CCNA 3 - Module 1 – Introduction au routage sans classe (routage CIDR)

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 utilisateurs • Configuration d'adresses IP, de masques de sous-réseau et d'adresses de passerelles sur des routeurs et des hôtes • 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 fonctionnement	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.

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:

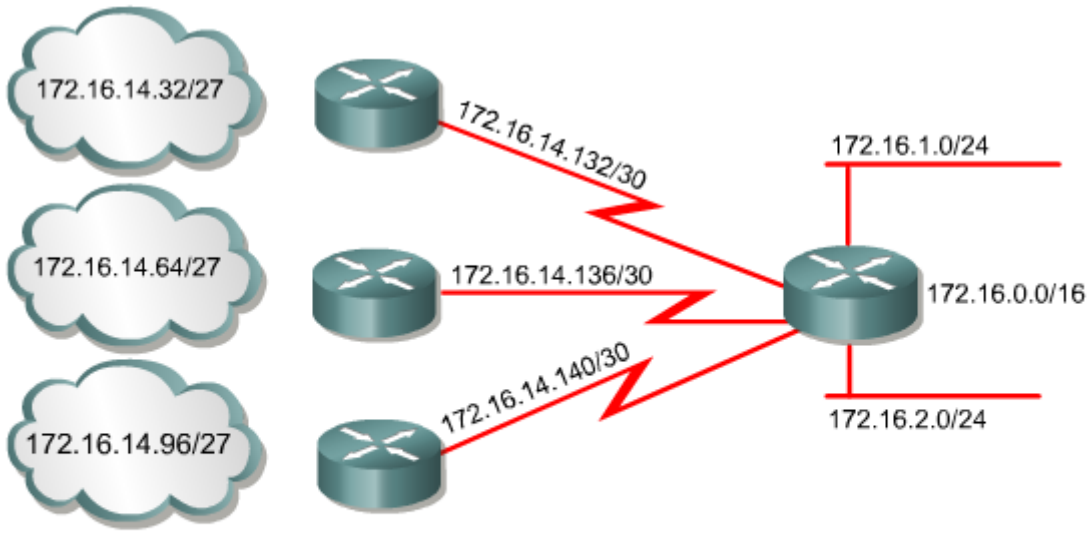
- Dernière solution : espace d'adressage IPv6 sur 128 bits
- Offre 340 283 366 920 938 463 374 607 431 768 211 456 possibilités

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.

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.



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.

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 111111**00** 00000000	22 bits

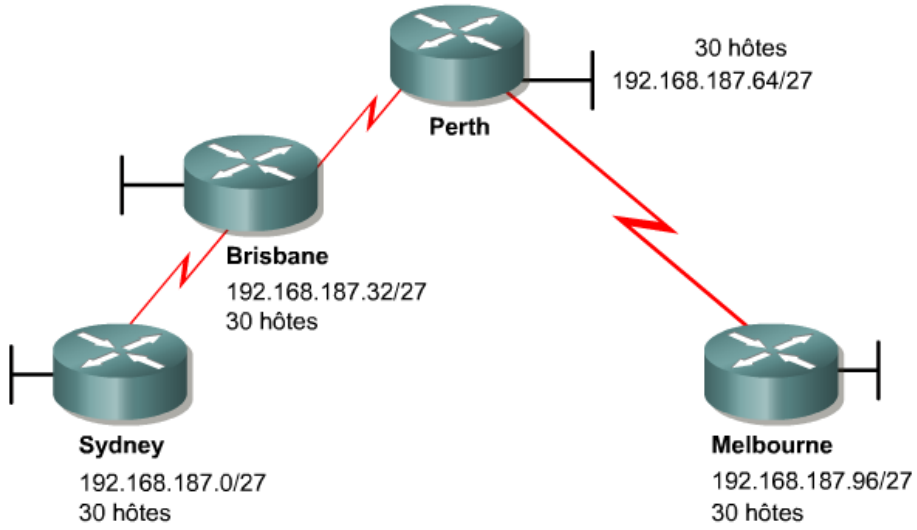
1.1.2 Gaspillage de l'espace

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.

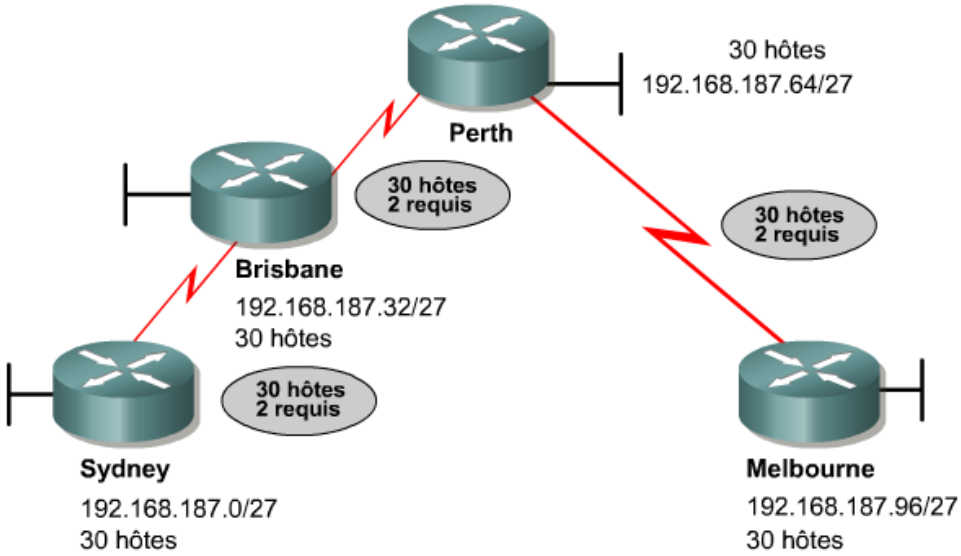
N° de sous-réseau	Adresse de sous-réseau	
Sous-réseau 0	192.168.187.0	/27
Sous-réseau 1	192.168.187.32	/27
Sous-réseau 2	192.168.187.64	/27
Sous-réseau 3	192.168.187.96	/27
Sous-réseau 4	192.168.187.128	/27
Sous-réseau 5	192.168.187.160	/27
Sous-réseau 6	192.168.187.192	/27
Sous-réseau 7	192.168.187.224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



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.

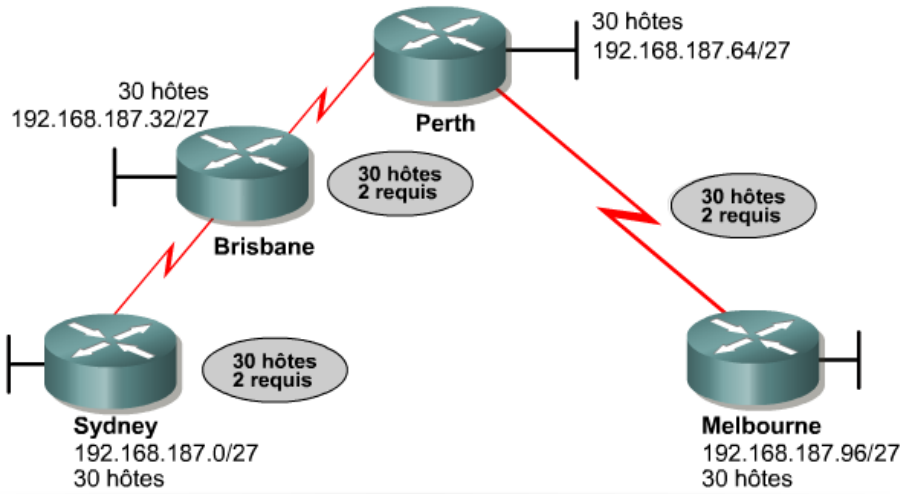
Un tel système d'adressage convient pour un petit LAN. Néanmoins, il entraîne un gaspillage énorme lorsqu'il est utilisé avec des connexions point à point.



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.



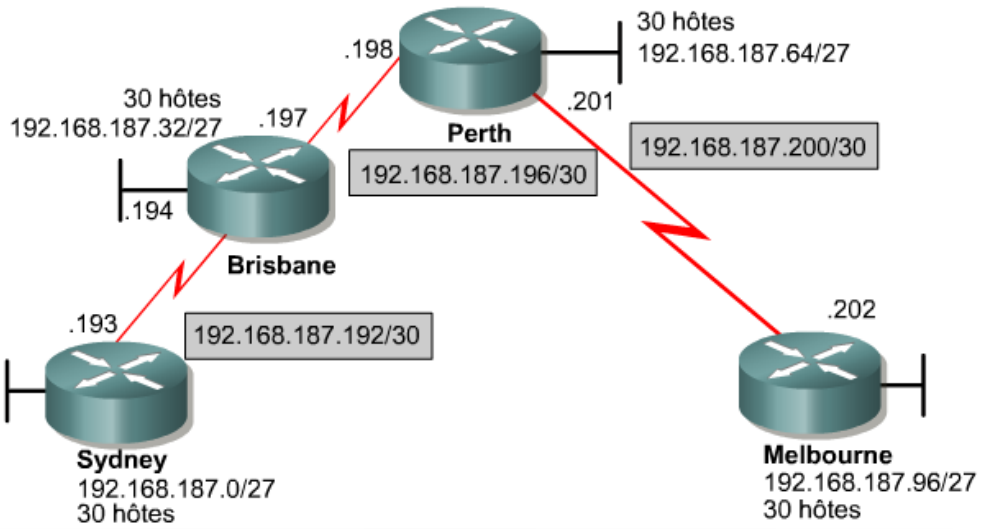
Utilisez VLSM sur les liaisons point-à-point pour n'utiliser que deux adresses hôte valides au lieu d'en gaspiller 28.

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. Ces deux figures 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

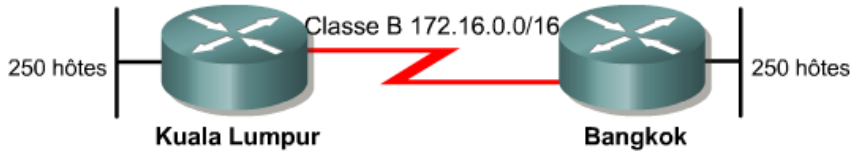
N° de sous-réseau	Adresse de sous-réseau	
Sous-sous-réseau 0	192.168.187.192	/30
Sous-sous-réseau 1	192.168.187.196	/30
Sous-sous-réseau 2	192.168.187.200	/30
Sous-sous-réseau 3	192.168.187.204	/30
Sous-sous-réseau 4	192.168.187.208	/30
Sous-sous-réseau 5	192.168.187.212	/30
Sous-sous-réseau 6	192.168.187.216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

1.1.4 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



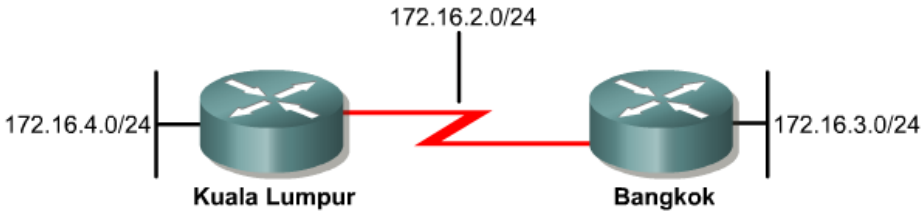
Chaque réseau LAN doit accepter jusqu'à 250 hôtes. Le réseau de classe B 172.16.0.0/16 peut être subdivisé avec un masque sur 24 bits (255.255.255.0) pour créer des sous-réseaux suffisamment importants pour chaque LAN.

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

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.

Classe B subdivisée sous la forme 255.255.255.0

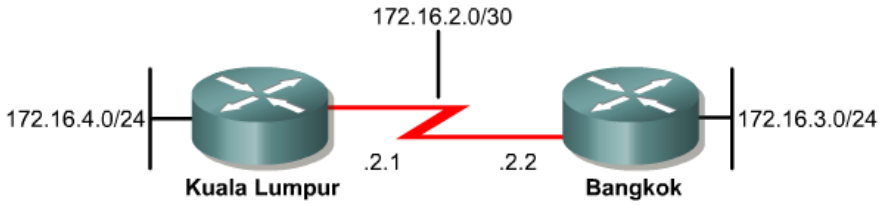
N°	Sous-réseau	Plage d'adresses	Adresse de broadcast
0	172.16.0.0	172.16.0.1 - 172.16.0.254	172.16.0.255
1	172.16.1.0	172.16.1.1 - 172.16.1.254	172.16.1.255
2	172.16.2.0	172.16.2.1 - 172.16.2.254	172.16.2.255
3	172.16.3.0	172.16.3.1 - 172.16.3.254	172.16.3.255
4	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
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.



/30 permet de gaspiller moins d'adresses.

Dans la figure ci-dessous, es 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.

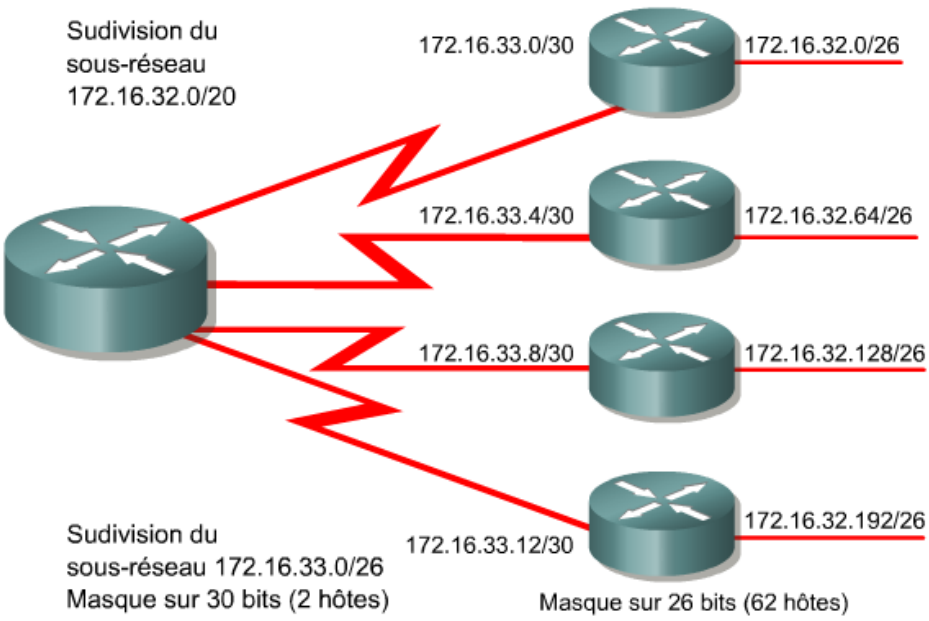
Pour calculer les adresses de sous-réseau utilisées sur les liaisons WAN, vous devez subdiviser un des réseaux /26 inutilisé. Dans cet exemple, 172.16.33.0/26 est subdivisé avec le préfixe /30. Quatre bits de sous-réseau supplémentaires sont ainsi générés ce qui crée 16 (2^4) sous-réseaux pour les WAN.

Adresse de réseau subdivisée : 172.16.32.0/20
Format binaire : 10101100.00010000.00100000.00000000

Adresse VLSM : 172.16.32.0/26
Format binaire: 10101100.00010000.0010 0000.00000000

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

La figure ci-dessous 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.

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.

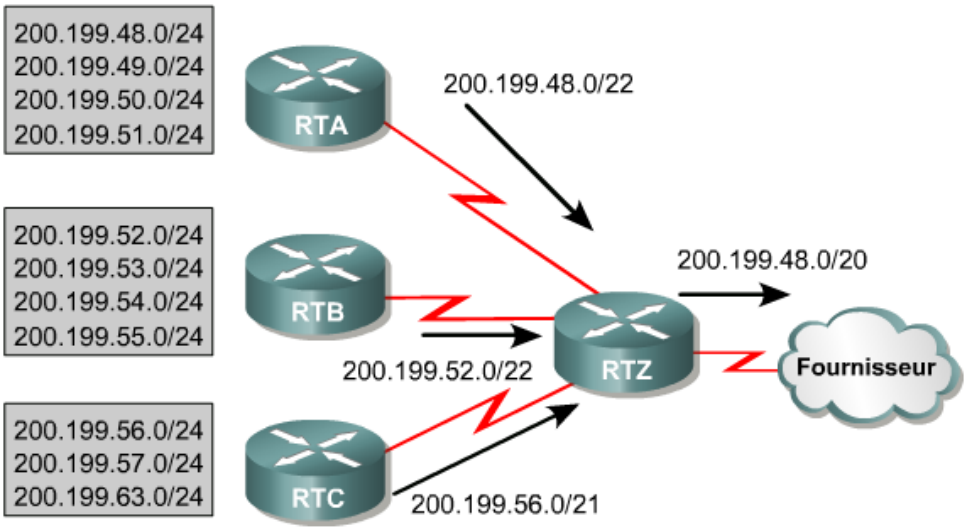
1.1.5 Regroupement de routes avec VLSM

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.

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.



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

Le 2ème figure 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 2ème figure , 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

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 ci-dessous, 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.

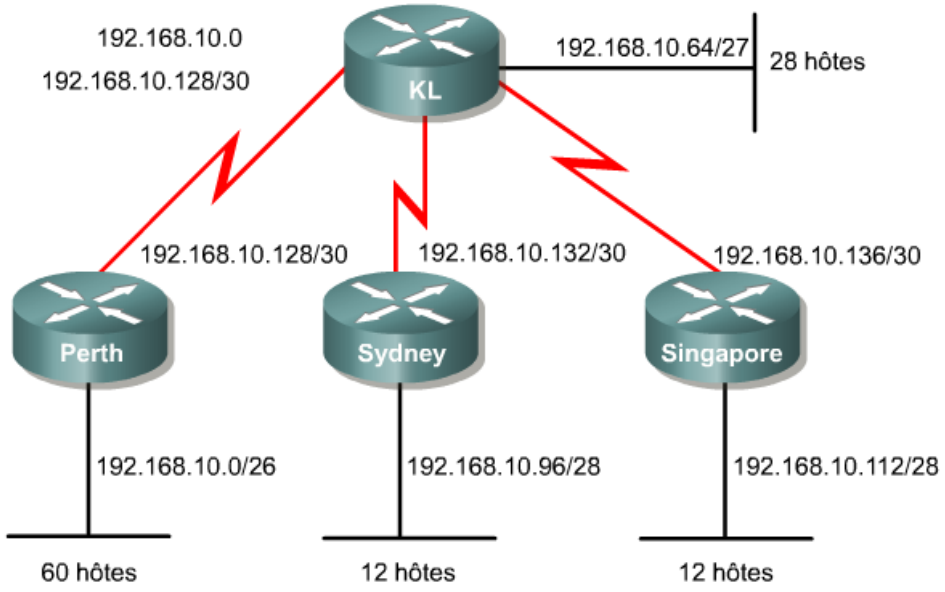
Adresses	Premier Octet	Second Octet	Troisième Octet	Quatrième Octet
172.16.0.0	10101100	00010000	00000000	00000000
172.16.2.0	10101100	00010000	00000010	00000000
172.16.3.128	10101100	00010000	00000011	10000000
172.16.4.0	10101100	00010000	00000100	00000000
172.16.4.128	10101100	00010000	00000100	10000000

Réponse :

172.16.0.0/21	10101100	00010000	00000000	00000000

1.1.6 Configuration de VLSM

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



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.

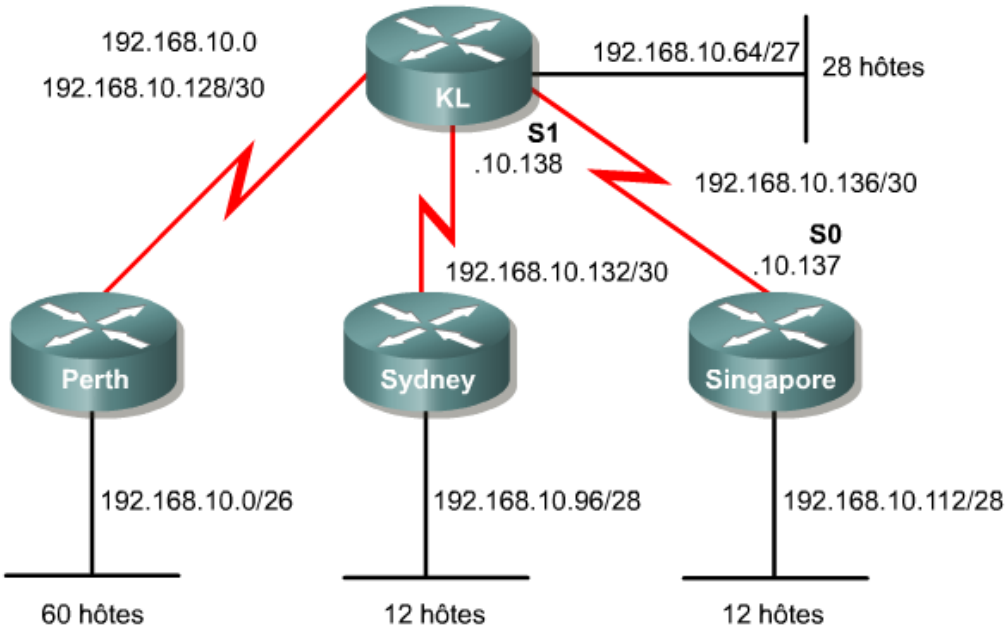
Le routeur Kuala Lumpur doit gérer 28 hôtes. Dans ce cas, il faut au moins cinq bits dans la portion hôte de l'adresse. Cinq bits permettent de générer 30 adresses hôte, $2^5 = 32 – 2 = 30$, la division donne donc ici 192.168.10.64/27.

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.



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
```

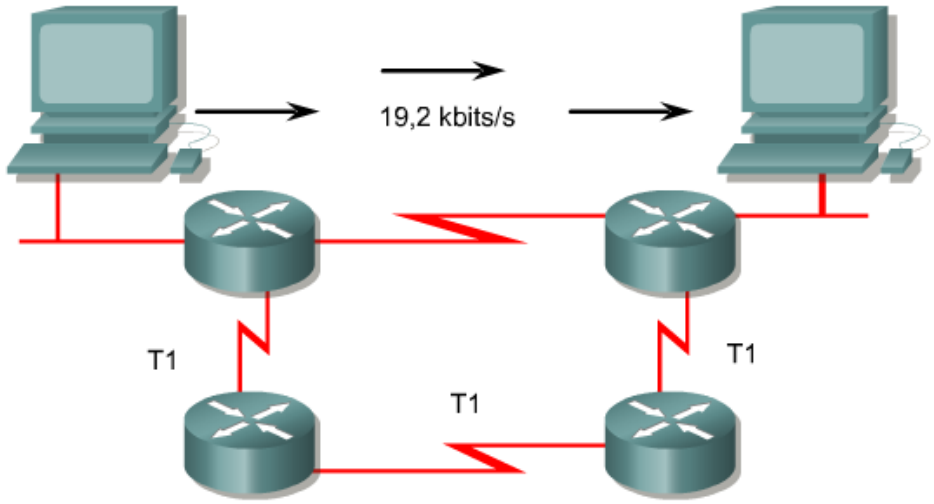
```
KualaLumpur(config)#interface serial 1
KualaLumpur(config-if)#ip address 192.168.10.138 255.255.255.252
```

1.2.1 Historique du protocol 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.

RIP v1 est considéré comme un protocole IGP par classes (classful).



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 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 2ème figure.

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:

- 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.

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.

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.

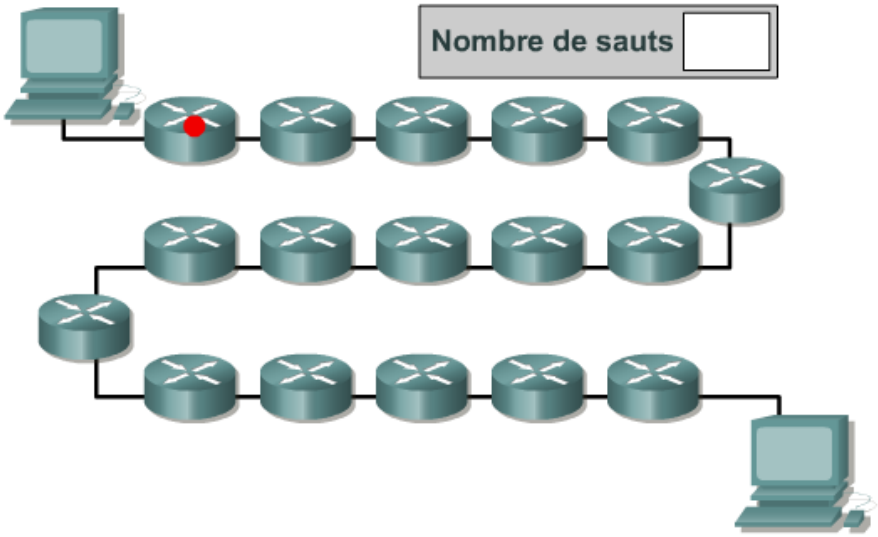
RIP v2 permet l'authentification dans ses mises à jour. Il est possible d'utiliser une combinaison de clés sur une interface comme vérification d'authentification. RIP v2 permet de choisir le type d'authentification à utiliser dans les paquets RIP v2. Il peut s'agir de texte en clair ou d'un cryptage 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.

1.2.3 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.



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 2ème figure 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.

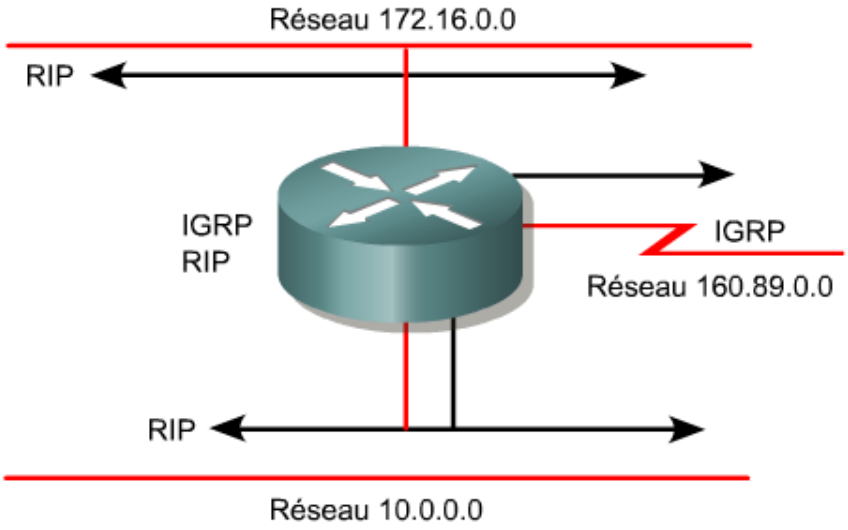
RIP v2 est une version améliorée de RIP v1. Ils ont beaucoup de fonctions communes. RIP v2 est également un protocole à vecteur de distance qui utilise le nombre de sauts, les compteurs de retenue et la règle «split horizon».

La 3ème figure 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.

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.



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.

La commande router lance le processus de routage.

```
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
```

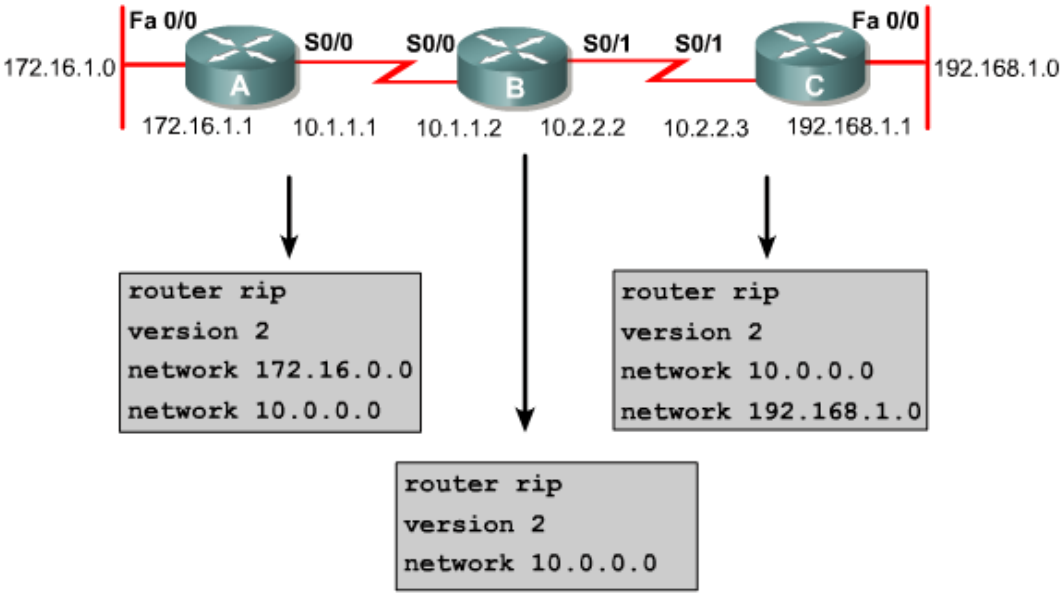
• Commande de configuration obligatoire pour chaque processus de routage IP
• Identifie le réseau physiquement connecté auquel sont transmises les mises à jour de routage.

La commande 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.

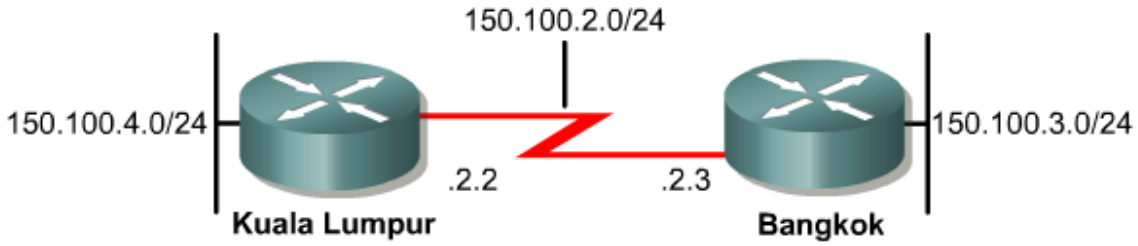


Dans cet exemple, la configuration du routeur A inclut les commandes suivantes:

- 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 ci-dessous présente un autre exemple de configuration RIP v2.

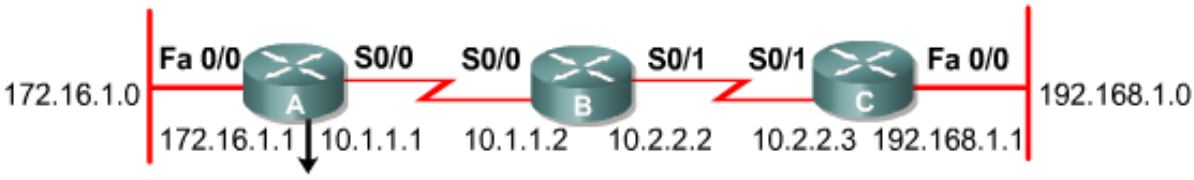



```
Kuala Lumpur(config)#router rip
Kuala Lumpur(config-router)#version 2
Kuala Lumpur(config-router)#network 150.100.0.0
```

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

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.

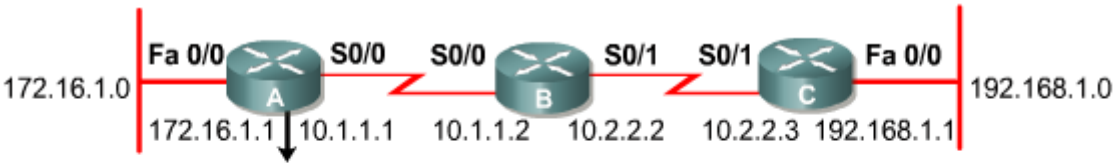



```
RouterA#show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 12 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing 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)
```

Cette section explique comment utiliser les commandes show pour vérifier la configuration RIP.

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 2ème figure , 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. 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.

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.

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.

Les commandes no debug all ou undebug all permettent de désactiver toutes les opérations 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.


```
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
```

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.

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 3ème figure 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

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 ci-dessus, 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

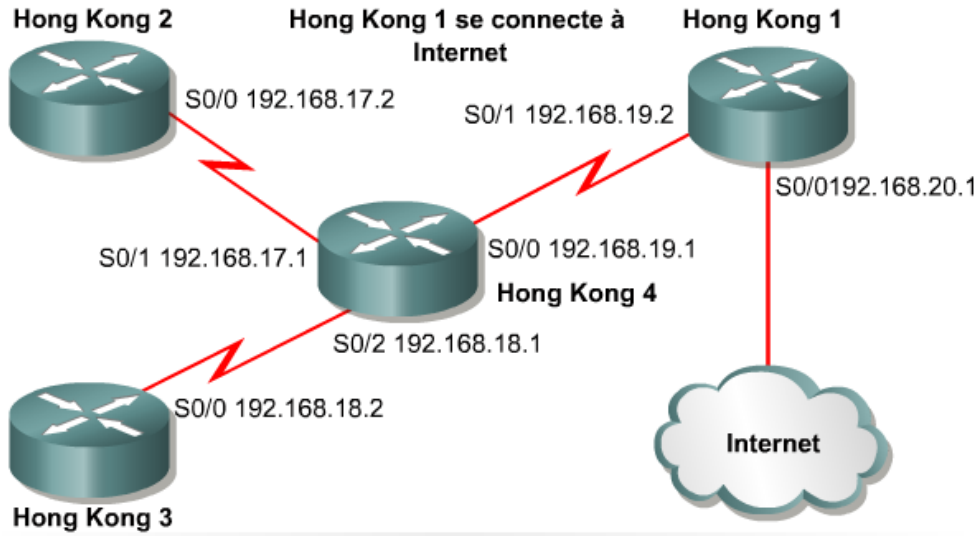
Commande	Description
`Router(config)#ip default-network 192.168.20.0`	Numéro de réseau IP défini en tant que valeur par défaut. Le numéro de réseau spécifié ici doit être sans classe puisqu'il s'agit d'une commande sans classe (classful).

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

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 ci-dessus, 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

• 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.

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