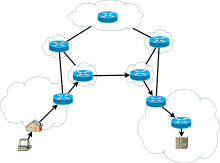
Routage

[](https://commons.wikimedia.org/wiki/File:Internet-transit.svg)

Exemple de routage dans un réseau.

Le routage est le mécanisme par lequel des chemins sont sélectionnés dans un réseau pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Le routage est une tâche exécutée dans de nombreux réseaux, tels que le réseau téléphonique, les réseaux de données électroniques comme Internet, et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés, c'est-à-dire où l'information n'est pas distribuée par une seule source, mais échangée entre des agents indépendants.

Historique

Les réseaux informatiques ont mis beaucoup de temps à déployer le routage dans toute sa dimension en raison des monopoles dans les télécommunications. Dans les années 1970 aux États-Unis, lors de la digitalisation du réseau d'AT&T (voir Réseau téléphonique commuté)1, IBM et DEC créent les architectures SNA et DECnet, encore très centralisées et peu ouvertes. En France, le réseau Cyclades, poussé par la CII et sa Distributed System Architecture, est plus ouvert et permet de partager les ressources informatiques des centres universitaires et de grandes entreprises en forte croissance comme EDF ou le Commissariat à l'énergie atomique, mais freiné par les prétentions du Réseau Transpac, imposé par les PTT et orienté vers la commutation de circuits plutôt que le routage. La Distributed System Architecture a cependant été reconnue par la création du Modèle OSI, encourageant l'étape suivante, avec les protocoles TCP/IP.

Types de cardinalité de la communication

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [Anycast.svg](https://commons.wikimedia.org/wiki/File:Anycast.svg) | [Broadcast.svg](https://commons.wikimedia.org/wiki/File:Broadcast.svg) | [Multicast.svg](https://commons.wikimedia.org/wiki/File:Multicast.svg) | [Unicast.svg](https://commons.wikimedia.org/wiki/File:Unicast.svg) | [Geocast.svg](https://commons.wikimedia.org/wiki/File:Geocast.svg) |
| anycast | broadcast | multicast | unicast | géocast |

Types de routages

En fonction du nombre de destinataires et de la manière de délivrer le message, on distingue :

*unicast*, qui consiste à acheminer les données vers une seule destination déterminée,

*broadcast* qui consiste à diffuser les données à toutes les machines,

*multicast* qui consiste à délivrer le message à un ensemble de machines manifestant un intérêt pour un groupe,

*anycast* qui consiste à délivrer les données à un seul membre d'un groupe, généralement le plus proche, au sens du réseau.

Application informatique du routage

Concepts

Pour effectuer le routage, on considère deux types de machines ou composants du réseau : les *routeurs*, qui servent d'intermédiaire dans la transmission d'un message, et les *hôtes* qui émettent ou reçoivent les messages. Lorsque le routeur se trouve entre deux réseaux dépendant d'autorités différentes, comme entre le réseau local d'une entreprise et l'Internet, on utilise alors une passerelle ; cet élément peut être considéré comme plus évolué qu'un simple routeur en raison de la conversion entre protocoles effectuée.

Le routage est un processus décentralisé, c'est-à-dire que chaque routeur possède des informations sur son voisinage. Chaque routeur maintient une liste des réseaux connus, chacun de ces réseaux étant associé à un ou plusieurs routeurs voisins à qui le message peut être passé. Cette liste s'appelle la *table de routage*, et contient trois types de routes :

les routes correspondant à des réseaux directement connectés : pour ces réseaux, le routeur peut acheminer le paquet directement à la destination finale en faisant appel au protocole de niveau 2 (Ethernet par exemple).

les routes statiques, configurées *en dur* sur le routeur par l'administrateur du réseau,

les routes dynamiques, apprises d'un protocole de routage dynamique dont le rôle est de diffuser les informations concernant les réseaux disponibles.

Une table de routage peut être réduite à sa plus simple expression en ne comportant que la liste des réseaux directement connectés ainsi qu'une *route par défaut*, c'est-à-dire que tous les paquets qui ne correspondent pas à un réseau connu dans la table de routage seront dirigés vers un routeur déterminé (le *routeur par défaut*). La route par défaut peut être statique ou bien apprise dynamiquement. À l'inverse, un routeur qui ne dispose pas de route par défaut doit connaître toutes les destinations possibles. C'est le cas des routeurs participant à la dorsale d'Internet, on dit alors qu'ils disposent d'une table de routage complète (ce qui représente actuellement plus de 360 000 réseaux individuels en 20112) ou qu'ils appartiennent à la *default-free zone* d'Internet.

Pour permettre à ce que les routeurs aient une idée de la topologie du réseau, et puissent ainsi employer des algorithmes de routage efficaces, il faut que les routeurs diffusent leurs informations. Cette diffusion s'effectue par le biais des protocoles de routage, spécifiant la façon dont les informations sont échangées entre les routeurs.

Protocoles de routage

Les protocoles de routages externe, tels que Border Gateway Protocol (BGP), échangent des informations de routage entre systèmes autonomes. Les IGP, ou *protocoles de routage interne*, échangent des informations de routage à l'intérieur d'un système autonome, par une des façons suivantes :

dits *à états de lien*, ils transmettent la totalité des informations de routage à tous les routeurs participants et établissent des tables de voisins directs, c'est le cas d'OSPF ou d'IS-IS,

dits à *vecteur de distance*, qui ne diffusent que leurs meilleures routes sur leurs interfaces, comme RIP ou IGRP

ou encore un hybride des deux premiers, comme EIGRP

Exemples de protocoles de routage interne :

Routing Information Protocol (RIP)

Interior Gateway Routing Protocol (IGRP)

Open Shortest Path First (OSPF)

Integrated Intermediate System to Intermediate System (Integrated IS-IS)

Enhanced Interior Gateway Routing Protocol (EIGRP)

Implémentation

Dans le modèle OSI, le routage s'effectue en examinant les informations situées dans la couche de réseau tels que l'IP.

Aspects théoriques

On parle de *routage inconscient* (anglais *oblivious routing*) lorsque les chemins sont choisis à l'avance pour toute paire de source et destination et tout message doit emprunter l'un de ces chemins. Autrement dit, le trajet d'un message ne dépend que de la source et de la destination (et de l'heuristique effectuant le choix entre plusieurs chemins si le cas se présente). Le routage est *adaptif* si le chemin emprunté par un message dépend des autres communications survenant dans le réseau.

Etude d’un protocole de routage : Open Shortest Path First

***Open Shortest Path First*** (OSPF) est un protocole de routage interne IP de type « à état de liens ». Il a été développé au sein de l'Internet Engineering Task Force (IETF) à partir de 1987. La version actuelle d'OSPFv2 est décrite dans la RFC 2328 en 1997. Une version 3 est définie dans la RFC 2740 et permet l'utilisation d'OSPF dans un réseau IPv6.

Histoire

Le groupe de travail OSPF a été formé au sein de l'IETF en 1987 pour remplacer RIP. Il est inspiré du protocole ARPANET développé par BBN. La version 1 est publiée dans la RFC 1131 en 1990. La version 2 est décrite RFC 1247 en 1991. En 1992, l'Internet Engineering Steering Group (IESG) recommande OSPF comme IGP pour Internet dans la RFC 1371.

Fonctionnement général

Dans OSPF, chaque routeur établit des relations d'adjacence avec ses voisins immédiats en envoyant des messages *hello* à intervalle régulier. Chaque routeur communique ensuite la liste des réseaux auxquels il est connecté par des messages *Link-state advertisements* (LSA) propagés de proche en proche à tous les routeurs du réseau. L'ensemble des LSA forme une base de données de l'état des liens *Link-State Database* (LSDB) pour chaque aire, qui est identique pour tous les routeurs participants dans cette aire. Chaque routeur utilise ensuite l'algorithme de Dijkstra, *Shortest Path First* (SPF) pour déterminer la route la plus courte vers chacun des réseaux connus dans la LSDB.

Le bon fonctionnement d'OSPF requiert donc une complète cohérence dans le calcul SPF, il n'est donc par exemple pas possible de filtrer des routes ou de les résumer à l'intérieur d'une aire.

En cas de changement de topologie, de nouveaux LSA sont propagés de proche en proche, et l'algorithme SPF est exécuté à nouveau sur chaque routeur.

Notion d'aire et types de routeurs

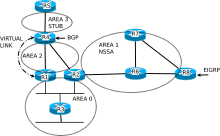
Afin d'éviter de propager la totalité de la base de données des liens et de limiter l'impact négatif du bagottement ou *flapping* (alternance rapide dans la disponibilité d'un lien), on segmente l'ensemble des routeurs en groupes connexes appelés *aires*, à la frontière desquels on peut procéder à des résumés. Chaque aire est distinguée par un nombre entier positif ou nul variant de 0 à 4 294 967 295, ce nombre est parfois exprimé en notation décimale pointée, de la même manière qu'une adresse IP. Chaque sous-réseau appartient à une seule aire.

Il existe toujours une aire dorsale (*backbone area*), *area 0* ou encore *area 0.0.0.0* à laquelle toutes les autres aires sont connectées.

Les aires sont logiquement contigües. Si les routeurs qui constituent une aire ne sont pas physiquement contigus, alors des *liens virtuels* sont configurés entre les routeurs qui ont en commun une aire de transit. Ces liens virtuels appartiennent à l'aire 0. Le protocole les traite comme des liens point-à-point non numérotés.

Chaque routeur est identifié à l'aide d'un *router-id* unique dans le réseau. Le router-id est un nombre positif codé sur 32 bits, il est habituellement représenté sous la forme d'une adresse IP. À défaut d'une configuration explicite, l'adresse IP locale la plus élevée sera utilisée, et s'il existe des interfaces de type loopback, l'adresse IP la plus élevée de celles-ci sera utilisée comme router-id. La détermination du router-id a lieu uniquement à l'initialisation du processus OSPF et persiste ensuite, indépendamment de la reconfiguration ou du changement d'état des interfaces.

Types de routeurs

[](https://commons.wikimedia.org/wiki/File:OSPF_Network.svg)

R1, R2 et R3 sont des routeurs backbone. R1, R2 et R4 sont des ABR. R4 et R8 sont des ASBR. L'area 3 est connectée à l'area 0 grâce à un virtual link.

On distingue les types de routeurs suivants :

Routeur interne

un routeur dont toutes les interfaces se trouvent dans la même aire ;

*Area Border Router* (ABR)

un routeur qui dispose d'interfaces dans des aires différentes ;

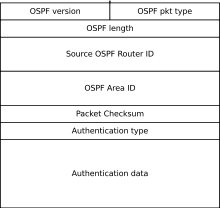
*Autonomous System Boundary Router* (ASBR)

un routeur qui injecte dans OSPF des routes qui proviennent d'autres protocoles de routage ou des routes statiques ;

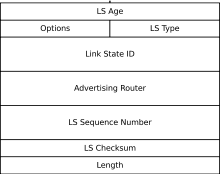
Routeur backbone

un routeur dont au moins une interface appartient à l'aire 0. Tous les ABR sont des routeurs backbone.

Paquets OSPF et LSA

[](https://commons.wikimedia.org/wiki/File:OSPF_header.svg)

En-tête du paquet OSPF (24 octets).

[](https://commons.wikimedia.org/wiki/File:OSPF_LSA.svg)

En-tête du LSA (20 octets).

OSPF fait usage du numéro de protocole 89 d'IP. Le TTL des paquets est fixé à 1 pour éviter leur propagation au-delà du sous-réseau et le champ ToS est fixé à 0. OSPF utilise des adresses multicast sur les réseaux de type broadcast et point à point.

Les paquets OSPF ont une taille qui peut aller jusqu'à 65535 octets et faire usage de la fragmentation IP si c'est nécessaire. Il est cependant recommandé de tenir compte du MTU du lien pour éviter la fragmentation en répartissant les LSA dans des messages LS Update plus petits que le MTU, si c'est possible.

Les LSA peuvent également atteindre 64 KB, cependant ils sont généralement de petite taille à l'exception du type 1 (*router LSA*), qui peut être volumineux pour des routeurs avec de nombreuses interfaces OSPF.

Il existe 5 types de paquets OSPF :

**Hello (Type 1)**

découverte des voisins et maintien des adjacences ;

**Database Description (DBD, Type 2)**

description des LSA ;

**Link State Request (Type 3)**

requête d'un LSA ;

**Link State Update (Type 4)**

mise à jour d'un LSA ;

**Link State Acknowledgement (Type 5)**

acquittement d'un LSA.

Le type 1 (hello) est utilisé pour l'établissement et le maintien des adjacences, les autres types sont utilisés pour la synchronisation de la LSDB.

Les types suivants de LSA sont définis :

**Type 1 (router)**

diffusé par un routeur, décrit l'état de ses interfaces ;

**Type 2 (network)**

diffusé par un DR (Designated Router), décrit les routeurs attachés à un sous-réseau ;

**Type 3 (summary)**

résumé de route par un ABR ;

**Type 4 (interarea summary)**

route vers l'ASBR, généré par un ABR ;

**Type 5 (external)**

diffusé par un ASBR, décrit une route externe ;

**Type 6 (multicast group membership)**

utilisé par MOSPF ;

**Type 7 (external NSSA)**

route externe générée par un ASBR d'un NSSA.

Les types 1 et 2 constituent les *routes internes* d'une aire (intra-area), les types 3 et 4 sont des routes inter-area (IA). Les routeurs backbone sont responsables de la diffusion des informations de routage inter-area.

Les routes externes se subdivisent en :

Type E1

le coût de l'accès à l'ASBR est ajouté à la métrique initiale de la route externe ;

Type E2

le coût de la métrique est fixe et ne dépend pas du coût vers l'ASBR.

Les LSA sont identifiés par le routeur d'origine, le type de LSA et le LSA ID. La signification de ce dernier varie en fonction du type de LSA :

|  |  |
| --- | --- |
| LSA Type | LSA ID |
| 1 | Le router-id de l'émetteur |
| 2 | L'adresse IP de l'interface du DR |
| 3 | L'adresse du réseau de destination |
| 4 | Le router-id de l'ASBR |
| 5 | L'adresse du réseau externe |

Le LSA de type 1 (router) se subdivise en quatre sous-types qui dépendent du type de réseau décrit.

+ Link type 1

|  |  |  |  |
| --- | --- | --- | --- |
| Sous-type | Description | Link ID | Link data |
| 1 | point-to-point | router-id du voisin | Adresse IP de l'interface ou MIB-II ifIndex si l'interface n'est pas numérotée |
| 2 | lien vers un réseau de transit | adresse de l'interface du DR | Adresse IP de l'interface |
| 3 | lien vers un réseau stub | adresse du réseau | masque réseau |
| 4 | lien virtuel | router-id du voisin | Adresse IP de l'interface |

Tous les LSA sont accompagnés d'une somme de contrôle qui assure l'intégrité des données. Celle-ci est vérifiée à la réception du LSA, enregistrée dans la LSDB et transmise aux voisins sans modification. Elle est ensuite revérifiée à intervalle régulier pour s'assurer que le contenu de la LSDB n'a pas été corrompu.

Gestion des LSA

Les LSA sont caractérisés par leur routeur d'origine, leur type et le LSA ID. Les numéros de séquence augmentent de 1 à chaque changement, le premier numéro de séquence étant 0x80000001 (InitialSequenceNumber, -231+1) jusqu'à 0x7fffffff (231). Chaque version du LSA remplace les versions de numéro de séquence inférieur. En l'absence de changement, les LSA sont rafraîchis toutes les 30 minutes (LSRefreshTime). Un LSA qui atteint l'âge d'une heure (MaxAge) est éliminé de la LSDB. Le routeur d'origine du LSA peut spécifier que le LSA n'est pas rafraîchi en plaçant le bit DoNotAge à 1 dans les options.

Les LSA sont diffusés de façon fiable. Quand un routeur doit mettre à jour un LSA à la suite d'un changement de topologie, il incrémente son numéro de séquence et le diffuse à ses voisins adjacents sous forme d'un paquet Link-State Update (qui peut contenir plus d'un LSA). Les LSA font alors l'objet d'un acquittement explicite, faute de quoi ils sont retransmis. Les routeurs qui reçoivent le LSA comparent son numéro de séquence à celui qu'ils possèdent déjà, et s'il est plus élevé, ils l'enregistrent le LSA dans la LSDB et le transmettent également à leur voisin. Le champ LS Age est incrémenté à chaque transmission pour éviter les boucles infinies à la suite d'une erreur logicielle. Si un LSA est reçu avec un numéro de séquence identique à celui déjà présent de la LSDB mais avec une différence d'âge inférieure à 15 minutes (MaxAgeDiff), le LSA sera ignoré.

Un routeur à l'origine d'un LSA qu'il veut faire disparaître de la LSDB le diffuse avec un LS Age = MaxAge, ce qui cause son élimination.

Les routeurs s'abstiennent de mettre à jour un LSA plus fréquemment que toutes les 5 secondes (MinLSInterval). Les routeurs rejettent les mises à jour d'un LSA qui a déjà fait l'objet d'une mise à jour il y a moins d'une seconde.

Types d'aires

On distingue les types d'aires suivantes :

aire 0

aire backbone ;

stub area

aire vers laquelle ne sont pas propagées les LSA de type 5 (routes externes) ;

totally stub area

aucun LSA de type 3, 4, 5 ou 7 n'y est propagée, à l'exception d'une route par défaut ;

not-so-stubby area (NSSA)

type de stub area qui permet l'injection de routes externes via un LSA de type 7. Le type 7 sera converti en type 5 quand il sera transmis en dehors de l'aire ;

totally NSSA

NSSA sans LSA 3 et 4 à l'exception d'une route par défaut.

Il n'est pas possible de créer des liens virtuels à travers une stub area, ni des ASBR internes à une stub area.

Types de réseaux

Point-to-point

le sous réseau correspond à un lien point à point ;

Broadcast multiaccess

le sous-réseau peut comporter plus de deux routeurs qui peuvent tous communiquer entre eux, une adresse broadcast est disponible ;

Point-to-multipoint

le sous-réseau est constitué d'un routeur central et d'autres routeurs qui ne communiquent pas entre eux. OSPF traite le réseau comme une collection de liens point-à-point ;

NBMA (Non-broadcast multiaccess)

le sous-réseau est constitué de routeurs qui peuvent communiquer entre eux mais il n'existe pas d'adresse broadcast. Dans ce type de réseau, OSPF émule le type broadcast en répliquant les LSA à tous les voisins adjacents ;

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Point-to-point | Broadcast | Point-to-multipoint (non-broadcast) | Point-to-multipoint (broadcast) | NBMA |
| DR/BDR | non | oui | non | non | oui |
| hello/dead | 10s/40s | 10s/40s | 30s/120s | 30s/120s | 30s/120s |
| découverte des voisins | oui | oui | non | oui | non |
| RFC 2328 | oui | oui | oui | Cisco | oui |

Formation des adjacences

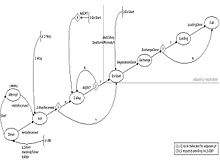
[](https://commons.wikimedia.org/wiki/File:Neigospf.jpg)

Diagramme d'état des adjacences.

Dans un sous-réseau, les routeurs qui se découvrent grâce au protocole *hello* sont appelés *voisins*. Dans les réseaux de type point-à-multipoint et NBMA, les voisins sont configurés explicitement. Pour autant que les paramètres des voisins soient compatibles, ils tentent alors de former une relation d'adjacence. L'établissement de l'adjacence est requise avant l'échange d'information de routage.

L'adjacence peut prendre les états suivants :

Down

aucune information n'a été reçue sur ce segment ;

Attempt

sur les réseaux NBMA, indique qu'aucune information récente n'a été reçue du voisin configuré ;

Init

un paquet hello a été reçu ;

2-Way

un paquet hello a été reçu et celui-ci contient son propre router-id, ce qui montre qu'il existe une communication bidirectionnelle. L'élection du DR et du BDR a lieu dans cet état. La décision de former une adjacence est prise au terme de cet état.

ExStart

les routeurs tentent d'établir les numéro de séquence initiaux qui seront utilisés dans les paquets d'échange d'information. Pour cet échange, un des routeurs deviendra le routeur primaire et l'autre le secondaire.

Exchange

les routeurs envoient leur LSDB par des paquets *database description* (DBD) ;

Loading

l'échange des LSDB se finalise, les routeurs réclament les LSA dont ils ont besoin ;

Full

la LSDB est synchronisée et l'adjacence est établie.

Protocole hello

Les messages *hello* sont envoyés à intervalle régulier sur les interfaces où OSPF est actif. Sur les liens point-à-point et les liens broadcast, ils sont diffusés sur l'adresse multicast 224.0.0.5 (AllSPFRouters), sur les liens sans broadcast, ils sont envoyés vers l'adresse IP unicast du voisin.

Les informations suivantes se trouvent notamment dans le paquet hello :

le DR et le BDR

la priorité

le type de réseau

la liste des routeurs OSPF connus du sous-réseau

le masque de sous-réseau

les périodes hello et dead

des options

Le numéro d'aire est inclus dans l'en-tête paquet OSPF. Une adjacence ne se forme pas si certains paramètres ne sont pas compatibles (numéro d'aire, type d'aire (stub ou non), périodes hello/dead, authentification).

Adjacence sur un réseau à diffusion

Une relation d'adjacence est nécessaire pour que les routeurs OSPF se partagent des informations de routage. Dans un réseau broadcast (Ethernet) si chaque routeur devait établir une adjacence avec chaque autre routeur et échanger des informations d’état de liens la charge serait excessive, le nombre d'adjacences étant de \frac{n(n-1)}{2}, soit en O(n^2). Pour pallier ce problème, on choisit un DR (routeur désigné) qui va recevoir toutes les informations sur l'état des liens et les retransmettre aux autres routeurs. Celui-ci devenant un point critique du réseau, on désigne aussi un BDR (routeur désigné de secours). Le nombre d'adjacence est donc de 2n-1, soit en O(n). Les autres routeurs sont qualifiés de *DR Other*.

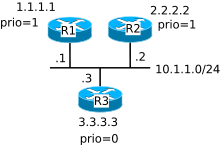
OSPF utilise uniquement du *multicast* pour communiquer, avec les deux adresses suivantes :

224.0.0.5 (AllSPFRouters) utilisé par le DR pour envoyer les informations d’état de liens à tous les autres routeurs sur le segment.

224.0.0.6 (AllDRouters) utilisé par tous les routeurs pour envoyer les LSA vers le DR et le BDR.

Seul le DR génère le *network* LSA (type 2) correspondant au sous-réseau. Le LSID de celui-ci vaudra l'adresse IP du DR dans le sous-réseau. Ce LSA liste également les routeurs attachés au sous-réseau.

Élection du DR

[](https://commons.wikimedia.org/wiki/File:OSPF_DR.svg)

Si les trois routeurs sont démarrés simultanément, R2 deviendra le DR en raison du router-id plus élevé et R1 le BDR. R3 ne participe pas à l'élection du DR car sa priority vaut 0.

Pour un sous-réseau déterminé de type broadcast ou NBMA, chaque routeur OSPF possède une valeur appelée *priority* comprise entre 0 et 255. Si la priorité est configurée à 0, le routeur ne participe pas à l'élection et ne peut donc devenir ni DR, ni BDR.

Les autres routeurs qui sont au moins dans l'état 2-Way sont éligibles.

L'élection commence par le BDR. S'il existe déjà plusieurs routeurs qui indiquent être le BDR dans leurs paquets hello, celui qui a la priorité la plus haute sera retenu comme BDR, et s'il existe plusieurs routeurs avec la priorité la plus haute, alors celui dont le router-ID est le plus élevé est retenu comme BDR. S'il n'existe qu'un routeur qui indique être le BDR, ce choix persiste. Si la liste des candidats est vide, alors le BDR est le routeur éligible non-DR dont la priorité est la plus élevée, et s'il en existe plusieurs, alors celui dont le router-id le plus élevé est retenu.

On procède de même avec le DR, s'il n'y a pas de candidat DR, alors le BDR est promu en DR et on recommence l'élection du BDR comme au paragraphe précédent.

Les autres routeurs sont adjacents au DR et au BDR. En cas de défaillance du DR, le BDR devient DR et on procède à une nouvelle élection du BDR.

Suivant cette procédure, si un routeur est ajouté au réseau alors qu'un DR et qu'un BDR existent déjà, alors les DR et BDR persistent même si la priorité du nouveau venu est plus élevée.

Synchronisation

Une fois l'adjacence établie, les routeurs vont déterminer un routeur primaire et un secondaire ainsi qu'un numéro de séquence initial. Le routeur primaire va envoyer des paquets Database Description (DBD) au secondaire, ceux-ci consistent en une liste des en-têtes de LSA (mais sans les données du LSA proprement dites), le secondaire va noter les LSA qu'il ne possède pas ou dont les numéros de séquence sont plus élevés que celui dans sa LSDB et va les réclamer ensuite au primaire avec des paquets Link State Requests. Le routeur primaire lui répond avec des paquets Link State Update qui contiennent les LSA demandés. Le secondaire envoie ensuite les paquets Link State Update qui correspondent aux LSA dont le primaire ne dispose pas ou qui sont plus à jour chez le secondaire.

Une fois la synchronisation terminée, l'adjacence bascule dans l'état Full et les LSA sont diffusés normalement.

Résumé de routes

Les routes peuvent être résumées à deux niveaux dans OSPF :

les routes externes peuvent être résumées par l'ASBR qui les injecte dans OSPF ;

les routes inter-area peuvent être résumées par l'ABR à la frontière de ces areas.

Métrique

OSPF utilise une métrique numérique, basée sur un *coût* additif qui peut varier de 1 à 65535. La spécification ne donne pas de signification particulière à cette métrique, la contrainte étant qu'additionner les coûts de liens successifs pour déterminer le coût total doit avoir un sens.

Cisco utilise une valeur par défaut du coût d'un lien qui vaut 108/bande passante du lien en bit/s. Un lien de 10 Mbit/s aura par exemple un coût de 10. Pour tenir compte des connexions à très haute vitesse (1 Gbit/s et plus), on peut fixer manuellement le coût de chaque lien, ou bien fixer une bande passante de référence supérieure à celle par défaut.

Indépendamment de la métrique, les types de routes suivants sont préférés dans cet ordre :

routes intra-area

routes inter-area

routes externes E1

routes externes E2

OSPF est capable de répartir la charge sur plusieurs liens, pour autant que la métrique soit exactement identique pour chaque destination.

Authentification

Les paquets OSPF peuvent faire l'objet de deux formes d'authentification, la première consiste en un mot de passe transmis en clair dans le paquet, la seconde consiste en une fonction de hachage MD5 calculée sur le paquet et un mot de passe partagé.

L’algorithme de Dijkstra

OSPF utilise l'algorithme de Dijkstra pour déterminer le meilleur chemin à prendre. On le nomme aussi algorithme SPF (*Shortest Path First*) ou algorithme du plus court chemin d’abord. Il a été formulé par Edsger Dijkstra.

OSPF déclenche ses mises à jour à chaque changement dans la topologie du réseau, ce qui permet de réduire le temps de convergence. À partir d'une mise à jour, un routeur met en place une base de données topologique permettant le calcul de l'accessibilité aux réseaux grâce au calcul d'un arbre de la topologie dont le routeur est la racine.

Avantages et inconvénients

Avantages d'OSPF

C'est un standard IETF qui fait l'objet du RFC 2328, il fait donc l'objet d'implémentations par de nombreux vendeurs et ne pose pas de problème d'interopérabilité, il est de ce fait particulièrement populaire,

son temps de convergence est particulièrement court,

il intègre la notion de taille de masque variable (VLSM), indispensable à la gestion des réseaux sans classe actuels,

il est économe en bande passante : en régime, seuls de courts messages *hello* sont envoyés, et en cas de changement de topologie, seuls les LSA modifiés sont envoyés aux voisins. Chaque routeur retransmet cependant l'ensemble de ses LSA à ses voisins toutes les trente minutes.

Inconvénients d'OSPF

comme chaque routeur dispose de la totalité de la base de données de liens, tous doivent disposer de la capacité mémoire suffisante pour la stocker,

OSPF est sensible au phénomène de bagottement ou *flapping*, la capacité CPU joue un rôle dans le calcul SPF et donc la vitesse de convergence, en particulier pour les topologies complexes et instables,

on estime en général qu'OSPF convient pour des topologies comprenant jusqu'à 1000 routeurs,

la configuration d'OSPF est plus complexe, principalement si le réseau est segmenté en aires,

le concept de *backbone area* peut limiter les topologies possibles,

il ne permet pas la répartition de la charge sur plusieurs liens de métrique différente, comme EIGRP peut le faire,

OSPFv2 est spécifique à IP. Pour d'autres protocoles, comme par exemple IPv6, une nouvelle version du protocole est nécessaire : OSPFv3.

OSPF ne peut pas être configuré sur un switch.