Module 1a – Topologie de base et OSPF

Objectif: Créer une interconnexion physique de base avec une zone OSPF. S'assurez 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 couramment utilisée pour la première série de séance de labo.

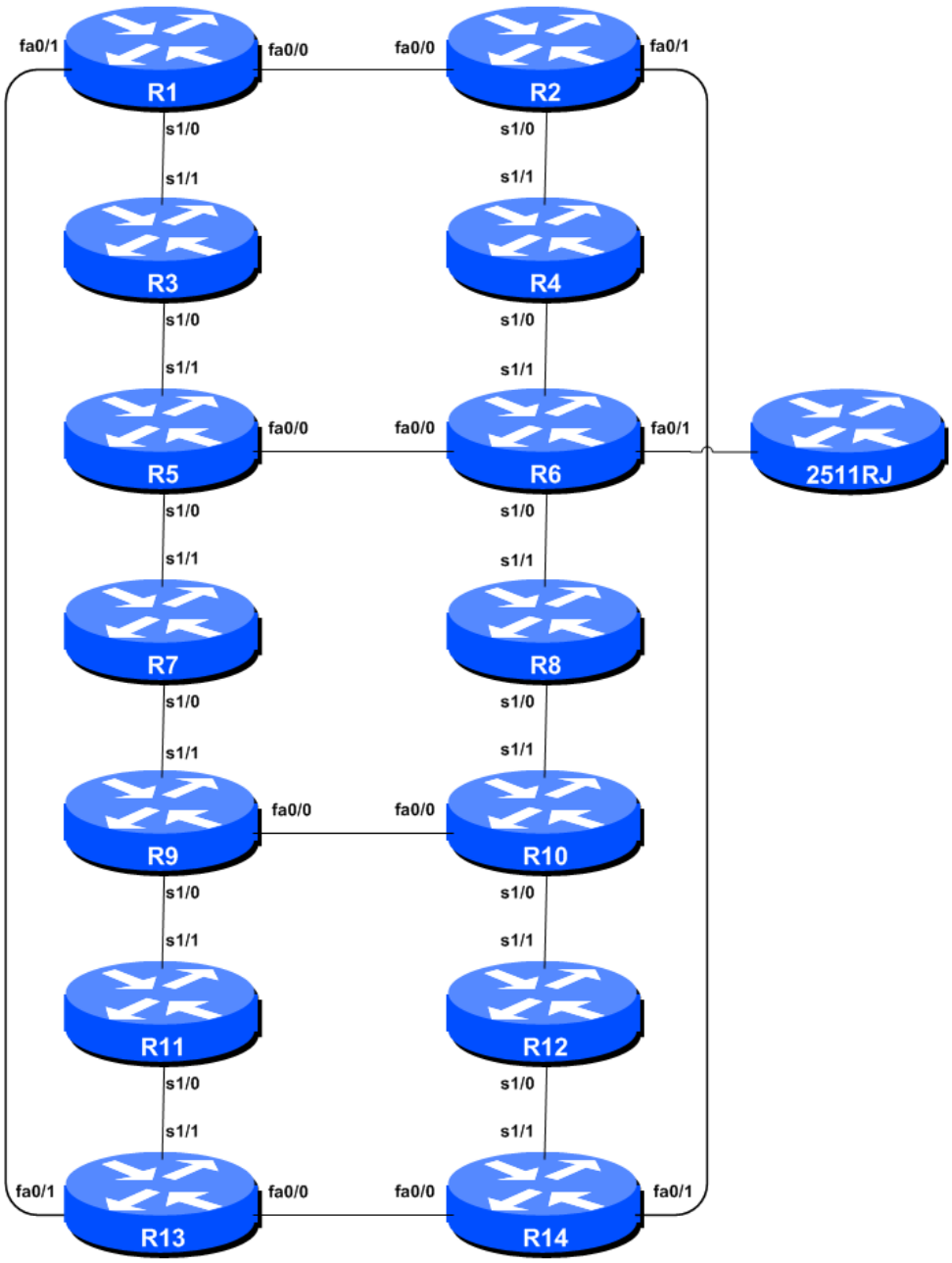

Figure 1 – Configuration de base Labo ISP

Remarques de Labo

Cet atelier est destiné à être exécuté sur un serveur Dynamips avec les topologies labo appropriées mises en place. Les routeurs dans l'environnement Dynamips utilisent un IOS "Service provider". Les configurations et les principes de configurations décrits ci-dessous fonctionneront sur les versions Cisco IOS 12.4 et les plus récentes. Les versions antérieures Cisco IOS ne sont pas supportées mais fonctionnent principalement avec les notes ci-dessous, mais vont manquer quelques-unes des fonctionnalités couvertes.

Le but de ce module est de construire l'atelier de laboratoire et de présenter 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 distincte à la construction d'un réseau opérationnel:

- Après que la conception **physique établie, les liens entre le matériel devraient être raccordés et vérifiés.**

- Ensuite, les routeurs devraient avoir la configuration de base **installée, et une sécurité élémentaire et suffisante doit être mis en place.**

- Ensuite la connectivité IP de base doit être testées et éprouvées. Ça consiste à attribuer des adresses IP sur tous les liens qui doivent être utilisés, et à tester les liens pour les dispositifs voisins.

- Une fois qu'un routeur peut voir son voisin il est logique de commencer la configuration des protocoles de routage. Et **commencer par** IGP (OSPF est choisi pour cet atelier). La construction de BGP ne sert à rien si l'IGP choisi (dans ce cas, OSPF) ne fonctionne pas correctement. BGP s'appuie sur le protocole OSPF pour trouver ses voisins et next hops, et un OSPF mal ou non-configuré 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 être commencée, d'abord BGP interne, puis BGP externe.

- **N'oubliez pas d'effectuer RTFM.** Qu'est ce que RTFM? Il est essentiel que les ingénieurs réseau ISP utilisent pleinement toutes les ressources 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.

- Enfin, **documentatez, prenez des notes**. 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, ou à la fin de cette brochure, il est dans votre intérêt de le faire. Il ne peut jamais y avoir trop de documentation, et au moment de la conception du réseau et de la construction, la documentation peut faire épargner beaucoup de frustration dans le futur.

Exercice en 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 partager les routeurs parmi les participants de l'atelier. Dans les notes suivantes, une «équipe routeur» désigne le groupe assigné à un routeur particulier.

2. **Routeur Hostname.** Chaque routeur sera nommé en fonction de l'emplacement des tables, Router1, Router2, Router3, etc Documentation et labo font également référence à *Router1* comme R1. Au prompt du routeur, tout d'abord passer en mode enable, puis entrez "config terminal", ou simplement "config":

```
Routeur> enable
Router# config terminal
Entrez les commandes de configuration, une par ligne.  Terminez avec CNTL/Z.
Router(config)# hostname Router1
Router1(config)#
```

3. **Désactiver la recherche de noms de domaine.** Les Routeurs Cisco tenterons toujours de rechercher le DNS pour un nom ou une adresse spécifiée dans la 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 par défaut tente d'utiliser les différents transports qu'il supporte pour résoudre les commandes dans la ligne de commande lors de 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'un ISP, car cela signifie que des erreurs typographiques peuvent entraîner des connexions étant tenté à des systèmes distants, ou les temps morts pendant que le routeur tente d'utiliser le DNS pour traduire le nom, et ainsi de suite..

```
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 routage source.** Sauf si vous croyez vraiment qu'il est nécessaire de l'activer, le routage source doit être désactivée. Cette option, activée par défaut, permet au routeur de traiter les paquets avec la source options header de routage. 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 de différents endroits sur Internet, mais ces dernières années il a été largement abusé des activités mécréant sur l'Internet).

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

6. **Les noms d'utilisateurs et mots de passe.** Tous les noms d'utilisateur du routeur doivent être ***isplab*** et tous les mots de passe doivent être lab-PW. S'il vous plaît, ne pas changer le nom d'utilisateur ou mot de passe, ou laisser le mot de passe non configuré (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 ont accès à tous les routeurs.

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

   Le 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: Il peut etre tentant 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 fournisseur de services ne doit jamais utiliser des mots de passe faciles à deviner sur leur réseau en ligne [1]opérationnel.

   Remarque B: pour IOS antérieures à la version 12.3, la paire nom d'utilisateur / secret n'est pas disponible, et 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 version ultérieure utilisent SHA256 pour remplacer MD5.

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

   ```
   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 configuré enable secret pour le enable login. 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 d'exploitation 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 Internet opérationnelles, comme la console est une connexion 9600 bauds, et peut placer une charge processeur élevée d'interruption au moment de trafic intense sur le réseau. Cependant, les logs du routeur peuvent également être enregistrées dans une mémoire tampon sur le routeur - ne prend 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, le laboratoire consistera à configurer le routeur pour envoyer les messages log vers un serveur SYSLOG.

[1] Cette phrase doit être soulignée. Les cyber-attaquants peuvent fréquemment avoir accès à des réseaux tout simplement parce que les opérateurs ont utilisé des mots de passe familiers ou faciles à deviner.

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

qui désactive les console logs et enregistre à la place tous les logs dans un tampon 8192 Byte mis de côté sur le routeur. Pour voir le contenu de ce tampon logging interne, à tout moment, la commande "`sh log`" doit être utilisé sur la ligne de commande.

9. **Sauvegarder la** configuration. Grâce à la configuration de base en place, sauvegardez la configuration. Pour faire ça, sortir du mode enable en tapant «end» ou « <ctrl> Z », et sur la ligne de commande, entrez “write memory”.

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

Il est fortement recommandé que la configuration soit sauvegardée dans NVRAM assez fréquemment, en particulier dans l'environnement atelier où il est possible pour les câbles d'alimentation de se détacher. Si la configuration n'est pas enregistrée dans NVRAM, toutes les modifications apportées à la configuration courante seront perdues après un cycle d'alimentation.

Déconnectez-vous au routeur en tapant exit, puis connectez-vous à nouveau. Remarquez comment la séquence de login a changé, demandant l'utilisateur à entrer un «nom d'utilisateur» et «mot de passe». Remarquez qu'à chaque point de contrôle dans l'atelier, vous devez sauvegarder la configuration de 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 pour mettre sur pied un plan d’adressage pour un backbone ISP. Nous mettons en place un système autonome sur les 14 routeurs que nous avons dans le laboratoire. Les RIR distribuent généralement de l’espace adresses IPv4 en morceaux / 20 (dépend de la région 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 typique dont les ISP divisent leur espace d'adressage alloué est de le découper en trois morceaux. Une pièce est utilisée pour des assignations à la clientèle, la deuxième pièce est utilisée pour les liens infrastructure point-à-point, et le dernier morceau est utilisé pour les adresses d'interface loopback pour l'ensemble de leurs routeurs backbone. Le schéma de la Figure 2 2 montre ce qui se fait habituellement.

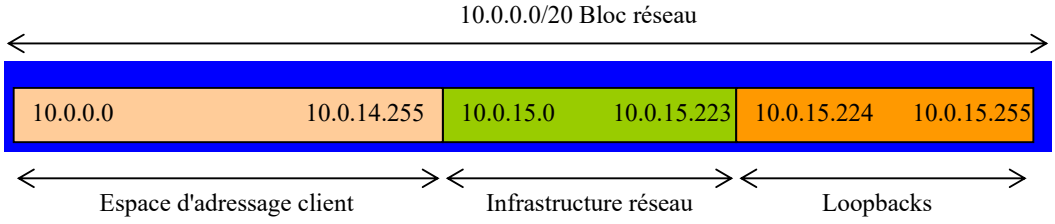

Figure 2 2 - division du bloc alloué de / 20 entre la clientèle, l'Infrastructure et les Loopbacks

Étudier le plan d'adressage qui a été distribué comme un additif au présent module d'atelier. Remarquez comment l'adressage d'infrastructure commence à 10.0.15.0 et porte sur un maximum de 10.0.15.70 - ce nous laisser de l'espace pour agrandir le réseau avec plus de liens point à point, jusqu'à 10.0.15.223. Remarquez comment nous avons mis de côté un seul / 27 pour les loopback des routeurs - 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), une proposition tout à fait réaliste pour un backbone 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 3 ci-dessous montre un extrait d'un exemple typique (à l'aide de notre schéma d'adressage ici).

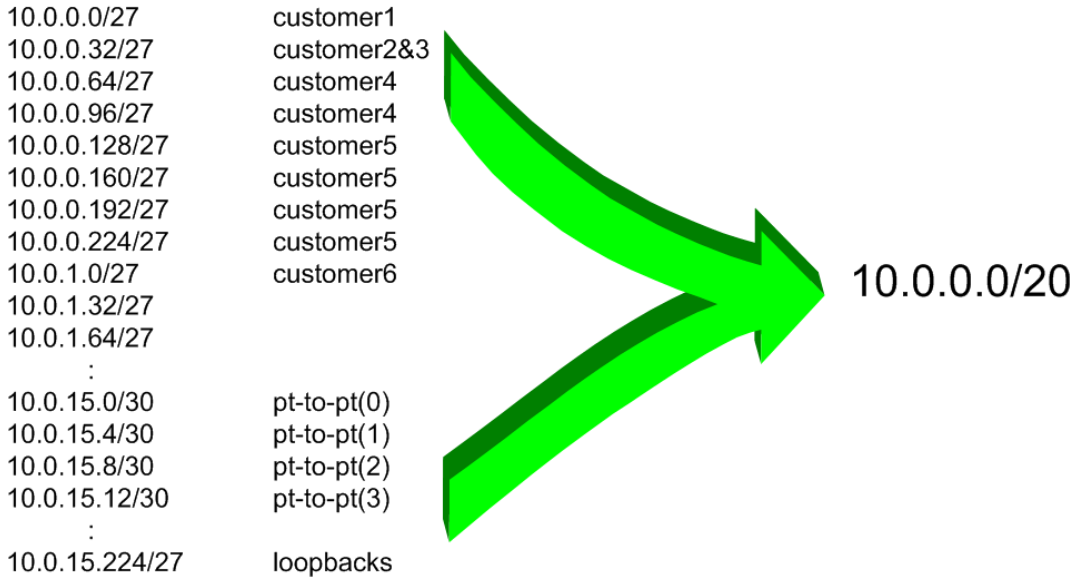

Figure 3 3 - Extrait d'un plan d'adressage ISP

11. **Connexions en série Back-to-Back.** Connecter les connexions en série comme dans la figure 1 Figure 1. TLe 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 clockrate***, maintenant caché mais toujours fonctionnel.) Vérifier le câble physiquement pour voir de quel côté est DCE et lequel est DTE. Sur certains routeurs, la commande ***show controller <interface>*** montrera 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 recommandées qui sont recommandés pour chaque Interface de l'ISP:

```
Router2(config)# interface serial 1/0
Router2(config-if)# ip address 100.1.17.1 255.255.255.252
Router2(config-if)# description 2 Mbps Link to Router4 via DTE/DCE Serial
Router2(config-if)# bandwidth 2000
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 de laboratoire auront dessiné une grande carte réseau sur le tableau blanc dans le laboratoire de l'atelier. Lorsque les adresses IP sont attribuées, prière de les annoter et d'informer l'instructeur. Tous les liens point à point **DOIVENT être annotées** là pour que les équipes d'autres routeurs peuvent documenter et comprendre les liens et routage dans les modules actuelles et futures.

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. Une adresse 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 doit être tout à fait suffisant.

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

```
show arp                                : Indique le protocole de résolution d'adresse
show interface <interface> <number> : État de l'interface et la configuration
show ip interface                       : Résumé bref de l'état des interfaces IP et la configuration
```

14. **Creation des Loopback Interfaces.** Les Interfaces Loopback seront utilisé dans cet atelier pour beaucoup de choses. Ceux-ci comprennent la production de route (à être annoncé) et la configuration des peerings 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 ont tendance à mettre de côté un bloc contigu d'adresses pour l'utilisation par leurs routeur loopbacks. Par exemple, si un ISP a eu 20 routeurs, ils auraient besoin d'un / 27 (ou 32 adresses hôte) 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 permet 32 loopbacks) mais en utiliser seulement 14 d'entre eux. Les adresses loopbacks assignées sont les suivantes:

R1	**10.0.15.241/32**	**R4**	**10.0.15.244/32**
R2	**10.0.15.242/32**	**R5**	**10.0.15.245/32**
R3	**10.0.15.243/32**	**R6**	**10.0.15.246/32**

R7	**10.0.15.247/32**	**R11**	**10.0.15.251/32**
R8	**10.0.15.248/32**	**R12**	**10.0.15.252/32**
R9	**10.0.15.249/32**	**R13**	**10.0.15.253/32**
R10	**10.0.15.250/32**	**R14**	**10.0.15.254/32**

Par exemple, l'équipe routeur 1 attribuera l'adresse et le masque suivant au 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 des masques / 32 pour l'adresse d'interface loopback?

A: Il n'y'a pas de réseau physique attachée au 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'assistant de laboratoire pour vérifier la connectivité. Montrez que vous pouvez faire un ping et Telnet aux routeurs adjacents.*

15. **OSPF avec une zone dans le même AS - activer le processus OSPF** Chaque équipe routeur doit activer le protocole OSPF sur le routeur. L'identificateur de processus OSPF doit être *41* (voir exemple). (L'identificateur de processus OSPF est juste un nombre pour identifier ce processus OSPF sur le routeur. Il n'est pas transmis entre les routeurs.)

```
Router1(config)#router ospf 41
```

La configuration IOS par défaut doit être modifiée de sorte que toutes les interfaces soient marqués comme passif pour OSPF par défaut. Cela supprime les mises à jour de routage sur toutes les interfaces du routeur et arrête le routeur de former involontairement les contiguïtés OSPF sur les interfaces externes, et évite les problèmes potentiels que cela peut apporter[2].

```
Router1(config-router)#passive-interface default
```

Toutes les interfaces sur lesquelles les contiguïtés OSPF doivent être formés doivent être marquées avec la sous-commande *no passive-interface*.

```
Router1(config-router)#no passive-interface fastethernet 0/0
Router1(config-router)#no passive-interface fastethernet 0/1
Router1(config-router)#no passive-interface serial 1/0
```

16. **Activation du protocole OSPF sur chaque interface.** Maintenant que le processus OSPF est configuré, chaque équipe doit activer le protocole OSPF sur les interfaces du chaque routeur selon les besoins. Contrairement aux versions précédentes de l'IOS, IOS 12.4 et versions ultérieures permettent également à l'OSPF d'être exécuté sur un lien (plutôt que sur un sub-net). Plutôt que

[2] C'est une erreur courante dans de nombreuses configurations ISP d'avoir l'IGP actif sur toutes les interfaces du routeur. Il ya eu de nombreux accidents documentés où un client IGP a établi une connexion avec l'IGP du ISP, ce qui entraîne une pollution croisée des informations de routage, et le chaos de trafic qui en résulte. Le fait de désactiver cette fonctionnalité en marquant toutes les interfaces passives par défaut permet d'éviter les oublis ou les erreurs dans le futur.

d'utiliser la déclaration «network» la plus ancienne, nous activons maintenant le protocole OSPF sur chaque interface qui va former une contiguïté:

```
Router1(config)#interface serial 1/0
Router1(config-if)#ip ospf 41 area 0
!
Router1(config-if)#interface fastethernet 0/0
Router1(config-if)#ip ospf 41 area 0
!
Router1(config-if)#interface fastethernet 0/1
Router1(config-if)#ip ospf 41 area 0
```

.

17. **Annoncer la loopback en / 32.** L'interface de loopback nécessite également que OSPF lui soit activé. Même s'il n'y a pas de contiguïté qui doit être formé (parce qu'il n'y a pas de voisin physique et l'interface est marquée comme passif par défaut à l'étape précédente), nous devons déclarer OSPF sur l'interface loopback afin que l'adresse IP utilisée pour le loopback est placé dans le RIB OSPF.

```
Router1(config)#interface loopback 0
Router1(config-if)#ip ospf 41 area 0
```

18. **Contiguïtés OSPF.** Chaque équipe doit activer la logging des changements de contiguïté OSPF. (**Remarque:** A de partir IOS 12.4, *log-voisin-changes* est activé par défaut lorsque OSPF est initialement configuré). Il en est ainsi pour qu'une notification soit générée à chaque fois que l'état d'un voisins OSPF change, et est utile pour le débogage:

```
Router2(config)#router ospf 41
Router2(config-router)#log-adjacency-changes
```

19. **Éviter Blackhole de trafic au Redémarraage.** Quand un routeur redémarre après avoir été mis hors service, OSPF va commencer la distribution des préfixes dès que les adjacences sont établies avec ses voisins. Dans la prochaine partie du laboratoire de l'atelier, nous présenterons iBGP. Donc, si un routeur redémarre, OSPF va démarrer bien avant que le maillage iBGP est rétabli. Ceci entraînera l'atterrissage du routeur dans le trajet de transit pour trafic, sans que la table de routage soit complétée par BGP. Il n'y aura pas d'information de routage complète sur le routeur, de sorte que tout le trafic de transit (à partir de client-to-peer ou en amont, ou vice-versa) seront soit abandonnées, ou résultant rebondissement des paquets entre routeurs adjacents. Pour éviter ce problème, Il nécessaire que le routeur n'annonce sa disponibilité jusqu'à ce que le maillage iBGP est en marche. Pour faire ça, nous devons fournir la commande suivante:

```
Router1(config)#router ospf 41
Router1(config-router)#max-metric router-lsa on-startup wait-for-bgp
```

Ceci met en place OSPF de telles sorte que les routes passant par ce routeur sera marqué comme inaccessible (très haute métrique) jusqu'à ce que iBGP soit en marche. Une fois iBGP est en marche, les préfixes distribués par OSPF vont revenir à des valeurs métriques standard, et le routeur va passer le trafic de transit comme d'habitude.

20. **(Optionnel). Activer le nom DNS et la résolution d'adresse sur les routeurs.** Si les instructeurs de l'atelier ont mis en place le nameserver dans l'atelier, à ce stade, toutes les équipes routeur devrait maintenant permettre DNS lookups sur leurs routeurs. OSPF est porteur de tous les préfixes, y compris le réseau de connexion à Router15, autour de la salle de classe, de sorte que tous les routeurs doivent être en mesure de voir Router15.

```
Router2(config)#ip domain-lookup
Router2(config)#ip name-server 192.168.1.4
Router2(config)#ip domain-name workshop.net
```

Ces commandes défont ce qui a été configurée à l'étape 3, au début de ce module. Assurez-vous que vous pouvez effectuer le ping du nameserver avant de faire cela. Si vous ne pouvez pas effectuer le ping sur le nameserver, chercher à savoir pourquoi.

Notez que l'équipe qui opère le routeur 6 sera ajouté pour pouvoir ajouter la configuration qui permettra au bloc adresse du serveur DNS de se propager à travers le réseau de classe. La configuration supplémentaire pour Router6 est la suivante:

```
router ospf 41
 network 192.168.1.0 0.0.0.255 area 0
!
interface FastEthernet0/1
 ip addr 192.168.1.254 255.255.255.0
 no shutdown
!
```

21. **(Optional). Activer OSPF name lookups sur les routeurs.** Enchainant l'étape précédente, permettre maintenant les name lookups OSPF sur le routeur.

```
Router2(config)#ip ospf name-lookup
```

Cette commande permet l'affichage de l'OSPF router-id comme noms de domaine. Ainsi, plutôt que d'afficher la sortie suivante avec les name lookups désactivés:

```
router2>sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address       Interface
10.0.15.241       1   FULL/BDR        00:00:36    10.0.15.1     FastEthernet0/0
10.0.15.244       1   FULL/  -        00:00:32    10.0.15.18    Serial1/0
10.0.15.254       1   FULL/DR         00:00:38    10.0.15.26    FastEthernet0/1
```

le routeur affichera les informations suivantes:

```
router2#sh ip ospf neigh

Neighbor ID     Pri   State           Dead Time   Address       Interface
router1.worksho   1   FULL/BDR        00:00:33    10.0.15.1     FastEthernet0/0
router4.worksho   1   FULL/  -        00:00:39    10.0.15.18    Serial1/0
router14.worksh   1   FULL/DR         00:00:35    10.0.15.26    FastEthernet0/1
```

ce qui est beaucoup plus informatif.

22. **Ping Test #2.** Ping toutes les interfaces loopback dans la salle de classe. Cela permettra d'assurer que l'IGP OSPF est connecté End-to-End. Si vous rencontrez des problèmes utilisez les commandes suivantes pour les résoudre :

`show ip route`	: : Voir s'il ya un itinéraire pour la destination prévue
`show ip ospf`	: Voir informations générales OSPF

`show ip ospf interface` : Vérifier si le protocole OSPF est activé sur toutes les interfaces destinées
`show ip ospf neighbor` : Voir la liste des voisins OSPF que le routeur voit

Checkpoint #2: *appelez l'assistant de laboratoire pour vérifier la connectivité. Sauvegarder la configuration telle qu'elle est sur le routeur - utiliser une feuille de calcul distincte ou l'espace de travail à la fin de ce module. Vous aurez besoin de cette configuration à plusieurs reprises tout au long de l'atelier.*

23. Traceroute vers tous les routeurs. Une fois que vous pouvez effectuer le ping sur tous les routeurs, essayez de suivre des routes vers tous les routeurs utilisant *trace xxxx* commande. Par exemple, équipe routeur 1 entre:

```
Router1# trace 10.0.15.252
```

pour suivre une route vers le routeur R12. Si le temps limite est écoulé sur chaque hop en raison de destinations inaccessibles, il est possible d'interrompre le *traceroute* à l'aide de la séquence d'interruption Cisco CTRL-^.

Q. Pourquoi certains chemins traces montrent plusieurs adresses IP par hop?

A. S'il ya plus d'un des chemins de coût égal, OSPF va effectuer le "load share" trafic entre ces chemins.

```
Router1>trace router12

Tapez la séquence d'échappement pour annuler.
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>
```

24. Autres caractéristiques dans OSPF. Revoir la documentation ou la ligne de commande d'aide en en tapant ? pour voir d'autres commandes *show* et d'autres fonctions de configuration OSPF .

25. Configuration avancée. Ces équipes routeur qui ont achevé ce module doivent se référer au module 11 de l'atelier avancée BGP. Les étapes set-up ont été étendues pour inclure toutes les exigences de base d'un routeur qui est utilisé dans un backbone ISP. En attendant que le module soit conclut, il serait maintenant un bon moment pour réviser le module avancé et incorporer les ajouts à la configuration utilisée ici.

Questions de révision

1. Quel protocole IP que Ping et Traceroute utilisent?

2. Ping sur l'adresse IP du routeur de votre voisin (par exemple 10.0.15.2). Notez le temps qu'il a fallu pour le ping à compléter la tache. Maintenant, un autre ping sur l'adresse IP de votre routeur sur le même segment (par exemple 10.0.15.1). Notez le temps qu'il a fallu pour compléter une table de ping. Quels sont les résultats? Pourquoi y a-t-il une différence?

3. Quel IOS show command(s) affiche la table de forwarding du routeur?

4. Quel IOS show command(s) affiche la base de données OSPF du routeur?