas immédiatement connus dans les autres parties du réseau. Il existe un délai de propagation. Un commutateur ne doit pas immédiatement faire passer l'état d'un port d'inactif à actif, car cela peut créer des boucles de données.

Chaque port d'un commutateur utilisant le protocole Spanning Tree passe par l'un des cinq états illustrés dans la figure 1



Le Spanning-Tree fait transiter chaque port à travers plusieurs états

.

À l'état de blocage, les ports peuvent seulement recevoir des unités BPDU. Les trames de données sont abandonnées et aucune adresse n'est apprise. Le passage à un autre état peut prendre jusqu'à 20 secondes.

Les ports passent de l'état de blocage à l'état d'écoute. Dans cet état, les commutateurs déterminent s'il existe un autre chemin vers le pont racine. Le chemin qui n'est pas le chemin le moins coûteux vers le pont racine retourne à l'état de blocage. La période d'écoute est appelée délai de transmission et dure 15 secondes. À l'état d'écoute, les données utilisateur ne sont pas acheminées et les adresses MAC ne sont pas apprises. Les unités BPDU sont toujours traitées.

Les ports passent de l'état d'écoute à l'état d'apprentissage. Dans cet état, les données utilisateur ne sont pas transmises, mais les adresses MAC de tout le trafic sont acquises. L'état d'apprentissage dure 15 secondes et est également appelé délai de transmission. Les unités BPDU sont toujours traitées.

Un port passe de l'état d'apprentissage à l'état de transmission. Dans cet état, les données utilisateur sont acheminées et les adresses MAC continuent d'être acquises. Les unités BPDU sont toujours traitées.

Un port peut être désactivé. Cet état peut survenir lorsqu'un administrateur désactive le port ou lorsque ce dernier tombe en panne.

Les valeurs de temps associées à chaque état sont les valeurs par défaut. Ces valeurs ont été calculées sur la base de sept commutateurs au maximum dans toute branche du Spanning Tree à partir du pont racine.

Activité de média interactive

Pointer-cliquer: États Spanning-Tree. À la fin de cette activité, l'étudiant sera en mesure d'identifier la fonction des états Spanning-Tree.

Activité de média interactive

Mots croisés: États Spanning-Tree

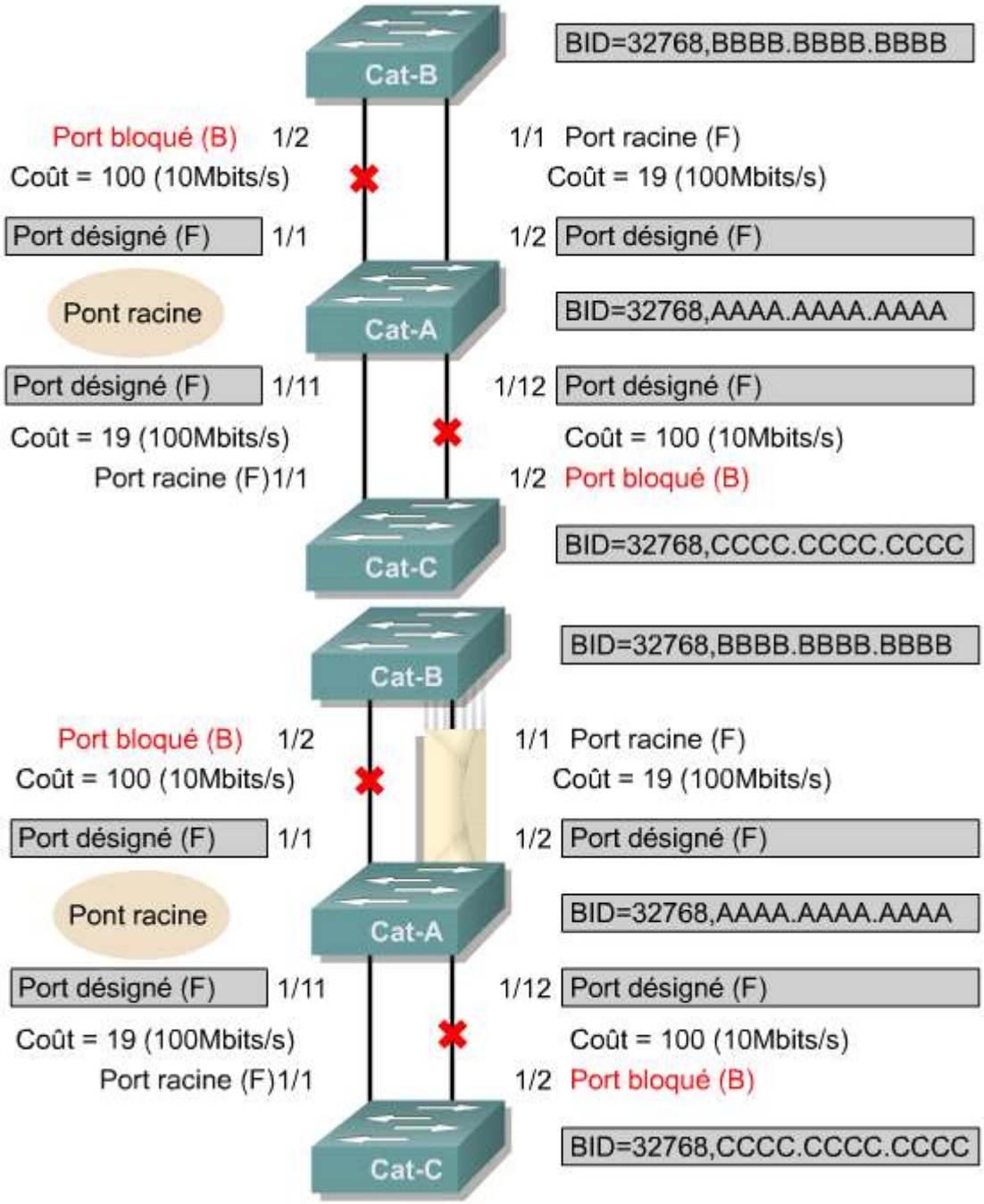
À la fin de cette activité, l'étudiant sera en mesure d'identifier la fonction des états Spanning-Tree.

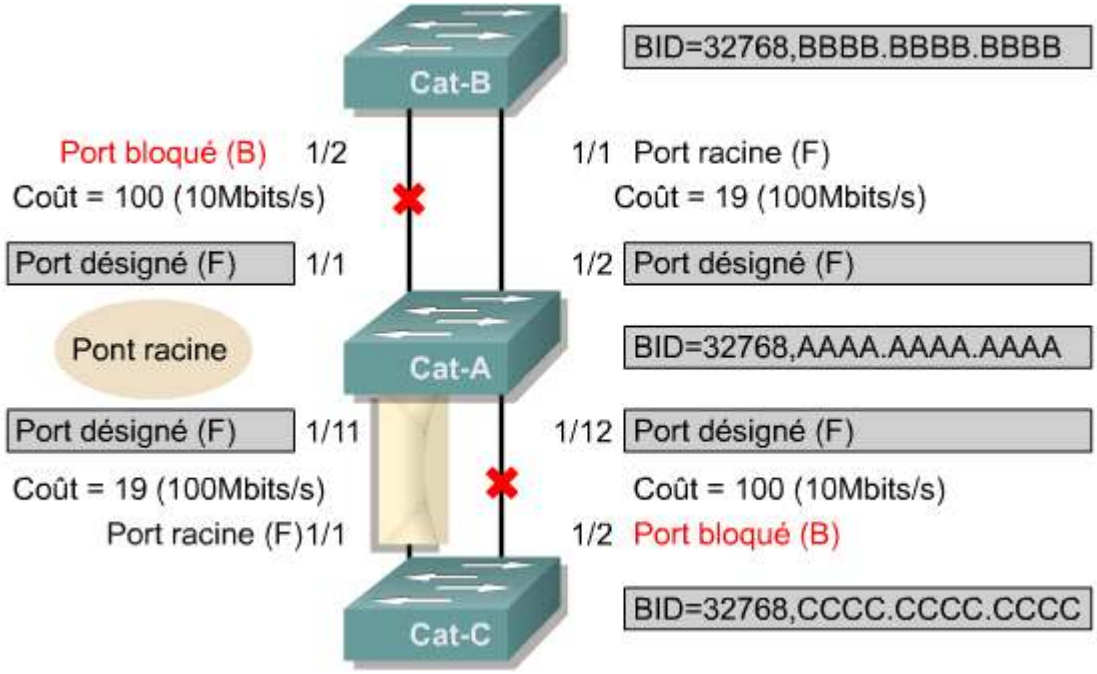
7.2 Protocole Spanning Tree (STP)

7.2.6 Recalcul du Spanning Tree

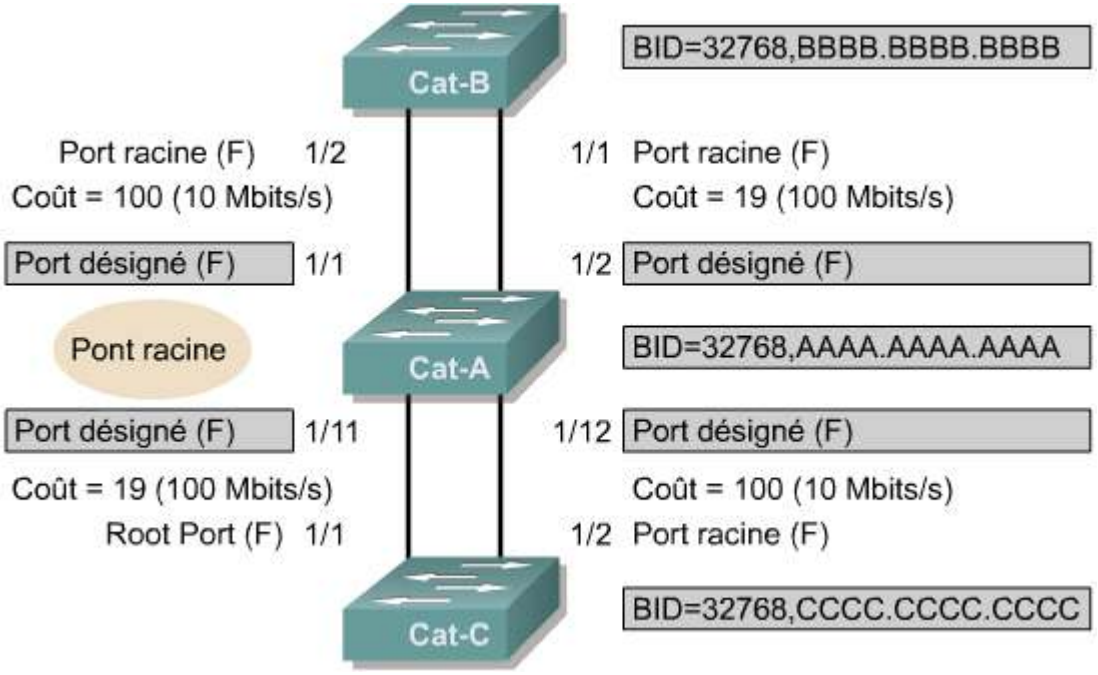
Un interréseau commuté a convergé lorsque tous les ports de commutateur et de pont sont à l'état de transmission ou de blocage. Les ports de transmission envoient et reçoivent le trafic de données et les unités BPDU. Les ports bloqués ne reçoivent que les unités BPDU.

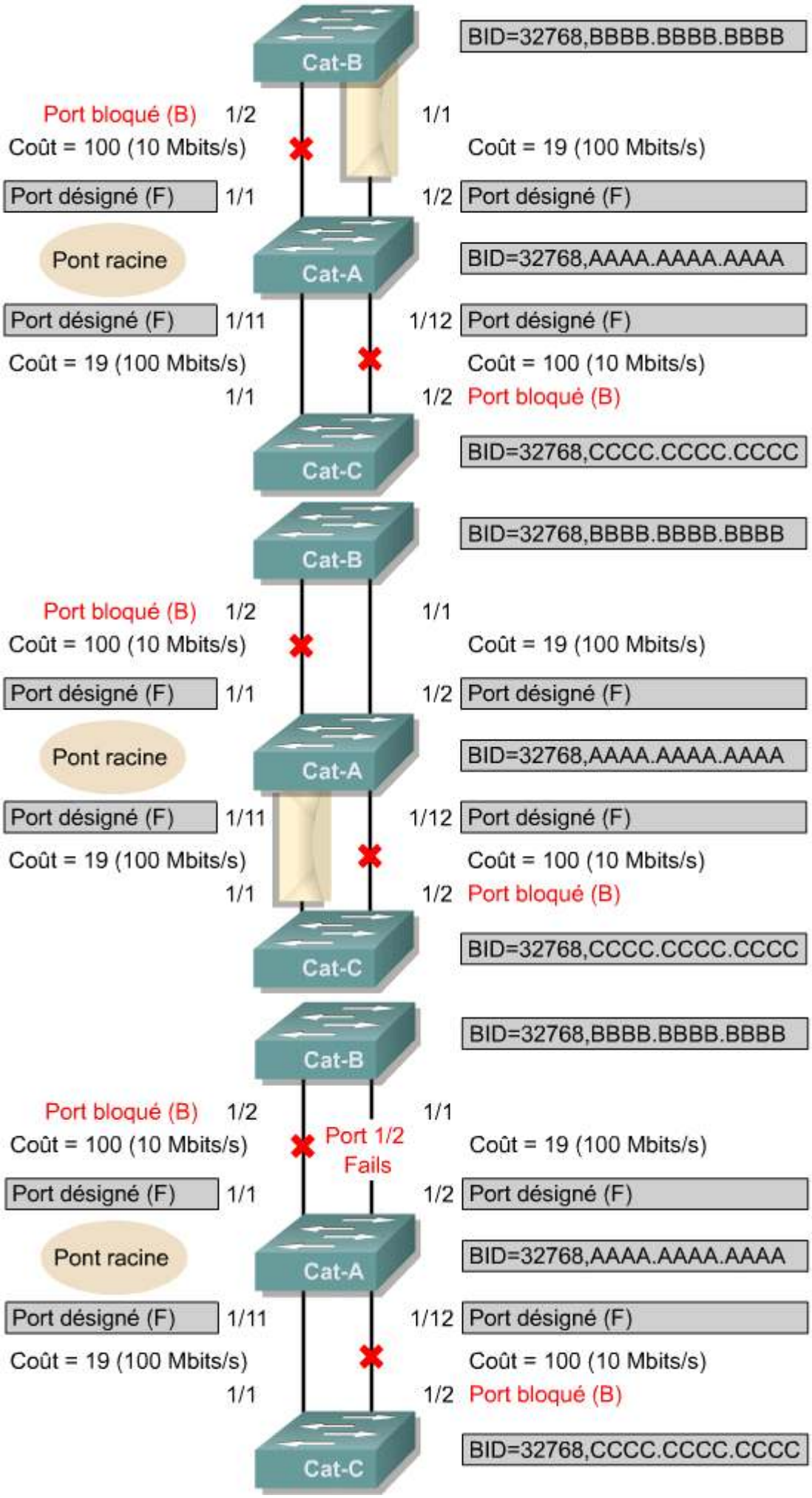
Lorsque la topologie du réseau change, les commutateurs et les ponts recalculent le Spanning Tree, ce qui interrompt le trafic utilisateur. 1 2

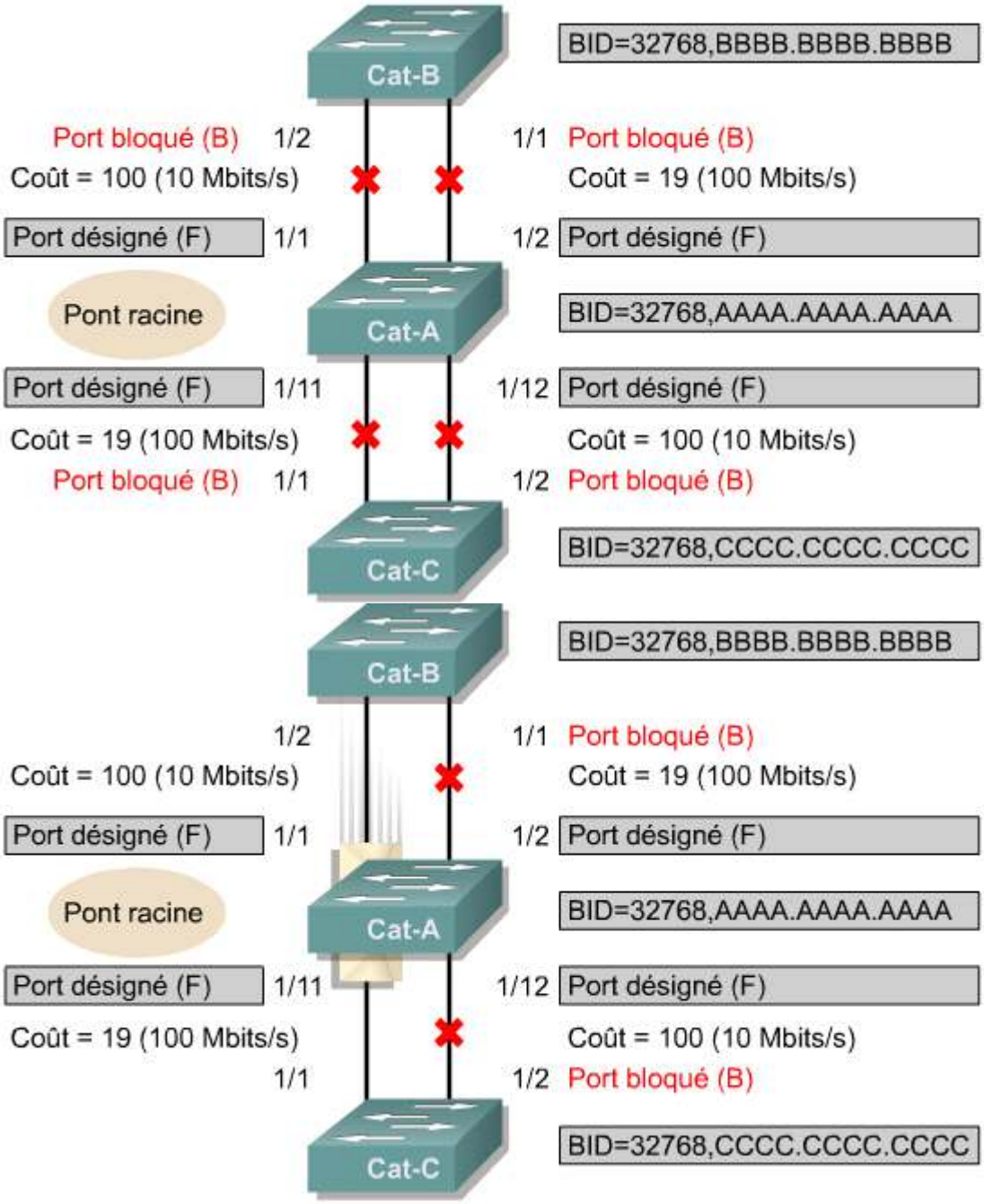

Cat-B
BID=32768,BBBB.BBBB.BBBB
Port bloqué (B) 1/2
Coût = 100 (10Mbits/s)
1/1 Port racine (F)
Coût = 19 (100Mbits/s)
Port désigné (F) 1/1
1/2 Port désigné (F)
Pont racine
Cat-A
BID=32768,AAAA.AAAA.AAAA
Port désigné (F) 1/11
1/12 Port désigné (F)
Coût = 19 (100Mbits/s)
Port racine (F)1/1
Coût = 100 (10Mbits/s)
1/2 Port bloqué (B)
Cat-C
BID=32768,CCCC.CCCC.CCCC
Cat-B
BID=32768,BBBB.BBBB.BBBB
Port bloqué (B) 1/2
Coût = 100 (10Mbits/s)
1/1 Port racine (F)
Coût = 19 (100Mbits/s)
Port désigné (F) 1/1
1/2 Port désigné (F)
Pont racine
Cat-A
BID=32768,AAAA.AAAA.AAAA
Port désigné (F) 1/11
1/12 Port désigné (F)
Coût = 19 (100Mbits/s)
Port racine (F)1/1
Coût = 100 (10Mbits/s)
1/2 Port bloqué (B)
Cat-C
BID=32768,CCCC.CCCC.CCCC


Cat-B
BID=32768,BBBB.BBBB.BBBB
Port bloqué (B) 1/2
Coût = 100 (10Mbits/s)
1/1 Port racine (F)
Coût = 19 (100Mbits/s)
Port désigné (F) 1/1
1/2 Port désigné (F)
Pont racine
Cat-A
BID=32768,AAAA.AAAA.AAAA
Port désigné (F) 1/11
1/12 Port désigné (F)
Coût = 19 (100Mbits/s)
Port racine (F)1/1
Coût = 100 (10Mbits/s)
1/2 Port bloqué (B)
Cat-C
BID=32768,CCCC.CCCC.CCCC

2-


Cat-B
BID=32768,BBBB.BBBB.BBBB
Port racine (F) 1/2
Coût = 100 (10 Mbits/s)
1/1 Port racine (F)
Coût = 19 (100 Mbits/s)
Port désigné (F) 1/1
1/2 Port désigné (F)
Pont racine
Cat-A
BID=32768,AAAA.AAAA.AAAA
Port désigné (F) 1/11
1/12 Port désigné (F)
Coût = 19 (100 Mbits/s)
Root Port (F) 1/1
Coût = 100 (10 Mbits/s)
1/2 Port racine (F)
Cat-C
BID=32768,CCCC.CCCC.CCCC


Cat-B
BID=32768,BBBB.BBBB.BBBB
Port bloqué (B)
1/2
1/1
Coût = 100 (10 Mbits/s)
Coût = 19 (100 Mbits/s)
Port désigné (F)
1/1
1/2
Port désigné (F)
Pont racine
Cat-A
BID=32768,AAAA.AAAA.AAAA
Port désigné (F)
1/11
1/12
Port désigné (F)
Coût = 19 (100 Mbits/s)
Coût = 100 (10 Mbits/s)
1/1
1/2
Port bloqué (B)
Cat-C
BID=32768,CCCC.CCCC.CCCC
Cat-B
BID=32768,BBBB.BBBB.BBBB
Port bloqué (B)
1/2
1/1
Coût = 100 (10 Mbits/s)
Coût = 19 (100 Mbits/s)
Port désigné (F)
1/1
1/2
Port désigné (F)
Pont racine
Cat-A
BID=32768,AAAA.AAAA.AAAA
Port désigné (F)
1/11
1/12
Port désigné (F)
Coût = 19 (100 Mbits/s)
Coût = 100 (10 Mbits/s)
1/1
1/2
Port bloqué (B)
Cat-C
BID=32768,CCCC.CCCC.CCCC
Cat-B
BID=32768,BBBB.BBBB.BBBB
Port bloqué (B)
1/2
1/1
Coût = 100 (10 Mbits/s)
Port 1/2
Fails
Coût = 19 (100 Mbits/s)
Port désigné (F)
1/1
1/2
Port désigné (F)
Pont racine
Cat-A
BID=32768,AAAA.AAAA.AAAA
Port désigné (F)
1/11
1/12
Port désigné (F)
Coût = 19 (100 Mbits/s)
Coût = 100 (10 Mbits/s)
1/1
1/2
Port bloqué (B)
Cat-C
BID=32768,CCCC.CCCC.CCCC



La convergence sur une nouvelle topologie Spanning Tree via la norme IEEE 802.1d peut prendre jusqu'à 50 secondes. La durée de convergence inclut l'âge maximum (20 secondes), le délai de transmission d'écoute (15 secondes) et le délai de transmission d'apprentissage (15 secondes).

Activité de TP

Exercice: Recalcul du Spanning Tree

Au cours de ce TP, l'étudiant va créer une configuration de commutateur de base et la vérifier. Il va également observer le comportement de l'algorithme «spanning tree» en présence de changements dans la topologie d'un réseau commuté.

Activité de TP

Activité en ligne: Recalcul du Spanning Tree

Au cours de ce TP, les étudiants vont créer une configuration de commutateur de base et la vérifier.

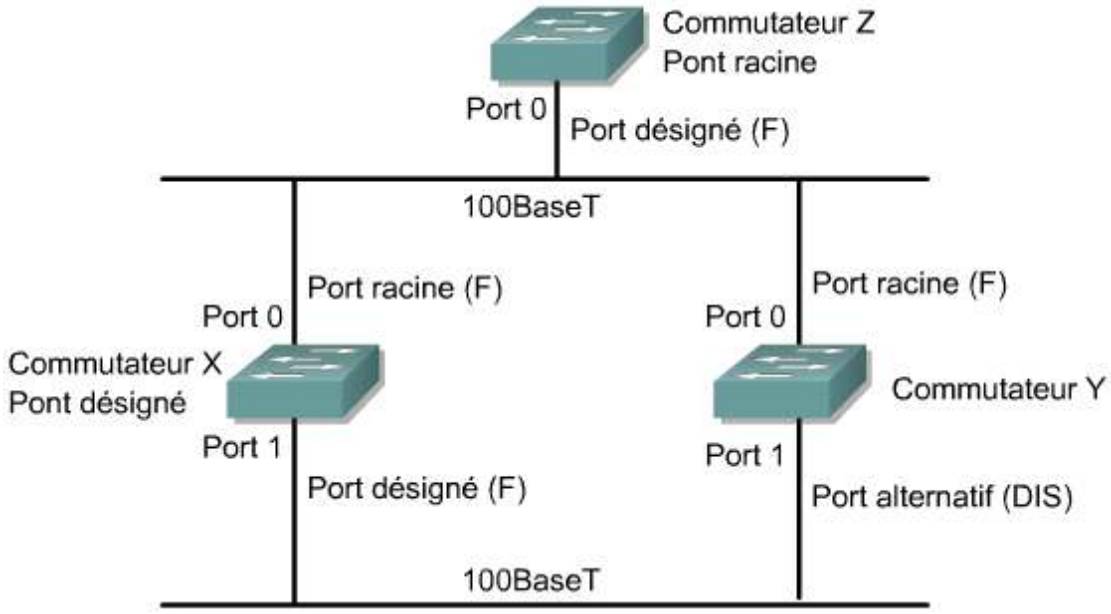
7.2 Protocole Spanning Tree (STP)

7.2.7 Protocole Spanning Tree rapide (RSTP)

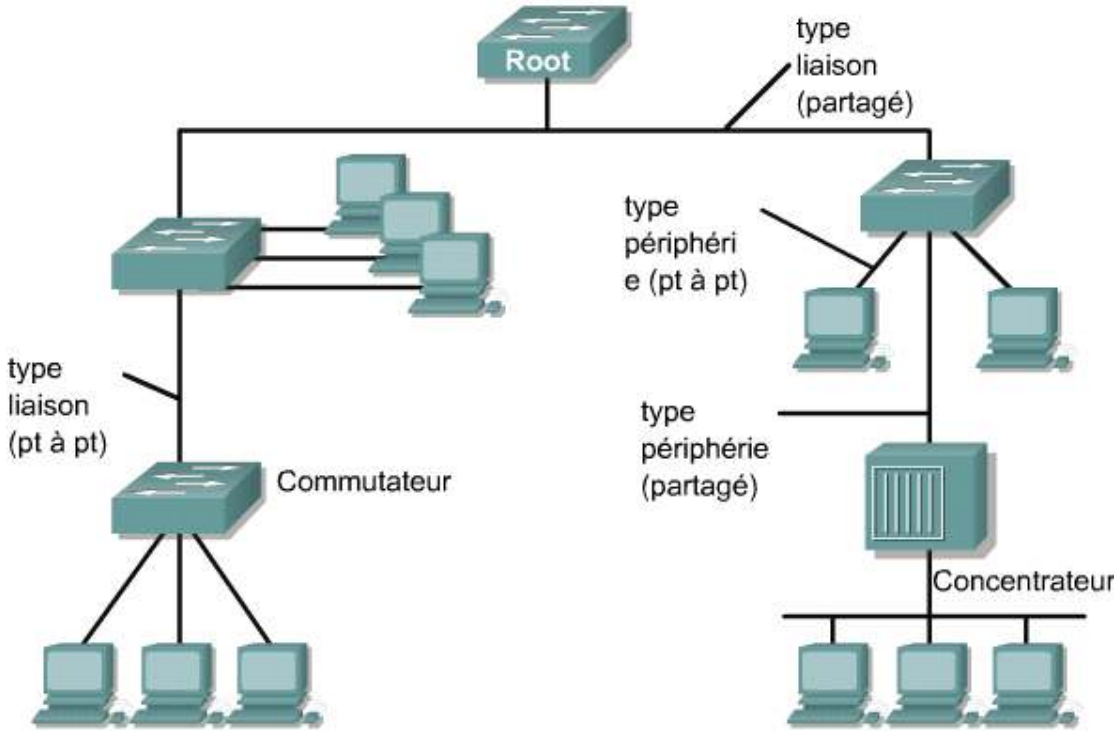
Le protocole Spanning Tree rapide est défini dans la norme LAN IEEE 802.1w. Cette norme et ce protocole introduisent les points suivants:

- Clarification des états et des rôles des ports
- Définition d'un ensemble de types de liaisons pouvant passer rapidement à l'état de transmission
- Concept autorisant les commutateurs, dans un réseau convergé, à générer leurs propres unités BPDU plutôt que de relayer celles du pont racine

L'état de «blocage» d'un port est appelé état d'« abandon ». Un port d'abandon est un «port alternatif». Le port d'abandon peut devenir le «port désigné» en cas de panne du port désigné pour le segment. 1



Les liaisons sont de type point à point, périphérie et partagé. 2



Ces modifications permettent l'apprentissage rapide des échecs de liaison dans les réseaux commutés.

Les liaisons point-à-point et les liaisons de type périphérie peuvent passer immédiatement à l'état de transmission.

Avec ces changements, la convergence du réseau ne dure pas plus de 15 secondes.

Le protocole Spanning Tree rapide, IEEE 802.1w, remplacera à long terme le protocole Spanning Tree IEEE 802.1D.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Redondance et compréhension de son importance dans les réseaux
- Principaux composants d'une topologie réseau redondante
- Tempêtes de broadcast et impact de ces tempêtes sur les réseaux commutés
- Transmissions de trames multiples et impact de ces transmissions sur les réseaux commutés
- Causes et effets de l'instabilité de la base de données des adresses MAC
- Avantages et risques d'une topologie redondante
- Rôle du Spanning Tree dans un réseau commuté à chemins redondants
- Principaux éléments du fonctionnement du Spanning Tree
- Processus de sélection du pont racine
- États Spanning Tree
- Protocole Spanning Tree (STP) comparé au protocole Spanning Tree rapide (RSTP)

Résumé

- La notion de redondance dans un réseau est extrêmement importante, car elle permet aux réseaux de tolérer les pannes.
- Les topologies redondantes constituent une protection contre les temps d'arrêt dus à une panne au niveau d'une liaison, d'un port ou d'une unité du réseau.
- Le protocole Spanning Tree est utilisé dans les réseaux commutés pour créer une topologie logique sans boucle à partir d'une topologie physique qui comporte des boucles.
- Les quatre états du port Spanning Tree sont : blocage, écoute, apprentissage et transmission.

Vue d'ensemble

Le concept de réseau local virtuel (VLAN) est une caractéristique importante de la commutation Ethernet. Un VLAN est un groupement logique d'unités ou d'utilisateurs. Ces unités ou utilisateurs peuvent être regroupés par fonction, par service ou par application, quel que soit l'emplacement du segment LAN physique. Les unités d'un VLAN peuvent uniquement communiquer avec les unités de leur propre VLAN. Tout comme les routeurs permettent de relier des segments LAN différents, ils permettent également de connecter des segments VLAN différents. L'approche de Cisco en matière d'interopérabilité est une approche positive, mais chaque fournisseur a développé son propre produit VLAN et la compatibilité peut ne pas être entièrement garantie.

Les VLAN améliorent les performances globales du réseau en regroupant les utilisateurs et les ressources de manière logique. Les entreprises utilisent souvent des VLAN pour garantir le regroupement logique d'un ensemble d'utilisateurs quel que soit l'emplacement physique. Ainsi, les utilisateurs du service Marketing sont affectés au VLAN Marketing, tandis que les utilisateurs du service Ingénierie sont associés au VLAN Ingénierie.

Les VLAN peuvent améliorer l'évolutivité, la sécurité et la gestion des réseaux. Les routeurs dans les topologies VLAN offrent des services de filtrage des broadcasts, de sécurité et de gestion du flux du trafic.

Lorsqu'ils sont correctement conçus et configurés, les VLAN sont des outils puissants pour les administrateurs réseau. Les VLAN simplifient les opérations d'ajout, de déplacement et de modification d'un réseau. Les VLAN améliorent la sécurité du réseau et facilitent le contrôle des broadcasts de couche 3. Toutefois, un VLAN mal configuré peut ralentir le fonctionnement d'un réseau ou même empêcher son fonctionnement. Il est donc important de comprendre le mode de mise en œuvre des VLAN sur les différents commutateurs au moment de la conception d'un réseau.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Définir des VLAN
- Énumérer les avantages des VLAN
- Expliquer comment les VLAN sont utilisés pour créer des domaines de broadcast
- Expliquer comment les routeurs sont utilisés pour la communication entre VLAN
- Énumérer les principaux types de VLAN
- Définir ISL et 802.1Q
- Expliquer le concept de VLAN géographique
- Configurer des VLAN statiques sur des commutateurs Catalyst de la série 29xx
- Vérifier et enregistrer les configurations VLAN
- Supprimer des VLAN d'une configuration de commutateur

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
8.1	Concepts VLAN
8.2	Configuration VLAN
8.3	Dépannage des VLAN

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Configuration d'un commutateur avec des VLAN et une communication entre commutateurs		

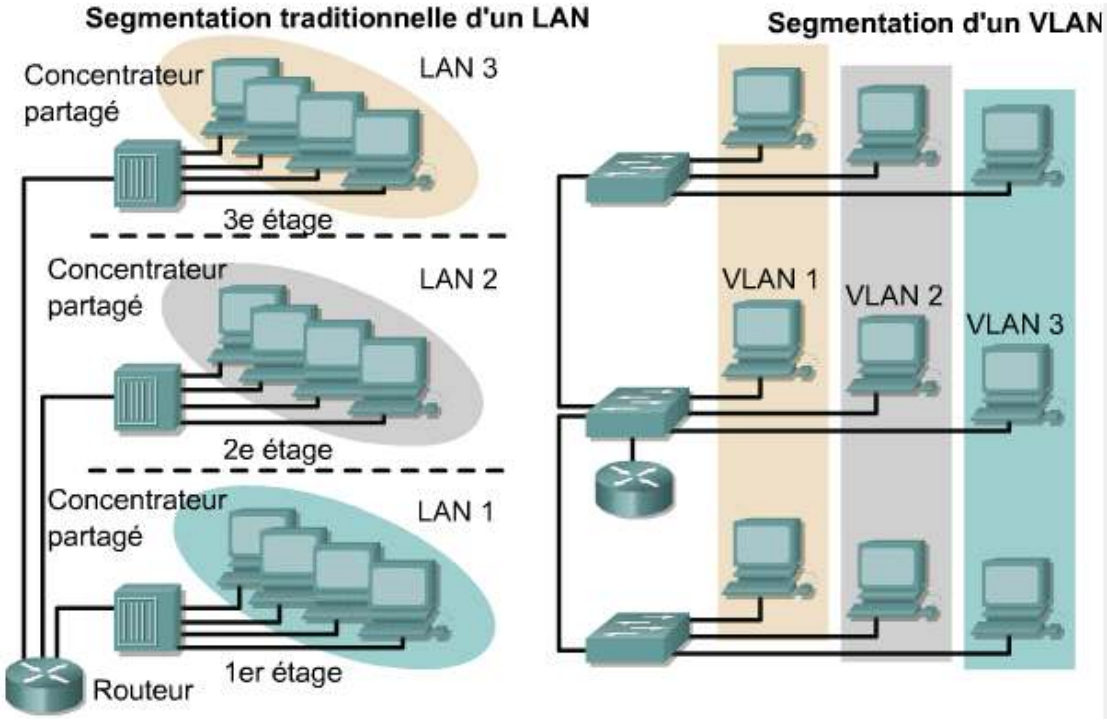
Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Configuration d'un commutateur avec des VLAN et une communication entre commutateurs		

8.1 Concepts VLAN

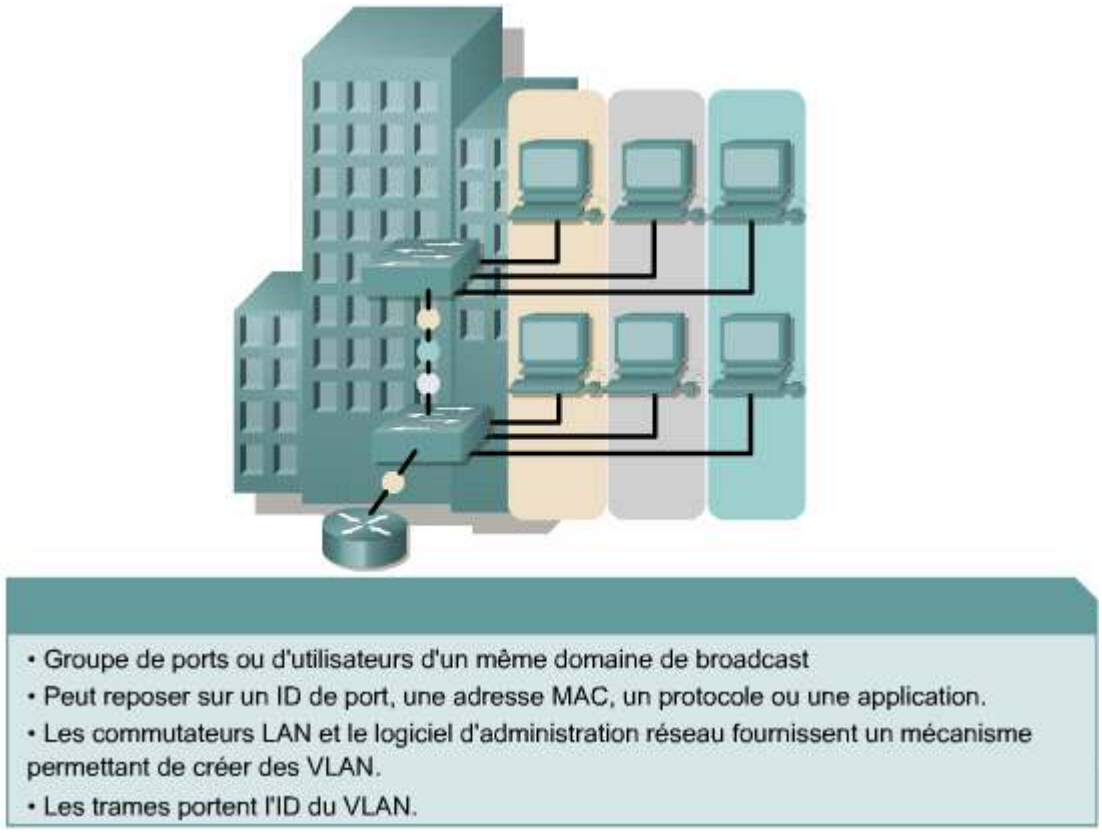
8.1.1 Introduction au LAN virtuel

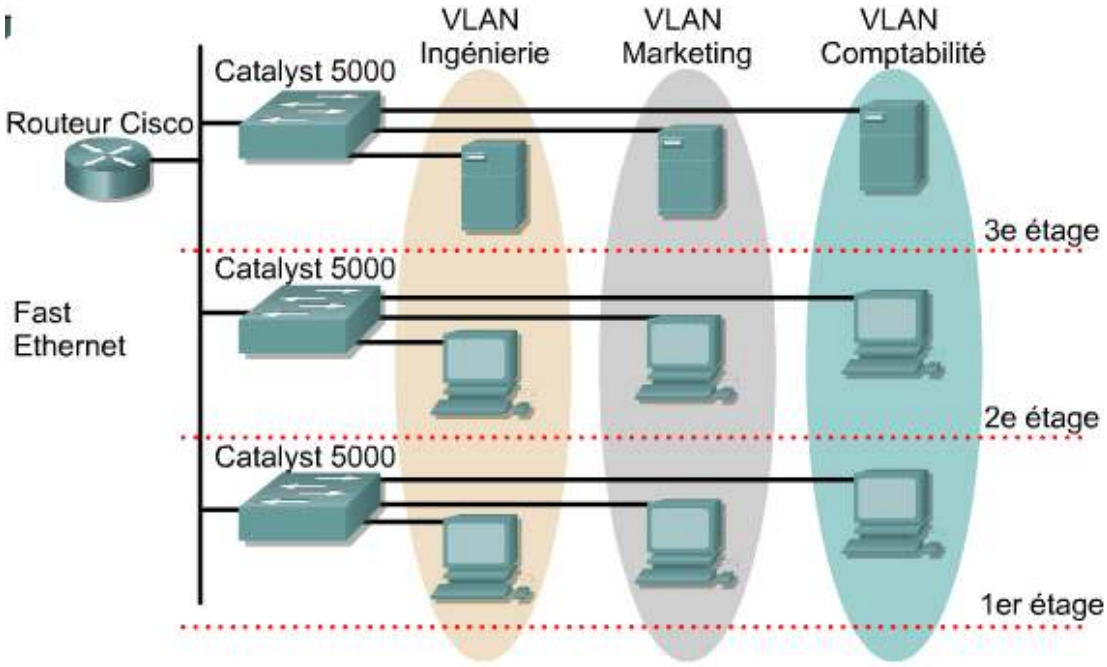
Un LAN virtuel (ou VLAN) est un groupe de services réseau qui ne sont pas limités à un segment physique ou à un commutateur LAN. 1



Les VLAN segmentent les réseaux commutés de manière logique sur la base des fonctions, des équipes de projet ou des applications de l'entreprise, quel que soit l'emplacement physique ou les connexions au réseau. L'ensemble des stations de travail et des serveurs utilisés par un groupe de travail partagent le même VLAN, indépendamment de l'emplacement ou de la connexion physique.

La configuration ou la reconfiguration des VLAN est effectuée par l'intermédiaire d'un logiciel. La configuration d'un VLAN ne nécessite pas de connecter ou de déplacer physiquement des câbles et des équipements. 2 3





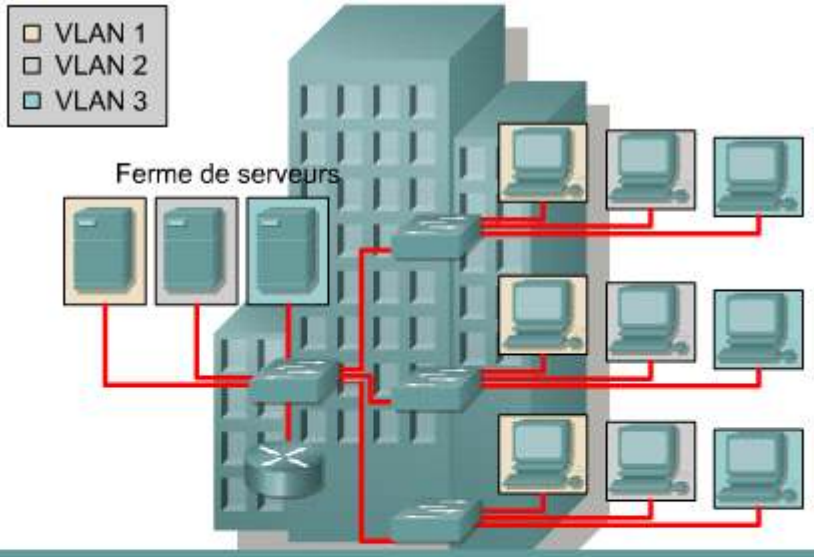
La communication d'une station de travail appartenant à un groupe VLAN est limitée aux serveurs de fichiers de ce groupe. Les LAN virtuels segmentent logiquement le réseau en différents domaines de broadcast, afin que les paquets soient commutés uniquement entre les ports d'un même VLAN. Les VLAN sont composés d'ordinateurs hôte ou d'équipements réseau connectés par un même domaine de pontage. Le domaine de pontage est pris en charge sur différents équipements de réseau. Les commutateurs LAN utilisent des protocoles de pontage avec un groupe de ponts distinct pour chaque VLAN.

Les VLAN sont créés pour fournir des services de segmentation habituellement fournis par les routeurs physiques dans les configurations LAN. Les VLAN répondent aux problèmes d'évolutivité, de sécurité et de gestion des réseaux. Les routeurs dans les topologies VLAN offrent des services de filtrage des broadcasts, de sécurité et de gestion du flux du trafic. Les commutateurs ne peuvent pas acheminer de paquets entre des VLAN par le biais de ponts, car cela pourrait violer l'intégrité du domaine de broadcast VLAN. Le trafic doit uniquement être routé entre les VLAN.

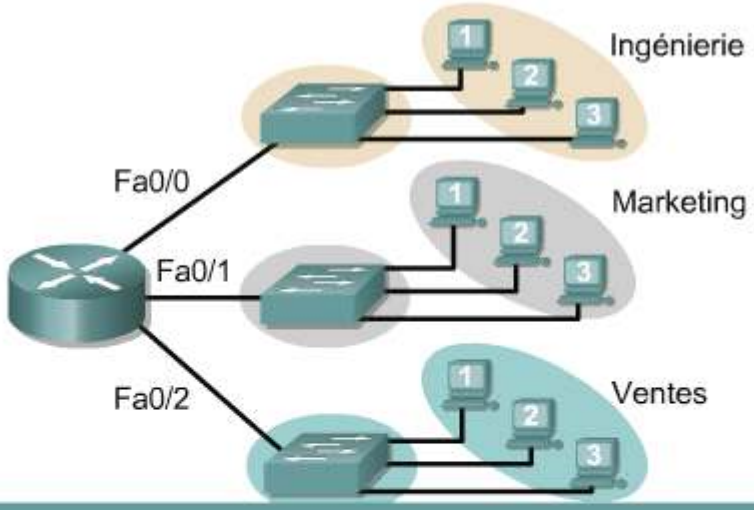
8.1 Concepts VLAN

8.1.2 Domaines de broadcast avec VLAN et routeurs

Un VLAN est un domaine de broadcast créé par un ou plusieurs commutateurs. La structure des réseaux présentés dans les figures 1 et 2 nécessite trois domaines de broadcast distincts.



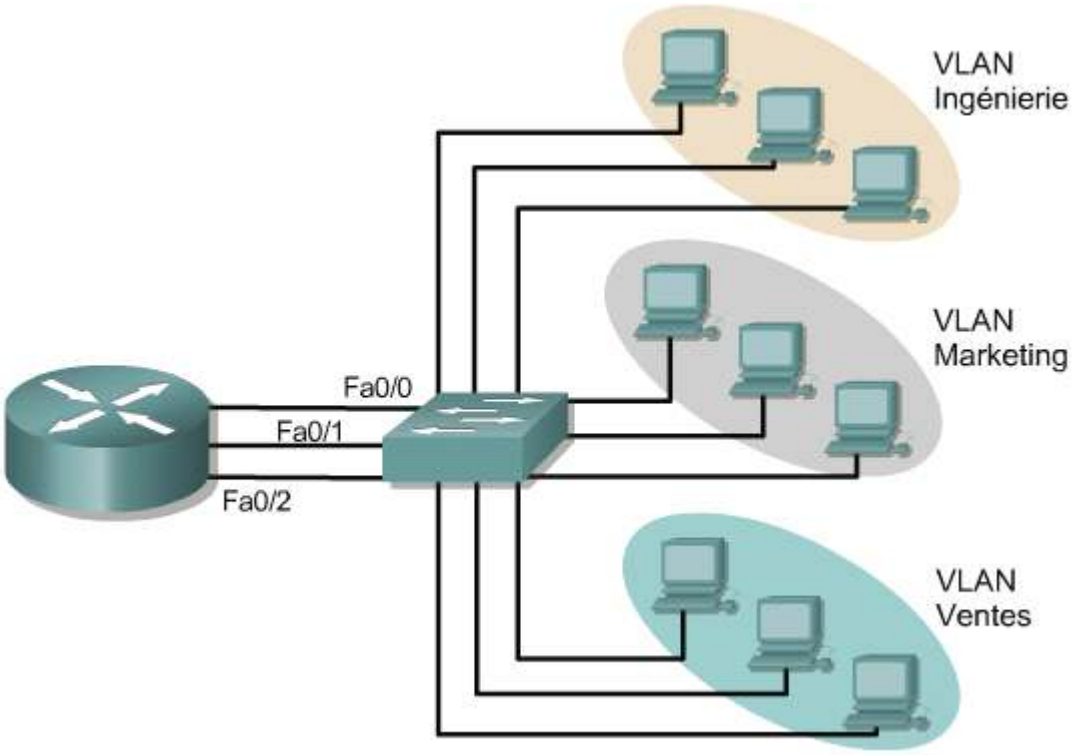
- Un commutateur crée un domaine de broadcast.
- Les LAN virtuels aident à gérer les domaines de broadcast.
- Les LAN virtuels peuvent être définis sur des groupes de ports, des utilisateurs ou des protocoles.
- Les commutateurs LAN et le logiciel d'administration réseau fournissent un mécanisme permettant de créer des VLAN.



Trois commutateurs et un routeur peuvent être utilisés sans VLAN :
- Un commutateur pour le service Ingénierie
- Un commutateur pour le service Ventes
- Un commutateur pour le service Marketing
- Chaque commutateur considère tous les ports comme appartenant à un domaine de broadcast.
- Le routeur est utilisé pour acheminer les paquets sur les trois domaines de broadcast.

La figure 2 montre comment trois domaines de broadcast séparés sont créés à l'aide de trois commutateurs différents. Le routage de couche 3 permet au routeur d'envoyer des paquets aux trois domaines de broadcast.

Dans la figure 3, un VLAN est créé avec un routeur et un commutateur. Toutefois, il y a trois domaines de broadcast séparés. Dans ce scénario, il y a un routeur et un commutateur, mais trois domaines de broadcast séparés.



Dans la figure 3, trois domaines de broadcast séparés sont créés. Le routeur achemine le trafic entre les VLAN à l'aide du routage de couche 3.

Le commutateur de la figure 3 transmet les trames aux interfaces du routeur:

- s'il s'agit de trames de broadcast;
- si elles sont destinées à l'une des adresses MAC du routeur.

Si la station de travail 1 du VLAN Ingénierie veut envoyer des trames à la station de travail 2 du VLAN Ventes, celles-ci sont envoyées à l'adresse MAC Fa0/0 du routeur. Le routage est effectué via l'adresse IP sur l'interface de routeur Fa0/0 pour le VLAN Ingénierie.

Si la station de travail 1 du VLAN Ingénierie souhaite envoyer une trame à la station de travail 2 du même VLAN, l'adresse MAC de destination de la trame est l'adresse MAC de la station de travail 2.

La mise en œuvre de LAN virtuels sur un commutateur implique ce qui suit:

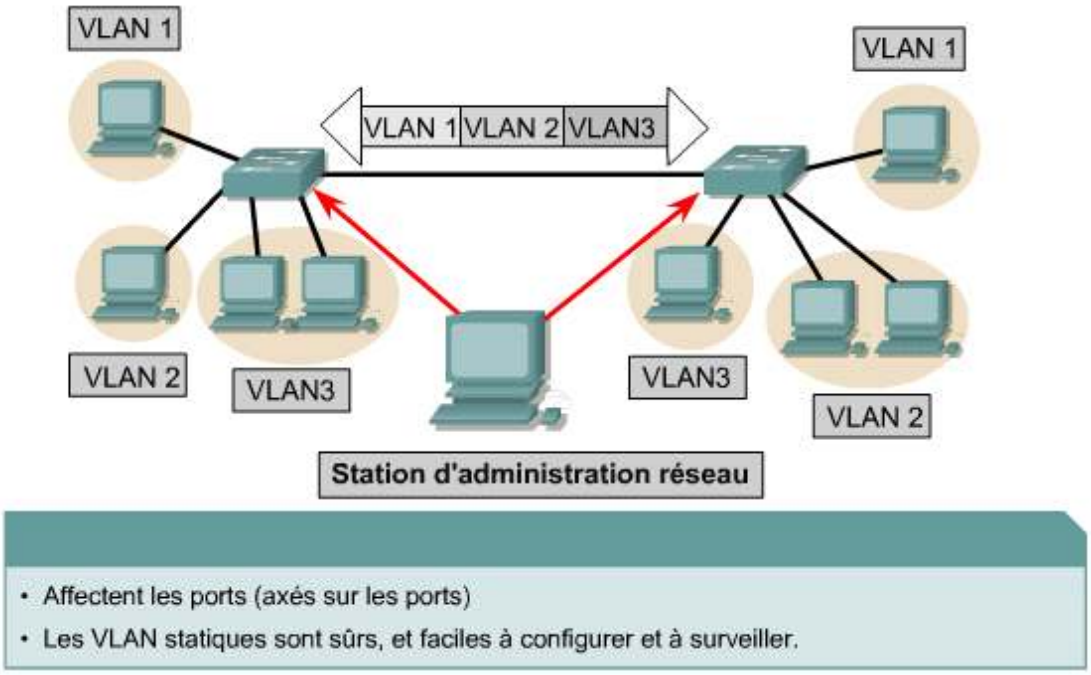
- Le commutateur doit mettre à jour une table de pontage séparée pour chaque VLAN.
- Si la trame arrive sur un port du VLAN 1, le commutateur recherche la table de pontage du VLAN 1.
- Lorsque la trame est reçue, le commutateur ajoute l'adresse source à la table de pontage si elle est inconnue.
- La destination est vérifiée, de sorte qu'une décision de transmission soit prise.
- Pour l'apprentissage et la transmission, la recherche est effectuée uniquement par rapport à la table d'adresses de ce VLAN.

8.1 Concepts VLAN

8.1.3 Fonctionnement d'un VLAN

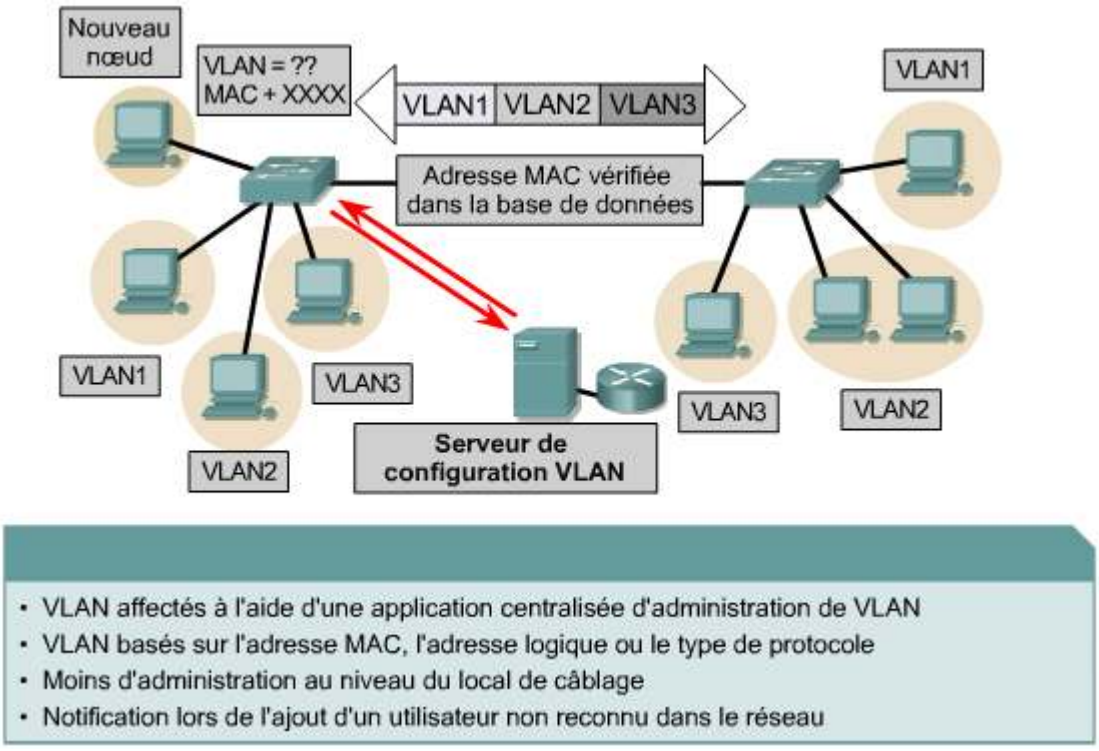
Chaque port de commutateur peut être attribué à un LAN virtuel différent. Les ports affectés au même LAN virtuel partagent les broadcasts. Les ports qui n'appartiennent pas à ce LAN virtuel ne partagent pas ces broadcasts. Cela améliore les performances globales du réseau.

Les VLAN statiques sont dits «axés sur le port». Lorsqu'un équipement accède au réseau, il adopte automatiquement le VLAN d'appartenance du port auquel il est connecté. 1



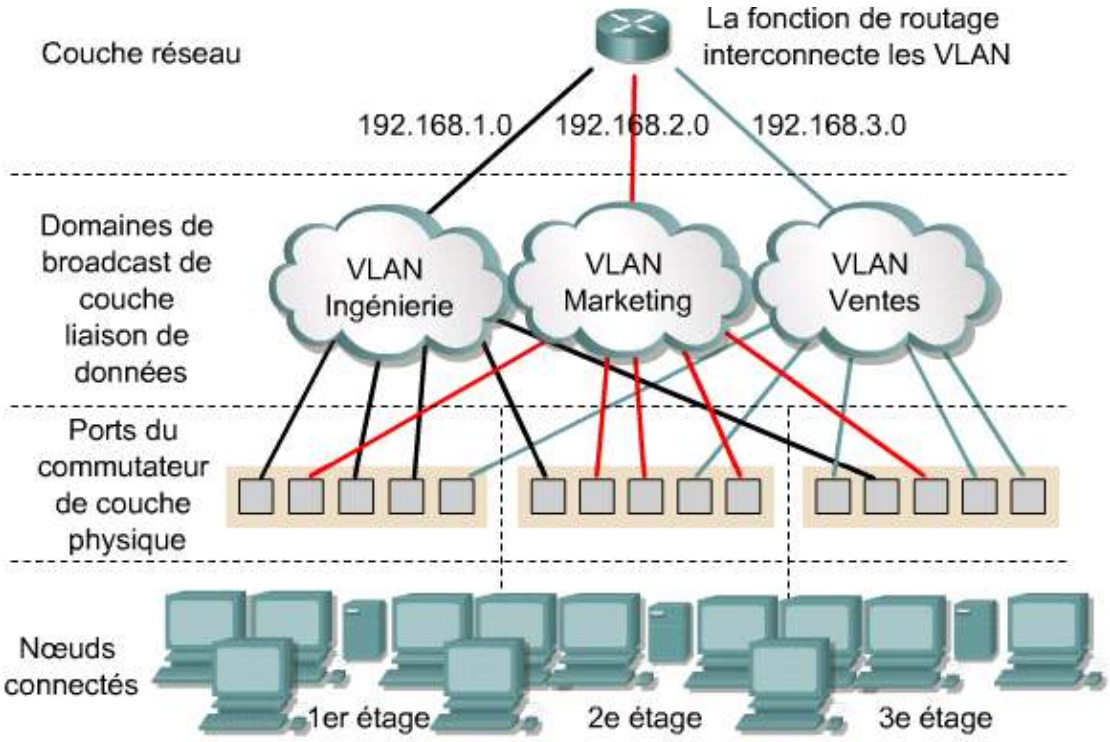
Les utilisateurs connectés au même segment partagé partagent la bande passante de ce segment. Chaque utilisateur supplémentaire connecté au support partagé implique une réduction de la bande passante et une détérioration des performances du réseau. Les LAN virtuels offrent aux utilisateurs une bande passante plus large qu'un réseau partagé. Le VLAN par défaut de chaque port du commutateur est le VLAN de gestion. Par défaut, le VLAN 1 est toujours le VLAN de gestion et ne peut pas être supprimé. Au moins un des ports doit être dans le VLAN 1 pour être en mesure de gérer le commutateur à distance. Tous les autres ports du commutateur peuvent être réaffectés à d'autres VLAN.

Les VLAN dynamiques sont créés par l'intermédiaire du logiciel d'administration réseau. CiscoWorks 2000 ou CiscoWorks for Switched Internetworks est utilisé pour créer des VLAN dynamiques. Les VLAN dynamiques permettent une appartenance axée sur l'adresse MAC de l'unité connectée au port du commutateur. Quand un appareil arrive sur un réseau, le commutateur auquel il est connecté questionne une base de données sur le serveur de configuration de VLAN pour déterminer son appartenance à un VLAN. 2



Dans le cas de l'appartenance à un VLAN axée sur le port, ce dernier est affecté à un membre VLAN spécifique indépendant de l'utilisateur ou du système connecté à ce port. Avec cette méthode d'appartenance, tous les utilisateurs du même port doivent faire partie du même LAN virtuel. Un utilisateur unique ou plusieurs utilisateurs peuvent être connectés à un port et

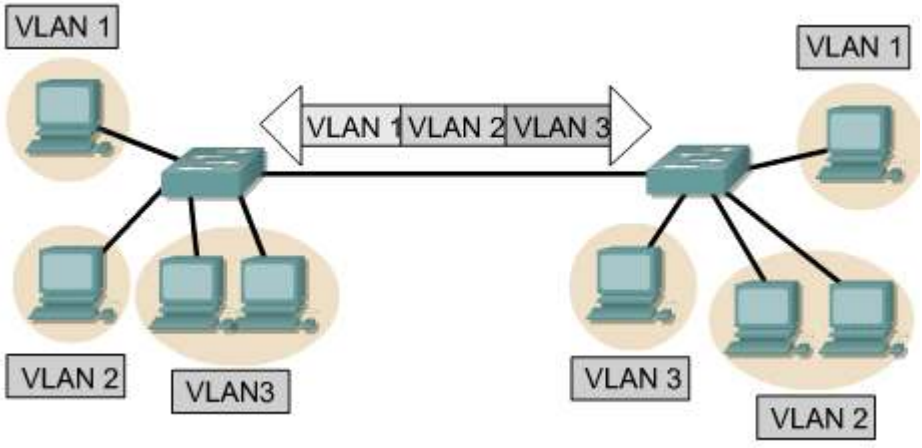
ne jamais réaliser qu'il existe un VLAN. 3 Cette approche est facile à gérer, car aucune table de recherche complexe n'est nécessaire pour la segmentation VLAN.

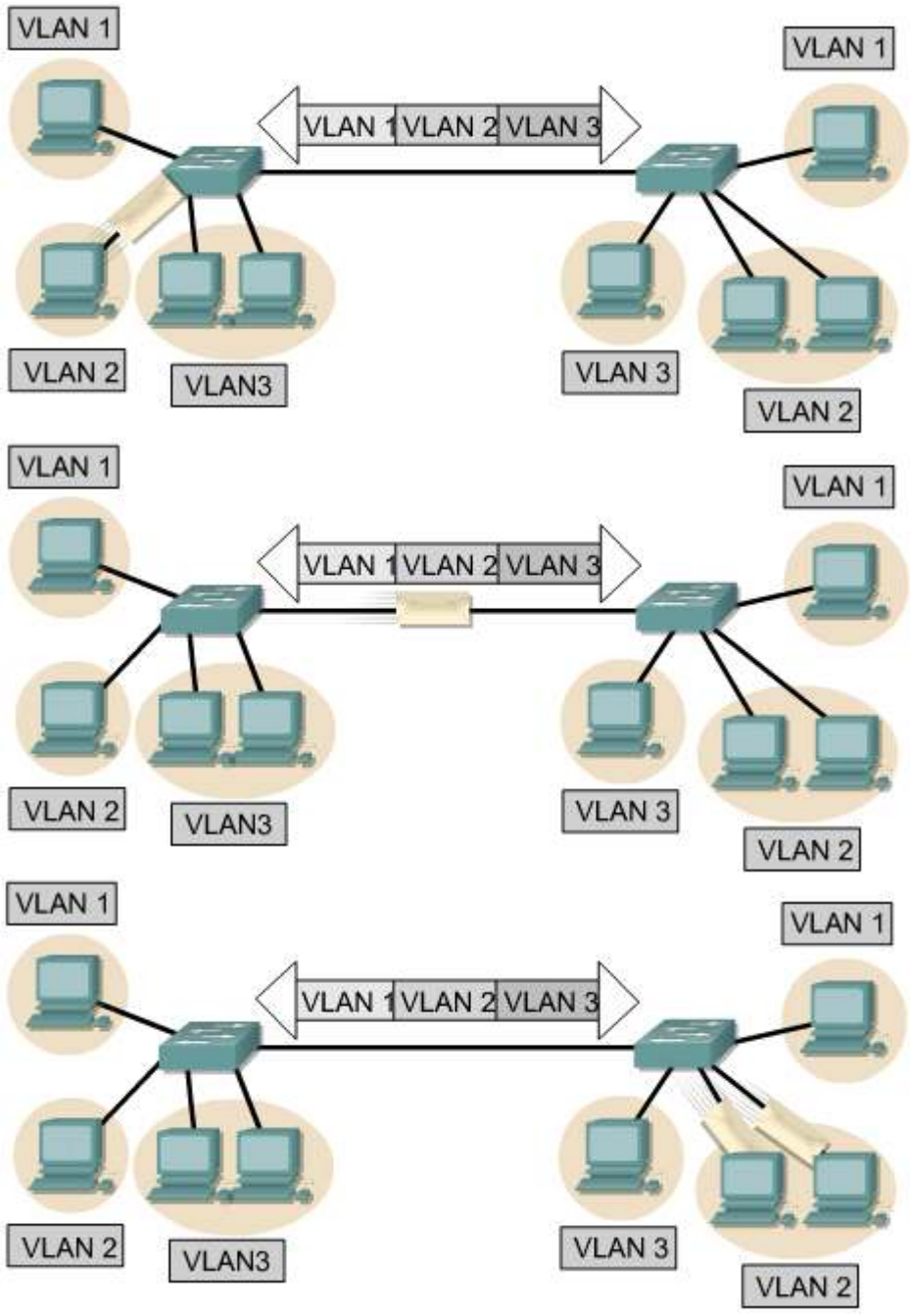


Les administrateurs réseau sont chargés de configurer les VLAN à la fois de manière statique et dynamique. 4

Configuration de VLAN	Description
Statique	Les administrateurs réseau effectuent une configuration port par port.Chaque port est associé à un VLAN spécifique.L'administrateur réseau est chargé de saisir les associations entre les ports et les VLAN.
Dynamique	Les ports sont capables de réaliser dynamiquement leur configuration VLAN.Utilisation d'une base de données logicielle d'adresses MAC pour les associations VLAN (que l'administrateur réseau doit préalablement définir).

Chaque interface d'un commutateur se comporte comme un port sur un pont. Les ponts filtrent le trafic qui n'a pas besoin d'être acheminé à des segments autres que le segment source. Si une trame a besoin de traverser le pont, ce dernier transmet la trame à l'interface appropriée et à aucune autre. Si le pont ou le commutateur ne connaît pas la destination, il transmet la trame à tous les ports du domaine de broadcast ou du VLAN, à l'exception du port source. 5





Activité de média interactive

Glisser-Positionner: Fonctionnement des VLAN

À la fin de cette activité, l'étudiant connaîtra le chemin suivi par les paquets dans un réseau doté de LAN virtuels. L'étudiant saura prévoir le chemin qu'un paquet va prendre en fonction des hôtes d'origine et de destination.

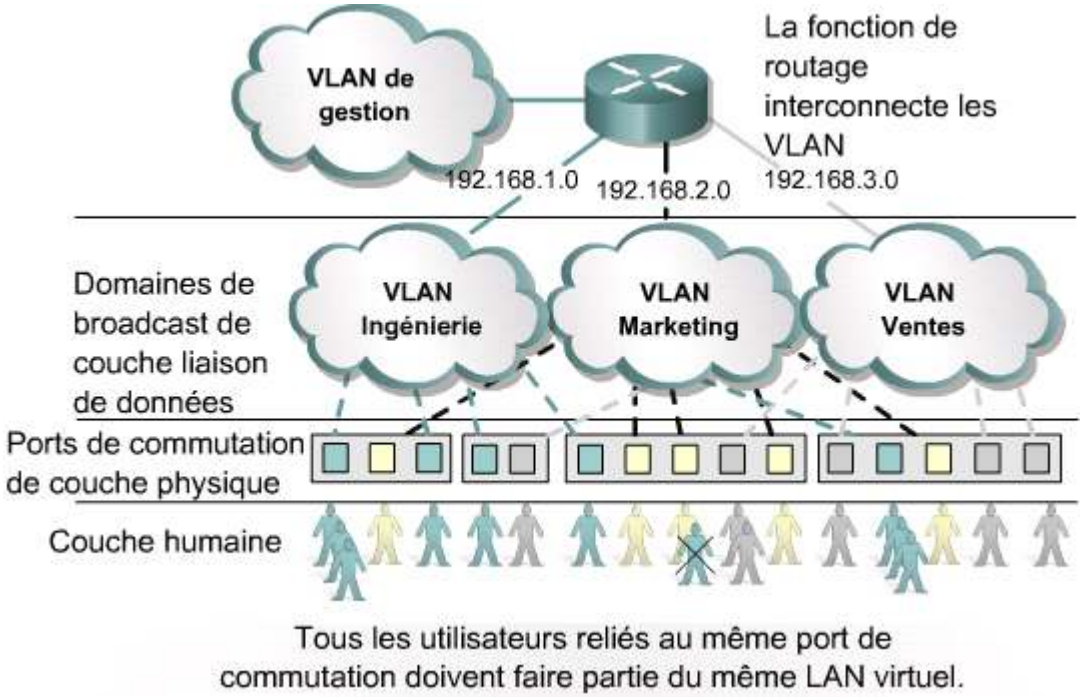
8.1 Concepts VLAN

8.1.4 Avantages des LAN virtuels (VLAN)

Le principal avantage des VLAN est qu'ils permettent à l'administrateur réseau d'organiser le LAN de manière logique et non physique. Cela signifie qu'un administrateur peut effectuer toutes les opérations suivantes: 1

- Déplacer facilement des stations de travail sur le LAN
- Ajouter facilement des stations de travail au LAN
- Modifier facilement la configuration LAN
- Contrôler facilement le trafic réseau

- Améliorer la sécurité

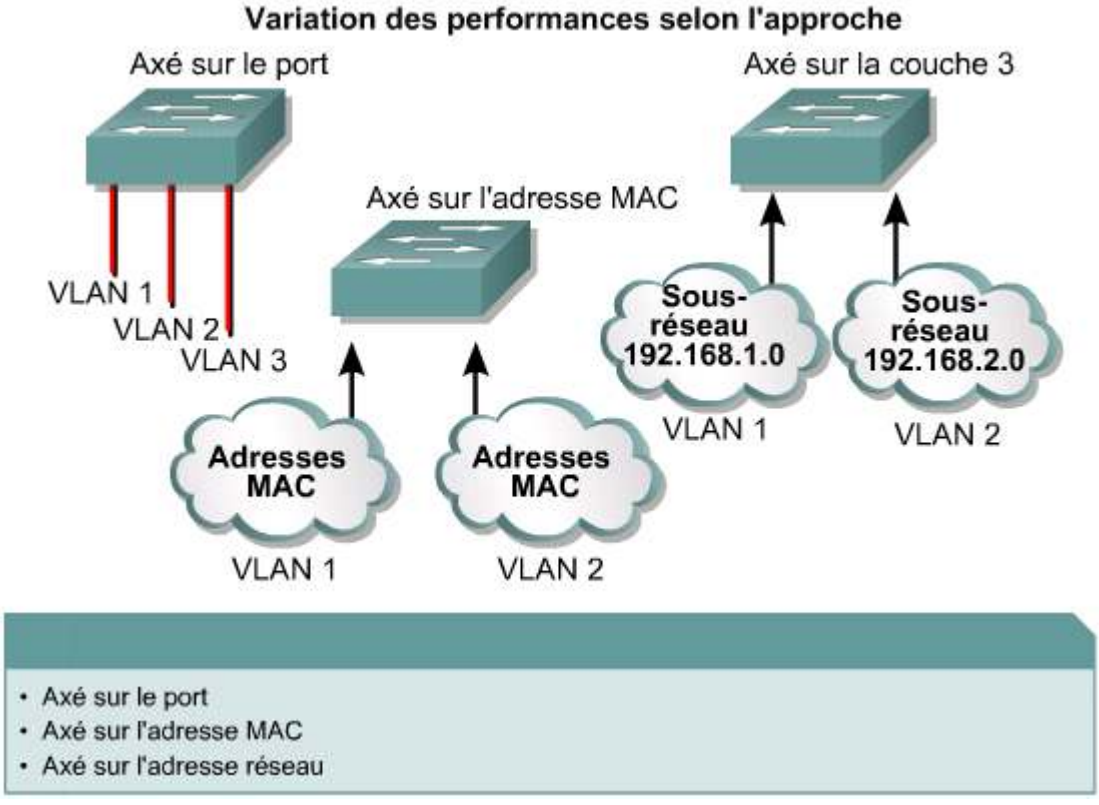


8.1 Concepts VLAN

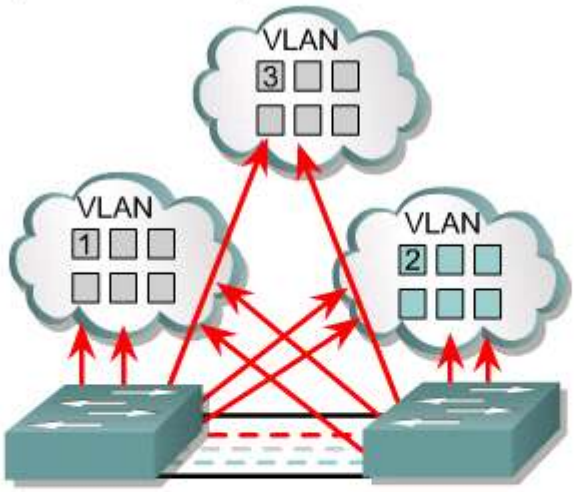
8.1.5 Types de VLAN

Il existe trois types d'appartenance à un VLAN permettant de déterminer et de contrôler le mode d'affectation d'une trame : 1 5

- VLAN axés sur le port
- VLAN axés sur l'adresse MAC
- VLAN axés sur le protocole

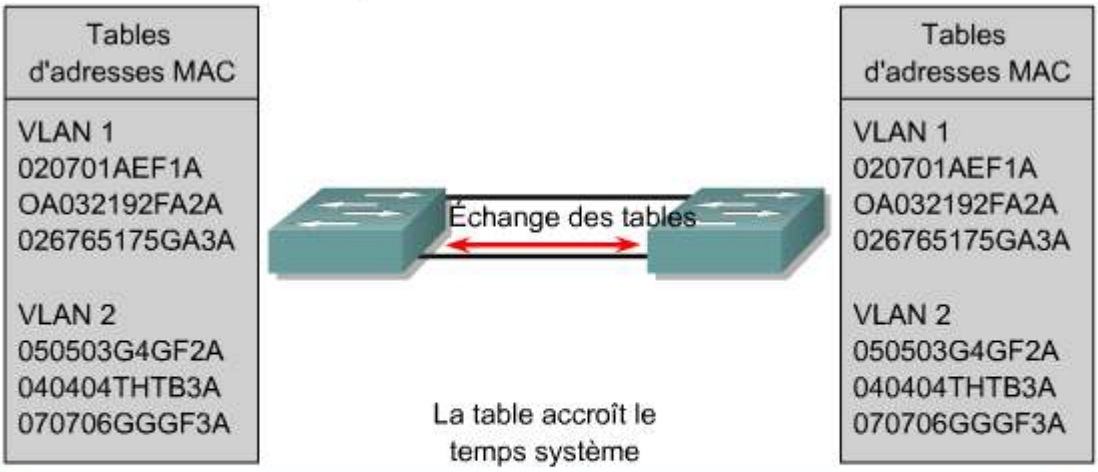


Optimisation des performances de transmission



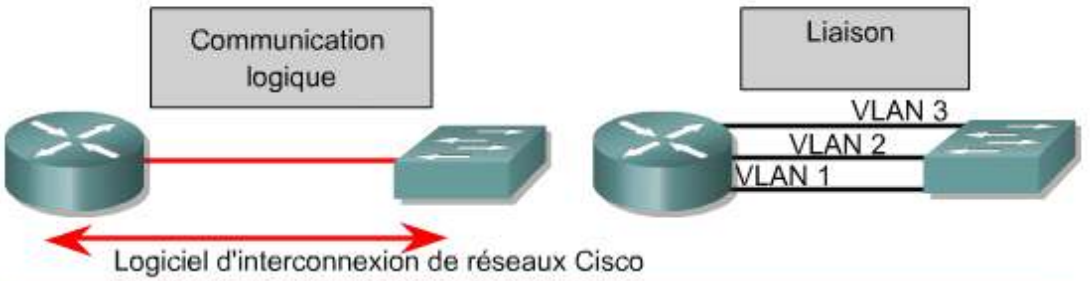
- Utilisateur affecté en fonction du port sur lequel il est connecté
- Ne nécessite aucune recherche dans le cas de circuits ASIC
- Facile à administrer par le biais de GUI
- Optimise la sécurité entre les VLAN
- Les paquets ne se dispersent pas dans d'autres domaines
- Facile à contrôler sur le réseau

Filtrage requis, impact sur les performances



- Utilisateur affecté sur la base des adresses MAC
- Flexibilité, ajoute du temps système
- Impact sur les performances, l'évolutivité et l'administration
- Offre un processus similaire pour les couches supérieures

Deux approches de topologie physique



L'utilisation de routeurs de couche 3 pour lier les VLAN procure les avantages suivants :

- Cela apporte plus de sécurité et améliore la gestion.
- Les liaisons logiques conservent les ports physiques.
- Les routeurs contrôlent l'accès aux VLAN.
- 255 VLAN ou plus peuvent être pris en charge par chaque routeur.

Types de VLAN	Description
Axé sur le port	• Méthode de configuration la plus courante. • Ports affectés individuellement, par groupes, par rangs ou sur au moins 2 commutateurs. • Facile à utiliser. • Souvent mis en œuvre lorsque que le protocole DHCP (Dynamic Host Control Protocol) est utilisé pour affecter des adresses IP aux hôtes du réseau.
Adresse MAC	• Rarement mis en œuvre de nos jours. • Chaque adresse doit être saisie dans le commutateur et configurée individuellement. • Utile d'après les utilisateurs. • Difficile à administrer, à dépanner et à gérer.
Axé sur le protocole	• Configuré comme les adresses MAC, mais utilise plutôt une adresse logique ou IP. • Plus utilisé en raison du protocole DHCP.

L'en-tête d'une trame est encapsulé ou modifié pour inclure un ID de VLAN avant que la trame ne soit envoyée sur la liaison entre les commutateurs. Avant le transfert de la trame vers l'unité de destination, le format d'origine de son en-tête est rétabli.

Le nombre de VLAN dans un commutateur varie en fonction des facteurs suivants:

- Modèles de trafic
- Types d'application
- Besoins d'administration réseau
- Standardisation de groupes

Le système d'adressage IP est également un facteur important à prendre en compte lors de la définition de la taille du commutateur et du nombre de VLAN.

Par exemple, un réseau utilisant un masque sur 24 bits pour définir un sous-réseau dispose d'un total de 254 adresses hôte autorisées sur un seul sous-réseau. Étant donné qu'une correspondance bi-univoque entre les VLAN et les sous-réseaux IP est fortement recommandée, il ne peut y avoir plus de 254 hôtes dans un des VLAN. Il est également recommandé de ne pas étendre les VLAN au-delà du domaine de couche 2 du commutateur de distribution.

Il existe deux méthodes principales d'étiquetage de trames: ISL (Inter-Switch Link) et 802.1Q. L'étiquetage de trames ISL, un protocole propriétaire Cisco, était autrefois très courant. Il est aujourd'hui remplacé progressivement par le standard 802.1Q d'étiquetage de trames.

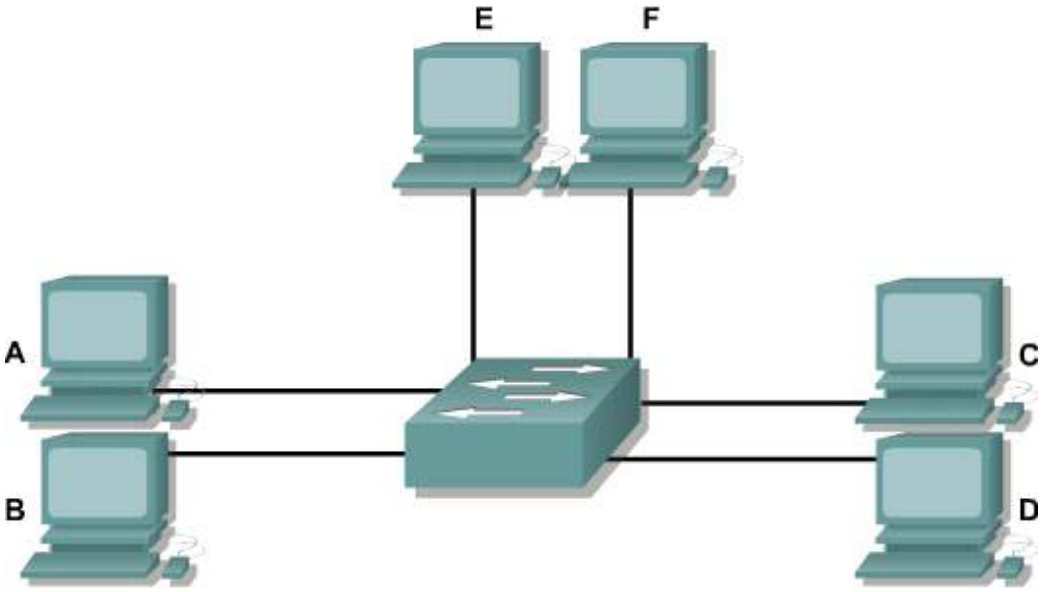
Étiquetage	Méthode	Médias	Description
ISL (Inter-Switch Link)	Fast Ethernet	L'en-tête ISL encapsule la trame LAN et contient un champ ID de VLAN.	La trame est allongée.
802.IQ	Fast Ethernet	Protocole VLAN Ethernet défini par l'IEEE.	L'en-tête est modifié.
Émulation de LAN (LANE)	ATM	Aucune étiquetage	Une connexion virtuelle implique un ID de VLAN.

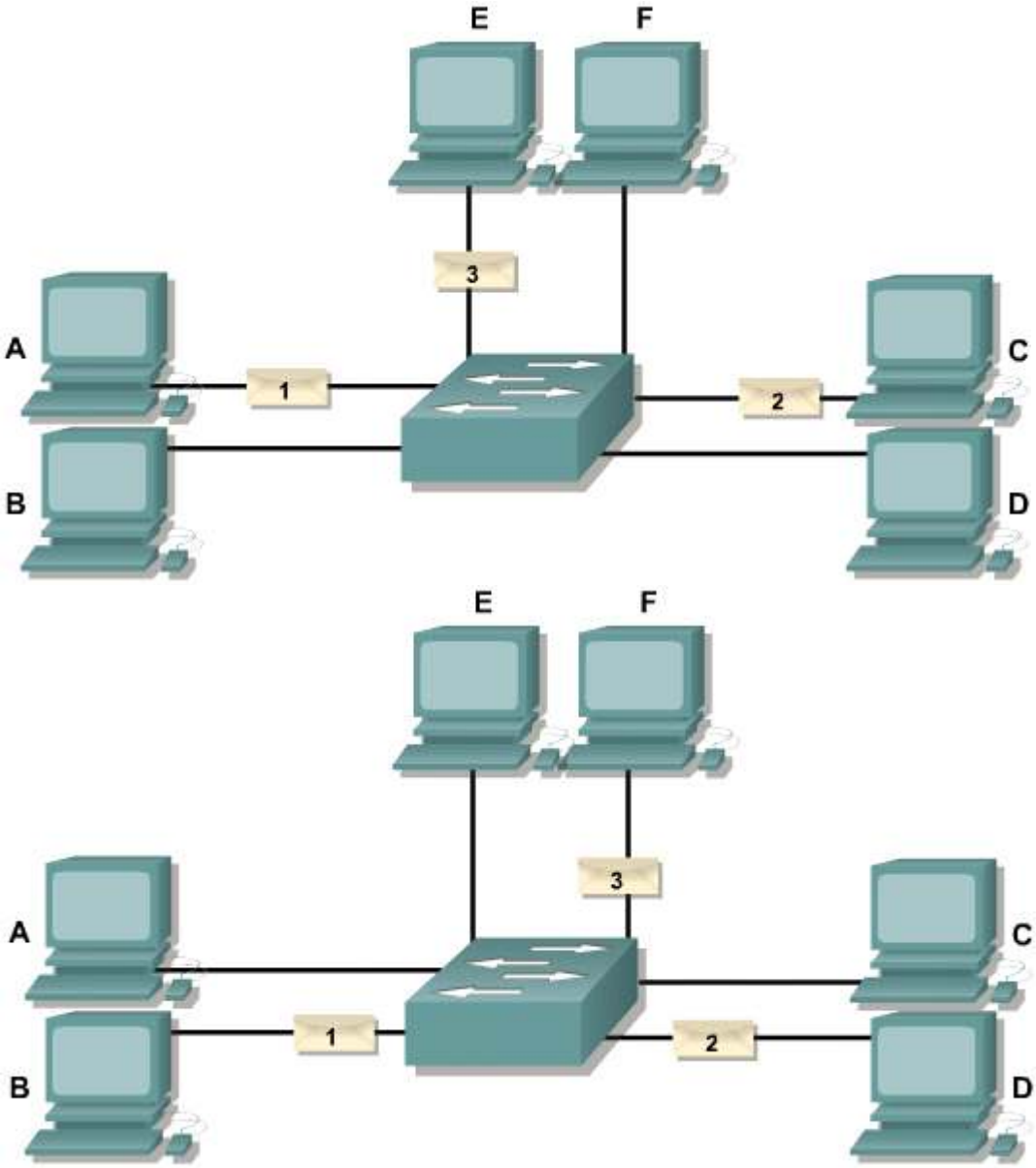
Lorsque des trames sont reçus par le commutateur à partir d'une unité de station d'extrémité reliée, un identifiant de trame unique est ajouté dans chaque en-tête. Cette information d'en-tête désigne l'appartenance à un VLAN de chaque trame. La trame est ensuite transmise aux commutateurs ou routeurs appropriés sur la base de l'ID de VLAN et de l'adresse MAC. Sur le nœud de destination, l'ID du VLAN est supprimé du trame par le commutateur contigu et transmis à l'unité connectée. L'étiquetage de trames est un mécanisme de contrôle du flux de broadcasts et d'applications qui n'interfère pas avec le réseau et les applications. L'émulation LAN (LANE) est une manière pour un réseau ATM (Asynchronous Transfer Mode) de simuler un réseau Ethernet. Il n'y a pas d'étiquetage dans LANE, mais la connexion virtuelle utilisée implique un ID de VLAN.

8.2 Configuration VLAN

8.2.1 Notions de base sur les VLAN

Dans un environnement commuté, une station ne voit que le trafic qui lui est destiné. Le commutateur filtre le trafic du réseau afin que la station de travail dispose de toute la bande passante pour l'envoi ou la réception de paquets. Contrairement à un système à concentrateur partagé sur lequel une seule station peut transmettre à la fois, le réseau commuté permet plusieurs transmissions simultanées au sein d'un domaine de broadcast. Le réseau commuté effectue cela sans effet direct sur les autres stations à l'intérieur ou à l'extérieur du domaine de broadcast. 1 Les paires de stations A/B, C/D et E/F peuvent toutes communiquer sans avoir un impact sur les autres paires de stations.





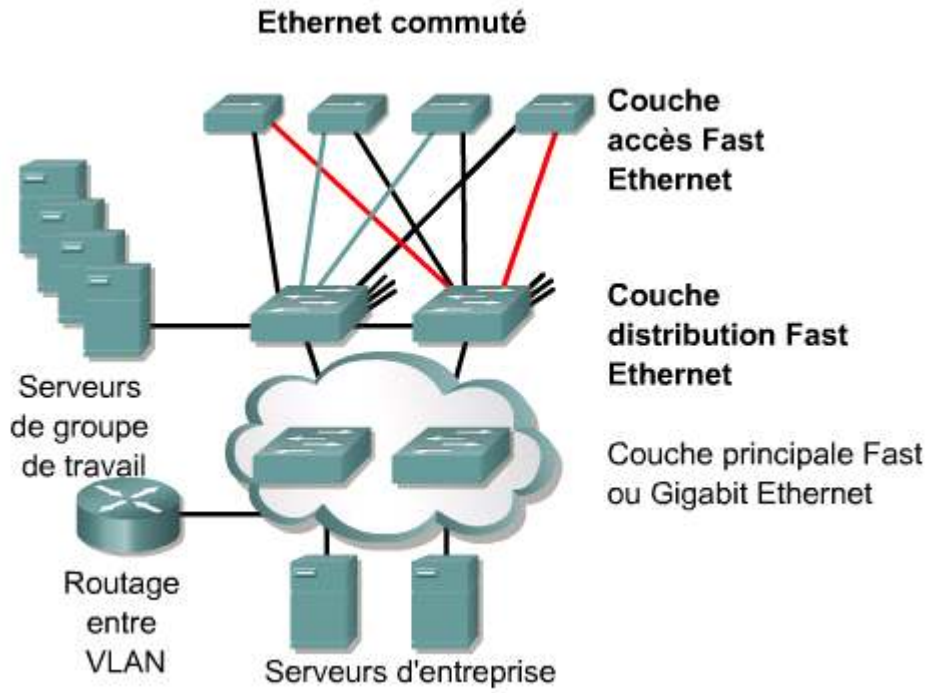
Une adresse réseau de couche 3 unique doit être affectée à chaque VLAN. Cela permet aux routeurs de commuter les paquets entre les VLAN.

Les VLAN peuvent être créés sous forme de réseaux de bout en bout ou exister à l'intérieur de frontières géographiques.

Un réseau VLAN de bout en bout a les caractéristiques suivantes:

- Les utilisateurs sont regroupés en VLAN qui dépendent de leur groupe de travail ou de leur fonction, mais pas de leur localisation physique.
- Tous les utilisateurs d'un VLAN doivent avoir les mêmes modèles de flux de trafic 80/20.
- Lorsqu'un utilisateur se déplace sur le campus, son appartenance à un VLAN ne doit pas changer.
- Chaque VLAN est caractérisé par un ensemble commun de besoins de sécurité pour tous les membres.

À partir de la couche accès, des ports de commutation sont fournis pour chaque utilisateur. 2Chaque couleur représente un sous-réseau. En raison du déplacement des personnes, chaque commutateur devient finalement un membre de tous les VLAN. L'étiquetage de trames est utilisé pour transporter des informations VLAN multiples entre les locaux de câblage de couche accès et les commutateurs de couche distribution.



ISL est un protocole propriétaire de Cisco qui met à jour les informations VLAN au fur et à mesure du transfert du trafic entre les commutateurs et les routeurs. IEEE 802.1Q est un mécanisme d'étiquetage VLAN (norme ouverte IEEE) dans les installations de commutation. Les commutateurs Catalyst 2950 ne prennent pas en charge l'agrégation ISL.

Les serveurs de groupe de travail fonctionnent selon un modèle client/serveur. C'est pour cette raison qu'il a été tenté de garder les utilisateurs dans le même VLAN que leur serveur afin d'optimiser les performances de commutation de couche 2 et de centraliser le trafic.

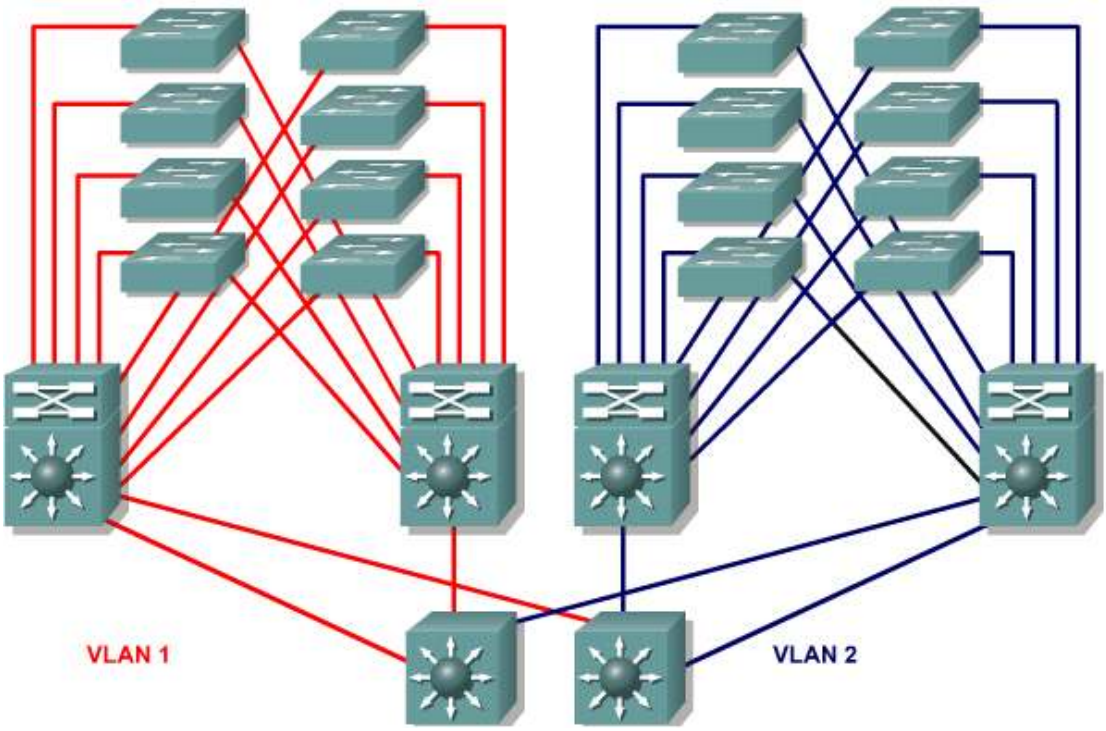
Dans la figure 2, un routeur de couche principale est utilisé pour acheminer les paquets entre les sous-réseaux. Le réseau est conçu sur la base de modèles de flux de trafic de telle sorte que 80 % du trafic soit contenu au sein d'un VLAN. Les 20 % restants traversent le routeur jusqu'aux serveurs d'entreprise et jusqu'aux réseaux Internet et WAN.

8.2.2 VLAN géographiques

8.2.2 VLAN géographiques

Les VLAN de bout en bout permettent de regrouper les équipements en fonction de l'utilisation des ressources. Cela inclut des paramètres comme l'utilisation du serveur, les équipes de projet et les services. Le but des VLAN de bout-en bout est de maintenir 80 % du trafic sur le VLAN local.

Les réseaux d'entreprise ayant centralisé leurs ressources, les VLAN de bout en bout sont devenus plus difficiles à mettre à jour. Les utilisateurs sont amenés à utiliser de nombreuses ressources différentes qui, pour la plupart, ne sont plus associées à leur VLAN. En raison de ces changements de localisation et d'utilisation des ressources, les VLAN sont à présent créés plus fréquemment autour de frontières géographiques plutôt que de frontières de standardisation. 1



Cette localisation géographique peut s'étendre à un bâtiment complet ou se limiter à un seul commutateur dans un local de câblage. Dans une structure VLAN, la nouvelle règle 20/80 est très fréquemment appliquée. 80 % du trafic est effectué à distance pour l'utilisateur contre 20 % en local. Bien que cette topologie implique pour l'utilisateur de traverser une unité de couche 3 afin d'atteindre 80 % des ressources, cette configuration permet au réseau de fournir une méthode cohérente et déterministe d'accès aux ressources.

8.2 Configuration VLAN

8.2.3 Configuration de VLAN statiques

Les VLAN statiques correspondent à l'affectation manuelle des ports d'un commutateur à un VLAN via une application de gestion de VLAN ou directement en travaillant sur le commutateur. Ces ports conservent la configuration VLAN qui leur est attribuée jusqu'à ce qu'elle soit changée manuellement. 1

VLAN statique

Un VLAN statique est qui réunissent les conditions suivantes:

- Les déplacements sont contrôlés et gérés.
- Il existe un logiciel d'administration de VLAN robuste pour configurer les ports.
- Il n'est pas souhaitable d'évaluer le temps système additionnel nécessaire pour mettre à jour les adresses MAC des stations d'extrémité et les tables de filtrages personnalisées.

- Les déplacements sont contrôlés et gérés.
- Il existe un logiciel d'administration de VLAN robuste pour configurer les ports.
- Il n'est pas souhaitable d'évaluer le temps système additionnel nécessaire pour mettre à jour les adresses MAC des stations d'extrémité et les tables de filtrage personnalisées.

Les VLAN dynamiques ne reposent pas sur des ports affectés à un VLAN spécifique.

Les lignes directrices suivantes doivent être suivies lors de la configuration de VLAN sur des commutateurs Cisco 29xx:

- Le nombre maximum de VLAN dépend du commutateur.
- Le VLAN 1 est l'un des VLAN par défaut.
- Le VLAN 1 est le VLAN Ethernet par défaut.
- Des annonces CDP (Cisco Discovery Protocol) et VTP (VLAN Trunking Protocol) sont envoyées sur le VLAN 1. (VTP sera abordé lors du module 9)

- L'adresse IP de Catalyst 29xx est associée par défaut au domaine de broadcast du VLAN 1.
- Le commutateur doit être en mode serveur VTP pour créer, ajouter ou supprimer des VLAN.

La création d'un VLAN sur un commutateur est une tâche très simple et directe. Si vous utilisez un commutateur à base de commandes Cisco IOS, passez en mode de configuration de VLAN en utilisant la commande **vlan database** en mode privilégié. Les étapes de création d'un VLAN sont indiquées ci-dessous. Un nom de VLAN peut également être configuré, si nécessaire.

```
Switch#vlan database
Switch(vlan)#vlan numéro_vlan
Switch(vlan)#exit
```

En quittant cette commande, le VLAN est appliqué au commutateur. L'étape suivante consiste à affecter le VLAN à une ou à plusieurs interfaces:

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#switchport access vlannuméro_vlan
```

Activité de TP

Exercice: Configuration de VLAN statiques

Dans ce TP, les étudiants vont apprendre à créer des VLAN statiques.

Activité de TP

Activité en ligne: Configuration de VLAN statiques

Dans ce TP, les étudiants créeront des VLAN statiques.

8.2 Configuration VLAN

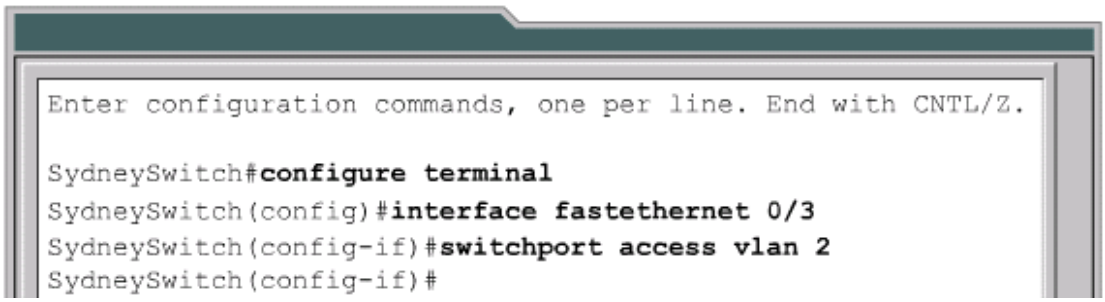
8.2.4 Vérification de la configuration VLAN

Il est fortement recommandé de vérifier la configuration VLAN à l'aide des commandes **show vlan**, **show vlan brief** ou **show vlan id***numéro_id*.

Les faits suivants s'appliquent aux VLAN:

- Un VLAN créé reste inutilisé jusqu'à ce qu'il soit associé à des ports de commutateur.
- Tous les ports Ethernet sont situés sur le VLAN 1 par défaut.

Reportez-vous à la figure 1 pour obtenir la liste des commandes applicables.



La figure 2 indique les étapes nécessaires pour affecter un nouveau VLAN à un port du commutateur Sydney.

```
Enter configuration commands, one per line. End with CNTL/Z.

SydneySwitch#configure terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 3
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

Les figures 3 et 4 présentent les informations affichées par les commandes **show vlan** et **show vlan brief**.

```
SydneySwitch#show vlan

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------

VLAN Name                Status    Ports
---- ------------------- ------- -------------------------------
1    default             active    Fa0/1, Fa0/2, Fa0/4
2    VLAN2               active    Fa0/3, Fa0/5, Fa0/6, Fa0/7
3    VLAN3               active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                   Fa0/12
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ---------- ------ -------
1    enet 100001 1500  -      -      -        -    -      1002   1003
2    enet 100002 1500  -      -      -        -    -      0      0
3    enet 100003 1500  -      -      -        -    -      0      0
1002 fddi 101002 1500  -      -      -        -    -      1      1003
1003 tr   101003 1500  1005   0      -        -    srb    1      1002
1004 fdnet 101004 1500  -      -      1        ibm  -      0      0
1005 trnet 101005 1500  -      -      1        bm   -      0      0
```

```
SydneySwitch#show vlan brief

VLAN Name                      Status    Ports
---- ----------------------- --------- -------------------------------
1    default                   active    Fa0/1, Fa0/2, Fa0/4
2    VLAN2                     active    Fa0/3, Fa0/5, Fa0/6, Fa0/7
3    VLAN3                     active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                         Fa0/12
1002 fddi-default              active
1003 token-ring-default        active
1004 fddinet-default           active
1005 trnet-default             active
```

Activité de TP

Exercice: Vérification des configurations VLAN.Dans ce TP, les étudiants créeront et nommeront deux VLAN, assigneront des ports et déplaceront des hôtes.

Activité de TP

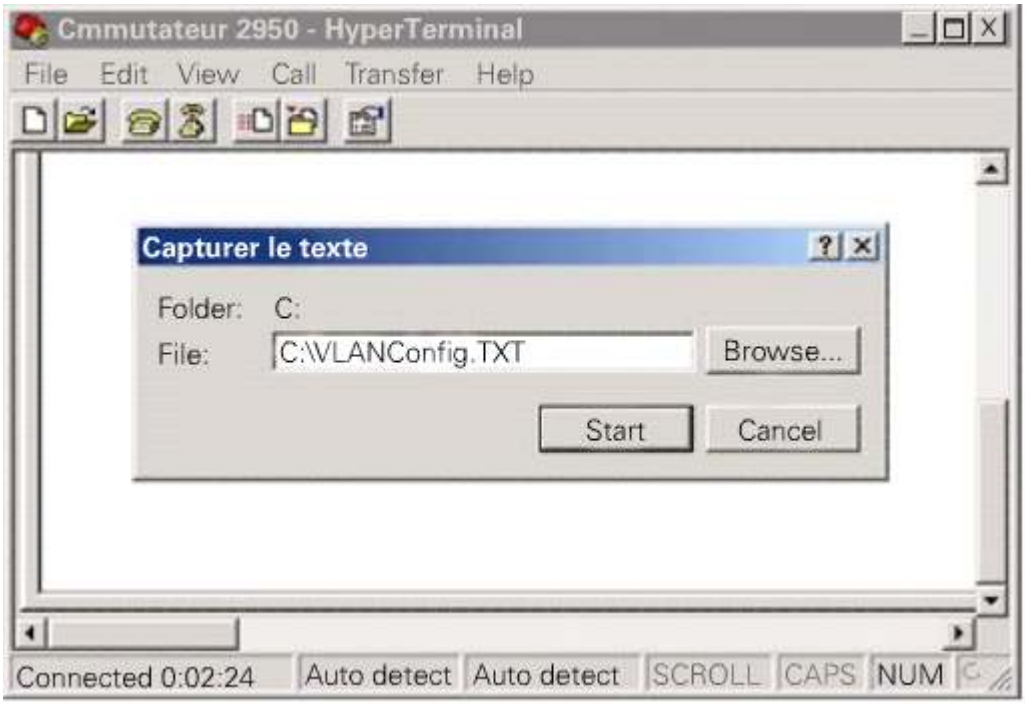
Activité en ligne: Vérification des configurations VLAN

Au cours de ce TP, les étudiants vont créer deux VLAN séparés sur le commutateur.

8.2 Configuration VLAN
8.2.5 Enregistrement de la configuration VLAN

Il est souvent utile de garder une copie de la configuration VLAN sous forme de fichier texte à des fins de sauvegarde ou d'audit.

Les paramètres de configuration du commutateur peuvent être sauvegardés de manière habituelle avec la commande **`copy running-config tftp`**. Alternativement, la fonction Capturer le texte de HyperTerminal peut être utilisée pour stocker les paramètres de configuration en démarrant la capture et ensuite en entrant des commandes telles que **`show running-config`** et **`show vlan`**. 1



8.2 Configuration VLAN
8.2.6 Suppression de VLAN

La suppression d'un VLAN à partir d'une interface de commutateur à base de commandes Cisco IOS est identique à la suppression d'une commande à partir d'un routeur.

```
Enter configuration commands, one per line. End with CNTL/Z.

SydneySwitch#configure terminal
SydneySwitch(config)#interface fastethernet 0/9
SydneySwitch(config-if)#switchport access vlan 300
SydneySwitch(config-if)#exit
SydneySwitch(config)#exit
```

Dans la figure 1, le FastEthernet 0/9 a été assigné au VLAN à l'aide de la commande switchport access vlan 300 en mode de configuration d'interface. Pour supprimer ce VLAN de l'interface, utilisez simplement la forme **no** de la commande. 2

```
Switch(config)#interface fastethernet 0/9
Switch(config-if)#no switchport access vlan 300
```

Pour enlever un VLAN entièrement d'un commutateur, entrez les commandes:

```
Switch#vlan database
Switch(vlan)#no vlan 300
```

Lorsqu'un VLAN est supprimé, tous les ports qui lui sont affectés deviennent inactifs. Toutefois, ces ports restent associés au VLAN supprimé jusqu'à ce qu'ils soient affectés à un nouveau VLAN.

```
Switch#show vlan brief

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

Switch#vlan database
Switch(vlan)#no vlan 300
Deleting VLAN 300...
Switch(vlan)#exit
APPLY completed.
Exiting....
Switch#show vlan brief

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

Switch#
```

Exercice: Suppression de configurations VLAN

Dans ce TP, les étudiants vont apprendre à supprimer des paramètres VLAN.

Activité de TP

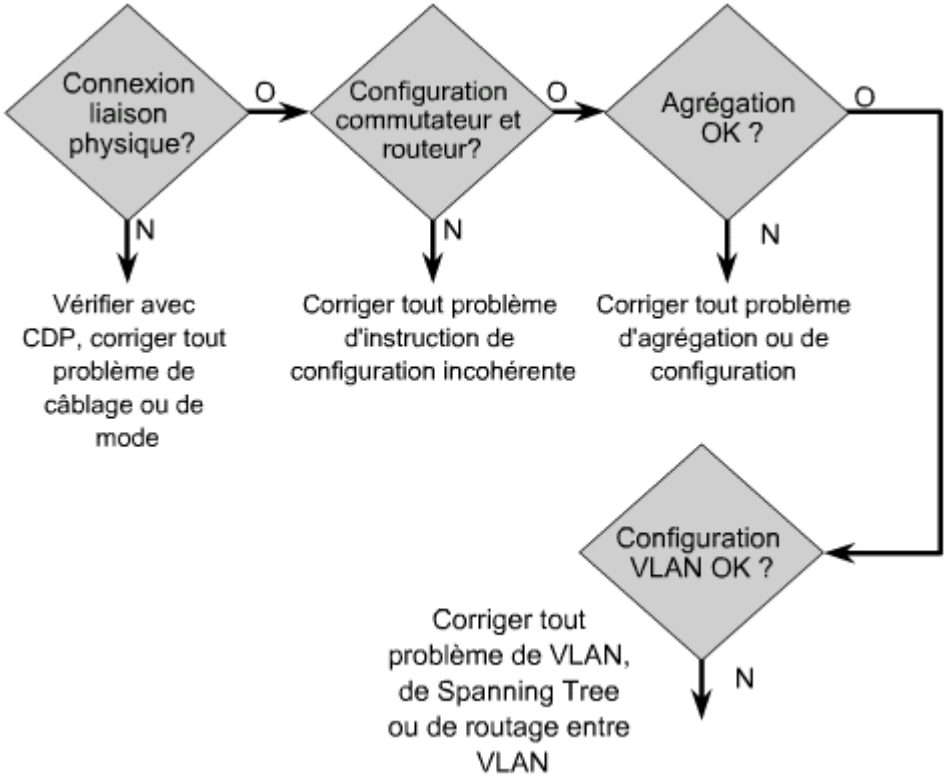
Activité en ligne: Suppression de configurations VLAN

Dans ce TP, les étudiants enlèveront la configuration d'un VLAN.

8.3 Dépannage des VLAN

8.3.1 Vue d'ensemble

Les VLAN sont fréquemment utilisés dans les réseaux de campus. Les VLAN offrent une grande souplesse de conception et de mise en œuvre aux ingénieurs réseau. Les VLAN assurent également la sécurité et le confinement des broadcasts, et les regroupements d'intérêts géographiquement différents. Toutefois, comme avec une commutation LAN de base, des problèmes peuvent survenir lors de la mise en œuvre des VLAN. Ce chapitre présente une partie des problèmes les plus courants pouvant survenir avec des VLAN, et fournit des outils et des techniques de dépannage. 1



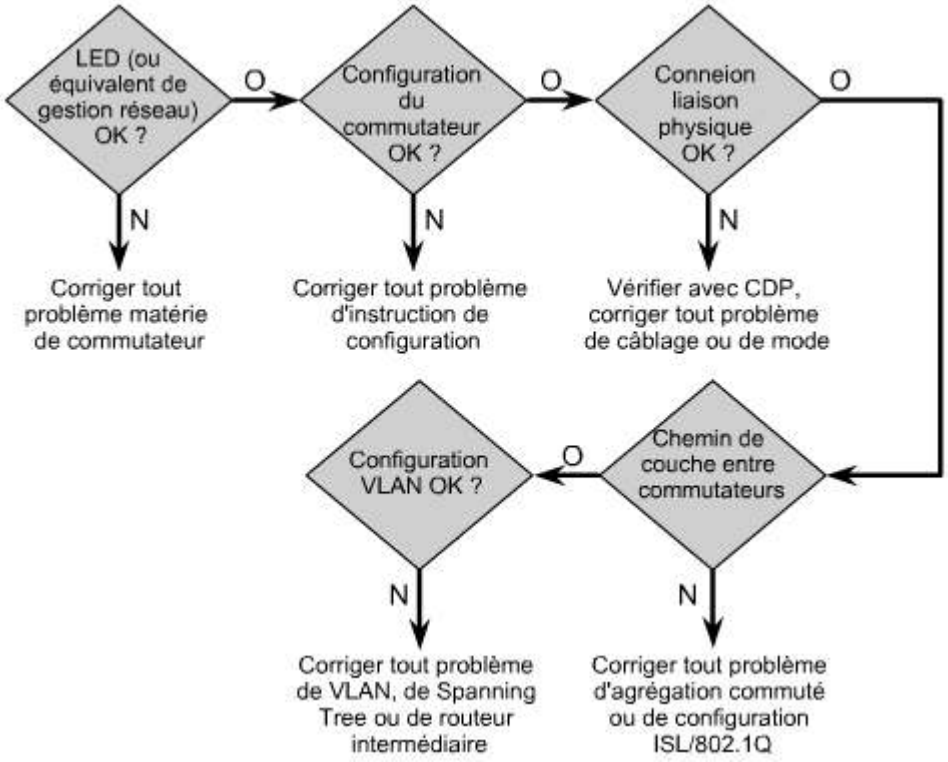
À la fin de ce chapitre, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Utiliser une approche systématique du dépannage VLAN
- Énumérer les étapes du dépannage général dans les réseaux commutés
- Décrire comment les problèmes de Spanning Tree peuvent conduire à des tempêtes de broadcast
- Utiliser les commandes **`show`** et **`debug`** pour dépanner les VLAN

8.3 Dépannage des VLAN

8.3.2 Processus de dépannage d'un VLAN

Il est important de développer une approche systématique pour le dépannage des problèmes liés aux commutateurs. Les étapes suivantes peuvent aider à identifier un problème sur un réseau commuté: [1]



1. Vérifiez les indications physiques, telles que l'état des LED.
2. Commencez par une configuration simple sur un commutateur, puis élargissez vos recherches.
3. Vérifiez la liaison de couche 1.
4. Vérifiez la liaison de couche 2.
5. Dépannez les VLAN qui s'étendent sur plusieurs commutateurs.

Lors du dépannage, vérifiez si le problème est récurrent ou résulte d'une défaillance isolée. Certains problèmes récurrents sont dus au nombre croissant de demandes de services par les ports de stations de travail qui, pour accéder aux ressources des serveurs, mettent en défaut les configurations, les agrégations ou la capacité du réseau. Par exemple, l'utilisation de technologies Web et d'applications traditionnelles, telles que le transfert de fichiers et le courrier électronique, engendre une augmentation du trafic réseau que les réseaux d'entreprise doivent gérer.

La plupart des réseaux LAN de campus doivent faire face à des modèles de trafic réseau imprévisibles qui résultent de la combinaison du trafic intranet, d'emplacements de serveurs de campus centralisés et de l'utilisation accrue des applications multicast. L'ancienne règle 80/20, par laquelle seulement 20 % du trafic réseau traversait le backbone, est obsolète. La navigation Web interne permet maintenant aux utilisateurs de localiser et de consulter des informations sur l'ensemble de l'intranet de l'entreprise. Les modèles de trafic sont dictés par l'emplacement des serveurs et non par les configurations de groupe de travail physiques auxquelles ils sont associés.

Si un réseau est souvent confronté à des symptômes de goulot d'étranglement, comme des dépassements de capacité excessifs, des trames abandonnées et des retransmissions, cela peut provenir d'un nombre trop élevé de ports dirigés vers une agrégation unique, ou de trop nombreuses requêtes à des ressources globales et aux serveurs intranet.

Les symptômes de goulot d'étranglement peuvent également survenir parce qu'une grande partie du trafic est obligée de traverser le backbone. La fréquence des accès sans contraintes est également un autre facteur, car les utilisateurs font appel à des applications multimédias et à des ressources d'entreprise basées sur le Web. Dans ce cas, il peut être nécessaire d'envisager une augmentation des ressources réseau afin de répondre à la demande.

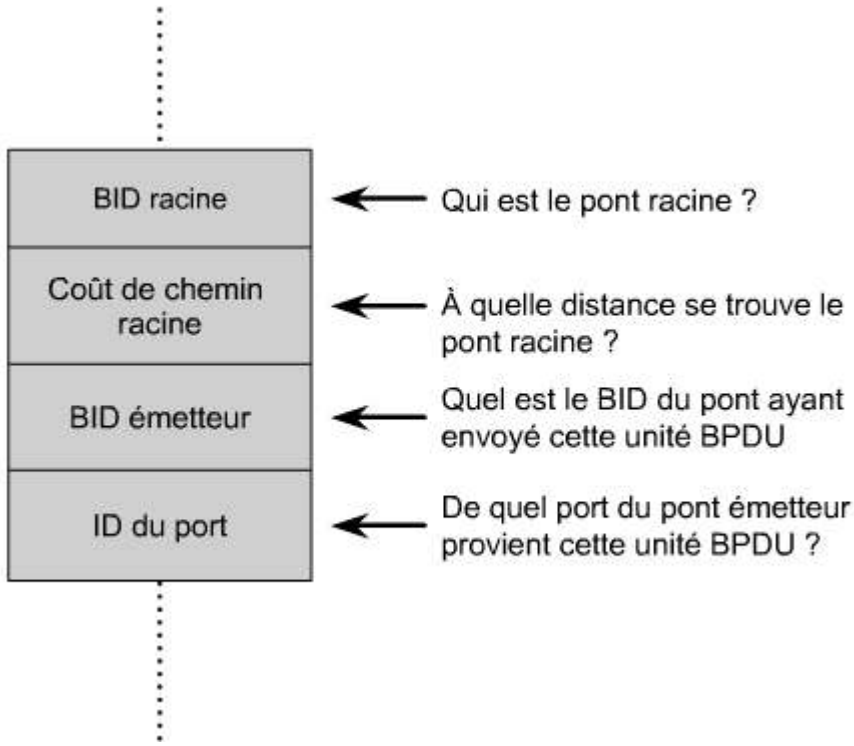
8.3 Dépannage des VLAN

8.3.3 Comment éviter les tempêtes de broadcast

Une tempête de broadcast se produit lorsqu'un grand nombre de paquets de broadcast sont reçus sur un port. La transmission de ces paquets peut provoquer un ralentissement ou une temporisation du réseau. Le contrôle des tempêtes est configuré globalement pour le commutateur, mais est exécuté au niveau de chaque port. Le contrôle des tempêtes est désactivé par défaut.

La prévention contre les tempêtes de broadcast par le paramétrage de valeurs de seuil élevées ou faibles permet d'éliminer l'excès de trafic MAC broadcast, multicast ou unicast. De plus, la configuration de valeurs pour augmenter les seuils sur un commutateur conduit à la désactivation du port.

Les problèmes STP incluent les tempêtes de broadcast, les boucles, ainsi que les unités BPDU et les paquets abandonnés. 1



La fonction de STP est de garantir qu'aucune boucle logique ne survient dans un réseau en désignant un pont racine. Le pont racine est le point central d'une configuration Spanning Tree qui contrôle le fonctionnement du protocole.

La localisation du pont racine dans le réseau étendu de routeurs et de commutateurs est nécessaire au dépannage. Les commandes **show** du routeur et du commutateur permettent d'afficher des informations sur le pont racine. 2

```
MDF_Switch#show spanning-tree

Spanning tree 1 is executing the IEEE compatible
Spanning Tree protocol
  Bridge Identifier has priority 32768, address
  0006.28ab.5e00 Configured hello time 2, max age
  20, forward delay 15 We are the root of the
  spanning tree Topology change flag not set,
  detected flag not set, changes 18
  Times: hold1, topology change 0, notification 2
         hello 2, max age 20, forward delay 15
  Timers:hello 0, topology change 0, notification 0

Interface Fa0/1 (port 13) in Spanning tree 1 is
  FORWARDING
  Port path cost 19, Port priority 128
  Designated root has priority 32768, address
  0006.28ab.5e00
  Designated bridge has priority 32768, address
  0006.28ab.5e00
  Designated port is 13, path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 13075, received 14

Interface Fa0/2 (port 14) in Spanning tree 1 is
  FORWARDING Port path cost 19, Port priority 128
  Designated root has priority 32768, address
  0006.28ab.5e00
  Designated bridge has priority 32768, address
  0006.28ab.5e00
  Designated port is 14, path cost 0
  Timers: message age 0, forward delay 0, hold 0
  BPDU: sent 6468, received 0
```

La configuration de compteurs de pont racine permet de définir des paramètres de délai de transmission ou d'âge maximum pour les informations STP. 3La configuration manuelle d'une unité en tant que pont racine est une autre option de configuration.

Compteur	Objectif principal	Par défaut
Délai Hello	Délai entre les envois d'unités BPDU de configuration par le pont racine	2 Secs
Délai de transmission	Durée des états d'écoute et d'apprentissage	15 Secs
max_age	Durée de stockage des unités BPDU	20 Secs

Si le réseau étendu de commutateurs et de routeurs connaît une période d'instabilité, cela aide à minimiser les processus STP entre les unités.

S'il devient nécessaire de réduire le trafic des unités BPDU, paramétrez les compteurs du pont racine sur leurs valeurs maximales. En particulier, définissez le paramètre de délai de transmission sur 30 secondes (valeur maximale) et le paramètre **max_age** sur 40 secondes (valeur maximale).

Un port physique sur un routeur ou un commutateur peut faire partie de plusieurs Spanning Tree s'il s'agit d'une agrégation.

Le protocole STP (Spanning-Tree Protocol) est considéré comme l'un des protocoles de couche 2 les plus importants sur les commutateurs Catalyst. En empêchant les boucles logiques dans un réseau ponté, STP permet une redondance de couche 2 sans générer de tempêtes de broadcast.

Minimisez les problèmes de Spanning Tree en développant activement une étude de base du réseau.

8.3 Dépannage des VLAN

8.3.4 Dépannage des VLAN

Les commandes **show** et **debug** peuvent être extrêmement utiles lors du dépannage de LAN virtuels. La figure 1 illustre les problèmes les plus fréquents rencontrés lors du dépannage de VLAN.

Problème	Explication et solution possible
La configuration des extrémités de l'agrégation indique des VLAN différents.	Les différentes extrémités d'une agrégation indiquent des VLAN différents. Par exemple, vlan1, vlan2 et vlan3 sont activés sur une extrémité, mais pas sur l'autre extrémité.
Protocole	Les différentes extrémités d'une liaison indiquent des protocoles différents. Par exemple, cela peut se produire sur une liaison Fast Ethernet avec ISL (Inter-Switch Link) activé sur une extrémité mais pas sur l'autre.
Unique	Les différentes extrémités d'une liaison VLAN unique indiquent des VLAN différents lorsque les commutateurs ne sont pas capables de prendre en charge plusieurs VLAN et lorsqu'aucun protocole d'encapsulation d'agrégation n'est exécuté.
Conflit de noms	Deux ensembles de commutateurs déconnectés ont des VLAN de même nom. Implications: • les VLAN sont divisés en au moins deux parties disjointes. • Les paquets d'une partie ne sont pas acheminés vers l'autre partie. Solution possible: • Renommez un des LAN virtuels.
Conflit d'index VLAN	Même nom de VLAN sur différents commutateurs mais avec des index ou des domaines de VLAN différents. Le trafic des commutateurs qui identifient ce VLAN avec un certain numéro n'est pas acheminé vers les ports des commutateurs qui ont un autre numéro pour ce VLAN. Solutions possibles: • Renommez un des LAN virtuels. • Supprimez les deux VLAN. Recréez un VLAN unique avec ce nom.
Conflit SAID	Indique des numéros SAID différents sur le même VLAN.

Pour dépanner le fonctionnement de connexions de routeur Fast Ethernet à des commutateurs, il est nécessaire de s'assurer que la configuration de l'interface du routeur est complète et correcte. Vérifiez qu'une adresse IP n'est pas configurée sur l'interface Fast Ethernet. Des adresses IP sont configurées sur chaque sous-interface d'une connexion VLAN. Vérifiez que la configuration duplex sur le routeur correspond à celle du port ou de l'interface approprié(e) sur le commutateur.

La commande **show vlan** permet d'afficher les informations VLAN du commutateur.

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

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1003 tr    101003     1500  -      -      -        -    srb      0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

Switch#
```

La figure 2 présente les informations affichées par la commande **show vlan**. L'affichage indique l'ID du VLAN, son nom, son état et les ports qui lui sont affectés.

La commande **show vlan** permet d'afficher des informations relatives au VLAN sur le routeur. La commande **show vlan** suivie du numéro de VLAN permet d'afficher les informations spécifiques à ce VLAN sur le routeur.

Mot-clé	Description
trunk	(Facultatif) Mot-clé qui demande de forcer l'affichage d'informations uniquement sur les ports multi-VLAN.
vlan	Numéro du VLAN. Si le numéro du VLAN n'est pas indiqué, tous les VLAN sont affichés.
notrunk	(Facultatif) Mot-clé qui demande de forcer l'affichage d'informations uniquement sur les ports en mode "access"
mapping	Mot-clé pour afficher les informations de la table de correspondance du VLAN.
type	Type de VLAN ; les valeurs valides sont Ethernet, FDDI, FDDInet, TrBRF et TrCRF.

3 Les informations affichées par la commande incluent l'ID du VLAN, ainsi que des informations sur la sous-interface du routeur et le protocole. 4

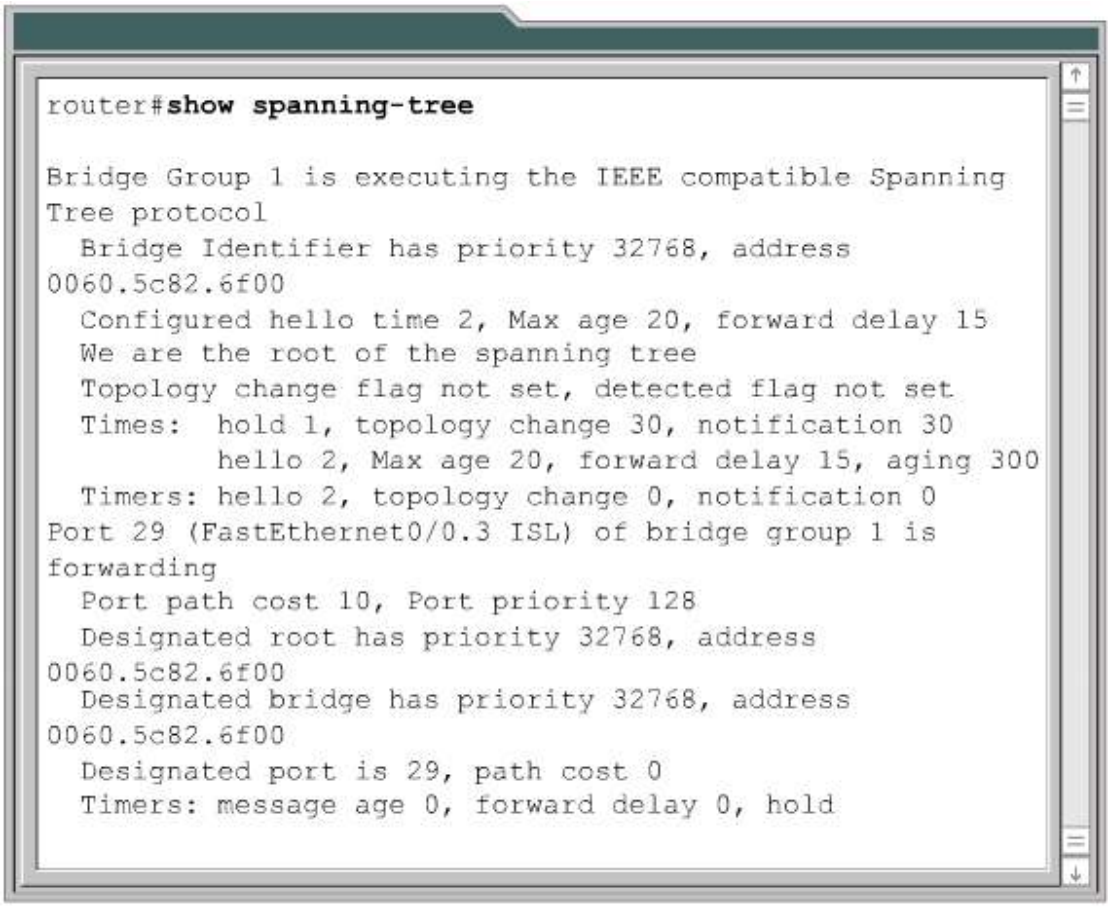
Champ	Description
VLAN	Numéro du VLAN.
Name	Nom, s'il est configuré, du VLAN.
Status	État du VLAN (activé ou arrêté).
IfIndex	Index d'interface, affecté par SNMP.
Mod/Ports, VLANs	Ports appartenant au VLAN.
Type	Type de média du VLAN.
SAID	Valeur ID d'association de sécurité du VLAN.
MTU	Taille d'unité de transfert d'information maximale (MTU) pour le VLAN.
Parent	VLAN parent, le cas échéant.
RingNo	Numéro d'anneau du VLAN, le cas échéant.
BrdgNo	Numéro de pont pour le VLAN, le cas échéant.
Stp	Type de protocole Spanning Tree utilisé sur le VLAN.
BrdgMode	Mode de pontage pour ce VLAN. Les valeurs possibles sont SRB et SRT ; la valeur par défaut est SRB.
Trans1	Premier VLAN de conversion utilisé pour convertir FDDI ou Token Ring en Ethernet.
Trans2	Second VLAN de conversion utilisé pour convertir FDDI ou Token Ring en Ethernet.
AREHops	Nombre maximum de sauts pour les trames d'exploration de routes. Les valeurs possibles sont comprises entre 1 et 13 ; la valeur par défaut est 7.
STEHops	Nombre maximum de sauts pour les trames d'exploration Spanning Tree. Les valeurs possibles sont comprises entre 1 et 13 ; la valeur par défaut est 7.
Backup CRF	Indique si TrCRF est un chemin de secours pour le trafic.

La commande **`show spanning-tree`** indique la topologie Spanning Tree connue du routeur.

Champ	Description
Port 29	Numéro de port associé à l'interface ; le numéro et la priorité du port forment l'ID du port
(FastEthernet0)	Interface sur laquelle le pontage de conversion a été configuré
of bridge group 1	Groupe de ponts auquel l'interface a été assignée
is forwarding	État de l'interface ; les valeurs possibles sont les suivantes : • Désactivation • Écoute • Apprentissage • Transmission • Blocage
Path cost 10	Coût de la route associé à l'interface, déterminé par défaut ou à l'aide de la commande bridge-group path cost
priority 128	Priorité du port

5 Cette commande affiche les paramètres STP utilisés par le routeur pour un pont Spanning Tree dans le réseau routeur/commutateur.

La première partie des informations affichées par la commande **`show spanning-tree`** répertorie les paramètres de configuration Spanning Tree globaux, suivis de ceux qui sont propres aux interfaces données. 6



Le groupe de ponts 1 exécute le protocole Spanning Tree compatible IEEE.

Les lignes suivantes des informations affichées indiquent les paramètres de fonctionnement actuels du Spanning Tree:

```
Bridge Identifier has priority 32768, address 0008.e32e.e600 Configured hello time
2, Max age 20, forward delay 15
```

La ligne suivante des informations affichées indique que le routeur est la racine du Spanning Tree:

```
We are the root of the spanning tree.
```

Les informations principales de la commande **`show spanning-tree`** créent une carte du réseau STP.

La commande **`debug sw-vlan packets`** affiche des informations générales sur les paquets VLAN reçus mais non configurés pour prendre en charge le routeur. Les paquets VLAN que le routeur peut acheminer ou commuter sont comptés et indiqués lors de l'exécution de la commande **`show sw-vlan`**.

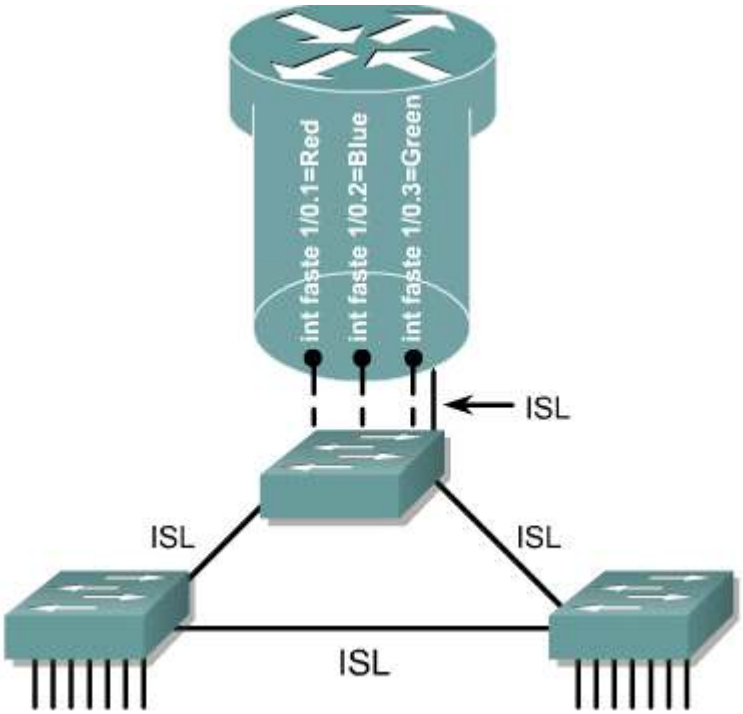
8.3 Dépannage des VLAN

8.3.5 Scénarios de dépannage d'un VLAN

Pour être compétent en matière de dépannage de réseaux commutés, il est nécessaire de connaître les techniques appropriées et de les adapter aux besoins de l'entreprise. L'expérience est le meilleur moyen d'améliorer ses compétences en matière de dépannage.

Deux scénarios de dépannage de VLAN correspondant aux problèmes les plus fréquents sont présentés. Chaque scénario part de l'analyse du problème jusqu'à sa résolution. Par le biais de commandes spécifiques et de la collecte d'informations pertinentes découlant des résultats, le processus de dépannage peut être mis en place.

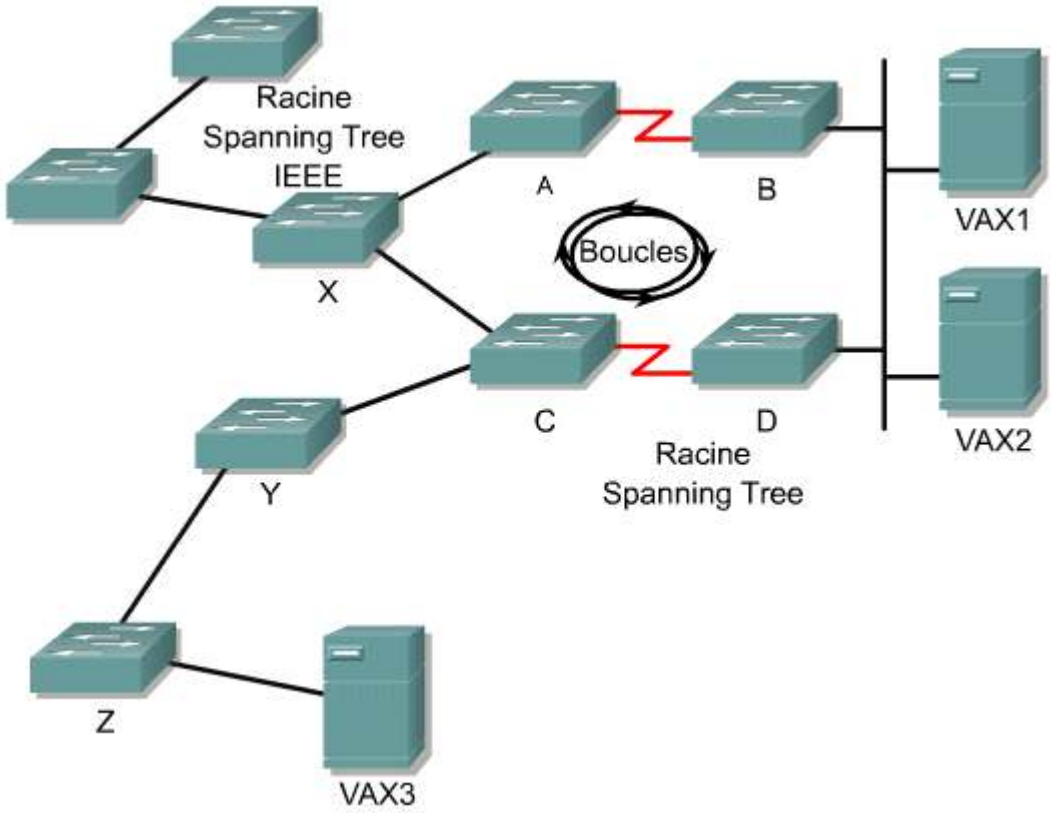
Scénario 1 : Aucun lien multi-VLAN ne peut être établi entre un commutateur et un routeur. 1



En cas de difficultés avec une connexion multi-VLAN entre un commutateur et un routeur, envisagez les causes possibles suivantes:

1. Vérifiez que le port est connecté et qu'il ne reçoit pas d'erreurs de couche physique, d'alignement ou de FCS (séquence de contrôle de trame). Pour cela, utilisez la commande **`show interface`** sur le commutateur.
2. Vérifiez que le mode duplex et la vitesse sont correctement paramétrés entre le commutateur et le routeur. Pour cela, utilisez la commande **`show interface status`** sur le commutateur ou la commande **`show interfaces`** sur le routeur.
3. Configurez l'interface de routeur physique avec une sous-interface pour chaque VLAN qui achemine le trafic. Pour vérifier cela, exécutez la commande **`show interfaces`** de l'IOS. Vérifiez également pour chaque sous-interface du routeur que le type d'encapsulation, le numéro de VLAN, l'adresse IP et le masque de sous-réseau sont correctement configurés. Pour cela, utilisez les commandes **`show interfaces`** ou **`show running-config`** de l'IOS.
4. Vérifiez que le routeur exécute une version de l'IOS qui prend en charge l'agrégation. Pour cela, utilisez la commande **`show version`**.

Scénario 2 : Paquets abandonnés et boucles.



Les ponts Spanning Tree utilisent des paquets BPDU de notification de changement de topologie pour signaler aux autres ponts un changement dans la topologie Spanning Tree du réseau. Le pont dont l'identifiant est le plus petit dans le réseau devient la racine. Les ponts envoient ces paquets BPDU chaque fois qu'un port passe à l'état de transmission ou en sort, tant qu'il y a d'autres ports dans le même groupe de ponts. Ces unités BPDU migrent vers le pont racine.

Il ne peut exister qu'un seul pont racine par réseau ponté. Un processus de sélection détermine le pont racine. La racine détermine les valeurs des messages de configuration, dans les unités BPDU, puis définit les compteurs pour les autres ponts. D'autres ponts désignés déterminent le chemin le plus court vers le pont racine et sont chargés d'annoncer les unités BPDU aux autres ponts par l'intermédiaire de ports désignés. Un pont doit avoir des ports à l'état de blocage s'il existe une boucle physique.

Des problèmes peuvent survenir pour les interréseaux dans lesquels les deux algorithmes Spanning Tree IEEE et DEC sont utilisés par des nœuds de pontage. Ces problèmes proviennent de divergences dans la manière dont les nœuds de pontage gèrent les paquets BPDU Spanning Tree ou les paquets HELLO, et dans la façon de gérer les données.

Dans ce scénario, les commutateurs A, B et C exécutent l'algorithme Spanning Tree IEEE. Par mégarde, le commutateur D est configuré pour utiliser l'algorithme Spanning Tree DEC.

Le commutateur A se proclame racine IEEE et le commutateur D, racine DEC. Les commutateurs B et C transmettent des informations racine sur toutes les interfaces pour le Spanning Tree IEEE. En revanche, le commutateur D abandonne les informations Spanning Tree IEEE. De même, les autres routeurs ignorent le fait que le routeur D se proclame racine.

En conséquence, aucun des ponts ne croit qu'il y a une boucle et lorsqu'un paquet de broadcast est envoyé sur le réseau, une tempête de broadcast se produit sur tout l'interréseau. Cette tempête de broadcast inclut les commutateurs X et Y, et même au-delà.

Pour résoudre ce problème, reconfigurez le commutateur D pour IEEE. Bien qu'un changement de configuration soit nécessaire, cela peut ne pas suffire pour rétablir la connectivité. Il existe un délai de reconvergence car les unités échangent des unités BPDU et recalculent un Spanning Tree pour le réseau.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Agrégation ISL et 802.1Q
- VLAN géographiques
- Configuration de VLAN statiques sur les commutateurs Catalyst de la série 29xx
- Vérification et enregistrement de configurations VLAN
- Suppression de VLAN d'un commutateur
- Définition de VLAN
- Avantages des LAN virtuels
- Utilisation de VLAN pour créer des domaines de broadcast
- Utilisation de routeurs pour les communications entre des VLAN
- Principaux types de VLAN
- Approche systématique du dépannage VLAN
- Étapes du dépannage général dans les réseaux commutés
- Problèmes de Spanning Tree engendrant des tempêtes de broadcast
- Utilisation des commandes **`show`** et **`debug`** pour dépanner les VLAN

Résumé

- Le concept de réseau local virtuel (VLAN) est une fonctionnalité importante de la commutation Ethernet. Un VLAN est un groupement logique d'unités ou d'utilisateurs. Ces unités ou ces utilisateurs peuvent être regroupés par fonction, service, application, etc., et ce, quel que soit le segment physique LAN où ils se trouvent.
- Les VLAN augmentent les performances globales du réseau en regroupant les utilisateurs et les ressources qui communiquent le plus fréquemment les uns avec les autres.
- Les VLAN peuvent améliorer l'évolutivité, la sécurité et la gestion des réseaux. Les routeurs dans les topologies VLAN offrent des services de filtrage des broadcasts, de sécurité et de gestion du flux du trafic.
- Les VLAN peuvent être créés sous forme de réseaux de bout en bout qui englobent l'ensemble de la matrice de commutation ou exister à l'intérieur de frontières géographiques. Les VLAN de bout en bout permettent de regrouper les équipements en fonction de l'utilisation des ressources.
- Les VLAN statiques correspondent aux ports d'un commutateur qui sont affectés manuellement à un VLAN via une application de gestion de VLAN ou directement à l'intérieur d'un commutateur.
- Les VLAN offrent une grande souplesse de conception et de mise en œuvre aux ingénieurs réseau.

Vue d'ensemble

Les premiers VLAN étaient difficiles à mettre en œuvre sur les réseaux. La plupart des VLAN étaient définis sur chaque commutateur, ce qui signifie que la création de VLAN sur un réseau étendu était une tâche complexe. Chaque fabricant de commutateur avait une conception différente de la mise en place des VLAN sur leurs commutateurs, ce qui compliquait davantage le processus. Le concept d'agrégation de VLAN a été développé pour résoudre ces problèmes.

Le mécanisme d'agrégation de VLAN permet de définir de nombreux VLAN au sein d'une société en ajoutant des étiquettes spéciales aux trames pour identifier le VLAN auquel elles appartiennent. Cet étiquetage permet à de nombreux VLAN d'être transférés sur un backbone commun ou sur une agrégation. L'agrégation de VLAN est standardisée à l'aide du protocole d'agrégation IEEE 802.1Q aujourd'hui largement utilisé. Le protocole ISL (Inter-Switch Link) de Cisco est un protocole d'agrégation propriétaire qui peut être mis en œuvre dans la plupart des réseaux Cisco.

L'agrégation de VLAN utilise des trames étiquetées pour permettre le transport de plusieurs VLAN sur un large réseau commuté par le biais de backbones partagés. La configuration et la mise à jour manuelles du protocole VTP (VLAN Trunking Protocol) sur de nombreux commutateurs est un vrai défi. VTP présente un avantage: une fois qu'un réseau a été configuré avec VTP, la plupart des tâches de configuration VLAN sont automatiques.

Ce module explique la mise en œuvre de VTP pour les VLAN dans un environnement LAN commuté.

La technologie VLAN offre de nombreux avantages aux administrateurs réseau. Les VLAN permettent notamment de contrôler les broadcasts de couche 3 ; ils améliorent la sécurité du réseau et facilitent le regroupement logique des utilisateurs du réseau. Toutefois, les VLAN ont une limite importante. Ils fonctionnent au niveau de la couche 2, ce qui signifie que les unités d'un VLAN ne peuvent pas communiquer avec les utilisateurs d'un autre VLAN sans utiliser des routeurs et des adresses de couche réseau.

À la fin de ce module, les étudiants doivent être en mesure de réaliser les tâches suivantes:

- Expliquer les origines et les fonctions de l'agrégation de VLAN
- Décrire comment l'agrégation permet la mise en œuvre de VLAN dans un grand réseau
- Définir le protocole 802.1Q de l'IEEE
- Définir le protocole ISL de Cisco
- Configurer et vérifier une agrégation de VLAN
- Définir VTP
- Expliquer pourquoi VTP a été développé
- Décrire le contenu des messages VTP
- Énumérer et définir les trois modes VTP
- Configurer et vérifier VTP sur un commutateur basé sur l'IOS
- Expliquer pourquoi le routage est nécessaire pour la communication entre les VLAN
- Expliquer la différence entre interfaces physiques et logiques
- Définir des sous-interfaces
- Configurer le routage entre les VLAN à l'aide de sous-interfaces sur un port de routeur

À la fin de ce module, l'étudiant sera capable d'effectuer des travaux liés aux thèmes suivants :	
9.1	Agrégation (Trunking)
9.2	VTP
9.3	Vue d'ensemble du routage entre VLAN

Ce module porte sur les objectifs suivants de l'examen de certification CCNA 640-801 :

Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Configuration d'un commutateur avec des VLAN et une communication entre commutateurs		

Ce module porte sur les objectifs suivants de l'examen ICND 640-811 :

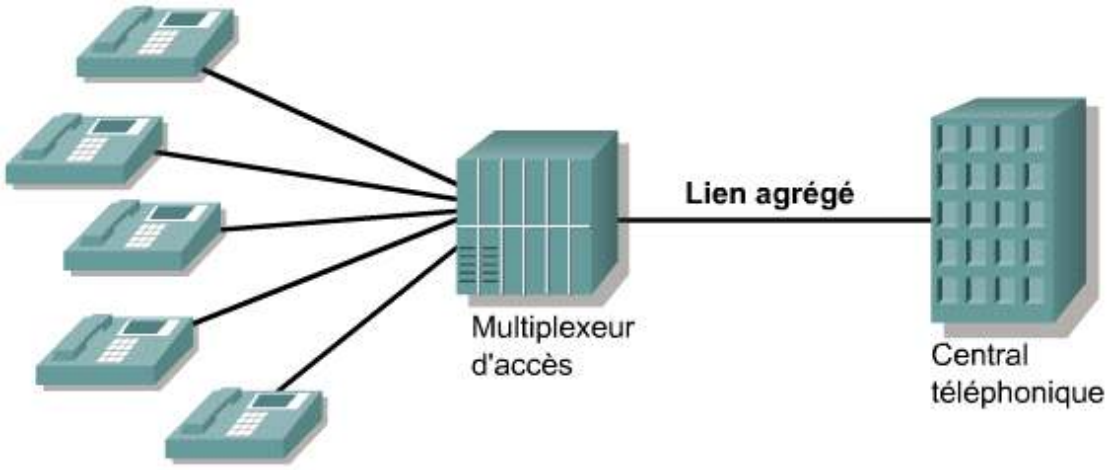
Planification et conception	Mise en œuvre et fonctionnement	Dépannage	Technologie
	• Configuration d'un commutateur avec des VLAN et une communication entre commutateurs		

9.1 Agrégation (Trunking)

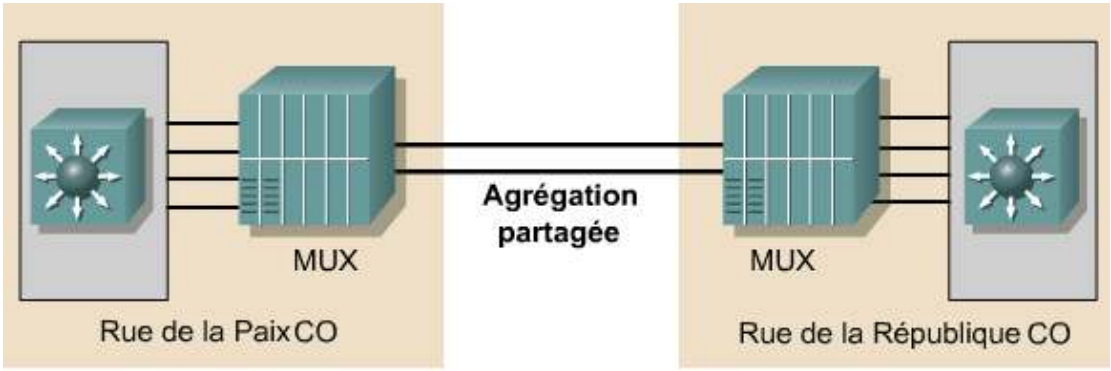
9.1.1 Historique de l'agrégation

L'apparition de l'agrégation (trunking) remonte aux origines des technologies radio et de téléphonie. Dans les technologies radio, une agrégation est une ligne de communication simple qui transporte plusieurs canaux de signaux radio.

Dans l'industrie de la téléphonie, le concept d'agrégation est associé au canal ou à la voie de communication téléphonique entre deux points. L'un de ces deux points est généralement le central téléphonique.



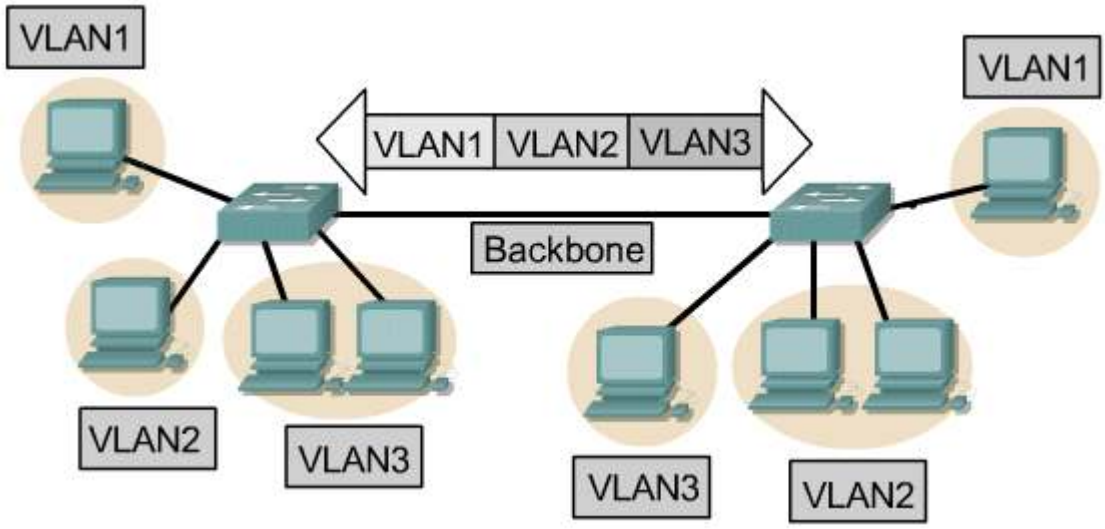
1Des agrégations partagées peuvent également être créées pour la redondance entre centraux téléphoniques. 2



L'industrie de la téléphonie utilisait des multiplexeurs pour transporter plusieurs signaux vocaux sur une seule agrégation entre des centraux téléphoniques (CO).

Le concept utilisé par les industries de la radio et de la téléphonie a ensuite été adopté pour les communications de données. Dans un réseau de communication, une liaison de backbone entre un répartiteur principal et un répartiteur intermédiaire en est un exemple. Un backbone est composé d'un certain nombre d'agrégations.

Actuellement, le même principe d'agrégation est appliqué aux technologies de commutation de réseaux. Une agrégation est une connexion physique et logique entre deux commutateurs par lesquels le trafic réseau est acheminé. 3

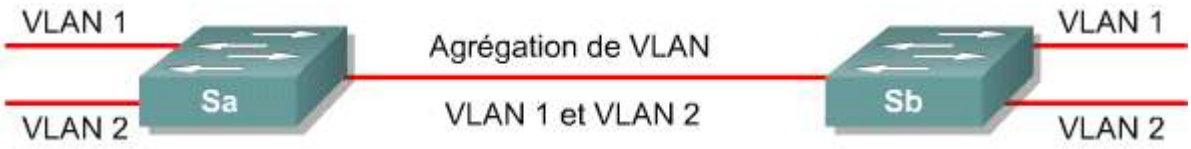


9.1 Agrégation (Trunking)

9.1.2 Concepts d'agrégation

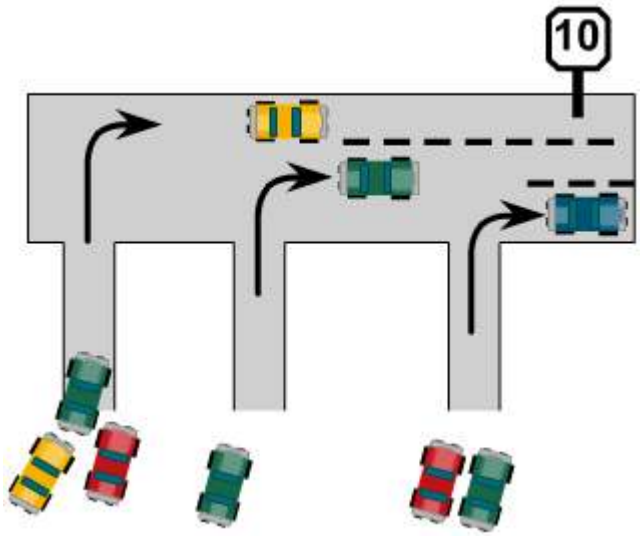
Comme nous l'avons indiqué précédemment, une agrégation est une connexion physique et logique entre deux commutateurs par lesquels le trafic réseau est acheminé. Il s'agit d'un canal de transmission simple entre deux points. Ces points sont généralement des centres de commutation.

Dans le contexte d'un environnement de commutation VLAN, une agrégation de VLAN est une liaison point-à-point physique ou logique qui prend en charge plusieurs VLAN. L'objectif d'une agrégation de VLAN est d'économiser des ports lors de la création d'une liaison entre deux unités contenant des VLAN. La figure 1 illustre deux VLAN répartis sur deux commutateurs (Sa et Sb). Chaque commutateur utilise deux liaisons physiques, de sorte que chaque port transporte le trafic d'un VLAN unique. Il s'agit de la méthode la plus simple de mise en œuvre d'une communication VLAN entre commutateurs, mais elle n'offre pas une évolutivité suffisante.



L'ajout d'un troisième VLAN nécessiterait l'utilisation de deux ports additionnels, un pour chaque commutateur connecté. Cette configuration est également inefficace en termes de partage de charges. De plus, le trafic sur certains VLAN peut ne pas justifier une liaison dédiée. Le concept d'agrégation de VLAN consiste à regrouper plusieurs liaisons virtuelles sur une liaison physique unique en permettant la transmission du trafic de plusieurs VLAN sur un câble unique entre les commutateurs. 2

Une agrégation est semblable à un réseau autoroutier. 3 Les routes avec différents points de départ et d'arrivée partagent une autoroute principale pendant quelques kilomètres, puis se divisent pour atteindre leurs destinations. Cette méthode est plus économique que la création d'une route complète du début à la fin pour chaque destination existante ou nouvelle.



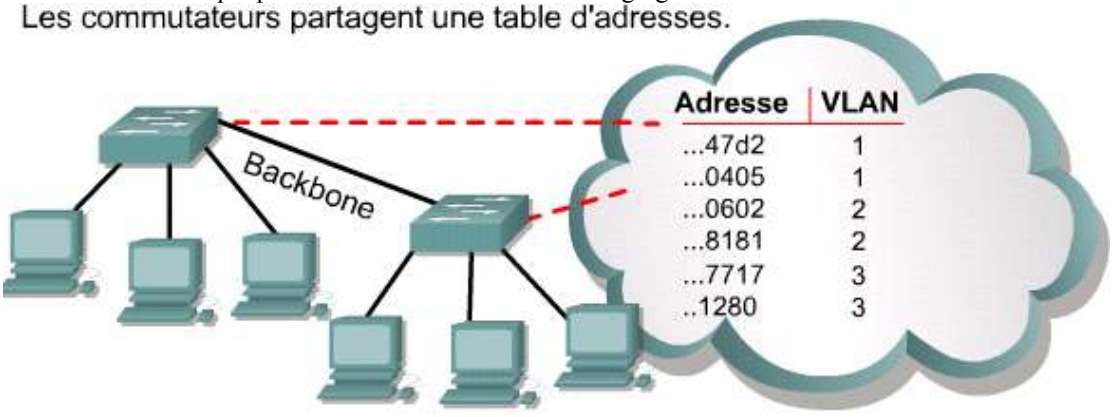
9.1 Agrégation (Trunking)

9.1.3 Fonctionnement d'une agrégation de VLAN

Les tables de commutation aux deux extrémités de l'agrégation peuvent être utilisées pour prendre des décisions de transmission sur la base des adresses MAC de destination des trames. Lorsque le nombre de VLAN circulant sur l'agrégation augmente, les décisions de transmission deviennent plus difficiles à gérer. Le processus de prise de décision est ralenti car le traitement de tables de commutation volumineuses prend plus de temps.

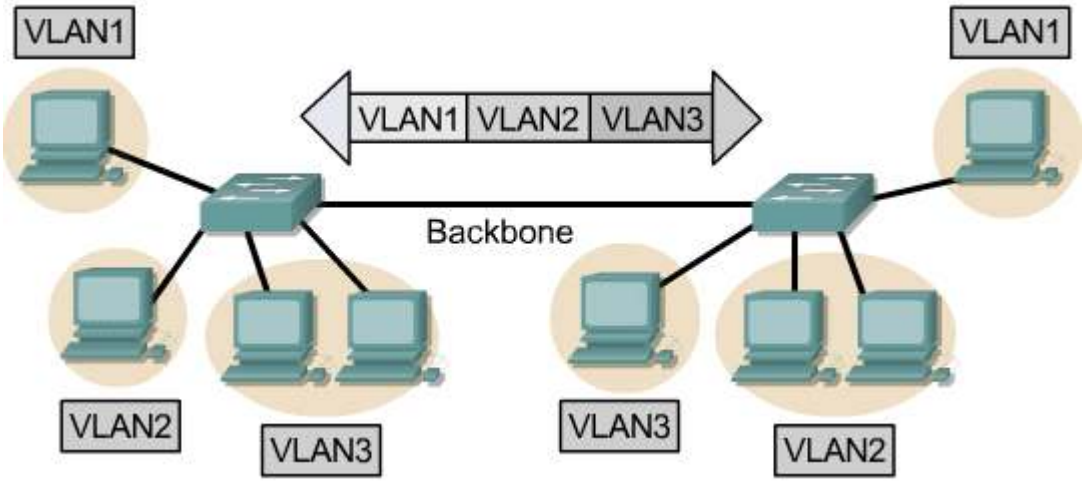
Des protocoles d'agrégation ont été développés pour gérer efficacement le transfert de trames de différents VLAN sur une liaison physique unique. Les protocoles d'agrégation définissent un consensus pour la distribution de trames aux ports associés aux deux extrémités de l'agrégation.

Actuellement, il existe deux types de mécanismes d'agrégation: le filtrage des trames et l'étiquetage des trames. L'étiquetage des trames a été adopté par l'IEEE comme mécanisme d'agrégation standard. [1] [2]



Similaire à la méthode utilisée par les routeurs

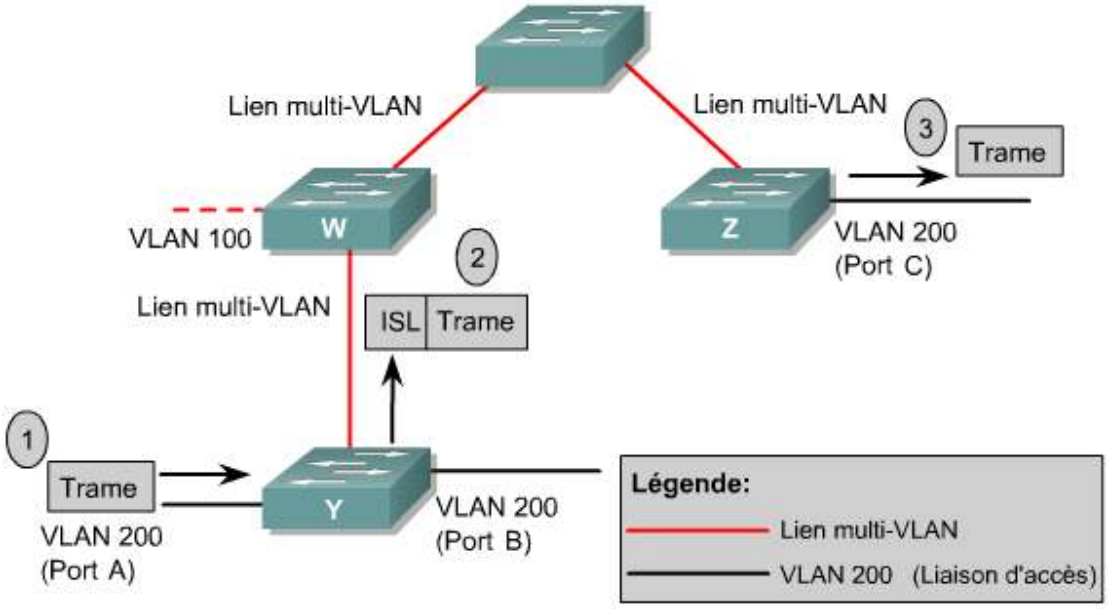
Une table de filtrage est développée pour chaque commutateur. Les commutateurs partagent les informations de table d'adresses. Les entrées de la table sont comparées avec les trames. Le commutateur entreprend l'action appropriée.



Les protocoles d'agrégation qui utilisent un mécanisme d'étiquetage des trames affectent un identifiant aux trames pour faciliter leur gestion et permettre un acheminement plus rapide des trames.

La liaison physique unique entre les deux commutateurs est capable de transporter le trafic pour n'importe quel VLAN. Pour cela, chaque trame envoyée sur la liaison est étiquetée afin d'identifier le VLAN auquel elle appartient. Il existe plusieurs systèmes d'étiquetage. Les systèmes d'étiquetage les plus courants pour les segments Ethernet sont répertoriés ci-dessous:

- **ISL** (Inter-Switch Link) – Protocole propriétaire de Cisco 3



- **802.1Q** – Norme IEEE plus particulièrement traitée dans cette section

Activité de média interactive

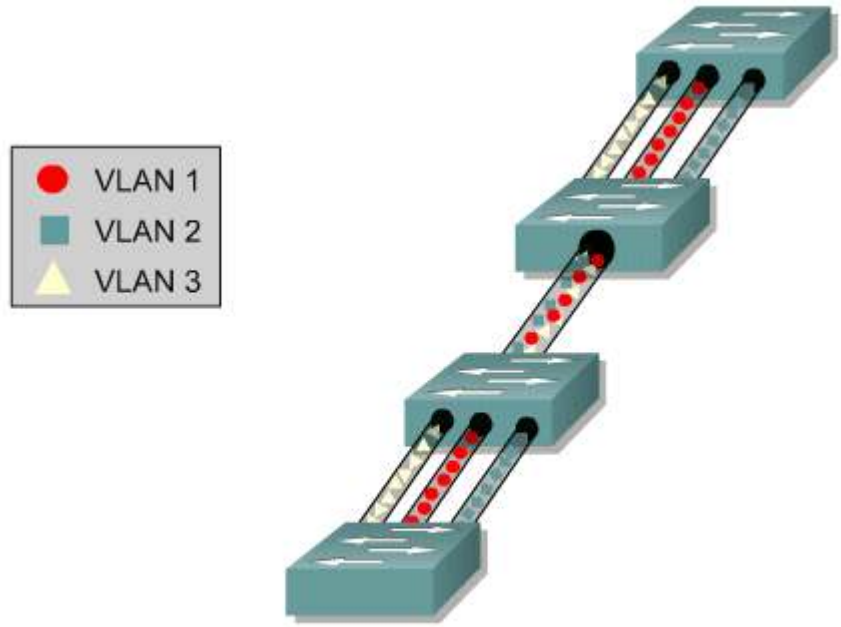
Compléter les zones vides : Fonctionnement de l'agrégation

À la fin de cette activité, l'étudiant sera en mesure de comprendre que l'utilisation de liaisons agrégées peut diminuer le nombre d'interfaces physiques nécessaires sur un commutateur.

9.1 Agrégation (Trunking)

9.1.4 VLAN et agrégation

Des protocoles ou des règles spécifiques sont utilisés pour mettre en œuvre une agrégation. L'agrégation fournit une méthode efficace de distribution des ID de VLAN aux autres commutateurs. 1



L'agrégation permet une communication efficace entre les commutateurs d'un réseau.

L'utilisation de l'étiquetage de trames comme mécanisme d'agrégation standard, par opposition au filtrage de trames, fournit une solution plus évolutive au déploiement VLAN. Selon la norme IEEE 802.1Q, l'étiquetage de trames est la meilleure façon de mettre en œuvre des LAN virtuels. 2

Méthode d'identification	Encapsulation	Étiquetage (insertion dans la	Médias
802.1Q	Non	Oui	Ethernet
ISL	Oui	Non	Ethernet
802.10	Non	Non	FDDI
LANE	Non	Non	ATM

La méthode d'étiquetage des trames VLAN a été développée spécialement pour les communications commutées. Cette méthode place un identificateur unique dans l'en-tête de chaque trame au moment où celle-ci est acheminée dans le backbone du réseau. L'identificateur est interprété et examiné par chaque commutateur avant tout broadcast ou transmission à d'autres commutateurs, routeurs ou équipements de station d'extrémité. Lorsque la trame quitte le backbone du réseau, le commutateur retire l'identificateur avant de transmettre la trame à la station d'extrémité cible. L'étiquetage des trames est effectué au niveau de la couche 2; il nécessite des temps de traitement ou d'administration peu importants.

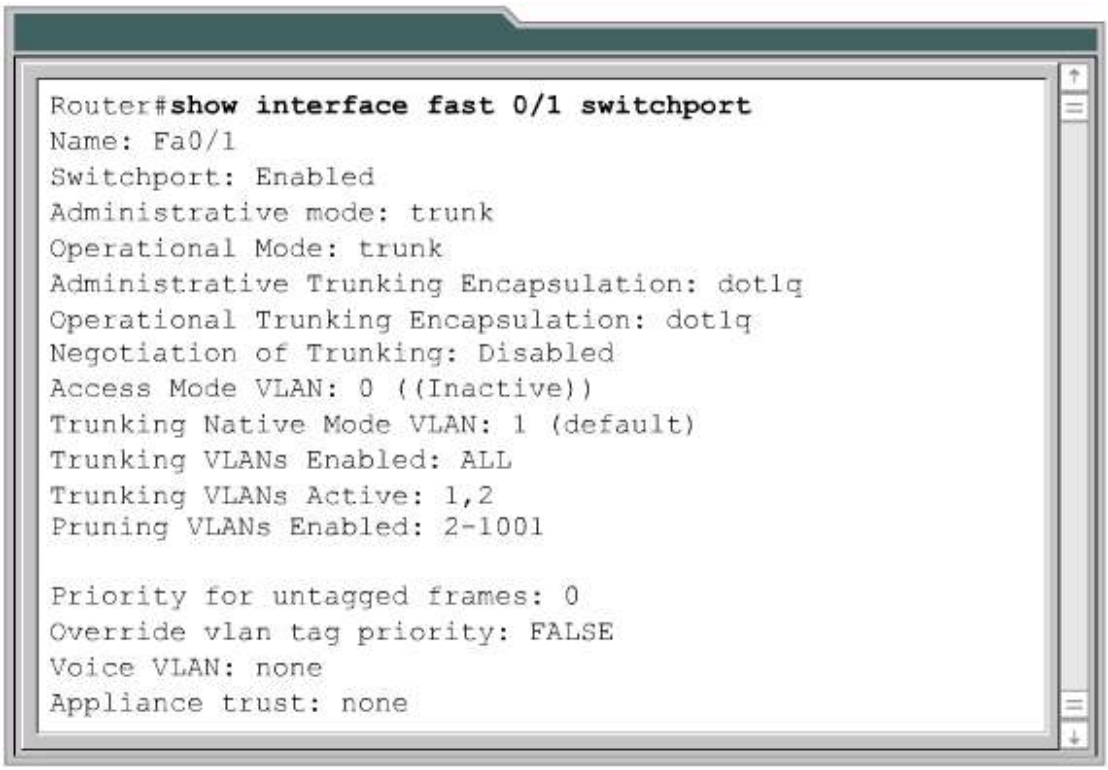
Il est important de comprendre qu'un lien multi-VLAN n'appartient à aucun VLAN spécifique. Un lien multi-VLAN doit servir de canal pour les VLAN entre les commutateurs et les routeurs.

ISL est un protocole qui met à jour les informations VLAN au fur et à mesure du transfert du trafic entre les commutateurs. Avec ISL, une trame Ethernet est encapsulée avec un en-tête contenant un ID de VLAN.

9.1 Agrégation (Trunking)

9.1.5 Mise en œuvre de l'agrégation de VLAN

Pour créer ou configurer une agrégation de VLAN sur un commutateur à base de commandes Cisco IOS, configurez d'abord le port en mode d'agrégation de VLAN puis spécifiez l'encapsulation d'agrégation à l'aide des commandes suivantes: 1



Vérifiez que le mécanisme d'agrégation a été configuré et contrôlez les paramètres en utilisant les commandes **show interfaces***Fa0/[num_port]* ou **show interfaces***trunk* en mode privilégié sur le commutateur.

Activité de TP

Exercice : Agrégation ISL

Dans ce TP, les étudiants vont créer une liaison multi-VLAN ISL entre les deux commutateurs pour permettre la communication entre des LAN virtuels associés.

Activité de TP

Exercice : Agrégation 802.1Q

Dans ce TP, les étudiants vont créer une liaison multi-VLAN 802.1Q entre les deux commutateurs pour permettre la communication entre des LAN virtuels associés.

Activité de TP

Activité en ligne : Agrégation ISL

Au cours de ce TP, l'étudiant va créer des VLAN sur deux commutateurs distincts, nommer les commutateurs et leur affecter des ports membres.

Activité de TP

Activité en ligne : Agrégation 802.1Q

Au cours de ce TP, l'étudiant va créer des VLAN sur deux commutateurs distincts, nommer les commutateurs et leur affecter des ports membres.

9.2 VTP (Virtual Trunking Protocol)

9.2.1 Historique du protocole VTP

Le protocole VTP (VLAN Trunking Protocol) a été créé par Cisco pour résoudre des problèmes opérationnels dans des réseaux commutés contenant des VLAN. C'est un protocole propriétaire Cisco.

Prenez l'exemple d'un domaine contenant des commutateurs interconnectés qui prennent en charge plusieurs VLAN. Pour mettre à jour la connectivité au sein de VLAN, il est nécessaire de configurer manuellement chaque VLAN sur chaque commutateur. Au fur et à mesure de la croissance de l'entreprise et de l'ajout de commutateurs au réseau, il convient de configurer manuellement chaque nouveau commutateur sur la base des informations VLAN. Une seule affectation de VLAN incorrecte peut engendrer deux types de problème:

- Connexions croisées entre VLAN en raison de l'incohérence des configurations VLAN
- Mauvaise configuration de VLAN sur des environnements à médias mixtes comme Ethernet et FDDI (Fiber Distributed Data Interface)

Avec VTP, la configuration VLAN est systématiquement mise à jour sur un domaine administratif commun. En outre, VTP facilite la gestion et la surveillance des réseaux VLAN. 1

9.2 VTP (Virtual Trunking Protocol)

9.2.2 Concepts VTP

Le rôle de VTP est de maintenir la cohérence de la configuration VLAN sur un domaine d'administration réseau commun. VTP est un protocole de messagerie qui utilise les trames d'agrégation de couche 2 pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique. De plus, VTP autorise les changements centralisés qui sont communiqués à tous les autres commutateurs du réseau.

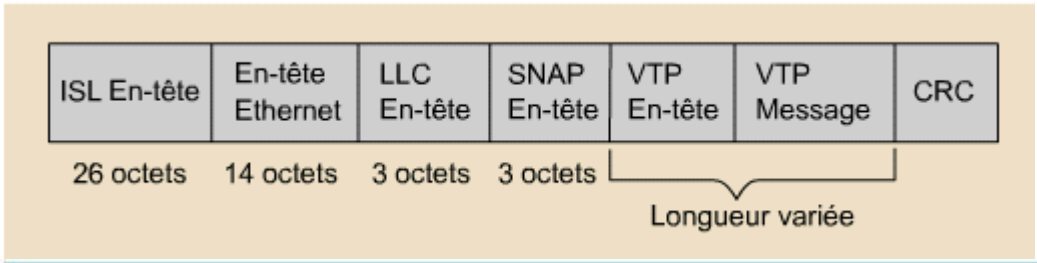
Les messages VTP sont encapsulés dans des trames de protocole Cisco ISL (Inter-Switch Link) ou IEEE 802.1Q, puis transmis sur des liens multi-VLAN aux autres unités. Dans les trames IEEE 802.1Q, un champ sur 4 octets est ajouté pour étiqueter les trames. Les deux formats transportent l'ID du VLAN.

Alors que les ports de commutateur sont normalement affectés à un seul VLAN, les ports multi-VLAN transportent, par défaut, les trames de tous les VLAN. 1

9.2 VTP (Virtual Trunking Protocol)

9.2.3 Fonctionnement de VTP

Un domaine VTP est composé d'un ou de plusieurs équipements interconnectés qui partagent le même nom de domaine VTP. Un commutateur ne peut appartenir qu'à un seul domaine VTP.



Spécifications de trame ISL :
- L'en-tête ISL comporte 26 octets.
- Le CRC est recalculé aprs l'encapsulation.

Lorsqu'un message VTP est transmis aux autres commutateurs du réseau, il est encapsulé dans une trame de protocole d'agrégation comme ISL ou IEEE 802.1Q. La figure 1 illustre l'encapsulation générale pour VTP à l'intérieur d'une trame ISL. L'en-tête VTP varie en fonction du type de message VTP, mais quatre éléments sont généralement inclus dans tous les messages VTP:

- Version du protocole VTP: version 1 ou 2
- Type de message VTP: indique l'un des quatre types
- Longueur du nom de domaine de gestion: indique la taille du nom qui suit
- Nom du domaine de gestion: nom configuré pour le domaine de gestion

Les commutateurs VTP exécutent l'un des trois modes suivants:

- Serveur
- Client
- Transparent

Les serveurs VTP peuvent créer, modifier et supprimer un VLAN et des paramètres de configuration VLAN pour l'ensemble du domaine. Les serveurs VTP enregistrent les informations de configuration VLAN dans la mémoire NVRAM du commutateur. Les serveurs VTP envoient des messages VTP par tous les ports multi-VLAN.

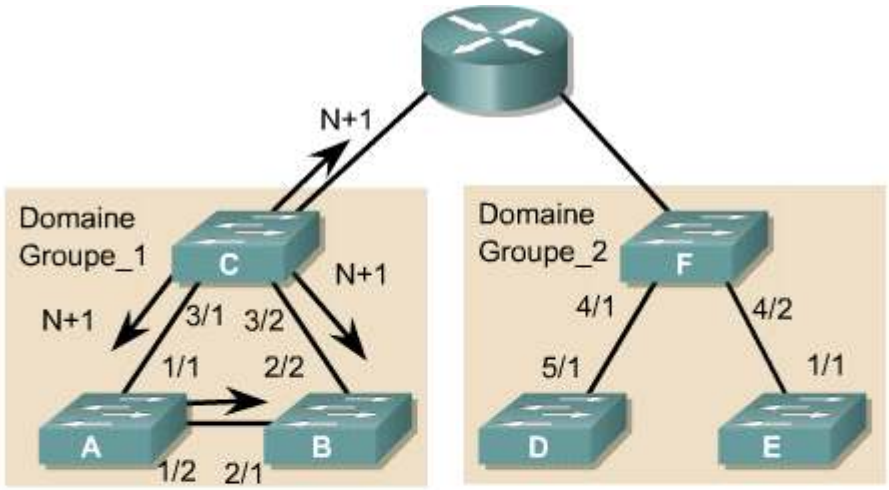
Les clients VTP ne peuvent pas créer, modifier ou supprimer des informations VLAN. Ce mode est utile pour les commutateurs qui manquent de mémoire pour stocker de grandes tables d'informations VLAN. Le seul rôle des clients VTP est de traiter les modifications VLAN et d'envoyer des messages VTP par tous les ports multi-VLAN.

Les commutateurs en mode transparent VTP transmettent des annonces VTP mais ignorent les informations contenues dans le message. Un commutateur transparent ne modifie pas sa base de données lors de la réception de mises à jour et il n'envoie pas de mises à jour indiquant une modification apportée à son état VLAN. Excepté pour la transmission d'annonces VTP, le protocole VTP est désactivé sur un commutateur transparent. 2

Caractéristique	Serveur	Client	Transparent
Fournir des messages VTP	Oui	Oui	Non
Être à l'écoute des messages VTP	Yes	Oui	Non
Créer des VLAN	Oui	Non	Oui*
Se souvenir des VLAN	Oui	Non	Oui*

*Significatif sur un plan local uniquement

Les VLAN détectés au sein des annonces servent de notification pour indiquer au commutateur qu'un trafic transportant les nouveaux ID de VLAN peut être attendu.



Groupe_1 Config rév. N+1	
1	default
2	first-vtp-vlan
1002	fddi-default
1003	token-ring-default
1004	fddinet-default
1003	trnet-default

Dans la figure 3, le commutateur C transmet une entrée de base de données VTP avec des ajouts ou des suppressions aux commutateurs A et B. La base de données de configuration dispose d'un numéro de révision qui est incrémenté de un. Un numéro de révision de configuration supérieur indique que les informations VLAN envoyées sont plus récentes que la copie stockée. Chaque fois qu'un commutateur reçoit une mise à jour avec un numéro de révision de configuration supérieur, il remplace les informations stockées par les nouvelles informations envoyées dans la mise à jour VTP. Le commutateur F ne traite pas la mise à jour, car il appartient à un autre domaine. Avec ce processus de remplacement, lorsque le VLAN n'existe pas dans la nouvelle base de données, il est supprimé du commutateur. En outre, VTP met à jour sa propre configuration dans la mémoire NVRAM. La commande **`erase startup-configuration`** efface les commandes de configuration en mémoire NVRAM, à l'exception du numéro de révision de la base de données VTP. Pour redéfinir le numéro de révision de configuration sur zéro, le commutateur doit être redémarré.

Par défaut, les domaines de gestion sont définis sur un mode non sécurisé, ce qui signifie que les commutateurs interagissent sans utiliser de mot de passe. L'ajout d'un mot de passe fait passer automatiquement le domaine de gestion en mode sécurisé. Le même mot de passe doit être configuré sur chaque commutateur du domaine de gestion pour utiliser le mode sécurisé.

9.2 VTP (Virtual Trunking Protocol)

9.2.4 Mise en œuvre de VTP

Grâce à VTP, chaque commutateur annonce sur les ports multi-VLAN, son domaine de gestion, son numéro de révision de configuration, les VLAN qu'il connaît et les paramètres correspondants. Ces trames d'annonce sont envoyées à une adresse multicast, de sorte que toutes les unités voisines puissent recevoir les trames. Toutefois, les trames ne sont pas transmises au moyen des procédures de pontage habituelles. Toutes les unités du même domaine de gestion acquièrent des informations sur les nouveaux VLAN configurés dans l'unité émettrice. Un nouveau VLAN doit être créé et configuré sur une unité uniquement dans le domaine de gestion. Toutes les autres unités du même domaine de gestion apprennent automatiquement les informations.

Les annonces sur les VLAN par défaut sont basées sur les types de média. Les ports utilisateur ne doivent pas être configurés en tant qu'agrégations VTP.

Chaque annonce commence par le numéro de révision de configuration 0. Lorsque des modifications sont apportées, le numéro de révision de la configuration augmente de un (n + 1). Le numéro de révision continue d'augmenter jusqu'au numéro 2 147 483 648. Une fois ce numéro atteint, le compteur est remis à zéro.

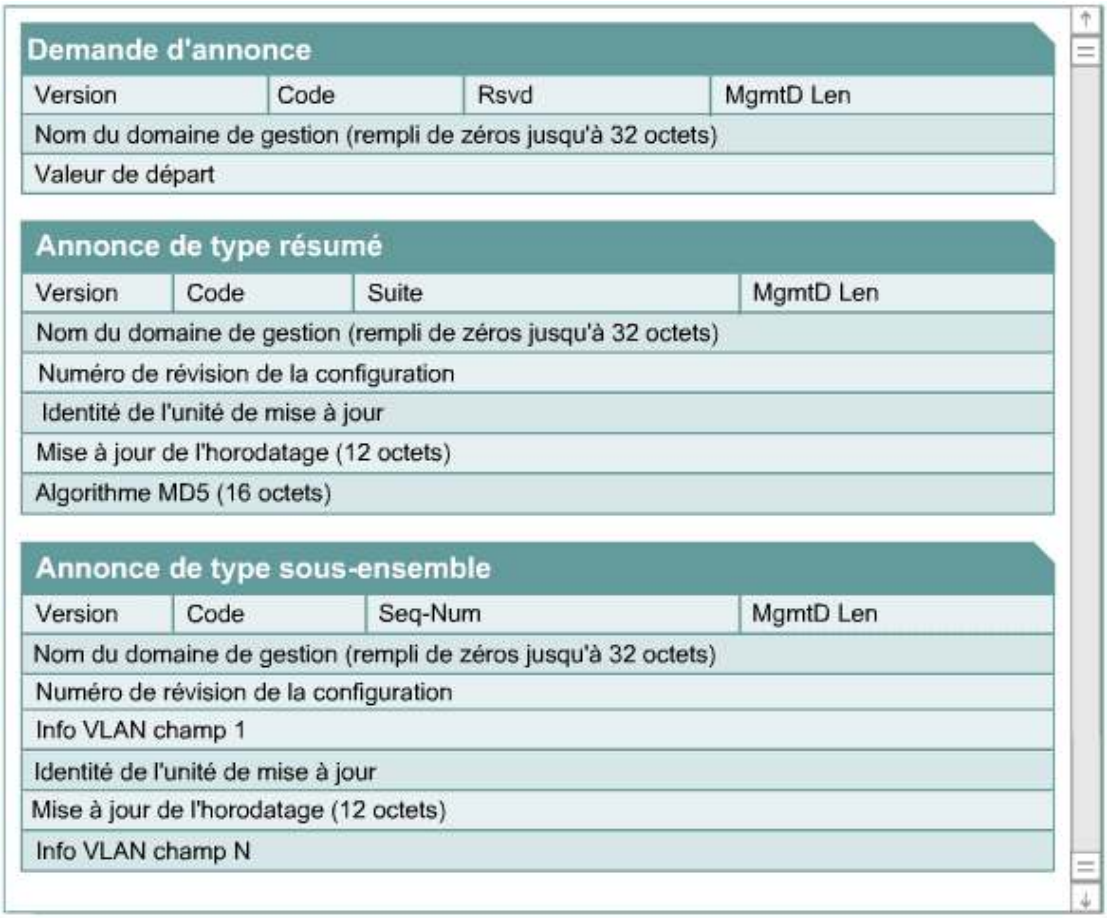
Il existe deux types d'annonce VTP:

- les demandes émanant de clients qui réclament des informations au démarrage;
- les réponses des serveurs.

Il existe trois types de message VTP:

- les demandes d'annonce;
- les annonces de type résumé;
- les annonces de type sous-ensemble.

Avec les demandes d'annonce, les clients demandent des informations VLAN et le serveur répond avec des annonces de type résumé ou sous-ensemble. 1



Demande d'annonce

Version	Code	Rsvd	MgmtD Len
Nom du domaine de gestion (rempli de zéros jusqu'à 32 octets)			
Valeur de départ			

Annonce de type résumé

Version	Code	Suite	MgmtD Len
Nom du domaine de gestion (rempli de zéros jusqu'à 32 octets)			
Numéro de révision de la configuration			
Identité de l'unité de mise à jour			
Mise à jour de l'horodatage (12 octets)			
Algorithme MD5 (16 octets)			

Annonce de type sous-ensemble

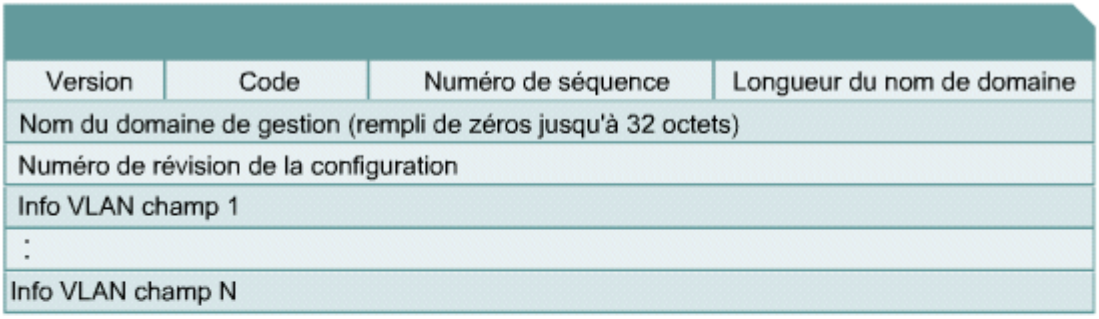
Version	Code	Seq-Num	MgmtD Len
Nom du domaine de gestion (rempli de zéros jusqu'à 32 octets)			
Numéro de révision de la configuration			
Info VLAN champ 1			
Identité de l'unité de mise à jour			
Mise à jour de l'horodatage (12 octets)			
Info VLAN champ N			

Par défaut, les commutateurs serveur et client Catalyst émettent des annonces de type résumé toutes les cinq minutes. Les serveurs indiquent aux commutateurs voisins ce qu'ils pensent être le numéro de révision VTP actuel. Si les noms de domaine correspondent, le serveur ou client récepteur compare le numéro de révision de la configuration. Si le numéro de révision dans l'annonce est supérieur à celui qui figure actuellement dans le commutateur récepteur, ce dernier émet une demande d'annonce pour les nouvelles informations VLAN. 2

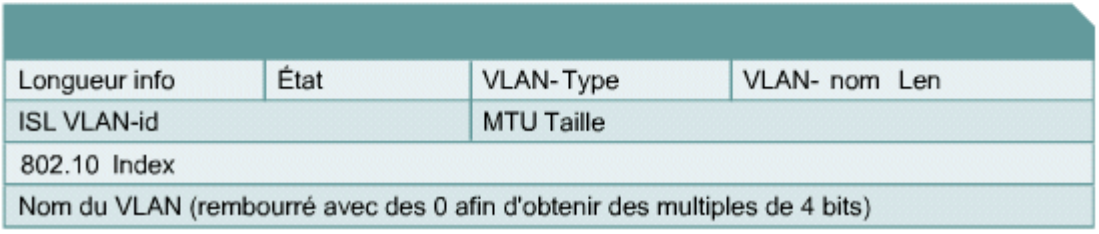
Version	Code	Nombre de messages d'annonce de sous-réseaux	Longueur du nom de domaine
Nom du domaine de gestion (rempli de zéros jusqu'à 32 octets)			
Numéro de révision de la configuration			
Identité de l'unité de mise à jour			
Mise à jour de l'horodatage (12 octets)			
Algorithme MD5 (16 octets)			

Les annonces de type sous-ensemble contiennent des informations détaillées sur les VLAN, telles que le type de version VTP, le nom du domaine et les champs associés, ainsi que le numéro de révision de la configuration. Les événements suivants peuvent créer ces annonces:

- Création ou suppression d'un VLAN
- Arrêt ou activation d'un VLAN
- Modification du nom d'un VLAN
- Modification de la MTU d'un VLAN 3



Le champ Info VLAN contient des informations pour chaque VLAN et est formaté comme suit :



Les annonces peuvent contenir toutes ou une partie des informations suivantes :

- Nom du domaine de gestion. Les annonces contenant des noms différents sont ignorées.
- Numéro de révision de la configuration. Un numéro supérieur reflète une configuration plus récente.
- Algorithme MD5. MD5 est la clé envoyée avec VTP lorsqu'un mot de passe a été affecté. Si la clé ne correspond pas, la mise à jour est ignorée.
- Identité de l'unité de mise à jour. Il s'agit de l'identité du commutateur qui envoie l'annonce de type résumé VTP.

9.2 VTP (Virtual Trunking Protocol)

9.2.5 Configuration de VTP

Les tâches de base suivantes doivent être effectuées avant de configurer le protocole VTP et les VLAN sur le réseau. 1

1. Déterminez le numéro de la version de VTP qui sera utilisée.
2. Indiquez si ce commutateur sera un membre d'un domaine de gestion existant ou si un nouveau domaine doit être créé. Si un domaine de gestion existe, déterminez son nom et son mot de passe.
3. Choisissez un mode VTP pour le commutateur.

Deux versions différentes de VTP sont disponibles: la version 1 et la version 2. Les deux versions ne peuvent pas fonctionner ensemble. Si un commutateur est configuré dans un domaine pour VTP version 2, tous les commutateurs du même domaine doivent l'être aussi. VTP version 1 est la valeur par défaut. La version 2 de VTP peut être mise en œuvre si certaines des fonctions qu'elle offre ne sont pas proposées dans la version 1. La fonction la plus couramment utilisée est la prise en charge VLAN Token Ring.

Pour configurer la version de VTP sur un commutateur à base de commandes Cisco IOS, passez d'abord en mode base de données VLAN. 2

Utilisez la commande suivante pour changer le numéro de version de VTP:

```
Switch#vlan database
Switch(vlan)#vtp v2-mode
```

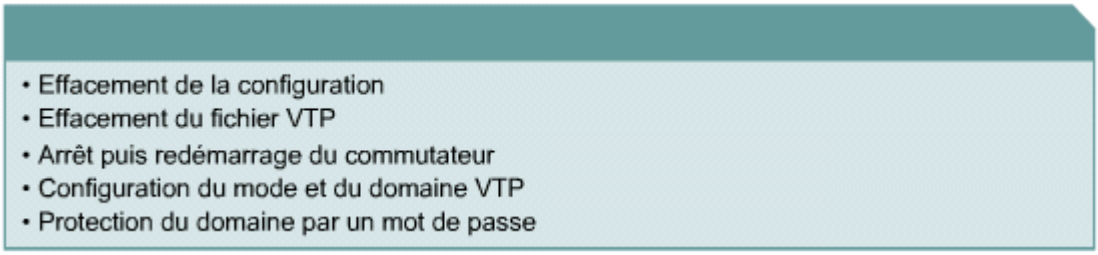
Si le commutateur installé est le premier commutateur du réseau, créez le domaine de gestion. Si le domaine de gestion a été sécurisé, configurez un mot de passe.

Pour créer un domaine de gestion, utilisez la commande suivante: 3


```
Switch(vlan)#vtp domain cisco
```

Le nom du domaine peut comporter entre 1 et 32 caractères. Le mot de passe peut comporter entre 8 et 64 caractères.

Pour ajouter un client VTP à un domaine VTP existant, vérifiez toujours que son numéro de révision de configuration VTP est inférieur à celui des autres commutateurs du domaine VTP. Utilisez la commande **show vtp status**. Les commutateurs d'un domaine VTP utilisent toujours la configuration VLAN du commutateur qui porte le numéro de révision de configuration VTP le plus élevé. Si un commutateur est ajouté et s'il porte un numéro de révision supérieur à celui du domaine VTP, il peut effacer toutes les informations VLAN du serveur et du domaine VTP. 4



Choisissez un des trois modes VTP disponibles pour le commutateur. S'il s'agit du premier commutateur du domaine de gestion et que d'autres commutateurs vont être ajoutés, définissez le mode sur serveur. Les autres commutateurs seront en mesure d'acquérir des informations VLAN de ce commutateur. Il doit y avoir au moins un serveur.

Des VLAN peuvent être créés, supprimés et renommés à volonté sans que le commutateur transmette les modifications aux autres commutateurs. Si un grand nombre de personnes configurent des unités au sein du réseau, il est possible que deux VLAN avec deux significations différentes mais le même identifiant soient créés.

Pour définir le mode approprié du commutateur à base de commandes Cisco IOS, utilisez la commande suivante: 5

```
Switch(vlan)#vtp {client | server | transparent}
```

La figure 6 présente les informations affichées par la commande **show vtp status**. Cette commande permet de vérifier les paramètres de configuration VTP sur un commutateur à base de commandes Cisco IOS.

```
MDF_Switch#show vtp status
VTP Version                          :2
Configuration Revision               :0
Maximum VLANs supported locally      :64
Number of existing VLANs             :7
VTP Operation Mode                   :Server
VTP Domain Name                      :cisco
VTP Pruning Mode                     :Disabled
VTP V2 Mode                          :Disabled
VTP Traps Generation                 :Disabled
MDS digest                           :0x30 0x50
Configuration last modified by 10.1.1.252 a local
updater ID 138.25.13.121 on interface found)
MDF_Switch#exit
```

La figure 7 affiche un exemple de commande **show vtp counters**. Cette commande est utilisée pour afficher des statistiques sur les annonces envoyées et reçues sur le commutateur.

```
MDF_Switch#show vtp counters
VTP statistics:
Summary advertisments received          :4
Subset advertisments received           :1
Request advertisments received          :2
Summary advertisments transmitted       :7
Subset advertisments transmitted        :4
Request advertisments transmitted       :1
Number of config revision errors        :0
Number of config digest errors          :0
Number of V1 summary errors             :0


VTP pruning statistics:

Trunk               Join Transmitted Join Received
----------------- ----------------- ------------
MDF_Switch#
```

Activité de TP

Activité en ligne : Configurations serveur et client VTP

Au cours de ce TP, l'étudiant va configurer le protocole VTP pour définir des commutateurs serveur et client.

Activité de TP

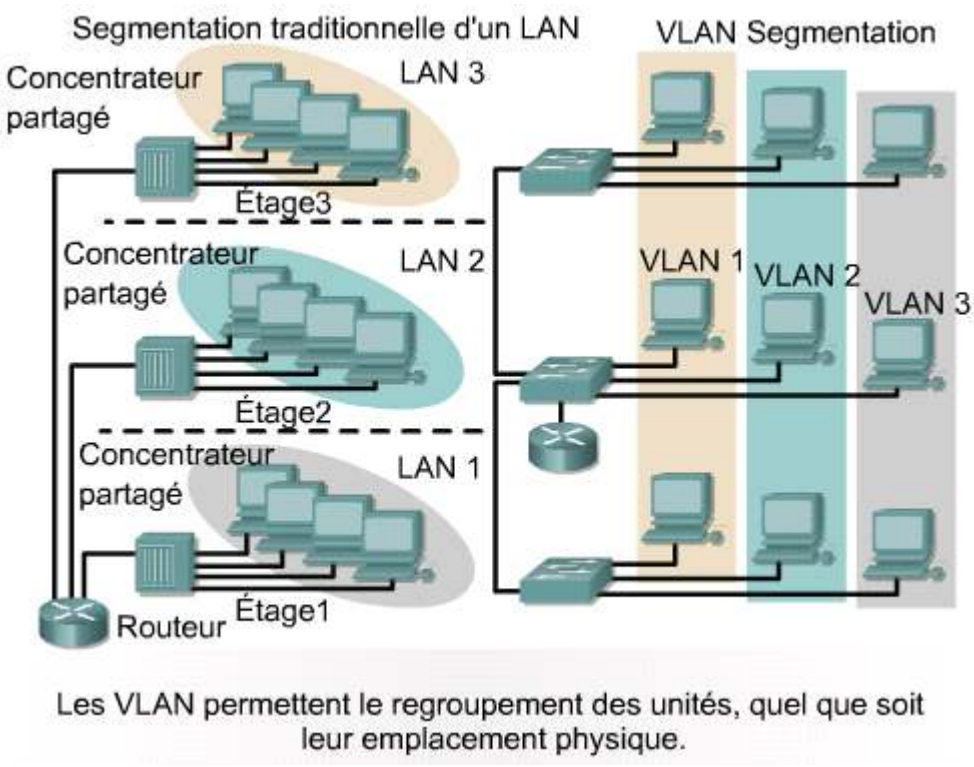
Activité en ligne : Configurations serveur et client VTP

Au cours de ce TP, l'étudiant va configurer le protocole VTP pour définir des commutateurs serveur et client.

9.3 Vue d'ensemble du routage entre VLAN

9.3.1 Notions de base sur les VLAN

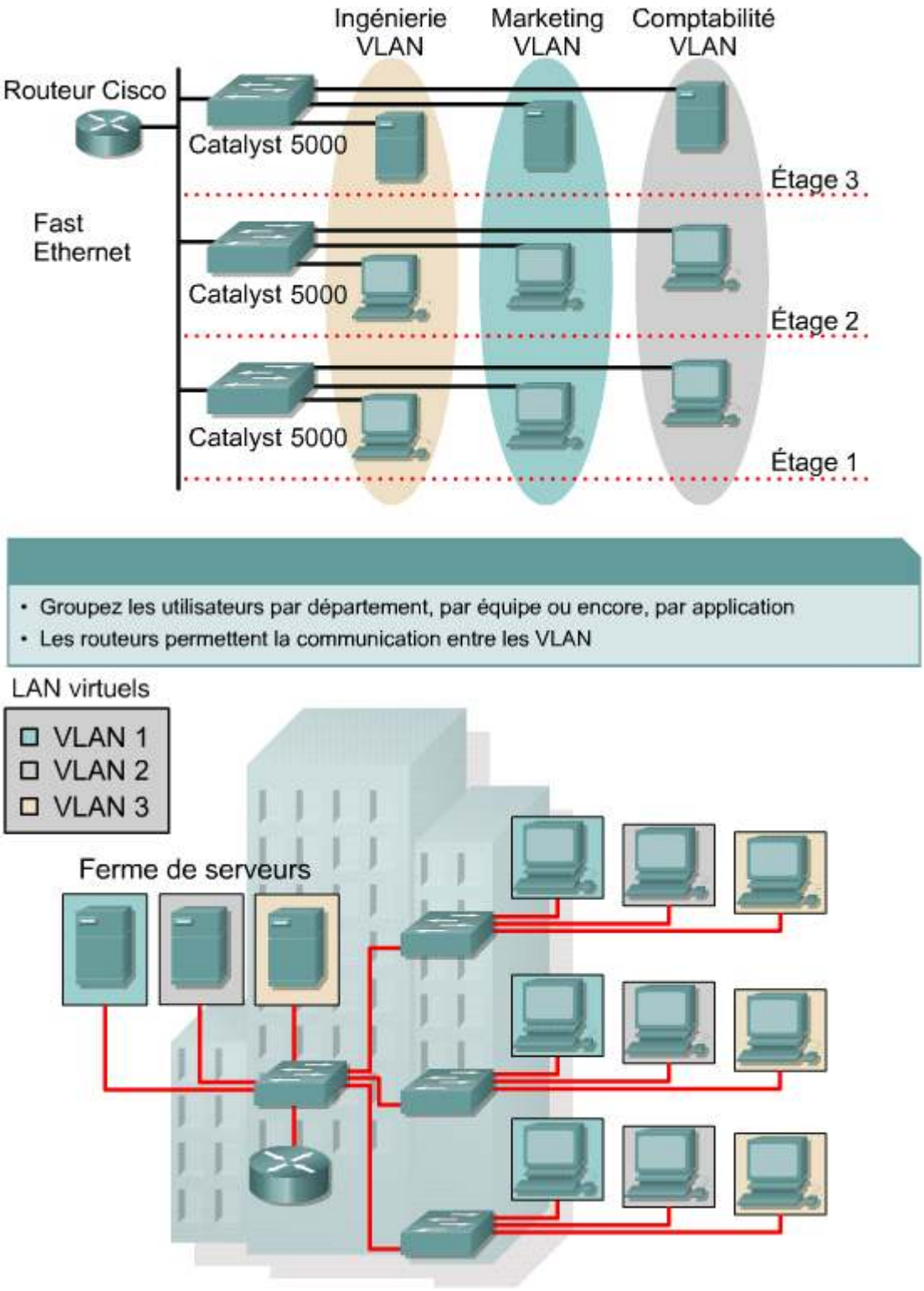
Un LAN virtuel est un ensemble logique d'unités ou d'utilisateurs qui peuvent être regroupés par fonction, par service ou par application, quel que soit leur emplacement physique. [1]



Les VLAN permettent le regroupement des unités, quel que soit leur emplacement physique.

La configuration d'un LAN virtuel est effectuée au niveau du commutateur par le biais d'un logiciel. La mise en œuvre de VLAN simultanés peut nécessiter l'utilisation d'un logiciel spécial fourni par le fabricant du commutateur. Le regroupement de ports et d'utilisateurs en communautés d'intérêt, appelées organisations VLAN, peut être réalisé par l'utilisation d'un seul commutateur ou de manière plus efficace sur des commutateurs connectés au sein de l'entreprise. En regroupant les ports et les utilisateurs de multiples commutateurs, les LAN virtuels peuvent s'étendre aux infrastructures d'un immeuble ou à des immeubles interconnectés. Les VLAN participent à l'utilisation efficace de la bande passante, car ils partagent le même domaine de broadcast ou réseau de couche 3. Les VLAN optimisent l'utilisation de la bande passante. Les VLAN se disputent la même bande passante, bien que les besoins en bande passante varient considérablement selon le groupe de travail ou le service. [2] [3] Voici quelques remarques sur la configuration d'un VLAN:

- Un commutateur crée un domaine de broadcast.
- Les LAN virtuels aident à gérer les domaines de broadcast.
- Les LAN virtuels peuvent être définis sur des groupes de ports, des utilisateurs ou des protocoles.
- Les commutateurs LAN et le logiciel d'administration réseau fournissent un mécanisme permettant de créer des VLAN.



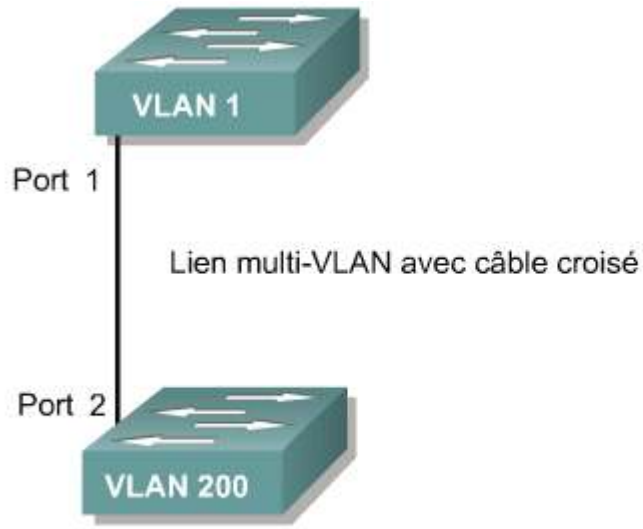
Les VLAN aident à contrôler la taille des domaines de broadcast et à localiser le trafic. Les VLAN sont associés à des réseaux individuels. Ainsi, les unités réseau dans des VLAN différents ne peuvent pas communiquer directement sans l'intervention d'une unité de routage de couche 3.

Lorsqu'un nœud d'un VLAN doit communiquer avec un nœud d'un autre VLAN, un routeur est nécessaire pour acheminer le trafic entre les VLAN. Sans unité de routage, le trafic entre VLAN est impossible.

9.3 Vue d'ensemble du routage entre VLAN

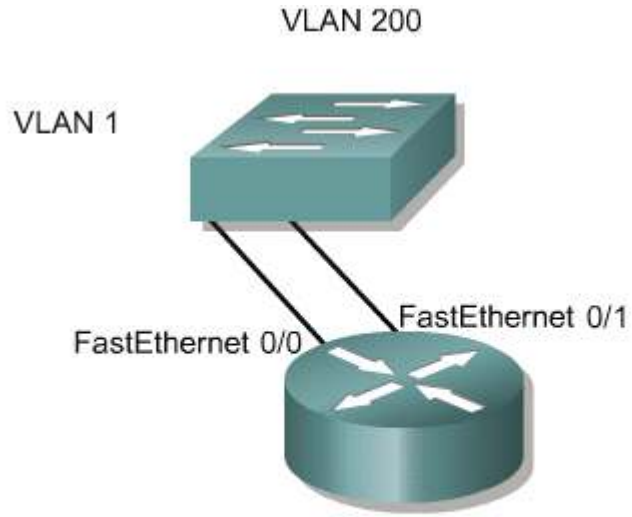
9.3.2 Introduction au routage entre VLAN

Lorsqu'un hôte d'un domaine de broadcast souhaite communiquer avec un hôte d'un autre domaine de broadcast, un routeur doit être utilisé.



Les VLAN 1 et 200 ne peuvent pas communiquer sans l'aide d'un routeur.

Le port 1 d'un commutateur fait partie du VLAN 1 et le port 2, du VLAN 200. 1 Si tous les ports de commutateur faisaient partie du VLAN 1, les hôtes connectés à ces ports pourraient communiquer. Dans ce cas, néanmoins, les ports appartiennent à des VLAN différents, le VLAN 1 et le VLAN 200. Un routeur doit être utilisé pour que les hôtes des différents VLAN communiquent. 2



Pour acheminer le trafic entre le VLAN 1 et le VLAN 200 dans un environnement sans agrégation de VLAN, un routeur doit être connecté à un port du VLAN1 et à un port du VLAN 200.

Le principal avantage du routage est sa faculté à faciliter les échanges sur les réseaux, notamment sur les grands réseaux. Bien que l'Internet en soit l'exemple le plus flagrant, cela est vrai pour tout type de réseau, et notamment pour un grand backbone de campus. Étant donné que les routeurs empêchent la propagation des broadcasts et utilisent des algorithmes de transmission plus intelligents que les ponts et les commutateurs, ils permettent d'utiliser plus efficacement la bande passante. En même temps, ils permettent une sélection de chemin optimale et flexible. Par exemple, il est très facile de mettre en œuvre l'équilibrage de charge sur plusieurs chemins dans la plupart des réseaux lors du routage. D'un autre côté, l'équilibrage de charge de couche 2 peut être très difficile à concevoir, à mettre en œuvre et à mettre à jour.

Lorsqu'un VLAN s'étend sur plusieurs équipements, une agrégation est utilisée pour interconnecter les équipements. L'agrégation transporte le trafic de plusieurs VLAN. Par exemple, une agrégation peut connecter un commutateur à un autre

commutateur, au routeur entre les VLAN ou à un serveur avec une carte NIC spéciale utilisée pour prendre en charge les agrégations.

N'oubliez pas que quand un hôte d'un VLAN veut communiquer avec un hôte d'un autre VLAN, un routeur est nécessaire.
3

Commutateurs, routeurs, serveurs, gestion		
	Établissement de l'appartenance	Commutateurs - Détermination de
	Communication sur la matrice	Agrégation - Échange VLAN commun
	Communications entre VLAN	Routage multiprotocole Échange entre VLAN
	Communication sur les serveurs	Serveurs-Multi - Communication entre VLAN
	Administration centralisée	Gestion - Sécurité, contrôle, administration

Activité de média interactive

Glisser-Positionner : Routage entre les VLAN

À la fin de cette activité, l'étudiant connaîtra le chemin suivi par les paquets dans un réseau avec routage entre LAN virtuels. L'étudiant saura prévoir le chemin qu'un paquet va prendre en fonction des hôtes d'origine et de destination.

9.3 Vue d'ensemble du routage entre VLAN

9.3.3 Communication inter-VLAN : Problématique et solutions

Lorsque des VLAN sont interconnectés, plusieurs problèmes techniques peuvent survenir. Les deux problèmes les plus courants dans un environnement à plusieurs VLAN sont les suivants:

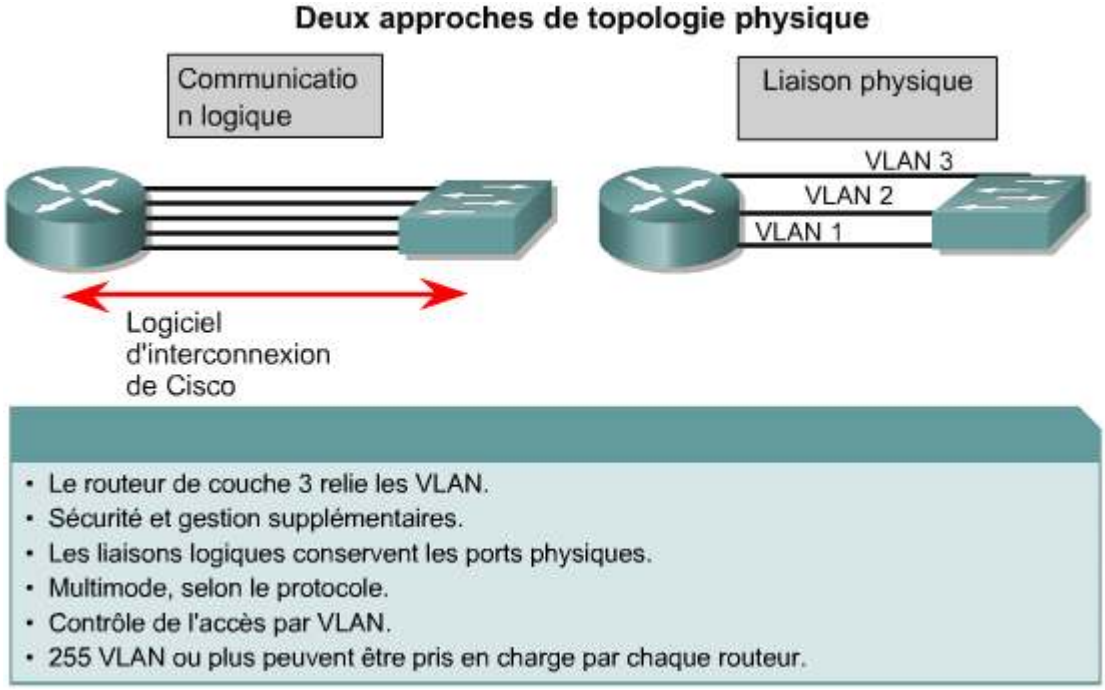
- La nécessité pour les unités d'utilisateur final d'atteindre des hôtes non locaux
- La nécessité pour les hôtes de VLAN différents de communiquer entre eux

Lorsqu'un routeur a besoin d'établir une connexion avec un hôte distant, elle vérifie sa table de routage pour déterminer s'il existe un chemin connu. Si l'hôte distant appartient à un sous-réseau qu'il sait comment atteindre, le système vérifie s'il peut se connecter sur cette interface. Si tous les chemins connus échouent, le système dispose d'une dernière possibilité: la route par défaut. Cette route est un type spécial de route passerelle et il s'agit généralement de la seule route présente dans le système. Sur un routeur, un astérisque (*) indique une route par défaut dans les informations affichées par la commande **`show ip route`**. Pour les hôtes d'un réseau local, cette passerelle correspond à la machine qui dispose d'une connexion directe avec le monde extérieur et il s'agit de la passerelle par défaut répertoriée dans les paramètres TCP/IP de la station de travail. Si la route par défaut est configurée pour un routeur qui lui-même sert de passerelle vers l'Internet public, la route par défaut désigne la machine passerelle au niveau du site du fournisseur d'accès Internet. Les routes par défaut sont mises en œuvre à l'aide de la commande **`ip route`**.

```
Router(Config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

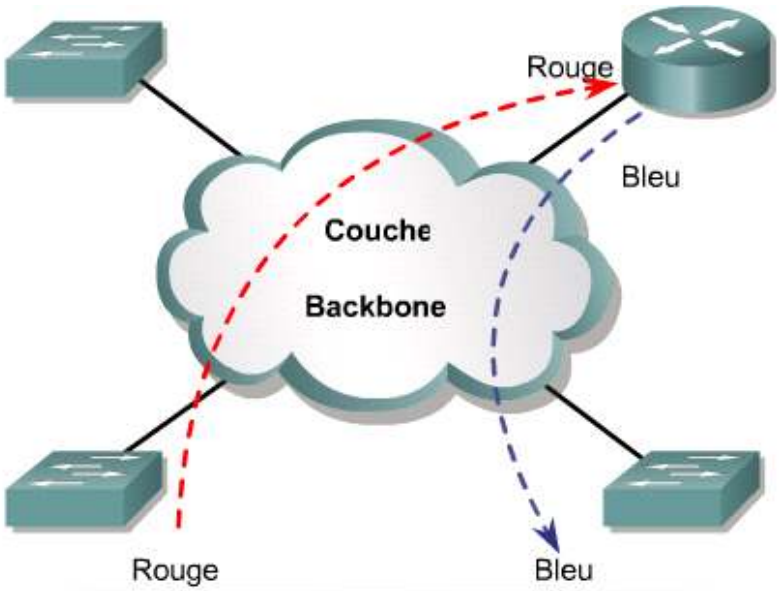
Dans cet exemple, 192.168.1.1 est la passerelle. La connectivité entre les VLAN peut être établie par le biais d'une connectivité physique ou logique.

Une connectivité logique implique une connexion unique, ou agrégation, du commutateur au routeur. Cette agrégation peut accepter plusieurs VLAN. Cette topologie est appelée «router-on-a-stick» car il n'existe qu'une seule connexion physique avec le routeur. En revanche, il existe plusieurs connexions logiques entre le routeur et le commutateur. [1]



Une connectivité physique implique une connexion physique séparée pour chaque VLAN. Cela signifie une interface physique distincte pour chaque VLAN.

Les premières configurations de VLAN reposaient sur des routeurs externes connectés à des commutateurs compatibles VLAN. Avec cette approche, les routeurs traditionnels sont connectés via une ou plusieurs liaisons à un réseau commuté. Les configurations «router-on-a-stick» utilisent un seul lien multi-VLAN qui connecte le routeur au reste du réseau du campus. [2] Le trafic entre les VLAN doit traverser le backbone de couche 2 pour atteindre le routeur par lequel il peut atteindre les différents VLAN. Le trafic circule ensuite vers la station d'extrémité souhaitée par une transmission de couche 2 normale. Ce flux «out-to-the-router-and-back» est caractéristique des conceptions «router-on-a-stick».

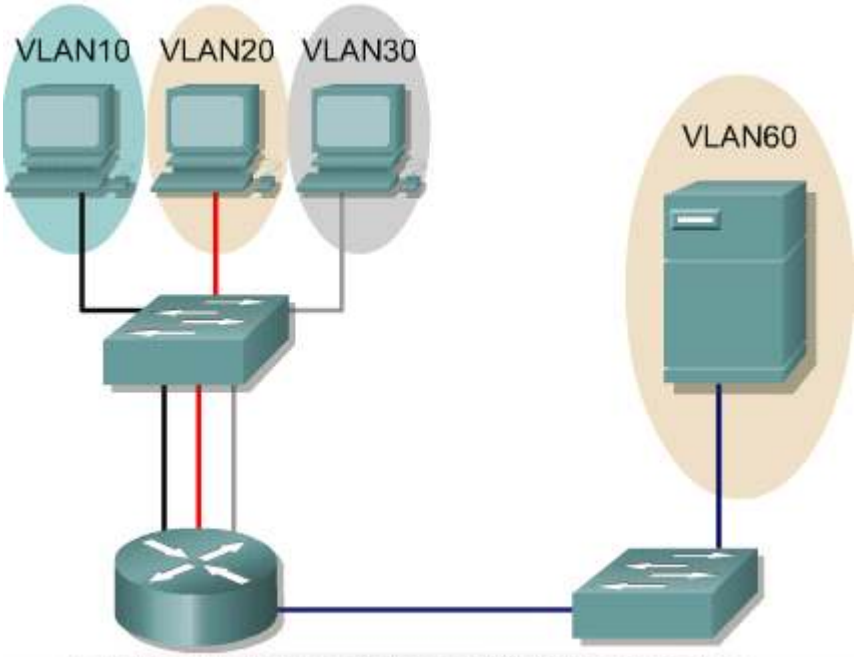


Pour que le trafic soit acheminé d'un VLAN à un autre, il doit passer par le routeur.

9.3 Vue d'ensemble du routage entre VLAN

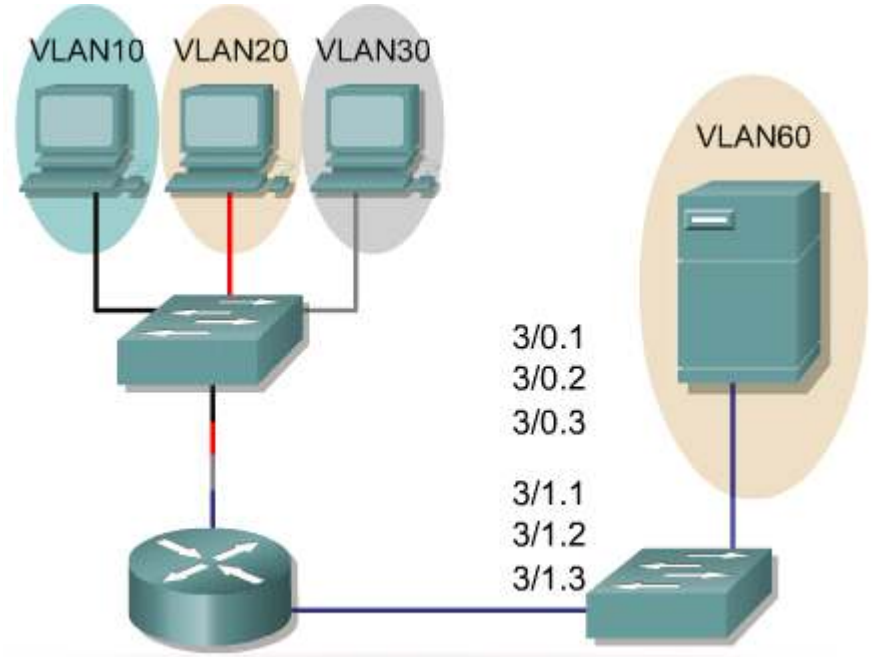
9.3.4 Interfaces physiques et logiques

Dans une situation traditionnelle, un réseau avec quatre VLAN nécessite quatre connexions physiques entre le commutateur et le routeur externe. 1



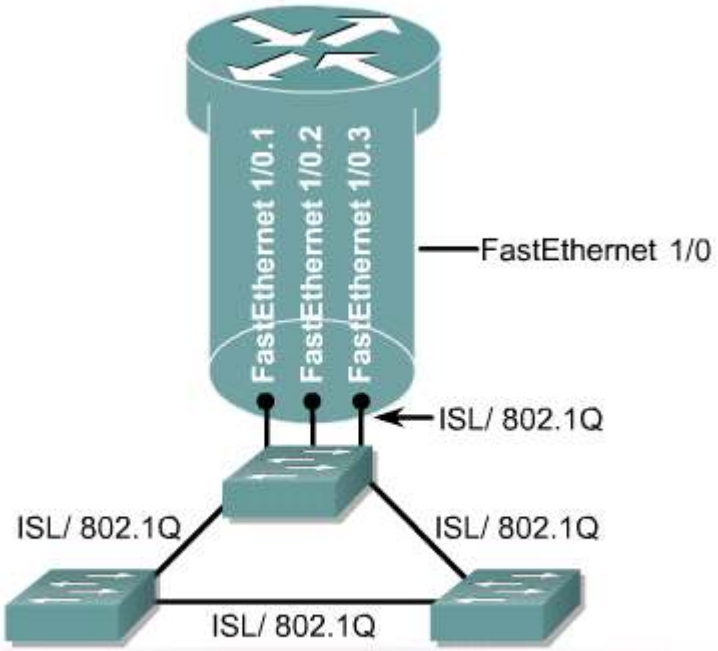
Le routeur prend en charge un VLAN par interface.

Avec l'arrivée de technologies comme ISL (Inter-Switch Link), les concepteurs de réseau ont commencé à utiliser des liens multi-VLAN pour connecter des routeurs à des commutateurs. 2 Bien que les technologies d'agrégation comme ISL, 802.1Q, 802.10 ou LANE (émulation LAN) puissent être utilisées, les approches basées sur Ethernet comme ISL et 802.1Q sont plus fréquentes.



Une liaison ISL unique peut prendre en charge plusieurs VLAN.

Le protocole Cisco ISL ainsi que la norme IEEE multifournisseur 802.1Q sont utilisés pour réunir des VLAN en une agrégation sur des liaisons Fast Ethernet. 3



Une interface ISL ou 802.1Q du routeur se connecte à un port multi-VLAN du commutateur.

La ligne continue dans l'exemple fait référence à la liaison physique unique entre le commutateur Catalyst et le routeur. Il s'agit de l'interface physique qui connecte le routeur au commutateur.

Lorsque le nombre de VLAN augmente sur un réseau, l'approche physique consistant à utiliser une interface de routeur par VLAN devient vite limitée en termes d'évolutivité. Les réseaux contenant de nombreux VLAN doivent utiliser le mécanisme d'agrégation de VLAN pour affecter plusieurs VLAN à une interface de routeur unique.

Les lignes en pointillé dans l'exemple correspondent aux liaisons logiques qui fonctionnent sur cette liaison physique par le biais de sous-interfaces. Le routeur peut prendre en charge de nombreuses interfaces logiques sur des liaisons physiques individuelles. Par exemple, l'interface Fast Ethernet FastEthernet 1/0 pourrait supporter trois interfaces virtuelles s'appelant FastEthernet 1/0.1, 1/0.2 et 1/0.3.

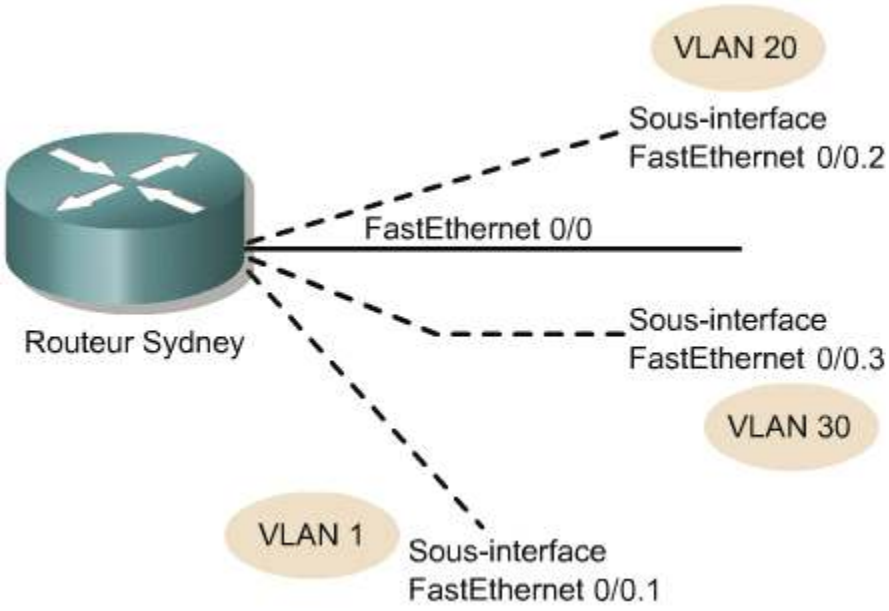
Le principal avantage de l'utilisation d'un lien multi-VLAN est la réduction du nombre de ports de routeur et de commutateur utilisés. Cela permet non seulement de réaliser une économie financière, mais peut également réduire la complexité de la configuration. Par conséquent, l'approche qui consiste à relier des routeurs par une agrégation peut évoluer vers un plus grand nombre de VLAN qu'une conception basée sur une liaison par VLAN.

9.3.5 Séparation des interfaces physiques en sous-interfaces

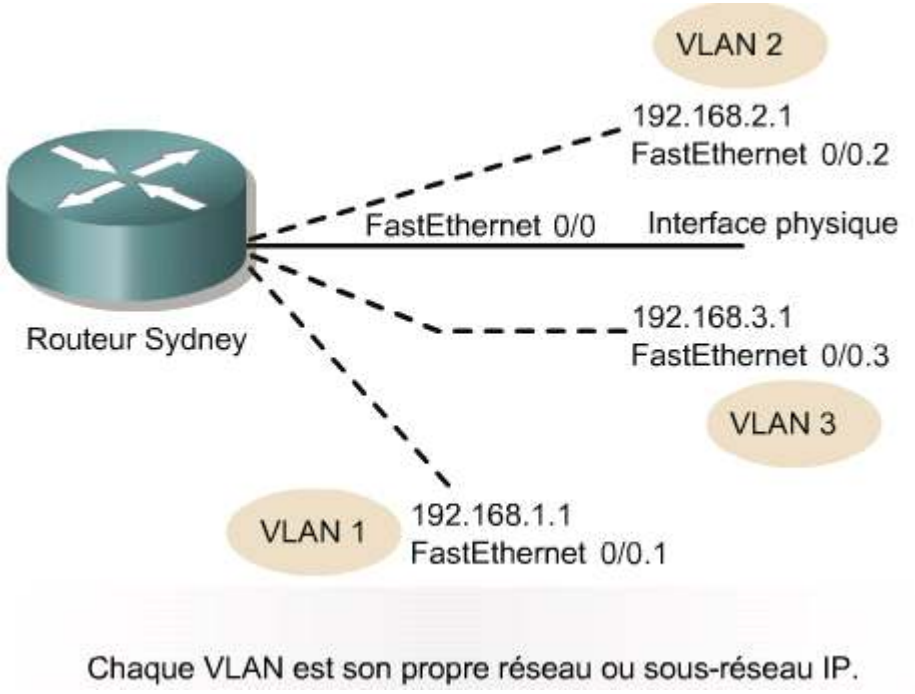
9.3.5 Séparation des interfaces physiques en sous-interfaces

Une sous-interface est une interface logique au sein d'une interface physique, telle que l'interface Fast Ethernet d'un routeur.

Plusieurs sous-interfaces peuvent coexister sur une seule interface physique. 1



Chaque sous-interface prend en charge un VLAN et dispose d'une adresse IP affectée. Pour que plusieurs unités d'un même VLAN communiquent, les adresses IP de toutes les sous-interfaces maillées doivent être sur le même réseau ou sous-réseau. Par exemple, si la sous-interface FastEthernet 0/0.1 a l'adresse IP 192.168.1.1, alors 192.168.1.2, 192.168.1.3 et 192.1.1.4 sont les adresses IP des unités connectées à la sous-interface FastEthernet0/0.1. [2]



Pour le routage entre VLAN avec sous-interfaces, une sous-interface doit être créée pour chaque VLAN. [3] [4]

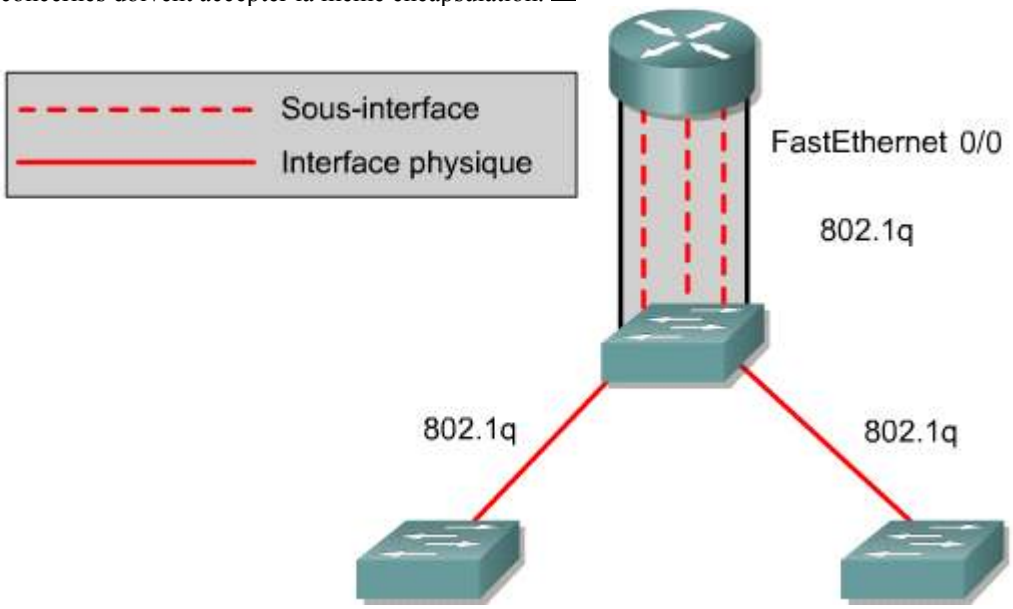
```
Sydney(config)#interface FastEthernet 0/0.1
Sydney(config-subif)#description Administration VLAN1
Sydney(config)#interface FastEthernet 0/0.2
Sydney(config-subif)#description Comptabilite VLAN 20
Sydney(config)#interface FastEthernet 0/0.3
Sydney(config-subif)#description Ventes VLAN 30
```

La section suivante évoque les commandes nécessaires à la création de sous-interfaces et à l'application d'un protocole d'agrégation et d'une adresse IP à chaque sous-interface.

9.3 Vue d'ensemble du routage entre VLAN

9.3.6 Configuration du routage entre des VLAN

Cette section présente les commandes nécessaires pour configurer un routage inter-VLAN entre un routeur et un commutateur. Avant de mettre en œuvre ces commandes, il est nécessaire de vérifier sur chaque routeur et commutateur le type d'encapsulation VLAN pris en charge. Les commutateurs Catalyst 2950 acceptent les agrégations 802.1Q depuis le lancement de la plate-forme logicielle Cisco IOS version 12.0(5.2)WC(1), mais ils ne prennent pas en charge les agrégations ISL (Inter-Switch Link). Pour que le routage entre VLAN fonctionne correctement, tous les routeurs et commutateurs concernés doivent accepter la même encapsulation. 1



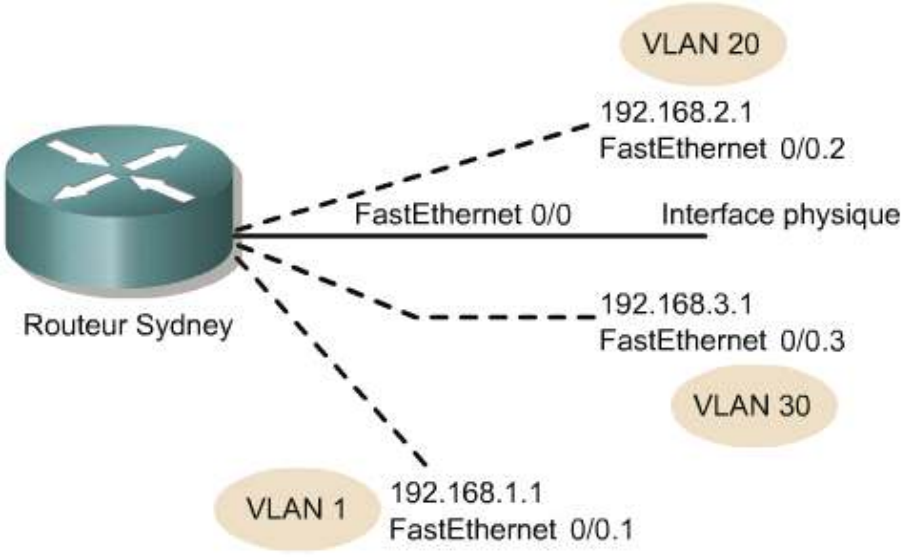
Sur un routeur, une interface peut être logiquement divisée en plusieurs sous-interfaces virtuelles. Les sous-interfaces fournissent une solution flexible pour le routage de plusieurs flux de données via une interface physique unique. Pour définir des sous-interfaces sur une interface physique, effectuez les tâches suivantes:

- Identifiez l'interface.
- Définissez l'encapsulation VLAN.
- Attribuez une adresse IP à l'interface.

Pour identifier l'interface, utilisez la commande **`interface`** en mode de configuration globale.

`Router(config)#`**`interface fastethernet`***`numéro-port. numéro-sous-interface`*

La variable *`numéro-port`* identifie l'interface physique tandis que la variable *`numéro-sous-interface`* identifie l'interface virtuelle. 2



Le routeur doit être capable de communiquer avec le commutateur à l'aide d'un protocole d'agrégation standardisé. Cela signifie que les deux unités interconnectées doivent se comprendre mutuellement. Dans l'exemple, 802.1Q est utilisé. Pour définir l'encapsulation VLAN, saisissez la commande **encapsulation** en mode de configuration d'interface.

```
Router(config-subif)#encapsulation dot1Qnuméro-vlan
```

La variable *numéro-vlan* identifie le VLAN pour lequel la sous-interface achemine le trafic. Un ID de VLAN est ajouté à la trame uniquement lorsque celle-ci est destinée à un réseau non local. Chaque paquet VLAN transporte l'ID du VLAN dans son en-tête.

Pour affecter l'adresse IP à la sous-interface, entrez la commande suivante en mode de configuration d'interface.

```
Router(config-subif)#ip addressadresse-ip masque-sous-réseau
```

Les variables *adresse-ip* et *masque-sous-réseau* correspondent au masque et à l'adresse réseau sur 32 bits de l'interface. 3

```
Sydney(config)#interface FastEthernet 0/0.1
Sydney(config-subif)#description Administration VLAN1
Sydney(config-subif)#encapsulation dot1q 1
Sydney(config-subif)#ip address 192.168.1.1
255.255.255.0
Sydney(config)#interface FastEthernet 0/0.2
Sydney(config-subif)#description Comptabilite VLAN 20
Sydney(config-subif)#encapsulation dot1q 20
Sydney(config-subif)#ip address 192.168.2.1
255.255.255.0
Sydney(config)#interface FastEthernet 0/0.3
Sydney(config-subif)#description Ventes VLAN 30
Sydney(config-subif)#encapsulation dot1q 30
Sydney(config-subif)#ip address 192.168.3.1
255.255.255.0
```

Dans l'exemple, le routeur a trois sous-interfaces configurées sur l'interface Fast Ethernet 0/0. Ces trois sous-interfaces sont identifiées par 0/0.1, 0/0.2 et 0/0.3. Toutes les interfaces sont encapsulées pour 802.1Q. L'interface 0/0.1 achemine les paquets du VLAN 1, tandis que l'interface 0/0.2 achemine les paquets du VLAN 20 et l'interface 0/0.3, ceux du VLAN 30.

Activité de TP

Exercice: Configuration du routage entre des VLAN

Dans ce TP, les étudiants vont créer une configuration de base sur un routeur et de tester la fonctionnalité de routage.

Activité de TP

Activité en ligne : Configuration du routage entre des VLAN

Au cours de ce TP, l'étudiant va créer une configuration de base sur un routeur et tester la fonctionnalité de routage.

Résumé

La compréhension des points clés suivants devrait être acquise:

- Origines et fonctions de l'agrégation de VLAN
- Comment une agrégation permet la mise en œuvre de VLAN dans un grand réseau
- Norme IEEE 802.1Q
- Cisco ISL
- Configuration et vérification d'une agrégation de VLAN
- Définition du protocole VTP
- Pourquoi VTP a été développé
- Contenu des messages VTP
- Modes VTP
- Configuration et vérification de VTP sur un commutateur basé sur l'IOS
- Pourquoi le routage est nécessaire pour la communication entre VLAN
- Différence entre interfaces physiques et logiques
- Sous-interfaces
- Configuration du routage entre les VLAN à l'aide de sous-interfaces sur un port de routeur

- L'agrégation de VLAN permet de définir de nombreux VLAN au sein d'une société en ajoutant des étiquettes spéciales aux trames pour identifier le VLAN auquel elles appartiennent.
- Le protocole VTP (VLAN Trunking Protocol) a été créé pour résoudre les problèmes de fonctionnement dans un réseau commuté comportant des LAN virtuels.
- Le rôle de VTP est de maintenir la cohérence de la configuration VLAN sur un domaine d'administration réseau commun. VTP est un protocole de messagerie qui utilise les trames d'agrégation de couche 2 pour gérer l'ajout, la suppression et l'attribution de nouveaux noms aux VLAN sur un domaine unique.
- Un domaine VTP est composé d'un ou de plusieurs équipements interconnectés qui partagent le même nom de domaine VTP. Un commutateur ne peut appartenir qu'à un seul domaine VTP.
- Lorsqu'une station d'extrémité dans un VLAN doit communiquer avec une station d'extrémité d'un autre VLAN, une communication entre VLAN est nécessaire. Pour cela, le routage est indispensable.