Module 1b – Topologie de base et IS-IS

Objectif: Créer une interconnexion physique pour la laboratoire de base. Ce réseau comporte un niveau IS-IS. Assurez-vous que tous les routeurs, les interfaces, les câbles et les connexions fonctionnent correctement.

Pré-requis: Connaissance de routeur Cisco CLI, expérience pratique antérieure.

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

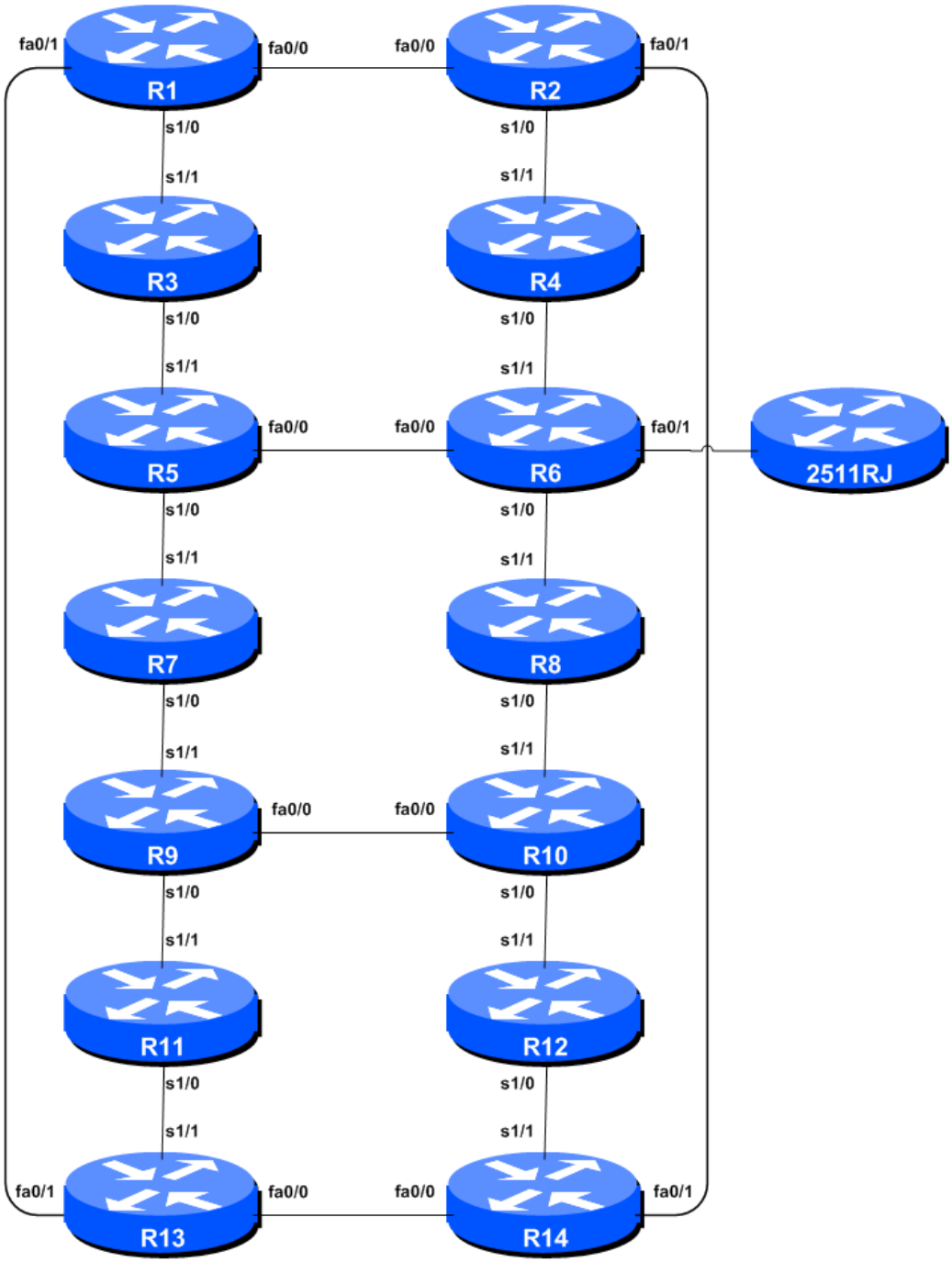

Figure 1 – ISP Lab Basic Configuration

Remarques

Cet atelier est destiné à être exécuté sur un serveur Dynamips avec les topologies appropriées. Les routeurs dans l'environnement Dynamips utilisent une version d'IOS pour fournisseur de services. Les configurations et les principes de configuration décrites ci-dessous fonctionneront sur tous les Cisco IOS Release 12.4 et plus récents. Les versions antérieures Cisco IOS ne sont pas supportée mais fonctionnent principalement pour les exercices ci-dessous. Il est possible que certaines fonctionnalités ne soient pas couvertes.

Le but de ce module est de construire le réseau de laboratoire et d'introduire les principes de base de la construction et de la configuration d'un réseau. Un point important à retenir, et celui qui sera souligné à maintes reprises tout au long de cet atelier, c'est qu'il y a une séquence précise à la construction d'un réseau opérationnel:

- Après la **conception du réseau,** les liens physiques entre le matériel doivent être construits et vérifiés.

- Ensuite, les routeurs sont initialisés avec une **configuration de base**, et une sécurité élémentaire mais suffisante doit être mise en place.

- Ensuite la connectivité IP de base est testée et éprouvée. Cela consiste à attribuer des adresses IP sur tous les liens utilisés, et à tester les liens vers les dispositifs voisins.

- Nous pouvons commencer la configuration des protocoles de routage uniquement après qu'un routeur voit ses voisins. Il s'agit de **commencer par l'IGP** (ISIS est choisi pour cet atelier). La construction de BGP ne sert à rien si l'IGP choisi (dans ce cas, ISIS) ne fonctionne pas correctement. BGP s'appuie sur le protocole ISIS pour trouver ses voisins et next hops, et un ISIS mal-configure ou ne fonctionnant pas correctement se traduira par beaucoup de temps perdu à essayer de déboguer les problèmes de routage.

- Une fois que l'IGP fonctionne correctement, la configuration BGP peut commencer, d'abord BGP a l'interieur de l'AS (iBGP), puis les sessions BGP externes (eBGP).

- **N'oubliez pas de lire le manuel (RTFM, en Anglais).** Il est essentiel que les ingénieurs réseaux utilisent pleinement toutes les sources d'information. La source n ° 1 est la documentation. ***Lire F#$% Manual (RTFM)*** est la phase traditionnelle utilisée pour informer les ingénieurs que la réponse est dans la documentation et qu'il faut aller la lire. Il en est de même avec ces instructions ! Si vous les suivez, vous n'aurez pas de surprises durant les laboratoires.

- Enfin, **documentation**. La documentation est souvent négligée ou oubliée. C'est un processus continu dans cet atelier. Si l'instructeur vous demande de documenter quelque chose, que ce soit sur le tableau blanc dans la classe, ou à la fin de cette brochure, il est dans votre intérêt de le faire. Il ne peut jamais y avoir trop de documentation. Elaborer la documentation au moment de la conception du réseau peut faire épargner beaucoup de frustrations dans le futur.

Configuration du labo

1. **Les routeurs et les participants de l'atelier.** Cet atelier est aménagé de telle sorte qu'un groupe de deux élèves puissent opérer un seul routeur. 14 routeurs impliquent généralement au moins 28 participants. Pour les ateliers avec un plus grand nombre de participants, ils doivent configurer un routeur unique, par groupes de trois. Les instructeurs de l'atelier vont diviser les routeurs parmi les participants de l'atelier. Dans les notes suivantes, une «équipe routeur» désigne le groupe assigné à un routeur particulier.

2. **Router Hostname.** Chaque routeur sera nommé en fonction de l'emplacement des tables, Router1, Router2, Router3, etc. La documentation des ateliers fait référence à *Router1* en tant que R1. Au prompt du routeur, tout d'abord passez en mode enable, puis entrez "config terminal", ou simplement "config":

```
Router> enable
Router# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname Router1
Router1(config)#
```

3. **Désactiver la recherche de noms de domaine.** Les Routeurs Cisco tentent toujours une recherche DNS pour les noms ou adresses spécifiées en ligne de commande. Vous pouvez voir cela lorsque vous faites une *trace* sur un routeur sans serveur DNS ou un serveur DNS avec aucune entrée in-addr.arpa pour les adresses IP. Nous allons désactiver pour le moment ce lookup pour le labo afin d'accélérer les traceroutes.

```
Router1 (config)# no ip domain-lookup
```

4. **Désactiver la résolution de noms en ligne de commande (Command-line Name Resolution).** Le routeur tente par défaut d'utiliser les différents transports qu'il supporte afin résoudre les commandes dans la ligne de commande (lors des modes normaux et de configuration). Si les commandes saisies ne font pas partie de Cisco IOS, le routeur tentera d'utiliser ses autres transports supportés pour interpréter la signification de ce nom. Par exemple, si la commande saisie est une adresse IP, le routeur tentera automatiquement de se connecter à cette destination distante. Cette fonctionnalité n'est pas souhaitable sur un routeur d'ISP, car cela signifie que des erreurs typographiques peuvent entraîner des connexions à des systèmes distants ainsi que l'expiration de timers pendant que le routeur tente d'utiliser le DNS pour traduire le nom.

```
Router1 (config)# line con 0
Router1 (config-line)# transport preferred none
Router1 (config-line)# line vty 0 4
Router1 (config-line)# transport preferred none
```

5. **Désactiver le « 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 ip source-route
```

6. **Noms d'utilisatuers et mots de passe.** Tous les noms d'utilisateur du routeur doivent être ***isplab*** et tous les mots de passe doivent être **lab-PW**. Veillez à ne pas changer le nom d'utilisateur ou mot de passe, ne laissez pas le mot de passe non configuré (l'accès aux ports vty n'est pas possible si aucun mot de passe n'est activé). Il est essentiel pour le fonctionnement en douceur d'un laboratoire que tous les participants aient accès à tous les routeurs.

```
Router1 (config)# username isplab secret lab-PW
Router1 (config)# enable secret lab-PW
Router1 (config)# service password-encryption
```

   La directive *service password-encryption* indique au routeur de crypter les mots de passe stockés dans la configuration du routeur (en dehors de *enable secret* qui est déjà encrypté).

   Remarque A: La tentation est grande d'avoir simplement un nom d'utilisateur *cisco* et mot de passe *cisco* comme une solution au problème nom d'utilisateur / mot de passe. En aucun cas un opérateur d'un fournisseur de services ne doit utiliser de tels mots de passe faciles à deviner sur leur réseau en ligne opérationnel[1].

   Remarque B: La paire nom d'utilisateur / secret n'est pas disponible sur les versions d'IOS antérieures à 12.3. Dans ce cas, les opérateurs devront configurer le nom d'utilisateur / mot de passe. Ce dernier format utilise le cryptage de type 7, alors que le premier est un cryptage basé sur md5 un peu mieux sécurisé. IOS 15.1 et les versions ultérieures utilisent SHA256 pour remplacer MD5.

7. **Activation de l'accès pour les autres équipes.** Afin de permettre à d'autres équipes un accès telnet sur le routeur, vous devez configurer un mot de passe pour toutes les lignes de terminal virtuel. Cet accès sera nécessaire lors de futurs modules de cet atelier.

```
Router1 (config)# aaa new-model
Router1 (config)# aaa authentication login default local
Router1 (config)# aaa authentication enable default enable
```

   Cette série de commandes indique au routeur de regarder localement pour la connexion utilisateur standard (le paire nom d'utilisateur /mot de passe configuré précédemment), et au niveau local le secret configure pour le login *enable*. Par défaut, le login sera activé sur tous les vtys pour que d'autres équipes y accèdent.

8. **Configurer system logging.** Une partie essentielle de tout système connecte a Internet est d'enregistrer les logs. Le routeur affiche par défaut les logs système sur la console du routeur. Toutefois, cela n'est pas souhaitable pour les routeurs en opération. La console est une connexion 9600 bauds. Elle peut créer une charge processeur élevée à cause des nombreuses interruptions lors de trafic intense sur le réseau. Cependant, les logs du routeur peuvent également être enregistrés dans une mémoire tampon sur le routeur – cela ne génère pas *d'interrupt load* et permet également à l'opérateur de vérifier l'historique de ce qui s'est passé sur le routeur. Dans un module futur, nous configurerons les routeurs pour envoyer les messages log vers un serveur SYSLOG.

```
Router1 (config)# no logging console
Router1 (config)# logging buffer 8192 debug
```

[1] Ceci est très important. Il arrive fréquemment que des attaquants accèdent aux ressources d'un réseau simplement parce que les mots de passe utilisés sont trop faciles à deviner.

qui désactive les console logs et enregistre à la place tous les logs dans un tampon de 8192 Bytes sur le routeur. Pour voir le contenu de ce tampon logging interne la commande "sh log" peut être utilisée, à tout moment, en la ligne de commande.

9. **Sauver la configuration.** Les routeurs sont munis d'une configuration de base. Sauvegardez la configuration. Pour faire ça, sortez du mode enable en tapant «end» ou «<ctrl> Z", et sur la ligne de commande, entrez "write memory".

```
Router1(config)#^Z
Router1# write memory
Building configuration...
[OK]
Router1#
```

Il est fortement recommandé de sauvegarder fréquemment la configuration dans la NVRAM, en particulier dans l'environnement atelier où il est possible que l'on doive redémarrer l'environnement virtuel et les routeurs. Si la configuration n'est pas enregistrée dans la NVRAM, toutes les modifications apportées à la configuration courante seront perdues après un reboot.

Déconnectez-vous du routeur en tapant exit, puis connectez-vous à nouveau. Remarquez comme la séquence de login a changé, demandant à l'utilisateur d'entrer un «nom d'utilisateur» et «mot de passe». Remarquez qu'à chaque point de contrôle dans l'atelier, vous devez sauvegarder la configuration dans la mémoire - se rappeler que l'interruption d'alimentation du routeur se traduira par revenir à la dernière configuration enregistrée dans la mémoire NVRAM.

10. **Adresses IP.** Ce module présente les concepts de base afin d'établir un plan d'adressage pour le backbone d'un ISP. Nous mettons en place un système autonome comprenant les 14 routeurs que nous avons dans le laboratoire. Les RIR distribuent généralement un ensemble d'adresses IPv4 en prefixes de longueur 20 (/20) en fonction de la région du RIR - on suppose pour les besoins de ce labo que notre ISP a reçu un /20. Plutôt que d'utiliser l'espace d'adressage public, nous allons utiliser une partie du 10/8 (RFC1918 ou espace d'adressage privé) pour ce labo. Dans le monde réel de l'Internet, nous pouvons utiliser l'espace d'adressage public pour notre infrastructure réseau.

La manière type dont les ISP divisent leur espace d'adressage alloué est de le découper en trois morceaux. Une partie est utilisée pour des allocations aux clients, la deuxième partie est utilisée pour les liens de notre infrastructure point-à-point, et le dernier morceau est utilisé pour les adresses des interfaces loopback pour l'ensemble des routeurs de backbone. Le schéma de la figure 2 illustre ce qui se fait habituellement.

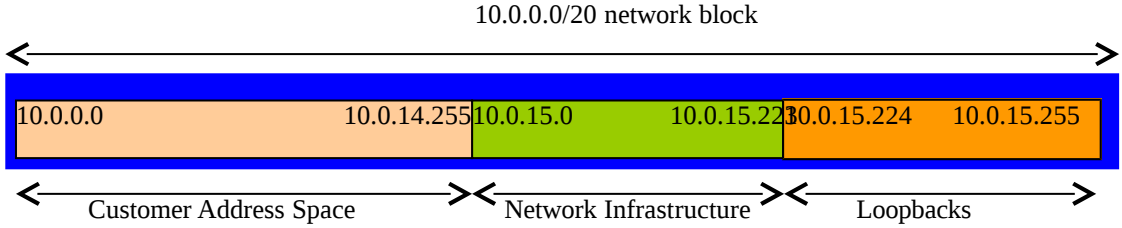

Figure 2 – Division du bloc /20 alloué en une partie pour les clients, l'infrastructure et les loopbacks

Étudiez le plan d'adressage distribué en annexe au présent document. Remarquez comment l'adressage d'infrastructure commence à 10.0.15.0 et porte sur un maximum de 10.0.15.70 - ce qui

nous laisse de l'espace pour agrandir le réseau avec plus de liens point à point, jusqu'à 10.0.15.223. Remarquez que nous avons mis un côté un seul / 27 pour les loopbacks ds routerus - mais nous avons seulement utilisé les 14 adresses à partir de 241 jusqu'à 254 pour notre réseau, ce qui laisse une certaine réserve pour la croissance future (non pas que nous avons une croissance future prévue pour l'atelier). Cette méthode est tout à fait réaliste pour le backbone d'un ISP. En effet, les ISP ont tendance à documenter leurs plans d'adressage dans des fichiers texte ou dans des feuilles de calcul (spreadsheets) - Figure 3 ci-dessous montre un extrait d'exemple type (se basant sur le schéma d'adressage présenté ici).

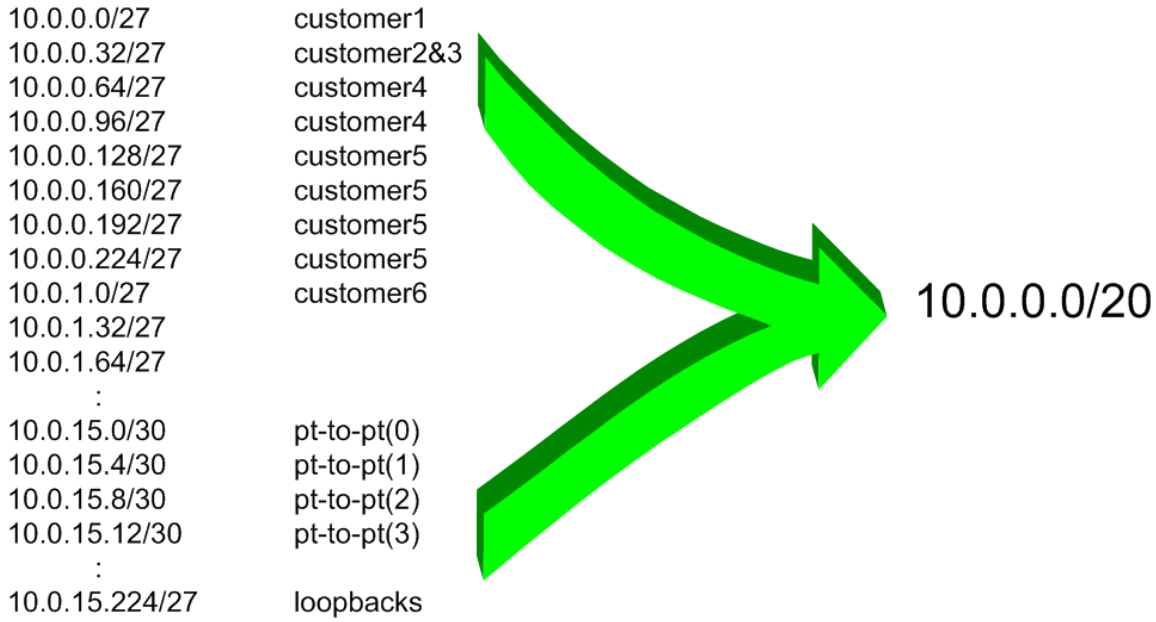

Figure 3 – Extrait d'un plan d'adressage d'ISP

11. **Connexions en série Back-to-Back.** Connecter les connexions en série comme dans la figure 1. Le côté DCE d'une connexion en série Back-to-Back est configuré avec la commande clock rate qui anime le circuit en série. (Les anciennes versions de l'IOS utilisaient la commande ***clock rate***, maintenant cachée mais toujours fonctionnelle.) Vérifier le câble physiquement pour voir de quel côté est DCE et lequel est DTE. Sur certains routeurs, la commande ***show controller <interface>*** montre l'état DCE / DTE. Par exemple, sur un routeur Cisco 3620, ***show controllers serial 0/0*** va produire un résultat qui affichera si le câble connecté au port en série 0/0 est DTE ou DCE.

    Une fois que les câbles DTE et DCE ont été déterminées et la commande ***clock rate*** a été appliquée, configurer l'adresse IP (selon le plan d'adressage discuté plus tôt) et d'autres commandes BCP (Best Common Practise) recommandées pour chaque Interface de l'ISP:

```
Router2(config)# interface serial 1/0
Router2(config-if)# ip address 10.0.15.17 255.255.255.252
Router2(config-if)# description 2 Mbps Link to Router4 via DTE/DCE Serial
Router2(config-if)# clock rate 2000000
Router2(config-if)# no ip redirects
Router2(config-if)# no ip directed-broadcast
Router2(config-if)# no ip proxy-arp
Router2(config-if)# no shutdown
```

    REMARQUE: Les instructeurs ont dessiné une grande carte réseau sur le tableau blanc dans la classe. Lorsque les adresses IP sont attribuées, prière de les annoter et d'informer l'instructeur. Tous

les liens point à point **DOIVENT être annotés** là pour que les équipes d'autres routeurs puissent documenter et comprendre les liens et le routage lors des modules à venir.

Q: Quel masque de réseau doit être utilisé sur le lien point-à-point?

A: Sur les interfaces en série, le masque de réseau devrait être / 30 (ou 255.255.255.252 en format dotted quad). Il est inutile d'utiliser une autre taille de masque car il y a seulement deux hôtes sur un tel lien. Un masque 255.255.255.252 signifie 4 adresses hôte disponibles, dont deux sont utilisables (les deux autres représentant les adresses réseau et broadcast).

12. **Connexions Ethernet.** Les liens Ethernet entre les routeurs seront effectués en utilisant des câbles RJ-45 *cross-over* -. Ceux-ci relieront directement les ports Ethernet sur les deux routeurs sans le besoin d'un switch Ethernet. Les subnets IP seront de nouveau tiré du plan d'adressage. Ne faites pas l'erreur d'attribuer un masque / 24 à l'adresse de l'interface - il y a seulement deux hôtes sur le réseau Ethernet reliant les deux routeurs, donc un masque / 30 est tout à fait suffisant.

13. **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 arp                                : Affiche le contenu de la cache ARP
show interface <interface> <number> : Configuration et état d'une interface
show ip interface                       : Résumé de l'état des interfaces IP et leur configuration
```

14. **Création des Interfaces Loopback.** Les Interfaces loopback seront utilisée à des fins multiples dans cet atelier. Celles-ci comprennent la génération de routes annoncées et la configuration des sessions de peering BGP. Comme indiqué précédemment dans l'étape 10, nous allons utiliser une partie du bloc d'adresses IP allouées pour les interfaces de loopback. La plupart des ISP a tendance à mettre de côté un bloc contigu d'adresses pour les loopbacks de leurs routeurs. Par exemple, si un ISP a 20 routeurs, il a besoin d'un / 27 (ou 32 adresses hôtes) afin de fournir une adresse loopback pour chaque routeur. Nous avons 14 routeurs dans notre laboratoire – pour faire preuve de prudence et permettre la croissance, nous allons mettre de côté un / 27 (nous permettant 32 loopbacks) mais en utiliser seulement 14 d'entre elles. Les adresses loopbacks assignées sont les suivantes:

R1	**10.0.15.241/32**	**R8**	**10.0.15.248/32**
R2	**10.0.15.242/32**	**R9**	**10.0.15.249/32**
R3	**10.0.15.243/32**	**R10**	**10.0.15.250/32**
R4	**10.0.15.244/32**	**R11**	**10.0.15.251/32**
R5	**10.0.15.245/32**	**R12**	**10.0.15.252/32**
R6	**10.0.15.246/32**	**R13**	**10.0.15.253/32**
R7	**10.0.15.247/32**	**R14**	**10.0.15.254/32**

Par exemple, l’équipe routeur 1 attribuera l’adresse et le masque suivant pour la loopback sur le routeur 1:

```
Router1(config)#interface loopback 0
Router1(config-if)#ip address 10.0.15.241 255.255.255.255
```

Q: Pourquoi utilisons-nous un masque / 32 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 / 32 - 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.*

15. **IS-IS avec une area et un niveau (level-2) dans un seul AS.** Chaque équipe routeur doit activer le protocole IS-IS sur son router et utiliser *workshop* comme identifiant IS-IS (IS-IS ID) lors de la configuration. Dans ce module, nous utilisons une area de niveau 2 (*49.0001*). Nous verrons au point suivant comment configurer *wide metric* (Le default IOS default est *narrow metric*, ce default n'est cependant pas considéré comme une bonne pratique). L'identifiant NET est configuré à *49.0001.x.x.x.x.00*, où *x.x.x.x* est la loopback du routeur. Par exemple, la loopback de Router1 est 10.0.15.241. Ceci conduit à une adresse NSAP égale a *49.0001.0100.0001.5241.00*.

```
Router1(config)# router isis workshop
Router1(config-router)#net 49.0001.0100.0001.5241.00
Router1(config-router)#is-type level-2-only
```

Q: Pourquoi configurer *`is-type level-2-only`* ? Répondez ci-dessous :

Astuce: Afin de convertir la loopback en une adresse NSAP, préfixez l'adresse loopback du nombre de zéros manquants. Par exemple, L'adresse loopback de Router 5 est 10.0.15.245; avec les zéros manquants cela donne 010.000.015.245. Ensuite, au lieu de mettre un point tous les 3 caractères, mettez un point tous les 4 caractères. 010.000.015.245 devient 0100.0001.5245.

16. **Configuration de Wide Metrics.** Nous allons maintenant configurer « metric-style » à *wide metric*. IS-IS supporte deux types de métriques appelées *narrow* (déprécié et inapproprié aux reseaux modernes) et *wide*. La valeur pare defaut pour IOS est mises à *narrow* metrics. Nous devons donc explicitement changer le type de metrique pour avoir des *wide metrics*. Nous faisons ceci pour le niveau 2:

```
Router1(config)# router isis workshop
Router1(config-router)#metric-style wide level-2
```

17. **Activation du protocole ISIS sur chaque interface.** Maintenant que le processus IS-IS est configuré, chaque équipe active IS-IS sur les interfaces point-à-point et ethernet. Sans cela, le routeur ne recevra pas annonces des réseaux à deux sauts ou plus du routeur. Voici un exemple de configuration pour Router1 :

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

```
Router1(config-if)# ip router isis workshop
```

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

18. **Type de circuit IS-IS et métriques IS-IS.** Chaque équipe configure maintenant le type de circuit et la métrique IS-IS pour chaque interface physique.

    Le type par défaut d'un circuit est level-1-2 même si le router a été défini comme étant un routeur level-2-only.

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

19. **Annonce des Loopback /32.** Il n'est pas nécessaire de configurer une adjacence IS-IS sur l'interface loopback, cette interface étant toujours joignable. Nous la marquons comme passive:

```
Router1(config)# router isis workshop
Router1(config-router)# passive-interface Loopback0
```

    Cette commande indique à IS-IS qu'il faut installer l'adresse de la loopback dans la RIB. Il n'est pas nécessaire d'ajouter la commande `ip router isis` dans la configuration de l'interface loopback. Ceci est diffèrent de ce qui est requis pour configurer OSPF et est souvent source d'erreurs, surtout de la part d'ingénieurs familiers avec OSPF qui débutent en IS-IS.

20. **Adjacences IS-IS.** 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.

    (**Note:** Les versions d'IOS 12.4 et superieures ont *log-adjacency-changes* activé par default lorsque IS-IS est activé.)

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

21. **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)#set-overload-bit on-startup wait-for-bgp
```

Ceci met en place IS-IS tel que les routes 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 ip 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 rib`	: voir les routes 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.*

22. 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 10.0.15.252
```

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 R **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 router12

Type escape sequence to abort.
Tracing the route to router12.workshop.net (10.0.15.224)

  1 fe0-0.router2.workshop.net (10.0.15.2) 4 msec
    fe0-1.router13.workshop.net (10.0.15.6) 0 msec
    fe0-0.router2.workshop.net (10.0.15.2) 0 msec
  2 fe0-0.router14.workshop.net (10.0.15.54) 4 msec
    fe0-1.router14.workshop.net (10.0.15.26) 4 msec
```

```
    fe0-0.router14.workshop.net (10.0.15.54) 0 msec
  3 ser0-0.router12.workshop.net (10.0.15.69) 4 msec *  4 msec
Router1>
```

23. **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.

24. **Configuration avancée.** Les équipes routeurs qui ont terminé ce module peuvent se référer au module 11 de l'atelier avancé BGP. Les instructions ont été étendues pour inclure toutes les exigences de base d'un routeur utilisé dans un backbone d'ISP. En attendant la conclusion du module courant, il vous est suggéré de lire ce module avancé et d'ajouter les éléments de configurations recommandés.

Questions de révision

1. Quel est le protocole IP utilisé par Ping et Traceroute?

2. Effectuez un Ping vers l'adresse IP du routeur de votre voisin (par exemple 10.0.15.2). Regardez le temps qu'il a fallu pour que le ping se termine. Maintenant, effectuez un ping vers l'adresse IP de votre routeur sur le même segment (par exemple 10.0.15.1). Regardez le temps qu'il a fallu pour compléter la tâche ping. Quels sont les résultats? Pourquoi y at-il une différence?

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

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