# OSI 3 : le routage IP dynamique

## 1. Introduction

Dans le tp sur le routage statique, nous avons péniblement saisi nos routes statiques afin de faire fonctionner notre maquette. Ce fut laborieux, mais heureusement, nous n'avions que quatre routeurs.
Conscient que la tâche était trop importante dans de grands réseaux et qui plus est dans l'internet, des protocoles de routage dynamiques furent inventés pour soulager nos tâches. Mais, méfiance, comme toujours, trop de « automatique » et pas assez de « humain » comporte des risques...

Dans cette introduction, nous présentons les principaux concepts des protocoles de routage dynamique.

### 1A. Avant OSPF

Historiquement, un des premiers protocoles de routage IP dynamique est RIP (*Routing Information Protocol*). C'est un excellent moyen pédagogique pour aborder la problématique du routage dynamique. Mais, en réalité, il s'agit d'un protocole « historique » qui n'est plus vraiment utilisé. En voici les limites :

• le diamètre maximum d'un réseau géré avec RIP est limité à 15 routeurs soit 16 segments de réseau
• RIP est un gros consommateur de bande passante du fait de la méthode utilisée pour diffuser les informations de routage (toutes les 30 secondes, l'intégralité de la table RIP est diffusée même si elle n'a subi aucune modification). C'est fâcheux, en particulier sur des liaisons lentes ou facturées au volume de données transféré
• la **métrique** utilisée (qui pour RIP reflète le nombre de routeurs à traverser) ne garantit pas que le routage soit optimal. En effet, cette « distance » masque les caractéristiques réelles de la voie de transmission (débit ou coût en particulier)
• temps de convergence (temps avant que tous les routeurs aient calculé de nouvelles routes) trop long lorsque la topologie du réseau change (rupture d'un lien par exemple).

### 1B. OSPF

Compte tenu de ces contraintes et afin de gagner du temps, nous abordons directement OSPF qui est LE protocole de routage de prédilection à l'intérieur des grands réseaux d'entreprise. On a bien dit à l'intérieur car entre les réseaux d'entreprise, d'autres protocoles de routage dynamique sont mis en oeuvre : BGP en particulier (voir en fin de séquence).

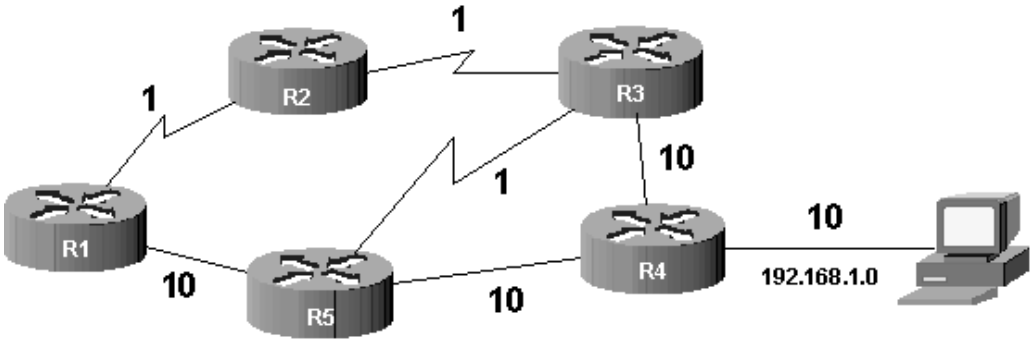
#### 1B1. Généralités

OSPF est un protocole de routage dynamique défini par l'IETF (*Internet Engineering Task Force* : organisme d'internet chargé de normaliser et de faire évoluer le réseau) à la fin des

années 80. Il a fait l'objet d'un historique relativement complexe de RFC. Ce protocole a deux caractéristiques essentielles :

• il est ouvert (le *Open* de OSPF), son fonctionnement peut être connu de tous ;
• il utilise l'algorithme SPF (*Shortest Path First*), plus connu sous le nom d'algorithme de Dijkstra, afin d'élire, parmi toutes les routes découvertes via ce protocole, la **meilleure** (mais pas forcément la plus courte) vers une destination donnée.

Examinons une topologie qui nous servira de support pour les explications :




**1B2. La notion de coût**

Supposons que du routeur R1 on cherche à atteindre le réseau 192.168.1.0. Dans une telle situation, RIP aurait élu la route passant par R5 puisque c'est la plus courte en termes de saut (nombre de routeurs traversés). Cependant, imaginez que les liens représentés sous forme d'éclairs soient « rapides » (type Ethernet à 100 Mbps par exemple) et que les liens « droits » soient « lents » (type Ethernet à 10 Mbps par exemple). Le choix de RIP n'est plus du tout pertinent !

OSPF fonctionne différemment. Il attribue un coût à chaque liaison (dénommée *lien* dans le jargon OSPF) afin de privilégier l'élection de certaines routes. Plus le coût est faible, plus le lien est intéressant. Par défaut, les coûts suivants sont utilisés en fonction de la bande passante du lien :

| Type de réseau | Coût par défaut |
|---|---|
| Ethernet > = 100 Mbps | 1 |
| FDDI | 1 |
| Ethernet 10 Mbps | 10 |
| E1 (2 Mbps) | 48 |
| T1 (1,5 Mbps) | 65 |
| 64 Kbps | 1562 |
| 56 Kbps | 1785 |

OSPF privilégie les routes qui ont un coût faible, donc celles qui sont supposées rapides en terme de débit théorique.

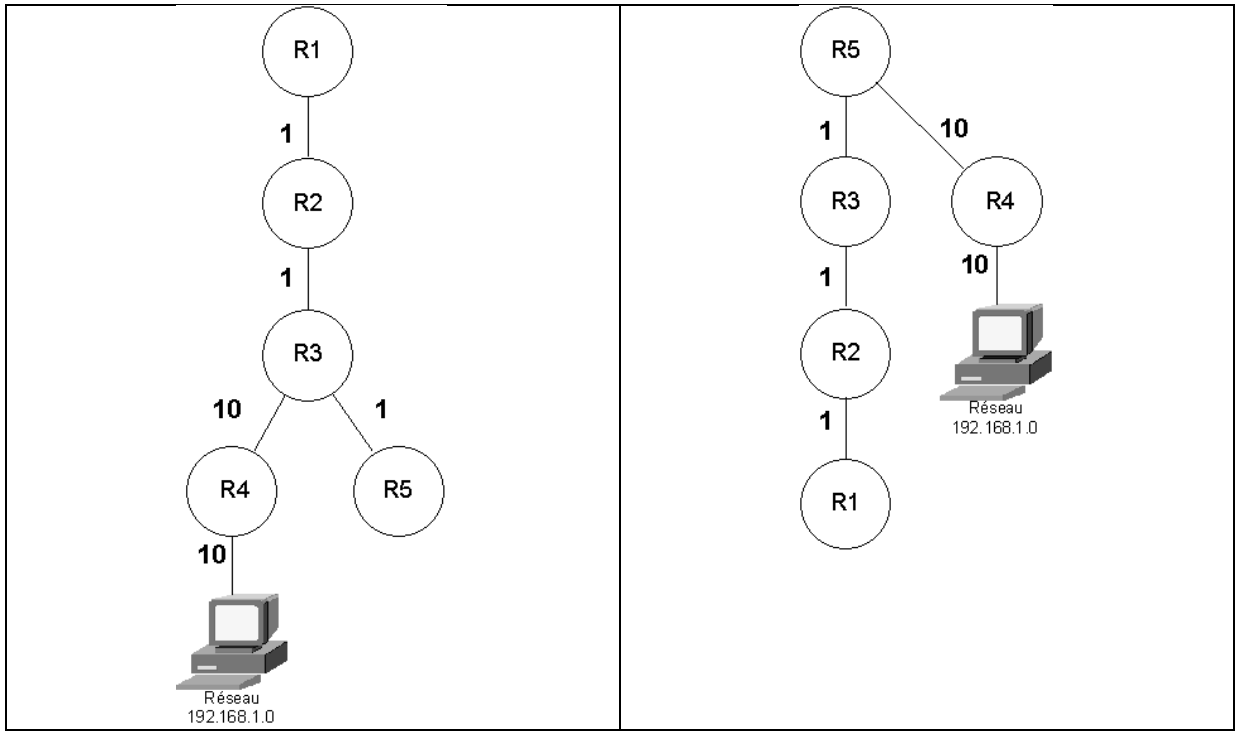
### 1B3. La base de données topologique

Avec OSPF, tous les routeurs d'un même réseau (on parle de **zone** dans le vocabulaire OSPF) travaillent sur une base de données topologique identique qui décrit le réseau. Cette base a été constituée pendant une première phase de découverte qui vous sera expliquée un peu plus loin. Examinons la base de données suivante qui décrit la topologie de la figure précédente :

| Arc | Coût |
|---|---|
| R1, R2 | 1 |
| R1, R5 | 10 |
| R2, R3 | 1 |
| R3, R4 | 10 |
| R3, R5 | 1 |
| R4, R5 | 10 |
| R4, 192.168.1.0 | 10 |

### 1B4. L'élection des meilleures routes

L'algorithme du SPF de Dijsktra va traiter cette base de données afin de déterminer les routes les moins coûteuses. Une fois le traitement réalisé, chaque routeur se voit comme la racine d'un arbre contenant les meilleures routes. Par exemple :




Dans l'exemple, entre R1 et 192.168.1.0, la meilleure route passe par R2, R3 et R4 pour un coût total de 1 + 1 + 10 + 10 soit 22.

### 1B5. La détermination d'une table de routage

La base de données topologique décrit le réseau mais ne sert pas directement au routage.
La table de routage est déterminée par l'application de l'algorithme du SPF sur la base topologique. Sur **R1**, voici un extrait de la table de routage calculée par SPF au sujet du réseau 192.168.1.0 :

| Réseau de destination | Moyen de l'atteindre | Coût |
|---|---|---|
| 192.168.1.0 | R2 | 22 |

Sur R5, on aura l'extrait suivant :

| Réseau de destination | Moyen de l'atteindre | Coût |
|---|---|---|
| 192.168.1.0 | R4 | 20 |

## 1C. Le fonctionnement d'OSPF un peu plus en détail

Pour administrer un réseau OSPF correctement, il est indispensable de comprendre le fonctionnement interne du protocole.
À l'intérieur d'une même zone, les routeurs fonctionnant sous OSPF doivent préalablement remplir les tâches suivantes avant de pouvoir effectuer leur travail de routage :

1. établir la liste des routeurs voisins ;
2. élire le routeur désigné (et le routeur désigné de secours) ;
3. découvrir les routes ;
4. élire les routes à utiliser ;
5. maintenir la base de données topologique.

***0. État initial***

Le processus de routage OSPF est inactif sur tous les routeurs de notre topologie.

***1. Établir la liste des routeurs voisins : Hello, my name is R1 and I'm an OSPF router.***

Les routeurs OSPF sont bien élevés. Dès qu'ils sont activés, ils n'ont qu'une hâte : se présenter et faire connaissance avec leurs voisins. En effet, lorsque le processus de routage est lancé sur R1 (commande *router ospf*), des paquets de données (appelés paquets HELLO) sont envoyés sur chaque interface où le routage dynamique a été activé (commande *network*). L'adresse *multicast* 224.0.0.5 est utilisée, tout routeur OSPF se considère comme destinataire. Ces paquets ont pour but de s'annoncer auprès de ses voisins.
Deux routeurs sont dits voisins s'ils ont au moins un lien en commun. Par exemple, sur la figure page 2, R1 et R2 sont voisins mais pas R1 et R3.
Lorsque le processus de routage OSPF est lancé sur R2, celui-ci récupère les paquets HELLO émis par R1 toutes les 10 secondes (valeur par défaut du temporisateur appelé *hello interval*). R2 intègre l'adresse IP de R1 dans une base de données appelée « base d'adjacences » (*adjacencies database*). Cette base contient les adresses des routeurs voisins. Vous pourrez visionner son contenu grâce à la commande *show ip ospf neighbor*. R2 répond à R1 par un paquet IP *unicast*. R1 intègre l'adresse IP de R2 dans sa propre base d'adjacences. Ensuite, généralisez ce processus à l'ensemble des routeurs de la zone.

Cette phase de découverte des voisins est fondamentale puisque OSPF est un protocole à **état de liens**. Il lui faut connaître ses voisins pour déterminer s'ils sont toujours joignables et donc déterminer l'état du lien qui les relie.

### *2. Élire le routeur désigné : c'est moi le chef !*

Dans une zone OSPF, l'un des routeurs doit être élu « routeur désigné » (DR pour *Designated Router*) et un autre « routeur désigné de secours » (BDR pour *BackupDesignated Router*). Le DR est un routeur particulier qui sert de référent au sujet de la base de données topologique représentant le réseau.

Pourquoi élire un routeur désigné ? Cela répond à trois objectifs :

• réduire le trafic lié à l'échange d'informations sur l'état des liens (car il n'y a pas d'échange entre tous les routeurs mais entre chaque routeur et le DR) ;
• améliorer l'intégrité de la base de données topologique (car il y a une base de données unique) ;
• accélérer la convergence (souvenez-vous, c'était le talon d'Achille de RIP).

Comment élire le DR ? Autrement dit, qui va se taper la corvée d'expliquer à ses petits camarades la topologie du réseau ? Mais comme il faut bien un critère, le routeur élu est celui qui a la plus grande priorité. La priorité est un nombre sur 8 bits fixé par défaut à 1 sur tous les routeurs. Pour départager les routeurs ayant la même priorité, c'est celui avec la plus grande adresse IP qui est élu. Le BDR sera le routeur avec la deuxième plus grande priorité. Afin de s'assurer que votre routeur préféré sera élu DR, il suffit de lui affecter une priorité supérieure à 1 avec la commande *ip ospf priority*.

Vous devrez faire ceci avant d'activer le processus de routage sur les routeurs car, une fois élu, le DR n'est jamais remis en cause même si un routeur avec une priorité plus grande apparaît dans la zone.

### *3. Découvrir les routes*

Il faut maintenant constituer la base de données topologique. Les routeurs communiquent automatiquement les routes pour les réseaux qui participent au routage dynamique (ceux déclarés avec la commande *network*). Les routeurs étant généralement multiprotocoles, ils peuvent également diffuser des routes provenant d'autres sources que OSPF, grâce à la commande *redistribute*.

Chaque routeur (non DR ou BDR) établit une relation maître/esclave avec le DR. Le DR initie l'échange en transmettant au routeur un résumé de sa base de données topologique via des paquets de données appelés LSA (*Link State Advertisement*). Ces paquets comprennent essentiellement l'adresse du routeur, le coût du lien et un numéro de séquence. Ce numéro est un moyen pour déterminer l'ancienneté des informations reçues. Si les LSA reçus sont plus récents que ceux dans sa base topologique, le routeur demande une information plus complète par un paquet LSR (*Link State Request*). Le DR répond par des paquets LSU (*Link State Update*) contenant l'intégralité de l'information demandée. Ensuite, le routeur (non DR ou BDR) transmet les routes meilleures ou inconnues du DR.

L'administrateur peut consulter la base de données topologique grâce à la commande *show ip ospf database*.

***4. Élire les routes à utiliser***

Lorsque le routeur est en possession de la base de données topologique, il est en mesure de créer la table de routage. L'algorithme du SPF est appliqué sur la base topologique. Il en ressort une table de routage contenant les routes les moins coûteuses.

Il faut noter que sur une base de données topologique importante, le calcul consomme pas mal de ressources CPU car l'algorithme est relativement complexe.

***5. Maintenir la base topologique***

Lorsqu'un routeur détecte un changement de l'état d'un lien (cette détection se fait grâce aux paquets HELLO adressés périodiquement par le routeur à ses voisins), celui-ci émet un paquet LSU sur l'adresse *multicast* 224.0.0.6 : le DR et le BDR de la zone se considèrent comme destinataires. Le DR (et le BDR) intègre cette information à sa base topologique et diffuse l'information sur l'adresse 224.0.0.5 (tous les routeurs OSPF sans distinction). C'est le protocole d'inondation.

Toute modification de la topologie déclenche une nouvelle exécution de l'algorithme du SPF et une nouvelle table de routage est constituée.

Voilà pour les principes fondamentaux d'OSPF, vous pouvez utiliser PacketTracer en mode simulation afin de mettre en évidence tout ce qui vient d'être dit.

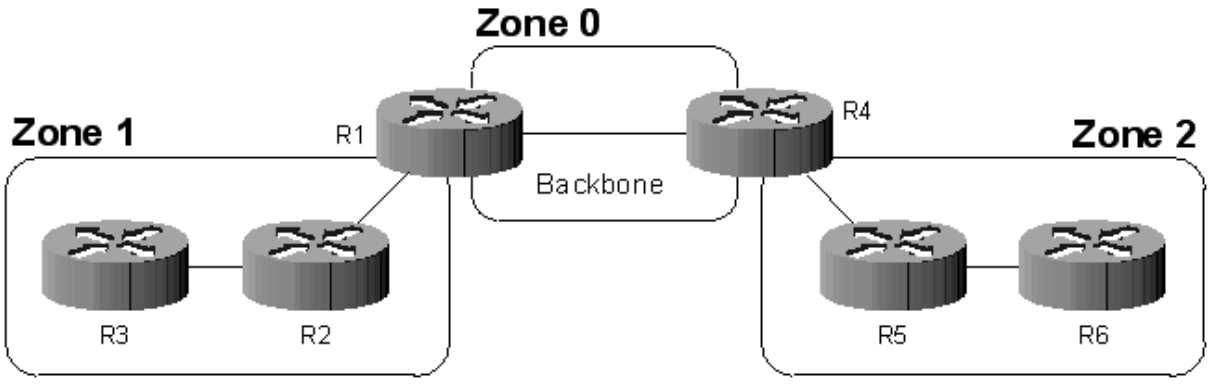
Avant d'attaquer la pratique, un dernier concept : les zones OSPF.

## 1D. Le concept de zone (area)

Contrairement à RIP, OSPF a été pensé pour supporter de très grands réseaux. Mais, qui dit grand réseau, dit nombreuses routes. Donc, afin d'éviter que la bande passante ne soit engloutie dans la diffusion des routes, OSPF introduit le concept de zone (*area*). Le réseau est divisé en plusieurs zones de routage qui contiennent des routeurs et des hôtes.

Chaque zone, identifiée par un numéro, possède sa propre topologie et ne connaît pas la topologie des autres zones. Chaque routeur d'une zone donnée ne connaît que les routeurs de sa propre zone ainsi que la façon d'atteindre une zone particulière, la zone numéro 0. Toutes les zones doivent être connectées physiquement à la zone 0 (appelée *backbone* ou réseau fédérateur). Elle est constituée de plusieurs routeurs interconnectés.

Le *backbone* est chargé de diffuser les informations de routage qu'il reçoit d'une zone aux autres zones. Tout routage basé sur OSPF doit posséder une zone 0.



Sur la figure ci-dessus, le réseau est découpé en trois zones dont le *backbone*. Les routeurs de la zone 1, par exemple, ne connaissent pas les routeurs de la zone 2 et encore moins la topologie de la zone 2. L'intérêt de définir des zones est de limiter le trafic de routage, de réduire la fréquence des calculs du plus court chemin par l'algorithme SPF ainsi que d'avoir une table de routage plus petite (ce qui accélère la convergence).

Les routeurs R1 et R4 sont particuliers puisqu'ils sont « à cheval » entre plusieurs zones (on les appelle ABR pour *Area Border Router* ou routeur de bordure de zone). Ces routeurs maintiennent une base de données topologique pour chaque zone à laquelle ils sont connectés. Les ABR sont des points de sortie pour les zones ce qui signifie que les informations de routage destinées aux autres zones doivent passer par l'ABR local à la zone.

L'ABR se charge alors de retransmettre les informations de routage au *backbone*. Les ABR du *backbone* redistribueront ensuite ces informations aux autres zones auxquelles ils sont connectés.

## 2. Sécurité

Tout comme les switches, les routeurs sont sensibles aux attaques.

Consultez le document ci-dessous pour vous en convaincre :

http://docwiki.cisco.com/wiki/Security_Technologies

Qui dit protocole « automatique », dit risque d'empoisonnement des tables de routage par de fausses annonces. La première des précautions sera donc de définir un mot de passe chiffré commun à tous les routeurs. Ceux-ci n'accepteront que les annonces avec un mot de passe valide.

Par interface sur laquelle les annonces OSPF sont activées :

```
router(config-if)# ip ospf message-digest-key 100 md5 !Cisco123!
```

Ensuite, dans la configuration du processus OSPF :

```
router(config-router)# area 0 authentication message-digest
```

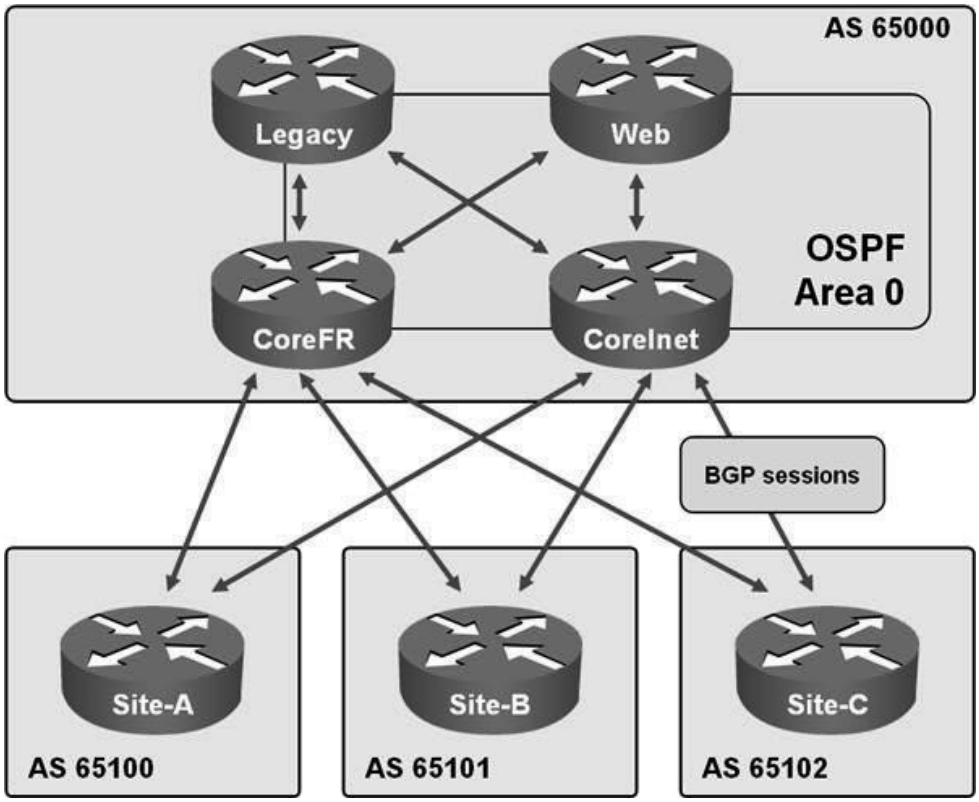
# 3. BGP

BGP pour *Border Gateway Protocol* est mis en oeuvre par les opérateurs Internet pour s'échanger à grande échelle des données de routage entre **systèmes autonomes (AS)**.

Un AS est un ensemble de réseaux informatiques IP intégrés à Internet et dont la politique de routage interne (routes à choisir en priorité, filtrage des annonces) est cohérente. Un AS est généralement sous le contrôle d'une entité unique, typiquement un fournisseur d'accès à Internet. Au sein d'un AS, le protocole de routage est qualifié d'« interne » (bien souvent OSPF). Entre deux AS, le routage est dit « externe » (BGP).

Chaque AS est identifié par un numéro de 16 (ou 32 depuis 2007, selon la RFC 4893) bits, appelé « Autonomous System Number » (ASN). Ce numéro est affecté par les organisations qui allouent les adresses IP, le Registre Internet Régional (RIR).

La figure ci-dessous montre 4 AS qui s'échangent des données de routage entre eux via BGP. À l'intérieur de l'AS 65000, OSPF est mis en oeuvre. Les routeurs CoreFR et CoreInet implémentent donc les deux protocoles OSPF et BGP.




Nous ne développerons pas plus cet aspect. Si vous souhaitez en savoir plus, consultez l'article Wikipedia sur BGP qui est très complet :

https://fr.wikipedia.org/wiki/Border_Gateway_Protocol