IPv6 Module 1b – ISIS

Objectif: Créer un réseau IPv6 avec un seul niveau IS-IS par dessus une infrastructure IPv4.

Pre-requis: IPv4 Module 1b, connaissance de routeur Cisco CLI, expérience pratique antérieure.

Ci-dessous la topologie utilisée pour la première série de séances de labo.

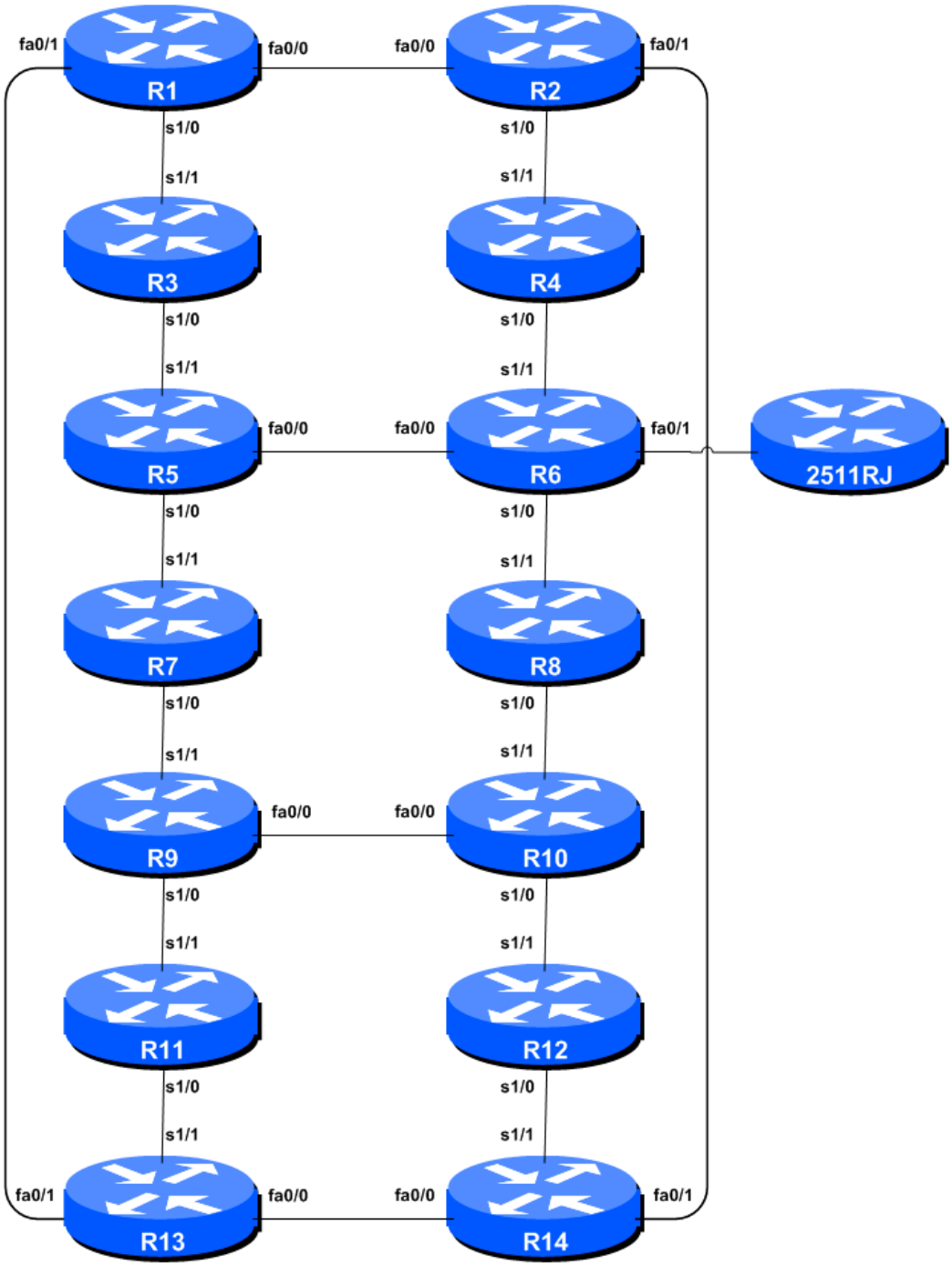

Figure 1 – ISP Lab Basic Configuration

Remarques

Ce module complète le module 1b IPv4. La topologie and la configuration IPv4 doivent être gardées à l'identique.

Les routeurs utilises pour cette partie du cours doivent supporter IPv6. N'importe quelle image IP Plus à partir de la version 12.2T inclue devrait convenir (IP Plus a été renommé Advanced IP Services pour la majorité des plateformes à partir de la version 12.3 de la branche principale). Comme toujours, il est recommandé de vérifier sur le *Cisco Feature Navigator* www.cisco.com/go/fn le set d'images et de plateformes supportant IPv6. Malheureusement IPv6 ne fait pas partie des images *basic IP only* or *Service Provider IOS* utilisées par la plupart des ISPs.

Configuration du labo

1. **Activer IPv6.** Les routeurs Cisco avec une image IOS supportant IPv6 n'ont pas IPv6 activé par défaut. Il faut dont activer IPv6 avant de passer à la suite. Ceci se fait à l'aide de la commande:

   ```
   Router(config)# ipv6 unicast-routing
   ```

   Maintenant le routeur est configuré pour supporter IPv6 en mode unicast (en plus de IPv4 en mode unicast qui est fourni par défaut). Sauvez la configuration.

2. **Activer IPv6 CEF.** Contrairement à IPv4, pour IPv6 , CEFv6 n'est pas activé par défaut. CEFv6 est activé à l'aide de la commande :

   ```
   Router(config)# ipv6 cef
   ```

   Rien ne va casser si IPv6 CEF n'est pas actif, mais il ne sera pas possible d'utiliser certaines fonctionnalités avancées comme NetFlow si IPv6 CEF n'est pas configuré.

1. **Désactiver IPv6 Source Routing.** A moins que vous ne croyez qu'il est vraiment nécessaire de l'activer, le routage source doit être désactivé. Cette option, activée par défaut, permet au routeur de traiter les paquets avec l'option « source routing header ». Cette fonction est un risque de sécurité bien connue car elle permet aux sites distants d'envoyer des paquets avec une adresse source différente à travers le réseau (ce qui était utile pour le dépannage des réseaux a partir d'endroits différents sur Internet, mais ces dernières années il a été largement abusé par des mécréants sur l'Internet).

   ```
   Router1 (config)# no ipv6 source-route
   ```

3. **IPv6 Addressing Plans.** En IPv6 l'adressage varie de ce qui se fait en IPv4. En IPv4, le système est basé sur les RIRs qui allouent de l'espace d'adressage à des LIR (ISP membre d'un RIR) en fonction des besoins de l'ISP; cette allocation est censée subvenir aux besoins de l'ISP pendant un an sans autre demande au RIR. Il est attendu des ISP qu'ils implémentent un processus similaire vis-à-vis de leurs clients – en allouant un espace d'adresse tenant compte des besoins du client.

   Pour IPv6, le système est un peu différent. Les RIRs allouent toujours de l'espace d'adressage en fonction des besoins de leurs membres mais la justification à fournir pour obtenir de l'espace v6 est moins forte que pour IPv4. Un des grands avantages d'IPv6 est qu'un ISP alloue systématiquement un /48 à chaque client. C'est l'allocation minimum pour un site/client. Un /48

comprend un multitude de /64. Cela est considéré comme suffisant pour tous sauf les plus grands réseaux disponibles à l'heure actuelle. La plus petite unité qui puisse être allouée hors d'un /48 est un /64. Chaque LAN, chaque lien point-à-point reçoit un /64. **Note: Dans cet atelier nous nous basons sur les recommandations du RFC6164. Nous utilisons in masque /127 pour les liens point-à-point même si un /64 lui est réservé.**

Ce système d'adressage IPv6 est largement simplifié par rapport a IPv4. Un ISP alloue un seul /48 pour son infrastructure réseau. Le reste de leur /32 est alloué aux clients. Comme nous allons le voir ci-dessous, cet atelier se base sur ce principe.

4. **Adresses IPv6.** Comme pour le module 1 relatif a IPv4, nous allons d'abord introduire les concepts de base afin de mettre au point un plan d'adressage IPv6 rationnel adaptés aux besoins d'un ISP. Etant donné que les RIRs délèguent habituellement les préfixes v6 par blocks de /32, nous supposons que notre ISP de laboratoire a obtenu un /32. Nous utilisons le préfixe 2001:db8::/32, l'espace réservé a des fins de documentation, au lieu d'utiliser un espace d'adressage public. Dans la réalité de l'Internet nous aurions utilisé une espace public qui nous aurait été alloué ultérieurement par un RIR.

   Typiquement, ISPs divisent leur block d'adressage en trois morceaux. Un morceau est utilisé pour les allocations aux clients, le deuxième pour les liens point-à-point de l'infrastructure de l'ISP, et le dernier morceau est réservé aux adresses loopback pour les routeurs du backbone. Le schéma de la
   Figure **2** illustre ce qui se fait habituellement.

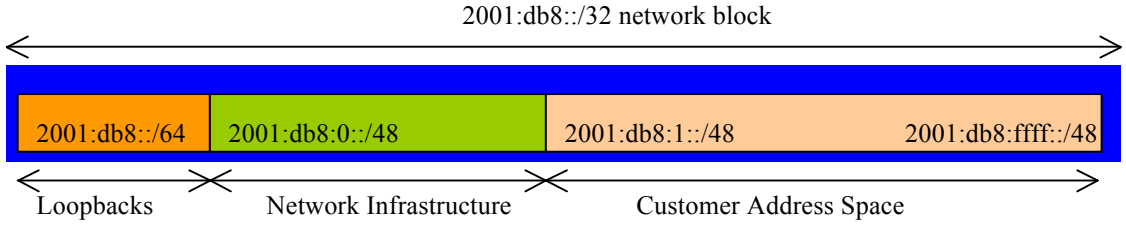

Figure 2 – Division du bloc /32 alloué en une partie pour les clients, l'infrastructure et les loopbacks

Etudiez le plan d'adressage fourni en annexe. Remarquez que l'infrastructure utilise le premier /48 du bloc /32 d'adresses. Voyez comme nous avons mis de côté un /64 hors du bloc pour l'infrastructure afin de numéroter les loopbacks de nos routeurs. Les ISPs tendent à documenter leur plan d'adressage plans dans les fichiers textes or des *spreadsheets* – Figure 3 ci dessous montre un extrait de plan d'adressage typique suivant les lignes directrices exposées plus haut.

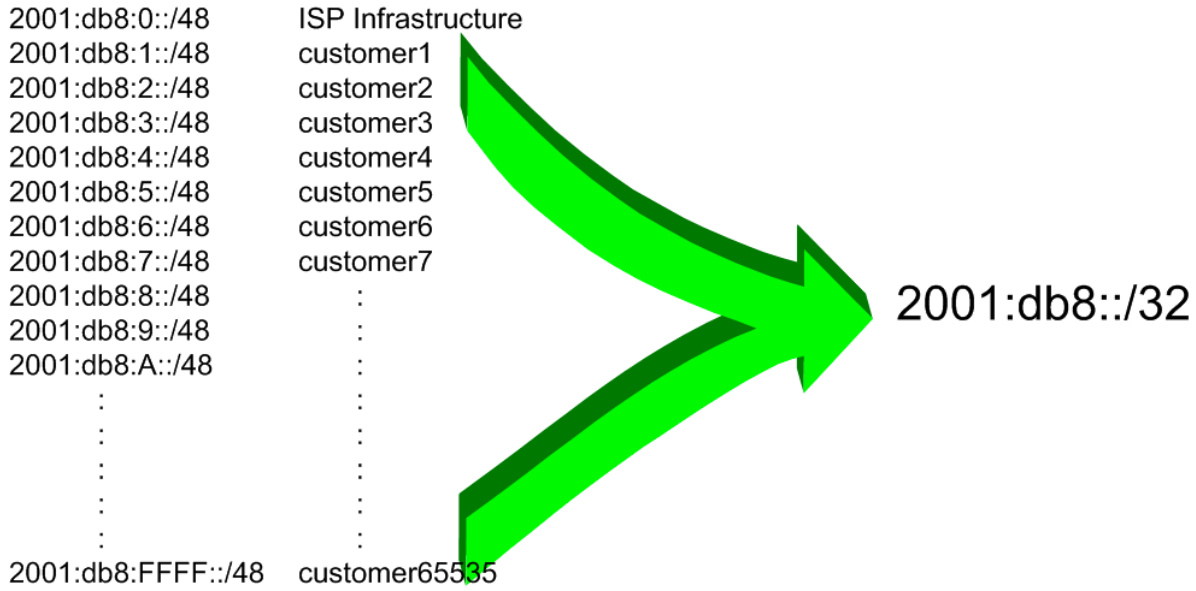

Figure 3 – Extrait d'un plan d'adressage d'ISP

6. **Connexions en série Back-to-Back.** Chaque équipe alloue maintenant les adresses IPv6 aux connexions série de son routeur. Voir plan d'adressage en annexe.

   Note: Dans cet atelier nous n'utilisons pas d'adresses de type EUI-64. Au lieu de cela nous attribuons des adresses absolues à chaque interface. Cette dernière méthode est beaucoup plus facile à gérer, plus facile pour gérer et référencer les liens point-à-point et les relations de voisinages entre routeurs.

   Voici un exemple de configuration simple :

   ```
   Router2(config)# interface serial 1/0
   Router2(config-if)# ipv6 address 2001:db8:0:6::/127
   ```

   Q: Quel masque réseau utiliser sur les interfaces où IPv6 est activé ?
   A: Le masque utilisé est /127. Ceci est le sous-réseau recommandé sur les liens point-à-point par le RFC6164. Nous réservons tout de même un /64 pour chaque lien point-à-point. Assigner le sous-réseau de taille minimale devrait nous permettre de faire face à de futures évolutions requérant plus d'adresses.

   Note: Comme mentionné lors de la présentation d'IPv6, certains ISPs utilisent des /126 et /120 comme masque sur leurs liens point-à-point. Nous aurions pu faire cela mais nous avons préféré suivre le RFC6164. Nous aurions également pu numéroter nos liens point-à-point hors d'un seul /64. Ceci pourrait cependant causer des problèmes lors de future développements du standard IPv6 si certains bits entre /65 et /128 sont dédiés à des cas d'utilisations spécifiques.

5. **Connexions Ethernet.** Comme à l'étape précédente, attribuez les adresses IPv6 de vos connexions Ethernet point-à-point.

6. **Ping Test n ° 1.** Envoyez un Ping vers tous les subnets des routeurs voisins connectés physiquement. Si les subnets connectés physiquement sont inaccessibles, consulter les équipes voisines pour trouver le problème. Ne pas ignorer le problème – il peut persister. Utilisez les commandes suivantes pour dépanner la connexion:

```
show ipv6 neighbors                          : Contenu de la cache IPv6 pour les voisins
show ipv6 interface <interface> <number>     : Configuration et état d'une interface
show ipv6 interface                          : Résumé de l'état des interfaces IP et leur
configuration
```

7. **Attribuer les Adresses IPv6 aux Interfaces Loopback.** Malgré le fait que nous n'ayons pas besoin des interfaces loopback à ce stade de l'atelier, il est tout de même utile de les configurer avec une adresse v6 dès à présent. La loopback sera utilisée plus tard pour l'établissement des sessions iBGP. Notons que les IDs OSPF et BGP router IDs sont des entiers de 32 bits qui derivent en IOS de l'IPv4 attribuée à l'interface Loopback (De ceci peut découler des problèmes lors de déploiements sans configuration d'adresses IPv4).

   Q. Pourquoi pensez-vous que le manque d'adresse IPv4 sur un routeur puisse poser problème ? Demandez à l'instructeur d'élaborer.

   Le sous-réseau minimum étant un /64 poir IPv6, nous attribuons les premiers /64 de notre /48 réservé à l'infrastructure pour les loopbacks – Nous allons donc utilisé des adresses dans 2001:db8:0:0/64 pour nos loopbacks. Il y a 14 routeurs dans le labo – l'attribution des adresses loopback est:

R1	**2001:db8::1/128**	**R8**	**2001:db8::8/128**
R2	**2001:db8::2/128**	**R9**	**2001:db8::9/128**
R3	**2001:db8::3/128**	**R10**	**2001:db8::a/128**
R4	**2001:db8::4/128**	**R11**	**2001:db8::b/128**
R5	**2001:db8::5/128**	**R12**	**2001:db8::c/128**
R6	**2001:db8::6/128**	**R13**	**2001:db8::d/128**
R7	**2001:db8::7/128**	**R14**	**2001:db8::e/128**

   Par exemple, l'équipe Router 1 configure l'adresse et le masque suivant pour sa loopback sur Router 1:

```
Router1(config)# interface loopback 0
Router1(config-if)# ipv6 address 2001:db8::1/128
```

   Q: Pourquoi utilisons-nous un masque /128 pour une interface loopback?

   A: Il n'y a pas de réseau physique attaché à la loopback, de sorte qu'il ne peut y avoir qu'un dispositif. Donc, nous avons seulement besoin d'affecter un masque /128 - c'est un gaspillage d'espace d'adressage d'utiliser autre chose.

Checkpoint #1: *Appelez l'isntructeur pour vérifier la connectivité. Montrez que vous pouvez faire un ping et telnet sur les routeurs adjacents.*

8. **ISIS dans un seul AS.** ISIS est déjà configuré pour IPv4 dans l'AS – chaque équipe vérifie maintenant que l'IGP opère toujours correctement avant de passer à l'étape suivant qui consiste a ajouter le support d'IPv6.

9. **Activation de Multi-Topology ISIS.** Nous avons besoin de multi-topology ISIS pour déployer IPv6 si le réseau supporte déjà IPv4 ISIS. Ceci permet un déploiement progressif d'IPv6. Chaque

équipe peut configurer le support ISIS IPv6 sans besoin de coordination avec les équipes des routeurs voisins.

```
Router1(config)# router isis workshop
Router1(config-router)# address-family ipv6
Router1(config-router-af)# multi-topology
```

NB. Si nous n'activons pas multi-topology, chaque equipe devra se coordonner avec la voisine pour activer IPv6 ISIS sur l'interface correspondante. Sinon, la session ISIS sera *down* car la topologie vue par les deux côtés du lien ne correspondra pas pour cette interface.

NB. Multi-topology est configurable pour IOS 12.3 et 12.4 mais ne fonctionne pas à cause d'un bug que cisco se refuse à corriger. L'alternative est d'utiliser *single topology* tout en sachant le problème précédent ou alors de déployer 12.2SRE, 12.2SXH, 12.4T, 15.0 ou des images plus récentes d'IOS.

10. **Activation d'ISIS sur chaque interface.** Toutes les interfaces point-à-point et ethernet doivent maintenant être configurées pour IPv6 ISIS. Sinon, vous ne verrez probablement pas les annonces ISIS des routeurs a 2 sauts ou plus de votre routeur.

    Pour Router 1 la configuration est:

```
Router1(config)# interface fastethernet 0/0
Router1(config-if)# ipv6 router isis workshop
!
Router1(config)# interface fastethernet 0/1
Router1(config-if)# ipv6 router isis workshop
!
Router1(config)# interface serial 1/0
Router1(config-if)# ipv6 router isis workshop
```

Note: L'identifiant IS-IS (IS-IS ID) utilisé pour les interfaces est le même que IS-IS ID configuré au niveau du router.

Métriques ISIS. Chaque équipe configure maintenant la métrique IS-IS pour chaque interface physique. La métrique IS-IS par défaut pour tous les types d'interface est 10. Contrairement à OSPF avec IOS, IS-IS ne converti pas automatiquement la bande-passante d'un lien en un coût/métrique. Les ISPs utilisant IS-IS doivent allouer eux-mêmes les métriques des liens (Notons que la majorité des ISPs déployant OSPF font de même). Ici nous utilisons une métrique de 2 pour les interfaces Ethernet et 20 pour les interfaces séries.

Ceci donne par exemple:

```
Router1(config)# interface fastethernet 0/0
Router1(config-if)# isis ipv6 metric 2 level-2
!
Router1(config)# interface fastethernet 0/1
Router1(config-if)# isis ipv6 metric 2 level-2
!
Router1(config)# interface serial 1/0
Router1(config-if)# isis ipv6 metric 20 level-2
```

11. **Annonce des Loopback /128.** Les interfaces loopback sont déjà marquées comme passives lors du setup d'ISIS pour le routage IPv4. Chaque équipe vérifie que la commande passive-interface est toujours présente pour la Loopback.

12. **Adjacences ISIS.** Activer le log des changements d'adjacences IS-IS. Une notification est générée à chaque changement d'un voisin CLNS. C'est très utile pour débugger.

```
Router1(config)# router isis workshop
Router1(config-router)# log-adjacency-changes
```

13. **Éviter le blackhole du trafic lors d'un redémarrage.** Lorsqu'un un routeur redémarre après avoir été mis hors service, IS-IS va commencer la distribution des préfixes dès que les adjacences avec ses voisins sont rétablies. Dans la suite des laboratoires, nous introduirons iBGP. Lors d'un reboot de routeur IS-IS démarre bien avant le rétablissement des sessions iBGP. Le router peut se retrouver sur le chemin du trafic qui transite d'un client vers un pair ou un fournisseur en amont, ou l'inverse, avant que la table BGP ne soit complète. Il en résulte que la table de forwarding ne contient pas tous les préfixes. Le trafic de transit sera alors jeté ou bouclera dans le réseau. Afin d'éviter ce problème, il est possible de forcer le routeur à ne pas s'annoncer comme étant disponible avant l'établissement des sessions iBGP. Ceci se fait à l'aide de la commande suivante :

```
Router1(config)#router isis workshop
Router1(config-router)#address-family ipv6
Router1(config-router-af)#set-overload-bit on-startup wait-for-bgp
```

    Ceci configure l'overload bit d'ISIS tel que les routes IPv6 passant par ce routeur soient marquées comme inaccessible (très haute métrique) jusqu'à ce que iBGP soit établi. Ensuite, les métriques distribuées par IS-IS reviennent à la normale et le routeur va forwarder le trafic de transit comme d'habitude.

Ping Test #2. Utilisez Ping vers toutes les loopback du laboratoire. Ceci permet de vérifier qu' IS-IS est configuré correctement. En cas de problèmes, utilisez les commandes suivantes afin de déterminer les problèmes :

`show ipv6 route`	: vérifier s'il y a une route vers une destination
`show clns neighbor`	: vérifier la liste des voisins CLNS-IS que le routeur voit
`show clns interface`	: vérifier si IS-IS est configuré et le type IS
`show isis database`	: voir la link state database IS-IS apprise par le router
`show isis ipv6 rib`	: voir les routes IPv6 IS-IS routes apprises par le routeur
`show isis topology`	: voir la topologie IS-IS apprise par le router

Checkpoint #2: *Demandez à l'instructeur de vérifier la connectivité. Enregistrez la configuration telle qu'elle est sur le routeur. Vous aurez besoin de cette configuration à plusieurs reprises tout au long de l'atelier.*

14. **Traceroute vers tous les routers.** Après les pings vers tous les routeurs, essayez traceroute vers tous les routeurs. Utilisez la commande *trace x.x.x.x*. Par exemple, l'équipe Router1 lance:

```
Router1# trace 2001:db8::c
```

pour tracer le chemin vers Router R12. Si la commande expire parce que certaines destinations sont injoignables, il est possible d'interrompre le *traceroute* a l'aide de la combinaison de touches CTRL-^. Ceci est appelé cisco break séquence.

Q. Pourquoi certains résultats montrent plusieurs adresses IP à un nombre de sauts fixé ?

A. S'il y a plusieurs chemins de coût égal, le routeur repartira le trafic le long de ces chemins. C'est le "load sharing".

```
Router1>trace 2001:db8::c

Type escape sequence to abort.
Tracing the route to 2001:db8::c

  1 2001:db8:0:3::1    4 msec
    2001:db8:0:2::1    0 msec
    2001:db8:0:3::1    0 msec
  2 2001:db8:0:f::1    4 msec
    2001:db8:0:8::1    4 msec
    2001:db8:0:f::1    0 msec
  3 2001:db8:0:13::    4 msec *  4 msec
Router1>
```

15. **Autres caractéristiques IS-IS.** Consultez la documentation ou l'aide en ligne de commande en tapant *?* pour découvrir d'autres commandes *show* et autres fonctions de configuration ISIS.

Questions de révision

1. Quelle commande show d'IOS affiche la table IPv6 de forwarding d'un routeur ?

2. Quelle commande show d'IOS affiche la base de données IPv6 d'ISIS ?