Groupe de travail Réseau
Request for Comments : 2328
STD : 54
RFC rendue obsolète : 2178
Catégorie : Norme

J. Moy, Ascend Communications, Inc.
avril 1998

Traduction Claude Brière de L'Isle

OSPF version 2

Statut du présent mémoire
Le présent document spécifie un protocole de l'Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et suggestions pour son amélioration. Prière de se référer à l'édition en cours des "Normes officielles des protocoles de l'Internet" (STD 1) pour connaître l'état de la normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent mémoire expose la version 2 du protocole OSPF. OSPF est un protocole d'acheminement par état de liaison. Il a été conçu pour fonctionner en interne sur un seul système autonome. Chaque routeur OSPF entretient une base de données identique qui décrit la topologie du système autonome. À partir de cette base de données est calculé un tableau d'acheminement en construisant un arbre des plus courts chemins.

OSPF recalcule rapidement les routes en présence d'un changement topologique, en utilisant un minimum de trafic de protocole d'acheminement. OSPF fournit la prise en charge de chemins multiples de coût égal. Il fournit une capacité d'acheminement de zone, qui procure une niveau supplémentaire de protection de l'acheminement et une réduction du trafic de protocole d'acheminement. De plus, tous les échanges de protocole d'acheminement OSPF sont authentifiés.

Les différences entre le présent mémoire et la RFC 2178 sont expliquées dans l'Appendice G. Toutes les différences sont rétrocompatibles par nature. Les mises en œuvre du présent mémoire et des RFC 2178, 1583, et 1247 interopèrent.

Prière d'envoyer vos commentaires à ospf@gated.cornell.edu.

(Cette traduction incorpore les errata 1420, 1745, 1833, 2394, 2632.)

Table des matières

1. Introduction

Le présent document est la spécification du protocole d'acheminement internet TCP/IP Ouverture du plus court chemin en premier (OSPF, *Open Shortest Path First*). OSPF est classé comme protocole de routeur intérieur (IGP, *Internal Gateway Protocol*). Cela signifie qu'il distribue des informations d'acheminement entre les routeurs qui appartiennent à un seul système autonome. Le protocole OSPF se fonde sur la technique de l'état de liaison ou SPF. Cela se distingue de la base Bellman-Ford utilisée par les protocoles d'acheminement traditionnels de l'internet TCP/IP.

Le protocole OSPF a été développé par le groupe de travail OSPF au sein de l'équipe d'ingénierie de l'Internet (IETF, *Internet Engineering Task Force*). Il a été conçu expressément pour l'environnement internet TCP/IP, en incluant la prise en charge explicite du CIDR *(Classless Interdomain Routing,* acheminement inter domaine sans classe) et l'étiquetage des informations d'acheminement déduites en externe. OSPF fournit aussi l'authentification des mises à jour d'acheminement, et utilise la diffusion groupée IP lors de l'envoi/réception des mises à jour. De plus, beaucoup de travail a été fait pour produire un protocole qui réponde rapidement aux changements de topologie, tout en n'impliquant que de petites quantités de trafic de protocole d'acheminement.

1.1 Généralités sur le protocole

OSPF achemine les paquets IP sur la seule base de l'adresse de destination IP qui se trouve dans l'en-tête du paquet IP. Les paquets IP sont acheminés "en l'état" – ils ne sont pas encapsulés dans d'autres en-têtes de protocole lorsqu'ils passent à travers le système autonome. OSPF est un protocole d'acheminement dynamique. Il détecte rapidement les changements topologiques dans l'AS (tels que les défaillances d'interface de routeur) et calcule de nouvelles routes sans boucle après une période de convergence. Cette période de convergence est courte et n'implique qu'un minimum de trafic de routage.

Dans un protocole d'acheminement par état de liaison, chaque routeur entretient une base de données qui décrit la topologie du système autonome. Cette base de données est appelée la base de données d'états de liaisons. Chaque routeur participant a une base de données identique. Chaque pièce individuelle de cette base de données est un état local d'un routeur particulier (par exemple, les interfaces utilisables du routeur et les voisins joignables). Le routeur distribue son état local dans tout le système autonome.

Tous les routeurs fonctionnent en parallèle avec exactement le même algorithme. À partir de la base de données d'états des liaisons, chaque routeur construit un arbre des plus courts chemins en se prenant lui-même comme racine. Cet arbre des plus courts chemins donne la route de chaque destination dans le système autonome. Les informations d'acheminement de provenance externe apparaissent comme les feuilles de l'arbre.

Lorsque plusieurs chemins à coût égal existent pour une destination, le trafic est distribué également entre eux. Le coût d'un chemin est décrit par une seule métrique sans dimension.

OSPF permet que des ensembles de réseaux soient groupés. Un tel groupement s'appelle une zone. La topologie d'une zone est cachée au reste du système autonome. Ces informations cachées permettent une réduction significative du trafic d'acheminement. L'acheminement au sein d'une zone n'est déterminé que par la propre topologie de la zone, protégeant la zone contre de mauvaises données d'acheminement. Une zone est une généralisation d'un réseau IP organisé en sous-réseaux.

OSPF permet une configuration souple des sous-réseaux IP. Chaque chemin distribué par OSPF a une destination et un gabarit. Deux sous-réseaux différents du même numéro de réseau IP peuvent avoir des tailles différentes (c'est-à-dire, des gabarits différents). Ceci est habituellement appelé du sous-réseautage à taille variable. Un paquet est acheminé au mieux (c'est-à-dire, à l'adresse la plus longue ou la plus spécifique). Les chemins d'hôtes sont considérés comme des sous-réseaux dont les gabarits sont "tout à uns" (0xffffffff).

Tous les échanges de protocole OSPF sont authentifiés. Cela signifie que seuls les routeurs de confiance peuvent participer à l'acheminement du système autonome. Divers schémas d'authentification peuvent être utilisés ; en fait, des schémas d'authentification distincts peuvent être configurés pour chaque sous-réseau IP.

Les données d'acheminement de provenance externe (par exemple, les chemins appris d'un protocole de routeur extérieur tel que BGP ; voir [Ref23]) sont publiés dans tout le système autonome. Ces données d'acquisition externes sont gardées séparément des données d'état de liaison du protocole. Chaque chemin externe peut aussi être étiqueté par le routeur qui le notifie, ce qui permet de passer les informations supplémentaires entre les routeurs sur les frontières du système autonome.

1.2 Définitions des termes couramment utilisés

Ce paragraphe donne les définitions des termes qui ont une signification spécifique pour le protocole OSPF et sont utilisés tout au long du texte. Les lecteurs qui ne sont pas familiers de la suite des protocoles de l'Internet se réfèreront à [Ref13] pour une introduction à IP.

Routeur
: Commutateur de paquets de protocole Internet de niveau trois. Précédemment appelé une passerelle dans la plupart des documents sur IP.

Système autonome
: Groupe de routeurs qui échangent des informations d'acheminement via un protocole d'acheminement commun. Abrégé en AS.

Protocole de routeur intérieur
: Protocole d'acheminement utilisé par les routeurs qui appartiennent à un système autonome. Abrégé en IGP. Chaque système autonome a un seul IGP. Des systèmes autonomes distincts peuvent fonctionner avec des IGP différents.

Identifiant de routeur
: Nombre de 32 bits alloué à chaque routeur fonctionnant avec le protocole OSPF. Ce nombre identifie de façon univoque le routeur au sein d'un système autonome.

Réseau
: Dans le présent mémoire, un réseau/sous-réseau/super-réseau IP. Il est possible qu'à un seul réseau physique soient alloués plusieurs numéros de réseau/sous-réseau IP. On les considère comme des réseaux distincts. Les réseaux physiques en point à point sont une exception – ils sont considérés comme un seul réseau sans égard aux numéros de réseau/sous-réseau IP (s'il en est) qui leur sont alloués.

Gabarit de réseau
Numéro de 32 bits qui indique la gamme des adresses IP qui résident sur un seul réseau/sous-réseau/super-réseau IP. La présente spécification affiche les gabarits de réseau sous forme de nombres hexadécimaux. Par exemple, le gabarit de réseau pour un réseau IP de classe C est affiché 0xffffff00. Un tel gabarit est souvent affiché ailleurs dans les documents sous la forme 255.255.255.0.

Réseau en point à point
Réseau qui joint une seule paire de routeurs. Une ligne de série à 56 kbit/s est un exemple de réseau point à point.

Réseau de diffusion
Réseau qui prend en charge plusieurs (plus de deux) routeurs rattachés, avec la capacité d'adresser un seul message physique à tous les routeurs rattachés (diffusion). Les routeurs voisins sont découverts de façon dynamique sur ces réseaux en utilisant le protocole Hello d'OSPF. Le protocole Hello lui-même tire parti de la capacité de diffusion. Le protocole OSPF fait d'autres usages des capacités de diffusion groupée, si elles existent. Chaque paire de routeurs d'un réseau de diffusion est supposée être capable de communiquer directement. Un ethernet est un exemple de réseau de diffusion.

Réseau qui n'est pas en diffusion
Réseau qui prend en charge plusieurs routeurs (plus de deux, mais qui n'a pas de capacité de diffusion. Les routeurs voisins sont maintenus sur ces réseaux en utilisant le protocole Hello d'OSPF. Cependant, du fait de l'absence de capacité de diffusion, certaines informations de configuration peuvent être nécessaires pour aider à la découverte des voisins. Sur les réseaux qui ne sont pas en diffusion, les paquets de protocole OSPF qui sont normalement en diffusion groupée ont besoin d'être envoyés à chaque routeur voisin, l'un après l'autre. Un réseau de données public (PDN, *Public Data Network*) X.25 est un exemple de réseau qui n'est pas en diffusion. OSPF fonctionne dans un des deux modes sur les réseaux qui ne sont pas en diffusion. Le premier mode, appelé multi accès sans diffusion (NBMA, *non-broadcast multi-access*) simule le fonctionnement d'OSPF sur un réseau de diffusion. Le second mode, appelé point à multipoint, traite le réseau qui n'est pas en diffusion comme une collection de liaisons point à point. Les réseaux qui ne sont pas en diffusion sont appelés réseaux NBMA ou réseaux en point à multipoint, selon le mode de fonctionnement d'OSPF sur le réseau.

Interface
Connexion entre un routeur et un des ses réseaux de rattachement. Une interface a des informations d'état qui lui sont associées, qui sont obtenues des protocoles de couches inférieures sous-jacentes et du protocole d'acheminement lui-même. Une interface avec un réseau est associée à une seule adresse et gabarit IP (sauf si le réseau est un réseau point à point non numéroté). Une interface est parfois aussi appelée une jonction.

Routeurs voisins
Deux routeurs qui ont des interfaces à un réseau commun. Les relations de voisinage sont entretenues, et généralement découvertes de façon dynamique, par le protocole Hello de OSPF.

Adjacence
Une relation formée entre des routeurs voisins choisis pour les besoins de l'échange d'informations d'acheminement. Toutes les paires de routeurs voisins ne deviennent pas adjacentes.

Avis d'état de liaison
Unité de données qui décrit l'état local d'un routeur ou d'un réseau. Pour un routeur, cela inclut l'état des interfaces du routeur et ses adjacences. Chaque avis d'état de liaison est diffusé sur tout le domaine d'acheminement. Les avis collectés d'état de liaisons de tous les routeurs et réseaux forment la base de données d'état de liaisons du protocole. Tout au long du présent mémoire, les avis d'état de liaison sont abrégés en LSA *(link state advertisement)*.

Protocole Hello
Partie du protocole OSPF utilisée pour établir et entretenir les relations de voisinage. Sur les réseaux de diffusion, le protocole Hello peut aussi découvrir de façon dynamique les routeurs voisins.

Arrosage
Partie du protocole OSPF qui distribue et synchronise la base de données d'états de liaisons entre les routeurs OSPF.

Routeur désigné
Chaque réseau de diffusion et NBMA qui a au moins deux routeurs rattachés a un routeur désigné. Le routeur désigné génère un LSA pour le réseau et a d'autres responsabilités particulières dans le fonctionnement du protocole. Le routeur désigné est choisi par le protocole Hello. Le concept de routeur désigné permet une réduction du nombre

d'adjacences requises sur un réseau de diffusion ou NBMA. Cela à son tour réduit la quantité de trafic de protocole d'acheminement et la taille de la base de données d'états de liaisons.

Protocoles de niveau inférieur
Protocoles d'accès réseau sous-jacents qui fournissent les services au protocole Internet et, à son tour, au protocole OSPF. Des exemples en sont les niveaux de paquet et de trame X.25 pour les PDN X.25, et la couche de liaison des données ethernet pour les ethernets.

1.3 Brève histoire de la technologie de l'acheminement par état de liaison

OSPF est un protocole d'acheminement par état de liaison. De tels protocoles sont aussi appelés dans la littérature des protocoles fondés sur SPF ou des protocoles à bases de données réparties. Ce paragraphe donne une brève description des développements de la technique de l'état de liaison qui ont influencé le protocole OSPF.

Le premier protocole d'acheminement par état de liaison a été développé pour être utilisé dans le réseau commuté de paquets ARPANET. Ce protocole est décrit dans [Ref3]. Il a formé le point de départ pour tous les autres protocoles par état de liaison. L'environnement homogène de l'ARPANET, c'est-à-dire, des commutateurs de paquets d'un seul fabricant connectés par des lignes de série synchrones, simplifiait la conception et la mise en œuvre du protocole d'origine.

Des modifications à ce protocole ont été proposées dans [Ref4]. Ces modifications se rapportaient à une tolérance accrue aux fautes du protocole d'acheminement, entre autres choses, en ajoutant une somme de contrôle aux LSA (détectant par ce moyen la corruption de la base de données). Le document incluait aussi des moyens pour réduire la redondance du trafic d'acheminement dans un protocole par état de liaison. Ceci était accompli en introduisant des mécanismes qui permettaient d'accroître d'un ordre de grandeur l'intervalle de génération des LSA.

L'utilisation d'un algorithme d'état de liaison a aussi été proposée comme protocole d'acheminement ISO IS-IS. Ce protocole est décrit dans [Ref2]. Le protocole inclut des méthodes de réduction des données et du trafic d'acheminement lors du fonctionnement sur des réseaux de diffusion. Ceci est accompli en choisissant un routeur désigné pour chaque réseau de diffusion, qui génère alors un LSA pour le réseau.

Le groupe de travail OSPF de l'IETF a étendu ce travail en développant le protocole OSPF. Le concept de routeur désigné a été largement amélioré pour réduire encore la quantité de trafic d'acheminement exigé. Des capacités de diffusion groupée sont utilisées pour une réduction supplémentaire de la bande passante d'acheminement. Un schéma d'acheminement de zone a été développé pour permettre de cacher/protéger/réduire les informations. Finalement, les algorithmes ont été retouchés pour un fonctionnement efficace dans les internets TCP/IP.

1.4 Organisation du présent document

Les trois premières sections de la présente spécification donnent une vue d'ensemble générale des capacités et fonctions du protocole. Les sections 4 à 16 expliquent en détail les mécanismes du protocole. Le format des paquets, les constantes du protocole et les éléments de configuration sont spécifiés dans les appendices.

Les étiquettes comme le HelloInterval qui se rencontrent dans le texte se réfèrent aux constantes du protocole. Elles peuvent être configurables ou non. Les constantes architecturales sont récapitulées dans l'Appendice B. Les constantes configurables sont récapitulées dans l'Appendice C.

La spécification détaillée du protocole est présentée en termes de structures de données. Ceci est fait afin de rendre les explications plus précises. Les mises en œuvre du protocoles doivent prendre en charge les fonctionnalités décrites, mais ne sont pas obligées d'utiliser les structures de données précises qui apparaissent dans le présent mémoire.

1.5 Remerciements

L'auteur tient à remercier Ran Atkinson, Fred Baker, Jeffrey Burgan, Rob Coltun, Dino Farinacci, Vince Fuller, Phanindra Jujjavarapu, Milo Medin, Tom Pusateri, Kannan Varadhan, Zhaohui Zhang et le reste du groupe de travail OSPF pour les idées et le soutien qu'ils ont apportés à ce projet.
L'interface OSPF Point à MultiPoint se fonde sur les travaux de Fred Baker.
L'option OSPF d'authentification cryptographique a été développée par Fred Baker et Ran Atkinson.

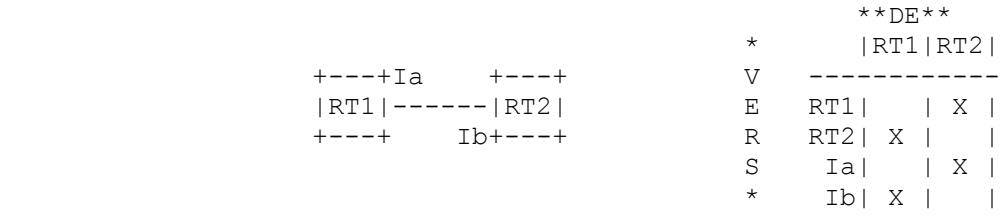
2. Base de données d'état de liaison : organisation et calculs

Les paragraphes suivants décrivent l'organisation de la base de données d'états de liaisons OSPF, et les calculs d'acheminement qui sont effectués sur la base de données afin de produire un tableau d'acheminement de routeur.

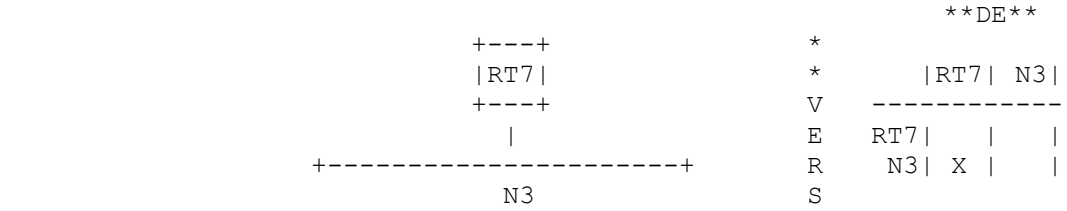
2.1 Représentation des routeurs et des réseaux

La base de données d'états de liaisons du système autonome décrit un graphe dirigé. Les vertex du graphe consistent en routeurs et en réseaux. Une case du graphe connecte deux routeurs quand ils sont rattachés via un réseau physique point à point. Une case connectant un routeur à un réseau indique que le routeur a une interface sur le réseau. Les réseaux peuvent être de transit ou des réseaux d'extrémité. Les réseaux de transit sont ceux qui sont capables de transporter du trafic de données qui n'est ni d'origine locale ni à destination locale. Un réseau de transit est représenté par un nœud du graphe ayant deux cases entrantes et sortantes. Un nœud de réseau de bout a seulement des cases entrantes.

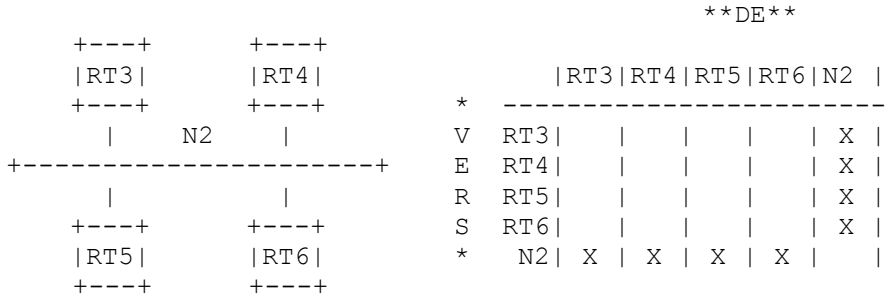
Le voisinage de chaque nœud de réseau dans le graphe dépend du type du réseau (point à point, diffusion, NBMA ou point à multipoint) et du nombre de routeurs qui ont une interface avec le réseau. Trois cas sont décrits à la Figure 1a. Les rectangles indiquent les routeurs. Les cercles et les ellipses indiquent les réseaux. Les noms des routeurs ont en préfixe les lettres RT et les noms de réseau ont la lettre N. Les noms d'interface de routeur ont en préfixe la lettre I. Les lignes entre les routeurs indiquent les réseaux point à point. Le côté gauche de la figure montre les réseaux avec les routeurs qui leurs sont connectés, avec les graphes résultants sur la droite.



Réseaux physiques point à point



Réseaux d'extrémité



Réseaux de diffusion ou NBMA

Figure 1a : Composants de cartographie de réseau

Les réseaux et les routeurs sont représenté par les vertex. Une case connecte le vertex A au vertex B si l'intersection de la colonne A et de la ligne B est marquée d'un X.

Le haut de la Figure 1a montre deux routeurs connectés par une liaison point à point. Dans le graphe résultant de base de données d'états de liaisons, les deux vertex de routeur sont directement connectés par une paire de cases, une dans chaque direction. Les interfaces de réseaux point à point n'ont pas besoin de recevoir des adresses IP. Lorsque des adresses d'interface sont allouées, elles sont modélisées comme des liaisons d'extrémité, chaque routeur notifiant une connexion d'extrémité à l'adresse d'interface de l'autre routeur. Facultativement, un sous-réseau IP peut être alloué au réseau point à

point. Dans ce cas, les deux routeurs notifient une liaison d'extrémité au sous-réseau IP, au lieu de se notifier l'un l'autre les adresses d'interface IP.

Le milieu de la Figure 1a montre un réseau avec un seul routeur rattaché (c'est-à-dire, un réseau de bout). Dans ce cas, le réseau apparaît sur la fin d'une connexion d'extrémité dans le graphe de la base de données d'états de liaisons.

Lorsque plusieurs routeurs sont rattachés à un réseau de diffusion, le graphe de la base de données d'états de liaisons montre tous les routeurs connectés en bidirectionnel au vertex de réseau. C'est ce qui est représenté au bas de la Figure 1a.

Chaque réseau (de bout ou de transit) dans le graphe a une adresse IP et un gabarit de réseau associé. Le gabarit indique le nombre de nœuds du réseau. Les hôtes rattachés directement aux routeurs (désignés comme routes d'hôtes) apparaissent sur le graphe comme réseaux de bout. Le gabarit de réseau pour une route d'hôte est toujours 0xffffffff, qui indique la présence d'un seul nœud.

2.1.1 Représentation des réseaux qui ne sont pas en diffusion

Comme mentionné précédemment, OSPF peut fonctionner sur des réseaux qui ne sont pas en diffusion d'un des deux modes, NBMA ou point à multipoint. Le choix du mode détermine la façon dont le protocole Hello et l'arrosage fonctionnent sur un réseau qui n'est pas en diffusion, et la façon dont le réseau est représenté dans la base de données d'états de liaisons.

En mode NBMA, OSPF émule le fonctionnement sur un réseau de diffusion : un routeur désigné est choisi pour le réseau NBMA, et le routeur désigné génère un LSA pour le réseau. La représentation en graphe des réseaux de diffusion et des réseaux NBMA est identique. Cette représentation est décrite dans le milieu de la Figure 1a.

Le mode NBMA est la façon la plus efficace de faire fonctionner OSPF sur les réseaux qui ne sont pas en diffusion, à la fois en termes de taille de base de données d'états de liaisons et en termes de quantité de trafic de protocole d'acheminement. Cependant, il y a une restriction significative : il exige que tous les routeurs rattachés au réseau NBMA soient capables de communiquer directement. Cette restriction peut être satisfaite sur certains réseaux qui ne sont pas en diffusion, tel qu'un sous-réseau ATM utilisant des SVC. Mais elle n'est souvent pas satisfaite sur d'autres réseaux qui ne sont pas en diffusion, tels que les réseaux en relais de trame à PVC seuls. Sur les réseaux qui ne sont pas en diffusion où tous les routeurs ne peuvent pas communiquer directement, on peut découper le réseau qui n'est pas en diffusion en sous-réseaux logiques, les routeurs de chaque sous-réseau étant capables de communiquer directement, et faire ensuite fonctionner chaque sous-réseau distinct comme un réseau NBMA (voir [Ref15]). Cela exige cependant une certaine quantité de redondance administrative, et est enclin aux mauvaises configurations. Il est probablement préférable de faire fonctionner un tel réseau de non-diffusion en mode point à multipoint.

En mode point à multipoint, OSPF traite toutes les connexions de routeur à routeur sur le réseau de non-diffusion comme si elles étaient des liaisons en point à point. Aucun routeur désigné n'est choisi pour le réseau, pas plus que n'est généré de LSA pour le réseau. En fait, il n'apparaît pas de vertex pour le réseau en point à multipoint dans le graphe de la base de données d'états de liaisons.

La Figure 1b illustre la représentation de la base de données d'états de liaisons d'un réseau en point à multipoint. Sur le côté gauche de la figure est représenté un réseau en point à multipoint. On suppose que tous les routeurs peuvent communiquer directement, excepté les routeurs RT4 et RT5. I3 à I6 indiquent les adresses IP d'interface des routeurs sur le réseau en point à multipoint. Dans la représentation graphique de la base de données d'états de liaisons, les routeurs qui peuvent communiquer directement sur le réseau en point à multipoint sont joints par des cases bidirectionnelles, et chaque routeur a aussi une connexion d'extrémité à sa propre adresse IP d'interface (à la différence de la représentation des liaisons en point à point réelles ; voir la Figure 1a).

Sur certains réseaux qui ne sont pas en diffusion, l'utilisation du mode point à multipoint et de protocoles de liaison de données tels que ARP inverse (voir [Ref14]) va permettre l'autodécouverte des voisins OSPF bien que la prise en charge de la diffusion ne soit pas disponible.

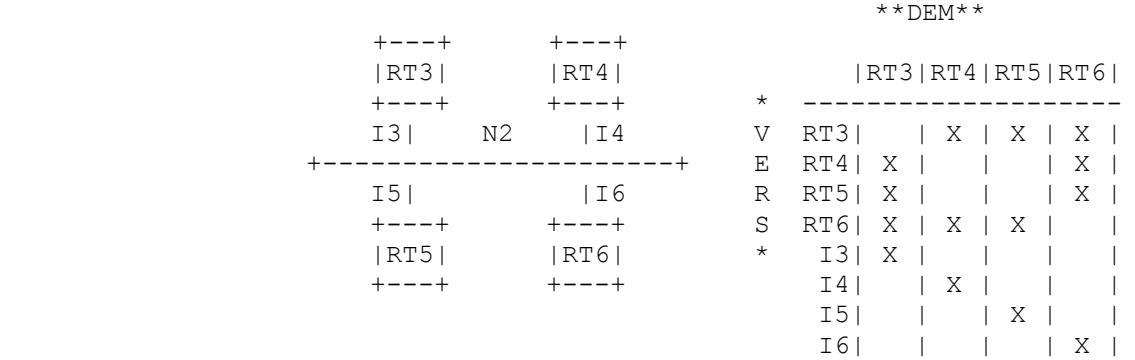


Figure 1b : Composants de cartographie des réseaux en point à multipoint

Tous les routeurs peuvent communiquer directement sur N2, sauf les routeurs RT4 et RT5. I3 à I6 indiquent les adresses IP d'interface

2.1.2 Exemple de base de données d'état de liaisonS

La Figure 2 montre un exemple de carte d'un système autonome. Le rectangle marqué H1 indique un hôte, qui a une connexion SLIP avec le routeur RT12. Le routeur RT12 notifie donc une route d'hôte. Les lignes entre les routeurs indiquent des réseaux point à point physiques. Le seul réseau point à point auquel ont été allouées des adresses d'interface est celui qui joint les routeurs RT6 et RT10. les routeurs RT5 et RT7 ont des connexions BGP avec les autres systèmes autonomes. Un ensemble de chemins appris par BGP a été affiché pour ces deux routeurs.

Un coût est associé au côté sortie de chaque interface de routeur. Ce coût est configurable par l'administrateur de système. Moins le coût est élevé, plus grande est la probabilité que l'interface soit utilisée pour transmettre du trafic de données. Les coûts sont aussi associés aux données d'acheminement d'acquisition externe (par exemple, les chemins appris par BGP).

Le graphe résultant de la carte de la Figure 2 est décrit à la Figure 3. Les arcs sont marqués avec le coût de l'interface de sortie du routeur correspondant. Les arcs qui n'ont pas de coût marqué ont un coût de 0. Noter que les arcs qui conduisent des réseaux aux routeurs ont toujours un coût de 0 ; ils ont néanmoins une signification. Noter aussi que les données d'acheminement d'importation apparaissent en bout de graphe.

La base de données d'états de liaisons est accolée aux LSA générés par les routeurs. Dans la représentation graphique associée, le voisinage de chaque routeur ou réseau de transit est représenté dans un seul LSA, séparé. La Figure 4 montre graphiquement ces LSA. Le routeur RT12 a une interface avec deux réseaux de diffusion et une ligne SLIP avec un hôte. Le réseau N6 est un réseau de diffusion avec trois routeurs rattachés. Le coût de toutes les liaisons du réseau N6 à ses routeurs rattachés est 0. Noter que le LSA pour le réseau N6 est en réalité généré par un des routeurs rattachés du réseau : le routeur qui a été élu routeur désigné pour le réseau.

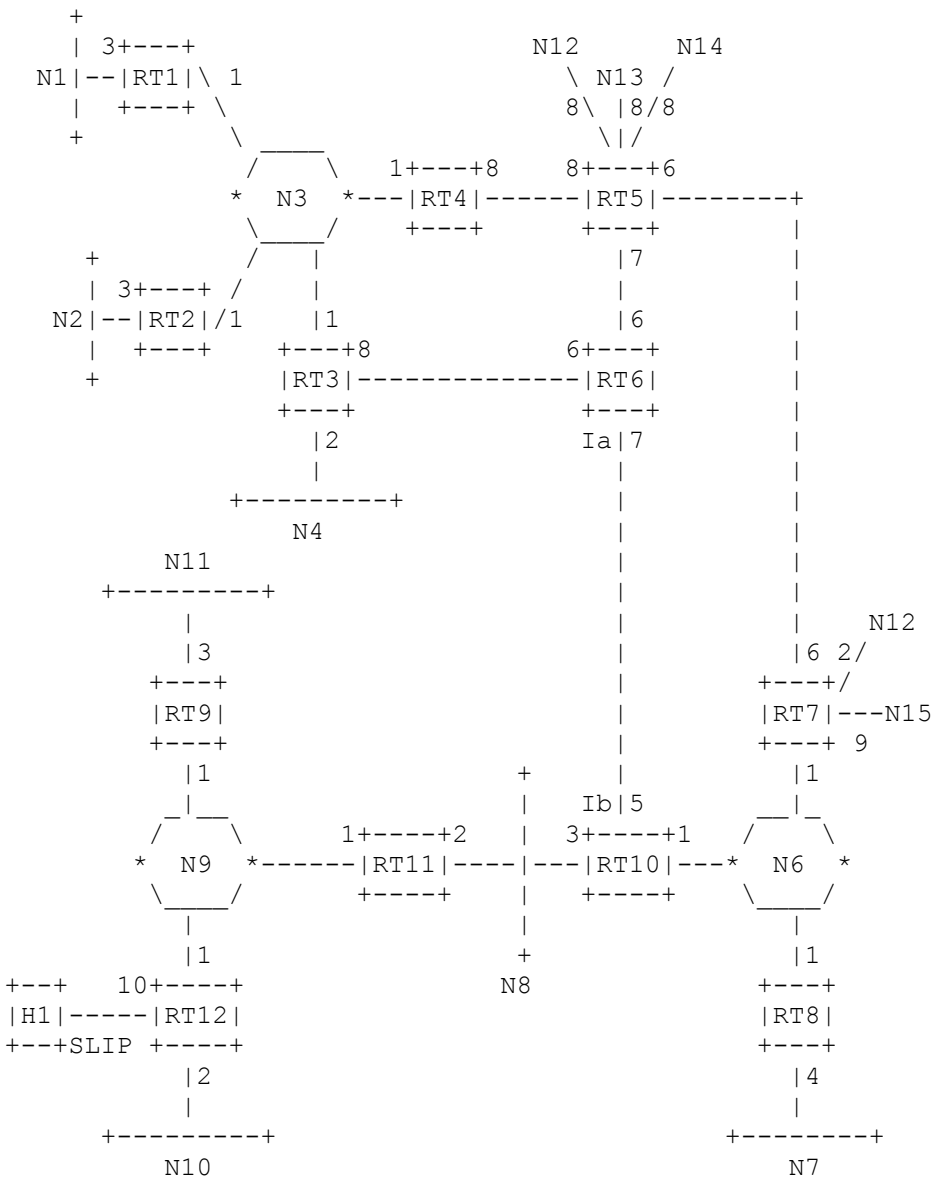


Figure 2 : Exemple de système autonome

DE/ VERS	RT1	RT2	RT3	RT4	RT5	RT6	RT7	RT8	RT9	RT10	RT11	RT12	N3	N6	N8	N9
RT1													0			
RT2													0			
RT3						6							0			
RT4					8								0			
RT5				8		6	6									
RT6			8		7					5						
RT7					6									0		
RT8														0		
RT9																0
RT10						7								|0	0	
RT11															0	0
RT12																0
N1	3															
N2		3														
N3	1	1	1	1												
N4			2													
N6							1	1		1						
N7								4								
N8										3	2					
N9									1		1	1				
N10												2				
N11									3							
N12					8		2									
N13					8											
N14					8											
N15							9									
H1												10				

Figure 3: Graphe dirigé résultant

Les réseaux et routeurs sont représentés par les vertex. Une ligne de coût X connecte le vertex A au vertex B si l'intersection de la colonne A et de la rangée B est marquée d'un X.

DE/ VERS	RT12	N9	N10	H1
RT12				
N9	1			
N10	2			
H1	10			

LSA de routeur de RT12

DE/ VERS	RT9	RT11	RT12	N9
RT9				0
RT11				0
RT12				0
N9				

Figure 4 : Composants d'état de liaison individuelle

Les réseaux et routeurs sont représenté par les vertex. Une ligne de coût X connecte le vertex A au vertex B si l'intersection de la colonne A et de la rangée B est marquée d'un X.

2.2 Arbre des plus courts chemins

Quand aucune zone OSPF n'est configurée, chaque routeur du système autonome a une base de données d'états de liaisons identique, ce qui conduit à une représentation graphique identique. Un routeur génère son tableau d'acheminement à partir de ce graphe en calculant un arbre des plus courts chemins avec le routeur lui-même comme racine. Évidemment, l'arbre des plus courts chemins dépend du routeur qui fait le calcul. L'arbre des plus courts chemins pour le routeur RT6 de notre exemple est décrit à la Figure 5.

L'arbre donne le chemin entier pour tout réseau ou hôte de destination. Cependant, seul le prochain bond vers la destination

est utilisé dans le processus de transmission. Noter aussi que le meilleur chemin pour tout routeur a aussi été calculé. Pour le traitement des données externes, on note le prochain bond et la distance vers chaque routeur qui annonce des chemins externes. Le tableau d'acheminement qui en résulte pour le routeur RT6 est décrit dans le Tableau 2. Noter qu'il y a un chemin distinct pour chaque extrémité d'un réseau point à point numéroté (dans ce cas, les lignes de série entre les routeurs RT6 et RT10).

Les chemins pour des réseaux qui appartiennent à d'autres AS (tels que N12) apparaissent en lignes pointillées dans l'arbre des plus courts chemins de la Figure 5. L'utilisation de ces conformations d'acheminement importées est examinée dans le paragraphe suivant.

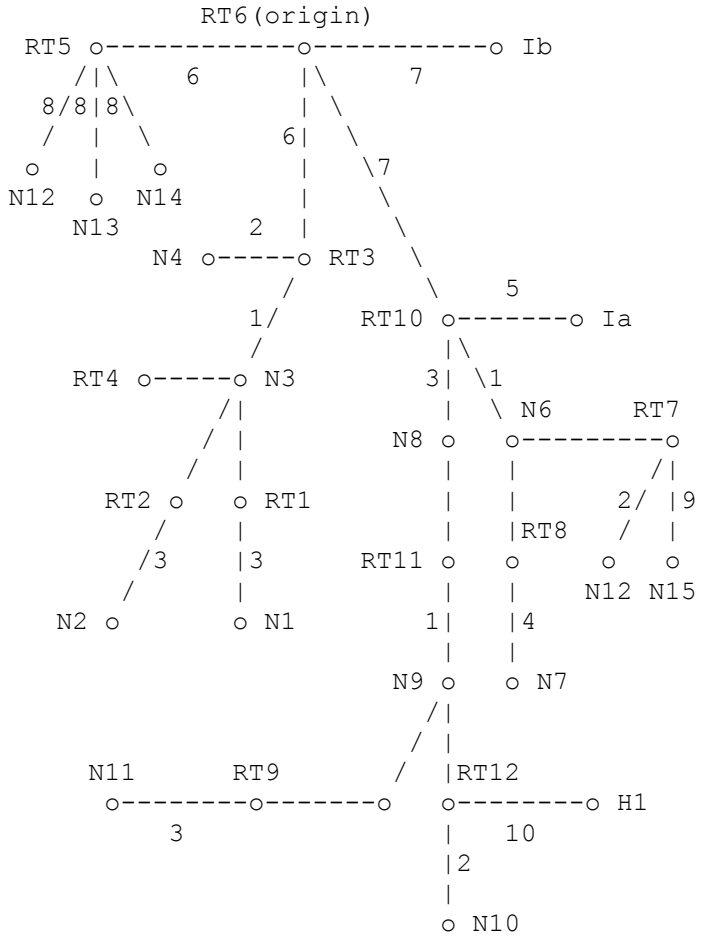


Figure 5 : Arbre SPF pour le routeur RT6

Les cases qui ne sont pas marquées avec un coût ont un coût de zéro (ce sont les liaisons de réseau à routeur). Les chemins pour les réseaux N12-N15 sont des informations externes qui sont examinées au paragraphe 2.3

Destination	Prochain bond	Distance
N1	RT3	10
N2	RT3	10
N3	RT3	7
N4	RT3	8
Ib	*	7
Ia	RT10	12
N6	RT10	8
N7	RT10	12
N8	RT10	10
N9	RT10	11
N10	RT10	13
N11	RT10	14
H1	RT10	21
RT5	RT5	6
RT7	RT10	8

Tableau 2 : Liste des destinations locales du tableau d'acheminement de la portion du routeur RT6.

2.3. Utilisation des informations d'acheminement externes

Après la création de l'arbre, les informations d'acheminement externes sont examinées. Ces informations d'acheminement externes peuvent provenir d'un autre protocole d'acheminement tel que BGP, ou être configurées de façon statique (chemins statiques). Les chemins par défaut peuvent aussi être inclus au titre des informations d'acheminement externes du système autonome.

Les informations d'acheminement externes s'écoulent sans altération dans tout l'AS. Dans notre exemple, tous les routeurs de notre système autonome savent que le routeur RT7 a deux chemins externes, avec les métriques 2 et 9.

OSPF prend en charge deux types de métriques externes. Les métriques externes de type 1 sont exprimées dans les mêmes unités que le coût d'une interface OSPF (c'est-à-dire, en termes de métrique d'état de liaison). Les métriques externes de type 2 sont d'un ordre de grandeur plus élevé ; toute métrique de type 2 est considérée comme supérieure au coût de tout chemin interne à l'AS. L'utilisation des métriques externes de type 2 suppose que l'acheminement entre les AS est le coût d'acheminement majeur d'un paquet, et élimine le besoin de conversion des coûts externes en métrique d'état de liaison interne.

À titre d'exemple de traitement de métrique externe de type 1, supposons que les routeurs RT7 et RT5 de la Figure 2 annoncent des métriques externes de type 1. Pour chaque chemin externe annoncé, le coût total à partir du routeur RT6 est calculé comme la somme des coûts de chemin externe annoncés et de la distance du routeur RT6 au routeur qui annonce. Lorsque deux routeurs annoncent la même destination externe, RT6 prend le routeur annonceur qui fournit le coût total minimum. RT6 règle alors le prochain bond à la destination externe égale au prochain bond qui sera utilisé lors de l'acheminement de paquets pour le routeur annonceur choisi.

Dans la Figure 2, les routeurs RT5 et RT7 annoncent tous deux un chemin externe pour le réseau de destination N12. Le routeur RT7 est préféré car il annonce N12 à une distance de 10 (8+2) au routeur RT6, ce qui est mieux que le 14 (6+8) du routeur RT5. Le Tableau 3 montre les entrées qui sont ajoutées au tableau d'acheminement lorsque des chemins externes sont examinés :

Destination	Prochain bond	Distance
N12	RT10	10
N13	RT5	14
N14	RT5	14
N15	RT10	17

Tableau 3 : Liste des destinations externes du tableau d'acheminement de la portion du routeur RT6.

Le traitement des métriques externes de type 2 est plus simple. Le routeur frontière de l'AS qui annonce la plus petite métrique externe est choisi, sans considération de la distance interne au routeur frontière de l'AS. Supposons dans notre exemple que les deux routeurs RT5 et RT7 annoncent des chemins externes de type 2. Tout le trafic destiné alors au réseau N12 serait transmis au routeur RT7, car 2 < 8. Lorsque plusieurs chemins de type 2 d'égal coût existent, la distance interne aux routeurs annonceurs est utilisée pour les départager.

Les deux métriques externes de type 1 et de type 2 peuvent être présentes dans l'AS au même moment. Dans ce cas, les métriques externes de type 1 ont toujours la préséance.

Ce paragraphe a supposé que les paquets pour les destinations externes sont toujours acheminés à travers le routeur frontière annonceur de l'AS. Cela n'est pas toujours souhaitable. Par exemple, supposons qu'il y ait dans la Figure 2 un routeur supplémentaire rattaché au réseau N6, appelé routeur RTX. Supposons de plus que RTX ne participe pas à l'acheminement OSPF, mais échange des informations BGP avec le routeur frontière de l'AS RT7. Alors, le routeur RT7 finirait par annoncer les chemins externes OSPF pour toutes les destinations qui devraient être acheminées à RTX. Un bond supplémentaire sera parfois introduit si les paquets pour ces destinations doivent toujours être acheminées d'abord par le routeur RT7 (le routeur annonceur).

Pour régler cette situation, le protocole OSPF permet à un routeur frontière de l'AS de spécifier une "adresse de transmission" dans ses LSA externes à l'AS. Dans l'exemple ci-dessus, le routeur RT7 spécifierait l'adresse IP de RTX comme "adresse de transmission" pour toute destination dont les paquets devraient être acheminés directement à RTX.

L'adresse de transmission a une autre application. Elle permet aux routeurs à l'intérieur du système autonome de fonctionner comme des "serveurs d'acheminement". Par exemple, dans la Figure 2 le routeur RT6 pourrait devenir un serveur d'acheminement, obtenant des informations d'acheminement externes à travers une combinaison de configurations statiques et de protocoles d'acheminement externes. RT6 commencerait alors à s'annoncer lui-même comme un routeur frontière de l'AS, et génèrerait une collection de LSA externes à l'AS OSPF. Dans chaque LSA externe à l'AS, le routeur RT6 spécifierait le point de sortie correct du système autonome à utiliser pour la destination par le réglage approprié du champ "adresse de transmission" du LSA.

2.4 Plusieurs chemins de coût égal

L'exposé ci-dessus a été simplifié en ne considérant qu'un seul chemin pour toute destination. En réalité, si plusieurs chemins à coût égal existent pour une destination, ils sont tous découverts et utilisés. Cela n'exige aucun changement conceptuel de l'algorithme, et sa discussion est retardée jusqu'à ce qu'on ait examiné plus en détail le processus de construction de l'arbre.

Avec plusieurs chemins de coût égal, un routeur a plusieurs prochains bonds potentiels disponibles pour toute destination donnée.

3. Partage de l'AS en zones

OSPF permet que des collections de réseaux et hôtes contigus se groupent ensemble. Un tel groupe, les routeurs ayant des interfaces avec tous les réseaux inclus, s'appelle une zone. Chaque zone détient une copie distincte de l'algorithme d'acheminement par état de liaisons. Cela signifie que chaque zone a sa propre base de données d'états de liaisons et de graphes correspondants, comme expliqué dans la section précédente.

La topologie d'une zone est invisible de l'extérieur de la zone. À l'inverse, les routeurs internes à une zone donnée ne savent rien de la topologie détaillée externe à la zone. Cet isolement des connaissances permet au protocole d'effectuer une réduction marquée du trafic d'acheminement par rapport au traitement du système autonome entier comme un seul domaine d'état de liaisons.

Avec l'introduction des zones, il n'est plus vrai que tous les routeurs dans l'AS aient une base de données d'états de liaisons identique. Un routeur a en réalité une base de données d'états de liaisons distincte pour chaque zone à laquelle il est connecté. (Les routeurs connectés à plusieurs zones sont appelés des routeurs frontière de zone). Deux routeurs appartenant à la même zone ont, pour cette zone, des bases de données d'états de liaisons de zone identiques.

Dans le système autonome, l'acheminement a lieu à deux niveaux, selon que la source et la destination d'un paquet résident dans la même zone (l'acheminement intra-zone est utilisé) ou dans des zones différentes (l'acheminement inter-zone est utilisé). Dans l'acheminement intra-zone, le paquet est acheminé seulement sur les informations obtenues au sein de la zone ; aucune information d'acheminement obtenue de l'extérieur de la zone ne peut être utilisée. Cela protège l'acheminement intra-zone contre l'injection de mauvaises informations d'acheminement. L'acheminement inter-zone est exposé au paragraphe 3.2.

3.1 Le cœur de réseau du système autonome

Le cœur de réseau OSPF est la zone OSPF spéciale 0 (souvent écrite Zone 0.0.0.0, car les identifiants de zone OSPF sont normalement formatés comme des adresses IP). Le cœur de réseau OSPF contient toujours tous les routeurs frontières de zone. Le cœur de réseau est chargé de la distribution des informations d'acheminement entre les zones non cœur de réseau. Le cœur de réseau doit être contigu. Cependant, il n'a pas besoin d'être physiquement contigu ; la connexité du cœur de réseau peut être établie/entretenue par la configuration de liaisons virtuelles.

Les liaisons virtuelles peuvent être configurées entre deux routeurs cœur de réseau quelconques qui ont une interface avec une zone non cœur de réseau commune. Les liaisons virtuelles appartiennent au cœur de réseau. Le protocole traite deux routeurs joins par une liaison virtuelle comme si ils étaient connectés par un cœur de réseau point à point non numéroté. Sur le graphe du cœur de réseau, deux routeurs de cette sorte sont joints par des arcs dont le coût est la distance intra-zone entre les deux routeurs. Le trafic de protocole d'acheminement qui s'écoule sur la liaison virtuelle utilise seulement l'acheminement intra-zone.

3.2 Acheminement inter-zone

Lors de l'acheminement d'un paquet entre deux zones non cœur de réseau, le cœur de réseau est utilisé. Le chemin que va suivre le paquet peut être séparé en trois parties contiguës : un chemin intra-zone de la source à un routeur frontière de zone, un chemin de cœur de réseau entre les zones de source et de destination, et puis un autre chemin intra-zone jusqu'à la destination. L'algorithme trouve l'ensemble de ces chemins qui a le plus faible coût.

Sous un autre angle de vue, l'acheminement inter-zone peut être décrit comme forçant une configuration en étoile du système autonome, avec le cœur de réseau comme pivot et chaque zone non cœur de réseau comme branche.

La topologie du cœur de réseau dicte les chemins de cœur de réseau utilisés entre les zones. La topologie du cœur de réseau peut être améliorée en ajoutant des liaisons virtuelles. Cela donne à l'administrateur de système un certain contrôle sur les chemins pris par le trafic inter-zone.

Le routeur frontière de zone correct à utiliser lorsque le paquet sort de la zone de source est choisi exactement de la même façon que sont choisis les routeurs qui annoncent les chemins externes. Chaque routeur frontière de zone dans une zone résume pour la zone son coût vers tous les réseaux externes à la zone. Après le calcul de l'arbre SPF pour la zone, les chemins vers toutes les destinations inter-zone sont calculés en examinant les résumés des routeurs frontière de zone.

3.3 Classification des routeurs

Avant l'introduction des zones, les seuls routeurs OSPF ayant une fonction spécialisée étaient ceux qui annoncent les informations d'acheminement externes, tels que le routeur RT5 de la Figure 2. Lorsque l'AS est partagée en zones OSPF, les routeurs sont encore divisés selon la fonction entre les quatre catégories suivantes qui se chevauchent :

Routeur interne
: Un routeur dont tous les réseaux directement connectés appartiennent à la même zone. Ces routeurs ont une seule copie de l'algorithme d'acheminement de base.

Routeur frontière de zone
: Un routeur qui se rattache à plusieurs zones. Les routeurs frontière de zone ont plusieurs copies de l'algorithme de base, une copie pour chaque zone de rattachement. Les routeurs frontière de zone condensent les informations topologiques de leurs zones de rattachement pour leur distribution au cœur de réseau. Le cœur de réseau à son tour distribue les informations aux autres zones.

Routeur de cœur de réseau
: Un routeur qui a une interface avec la zone cœur de réseau. Cela inclut tous les routeurs qui ont une interface avec plus d'une zone (c'est-à-dire, les routeurs frontière de zone). Cependant, les routeurs cœur de réseau ne sont pas obligatoirement des routeurs frontière de zone. Les routeurs avec toutes les interfaces se connectant à la zone cœur de réseau sont acceptés.

Routeur frontière de l'AS
: Un routeur qui échange des informations d'acheminement avec les routeurs appartenant à d'autres systèmes autonomes. Un tel routeur annonce les informations d'acheminement d'AS externes dans tout le système autonome. Les chemins vers chaque routeur frontière de l'AS sont connus de tout routeur dans l'AS. Cette classification est complètement indépendante de la précédente classification : les routeurs frontières de l'AS peuvent être internes ou routeurs frontières

de zone, et peuvent ou non participer au cœur de réseau.

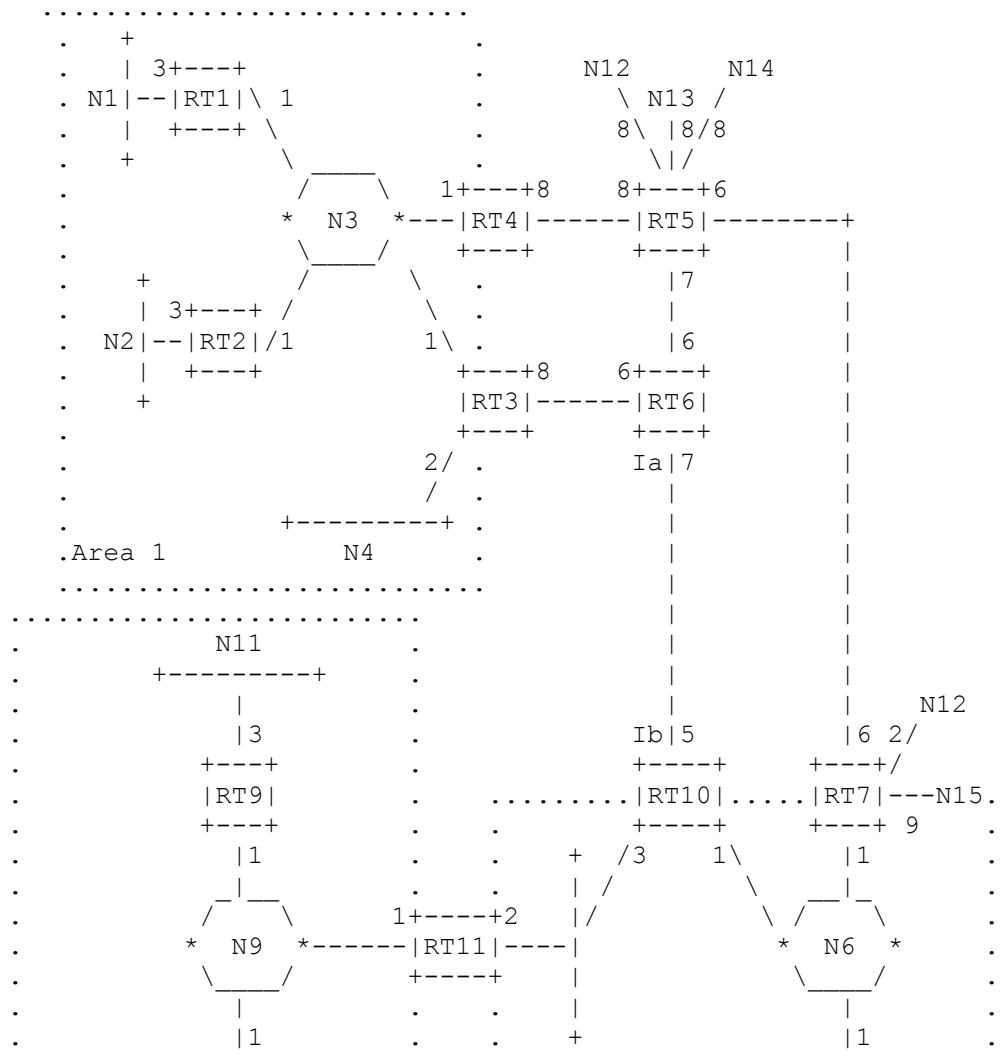
3.4 Exemple de configuration de zone

La Figure 6 donne un exemple de configuration de zone. La première zone comporte les réseaux N1-N4, ainsi que leurs routeurs rattachés RT1-RT4. La seconde zone comporte les réseaux N6-N8, ainsi que leurs routeurs rattachés RT7, RT8, RT10 et RT11. La troisième zone comporte les réseaux N9-N11 et l'hôte H1, ainsi que leurs routeurs rattachés RT9, RT11 et RT12. La troisième zone a été configurée de telle sorte que les réseaux N9-N11 et l'hôte H1 soient tous groupés sur un seul chemin, pour les annonces externes à la zone (voir des précisions au paragraphe 3.5).

Dans la Figure 6, les routeurs RT1, RT2, RT5, RT6, RT8, RT9 et RT12 sont des routeurs internes. les routeurs RT3, RT4, RT7, RT10 et RT11 sont des routeurs frontières de zone. Finalement, comme auparavant, les routeurs RT5 et RT7 sont des routeurs frontières de l'AS.

La Figure 7 montre la base de données d'états de liaisons résultante pour la zone 1. La figure décrit complètement l'acheminement intra-zone de cette zone. Elle montre aussi la vue complète de l'internet des deux routeurs internes RT1 et RT2. C'est le travail des routeurs frontières de zone, RT3 et RT4, d'annoncer dans la zone 1 les distances à toutes les destinations externes à la zone. Elles sont indiquées à la Figure 7 par les bouts de chemins en pointillés. RT3 et RT4 doivent aussi annoncer dans la zone 1 la localisation des routeurs frontières RT5 et RT7 de l'AS. Finalement, les LSA externes de l'AS à partir de RT5 et RT7 sont répandus dans l'AS entier, et en particulier dans la zone 1. Ces LSA sont inclus dans la base de données de la zone 1, et donnent les chemins des réseaux N12-N15.

Les routeurs RT3 et RT4 doivent aussi récapituler la topologie de la zone 1 pour la distribuer au cœur de réseau. Leurs LSA de cœur de réseau sont indiqués au Tableau 4. Ces récapitulations montrent quels réseaux sont contenus dans la zone 1 (c'est-à-dire, les réseaux N1-N4), et la distance à ces réseaux depuis, respectivement, les routeurs RT3 et RT4.



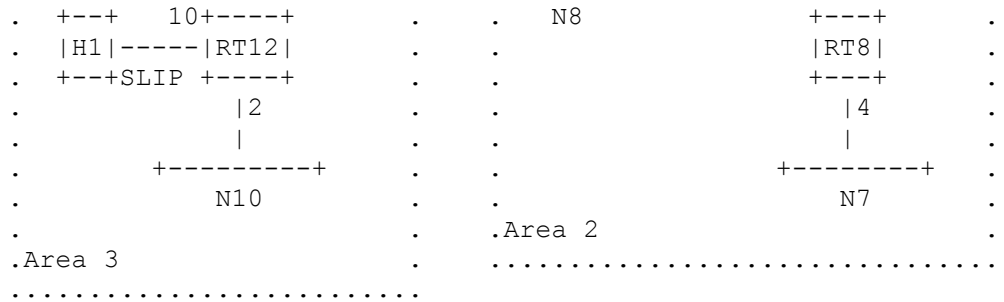


Figure 6 : Exemple de configuration de zone OSPF

La base de données d'états de liaisons pour le cœur de réseau est montrée à la Figure 8. L'ensemble de routeurs décrit est celui des routeurs cœur de réseau. Le routeur RT11 est routeur de cœur de réseau parce qu'il appartient aux deux zones. Afin de connecter le cœur de réseau, une liaison virtuelle a été configurée entre les routeurs R10 et R11.

Les routeurs frontières de zone RT3, RT4, RT7, RT10 et RT11 condensent les informations d'acheminement de leurs zones non cœur de réseau rattachées pour les distribuer via le cœur de réseau ; ce sont les bouts avec un tiret qui apparaissent à la Figure 8. Se souvenir que la troisième zone a été configurée pour condenser les réseaux N9-N11 et l'hôte H1 en un seul chemin. Cela donne une seule ligne en tirets pour les réseaux N9-N11 et l'hôte H1 sur la Figure 8. Les routeurs RT5 et RT7 sont des routeurs frontières de l'AS ; leurs informations importées apparaissent aussi sur le graphe de la Figure 8 comme des bouts.

Réseau	**Annonce de RT3**	**Annonce de RT4**
N1	4	4
N2	4	4
N3	1	1
N4	2	3

Tableau 4 : Réseaux annoncés au cœur de réseau par les routeurs RT3 et RT4.

DE/ VERS	RT1	RT2	RT3	RT4	RT5	RT7	N3
RT1							0
RT2							0
RT3							0
RT4							0
RT5			14	8			
RT7		20	14				
N1	3						
N2		3					
N3	1	1	1	1			
N4			2				
Ia,Ib			20	27			
N6			16	15			
N7			20	19			
N8			18	18|		
N9-N11,H1			29	36			
N12					8	2	
N13					8		
N14					8		
N15						9	

Figure 7 : Base de données de la zone 1.

Les réseaux et les routeurs sont représentés par les vertex. Une case de coût X connecte le vertex A au vertex B si l'intersection de la colonne A et de la rangée B est marquée d'un X.

DE/ VERS	RT3	RT4	RT5	RT6	RT7	RT10	RT11
RT3				6			
RT4			8				
RT5		8		6	6		
RT6	8		7			5	
RT7			6				
RT10				7			2
RT11						3	
N1	4	4					
N2	4	4					
N3	1	1					
N4	2	3					
Ia						5	
Ib				7			
N6					1	1	3
N7					5	5	7
N8					4	3	2
N9-N11, H1							11
N12			8		2		
N13			8				
N14			8				
N15					9		

Figure 8 : Base de données du cœur de réseau.

Les réseaux et les routeurs sont représentés par les vertex. Une case de coût X connecte le vertex A au vertex B si l'intersection de la colonne A et de la rangée B est marquée d'un X.

Le cœur de réseau permet l'échange de résumés d'informations entre routeurs frontières de zone. Chaque routeur frontière de zone écoute les résumés de zone provenant de tous les autres routeurs frontières de zone. Il se forme alors un tableau des distances de tous les réseaux en dehors de sa zone en examinant les LSA collectés, et en ajoutant la distance au cœur de réseau à chaque routeur annonceur.

En utilisant à nouveau les routeurs RT3 et RT4 comme exemple, la procédure se déroule comme suit : ils calculent d'abord l'arbre SPF pour le cœur de réseau. Cela donne les distances à tous les autres routeurs frontières de zone. Sont aussi notées les distances aux réseaux (Ia et Ib) et routeurs frontières de l'AS (RT5 et RT7) qui appartiennent au cœur de réseau. Ce calcul est montré au Tableau 5.

Ensuite, en regardant les résumés de zone provenant de ces routeurs frontières de zone, RT3 et RT4 peuvent déterminer la distance à tous les réseaux en dehors de leur zone. Ces distances sont alors annoncées en interne à la zone par RT3 et RT4. Les annonces que les routeurs RT3 et RT4 vont faire dans la zone 1 sont montrées au Tableau 6. Noter que le Tableau 6 suppose qu'un territoire de zone a été configuré pour le cœur de réseau qui groupe Ia et Ib en un seul LSA.

Les informations importées dans la zone 1 par les routeurs RT3 et RT4 permettent à un routeur interne, tel que RT1, de choisir intelligemment un routeur frontière de zone. Le routeur RT1 utiliserait RT4 pour le trafic vers le réseau N6, RT3 pour le trafic vers le réseau N10, et ferait un partage de charge entre les deux pour le trafic vers le réseau N8.

	Distance de RT3	Distance de RT4
à RT3	*	21
à RT4	22	*
à RT7	20	14
à RT10	15	22
à RT11	18	25
à Ia	15	22
à Ib	20	27
à RT5	14	8
à RT7	20	14

Tableau 5 : Distances de cœur de réseau calculées par les routeurs RT3 et RT4.

Destination	Annonce de RT3	Annonce de RT4
Ia,Ib	20	27
N6	16	15
N7	20	19
N8	18	18
N9-N11,H1	29	36
RT5	14	8
RT7	20	14

Tableau 6 : Destinations annoncées dans la zone 1 par les routeurs RT3 et RT4.

Le routeur RT1 peut aussi déterminer de cette manière le chemin le plus court pour les routeurs frontières de l'AS RT5 et RT7. Puis, en regardant les LSA externe d'AS de RT5 et RT7, le routeur RT1 peut décider entre RT5 ou RT7 lorsqu'il envoie à une destination d'un autre système autonome (un des réseaux N12-N15).

Noter qu'une défaillance de ligne entre les routeurs RT6 et RT10 causera la déconnexion du cœur de réseau. Configurer une liaison virtuelle entre les routeurs RT7 et RT10 donnera au cœur de réseau plus de connexité et plus de résistance à de telles défaillances.

3.5 Prise en charge du sous-réseautage IP

OSPF rattache un gabarit d'adresse IP à chaque chemin annoncé. Le gabarit indique la gamme d'adresses décrites par ce chemin particulier. Par exemple, un LSA de résumé pour la destination 128.185.0.0 avec un gabarit de 0xffff0000 décrit en réalité un seul chemin pour la collection de destinations 128.185.0.0 - 128.185.255.255. De même, les chemins d'hôtes sont toujours annoncés avec un gabarit de 0xffffffff, qui indique la présence d'une seule destination.

Inclure le gabarit à chaque destination annoncée permet la mise en œuvre de ce qu'on appelle communément le sous-réseautage à longueur variable. Cela signifie qu'un seul numéro de réseau IP de classe A, B, ou C peut être subdivisé en nombreux sous-réseaux de tailles variables. Par exemple, le réseau 128.185.0.0 pourrait être coupé en 62 sous-réseaux de taille variable : 15 sous-réseaux de taille 4 000, 15 sous-réseaux de taille 256, et 32 sous-réseaux de taille 8. Le Tableau 7 montre quelques adresses résultantes avec leur gabarit.

Adresse réseau	Gabarit d'adresse IP	Taille de sous-réseau
128.185.16.0	0xfffff000	4 000
128.185.1.0	0xffffff00	256
128.185.0.8	0xfffffff8	8

Tableau 7 : Exemples de taille de sous-réseau.

Il y a de nombreuses façons possibles de diviser un réseau de classe A, B, et C en sous-réseaux de tailles variables. La procédure précise pour le faire sort du domaine d'application de la présente spécification. Elle établit cependant les lignes directrices suivantes : lorsqu'un paquet IP est transmis, il est toujours transmis au réseau qui a la meilleure correspondance pour la destination du paquet. Ici, meilleure correspondance est synonyme de plus longue correspondance ou de correspondance la plus spécifique. Par exemple, le chemin par défaut avec la destination de 0.0.0.0 et le gabarit de 0x00000000 est toujours une correspondance pour toutes les destinations IP. Et il est donc toujours moins spécifique que toute autre correspondance. Les gabarits de sous-réseaux doivent être alloués de telle sorte que la meilleure correspondance pour toute destination IP soit sans ambiguïté.

Rattacher un gabarit d'adresse à chaque chemin permet aussi de prendre en charge le super-réseautage IP. Par exemple, un seul segment de réseau physique pourrait se voir allouer la paire [adresse,gabarit] [192.9.4.0,0xfffffc00]. Le segment serait alors un seul réseau IP, contenant les adresses provenant des quatre numéros de réseau de classe C consécutifs 192.9.4.0 à 192.9.7.0. Un tel adressage devient maintenant très courant avec l'avènement de CIDR (voir [Ref10]).

Afin d'avoir une meilleure agrégation aux frontières de zone, on peut utiliser les gammes d'adresse de zone (voir les détails au paragraphe C.2). Chaque gamme d'adresses est définie comme paire [adresse,gabarit]. De nombreux réseaux séparés peuvent donc être contenus dans une seule gamme d'adresse, exactement comme un réseau organisé en sous-réseaux est composé de nombreux sous-réseaux séparés. Les routeurs frontières de zone récapitulent alors le contenu de la zone (pour distribution au cœur de réseau) en annonçant un seul chemin pour chaque gamme d'adresse. Le coût du chemin est le coût maximum vers tout réseau tombant dans la gamme spécifiée.

Par exemple, un réseau IP organisé en sous-réseaux pourrait être configuré comme une seule zone OSPF. Dans ce cas, une seule gamme d'adresses pourrait être configurée : un numéro de réseau de classe A, B, ou C ainsi que son gabarit IP

naturel. À l'intérieur de la zone, tout numéro de sous-réseau de taille variable pourrait être défini. Cependant, en externe à la zone serait distribué un seul chemin pour le réseau subdivisé en sous-réseaux tout entier, cachant même le fait que le réseau est en sous-réseaux. Le coût de ce chemin est le maximum de l'ensemble des coûts des sous-réseaux composants.

3.6 Prise en charge des zones de bout

Dans certains système autonomes, la majorité des bases de données d'états de liaison peut consister en LSA externes à l'AS. Un LSA externe à l'AS d'OSPF est habituellement écoulé dans tout l'AS. Cependant, OSPF permet que certaines zones soient configurées comme "zones de bout". Les LSA externes à l'AS ne sont pas écoulés dans les zones de bout ; L'acheminement vers des destinations externes à l'AS dans ces zones est seulement par défaut (par zone). Cela réduit la taille de la base de données d'états de liaisons, et donc les exigences de mémoire pour les routeurs internes d'une zone de bout.

Pour tirer parti de la prise en charge de la zone de bout par OSPF, l'acheminement par défaut doit être utilisé dans la zone de bout. Cela se fait de la façon suivante. Un ou plusieurs routeurs frontières de zone de la zone de bout doivent annoncer un chemin par défaut dans la zone de bout via des LSA de résumés. Ces résumés par défaut sont écoulés partout dans la zone de bout, mais pas au delà. (Pour cette raison ces résumés par défaut appartiennent seulement à cette zone de bout particulière). Ces résumés de chemins par défaut seront utilisés pour toute destination qui n'est pas explicitement joignable par un chemin intra-zone ou inter-zone (c'est-à-dire, des destinations externes à l'AS).

Une zone peut être configurée comme bout lorsqu'il y a un seul point de sortie de la zone, ou quand le choix du point de sortie n'a pas besoin d'être fait sur la base de la destination externe. Par exemple, la zone 3 de la Figure 6 pourrait être configurée comme zone de bout, parce que tout le trafic externe doit passer à travers son seul routeur frontière de zone RT11. Si la zone 3 était configurée comme un bout, le routeur RT11 annoncerait un chemin par défaut pour la distribution à l'intérieur de la zone 3 (dans un LSA de résumé), au lieu d'écouler des LSA externes à l'AS pour les réseaux N12-N15 partout dans la zone.

Le protocole OSPF garantit que tous les routeurs appartenant à une zone sont d'accord sur le fait que la zone a été configurée comme bout. Cela garantit qu'il n'y aura pas de confusion lors de l'écoulement des LSA externes à l'AS.

Il y a deux restrictions à l'utilisation des zones de bout. Les liaisons virtuelles ne peuvent pas être configurées à travers des zones de bout, et les routeurs frontières de l'AS ne peuvent pas être placés à l'intérieur des zones de bout.

3.7 Partitions des zones

OSPF ne tente pas activement de réparer les partitions de zone. Quand une partition survient dans une zone, chaque composant devient simplement une zone distincte. Le cœur de réseau effectue alors l'acheminement entre les nouvelles zones. Certaines destinations joignables avant la partition via l'acheminement intra-zone exigeront dorénavant l'acheminement inter-zone.

Cependant, afin de maintenir le bon fonctionnement de l'acheminement après la partition, une gamme d'adresses ne doit pas être éclatée sur plusieurs composants de la partition de zone. De même, le cœur de réseau lui-même ne doit pas être partagé. S'il l'est, des parties du système autonome deviendront injoignables. Les partitions de cœur de réseau peuvent être repérées par la configuration de liaisons virtuelles (voir la Section 15).

Une autre façon de voir les partitions de zone est de regarder le graphe du système autonome qui a été introduit à la Section 2. Les identifiants de zone peuvent être vus comme des couleurs pour les bordures du graphe[1]. Chaque bord du graphe connecte à un réseau, ou est lui-même un réseau point à point. Dans les deux cas, le bord est coloré avec l'identifiant de zone du réseau.

Un groupe de bords, ayant tous la même couleur, et interconnectés par les vertex, représente une zone. Si la topologie du système autonome est intacte, le graphe aura plusieurs régions colorées, chaque couleur ayant un identifiant de zone distinct.

Lorsque la topologie de l'AS change, une des zones peut être éclatée. Le graphe de l'AS aura alors plusieurs régions de la même couleur (identifiant de zone). L'acheminement dans le système autonome continuera de fonctionner tant que ces régions de même couleur sont connectées par une seule région de cœur de réseau.

---

1 Les vertex du graphe représentent des routeurs, des réseaux de transit, ou des réseaux d'extrémité. Comme les routeurs peuvent appartenir à plusieurs zones, il n'est pas possible de colorier les vertex du graphe.

4. Résumé fonctionnel

Une copie distincte de l'algorithme d'acheminement de base OSPF fonctionne dans chaque zone. Les routeurs qui ont des interfaces avec plusieurs zones ont plusieurs copies de l'algorithme. Un bref résumé de l'algorithme d'acheminement suit.

Lorsqu'un routeur démarre, il initialise d'abord les structures de données du protocole d'acheminement. Le routeur attend alors l'indication provenant des protocoles de niveau inférieur que ses interfaces sont fonctionnelles.

Un routeur utilise alors le protocole Hello de OSPF pour acquérir des voisins. Le routeur envoie des paquets Hello à ses voisins, et reçoit en retour des paquets Hello. Sur les réseaux en diffusion et en point à point, le routeur détecte de façon dynamique ses routeurs voisins en envoyant ses paquets Hello à l'adresse de diffusion groupée AllSPFRouters. Sur les réseaux qui ne sont pas en diffusion, certaines informations de configuration peuvent être nécessaires afin de découvrir les voisins. Sur les réseaux en diffusion et NBMA, le protocole Hello choisit aussi un routeur désigné pour le réseau.

Le routeur va essayer de former des adjacences avec certains de ses nouveaux voisins. Les bases de données par état de liaisons sont synchronisées entre paires de routeurs adjacents. Sur les réseaux en diffusion et NBMA, le routeur désigné détermine quels routeurs devraient devenir adjacents.

Les adjacences contrôlent la distribution des informations d'acheminement. Les mises à jour d'acheminement sont envoyées et reçues seulement sur les adjacences.

Un routeur annonce périodiquement son état, ce qui est aussi appelé état de liaison. L'état de liaison est aussi annoncé lorsque l'état d'un routeur change. Les adjacences d'un routeur sont reflétées dans le contenu de ses LSA. Cette relation entre adjacences et état de liaison permet au protocole de détecter les routeurs morts à temps.

Les LSA sont écoulés sur toute la zone. L'algorithme d'écoulement est fiable, assurant que tous les routeurs d'une zone ont exactement la même base de données d'états de liaisons. Cette base de données consiste en la collection des LSA générés par chaque routeur qui appartient à la zone. À partir de cette base de données, chaque routeur calcule un arbre des plus courts chemins, dont il est lui-même la racine. Cet arbre des plus courts chemins donne à son tour un tableau d'acheminement pour le protocole.

4.1 Acheminement inter-zone

Le paragraphe précédent décrit le fonctionnement du protocole au sein d'une seule zone. Pour l'acheminement intra-zone, aucune autre information d'acheminement n'est pertinente. Pour être capable d'acheminer à des destinations en dehors de la zone, les routeurs frontières de zone injectent des informations d'acheminement supplémentaires dans la zone. Ces informations supplémentaires sont un distillat du reste de la topologie du système autonome.

Cette distillation se fait comme suit : chaque routeur frontière de zone est par définition connecté au cœur de réseau. Chaque routeur frontière de zone résume la topologie de ses zones non cœur de réseau rattachées pour transmission sur le cœur de réseau, et donc à tous les autres routeurs frontières de zone. Un routeur frontière de zone a alors les informations topologiques complètes concernant le cœur de réseau, et la zone les résume pour chacun des autres routeurs frontières de zone. À partir de ces informations, le routeur calcule les chemins vers toutes les destinations inter-zone. Le routeur annonce alors ces chemins dans les zones qui lui sont rattachées. Cela permet aux routeurs internes à la zone de prendre le meilleur routeur de sortie lorsqu'il transmet du trafic à des destinations inter-zone.

4.2 Chemins externes à l'AS

Les routeurs qui ont des informations concernant d'autres systèmes autonomes peuvent écouler ces informations partout dans l'AS. Ces informations d'acheminement externes sont distribuées mot à mot à chaque routeur participant. Il y a une exception : les informations d'acheminement externes ne sont pas écoulées dans les zones de "bout" (voir le paragraphe 3.6).

Pour utiliser les informations d'acheminement externes, le chemin pour tous les routeurs qui annoncent des informations externes doit être connu partout dans l'AS (à l'exception des zones de bout). Pour cette raison, les localisations de ces routeurs frontières de l'AS sont résumées par les routeurs frontières de zone (non bout).

4.3 Paquets de protocole d'acheminement

Le protocole OSPF fonctionne directement sur IP, en utilisant le protocole IP 89. OSPF ne fournit aucune prise en charge

de fragmentation/réassemblage explicite. Lorsque la fragmentation est nécessaire, on utilise la fragmentation/réassemblage IP. Les paquets de protocole OSPF ont été conçus de telle sorte que de grands paquets de protocole peuvent généralement être partagés en plusieurs paquets de protocole plus petits. Cette pratique est recommandée ; la fragmentation IP devrait être évitée chaque fois que possible.

Les paquets de protocole d'acheminement devraient toujours être envoyés avec le champ de TOS IP réglé à 0. Si c'est possible, les paquets de protocole d'acheminement devraient avoir la préférence sur le trafic de données IP régulier, à la fois en émission et en réception. À titre d'aide pour ce faire, les paquets de protocole OSPF devraient avoir leur champ de préséance IP réglé à la valeur de Contrôle inter-réseau (voir [Ref5]).

Tous les paquets de protocole OSPF ont le même en-tête de protocole décrit à l'Appendice A. La liste des types de paquet OSPF figure ci-dessous au Tableau 8. Leurs formats sont aussi décrits dans l'Appendice A.

Type	Nom du paquet	Fonction du protocole
1	Hello	Découverte/maintenance des voisins
2	Description de base de données	Résume le contenu des bases de données
3	Demande d'état de liaison	Télécharge la base de données
4	Mise à jour d'état de liaison	Met à jour la base de données
5	Accusé de réception d'état de liaison	Écoule les accusés de réception

Tableau 8 : Types de paquets OSPF

Le protocole Hello d'OSPF utilise les paquets Hello pour découvrir et entretenir les relations de voisinage. Les paquets Description de base de données et Demande d'état de liaison sont utilisés dans la formation des adjacences. Le mécanisme de mise à jour fiable d'OSPF est mis en œuvre par les paquets Mise à jour d'état de liaison et Accusé de réception d'état de liaison.

Chaque paquet Mise à jour d'état de liaison porte un ensemble de nouveaux avis d'état de liaison (LSA) d'un bond plus loin que leur point d'origine. Un seul paquet Mise à jour d'état de liaison peut contenir les LSA de plusieurs routeurs. Chaque LSA est étiqueté avec l'identifiant du routeur d'origine et d'une somme de contrôle de son contenu d'état de liaison. Chaque LSA a aussi un champ type ; la liste des différents types de LSA OSPF figure ci-dessous dans le Tableau 9.

Les paquets d'acheminement OSPF (à l'exception des Hello) ne sont envoyés que sur les adjacences. Cela signifie que tous les paquets de protocole OSPF voyagent sur un seul bond IP, excepté ceux qui sont envoyés sur des adjacences virtuelles. L'adresse IP de source d'un paquet de protocole OSPF est une extrémité d'une adjacence de routeur, et l'adresse de destination IP est l'autre extrémité de l'adjacence ou une adresse de diffusion groupée IP.

4.4 Exigences de base de mise en œuvre

Une mise en œuvre d'OSPF exige la prise en charge des pièces suivantes du système :

Temporisateurs

Deux sortes différentes de temporisateurs sont exigées. La première sorte, appelée "temporisateur à un coup", cause le traitement d'un événement de protocole dès qu'il arrive à expiration. La seconde sorte, appelée "temporisateur d'intervalle", arrive à expiration à des intervalles constants. Ceux-ci sont utilisés pour l'envoi des paquets à des intervalles réguliers. Un bon exemple en est la diffusion régulière des paquets Hello. La granularité des deux sortes de temporisateurs est d'une seconde.

Les temporisateurs d'intervalle devraient être mis en œuvre pour éviter les dérives. Dans certaines mises en œuvre de routeurs, le traitement de paquet peut affecter l'exécution du temporisateur. Lorsque plusieurs routeurs sont rattachés à un seul réseau, et qu'ils font tous de la diffusion, cela peut conduire à la synchronisation des paquets d'acheminement (qui devrait être évitée). Si les temporisateurs ne peuvent pas être mis en œuvre en évitant la dérive, de petites quantités aléatoires devraient être ajoutées ou soustraites à chaque expiration d'un temporisateur d'intervalle.

Type de LSA	Nom du LSA	Description du LSA
1	LSA de routeur	Généré par tous les routeurs. Ce LSA décrit les états collectés des état des interfaces du routeur avec une zone. Écoulés sur une seule zone.
2	LSA de réseau	Généré pour les réseaux NBMA et de diffusion par le routeur désigné. Ce LSA contient la liste des routeurs connectés au réseau. Écoulés sur une seule zone.
3, 4	LSA de résumé	Générés par les routeurs frontières de zone, et écoulés dans toute la zone associée du LSA. Chaque LSA de résumé décrit un chemin pour une destination en dehors de la zone, bien qu'encore à l'intérieur de l'AS (c'est-à-dire, un chemin inter-zone). Les LSA de résumé de type 3 décrivent les chemins vers des réseaux. Les LSA de résumé de type 4 décrivent des chemins vers des routeurs frontières de l'AS.
5	LSA externe à l'AS	Générés par les routeurs frontières de l'AS, et écoulés partout dans l'AS. Chaque LSA externe à l'AS décrit un chemin vers une destination dans un autre système autonome. Les chemins par défaut pour l'AS peuvent aussi être décrites par les LSA externes à l'AS.

Tableau 9 : Avis d'état de liaison (LSA) OSPF.

Diffusion groupée IP
Certains paquets OSPF prennent la forme de datagrammes IP en diffusion groupée. La prise en charge ou la réception et l'envoi des datagrammes IP en diffusion groupée, ainsi que la prise en charge du protocole de niveau inférieur approprié est exigée. Les datagrammes IP en diffusion groupée utilisés par OSPF ne font jamais un déplacement supérieur à un bond. Pour cette raison, la capacité de transmettre des datagrammes IP en diffusion groupée n'est pas exigée. Pour des informations sur la diffusion groupée IP, voir [Ref7].

Prise en charge de sous-réseau de longueur variable
La prise en charge du protocole IP du routeur doit inclure la capacité à diviser un numéro de réseau IP de classe A, B, ou C en de nombreux sous-réseaux de diverses tailles. C'est ce qui est couramment appelé sous-réseautage de longueur variable ; voir des précisions au paragraphe 3.5.

Prise en charge du super-réseautage IP
La prise en charge du protocole IP du routeur doit inclure la capacité à agréger des collections contiguës de réseaux IP de classe A, B, et C en de plus grandes entités appelées super-réseaux. Le super-réseautage a été proposé comme moyen d'améliorer l'échelonnement de l'acheminement IP dans l'Internet mondial. Pour des informations complémentaires sur le super-réseautage IP, voir [Ref10].

Prise en charge de protocole de niveau inférieur
Les protocoles de niveau inférieur visés ici sont les protocoles d'accès réseau, tels que la couche de liaison des données Ethernet. Des indications doivent être passées de ces protocoles à OSPF car l'interface réseau s'ouvre et se ferme. Par exemple, sur un ethernet il serait précieux de savoir quand le câble émetteur-récepteur ethernet est débranché.

Prise en charge de protocole de niveau inférieur non diffusion
Sur les réseaux qui ne sont pas en diffusion, le protocole Hello d'OSPF peut être aidé par la fourniture d'une indication lorsqu'est faite une tentative d'envoi d'un paquet à un routeur mort ou non existant. Par exemple, sur un PDN X.25 un routeur voisin mort peut être indiqué par la réception d'un message libération X.25 avec une cause et un diagnostic appropriés, et cette information sera passée à OSPF.

Primitives de manipulation de liste
La plupart des fonctions OSPF sont décrites en termes de fonctionnement sur les listes de LSA. Par exemple, la collection des LSA sera retransmise à un routeur adjacent jusqu'à ce qu'il en soit accusé réception comme décrite sous forme de liste. Tout LSA particulier peut être sur de nombreuses listes de cette sorte. Une mise en œuvre OSPF doit être capable de manipuler ces listes, en ajoutant et supprimant les LSA constitutifs en tant que de besoin.

Prise en charge de tâches
Certaines procédures décrites dans la présente spécification invoquent d'autres procédures. Par moment, ces autres procédures devraient être exécutées en ligne, c'est-à-dire, avant la fin de la procédure en cours. Ceci est indiqué dans le texte par des instructions pour exécuter une procédure. À d'autres moments, les autres procédures sont à exécuter seulement quand la procédure en cours est terminée. Ceci est indiqué par des instructions pour planifier une tâche.

4.5 Capacités OSPF facultatives

Le protocole OSPF définit plusieurs capacités facultatives. Un routeur indique les capacités facultatives qu'il prend en charge dans ses paquets OSPF Hello, Description de base de données, et dans ses LSA. Cela permet aux routeurs qui

prennent en charge un mélange de capacités facultatives de coexister dans un seul système autonome.

Certaines capacités doivent être prises en charge par tous les routeurs rattachés à une zone spécifique. Dans ce cas, un routeur n'acceptera un paquet Hello de son voisin que si il y a une correspondance dans les capacités rapportées (c'est-à-dire qu'une discordance de capacités empêche de former une relation de voisinage). Un exemple en est ExternalRoutingCapability (voir ci-dessous).

D'autres capacités peuvent être négociées durant le processus d'échange de base de données. Ceci est accompli en spécifiant les capacités facultatives dans les paquets de description de base de données. Une discordance de capacités avec un voisin résulte dans ce cas en un échange de seulement un sous-ensemble de la base de données d'état des liaisons entre les deux voisins.

Le processus de construction du tableau d'acheminement peut aussi être affecté par la présence/absence des capacités facultatives. Par exemple, comme les capacités facultatives sont rapportées dans les LSA, les routeurs incapables de certaines fonctions peuvent être évités lors de la construction de l'arbre des plus courts chemins.

La liste des capacités facultatives d'OSPF définies dans le présent mémoire figure ci-dessous. Voir le paragraphe A.2 pour des informations complémentaires.

Capacité d'acheminement externe (ExternalRoutingCapability)
: Des zones OSPF entières peuvent être configurées comme des "bouts" (voir le paragraphe 3.6). Les LSA externes à l'AS ne seront pas écoulés dans les zones de bout. Cette capacité est représentée par le bit E dans le champ Options OSPF (voir le paragraphe A.2). Afin d'assurer une configuration cohérente des zones de bout, tous les routeurs qui ont une interface avec une telle zone doivent avoir le bit E à zéro dans leurs paquets Hello (voir les paragraphes 9.5 et 10.5).

5. Structures des données du protocole

Le protocole OSPF est décrit ici en termes de fonctionnement sur diverses structures de données de protocole. La liste suivante comprend les structures de données OSPF de niveau supérieur. Toute initialisation qui doit être faite est notée. Les zones, interfaces et voisins OSPF ont aussi des structures de données associées qui sont décrites plus loin dans la présente spécification.

Identifiant de routeur
: Nombre de 32 bits qui identifie de façon univoque ce routeur dans l'AS. Une stratégie possible de mise en œuvre serait d'utiliser la plus petite adresse IP d'interface appartenant au routeur. Si l'identifiant de routeur OSPF d'un routeur est changé, le logiciel OSPF du routeur devrait être redémarré avant que le nouvel identifiant de routeur prenne effet. Dans ce cas, le routeur devrait purger les LSA qu'il a générés du domaine d'acheminement (voir le paragraphe 14.1) avant de redémarrer, ou ils vont persister jusqu'à MaxAge minutes.

Structures de zone
: Chaque zone de celles auxquelles le routeur est connecté a sa propre structure de données. Cette structure de données décrit le travail de l'algorithme OSPF de base. On rappelle que chaque zone possède une copie distincte de l'algorithme OSPF de base.

Structure de cœur de réseau (zone)
: La zone cœur de réseau OSPF est chargée de la dissémination des informations d'acheminement inter-zone.

Liaisons virtuelles configurées
: Les liaisons virtuelles configurées avec ce routeur comme un point d'extrémité. Afin d'avoir des liaisons virtuelles configurées, le routeur lui-même doit être un routeur frontière de zone. Les liaisons virtuelles sont identifiées par l'identifiant de routeur de l'autre point d'extrémité – qui est un autre routeur frontière de zone. Ces deux routeurs points d'extrémité doivent être rattachés à une zone commune, appelée la zone de transit de la liaison virtuelle. Les liaisons virtuelles font partie du cœur de réseau, et se comportent comme si elles étaient des réseaux point à point non numérotés entre les deux routeurs. Une liaison virtuelle utilise l'acheminement intra-zone de sa zone de transit pour transmettre les paquets. Les liaisons virtuelles sont établies et supprimées par la construction des arbres des plus courts chemins pour la zone de transit.

Liste des chemins externes
: Ce sont les chemins pour les destinations externes au système autonome, qui ont été obtenues par expérience directe avec un autre protocole d'acheminement (tel que BGP), ou par des informations de configuration, ou par une combinaison des deux (par exemple, informations dynamiques externes à annoncer par OSPF avec une métrique

configurée). Tout routeur qui a ces chemins externes est appelé un routeur frontière de l'AS. Ces chemins sont annoncés par le routeur dans le domaine d'acheminement OSPF via les LSA externes à l'AS.

Liste des LSA externes à l'AS
Partie de la base de données d'états de liaisons. Elles ont été générées à partir des routeurs frontières de l'AS. Elles comportent les chemins pour les destinations externes au système autonome. Noter que, si le routeur est lui-même un routeur frontière de l'AS, certaines de ces LSA externes à l'AS ont été auto-générées.

Tableau d'acheminement
Dérivé de la base de données d'états de liaisons. Chaque entrée dans le tableau d'acheminement est indexé par une destination, et contient le coût de la destination et un ensemble de chemins à utiliser pour la transmission des paquets à la destination. Un chemin est décrit par son type et son prochain bond. Pour plus d'informations, voir la Section 11.

La Figure 9 montre la collection des structures de données présentes dans un routeur normal. Le routeur décrit est RT10, d'après la carte de la Figure 6. Noter que le routeur RT10 a une liaison virtuelle configurée avec le routeur RT11, et que la zone 2 est la zone de transit de la liaison. Ceci est indiqué par la ligne en pointillés de la Figure 9. Lorsque la liaison virtuelle devient active, grâce à la construction de l'arbre des plus courts chemins pour la zone 2, elle devient une interface avec le cœur de réseau (voir les deux interfaces de cœur de réseau décrites à la Figure 9).

6. Structure des données de zone

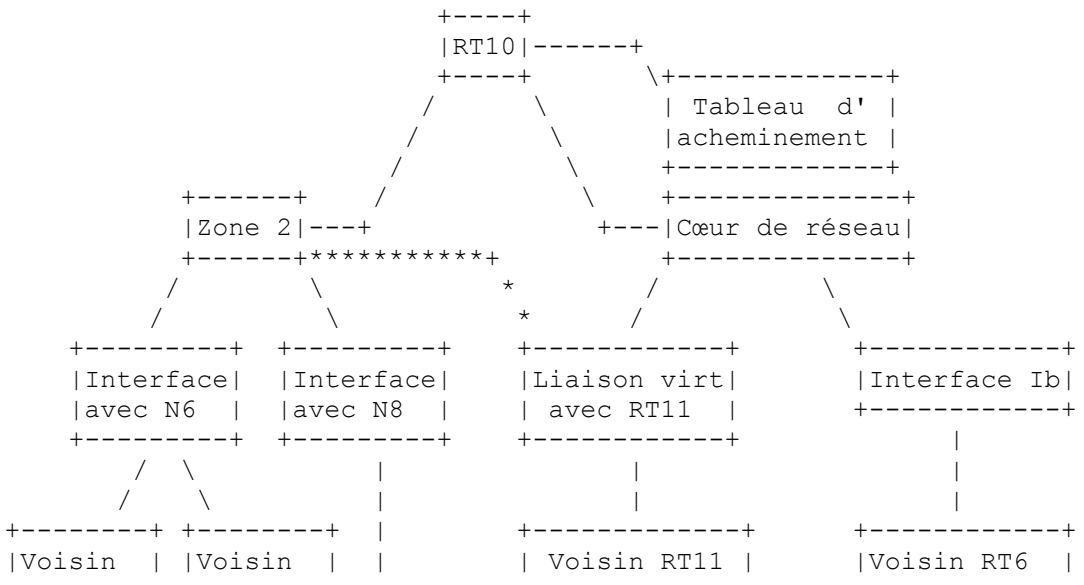
La structure des données de zone contient toutes les informations utilisées pour faire fonctionner l'algorithme d'acheminement OSPF de base. Chaque zone entretient sa propre base de données d'états de liaisons. Un réseau appartient à une seule zone, et une interface de routeur se connecte à une seule zone. Chaque adjacence de routeur appartient aussi à une seule zone.

Le cœur de réseau OSPF est la zone OSPF particulière chargée de la dissémination des informations d'acheminement inter-zone.

La base de données d'états de liaisons de la zone consiste en la collection des LSA de routeur, LSA de réseau et LSA de résumés qui ont été générés par les routeurs de la zone. Ces informations sont écoulées partout à l'intérieur d'une seule zone. La liste des LSA externes à l'AS (voir la Section 5) est aussi considérée comme faisant partie de la base de données d'états de liaisons de chaque zone.

Identifiant de zone
Nombre de 32 bits qui identifie la zone. L'identifiant de zone de 0.0.0.0 est réservé pour le cœur de réseau.

Liste des gammes d'adresses de la zone
Afin d'agréger les informations d'acheminement aux frontières de la zone, les gammes d'adresse de la zone peuvent être utilisées. Chaque gamme d'adresse est spécifiée par une paire [adresse,gabarit] et une indication d'état de Annoncer ou NePasAnnoncer (voir au paragraphe 12.4.3).



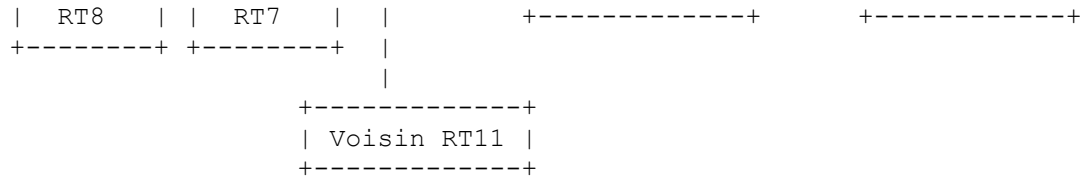


Figure 9 : Structure des données du routeur RT10

Interfaces associées au routeur
Les interfaces du routeur qui le connectent à la zone. Une interface de routeur appartient à une zone et une seule (ou au cœur de réseau). Pour la zone cœur de réseau cette liste comporte toutes les liaisons virtuelles. Une liaison virtuelle est identifiée par l'identifiant de routeur de son autre point d'extrémité ; son coût est le coût du plus court chemin intra-zone à travers la zone de transit qui existe entre les deux routeurs.

Liste des LSA de routeur
Un LSA de routeur est généré par chaque routeur dans la zone. Il décrit l'état des interfaces du routeur avec la zone.

Liste des LSA de réseau
Un LSA de réseau est généré pour chaque réseau de diffusion en transit et réseau NBMA dans la zone. Un LSA de réseau décrit l'ensemble des routeurs actuellement connectés au réseau.

Liste des LSA de résumé
Les LSA de résumé sont générés à partir des routeurs frontières de zone de la zone. Ils décrivent les chemins vers les destinations internes au système autonome, et donc externes à la zone (c'est-à-dire, les destinations inter-zone).

Arbre des plus courts chemins
L'arbre des plus courts chemins pour la zone, avec ce routeur lui-même comme racine. Déduit des LSA de routeur et des LSA de réseau collectés par l'algorithme de Dijkstra (voir le paragraphe 16.1).

TransitCapability
Ce paramètre indique si la zone peut porter du trafic de données qui n'est pas généré dans la zone elle-même ni ne s'y termine. Ce paramètre est calculé lorsque est construit l'arbre des plus courts chemins de la zone (voir le paragraphe 16.1, où TransitCapability est mis à VRAI si et seulement si il y a une ou plusieurs liaisons virtuelles pleinement adjacentes utilisant la zone comme zone de transit), et il est utilisé comme entrée pour une étape ultérieure du processus de construction du tableau d'acheminement (voir le paragraphe 16.3). Lorsque le paramètre TransitCapability d'une zone est mis à VRAI, la zone est dite "zone de transit".

ExternalRoutingCapability
Dit si les LSA externes à l'AS seront écoulés dans et partout dans la zone. C'est un paramètre configurable. Si les LSA externes à l'AS sont exclus de la zone, la zone est appelée un "bout". Dans les zones bouts, l'acheminement vers les destination externes à l'AS sera uniquement fondé sur un résumé de chemin par défaut. Le cœur de réseau ne peut pas être configuré comme zone bout. Aussi, les liaisons virtuelles ne peuvent pas être configurées à travers des zones bouts. Pour des informations complémentaires, voir le paragraphe 3.6.

StubDefaultCost
Si la zone a été configurée comme zone de bout, et si le routeur lui-même est un routeur frontière de zone, le paramètre StubDefaultCost indique alors le coût du LSA de résumé par défaut que le routeur devrait annoncer dans la zone. Voir au paragraphe 12.4.3 des informations complémentaires.

Sauf spécification contraire, les autres sections du présent document se réfèrent au fonctionnement du protocole OSPF au sein d'une seule zone.

7. Construction des adjacences

OSPF crée des adjacences entre les routeurs voisins pour les besoins de l'échange des informations d'acheminement. Tous les routeurs voisins ne vont pas devenir adjacents. Cette section traite des généralités impliquées dans la création des adjacences. Des détails complémentaires figurent à la Section 10.

7.1 Le protocole Hello

Le protocole Hello est chargé de l'établissement et de la maintenance des relations de voisinage. Il assure aussi que la communication entre voisins est bidirectionnelle. Les paquets Hello sont envoyés périodiquement des interfaces de routeur. La communication bidirectionnelle est indiquée lorsque le routeur se voit lui-même dans la liste des paquets Hello du voisin. Sur les réseaux NBMA et en diffusion, le protocole Hello choisit un routeur désigné pour le réseau.

Le protocole Hello fonctionne de façon différente sur les réseaux de diffusion, les réseaux NBMA et les réseaux en point à multipoint. Sur les réseaux de diffusion, chaque routeur s'annonce lui-même en faisant périodiquement des paquets Hello en diffusion groupée. Cela permet aux voisins d'être découverts de façon dynamique. Ces paquets Hello contiennent la vue du routeur de l'identité du routeur désigné, et la liste des routeurs dont les paquets Hello ont été vus récemment.

Sur les réseaux NBMA, des informations de configuration peuvent être nécessaires pour le fonctionnement du protocole Hello. Chaque routeur qui peut éventuellement devenir routeur désigné a une liste de tous les autres routeurs rattachés au réseau. Un routeur, qui a le potentiel de routeur, envoie des paquets Hello à tous les autres routeurs désignés potentiels lorsque son interface au réseau NBMA devient fonctionnelle. C'est une tentative pour trouver le routeur désigné pour le réseau. Si le routeur lui-même est choisi comme routeur désigné, il commence à envoyer des paquets Hello à tous les autres routeurs rattachés au réseau.

Sur les réseaux en point à multipoint, un routeur envoie des paquets Hello à tous ses voisins avec lesquels il peut communiquer directement. Ces voisins peuvent être découverts de façon dynamique à travers un protocole tel que l'ARP inverse (voir [Ref14]), ou ils peuvent être configurés.

Après qu'un voisin a été découvert, que la communication bidirectionnelle est assurée, et (sur un réseau NBMA ou en diffusion) qu'un routeur désigné a été choisi, une décision est prise concernant la formation ou non de l'adjacence avec le voisin (voir le paragraphe 10.4). Si une adjacence doit être formée, la première étape est de synchroniser les bases de données d'états de liaisons des voisins. Ceci est traité au paragraphe suivant.

7.2 Synchronisation des bases de données

Dans un algorithme d'acheminement par état de liaison, il est très important que toutes les bases de données d'états de liaisons des routeurs restent synchronisées. OSPF simplifie cela en exigeant que seuls les routeurs adjacents restent synchronisés. Le processus de synchronisation commence aussitôt que le routeur essaye de construire l'adjacence. Chaque routeur décrit sa base de données en envoyant une séquence de paquets Description de base de données à son voisin. Chaque paquet Description de base de données décrit un ensemble de LSA qui appartiennent à la base de données du routeur. Lorsque le voisin voit un LSA qui est plus récent que sa propre copie de la base de données, il fait une note disant qu'un LSA plus récent devrait être demandé.

Cet envoi et cette réception de paquet Description de base de données est appelé "Processus d'échange de base de données". Durant ce processus, les deux routeurs forment une relation maître/esclave. Chaque paquet Description de base de données a un numéro de séquence. Les paquets Description de base de données envoyés par le maître (interrogations) sont acquittés par l'esclave au moyen de l'écho du numéro de séquence. Les interrogations et leurs réponses contiennent des résumés des données d'état de liaison. Le maître est le seul autorisé à transmettre des paquets Description de base de données. Il ne le fait qu'à intervalles fixes, dont la longueur est l'intervalle configuré constant par interface RxmtInterval.

Chaque Description de base de données contient une indication que d'autres paquets sont à suivre --- le bit M. Le processus d'échange de base de données est terminé lorsqu'un routeur a reçu et envoyé les paquets Description de base de données avec le bit M à zéro.

Pendant et après le processus d'échange de base de données, chaque routeur a une liste des LSA pour lesquels le voisin a des instances mieux à jour. Ces LSA sont demandés dans des paquets Demande d'état de liaison. Les paquets Demande d'état de liaison qui ne sont pas satisfaits sont retransmis à des intervalles de temps fixés de RxmtInterval. Lorsque le processus Description de base de données est terminé et que toutes les demandes d'état de liaison ont été satisfaites, les bases de données sont réputées synchronisées et les routeurs sont marqués comme pleinement adjacents. À ce moment, l'adjacence est pleinement fonctionnelle et est annoncée dans les LSA de routeur des deux routeurs.

L'adjacence est utilisée par la procédure d'arrosage aussitôt que commence le processus d'échange de base de données. Cela simplifie la synchronisation des bases de données, et garantit qu'elle va se terminer dans un délai prévisible.

7.3 Routeur désigné

Chaque réseau NBMA et de diffusion a un routeur désigné. Le routeur désigné effectue deux fonctions principales pour le protocole d'acheminement :

- Le routeur désigné génère un LSA de réseau au nom du réseau. Ce LSA fait la liste de l'ensemble des routeurs (y compris le routeur désigné lui-même) actuellement rattachés au réseau. L'identifiant d'état de liaison pour ce LSA (voir le paragraphe 12.1.4) est l'adresse IP d'interface du routeur désigné. Le numéro de réseau IP peut alors être obtenu en utilisant le gabarit de réseau/sous-réseau du réseau.

- Le routeur désigné devient adjacent à tous les autres routeurs du réseau. Comme les bases de données d'état de liaison sont synchronisées à travers les adjacences (par la construction de l'adjacence puis la procédure d'arrosage), le routeur désigné joue un rôle central dans le processus de synchronisation.

Le routeur désigné est choisi par le protocole Hello. Un paquet Hello de routeur contient sa priorité de routeur, qui est configurable interface par interface. En général, lorsqu'une interface d'un routeur à un réseau devient fonctionnelle pour la première fois, elle vérifie pour savoir si il est actuellement le routeur désigné pour le réseau. Si il l'est, elle accepte ce routeur désigné, sans considération de sa Priorité de routeur. (Cela rend plus difficile de prédire l'identité du routeur désigné, mais assure que le routeur désigné change moins souvent. Voir ci-dessous.) Autrement, le routeur lui-même devient routeur désigné si il a la plus forte priorité de routeur sur le réseau. Une description plus détaillée (et plus précise) du choix du routeur désigné est présentée au paragraphe 9.4.

Le routeur désigné est le point d'extrémité de nombreuses adjacences. Afin d'optimiser la procédure d'arrosage sur les réseaux de diffusion, le routeur désigné fait une diffusion groupée de ses paquets de mise à jour d'état de liaison à l'adresse AllSPFRouters, plutôt que d'envoyer des paquets distincts sur chaque adjacence.

La Section 2 du présent document expose la représentation du graphe dirigé d'une zone. Les nœuds routeurs sont marqués avec leur identifiant de routeur. Les nœuds de réseau de transit sont en fait étiquetés avec l'adresse IP de leur routeur désigné. Il s'ensuit que lorsque le routeur désigné change, cela apparaît comme si le nœud de réseau sur le graphe était remplacé par un nœud entièrement nouveau. Cela va amener le réseau et tous ses routeurs rattachés à générer de nouveaux LSA. Jusqu'à ce que les bases de données d'états de liaisons convergent à nouveau, il peut en résulter une certaine perte temporaire de connexité. Cela peut déboucher sur l'envoi de messages ICMP Injoignable en réponse à du trafic de données. Pour cette raison, le routeur désigné ne devrait changer que rarement. Les priorités de routeur devraient être configurées de telle sorte que le routeur le plus digne de confiance d'un réseau devienne en fin de compte le routeur désigné.

7.4 Routeur désigné de secours

Pour rendre plus douce la transition avec un nouveau routeur désigné, il y a un routeur désigné de secours pour chaque réseau NBMA et de diffusion. Le routeur désigné de secours est aussi adjacent à tous les routeurs sur le réseau, et devient le routeur désigné en cas de défaillance du précédent routeur désigné. S'il n'y avait pas de routeur désigné de secours, lorsqu'un nouveau routeur désigné devient nécessaire, de nouvelles adjacences devraient être formées entre le nouveau routeur désigné et tous les autres routeurs rattachés au réseau. Une partie du processus de formation de l'adjacence est la synchronisation des bases de données d'états de liaisons, qui peut éventuellement prendre assez longtemps. Durant ce temps, le réseau ne serait pas disponible pour la transmission du trafic de données. Le routeur désigné de secours supplée au besoin de former ces adjacences, car elles existent déjà. Cela signifie que la période d'interruption du transit du trafic ne dure qu'autant que prend l'écoulement des nouveaux LSA (qui annoncent le nouveau routeur désigné).

Le routeur désigné de secours ne génère pas de LSA de réseau pour le réseau. (S'il le faisait, la transition d'un nouveau routeur désigné serait encore plus rapide. Cependant, c'est un compromis entre taille de base de données et vitesse de convergence lorsque le routeur désigné disparaît.)

Le routeur désigné de secours est aussi choisi par le protocole Hello. Chaque protocole Hello a un champ qui spécifie le routeur désigné de secours pour le réseau.

Dans certaines étapes de la procédure d'arrosage, le routeur désigné de secours joue un rôle passif, laissant le routeur désigné faire la plus grande partie du travail. Cela réduit la quantité de trafic d'acheminement local. Voir au paragraphe 13.3 des informations complémentaires.

7.5 Graphe des adjacences

Une adjacence est liée au réseau que les deux routeurs ont en commun. Si deux routeurs ont plusieurs réseaux en commun,

ils peuvent avoir plusieurs adjacences entre eux.

On peut dépeindre la collection des adjacences sur un réseau comme formant un graphe non dirigé. Les vertex consistent en routeurs, avec un bord qui joint deux routeurs si ils sont adjacents. Le graphe des adjacences décrit le flux des paquets d'acheminement de protocole, et en particulier des paquets Mise à jour d'état de liaison, à travers le système autonome.

Deux graphes sont possibles, selon qu'un routeur désigné est choisi pour le réseau ou non. Sur les réseaux physiques point à point, les réseaux en point à multipoint et les liaisons virtuelles, les routeurs voisins deviennent adjacents chaque fois qu'ils peuvent communiquer directement. À l'opposé, sur les réseaux NBMA et en diffusion, seul le routeur désigné et le routeur désigné de secours deviennent adjacents à tous les autres routeurs rattachés au réseau.

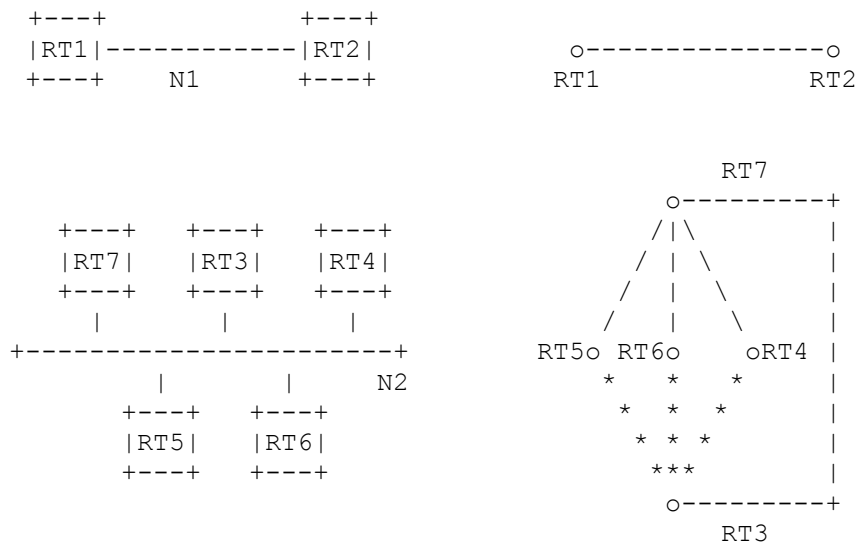


Figure 10 : Graphe des adjacences

Ces graphes sont montrés à la Figure 10. On suppose que le routeur RT7 est devenu le routeur désigné, et le routeur RT3 le routeur désigné de secours, pour le réseau N2. Le routeur désigné de secours effectue une fonction moindre que celle du routeur désigné durant la procédure d'arrosage (voir le paragraphe 13.3). C'est la raison des lignes en pointillé qui connectent le routeur désigné de secours RT3.

8. Traitement des paquets de protocole

La présente section expose le traitement général des paquets de protocole d'acheminement OSPF. Il est très important que les bases de données d'états de liaisons du routeur restent synchronisées. Pour cette raison, les paquets de protocole d'acheminement devraient obtenir un traitement préférentiel sur les paquets de données ordinaires, aussi bien à l'envoi qu'à la réception.

Les paquets de protocole d'acheminement sont envoyés seulement le long des adjacences (à l'exception des paquets Hello, qui sont utilisés pour découvrir les adjacences). Cela signifie que tous les paquets de protocole d'acheminement voyagent sur un seul bond IP, sauf ceux envoyés sur les liaisons virtuelles.

Tous les paquets de protocole d'acheminement commencent par un en-tête standard. Les paragraphes ci-dessous fournissent les détails du remplissage et de la vérification de cet en-tête standard. Puis, pour chaque type de paquet, figure la liste des paragraphes qui donnent des précisions sur le traitement de ce type de paquet particulier.

8.1 Envoi des paquets de protocole

Lorsqu'un routeur envoie un paquet de protocole d'acheminement, il remplit comme suit les champs de l'en-tête de paquet OSPF standard. Des précisions sur le format d'en-tête figurent au paragraphe A.3.1 :

N° de version : Réglé à 2, c'est le numéro de version du protocole tel qu'il figure dans la présente spécification.
Type de paquet : Type de paquet OSPF, tel que paquet Mise à jour d'état de liaison ou Hello.
Longueur de paquet : Longueur totale en octets du paquet OSPF, y compris l'en-tête standard de paquet OSPF.
Identifiant de routeur : Identité du routeur lui-même (qui génère le paquet).

Identifiant de zone : Zone OSPF dans laquelle le paquet est envoyé.

Somme de contrôle : Somme de contrôle IP standard de 16 bits de complément à un sur le paquet OSPF entier, à l'exclusion du champ d'authentification de 64 bits. Cette somme de contrôle est calculée au titre de la procédure d'authentification appropriée ; pour certains types d'authentification OSPF, le calcul de la somme de contrôle est omis. Voir les précisions au paragraphe D.4.

AuType et authentification : Chaque échange de paquet OSPF est authentifié. Les types d'authentification sont alloués par le protocole et sont indiqués à l'Appendice D. Une procédure d'authentification différente peut être utilisée pour chaque réseau/sous-réseau IP. Autype indique le type de la procédure d'authentification utilisée. Le champ d'authentification de 64 bits est alors à utiliser par la procédure d'authentification choisie. Cette procédure devrait être invoquée en dernier lors de la formation du paquet à envoyer. Voir les précisions au paragraphe D.4.

L'adresse de destination IP pour le paquet est choisie comme suit. Sur les réseaux point à point physiques, la destination IP est toujours réglée à l'adresse AllSPFRouters. Sur tous les autres types de réseau (y compris les liaisons virtuelles), la majorité des paquets OSPF est envoyée en envoi individuel, c'est-à-dire, envoyés directement à l'autre extrémité de l'adjacence. Dans ce cas, la destination IP est simplement l'adresse IP du voisin associée à l'autre extrémité de l'adjacence (voir la Section 10). Les seuls paquets qui ne sont pas envoyés en envoi individuels sont sur les réseaux de diffusion ; sur ces réseaux les paquets Hello sont envoyés à la destination de diffusion groupée AllSPFRouters, le routeur désigné et son secours envoient tous deux les paquets Mise à jour d'état de liaison et les paquets Accusé de réception d'état de liaison à l'adresse de diffusion groupée AllSPFRouters, alors que tous les autres routeurs envoient aussi bien les paquets Mise à jour d'état de liaison que Accusé de réception d'état de liaison à l'adresse de diffusion groupée AllDRouters.

Les retransmissions des paquets Mise à jour d'état de liaison sont TOUJOURS envoyées directement au voisin. Sur les réseaux multi accès, cela signifie que les retransmissions devraient être envoyées à l'adresse IP du voisin.

L'adresse IP de source devrait être réglée à l'adresse IP de l'interface d'envoi. Les interfaces avec des réseaux point à point non numérotés n'ont pas d'adresse IP associée. Sur ces interfaces, la source IP devrait être réglée à n'importe laquelle des autres adresses IP qui appartiennent au routeur. Pour cette raison, il doit y avoir au moins une adresse IP allouée au routeur[2]. Noter que, pour la plupart des besoins, les liaisons virtuelles agissent précisément comme des réseaux point à point non numérotés. Cependant, chaque liaison virtuelle n'a pas une adresse IP d'interface (découverte durant le processus de construction du tableau d'acheminement) utilisée comme source IP lors de l'envoi des paquets sur la liaison virtuelle.

Pour des informations complémentaires sur le format de types spécifiques de paquets OSPF, consulter les paragraphes cités au Tableau 10.

Type	Nom de paquet	paragraphe (émission)
1	Hello	paragraphe 9.5
2	Description de base de données	paragraphe 10.8
3	Demande d'état de liaison	paragraphe 10.9
4	Mise à jour d'état de liaison	paragraphe 13.3
5	Accusé de réception d'état de liaison	paragraphe 13.5

Tableau 10 : Paragraphes décrivant la transmission de paquet de protocole OSPF.

8.2 Réception des paquets de protocole

Chaque fois qu'un paquet de protocole est reçu par le routeur, il est marqué de l'interface sur laquelle il a été reçu. Pour les routeurs qui ont des liaisons virtuelles configurées, l'interface à associer au paquet peut n'être pas immédiatement évidente. Par exemple, considérons le routeur RT11 décrit à la Figure 6. Si RT11 reçoit un paquet de protocole OSPF sur son interface au réseau N8, il peut vouloir associer le paquet à l'interface à la zone 2, ou à la liaison virtuelle au routeur RT10 (qui fait partie du cœur de réseau). Dans ce qui suit, on suppose que le paquet est initialement associé à la liaison non virtuelle[3].

Pour que le paquet soit accepté au niveau IP, il doit passer un certain nombre d'essais, même avant que le paquet soit passé à OSPF pour le traitement :

o La somme de contrôle IP doit être correcte.

2 Il est possible que toutes les interfaces d'un routeur soient des liaisons point à point non numérotées. Dans ce cas, une adresse IP doit être allouée au routeur. Cette adresse sera alors annoncée dans le LSA de routeur du routeur comme chemin d'hôte.

3 Noter que dans ces cas les deux interfaces, la non virtuelle et la virtuelle, auront la même adresse IP.

- o L'adresse de destination IP du paquet doit être l'adresse IP de l'interface de réception, ou une des adresses de diffusion groupée IP AllSPFRouters ou AllDRouters.
- o Le protocole IP spécifié doit être OSPF (89).
- o Les paquets générés localement ne devraient pas être passés à OSPF. C'est-à-dire que l'adresse IP de source devrait être examinée pour s'assurer que ce n'est pas un paquet en diffusion groupée que le routeur a généré lui-même.

Ensuite, l'en-tête du paquet OSPF est vérifié. Les champs spécifiés dans l'en-tête doivent correspondre à ceux configurés pour l'interface de réception. S'ils ne correspondent pas, le paquet devrait être éliminé :

- o Le champ numéro de version doit spécifier la version 2 du protocole.
- o L'identifiant de zone qui se trouve dans l'en-tête OSPF doit être vérifié. Si les deux cas suivants échouent, le paquet devrait être éliminé. L'identifiant de zone spécifié dans l'en-tête doit soit :
  (1) Correspondre à l'identifiant de zone de l'interface de réception. Dans ce cas, le paquet a été envoyé sur un seul bond. Donc, l'adresse IP de source du paquet est nécessairement sur le même réseau que l'interface de réception. Cela peut être vérifié en comparant l'adresse IP de source du paquet à l'adresse IP de l'interface, après avoir passé les deux adresses au gabarit de l'interface. Cette comparaison ne devrait pas être effectuée sur les réseaux point à point. Sur les réseaux point à point, les adresses d'interface de chaque extrémité de la liaison devraient être allouées indépendamment, si elles sont allouées.
  (2) Indiquer le cœur de réseau. Dans ce cas, le paquet a été envoyé sur une liaison virtuelle. Le routeur de réception doit être un routeur frontière de zone, et l'identifiant de routeur spécifié dans le paquet (le routeur de source) doit être l'autre extrémité d'une liaison virtuelle configurée. L'interface de réception doit aussi se rattacher à la zone de transit configurée de la liaison virtuelle. Si toutes ces vérification réussissent, le paquet est accepté et est à partir de ce moment associé à la liaison virtuelle (et à la zone cœur de réseau).
- o Les paquets dont la destination IP est AllDRouters ne devraient être acceptés que si l'état de l'interface de réception est DR ou Secours (voir le paragraphe 9.1).
- o Le AuType spécifié dans le paquet doit correspondre au AuType spécifié pour la zone associée.
- o Le paquet doit être authentifié. La procédure d'authentification est indiquée par le réglage du AuType (voir l'Appendice D). La procédure d'authentification peut utiliser une ou plusieurs clés d'authentification, qui peuvent être configurées interface par interface. La procédure d'authentification peut aussi vérifier le champ Somme de contrôle dans l'en-tête du paquet OSPF (qui, quand il est utilisé, est réglé à la somme de contrôle IP standard de complément à un de 16 bits du contenu du paquet OSPF après exclusion du champ d'authentification de 64 bits). Si la procédure d'authentification échoue, le paquet devrait être éliminé.

Si le type de paquet est Hello, il devrait alors subir un autre traitement par le protocole Hello (voir au paragraphe 10.5). Tous les autres types de paquet ne sont envoyés/reçus que sur les adjacences. Cela signifie que le paquet doit avoir été envoyé par un des voisins actifs du routeur. Si l'interface de réception se connecte à un réseau de diffusion, un réseau en point à multipoint ou un réseau NBMA, l'envoyeur est identifié par l'adresse IP de source trouvée dans l'en-tête IP du paquet. Si l'interface de réception se connecte à un réseau point à point ou une liaison virtuelle, l'envoyeur est identifié par l'identifiant de routeur (routeur de source) trouvé dans l'en-tête OSPF du paquet. La structure des données associée à l'interface de réception contient la liste des voisins actifs. Les paquets ne correspondant à aucun voisin actif sont éliminés.

À ce moment, tous les paquets de protocole reçus sont associés à un voisin actif. Pour le traitement d'entrée ultérieur des types de paquet spécifiques, consulter les paragraphes indiqués au Tableau 11.

Type	**Nom du paquet**	**paragraphe de l'exposé (réception)**
1	Hello	paragraphe 10.5
2	Description de la base de données	paragraphe 10.6
3	Demande d'état de liaison	paragraphe 10.7
4	Mise à jour d'état de liaison	Section 13
5	Accusé de réception d'état de liaison	paragraphe 13.7

Tableau 11 : Paragraphes qui décrivent la réception des paquets de protocole OSPF.

9. Structure des données de l'interface

Une interface OSPF est la connexion entre un routeur et un réseau. On suppose une seule interface OSPF à chaque réseau/sous-réseau rattaché bien que la prise en charge de plusieurs interfaces sur un seul réseau soit examinée dans l'Appendice F. Chaque structure d'interface a au plus une adresse IP d'interface.

Une interface OSPF peut être estimée appartenir à la zone qui contient le réseau rattaché. Tous les paquets de protocole d'acheminement générés par le routeur sur cette interface sont étiquetés avec l'identifiant de zone de l'interface. Une ou

plusieurs adjacences de routeur peuvent se développer sur une interface. Les LSA d'un routeur reflètent l'état de ses interfaces et de leurs adjacences associées.

Les éléments de données suivants sont associés à une interface. Noter qu'un certain nombre de ces éléments sont en fait configurés pour le réseau rattaché ; de tels éléments doivent être les mêmes pour tous les routeurs connectés au réseau.

Type
Le type d'interface OSPF est point à point, diffusion, NBMA, point à multipoint ou liaison virtuelle.

État
Niveau fonctionnel d'une interface. L'état détermine si la formation de pleines adjacences est permise ou non sur l'interface. L'état est aussi reflété dans les LSA du routeur.

Adresse IP d'interface
Adresse IP associée à l'interface. Elle apparaît comme l'adresse IP de source dans tous les paquets de protocole d'acheminement générés sur cette interface. Les interfaces avec des réseaux point à point non numérotés n'ont pas d'adresse IP associée.

Gabarit d'interface IP
Aussi appelé gabarit de sous-réseau, il indique la portion de l'adresse IP d'interface qui identifie le réseau de rattachement. Rentrer l'adresse IP d'interface dans le gabarit d'interface IP donne le numéro de réseau IP du réseau de rattachement. Sur les réseaux point à point et les liaisons virtuelles, le gabarit d'interface IP n'est pas défini. Sur ces réseaux, il n'est pas alloué de numéro de réseau IP à la liaison elle-même, et donc les adresses de chaque côté de la liaison sont allouées indépendamment, si il en est alloué.

Identifiant de zone
L'identifiant de zone de la zone à laquelle appartient le réseau de rattachement. Tous les paquets de protocole d'acheminement générés de cette interface sont étiquetés avec cet identifiant de zone.

HelloInterval
Durée, en secondes, entre les paquets Hello que le routeur envoie sur l'interface. Annoncé dans les paquets Hello envoyés par cette interface.

RouterDeadInterval
Nombre de secondes avant que les voisins du routeur ne le déclarent mort, lorsqu'ils cessent d'entendre les paquets Hello du routeur. Annoncé dans les paquets Hello envoyés de cette interface.

InfTransDelay
Nombre estimé de secondes que prend la transmission d'un paquet Mise à jour d'état de liaison sur cette interface. Les LSA contenus dans le paquet Mise à jour d'état de liaison auront leur âge incrémenté de cette quantité avant la transmission. Cette valeur devrait tenir compte des délais de transmission et de propagation ; elle doit être supérieure à zéro.

Priorité de routeur
Entier non signé de 8 bits. Lorsque deux routeurs rattachés à un réseau tentent tous deux de devenir routeur désigné, celui qui a la plus forte priorité de routeur a la préséance. Un routeur dont la priorité de routeur est réglée à 0 est inéligible pour devenir routeur désigné sur le réseau de rattachement. Annoncé dans les paquets Hello envoyés de cette interface.

Temporisateur Hello
Temporisateur d'intervalle qui cause l'envoi d'un paquet Hello par l'interface. Ce temporisateur arrive à expiration toutes les HelloInterval secondes. Noter que sur les réseaux qui ne sont pas en diffusion un paquet Hello distinct est envoyé à chaque voisin qualifié.

Temporisateur d'attente
Temporisateur à utilisation unique qui cause la sortie de l'état Attente de l'interface, et par conséquent choisit un routeur désigné sur le réseau. La durée du temporisateur est de RouterDeadInterval secondes.

Liste des routeurs voisins
Les autres routeurs rattachés à ce réseau. Cette liste est formée par le protocole Hello. Les adjacences seront formées avec certains de ces voisins. L'ensemble des voisins adjacents peut être déterminé par un examen des états de tous les voisins.

Routeur désigné
Routeur désigné choisi pour le réseau de rattachement. Le routeur désigné est choisi sur tous les réseaux NBMA et les réseaux en diffusion par le protocole Hello. Deux éléments d'identification sont gardés pour le routeur désigné : son identifiant de routeur et son adresse IP d'interface sur le réseau. Le routeur désigné annonce l'état de la liaison pour le réseau ; ce LSA de réseau est étiqueté avec l'adresse IP du routeur désigné. Le routeur désigné est initialisé à 0.0.0.0, ce qui indique l'absence de routeur désigné.

Routeur désigné de secours
Le routeur désigné de secours est aussi choisi sur tous les réseaux NBMA et en diffusion par le protocole Hello. Tous les routeurs sur le réseau rattaché deviennent adjacents à la fois au routeur désigné et au routeur désigné de secours. Le routeur désigné de secours devient routeur désigné en cas de défaillance du routeur désigné actuel. Le routeur désigné de secours est initialisé à 0.0.0.0, ce qui indique l'absence de routeur désigné de secours.

Coûts de sortie d'interface
Coût de l'envoi d'un paquet de données sur l'interface, exprimé dans la métrique d'état de liaison. C'est annoncé comme le coût de la liaison pour cette interface dans le LSA de routeur. Le coût d'une interface doit être supérieur à zéro.

RxmtInterval
Nombre de secondes entre les retransmissions de LSA, pour les adjacences qui appartiennent à cette interface. Aussi utilisé lors de la retransmission des paquets Description de base de données et Demande d'état de liaison.

AuType
Type d'authentification utilisé sur le réseau/sous-réseau de rattachement. Les types d'authentification sont définis à l'Appendice D. Tous les échanges de paquets OSPF sont authentifiés. Différents schémas d'authentification peuvent être utilisés sur des réseaux/sous-réseaux différents.

Clé d'authentification
Ces données configurées permettent à la procédure d'authentification de générer et/ou vérifier les paquets de protocole OSPF. La clé d'authentification peut être configurée interface par interface. Par exemple, si le AuType indique un simple mot de passe, la clé d'authentification sera un mot de passe en clair de 64 bits inséré dans l'en-tête du paquet OSPF. Au lieu de cela, si Autype indique une authentification cryptographique, la clé d'authentification sera un secret partagé qui permet la génération/vérification des résumés de message qui sont ajoutés aux paquets de protocole OSPF. Lorsque l'authentification cryptographique est utilisée, plusieurs clés simultanées sont acceptées afin de réaliser une transition en douceur d'une clé à l'autre (voie au paragraphe D.3).

9.1 États d'interface

Les divers états que les interfaces de routeur peuvent atteindre sont exposés dans ce paragraphe. La liste des états est donnée dans l'ordre croissant des fonctionnalités. Par exemple, l'état de non fonctionnement est donné en premier, suivi par une liste d'états intermédiaires avant l'état final, pleinement fonctionnel. La spécification utilise cet ordre en faisant parfois référence à la proposition "interfaces d'état supérieur à X". La Figure 11 donne le graphe des changements d'état de l'interface. Les arcs du graphe sont étiquetés avec l'événement qui cause le changement d'état. Ces événements sont détaillés au paragraphe 9.2. L'automate à état de l'interface est décrit plus en détails au paragraphe 9.3.

Down
C'est l'état initial de l'interface. Dans cet état, les protocoles de niveau inférieur ont indiqué que l'interface est inutilisable. Aucun trafic de protocole ne sera envoyé ni reçu sur une telle interface. Dans cet état, les paramètres de l'interface devraient être réglés à leurs valeurs initiales. Tous les temporisateurs de l'interface devraient être désactivés, et il ne devrait pas y avoir d'adjacences associées à l'interface.

Bouclage
Dans cet état, l'interface du routeur au réseau est en boucle. L'interface peut être mise en boucle matériellement ou logiquement. L'interface sera indisponible pour le trafic régulier de données. Cependant, il peut toujours être souhaitable d'obtenir des informations sur la qualité de cette interface, soit par l'envoi de pings ICMP à l'interface soit par quelque chose comme un essai d'erreurs binaires. Pour cette raison, les paquets IP peuvent toujours être adressés à une interface en état de bouclage. Pour le rendre plus facile, de telles interfaces sont annoncées dans les LSA de routeur comme un seul chemin d'hôte, dont la destination est l'adresse IP d'interface[4].

4 Noter qu'aucun chemin d'hôte n'est généré pour, et aucun paquet IP ne peut être adressé aux interfaces avec des réseaux point à point non numérotés. Ceci sans considération de l'état d'une telle interface.

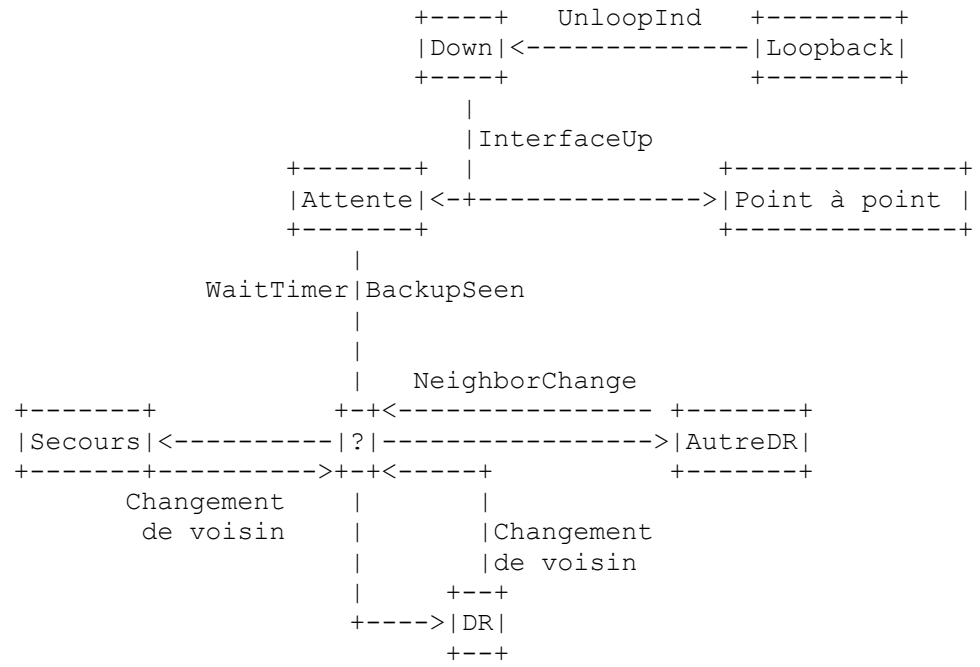


Figure 11 : Changements d'état d'interface

En plus des transitions d'état représentées, l'événement InterfaceDown force l'état Down, et l'événement LoopInd force toujours l'état Bouclage.

Attente
Dans cet état, le routeur essaye de déterminer l'identité du routeur désigné (de secours) pour le réseau. Pour ce faire, le routeur surveille les paquets Hello qu'il reçoit. Il n'est pas permis au routeur de choisir un routeur désigné de secours ni un routeur désigné jusqu'à ce qu'il sorte de l'état Attente. Cela empêche les changements inutiles de routeur désigné (de secours).

Point à point
Dans cet état, l'interface est opérationnelle, et se connecte soit à un réseau point à point physique soit à une liaison virtuelle. En entrant dans cet état, le routeur tente de former une adjacence avec le routeur voisin. Les paquets Hello sont envoyés au voisin toutes les HelloInterval secondes.

Autre DR
L'interface est avec un réseau NBMA ou de diffusion dont un autre routeur a été choisi comme routeur désigné. Dans cet état, le routeur lui-même n'a pas été choisi non plus comme routeur désigné de secours. Le routeur forme des adjacences à la fois avec le routeur désigné et le routeur désigné de secours (si ils existent).

Secours
Dans cet état, le routeur lui-même est le routeur désigné de secours sur le réseau de rattachement. Il sera promu routeur désigné en cas de défaillance du présent routeur désigné. Le routeur établit les adjacences avec tous les autres routeurs rattachés au réseau. Le routeur désigné de secours effectue des fonctions légèrement différentes de celle du routeur désigné durant la procédure d'arrosage (voir au paragraphe 13.3). Voir au paragraphe 7.4 des précisions sur les fonctions effectuées par le routeur désigné de secours.

DR
Dans cet état, ce routeur est lui-même le routeur désigné sur le réseau de rattachement. les adjacences sont établies avec tous les autres routeurs rattachés au réseau. Le routeur doit aussi générer un LSA de réseau pour le nœud de réseau. Le LSA de réseau contiendra les liaisons avec tous les routeurs (y compris le routeur désigné lui-même) rattachés au réseau. Voir au paragraphe 7.3 des précisions sur les fonctions effectuées par le routeur désigné.

9.2 Événements causant des changements d'état de l'interface

Les changements d'état peuvent être opérés par un certain nombre d'événements. Ces événements sont représentés comme les arcs de la Figure 11. La définition des étiquettes est donnée ci-dessous. Pour une explication détaillée des effets de ces événements sur le fonctionnement du protocole OSPF, consulter le paragraphe 9.3.

InterfaceUp
Les protocoles de niveau inférieur ont indiqué que l'interface réseau est opérationnelle. Ceci permet à l'interface de sortir de l'état Down. Sur les liaisons virtuelles, l'indication d'interface opérationnelle résulte en fait du calcul du plus court chemin (voir au paragraphe 16.7).

WaitTimer
Le temporisateur d'attente est arrivé à expiration, indiquant la fin de la période d'attente qui est exigée avant de choisir un routeur désigné (de secours).

BackupSeen
Le routeur a détecté l'existence ou la non-existence d'un routeur désigné de secours pour le réseau. Ceci est fait d'une des deux façons suivantes. D'abord, un paquet Hello peut être reçu d'un voisin revendiquant pour lui-même la fonction de routeur désigné de secours. Autrement, un paquet Hello peut être reçu d'un voisin revendiquant pour lui-même la fonction de routeur désigné, et indiquant qu'il n'y a pas de routeur désigné de secours. Dans les deux cas, il doit y avoir une communication bidirectionnelle avec le voisin, c'est-à-dire que le routeur doit aussi apparaître dans le paquet Hello du voisin. Cet événement signale la fin de l'état d'attente.

NeighborChange
Il y a eu un changement dans l'ensemble des voisins bidirectionnels associés à l'interface. Le routeur désigné (de secours) a besoin d'être recalculé. Les changements de voisins suivants conduisent à l'événement NeighborChange. L'explication des états de voisins figure au paragraphe 10.1.

- Une communication bidirectionnelle a été établie avec un voisin. En d'autres termes, l'état du voisin est passé à 2-Way ou plus haut.
- Il n'y a plus de communication bidirectionnelle avec un voisin. En d'autres termes, l'état du voisin est passé à Init ou inférieur.
- Un des voisins bidirectionnels se déclare lui-même comme routeur désigné ou routeur désigné de secours. Ceci est détecté par l'examen des paquets Hello de ce voisin.
- Un des voisins bidirectionnels ne se déclare plus lui-même comme le routeur désigné, ou ne se déclare plus lui-même comme routeur désigné de secours. Ceci est encore détecté par l'examen des paquets Hello de ce voisin.
- La priorité de routeur annoncée pour un voisin bidirectionnel a changée. Ceci est encore détecté par l'examen des paquets Hello de ce voisin.

LoopInd
L'indication que l'interface est maintenant bouclée sur elle-même a été reçue. Cette indication peut être reçue de la gestion de réseau ou des protocoles de niveau inférieur.

UnloopInd
Une indication a été reçue que l'interface n'est plus en bouclage. Comme avec l'événement LoopInd, cette indication peut être reçue de la gestion de réseau ou des protocoles de niveau inférieur.

InterfaceDown
Les protocoles de niveau inférieur indiquent que cette interface n'est plus fonctionnelle. Quel que soit l'état actuel de l'interface, le nouvel état de l'interface sera Down.

9.3 Automate à états d'interface

Voici une description détaillée des changements d'état de l'interface. Chaque changement d'état est invoqué par un événement (paragraphe 9.2). Cet événement peut produire différents effets, selon l'état en cours de l'interface. Pour cette raison, l'automate à états ci-dessous est organisé par l'état actuel de l'interface et l'événement reçu. Chaque entrée dans l'automate à états décrit le nouvel état résultant de l'interface et l'ensemble exigé d'actions additionnelles.

Lorsqu'un état d'interface change, il peut être nécessaire de générer un nouveau LSA de routeur. Voir des précisions au paragraphe 12.4.

Certaines des actions requises ci-dessous impliquent de générer des événements pour l'automate à états voisin. Par exemple, lorsque une interface devient inopérante, toutes les connexions voisines associées à l'interface doivent être détruites. Pour des informations complémentaires sur l'automate à états voisin, voir au paragraphe 10.3.

États : Down
Événement : InterfaceUp
Nouvel état : Dépend de la routine d'action

Action : Lance le temporisateur d'intervalle de Hello, permettant l'envoi périodique de paquets Hello de l'interface. Si le réseau de rattachement est un réseau point à point physique, un réseau en point à multipoint ou une liaison virtuelle, l'état de l'interface passe à point à point. Autrement, si le routeur n'est pas éligible à devenir routeur désigné, l'état de l'interface passe à Autre DR.

Autrement, le réseau de rattachement est un réseau NBMA ou en diffusion et le routeur est éligible à devenir routeur désigné. Dans ce cas, tentant de découvrir le routeur désigné du réseau de rattachement, l'état de l'interface est réglé à Attente et le temporisateur d'attente à utilisation unique est lancé. De plus, si le réseau est un réseau NBMA, il examine la liste configurée des voisins pour cette interface et génère l'événement voisin Début pour chaque voisin qui est aussi éligible à devenir routeur désigné.

États : Attente
Événement : BackupSeen
Nouvel état : Dépend de la routine d'action.
Action : Calcule le routeur désigné de secours et le routeur désigné du réseau de rattachement, comme indiqué au paragraphe 9.4. En résultat de ce calcul, le nouvel état de l'interface sera Autre DR, Secours ou DR.

États : Attente
Événement : WaitTimer
Nouvel état : Dépend de la routine d'action.
Action : Calcule le routeur désigné de secours et le routeur désigné du réseau de rattachement, comme indiqué au paragraphe 9.4. En résultat de ce calcul, le nouvel état de l'interface sera Autre DR, Secours ou DR.

États : Autre DR, Secours ou DR
Événement : NeighborChange
Nouvel état : Dépend de la routine d'action.
Action : Recalcule le routeur désigné de secours et le routeur désigné du réseau de rattachement, comme indiqué au paragraphe 9.4. En résultat de ce calcul, le nouvel état de l'interface sera Autre DR, Secours ou DR.

États : Tout état
Événement : InterfaceDown
Nouvel état : Down
Action : Toutes les variables de l'interface sont réinitialisées, et les temporisateurs de l'interface sont désactivés. Aussi, toutes les connexions voisines associées à l'interface sont détruites. Ceci est fait en générant l'événement KillNbr sur tous les voisins associés (voir au paragraphe 10.2).

États : Tout état
Événement : LoopInd
Nouvel état : Bouclage
Action : Comme cette interface n'est plus connectée au réseau de rattachement, les actions associées à l'événement InterfaceDown ci-dessus sont exécutées.

États : Bouclage
Événement : UnloopInd
Nouvel état : Down
Action : Aucune actions n'est nécessaire. Par exemple, les variables de l'interface ont déjà été réinitialisées en entrant dans l'état Bouclage. Noter que la réception d'un événement InterfaceUp est nécessaire avant que l'interface ne redevienne pleinement fonctionnelle.

9.4 Choix du routeur désigné

Ce paragraphe décrit l'algorithme utilisé pour le calcul du routeur désigné et du routeur désigné de secours du réseau. Cet algorithme est invoqué par l'automate à état de l'interface. La première fois qu'un routeur fait fonctionner l'algorithme de sélection pour un réseau, le routeur désigné et le routeur désigné de secours du réseau sont initialisés à 0.0.0.0. Cela indique l'absence à la fois de routeur désigné et de routeur désigné de secours.

L'algorithme de sélection de routeur désigné procède comme suit : appelons Routeur X le routeur qui fait le calcul. La liste des voisins rattachés au réseau et qui ont établi des communications bidirectionnelles avec le Routeur X est examinée. Cette liste est précisément la collection des voisins du Routeur X (sur ce réseau) dont l'état est supérieur ou égal à 2-Way (voir le paragraphe 10.1). Le Routeur X lui-même est aussi considéré comme étant sur la liste. Éliminer de la liste tous les routeurs qui ne sont pas éligibles à devenir routeur désigné. (Les routeurs qui ont la priorité de routeur de 0 sont inéligibles à devenir routeur désigné.) Les étapes suivantes sont alors exécutées, en considérant seulement les routeurs qui restent sur la liste :

(1) Noter les valeurs actuelles du routeur désigné et du routeur désigné de secours pour le réseau. Ceci sera utilisé ensuite pour des comparaisons.

(2) Calculer le nouveau routeur désigné de secours pour le réseau comme suit. Seuls les routeurs de la liste qui ne se sont

pas déclarés eux-mêmes comme étant le routeur désigné sont éligibles à devenir routeur désigné de secours. Si un ou plusieurs de ces routeurs se sont déclarés eux-mêmes comme routeur désigné de secours (c'est-à-dire qu'ils s'annoncent actuellement eux-mêmes comme routeur désigné de secours, mais pas comme routeur désigné, dans leurs paquets Hello) celui qui a la plus forte priorité de routeur est déclaré être le routeur désigné de secours. En cas de concurrence, on choisit celui qui a le plus fort identifiant de routeur. Si aucun routeur ne s'est déclaré lui-même comme routeur désigné de secours, choisir le routeur qui a la plus forte priorité de routeur (toujours en excluant les routeurs qui se sont déclarés eux-mêmes routeur désigné) et à nouveau en utilisant l'identifiant de routeur pour résoudre les conflits.

(3) Calculer le nouveau routeur désigné pour le réseau comme suit. Si un ou plusieurs routeurs se sont déclarés eux-mêmes comme routeur désigné (c'est-à-dire qu'ils s'annoncent actuellement comme routeur désigné dans leurs paquets Hello) celui qui a la plus forte priorité de routeur est déclaré routeur désigné. En cas de concurrence, celui qui a le plus fort identifiant de routeur est choisi. Si aucun routeur ne s'est déclaré lui-même comme routeur désigné, allouer le titre de routeur désigné au même que celui qui vient d'être choisi comme routeur désigné de secours.

(4) Si le routeur X est maintenant le nouveau routeur désigné ou le nouveau routeur désigné de secours, ou n'est plus le routeur désigné ou plus le routeur désigné de secours, répéter les étapes 2 et 3, puis passer à l'étape 5. Par exemple, si le routeur X est maintenant le routeur désigné, lorsque l'étape 2 est répétée, X ne sera plus éligible comme routeur désigné de secours. Entre autres choses, cela va garantir qu'aucun routeur ne se déclarera lui-même à la fois routeur désigné de secours et routeur désigné[5].

(5) En résultat de ces calculs, le routeur lui-même peut maintenant être routeur désigné ou routeur désigné de secours. Voir aux paragraphes 7.3 et 7.4 les devoirs additionnels que cela entraîne. L'état de l'interface du routeur devrait être réglé en conséquence. Si le routeur lui-même est maintenant routeur désigné, le nouvel état de l'interface est DR. Si le routeur lui-même est maintenant routeur désigné de secours, le nouvel état de l'interface est Secours. Autrement, le nouvel état de l'interface est Autre DR.

(6) Si le réseau de rattachement est un réseau NBMA, et si le routeur lui-même vient de devenir routeur désigné ou routeur désigné de secours, il doit commencer à envoyer des paquets Hello à ceux des voisins qui ne sont pas éligibles à devenir routeur désigné (voir au paragraphe 9.5.1). Ceci est fait en invoquant l'événement de voisin Début pour chaque voisin qui a une priorité de routeur de 0.

(7) Si les calculs ci-dessus ont causé un changement d'identité du routeur désigné ou du routeur désigné de secours, l'ensemble d'adjacences associées à cette interface devra être modifié. Certaines adjacences pourront devoir être formées, et d'autres devoir être rompues. Pour faire cela, invoquer l'événement AdjOK? sur tous les voisins dont l'état est au moins 2-Way. Cela causera le réexamen de leur éligibilité à l'adjacence (voir les paragraphes 10.3 et 10.4).

La raison de la complexité de l'algorithme de sélection est le désir d'une transition ordonnée du routeur désigné de secours au routeur désigné, en cas de défaillance du routeur désigné actuel. Cette transition ordonnée est assurée par l'introduction de l'hystérésis : aucun nouveau routeur désigné de secours ne peut être choisi tant que le vieux routeur de secours n'accepte pas sa nouvelle responsabilité de routeur désigné.

La procédure ci-dessus peut choisir le même routeur comme routeur désigné et routeur désigné de secours, mais ce routeur ne sera jamais le routeur qui fait le calcul lui-même (le Routeur X). Le routeur désigné choisi peut n'être pas le routeur qui a la plus forte priorité de routeur, et le routeur désigné de secours n'a pas nécessairement la seconde plus forte priorité de routeur. Si le Routeur X n'est pas lui-même éligible pour devenir le routeur désigné, il est possible que ni un routeur désigné de secours ni un routeur désigné ne soient choisis dans la procédure ci-dessus. Noter aussi que si le Routeur X est le seul routeur rattaché éligible pour devenir routeur désigné, il va se sélectionner lui-même comme routeur désigné et il n'y aura pas de routeur désigné de secours pour le réseau.

9.5 Envoi des paquets Hello

Les paquets Hello sont envoyés par chaque interface de routeur qui fonctionne. Ils sont utilisés pour découvrir et maintenir les relations de voisinage[6]. Sur les réseaux NBMA et de diffusion, les paquets Hello sont aussi utilisés pour choisir le

5 Il est instructif de voir ce qui arrive lorsque le routeur désigné réseau a une défaillance. Soit RT1 le routeur désigné pour le réseau et RT2 le routeur désigné de secours. Si RT1 lâche (ou si son interface réseau lâche), les autres routeurs du réseau vont détecter l'absence de RT1 dans RouterDeadInterval secondes. Tous les routeurs peuvent ne pas détecter cela au même moment précis ; les routeurs qui détectent l'absence de RT1 avant RT2 vont, pour un temps, choisir RT2 à la fois comme routeur désigné et routeur désigné de secours. Lorsque RT2 détecte que RT1 est parti, il va passer de lui-même en routeur désigné. À ce moment, le routeur restant à la plus forte priorité de routeur sera choisi comme routeur désigné de secours.

6 Sur les réseaux en point à point, les protocoles de niveau inférieur indiquent si le voisin est éveillé et actif. De plus, l'existence du

routeur désigné et le routeur désigné de secours.

Le format d'un paquet Hello est détaillé au paragraphe A.3.2. Le paquet Hello contient la priorité de routeur du routeur (utilisée pour choisir le routeur désigné) et l'intervalle entre paquets Hello envoyés de l'interface (HelloInterval). Le paquet Hello indique aussi la fréquence à laquelle un voisin doit être écouté pour rester actif (RouterDeadInterval). Les HelloInterval et RouterDeadInterval doivent tous deux être les mêmes pour tous les routeurs rattachés à un réseau commun. Le paquet Hello contient aussi le gabarit d'adresse IP du réseau de rattachement (Gabarit de réseau). Sur les réseaux point à point non numérotés et sur les liaisons virtuelles ce champ devrait être réglé à 0.0.0.0.

Le champ Options du paquet Hello décrit les capacités OSPF facultatives du routeur. Une capacité facultative est définie dans la présente spécification (voir aux paragraphes 4.5 et A.2). Le bit E du champ Options devrait être établi si et seulement si la zone rattachée est capable de traiter les LSA externes à l'AS (c'est-à-dire, si ce n'est pas une zone de bout). Si le bit E est réglé de façon incorrecte, les routeurs voisins vont refuser d'accepter le paquet Hello (voir le paragraphe 10.5). Les bits non reconnus dans le champ Options du paquet Hello devraient être réglés à zéro.

Pour assurer une communication bidirectionnelle entre routeurs adjacents, le paquet Hello contient la liste de tous les routeurs du réseau d'où des paquets Hello ont été vus récemment. Le paquet Hello contient aussi le choix actuel du routeur du routeur désigné et du routeur désigné de secours. Une valeur de 0.0.0.0 dans ces champs signifie qu'il n'en a pas encore été choisi un.

Sur les réseaux de diffusion et les réseaux point à point physiques, les paquets Hello sont envoyés toutes les HelloInterval secondes à l'adresse de diffusion groupée IP AllSPFRouters. Sur les liaisons virtuelles, les paquets Hello sont envoyés en envoi individuel (adressés directement à l'autre extrémité de la liaison virtuelle) toutes les HelloInterval secondes. Sur les réseaux en point à multipoint, des paquets Hello distincts sont envoyés à chaque voisin rattaché toutes les HelloInterval secondes. L'envoi des paquets Hello sur les réseaux NBMA est traité dans le paragraphe suivant.

9.5.1 Envoi des paquets Hello sur les réseaux NBMA

Les informations de configuration statique peuvent être nécessaires afin que le protocole Hello fonctionne sur les réseaux qui ne sont pas en diffusion (voir aux paragraphes C.5 et C.6). Sur les réseaux NBMA, chaque routeur rattaché qui est éligible à devenir routeur désigné obtient la connaissance de tous ses voisins sur le réseau (soit par configuration, soit par un mécanisme non spécifié). Chaque voisin est étiqueté avec l'éligibilité de routeur désigné du voisin.

L'état de l'interface doit être au moins Attente pour tout paquet Hello envoyé de l'interface NBMA. Les paquets Hello sont alors envoyés directement (en envoi individuel) à un ensemble de voisins du routeur. Parfois, un paquet Hello est envoyé périodiquement sur un temporisateur ; d'autres fois, il est envoyé en réponse à un paquet Hello reçu. Le comportement d'envoi des hello d'un routeur varie selon que le routeur est ou non lui-même éligible à devenir routeur désigné.

Si le routeur est éligible à devenir routeur désigné, il doit périodiquement envoyer des paquets Hello à tous les voisins qui sont aussi éligibles. De plus, si le routeur est lui-même le routeur désigné ou le routeur désigné de secours, il doit aussi envoyer des paquets Hello périodiques à tous les autres voisins. Cela signifie que deux routeurs éligibles quelconques échangent toujours des paquets Hello, ce qui est nécessaire pour le fonctionnement correct de l'algorithme de sélection du routeur désigné. Pour minimiser le nombre de paquets Hello envoyés, le nombre de routeurs éligibles sur un réseau NBMA devrait être gardé faible.

Si le routeur n'est pas éligible à devenir routeur désigné, il doit périodiquement envoyer des paquets Hello à la fois au routeur désigné et au routeur désigné de secours (si ils existent). Il doit aussi envoyer un paquet Hello en réponse à un paquet Hello reçu de tout voisin éligible (autre que le routeur désigné et routeur désigné de secours actuels). Ceci est nécessaire pour établir une relation bidirectionnelle initiale avec tout routeur désigné potentiel.

Lors de l'envoi des paquets Hello périodiques à tout voisin, l'intervalle entre les paquets Hello est déterminé par l'état du voisin. Si le voisin est dans l'état Down, les paquets Hello sont envoyés toutes les PollInterval secondes. Autrement, les paquets Hello sont envoyés toutes les HelloInterval secondes.

10. Structure des données du voisin

Un routeur OSPF converse avec ses routeurs voisins. Chaque conversation distincte est décrite par une "structure de

---

voisin est indiquée sur les liaisons virtuelles par le calcul du tableau d'acheminement. Cependant, dans ces deux cas, le protocole Hello est encore utilisé. Cela assure que la communication entre les voisins est bidirectionnelle, et que chacun des voisins a une couche de protocole d'acheminement qui fonctionne.

données voisine". Chaque conversation est liée à une interface particulière de routeur OSPF, et est identifiée par l'identifiant de routeur OSPF du routeur voisin ou par son adresse IP de voisin (voir ci-dessous). Et donc, si le routeur OSPF et un autre routeur ont plusieurs réseaux de rattachement en commun, plusieurs conversations s'ensuivent, chacune étant décrite par une structure unique de données voisine. Chaque conversation distincte est mentionnée dans le texte comme étant un "voisin" distinct.

La structure de données voisine contient toutes les informations pertinentes pour la formation des adjacences ou pour les adjacences formées entre les deux voisins. (Cependant, il faut se rappeler que tous les voisins ne deviennent pas adjacents.) Une adjacence peut être vue comme une conversation très développée entre deux routeurs.

État
Niveau fonctionnel de la conversation de voisin. Ceci est précisé au paragraphe 10.1.

Temporisateur d'inactivité
Temporisateur à utilisation unique dont l'expiration indique qu'aucun paquet Hello n'a été vu récemment de ce voisin. La durée du temporisateur est de RouterDeadInterval secondes.

Maître/esclave
Lorsque les deux voisins échangent leurs bases de données, ils forment une relation de maître/esclave. Le maître envoie la premier paquet de description de base de données, et est le seul admis à retransmettre. L'esclave peut seulement répondre aux paquets de description de base de données du maître. La relation maître/esclave est négociée dans l'état ExStart.

Numéro de séquence DD
Numéro de séquence DD du paquet de description de base de données qui est en train d'être envoyé au voisin.

Dernier paquet de description de base de données reçu
Les bits initialise (I), plus (M) et maître (MS), le champ Options, et le numéro de séquence DD contenus dans le dernier paquet de description de base de données reçu du voisin. Utilisé pour déterminer si le prochain paquet de description de base de données reçu du voisin est un duplicata.

Identifiant de voisin
Identifiant de routeur OSPF du routeur voisin. L'identifiant de voisin est appris lors de la réception des paquets Hello du voisin, ou est configuré si il s'agit d'une adjacence virtuelle (voir le paragraphe C.4).

Priorité de voisin
La priorité de routeur du routeur voisin. Contenue dans les paquets Hello du voisin, cet élément est utilisé lors du choix du routeur désigné pour le réseau de rattachement.

Adresse IP de voisin
L'adresse IP de l'interface au réseau de rattachement du routeur voisin. Utilisée comme adresse de destination IP lorsque des paquets de protocole sont envoyés en envoi individuel le long de cette adjacence. Aussi utilisé dans les LSA de routeur comme l'identifiant de liaison pour le réseau de rattachement si le routeur voisin est choisi comme routeur désigné (voir le paragraphe 12.4.1). L'adresse IP de voisin est apprise lorsque les paquets Hello sont reçus du voisin. Pour les liaisons virtuelles, l'adresse IP du voisin est apprise durant le processus de construction du tableau d'acheminement (voir la section 15).

Options de voisin
Capacités OSPF facultatives prises en charge par le voisin. Apprises durant le processus d'échange de base de données (voir au paragraphe 10.6). La liste des capacités OSPF facultatives du voisin est aussi dans ses paquets Hello. Cela permet de rejeter les paquets Hello reçus (c'est-à-dire que les relations de voisinage ne commenceront jamais à se former) si il y a une discordance dans certaines capacités OSPF cruciales (voir au paragraphe 10.5). Les capacités OSPF facultatives sont exposées au paragraphe 4.5.

Routeur désigné du voisin
Idée que se fait le voisin du routeur désigné. Si c'est le voisin lui-même, c'est important dans le calcul local du routeur désigné. N'est défini que sur les réseaux NBMA et en diffusion.

Routeur désigné de secours du voisin
Idée que se fait le voisin du routeur désigné de secours. Si c'est le voisin lui-même, c'est important dans le calcul local du routeur désigné de secours. N'est défini que sur les réseaux NBMA et en diffusion.

L'ensemble de variables suivant est la liste des LSA. Ces listes décrivent des sous-ensembles de la base de données d'états de liaisons de la zone. Le présent mémoire définit cinq types distincts de LSA, dont tous peuvent être présents dans une base de données d'états de liaisons de zone : LSA de routeur, LSA de réseau, et LSA résumé de type 3 et 4 (tous mémorisés dans la structure de données de la zone), et LSA externes à l'AS (mémorisés dans la structure de données globale).

Liste de retransmission des états de liaison
: Liste des LSA qui ont été écoulés sur cette adjacence mais dont il n'a pas été accusé réception. Ils seront retransmis périodiquement jusqu'à ce qu'il en soit accusé réception, ou jusqu'à ce que l'adjacence soit détruite.

Liste sommaire de la base de données
: Liste complète des LSA qui constituent la base de données d'états de liaisons de la zone, au moment où le voisin entre dans l'état Échange de base de données. Cette liste est envoyée au voisin dans les paquets de description de base de données.

Liste des demandes d'état de liaison
: Liste des LSA qui doivent être reçus de ce voisin afin de synchroniser les bases de données d'états de liaisons des deux voisins. Cette liste est crée lorsque les paquets de description de base de données sont reçus, et est ensuite envoyée au voisin dans les paquets de demande d'état de liaison. La liste diminue alors que sont reçus les paquets appropriés de mise à jour d'état de liaison.

10.1 États du voisin

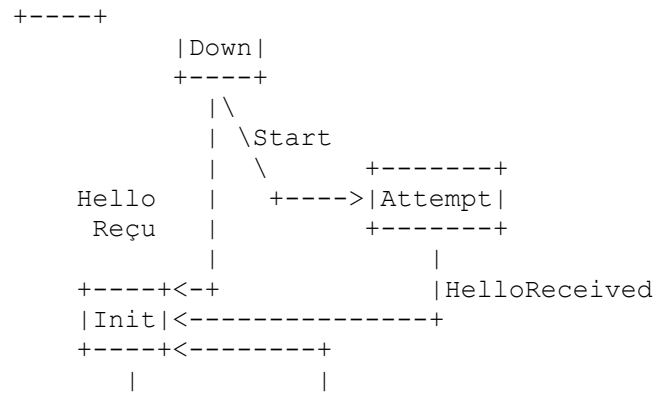
L'état d'un voisin (en fait l'état d'une conversation qui se tient avec un routeur voisin) est exposé dans les paragraphes suivants. La liste des états est dans l'ordre croissant des fonctionnalités. Par exemple, l'état de non fonctionnement figure en premier sur la liste, suivi par une liste d'états intermédiaires avant la réalisation de l'état final, pleinement fonctionnel. La spécification utilise cet ordre pour faire parfois des références telles que "les voisins/adjacences dans un état supérieur à X". Les Figures 12 et 13 montrent le graphe des changements d'état de voisin. Les arcs des graphes sont étiquetés avec l'événement qui cause le changement d'état. Les événements du voisin sont exposés au paragraphe 10.2.

Le graphe de la Figure 12 montre les changements d'état effectués par le protocole Hello. Le protocole Hello est responsable de l'acquisition et de la maintenance des voisins, et de s'assurer de la communication bidirectionnelle entre voisins.

Le graphe de la Figure 13 montre la formation d'une adjacence. Tous les routeurs voisins ne deviennent pas adjacents (voir au paragraphe 10.4). L'adjacence commence à se former lorsque le voisin est dans l'état ExStart. Après que les deux routeurs ont découvert leur statut de maître/esclave, l'état passe à Échange. À ce point, le voisin commence à être utilisé dans la procédure d'arrosage, et les deux routeurs voisins commencent à synchroniser leurs bases de données. Lorsque cette synchronisation est finie, le voisin est dans l'état Plein et on dit que les deux routeurs sont pleinement adjacents. À ce moment l'adjacence est annoncée dans les LSA.

Pour une description plus détaillée des changements d'état de voisin, ainsi que des actions supplémentaires impliquées dans chaque changement, voir au paragraphe 10.3.

Down
: C'est l'état initial d'une conversation de voisins. Il indique qu'il n'y a pas eu d'informations récentes reçues du voisin. Sur les réseaux NBMA, les paquets Hello peuvent cependant être envoyés à des voisins "Down", bien qu'à une fréquence réduite (voir au paragraphe 9.5.1).



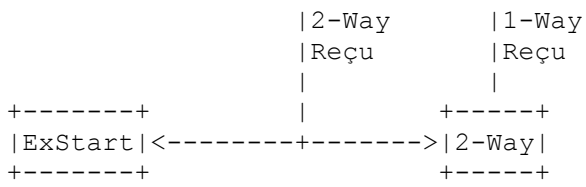


Figure 12 : Changements d'état du voisin (protocole Hello)

En plus des transitions d'état décrites, les événements KillNbr, InactivityTimer et LLDown forcent toujours l'état Down.

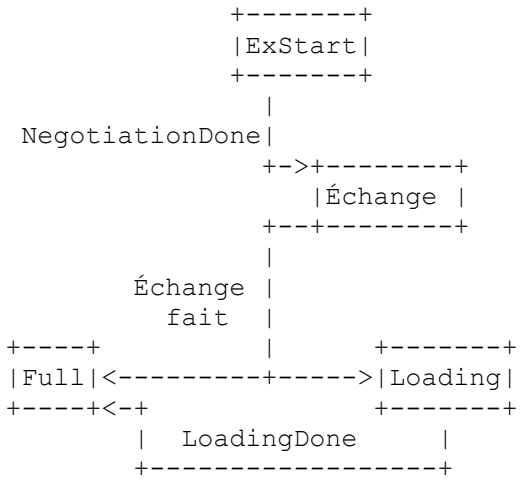


Figure 13 : Changements d'état du voisin (Échange de base de données)

En plus des transitions d'état décrites, l'événement SeqNumberMismatch force l'état ExStart, l'événement BadLSReq force l'état ExStart, l'événement 1-Way force l'état Init, l'événement KillNbr force toujours l'état Down, l'événement InactivityTimer force toujours l'état Down, l'événement LLDown force toujours l'état Down, et l'événement AdjOK? conduit à la formation/rupture d'adjacence.

Attempt
Cet état n'est valide que pour des voisins rattachés à des réseaux NBMA. Il indique qu'aucune information récente n'a été reçue du voisin, mais que des efforts plus concertés devraient être faits pour contacter le voisin. Ceci est fait en envoyant au voisin des paquets Hello à l'intervalle de HelloInterval (voir au paragraphe 9.5.1).

Init
Dans cet état, un paquet Hello du voisin a été vu récemment. Cependant, la communication bidirectionnelle n'a pas encore été établie avec le voisin (c'est-à-dire, le routeur lui-même n'apparaît pas dans le paquet Hello du voisin). Tous les voisins dans cet état (ou supérieur) figurent dans les paquets Hello envoyés de l'interface associée.

2-Way
Dans cet état, la communication entre les deux routeurs est bidirectionnelle. Ceci a été assuré par le fonctionnement du protocole Hello. C'est l'état le plus avancé peu avant le début de l'établissement de l'adjacence. Le routeur désigné (de secours) est choisi dans l'ensemble des voisins qui sont dans l'état 2-Way ou supérieur.

ExStart
C'est la première étape de la création d'une adjacence entre les deux routeurs voisins. Le but de cette étape est de décider quel routeur est le maître, et de décider du numéro de séquence DD initial. Les conversations de voisins dans cet état ou supérieur sont appelées adjacences.

Échange
Dans cet état le routeur décrit sa base de données d'état de liaison toute entière en envoyant au voisin des paquets de description de base de données. Chaque paquet de description de base de données a un numéro de séquence DD, et est explicitement acquitté. Un seul paquet de description de base de données est permis à un instant donné. Dans cet état, les paquets de demande d'état de liaison peuvent aussi être envoyés en demandant les LSA les plus récents du voisin. Toutes les adjacences dans l'état Échange ou supérieur sont utilisées pour la procédure d'arrosage. En fait, ces adjacences sont parfaitement capables d'émettre et recevoir tous types de paquets de protocole d'acheminement OSPF.

Loading
Dans cet état, les paquets de demande d'état de liaison sont envoyés au voisin en demandant les LSA les plus récents qui ont été découverts (mais pas encore reçus) dans l'état Échange.

Full
Dans cet état, les routeurs voisins sont pleinement adjacents. Ces adjacences vont maintenant apparaître dans les LSA de routeur et les LSA de réseau.

10.2 Événements causant des changements d'état de voisin

Les changements d'état peuvent être effectués par un certain nombre d'événements. Ces événements sont indiqués dans les étiquettes des arcs des Figures 12 et 13. La définition des étiquettes est la suivante :

Hello reçu
Un paquet Hello a été reçu du voisin.

Début
C'est l'indication que les paquets Hello devraient maintenant être envoyés au voisin à des intervalles de HelloInterval secondes. Cet événement est généré seulement pour les voisins associés aux réseaux NBMA.

2-Way reçu
Une communication bidirectionnelle a été réalisée entre les deux routeurs voisins. Ceci est indiqué par le routeur qui se voit lui-même dans le paquet Hello du voisin.

Négociation Faite
La relation maître/esclave a été négociée, et les numéros de séquence DD ont été échangés. Cela signale le début de l'envoi/réception des paquets de description de base de données. Pour plus d'informations sur la génération de cet événement, consulter le paragraphe 10.8.

Echange Fait
Les deux routeurs ont réussi à transmettre une pleine séquence de paquets de description de base de données. Chaque routeur sait maintenant quelles parties de sa base de données d'état de liaison sont périmées. Pour des informations complémentaires sur la génération de cet événement, consulter le paragraphe 10.8.

BadLSReq
Une demande d'état de liaison a été reçue pour un LSA non contenu dans la base de données. Cela indique une erreur dans le processus d'échange de base de données.

Loading Fait
Les mises à jour d'état de liaison ont été reçues pour toutes les portions périmées de la base de données. Ceci est indiqué par le fait que la liste des demandes d'état de liaisons devient vide après l'achèvement du processus d'échange de base de données.

AdjOK?
Une décision doit être prise sur la question de savoir si une adjacence devrait être établie/maintenue avec le voisin. Cet événement commencera la formation de certaines adjacences, et en détruira d'autres.

Les événements suivants causent le retour de voisins pleinement développés à des états inférieurs. À la différence des événements ci-dessus, ces événements peuvent survenir lorsque la conversation de voisin est dans l'un de ces états.

SeqNumberMismatch
Un paquet de description de base de données a été reçu qui : a) a un numéro de séquence DD inattendu, b) a le bit Init établi contre toute attente ou c) a un champ Options différant du dernier champ Options reçu dans un paquet de description de base de données. Une de ces conditions indique qu'une erreur est survenue durant l'établissement de l'adjacence.

1-Way
Un paquet Hello a été reçu du voisin, dans lequel le routeur n'est pas mentionné. Cela indique que la communication avec le voisin n'est pas bidirectionnelle.

KillNbr
C'est l'indication que toutes les communications avec le voisin sont maintenant impossibles, forçant le voisin à revenir à l'état Down.

InactivityTimer

Le temporisateur d'inactivité est arrivé à expiration. Cela signifie qu'aucun paquet Hello n'a été vu récemment en provenance du voisin. Le voisin revient à l'état Down.

LLDown
C'est l'indication provenant des protocoles de niveau inférieurs que le voisin est maintenant injoignable. Par exemple, sur un réseau X.25, cela pourrait être indiqué par une indication X.25 claire avec les champs de cause et de diagnostic appropriés. Cet événement force le voisin à passer à l'état Down.

10.3 Automate à états de voisin

Une description détaillée des changements d'état du voisin suit. Chaque changement d'état est invoqué par un événement (paragraphe 10.2). Cet événement peut produire différents effets, selon l'état actuel du voisin. Pour cette raison, l'automate à états ci-dessous est organisé par l'état actuel du voisin et l'événement reçu. Chaque entrée dans l'automate décrit le nouvel état de voisin résultant et l'ensemble des actions supplémentaires requises.

Lorsqu'un voisin change d'état, il peut être nécessaire de refaire fonctionner l'algorithme de sélection du routeur désigné. Ceci est déterminé par le fait qu'est généré l'événement NeighborChange à l'interface (voir au paragraphe 9.2). Aussi, si l'interface est dans l'état DR (le routeur est lui-même routeur désigné), les changements d'état du voisin peuvent causer la génération d'un nouveau LSA de réseau (voir au paragraphe 12.4).

Lorsque l'automate du voisin a besoin d'invoquer l'automate d'états de l'interface, cela devrait être fait comme une tâche programmée (voir au paragraphe 4.4). Cela simplifie les choses, en assurant qu'aucun des automates ne fonctionnera de façon récurrente.

État : Down
Événement : Début
Nouvel état : Attempt
Action : Envoi un paquet Hello au voisin (ce voisin est toujours associé à un réseau NBMA) et lance le temporisateur d'inactivité pour le voisin. L'arrivée à expiration ultérieure du temporisateur indiquerait que la communication avec le voisin n'a pas abouti.

État : Attempt
Événement : Hello reçu
Nouvel état : Init
Action : Redémarre le temporisateur d'inactivité pour le voisin, car le voisin a maintenant été entendu.

État : Down
Événement : Hello reçu
Nouvel état : Init
Action : Lance le temporisateur d'inactivité pour le voisin. L'arrivée à expiration ultérieure du temporisateur indiquerait que le voisin est mort.

État : Init ou supérieur
Événement : Hello reçu
Nouvel état : Pas de changement d'état.
Action : Redémarre le temporisateur d'inactivité pour le voisin, car le voisin a de nouveau donné de ses nouvelles.

État : Init
Événement : 2-Way reçu
Nouvel état : Dépend de la routine d'action.
Action : Détermine si une adjacence devrait être établie avec le voisin (voir au paragraphe 10.4). Si c'est non, le nouvel état du voisin est 2-Way. Autrement (une adjacence devrait être établie) l'état du voisin passe à ExStart. En entrant dans cet état, le routeur incrémente le numéro de séquence DD dans la structure de données du voisin. Si c'est la première fois qu'une adjacence est tentée, le numéro de séquence DD devrait être alloué à une valeur univoque (comme celle de l'horloge). Il se déclare alors lui-même maître (établit le bit maître/esclave à maître), et commence à envoyer des paquets de description de base de données, dont les bits initialiser (I), plus (M) et maître (MS) sont mis à 1. Ce paquet de description de base de données devrait autrement être vide. Ce paquet de description de base de données devrait être retransmis à l'intervalle de RxmtInterval jusqu'à ce qu'on entre dans le nouvel état (voir au paragraphe 10.8).

État : ExStart
Événement : Négociation Faite

Nouvel état : Échange
Action : Le routeur doit faire la liste des contenus de sa base de données d'états de liaison de zone entière dans le résumé de base de données du voisin. La base de données d'états de liaison de zone comporte les LSA de routeur, les LSA de réseau et les LSA de résumé contenus dans la structure de zone, avec les LSA externes à l'AS contenus dans la structure globale. Les LSA externes à l'AS sont omis dans une liste de résumés de base de données d'un voisin virtuel. Les LSA externes à l'AS sont omis dans une liste de résumés de base de données si la zone a été configurée comme bout (voir au paragraphe 3.6). Au lieu de cela, les LSA dont l'âge est égal à MaxAge sont ajoutés à la liste de retransmission d'état de liaison du voisin. Un résumé de la liste de résumés de base de données sera envoyé au voisin dans les paquets de description de base de données. Chaque paquet de description de base de données a un numéro de séquence DD, et reçoit un accusé de réception explicite. Un seul paquet de description de base de données en cours est admis à un instant donné. Pour des précisions sur l'envoi et la réception de paquets de description de base de données, voir aux paragraphes 10.8 et 10.6.

État : Échange
Événement : Echange Fait
Nouvel état : Dépend de la routine d'action.
Action : Si la liste de demande d'état de liaison du voisin est vide, le nouvel état du voisin est Full. Aucune autre action n'est exigée. C'est l'état final d'une adjacence. Autrement, le nouvel état du voisin est Loading. On commence (ou continue) d'envoyer des paquets de demande d'état de liaison au voisin (voir au paragraphe 10.9). Ce sont des demandes des LSA les plus récents du voisin (qui ont été découverts mais pas encore reçus dans l'état Échange). La liste de ces LSA figure dans la liste des demandes d'état de liaison associée au voisin.

État : Loading
Événement : Loading Fait
Nouvel état : Full
Action : Pas d'action requise. C'est un état final d'adjacence.

État : 2-Way
Événement : AdjOK?
Nouvel état : Dépend de la routine d'action.
Action : Détermine si une adjacence devrait être formée avec le routeur voisin (voir au paragraphe 10.4). Si c'est non, l'état du voisin reste à 2-Way. Autrement, transition de l'état du voisin à ExStart et exécution des actions associées à l'entrée d'automate ci-dessus pour l'état Init et l'événement 2-Way reçu.

État : ExStart ou supérieur
Événement : AdjOK?
Nouvel état : Dépend de la routine d'action.
Action : Détermine si le routeur voisin devrait encore être adjacent. Si c'est oui, il n'y a pas de changement d'état et aucune autre action n'est nécessaire. Autrement, l'adjacence (éventuellement partiellement formée) doit être détruite. L'état du voisin passe à 2-Way. Les listes Retransmission d'état de liaison, Résumé de base de données et Demandes d'état de liaison sont éliminées des LSA.

État : Échange ou supérieur.
Événement : SeqNumberMismatch
Nouvel état : ExStart
Action : L'adjacence (éventuellement partiellement formée) est rompue, et ensuite il est tenté de la rétablir. L'état du voisin passe d'abord à ExStart. Les listes Retransmission d'état de liaison, Résumé de base de données et Demande d'état de liaison sont éliminées des LSA. Le routeur incrémente ensuite le numéro de séquence DD dans la structure de données du voisin, se déclare lui-même maître (règle le bit maître/esclave à maître), et commence à envoyer des paquets de description de base de données, avec les bits initialise (I), plus (M) et maître (MS) mis à 1. Ce paquet de description de base de données devrait autrement être vide (voir au paragraphe 10.8).

État : Échange ou supérieur
Événement : BadLSReq
Nouvel état : ExStart
Action : L'action pour l'événement BadLSReq est exactement la même que pour l'événement voisin SeqNumberMismatch. L'adjacence (éventuellement partiellement formée) est rompue, et ensuite il est tenté de la rétablir. Pour des précisions, voir l'entrée d'automate du voisin qui est invoquée lors de la génération de l'événement SeqNumberMismatch dans l'état Échange ou supérieur.

État : Tout état
Événement : KillNbr
Nouvel état : Down
Action : Les listes Retransmission d'état de liaison, Résumé de base de données et Demandes d'état de liaison sont éliminées des LSA. Le temporisateur d'inactivité est aussi désactivé.

État : Tout état
Événement : LLDown
Nouvel état : Down
Action : Les listes Retransmission d'état de liaison, Résumé de base de données et Demande d'état de liaison sont éliminées des LSA. Le temporisateur d'inactivité est aussi désactivé.

État : Tout état
Événement : InactivityTimer
Nouvel état : Down
Action : Les listes Retransmission d'état de liaison, Résumé de base de données et Demandes d'état de liaison sont éliminées des LSA.

État : 2-Way ou supérieur
Événement : 1-Way reçu
Nouvel état : Init
Action : Les listes Retransmission d'état de liaison, Résumé de base de données et Demande d'état de liaison sont éliminées des LSA.

État : 2-Way ou supérieur
Événement : 2-Way reçu
Nouvel état : Pas de changement d'état
Action : Pas d'action requise.

État : Init
Événement : 1-Way reçu
Nouvel état : Pas de changement d'état.
Action : Pas d'action requise.

10.4 Quand devenir adjacent

Les adjacences sont établies avec un sous-ensemble des voisins du routeur. Les routeurs connectés par des réseaux point à point, des réseaux en point à multipoint et des liaisons virtuelles deviennent toujours adjacents. Sur les réseaux NBMA et en diffusion, les routeurs deviennent adjacents à la fois au routeur désigné et au routeur désigné de secours.

La décision de former l'adjacence survient en deux endroits dans l'automate à états du voisin. D'abord, lorsque la communication bidirectionnelle est initialement établie avec le voisin, et ensuite, lorsque change l'identité du routeur désigné (de secours) du réseau de rattachement. Si la décision est prise de ne pas tenter une adjacence, l'état de la communication de voisin s'arrête à 2-Way.

Une adjacence devrait être établie avec un voisin bidirectionnel lorsqu'au moins une des conditions suivante existe :
- Le type de réseau sous-jacent est point à point
- Le type de réseau sous-jacent est point à multipoint
- Le type de réseau sous-jacent est liaison virtuelle
- Le routeur lui-même est le routeur désigné
- Le routeur lui-même est le routeur désigné de secours
- Le routeur voisin est le routeur désigné
- Le routeur voisin est le routeur désigné de secours

10.5 Réception des paquets Hello

Ce paragraphe explique le traitement détaillé de la réception d'un paquet Hello. (Voir au paragraphe A.3.2 le format des paquets Hello.) Le traitement générique d'entrée des paquets OSPF aura vérifié la validité de l'en-tête IP et de l'en-tête de paquet OSPF. Ensuite, les valeurs des champs Gabarit de réseau, HelloInterval, et RouterDeadInterval dans le paquet Hello reçu doivent être confrontées aux valeurs configurées pour l'interface de réception. Toute discordance cause l'arrêt du

processus et l'abandon du paquet. En d'autres termes, les champs ci-dessus décrivent réellement la configuration du réseau de rattachement. Cependant, il y a une exception à la règle ci-dessus : sur les réseaux point à point et les liaisons virtuelles, le gabarit de réseau dans le paquet Hello reçu devrait être ignoré.

L'interface qui reçoit se rattache à une seule zone OSPF (elle pourrait être le cœur de réseau). Le réglage du bit E qui se trouve dans le champ Options du paquet Hello doit correspondre à la ExternalRoutingCapability de cette zone. Si les LSA externes à l'AS ne sont pas écoulés dans toute la zone (c'est-à-dire, si la zone est un "bout") le bit E doit être à zéro dans les paquets Hello reçus, autrement, le bit E doit être à 1. Une discordance cause l'arrêt du traitement et l'abandon du paquet. Le réglage du reste des bits dans le champ Options du paquet Hello devrait être ignoré.

À ce moment est faite une tentative pour faire correspondre la source du paquet Hello à un des voisins de l'interface qui reçoit. Si l'interface qui reçoit est connectée à un réseau de diffusion, point à multipoint ou NBMA, la source est identifiée par l'adresse IP de source trouvée dans l'en-tête IP du paquet Hello. Si l'interface qui reçoit se connecte à une liaison en point à point ou à une liaison virtuelle, la source est identifiée par l'identifiant de routeur qui se trouve dans l'en-tête OSPF du paquet Hello. La liste actuelle des voisins de l'interface est contenue dans la structure de données de l'interface. Si on ne peut pas trouver une structure de voisin correspondante, (c'est-à-dire, si c'est la première fois que le voisin a été détecté), il en est créé une. L'état initial d'un voisin nouvellement créé est réglé à Down.

Lors de la réception d'un paquet Hello provenant d'un voisin sur un réseau en diffusion, en point à multipoint ou NBMA, on règle l'identifiant de voisin de la structure du voisin égale à l'identifiant de routeur trouvé dans l'en-tête OSPF du paquet. Pour ces types de réseau, le champ priorité de routeur de la structure du voisin , le champ routeur désigné du voisin, et le champ routeur désigné de secours du voisin sont aussi réglés égaux aux champs correspondants trouvés dans le paquet Hello reçu ; les changements dans ces champs devraient être notés pour une utilisation possible dans les étapes ultérieures. Lors de la réception d'un Hello sur un réseau point à point (mais pas sur une liaison virtuelle) régler l'adresse IP du voisin de la structure du voisin à l'adresse IP de source du paquet.

Maintenant, on examine le reste du paquet Hello, générant les événements à donner au voisin et aux automates à états de l'interface. Ces automates à état sont spécifiés pour être exécutés ou programmés (voir au paragraphe 4.4). Par exemple, en spécifiant ci-dessous que l'automate à états du voisin sera exécuté en ligne, plusieurs transitions d'état de voisin peuvent être effectuées par un seul Hello reçu :

- Chaque paquet Hello cause l'exécution de l'automate voisin avec l'événement Hello reçu.

- Puis la liste des voisins contenue dans le paquet Hello est examinée. Si le routeur lui-même apparaît dans cette liste, l'automate à états voisin devrait être exécuté avec l'événement 2-Way reçu. Autrement, l'automate à états voisin devrait être exécuté avec l'événement 1-Way reçu, et le traitement des paquet s'arrête.

- Ensuite, si on note un changement dans le champ priorité de routeur du voisin, l'automate à états de l'interface qui reçoit est programmé avec l'événement Changement de voisin.

- Si le voisin se déclare lui-même comme routeur désigné (champ routeur désigné du paquet Hello = adresse IP du voisin) et le champ routeur désigné de secours dans le paquet est égal à 0.0.0.0 et si l'interface qui reçoit est dans l'état Waiting, l'automate à états de l'interface qui reçoit est programmé avec l'événement BackupSeen. Autrement, si le voisin se déclare lui-même comme routeur désigné et ne le faisait pas avant, ou si le voisin ne se déclare pas lui-même comme routeur désigné alors qu'il le faisait avant, l'automate à état de l'interface qui reçoit est programmé avec l'événement Changement de voisin.

- Si le voisin se déclare lui-même comme routeur désigné de secours (le champ routeur désigné de secours du paquet Hello = adresse IP du voisin) et si l'interface qui reçoit est dans l'état Waiting, l'automate à états de l'interface qui reçoit est programmé avec l'événement BackupSeen. Autrement, si le voisin se déclare lui-même comme routeur désigné de secours et ne le faisait pas avant, ou si le voisin ne se déclare pas lui-même comme routeur désigné de secours alors qu'il le faisait avant, l'automate à états de l'interface qui reçoit est programmé avec l'événement Changement de voisin.

Sur les réseaux NBMA, la réception d'un paquet Hello peut aussi causer le renvoi d'un paquet Hello en réponse au voisin. Voir au paragraphe 9.5.1 pour des précisions.

10.6 Réception des paquets de description de base de données

Ce paragraphe explique en détail le traitement d'un paquet de description de base de données reçu. Le paquet de description de base de données entrant a déjà été associé à un voisin et à une interface de réception par le traitement générique de paquet d'entrée (paragraphe 8.2). La réponse à la question de savoir si le paquet de description de base de données devrait

être accepté, et si oui, comment il devrait être traité ensuite dépend de l'état du voisin. Si un paquet de description de base de données est accepté, les champs de paquet suivants devraient être sauvegardés dans la structure de données de voisin correspondante sous "dernier paquet de description de base de données reçu" : les bits initialise (I), plus (M) et maître (MS), le champ Options, et le numéro de séquence DD. Si ces champs sont réglés de façon identique dans deux paquets de description de base de données consécutifs reçus du voisin, le second paquet de description de base de données est considéré comme étant un "duplicata" dans le processus décrit ci-dessous. Si le champ MTU d'interface dans le paquet de description de base de données indique une taille de datagramme IP qui est supérieure à celle que le routeur peut accepter sur l'interface de réception sans fragmentation, le paquet de description de base de données est rejeté. Autrement, si l'état du voisin est :

Down
Le paquet devrait être rejeté.

Attempt
Le paquet devrait être rejeté.

Init
L'automate à états du voisin devrait être exécuté avec l'événement 2-Way reçu. Cela cause un changement d'état immédiat à l'état 2-Way ou à l'état ExStart. Si le nouvel état est ExStart, le traitement du paquet en cours devrait alors continuer dans ce nouvel état en retombant au cas ExStart ci-dessous.

2-Way
Le paquet devrait être ignoré. Les paquets de description de base de données ne sont utilisés que pour les besoins de la construction des adjacences[7].

ExStart
Si le paquet reçu correspond à un des cas suivants, l'automate à états voisin devrait être exécuté avec l'événement Négociation Faite (causant la transition à l'état Échange), le champ Option du paquet devrait être enregistré dans le champ Options de voisin de la structure de données du voisin, le paquet devrait être accepté comme le suivant en séquence et le traitement poursuivi (voir ci-dessous). Autrement, le paquet devrait être ignoré.

- Les bits initialise (I), plus (M) et maître (MS) sont à un, le contenu du paquet est vide, et l'identifiant de routeur du voisin est supérieur à celui du routeur. Dans ce cas, le routeur est maintenant esclave. Régler le bit maître/esclave à esclave, et régler le numéro de séquence DD de la structure de données du voisin à celui spécifié par le maître.
- Les bits initialise (I) et maître (MS) sont à zéro, le numéro de séquence DD du paquet est égal au numéro de séquence DD de la structure de données du voisin (indiquant l'accusé de réception) et l'identifiant de routeur du voisin est inférieur à celui du routeur. Dans ce cas, le routeur est le maître.

Échange
Les duplicata de paquets de description de base de données sont éliminés par le maître, et causent la retransmission par l'esclave du dernier paquet de description de base de données qu'il a envoyé. Autrement (le paquet n'est pas un duplicata) :

- Si l'état du bit MS n'est pas cohérent avec l'état maître/esclave de la connexion, générer l'événement SeqNumberMismatch de voisin et arrêter le traitement du paquet.
- Si le bit initialise (I) est à un, générer l'événement SeqNumberMismatch de voisin et arrêter le traitement du paquet.
- Si le champ Options du paquet indique un ensemble de capacités OSPF facultatives différent de celui reçu précédemment du voisin (enregistré dans le champ Options de voisin de la structure de données du voisin) générer l'événement voisin SeqNumberMismatch et arrêter le traitement du paquet.
- Les paquets de description de base de données doivent être traités en séquence, comme indiqué par les numéros de séquence DD du paquet. Si le routeur est maître, le prochain paquet reçu devrait avoir le numéro de séquence DD égal au numéro de séquence DD qui figure dans la structure de données du voisin. Si le routeur est esclave, le prochain paquet reçu devrait avoir son numéro de séquence DD égal à un de plus que le numéro de séquence DD mémorisé dans la structure de données du voisin. Dans l'un et l'autre cas, si le paquet est le suivant de la séquence, il devrait être accepté et son contenu traité comme spécifié ci-dessous.
- Autrement, générer l'événement SeqNumberMismatch de voisin et arrêter le traitement du paquet.

Loading ou Full
Dans cet état, le routeur a envoyé et reçu une séquence entière de paquets de description de base de données. Les seuls paquets reçus devraient être des duplicata (voir ci-dessus). En particulier, le champ Options du paquet devrait correspondre à l'ensemble des capacités OSPF facultatives précédemment indiquées par le voisin (mémorisées dans le champ Options de voisin de la structure du voisin). Tout autre paquet reçu, y compris la réception d'un paquet avec le bit Initialise (I) mis à 1, devrait générer l'événement SeqNumberMismatch de voisin[8]. Les duplicata devraient être éliminés par le maître. L'esclave

7 Lorsque l'identité du routeur désigné change, il arrive couramment qu'un voisin dans cet état envoie au routeur un paquet de description de base de données ; cela signifie un désaccord momentané sur l'identité du routeur désigné.

8 Noter qu'il est possible à un routeur de resynchroniser toute adjacence pleinement établie en réglant l'état de l'adjacence de nouveau à ExStart. Cela cause le traitement de l'événement SeqNumberMismatch par l'autre extrémité de l'adjacence, et donc aussi le retour à l'état ExStart.

doit répondre aux duplicata en répétant le dernier paquet de description de base de données qu'il a envoyé.

Lorsque le routeur accepte un paquet de description de base de données reçu comme le suivant dans la séquence de paquets le contenu est traité comme suit. Pour chaque LSA figurant sur la liste, la validité du type LS du LSA est vérifiée. Si le type LS est inconnu (par exemple, pas un des types LS 1 à 5 définis dans la présente spécification) ou si c'est un LSA externe à l'AS (type LS = 5) et si le voisin est associé à une zone de bout, générer l'événement de voisin SeqNumberMismatch et arrêter le traitement du paquet. Autrement, le routeur cherche le LSA dans sa base de données pour voir si il a aussi une instance du LSA. S'il n'en a pas, ou si la copie de la base de données est moins récente (voir au paragraphe 13.1) le LSA est mis sur la liste des demandes d'état de liaison de façon à ce qu'il puisse être demandé (immédiatement ou ultérieurement) dans les paquets de demande d'état de liaison.

Lorsque le routeur accepte un paquet de description de base de données reçu comme étant le prochain dans la séquence, il effectue aussi les actions suivantes, selon qu'il est maître ou esclave :

Maître
: Incrémente le numéro de séquence DD dans la structure de données du voisin. Si le routeur a déjà envoyé sa séquence entière de paquets de description de base de données, et si le paquet qui vient d'être accepté a le bit Plus (M) mis à 0, l'événement voisin EchangeFait est généré. Autrement, il devrait envoyer une nouvelle Description de base de données à l'esclave.

Esclave
: Règle le numéro de séquence DD dans la structure de données du voisin au numéro de séquence DD qui apparaît dans le paquet reçu. L'esclave doit envoyer un paquet de description de base de données en réponse. Si le paquet reçu a le bit Plus (M) mis à 0, et si le paquet à envoyer par l'esclave va aussi avoir le bit M mis à 0, l'événement de voisin EchangeFait est généré. Noter que l'esclave génère toujours cet événement avant le maître.

10.7 Réception des paquets de demande d'état de liaison

Ce paragraphe explique le processus détaillé de réception des paquets de demande d'état de liaison. Les paquets de demande d'état de liaison reçus spécifient une liste des LSA que le voisin souhaite recevoir. Les paquets de demande d'état de liaison devraient être acceptés lorsque le voisin est dans les états Échange, Loading, ou Full. Dans tous les autres états les paquets de demande d'état de liaison devraient être ignorés.

Chaque LSA spécifié dans le paquet de demande d'état de liaison devrait être situé dans la base de données du routeur, et copié dans les paquets Mise à jour d'état de liaison pour transmission au voisin. Ces LSA NE DEVRAIENT PAS être placés dans la liste de retransmission d'état de liaison pour le voisin. Si un LSA ne peut pas être trouvé dans la base de données, quelque chose va mal dans le processus d'échange de base de données, et l'événement de voisin BadLSReq devrait être généré.

10.8 Envoi des paquets de description de base de données

Ce paragraphe décrit la façon dont les paquets de description de base de données sont envoyés à un voisin. Le champ MTU d'interface du paquet de description de base de données est réglé à la taille du plus grand datagramme IP qui peut être envoyé de l'interface qui envoie, sans fragmentation. Les MTU courantes utilisées dans l'Internet se trouvent dans le Tableau 7-1 de [Ref22]. La MTU de l'interface devrait être réglée à 0 dans les paquets de description de base de données envoyés sur des liaisons virtuelles.

Les capacités OSPF facultatives du routeur (voir au paragraphe 4.5) sont transmises au voisin dans le champ Options du paquet de description de base de données. Le routeur devrait maintenir le même ensemble de capacités facultatives pendant tout l'échange de base de données et les procédures d'arrosage. Si pour une raison quelconque les capacités facultatives du routeur changent, la procédure d'échange de base de données devrait être recommencée en revenant à l'état ExStart du voisin. Une capacité facultative est définie dans la présente spécification (voir aux paragraphes 4.5 et A.2). Le bit E devrait être mis si et seulement si le réseau de rattachement appartient à une zone qui n'est pas de bout. Les bits non reconnus dans le champ Options devraient être mis à zéro.

L'envoi des paquets de description de base de données dépend de l'état du voisin. Dans l'état ExStart le routeur envoie des paquets de description de base de données vides, avec les bits initialise (I), plus (M) et maître (MS) mis à un. Ces paquets sont retransmis toutes les RxmtInterval secondes.

Dans l'état Échange, les paquets de description de base de données contiennent en fait les résumés des informations d'état de liaison contenus dans la base de données du routeur. Chaque LSA dans la base de données d'états de liaisons de la zone

(au moment où le voisin passe dans l'état Échange) figure sur la liste des résumés de base de données du voisin. Chaque nouveau paquet de description de base de données copie son numéro de séquence DD d'après la structure de données du voisin puis décrit le sommet actuel de la liste de résumés de base de données. Les éléments sont retirés de la liste de résumés de base de données lorsqu'il est accusé réception du paquet précédent.

Dans l'état Échange, la détermination du moment où envoyer un paquet de description de base de données dépend de si le routeur est maître ou esclave :

Maître
: Les paquets de description de base de données sont envoyés quand a) l'esclave accuse réception du précédent paquet de description de base de données en faisant écho au numéro de séquence DD ou b) RxmtInterval secondes s'écoulent sans accusé de réception, auquel cas le précédent paquet de description de base de données est retransmis.

Esclave
: Les paquets de description de base de données sont envoyés seulement en réponse aux paquets de description de base de données reçus du maître. Si le paquet de description de base de données reçu du maître est nouveau, un nouveau paquet de description de base de données est envoyé, autrement, le précédent paquet de description de base de données est renvoyé.
Dans les états Loading et Full, l'esclave doit renvoyer son dernier paquet de description de base de données en réponse aux paquets de description de base de données dupliqués reçus du maître. Pour cette raison, l'esclave doit attendre RouterDeadInterval secondes avant de libérer le dernier paquet de description de base de données. La réception d'un paquet de description de base de données du maître après cet intervalle va générer un événement SeqNumberMismatch de voisin.

10.9 Envoi des paquets de demande d'état de liaison

Dans les états de voisin Échange ou Loading, la liste de demande d'état de liaison contient une liste des LSA qui doivent être obtenus du voisin. Pour demander ces LSA, un routeur envoie au voisin le début de la liste de demande d'état de liaison, enveloppée dans un paquet de demande d'état de liaison.

Lorsque le voisin répond à ces demandes par le ou les paquets appropriés de mise à jour d'état de liaison, la liste de demande d'état de liaison est raccourcie et un nouveau paquet de demande d'état de liaison est envoyé. Ce processus continue jusqu'à ce que la liste de demande d'état de liaison soit vide. Les LSA sur la liste de demande d'état de liaison qui ont été demandés, mais ne sont pas encore reçus, sont enveloppés dans les paquets de demande d'état de liaison pour retransmission aux intervalles de RxmtInterval. Il devrait y avoir au plus un paquet de demande d'état de liaison en cours à tout instant.

Lorsque la liste de demande d'état de liaison devient vide, et que l'état du voisin est Loading (c'est-à-dire qu'une séquence complète de paquets de description de base de données a été envoyée et reçue du voisin) l'événement de voisin Loading Done *(chargement fait)* est généré.

10.10 Exemple

La Figure 14 montre un exemple de formation d'une adjacence. Les routeurs RT1 et RT2 sont tous deux connectés à un réseau de diffusion. On suppose que RT2 est le routeur désigné pour le réseau, et que RT2 a un identifiant de routeur supérieur à celui du routeur RT1.

La liste des changements d'état de voisin réalisés par chaque routeur est donnée sur les côtés de la figure.

Au début de la Figure 14, l'interface du routeur RT1 avec le réseau devient opérationnelle. Il commence par envoyer des paquets Hello, bien qu'il ne sache pas l'identité du routeur désigné ni d'aucun des autres routeurs voisins. Le routeur RT2 entend ce hello (passant le voisin à l'état Init), et dans son prochain paquet Hello indique qu'il est lui-même le routeur désigné et qu'il a entendu les paquets Hello provenant de RT1. Cela cause à son tour le passage de RT1 à l'état ExStart, car il commence à construire l'adjacence.

RT1 commence par s'affirmer lui-même comme maître. Lorsqu'il voit que c'est RT2 qui est le maître (à cause de l'identifiant de routeur plus élevé de RT2) RT1 passe à l'état d'esclave et adopte le numéro de séquence DD de son voisin. Les paquets de description de base de données sont alors échangés, avec des interrogations provenant du maître (RT2) et des réponses de l'esclave (RT1). Cette séquence de paquets de description de base de données se termine lorsque les interrogations et leurs réponses associées ont le bit M à zéro.

Dans cet exemple, on suppose que RT2 a une base de données complètement à jour. Dans ce cas, RT2 va immédiatement à l'état Full. RT1 ira à l'état Full après avoir mis à jour les parties nécessaires de sa base de données. Ceci est fait par l'envoi des paquets de demande d'état de liaison, et la réception des paquets de mise à jour d'état de liaison en réponse. Noter que, alors que RT1 a attendu jusqu'à ce qu'un ensemble complet de paquets de description de base de données ait été reçu (de RT2) avant d'envoyer aucun des paquets de demande d'état de liaison, ceci n'est pas nécessairement le cas. RT1 pourrait avoir entremêlé l'envoi des paquets de demande d'état de liaison avec la réception de paquets de description de base de données.

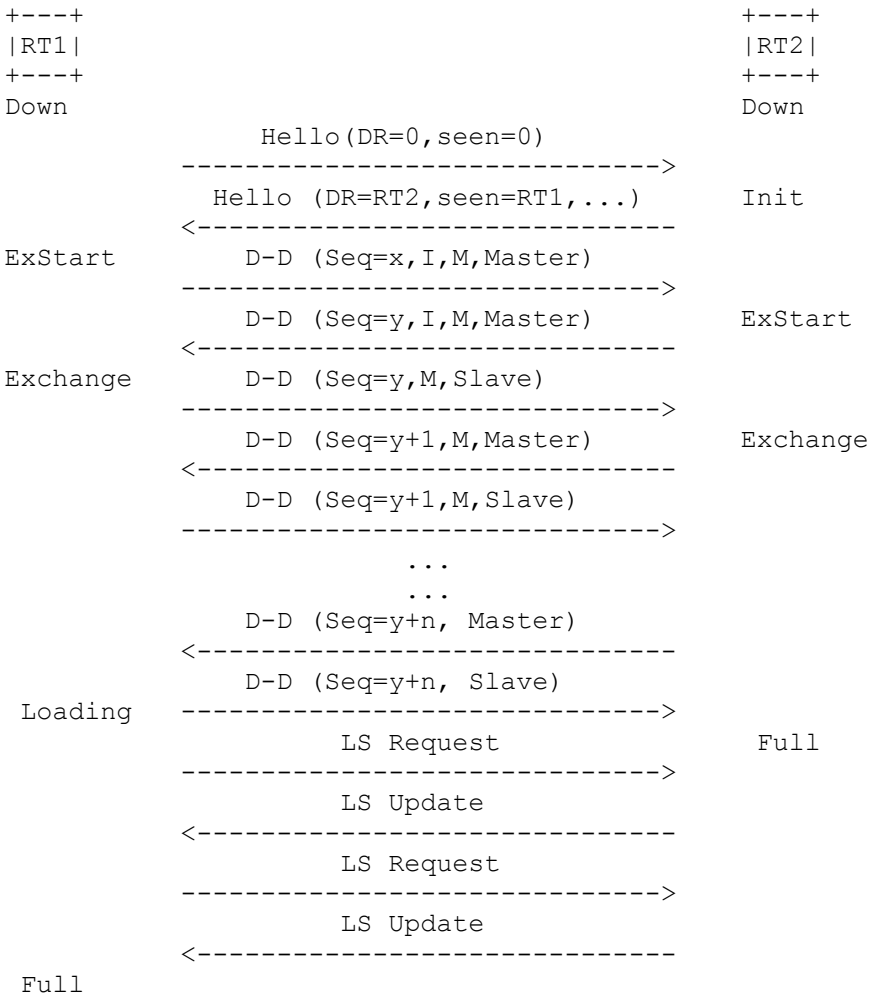


Figure 14 : Exemple de construction d'adjacence

11. Structure du tableau d'acheminement

La structure de données du tableau d'acheminement contient toutes les informations nécessaires pour transmettre un paquet de données IP jusqu'à sa destination. Chaque entrée de tableau d'acheminement décrit la collection des meilleurs chemins pour une destination particulière. Lors de la transmission d'un paquet de données IP, l'entrée de tableau d'acheminement qui fournit la meilleure correspondance pour la destination IP du paquet est localisée. L'entrée de tableau d'acheminement correspondante donne alors le prochain bond vers la destination du paquet. OSPF fournit aussi un chemin par défaut (Identifiant de destination = DefaultDestination, Gabarit d'adresse = 0x00000000). Lorsque le chemin par défaut existe, il correspond à toutes les destinations IP (bien que toute autre entrée correspondante soit une meilleure correspondance). Trouver l'entrée de tableau d'acheminement qui correspond le mieux à une destination IP est décrit plus en détail au 11.1.

Il y a un seul tableau d'acheminement dans chaque routeur. Deux échantillons de tableaux d'acheminements sont décrits aux paragraphes 11.2 et 11.3. La construction d'un tableau d'acheminement est exposée à la Section 16.

Le reste de cette section définit les champs trouvés dans une entrée de tableau d'acheminement. Le premier ensemble de champs décrit la destination d'une entrée de tableau d'acheminement.

Type de destination

Le type de destination est "réseau" ou "routeur". Seules les entrées réseau sont en fait utilisées lors de la transmission de trafic de données IP. Les entrées de tableau d'acheminement routeur sont seulement utilisées comme étapes intermédiaires dans le processus de construction du tableau d'acheminement.

Un réseau est une gamme d'adresses IP, auxquelles le trafic de données IP peut être transmis. Cela inclut les réseaux IP (classe A, B, ou C) les sous-réseaux IP, les super-réseaux IP et les hôtes IP individuels. Le chemin par défaut entre aussi dans cette catégorie.

Les entrées de routeur sont gardées pour les routeurs frontière de zone et les routeurs frontière de l'AS. Les entrées de tableau d'acheminement pour les routeurs frontières de zone sont utilisées lors du calcul des chemins inter-zones (voir paragraphe 16.2) et lors de l'entretien des liaisons virtuelles configurées (voir Section 15). Les entrées de tableau d'acheminement pour les routeurs frontière de l'AS sont utilisées lors du calcul des chemins externes à l'AS (voir paragraphe 16.4).

Identifiant de destination
C'est l'identifiant ou le nom de la destination. Cela dépend du type de destination. Pour les réseaux, l'identifiant est leur adresse IP associée. Pour les routeurs, l'identifiant est l'identifiant de routeur OSPF [9].

Gabarit d'adresse
Seulement défini pour les réseaux. L'adresse IP du réseau jointe à son gabarit d'adresse définit une gamme d'adresses IP. Pour les sous-réseaux IP, le gabarit d'adresse est appelé gabarit de sous-réseau. Pour les chemins d'hôtes, le gabarit est "tout à un" (0xffffffff).

Capacités facultatives
Lorsque la destination est un routeur, ce champ indique les capacités OSPF facultatives prises en charge par le routeur de destination. La seule capacité facultative définie dans la présente spécification est la capacité à traiter les LSA externes à l'AS. Voir au paragraphe 4.5 un exposé plus complet sur les capacités OSPF facultatives.
L'ensemble des chemins à utiliser pour une destination peut varier selon la zone OSPF à laquelle appartiennent les chemins. Cela signifie qu'il peut y avoir plusieurs entrées de tableau d'acheminement pour la même destination, selon les valeurs du prochain champ.

Zone
Ce champ indique la zone dont les informations d'état de liaison ont conduit à la collection de chemins de l'entrée du tableau d'acheminement. C'est ce qu'on appelle la zone associée à l'entrée. Pour les ensembles de chemins externes à l'AS, ce champ n'est pas défini. Pour les destinations de type "routeur", il peut y avoir des ensembles de chemins distincts (et donc des entrées séparées de tableau d'acheminement) associés à chacune des zones. Par exemple, cela va arriver lorsque deux routeurs frontières de zone ont plusieurs zones en commun. Pour les destinations de type "réseau", seul l'ensemble de chemins associés à la meilleure zone (celle qui fournit le chemin préféré) est gardé.

Le reste des entrées du tableau d'acheminement décrit l'ensemble des chemins vers la destination. Les champs suivants appartiennent à l'ensemble des chemins pris globalement. En d'autres termes, chacun des chemins contenus dans une entrée d'un tableau d'acheminement est du même type de chemin et du même coût (voir ci-dessous).

Type de chemin
Quatre types de chemin possibles sont utilisés pour acheminer le trafic à destination, figurant en ordre de préférence décroissante : intra-zone, inter-zone, externe type 1 ou externe type 2. Les chemins intra-zone indiquent des destinations appartenant à une des zones de rattachement du routeur. Les chemins inter-zone sont des chemins vers des destinations situées dans d'autres zones OSPF. Ils sont découverts par l'examen des LSA de résumé reçus. Les chemins externes à l'AS sont des chemins vers des destinations externes à l'AS. Ils sont détectés par l'examen des LSA externes à l'AS reçus.

Coût
Coût de l'état de liaison du chemin vers la destination. Pour tous les chemins excepté les chemins externes de type 2, cela décrit le coût du chemin entier. Pour les chemins externes de type 1, ce champ décrit le coût de la portion de chemin interne à l'AS. Ce coût est calculé comme la somme des coûts des liaisons constitutives du chemin.

Coût de type 2
Valide pour les seuls chemins externes de type 2. Pour ces chemins, ce champ indique le coût de la portion externe du chemin. Ce coût a été annoncé par un routeur frontière de l'AS, et est la partie la plus significative du coût total du chemin. Par exemple, un chemin externe de type 2 avec un coût de type 2 de 5 est toujours préféré à un chemin ayant un coût de type 2 de 10, sans considération du coût des composantes internes des deux chemins.

---

9 Les espaces adresse des réseaux IP et des identifiants de routeur OSPF peuvent se chevaucher. C'est à dire qu'un réseau peut avoir une adresse IP identique (considérée comme un nombre de 32 bits) à l'identifiant de routeur de quelque routeur.

Origine de l'état de liaison
Valide pour les seuls chemins intra-zone, ce champ indique le LSA (LSA de routeur ou LSA de réseau) qui fait directement référence à la destination. Par exemple, si la destination est un réseau de transit, c'est le LSA de réseau du réseau de transit. Si la destination est un réseau de bout, c'est le LSA de routeur pour le routeur rattaché. Le LSA est découvert durant le calcul de l'arbre des plus courts chemins (voir au paragraphe 16.1). Plusieurs LSA peuvent se référer à la destination, cependant un schéma de départage réduit toujours le choix à un seul LSA. Le champ Origine d'état de liaison n'est pas utilisé par le protocole OSPF, mais est utilisé par le calcul de tableau d'acheminement dans les extensions d'acheminement en diffusion groupée d'OSPF (MOSPF, *OSPF Multicast routing extension*).

Lorsqu'existent plusieurs chemins ayant des types de chemin et des coûts égaux pour une même destination (qu'on appelle par ailleurs des chemins de "coût égal") ils sont mémorisés dans une seule entrée de tableau d'acheminement. Chacun des chemins de "coût égal" est distingué par les champs suivants :

Prochain bond
Interface sortante de routeur à utiliser lors de la transmission du trafic à destination. Sur les réseaux en diffusion, en point à multipoint et NBMA, le prochain bond inclut aussi l'adresse IP du prochain routeur (s'il en est) sur le chemin vers la destination.

Routeur annonceur
Valide seulement pour les chemins inter-zone et externes à l'AS. Ce champ indique l'identifiant de routeur du routeur qui annonce le LSA de résumé ou le LSA externe à l'AS qui a mené à ce chemin.

11.1 Examen du tableau d'acheminement

Lors de la réception d'un paquet de données IP, un routeur OSPF trouve l'entrée de tableau d'acheminement qui correspond le mieux à la destination du paquet . Cette entrée de tableau d'acheminement fournit alors l'interface de sortie et le routeur du prochain bond à utiliser pour transmettre le paquet. Ce paragraphe décrit le processus de détermination de l'entrée de tableau d'acheminement qui correspond le mieux.

Avant que commence la recherche, les entrées de tableau d'acheminement "discard" devraient être insérées dans le tableau d'acheminement pour chacune des gammes actives d'adresses de zone du routeur (voir au paragraphe 3.5). (Une gamme de zone est considérée comme "active" si la gamme contient un ou plusieurs réseaux accessibles par des chemins intra-zone.) La destination d'une entrée "discard" est l'ensemble des adresses décrites par sa gamme active d'adresses de zone associée, et le type de chemin de chaque entrée "discard" est réglé à "inter-zone"[10].

Plusieurs entrées de tableau d'acheminement peuvent correspondre à l'adresse de destination. Dans ce cas, la "meilleure correspondance" est l'entrée de tableau d'acheminement qui fournit la correspondance la plus spécifique (la plus longue). Une autre façon de le dire est de choisir l'entrée qui spécifie la gamme la plus étroite d'adresses IP[11]. Par exemple, l'entrée pour la paire adresse/gabarit (128.185.1.0, 0xffffff00) est plus spécifique qu'une entrée pour la paire (128.185.0.0, 0xffff0000). Le chemin par défaut est la correspondance la moins spécifique, car elle correspond à toutes les destinations. (Noter que pour toute entrée de tableau d'acheminement, plusieurs chemins sont éventuellement possibles. Dans ces cas, le calcul des paragraphes 16.1, 16.2, et 16.4 donne toujours le chemin qui a le type de chemin préféré, comme décrit à la Section 11).

S'il n'y a pas d'entrée de tableau d'acheminement correspondante, ou si la meilleure correspondance d'entrée de tableau d'acheminement est une des entrées de tableau d'acheminement du "discard" ci-dessus, la destination IP du paquet est alors considérée comme injoignable. Au lieu d'être transmis, le paquet devrait alors être éliminé et un message ICMP Destination injoignable devrait être retourné à la source du paquet.

11.2 Exemple de tableau d'acheminement, sans zone

Considérons le système autonome dépeint à la Figure 2. Aucune zone OSPF n'a été configurée. Une seule métrique est montrée à l'interface de sortie. Le calcul du tableau d'acheminement du routeur RT6 se déroule comme décrit au paragraphe 2.2. Le tableau d'acheminement résultant figure au Tableau 12. Les types de destination sont abrégés : réseau en "N", routeur en "R".

---

10 Les entrées "discard" sont nécessaires pour assurer que la totalisation des chemins aux frontières de zone ne causera pas de boucle d'acheminement des paquets.

11 On suppose que pour deux différentes gammes d'adresses correspondant à la destination, une gamme est plus spécifique que l'autre. Des gabarits de sous-réseau non contigus peuvent être configurés en violation de cette hypothèse. De telles configurations de gabarit de sous-réseau ne peuvent pas être traitées par le protocole OSPF.

Il n'y a pas d'instance de plusieurs plus courts chemins de coût égal dans cet exemple. Et aussi, comme il n'y a pas de zones, il n'y a pas de chemins inter-zone.

Les routeurs RT5 et RT7 sont les routeurs frontières de l'AS. Les chemins intra-zone ont été calculés vers les routeurs RT5 et RT7. Cela permet de calculer les chemins externes pour les destinations annoncées par RT5 et RT7 (c'est-à-dire, les réseaux N12, N13, N14 et N15). On suppose que tous les LSA externes à l'AS générés par RT5 et RT7 sont annoncés avec une métrique externe de type 1. Il en résulte que des chemins externes de type 1 sont calculés pour les destinations N12-N15.

11.3 Exemple de tableau d'acheminement, avec zones

Considérons l'exemple précédent, cette fois partagé en zones OSPF. Une configuration de zone OSPF est décrite à la Figure 6. Le tableau d'acheminement du routeur RT4 sera décrit pour cette configuration de zone. Le routeur RT4 a une connexion à la zone 1 et une connexion de cœur de réseau. Cela amène le routeur RT4 à voir l'AS comme l'enchaînement des deux graphes montrés aux Figures 7 et 8. Le tableau d'acheminement résultant est donné au Tableau 13.

À nouveau, les routeurs RT5 et RT7 sont des routeurs frontières de l'AS. Les routeurs RT3, RT4, RT7, RT10 et RT11 sont des routeurs frontières de zone. Noter qu'il y a deux entrées d'acheminement pour le routeur frontière de zone RT3, car il a deux zones en commun avec RT4 (zone 1 et le cœur de réseau).

Les chemins de cœur de réseau ont été calculés vers tous les routeurs frontières de zone. Ils sont utilisés pour déterminer les chemins inter-zone. Noter que tous les chemins inter-zone sont associés au cœur de réseau ; c'est toujours le cas lorsque le routeur qui fait le calcul est lui-même un routeur frontière de zone. Les informations d'acheminement sont concentrées à la frontière de zone. Dans cet exemple, on suppose que la zone 3 a été définie de telle sorte que les réseaux N9 à N11 et le chemin d'hôte vers H1 sont tous concentrés en un seul chemin lors de l'annonce dans le cœur de réseau (par le routeur RT11). Noter que le coût de ce chemin est le maximum de l'ensemble des coûts vers ses composants individuels.

Type	Destination	Zone	Type de chemin	Coût	Prochains bonds	Routeurs annoncés
N	N1	0	intra-zone	10	RT3	*
N	N2	0	intra-zone	10	RT3	*
N	N3	0	intra-zone	7	RT3	*
N	N4	0	intra-zone	8	RT3	*
N	Ib	0	intra-zone	7	*	*
N	Ia	0	intra-zone	12	RT10	*
N	N6	0	intra-zone	8	RT10	*
N	N7	0	intra-zone	12	RT10	*
N	N8	0	intra-zone	10	RT10	*
N	N9	0	intra-zone	11	RT10	*
N	N10	0	intra-zone	13	RT10	*
N	N11	0	intra-zone	14	RT10	*
N	H1	0	intra-zone	21	RT10	*
R	RT5	0	intra-zone	6	RT5	*
R	RT7	0	intra-zone	8	RT10	*
N	N12	*	type 1 ext.	10	RT10	RT7
N	N13	*	type 1 ext.	14	RT5	RT5
N	N14	*	type 1 ext.	14	RT5	RT5
N	N15	*	type 1 ext.	17	RT10	RT7

Tableau 12 : Tableau d'acheminement pour le routeur RT6 (pas de zone configurée).

Il y a une liaison virtuelle configurée entre les routeurs RT10 et RT11. Sans cette liaison virtuelle configurée, RT11 serait incapable d'annoncer un chemin pour les réseaux N9 à N11 et l'hôte H1 vers le cœur de réseau, et il n'y aurait pas d'entrée pour ces réseaux dans le tableau d'acheminement du routeur RT4 .

Dans cet exemple, il y a deux chemins de coût égal vers le réseau N12. Cependant, ils utilisent tous deux le même prochain bond (routeur RT5).

Le tableau d'acheminement du routeur RT4 serait amélioré (c'est-à-dire, certains des chemins du tableau d'acheminement deviendraient plus courts) si une liaison virtuelle supplémentaire était configurée entre le routeur RT4 et le routeur RT3. La nouvelle liaison virtuelle serait elle-même associée à la première entrée pour le routeur frontière de zone RT3 dans le Tableau 13 (un chemin intra-zone à travers la zone 1). Cela donnerait un coût de 1 pour la liaison virtuelle. Les changements d'entrées de tableau d'acheminement qui seraient causés par l'ajout de cette liaison virtuelle figurent au

Tableau 14.

Type	Destination	Zone	Type de chemin	Coût	Prochains bonds	Routeurs annoncés
N	N1	1	intra-zone	4	RT1	*
N	N2	1	intra-zone	4	RT2	*
N	N3	1	intra-zone	1	*	*
N	N4	1	intra-zone	3	RT3	*
R	RT3	1	intra-zone	1	*	*
N	Ib	0	intra-zone	22	RT5	*
N	Ia	0	intra-zone	27	RT5	*
R	RT3	0	intra-zone	21	RT5	*
R	RT5	0	intra-zone	8	*	*
R	RT7	0	intra-zone	14	RT5	*
R	RT10	0	intra-zone	22	RT5	*
R	RT11	0	intra-zone	25	RT5	*
N	N6	0	inter-zone	15	RT5	RT7
N	N7	0	inter-zone	19	RT5	RT7
N	N8	0	inter-zone	18	RT5	RT7
N	N9-N11,H1	0	inter-zone	36	RT5	RT11
N	N12	*	type 1 ext.	16	RT5	RT5,RT7
N	N13	*	type 1 ext.	16	RT5	RT5
N	N14	*	type 1 ext.	16	RT5	RT5
N	N15	*	type 1 ext.	23	RT5	RT7

Tableau 13 : Tableau d'acheminement du routeur RT4 en présence de zones.

Type	Destination	Zone	Type de chemin	Coût	Prochains bonds	Routeurs annonceurs
N	Ib	0	intra-zone	16	RT3	*
N	Ia	0	intra-zone	21	RT3	*
R	RT3	0	intra-zone	1	*	*
R	RT10	0	intra-zone	16	RT3	*
R	RT11	0	intra-zone	19	RT3	*
N	N9-N11,H1	0	inter-zone	30	RT3	RT11

Tableau 14 : Changements résultant d'une liaison virtuelle supplémentaire.

12. Avis d'état de liaison (LSA)

Chaque routeur dans le système autonome génère un ou plusieurs avis d'état de liaison (LSA, *link state advertisement*). le présent mémoire définit cinq types distincts de LSA, qui sont décrits au paragraphe 4.3. La collection des LSA forme la base de données d'états de liaisons. Chaque type distinct de LSA a une fonction propre. Les LSA de routeur et les LSA de réseau décrivent comment les routeurs et les réseaux d'une zone sont interconnectés. Les LSA de résumé fournissent un moyen de concentrer les informations d'acheminement d'une zone. Les LSA externes à l'AS fournissent un moyen d'annoncer de façon transparente les informations d'acheminement déduites de l'extérieur dans tout le système autonome.

Chaque LSA commence par un en-tête standard de 20 octets. Cet en-tête de LSA est exposé ci-dessous.

12.1 En-tête de LSA

L'en-tête de LSA contient les champs Type LS, Identifiant d'état de liaison et Routeur annonceur. La combinaison de ces trois champs identifie de façon univoque le LSA.

Plusieurs instances d'un LSA peuvent être présentes dans le système autonome, toutes en même temps. On doit alors déterminer quelle instance est la plus récente. Cette détermination est faite en examinant les champs Séquence LS, Somme de contrôle LS et Age LS. Ces champs sont aussi contenus dans l'en-tête de LSA de 20 octets.

Plusieurs des types de paquet OSPF font la liste des LSA. Quand l'instance n'est pas importante, un LSA est désigné par son type LS, identifiant d'état de liaison et routeur annonceur (voir les paquets de demande d'état de liaison). Autrement, les champs Numéro de séquence LS, Age LS et Somme de contrôle LS doivent aussi être mentionnés.

Ci-après figure une explication détaillée des champs contenus dans l'en-tête de LSA.

12.1.1 Age LS

Ce champ est l'âge du LSA en secondes. Il devrait être traité comme un entier non signé de 16 bits. Il est réglé à 0 lors de la création du LSA. Il doit être incrémenté de InfTransDelay à chaque bond de la procédure d'arrosage. Les LSA sont aussi vieillis lorsqu'ils sont détenus par la base de données de chaque routeur.

L'âge d'un LSA n'est jamais incrémenté au-delà de MaxAge. Les LSA qui ont un âge de MaxAge ne sont pas utilisés dans le calcul du tableau d'acheminement. Lorsque l'âge d'un LSA atteint MaxAge pour la première fois, il est rediffusé. Un LSA d'âge MaxAge est finalement purgé de la base de données quand il n'est plus nécessaire pour assurer la synchronisation de la base de données. Pour des informations complémentaires sur le vieillissement des LSA, consulter la Section 14.

Le champ Age LS est examiné quand un routeur reçoit deux instances d'un LSA, qui ont des numéros de séquence LS et des sommes de contrôle LS identiques. Une instance d'âge MaxAge est alors toujours acceptée comme la plus récente ; ceci permet de purger les vieux LSA rapidement du domaine d'acheminement. Autrement, si les âges diffèrent de plus que MaxAgeDiff, l'instance qui a le plus petit âge est acceptée comme la plus récente[12]. Voir des précisions au paragraphe 13.1.

12.1.2 Options

Le champ Options dans l'en-tête de LSA indique quelles capacités facultatives sont associées au LSA. Les capacités OSPF facultatives sont décrites au paragraphe 4.5. Une capacité facultative est définie dans la présente spécification, représentée par le bit E qui se trouve dans le champ Options. Les bits non reconnus dans le champ Options devraient être mis à zéro.

Le bit E représente ExternalRoutingCapability d'OSPF *(Capacité d'acheminement extérieur)*. Ce bit devrait être mis dans tous les LSA associés au cœur de réseau, et dans tous les LSA associés à des zones non bout (voir au paragraphe 3.6). Il devrait aussi être mis dans tous les LSA externes à l'AS. Il devrait être remis dans tous les LSA de routeur, les LSA de réseau et les LSA de résumé associés à une zone de bout. Pour tous les LSA, le réglage du bit E est seulement à des fins d'information ; il n'affecte pas le calcul du tableau d'acheminement.

12.1.3 Type de LSA

Le champ Type LS dicte le format et la fonction du LSA. Les LSA de types différents ont des noms différents (par exemple, les LSA de routeur ou les LSA de réseau). Tous les types de LSA définis dans le présent mémoire, excepté les LSA externes à l'AS (LS type = 5), sont diffusés seulement dans une seule zone. Les LSA externes à l'AS sont diffusés dans tout le système autonome, excepté les zones de bout (voir au paragraphe 3.6). Chaque type de LSA est brièvement décrit ci-dessous au Tableau 15.

12.1.4 Identifiant d'état de liaison

Ce champ identifie la partie du domaine d'acheminement qui est décrite par le LSA. Selon le type LS du LSA, l'identifiant d'état de liaison prend une des valeurs figurant au Tableau 16.

12 MaxAgeDiff est une constante architecturale. Elle indique la dispersion maximum des âges, en secondes, qui peut survenir pour une seule instance de LSA lorsqu'il est diffusé dans le domaine d'acheminement. Si deux LSA diffèrent de plus de cela, ils sont supposés être des instances différentes du même LSA. Cela peut arriver quand un routeur redémarre et perd la trace du numéro de séquence LS précédent du LSA. Voir des précisions au paragraphe 13.4.

Type LS	Description du LSA
1	Ce sont les LSA de routeur. Ils décrivent les états collectés des interfaces du routeur. Pour des informations complémentaires, consulter le paragraphe 12.4.1.
2	Ce sont les LSA de réseau. Ils décrivent l'ensemble des routeurs rattachés au réseau. Pour des informations complémentaires, consulter le paragraphe 12.4.2.
3 ou 4	Ce sont les LSA de résumé. Ils décrivent les chemins inter-zone, et permettent la concentration des informations d'acheminement aux frontières de zone. Générés par les routeurs frontières de zone, les LSA de résumé de type 3 décrivent les chemins des réseaux alors que les LSA de résumé de type 4 décrivent les chemins des routeurs frontières de l'AS.
5	Ce sont les LSA externes à l'AS. Générés par les routeurs frontières de l'AS, ils décrivent les chemins pour les destinations externes au système autonome. Un chemin par défaut pour le système autonome peut aussi être décrit par un LSA externe à l'AS.

Tableau 15 : Avis d'état de liaison (LSA) OSPF.

En fait, pour les LSA de résumé de type 3 (LS type = 3) et les LSA externes à l'AS (LS type = 5) l'identifiant d'état de liaison peut de plus avoir un ou plusieurs bits "hôte" du réseau de destination mis *(à 1)*. Par exemple, en générant un LSA externe à l'AS pour le réseau 10.0.0.0 avec le gabarit de 255.0.0.0, l'identifiant d'état de liaison peut être mis à n'importe quoi dans la gamme de 10.0.0.0 à 10.255.255.255 inclus (bien que 10.0.0.0 devrait être utilisé chaque fois que possible). La faculté de régler certains bits d'hôte permet à un routeur de générer des LSA distincts pour deux réseaux qui ont la même adresse mais des gabarits différents. Voir des précisions à l'Appendice E.

Type LS	Identifiant d'état de liaison
1	Identifiant de routeur du routeur d'origine
2	Adresse IP d'interface du routeur désigné du réseau.
3	Adresse IP du réseau de destination.
4	Identifiant de routeur du routeur frontière de l'AS décrit.
5	Adresse IP du réseau de destination.

Tableau 16 : Identifiant d'état de liaison du LSA.

Lorsque le LSA décrit un réseau (LS type = 2, 3 ou 5) l'adresse IP du réseau est facilement déduite en appliquant l'identifiant d'état de liaison au gabarit de réseau/sous-réseau contenu dans le corps du LSA. Lorsque le LSA décrit un routeur (LS type = 1 ou 4) l'identifiant d'état de liaison est toujours l'identifiant de routeur OSPF du routeur décrit.

Lorsqu'un LSA externe à l'AS (LS type = 5) décrit un chemin par défaut, son identifiant d'état de liaison est mis à DefaultDestination (0.0.0.0).

12.1.5 Routeur d'annonce

Ce champ spécifie l'identifiant de routeur OSPF du générateur du LSA. Pour les LSA de routeur, ce champ est identique au champ Identifiant d'état de liaison. Les LSA de réseau sont générés par le routeur désigné du réseau. Les LSA de résumé sont générés par les routeurs frontières de zone. Les LSA externes à l'AS sont générés par les routeurs frontières de l'AS.

12.1.6 Numéro de séquence de LSA

Le champ numéro de séquence est un entier signé de 32 bits. Il est utilisé pour détecter les LSA vieux et dupliqués. L'espace des numéros de séquence est ordonné et linéaire. Plus le numéro de séquence est grand (comparé à des entiers signés de 32 bits) plus le LSA est récent. Pour décrire plus précisément l'espace de numéros de séquence, appelons N la constante 2**31 dans l'exposé ci-dessous.

Le numéro de séquence -N (0x80000000) est réservé (et inutilisé). Cela laisse -N + 1 (0x80000001) comme le plus petit (et donc le plus vieux) numéro de séquence ; ce numéro de séquence est appelé la constante InitialSequenceNumber. Un routeur utilise InitialSequenceNumber la première fois qu'il génère un LSA. Ensuite, le numéro de séquence du LSA est incrémenté chaque fois que le routeur génère une nouvelle instance du LSA. Lorsqu'il essaye d'incrémenter le numéro de séquence au delà de la valeur maximum de N - 1 (0x7fffffff; aussi appelé MaxSequenceNumber) l'instance de LSA en cours doit d'abord être purgée du domaine d'acheminement. Cela est fait en vieillissant prématurément le LSA (voir au paragraphe 14.1) et en le rediffusant. Aussitôt qu'il a été accusé réception de cet arrosage par tous les voisins adjacents, une nouvelle instance peut être générée avec le numéro de séquence de InitialSequenceNumber.

Le routeur peut être forcé de relever le numéro de séquence d'un de ses LSA lorsqu'une instance plus récente du LSA est reçue de façon inattendue durant le processus d'arrosage. Ceci devrait être un événement rare. Cela peut indiquer qu'un

LSA périmé, généré par le routeur lui-même avant son dernier redémarrage/rechargement, existe toujours dans le système autonome. Pour des informations complémentaires, voir au paragraphe 13.4.

12.1.7 Somme de contrôle de LSA

Ce champ est la somme de contrôle du contenu entier du LSA, excepté le champ Age LS. Le champ Age LS est excepté de sorte que l'âge d'un LSA puisse être incrémenté sans mettre à jour la somme de contrôle. La somme de contrôle utilisée est la même que celle utilisée pour les datagrammes sans connexion ISO ; elle est communément appelée la somme de contrôle de Fletcher. Elle est exposée dans l'Annexe B de [Ref6]. L'en-tête de LSA contient aussi la longueur du LSA en octets ; soustraire la taille du champ Age LS (deux octets) donne la quantité de données à soumettre à la somme de contrôle.

La somme de contrôle est utilisée pour détecter la corruption des données d'un LSA. Cette corruption peut survenir alors qu'un LSA est en cours de diffusion, ou pendant qu'il est détenu dans la mémoire d'un routeur. Le champ Somme de contrôle LS ne peut pas prendre la valeur de zéro ; l'occurrence d'une telle valeur devrait être considérée comme une somme de contrôle défaillante. En d'autres termes, le calcul de la somme de contrôle n'est pas facultatif.

La somme de contrôle d'un LSA est vérifiée dans deux cas : a) lorsqu'elle est reçue dans un paquet de mise à jour d'état de liaison et b) à certains moments durant le vieillissement de la base de données d'état de liaison. La détection d'une défaillance de somme de contrôle conduit à des actions distinctes dans chaque cas. Voir les Sections 13 et 14 pour des précisions.

Chaque fois que le champ Numéro de séquence LS indique que deux instances d'un LSA sont les mêmes, le champ Somme de contrôle LS est examiné. Si il y a une différence, l'instance qui a la somme de contrôle LS la plus grande est considérée comme la plus récente.[13] Voir au paragraphe 13.1 pour des précisions.

12.2 Base de données d'état de liaison

Un routeur a une base de données d'état de liaison distincte pour chaque zone à laquelle il appartient. Tous les routeurs appartenant à la même zone ont une base de données d'état de liaisons identique pour la zone.

Les bases de données pour chaque zone individuelle sont toujours traitées séparément. Le calcul du plus court chemin est effectué séparément pour chaque zone (voir la Section 16). Les composants de la base de données d'états de liaisons de la zone sont diffusés seulement dans la zone. Finalement, lors de la construction d'une adjacence (appartenant à la zone A) seule la base de données pour la zone A est synchronisée entre les deux routeurs.

La base de données de la zone se compose des LSA de routeur, des LSA de réseau et des LSA de résumé (tous figurent dans la liste de la structure des données de la zone). De plus, les chemins externes (LSA externes à l'AS) sont inclus dans toutes les bases de données de zone non de bout (voir au paragraphe 3.6).

Une mise en œuvre d'OSPF doit être capable d'accéder aux pièces individuelles d'une base de données de zone. Cette fonction de recherche se fonde sur le type LS, l'identifiant d'état de liaison et le routeur annonceur d'un LSA[14]. Il y aura une seule instance (la plus à jour) de chaque LSA dans la base de données. La fonction de recherche de la base de données est invoquée durant la procédure d'arrosage des LSA (Section 13) et de calcul du tableau d'acheminement (Section 16). De plus, en utilisant cette fonction de recherche, le routeur peut déterminer si il a lui-même jamais généré un LSA particulier, et si c'est le cas, avec quel numéro de séquence LS.

Un LSA est ajouté à la base de données d'un routeur lorsque
a) il est reçu durant le processus d'arrosage (Section 13) ou
b) il est généré par le routeur lui-même (paragraphe 12.4).
Un LSA est supprimé de la base de données d'un routeur lorsque
a) il a été supplanté par une instance plus récente durant le processus d'arrosage (Section 13) ou
b) le routeur génère une instance plus récente de l'un des LSA qu'il a lui-même généré (paragraphe 12.4) ou
c) le LSA est devenu périmé et est retiré du domaine d'acheminement (Section 14).
Chaque fois qu'un LSA est supprimé de la base de données, il doit aussi être retiré des listes de retransmission d'état de liaison de tous les voisins (voir Section 10).

---

13 Lorsque deux LSA ont des sommes de contrôle LS différentes, ils sont supposés être des instances distinctes. Cela peut arriver lorsqu'un routeur redémarre, et perd la trace du précédent numéro de séquence LS du LSA. Dans le cas où les deux LSA ont le même numéro de séquence LS, il n'est pas possible de déterminer quel LSA est réellement plus récent. Cependant, si le mauvais LSA est accepté comme plus récent, le routeur d'origine va simplement générer une autre instance. Voir des précisions complémentaires au paragraphe 13.4.

14 Une recherche doit être faite sur la base d'informations partielles dans un seul cas, durant le calcul du tableau d'acheminement, lorsqu'un LSA de réseau doit être trouvé sur la seule base de son identifiant d'état de liaison. La recherche dans ce cas est cependant bien définie, car il n'y a pas deux LSA de réseau qui puissent avoir le même identifiant d'état de liaison.

12.3 Représentation du TOS

Pour la rétro compatibilité avec les précédentes versions de la spécification OSPF ([Ref9]), les informations spécifiques du type de service (TOS, *type of service*) peuvent être incluses dans les LSA de routeur, les LSA de résumé et les LSA externes à l'AS. Le codage du TOS dans les LSA OSPF est spécifié au Tableau 17. Ce tableau met en rapport le codage OSPF avec le champ TOS de l'en-tête de paquet IP (défini dans [Ref12]). Le codage OSPF est exprimé comme un entier décimal, et le champ TOS de l'en-tête de paquet IP est exprimé dans les valeurs binaires de TOS utilisées dans [Ref12].

Codage OSPF	Valeur de TOS de la RFC 1349
0	0000 service normal
2	0001 minimise le coût monétaire
4	0010 maximise la fiabilité
6	0011
8	0100 maximise le débit
10	0101
12	0110
14	0111
16	1000 minimise le délai
18	1001
20	1010
22	1011
24	1100
26	1101
28	1110
30	1111

Tableau 17 : Représentation du TOS dans OSPF.

12.4 Génération des LSA

Dans toute zone OSPF donnée, un routeur va générer plusieurs LSA. Chaque routeur génère un LSA de routeur. Si le routeur est aussi le routeur désigné pour n'importe lequel des réseaux de la zone, il va générer les LSA de réseau pour ces réseaux.

Les routeurs frontière de zone génèrent un seul LSA de résumé pour chaque destination inter-zone connue. Les routeurs frontière de l'AS génèrent un seul LSA externe à l'AS pour chaque destination externe à l'AS connue. Les destinations sont annoncées une par une de sorte qu'un changement d'un chemin quelconque puisse être diffusé sans avoir à rediffuser la collection entière des chemins. Durant la procédure d'arrosage, de nombreux LSA peuvent être portés par un seul paquet de mise à jour d'état de liaison.

Par exemple, considérons le routeur RT4 de la Figure 6. C'est un routeur frontière de zone, qui a une connexion avec la zone 1 et le cœur de réseau. Le routeur RT4 génère cinq LSA distincts dans le cœur de réseau (un LSA de routeur et un LSA de résumé pour chacun des réseaux N1 à N4). Le routeur RT4 va aussi générer huit LSA distincts dans la zone 1 (un LSA de routeur et sept LSA de résumé comme décrit à la Figure 7). Si RT4 avait été choisi comme routeur désigné pour le réseau N3, il génèrerait aussi un LSA de réseau pour N3 dans la zone 1.

Sur la même figure, le routeur RT5 va générer trois LSA externes à l'AS distincts (un pour chacun des réseaux N12 à N14). Ils seront diffusés à travers l'AS tout entier, en supposant qu'aucune des zones n'a été configurée comme bout. Cependant, si la zone 3 a été configurée comme zone de bout, les LSA externes à l'AS pour les réseaux N12 à N14 ne seront pas diffusés dans la zone 3 (voir au paragraphe 3.6). Au lieu de cela, le routeur RT11 génèrerait un LSA de résumé par défaut qui serait diffusé dans toute la zone 3 (voir au paragraphe 12.4.3). Cela ordonne à tous les routeurs internes de la zone 3 d'envoyer leur trafic extérieur à l'AS à RT11.

Chaque fois qu'est générée une nouvelle instance d'un LSA, son numéro de séquence LS est incrémenté, son âge LS est mis à 0, sa somme de contrôle LS est calculée, et le LSA est ajouté à la base de données d'état de liaison et diffusé sur les interfaces appropriées. Voir au paragraphe 13.2 les détails concernant l'installation du LSA dans la base de données d'état de liaison. Voir au paragraphe 13.3 les détails concernant la diffusion des LSA nouvellement générés.

Les dix événements qui peuvent causer la génération d'une nouvelle instance d'un LSA sont :

(1) Le champ Age LS d'un des LSA générés par le routeur lui-même atteint la valeur LSRefreshTime. Dans ce cas, une nouvelle instance du LSA est générée, même si le contenu du LSA (mis à part l'en-tête de LSA) sera le même. Ceci garantit une génération périodique de tous les LSA. Cette mise à jour périodique des LSA ajoute de la robustesse à l'algorithme d'état de liaison. Les LSA qui décrivent seulement des destinations injoignables ne devraient pas être rafraîchis, mais devraient plutôt être purgés du domaine d'acheminement (voir au paragraphe 14.1).

Lorsque tout ce qui est décrit par un LSA change, un nouveau LSA est généré. Cependant, deux instances du même LSA ne doivent pas être générées dans la période MinLSInterval. Cela peut exiger de retarder la génération de la prochaine instance jusqu'à MinLSInterval. Les événements suivants peuvent causer le changement du contenu d'un LSA. Ces événements ne devraient causer une nouvelle génération que si et seulement si le contenu du nouveau LSA sera différent.

(2) Les changements d'état d'une interface (voir au paragraphe 9.1). Cela peut signifier qu'il est nécessaire de produire une nouvelle instance du LSA de routeur.

(3) Un changement du routeur désigné du réseau de rattachement. Un nouveau LSA de routeur devrait être généré. Également, si le routeur lui-même est maintenant le routeur désigné, un nouveau LSA de réseau devrait être produit. Si le routeur lui-même n'est plus le routeur désigné, tout LSA de réseau qui pourrait avoir été généré pour le réseau devrait être évacué du domaine d'acheminement (voir au paragraphe 14.1).

(4) Un des routeurs voisins change de/vers l'état FULL. Cela peut vouloir dire qu'il est nécessaire de produire une nouvelle instance de LSA de routeur. Également, si le routeur est lui-même le routeur désigné pour le réseau de rattachement, un nouveau LSA de réseau devrait être produit.

Les quatre événements suivants concernent seulement les routeurs frontières de zone :

(5) Un chemin intra-zone a été ajouté/supprimé/modifié dans le tableau d'acheminement. Cela peut causer la génération d'une nouvelle instance de LSA de résumé (pour ce chemin) dans chaque zone rattachée (ce qui peut inclure le cœur de réseau).

(6) Un chemin inter-zone a été ajouté/supprimé/modifié dans le tableau d'acheminement. Cela peut causer la génération d'une nouvelle instance de LSA de résumé (pour ce chemin) dans chaque zone rattachée (mais JAMAIS pour le cœur de réseau).

(7) Le routeur devient rattaché à une zone. Le routeur doit alors générer des LSA de résumé dans la nouvelle zone de rattachement pour tous les chemins intra-zone et inter-zone pertinents dans le tableau d'acheminement du routeur. Voir au paragraphe 12.4.3 pour plus de détails.

(8) Lorsque l'état d'une des liaisons virtuelles configurée du routeur change, il peut être nécessaire de générer un nouveau LSA de routeur dans la zone de transit de la liaison virtuelle (voir l'exposé sur le bit V du LSA de routeur au paragraphe 12.4.1), ainsi que de générer un nouveau LSA de routeur dans le cœur de réseau.

Les deux derniers événements concernent seulement les routeurs frontière de l'AS (et anciens routeurs frontière de l'AS) :

(9) Un chemin externe acquis par expérience directe avec un protocole d'acheminement externe (comme BGP) change. Cela va causer la génération d'une nouvelle instance d'un LSA externe à l'AS par le routeur frontière de l'AS.

(10) Un routeur cesse d'être un routeur frontière de l'AS, peut-être après redémarrage. Dans cette situation, le routeur devrait purger tous les LSA externes à l'AS qu'il avait précédemment généré. Ces LSA peuvent être purgés par la procédure de vieillissement prématuré spécifiée au paragraphe 14.1.

La construction de chaque type de LSA est expliquée en détail ci-dessous. En général, ces paragraphes décrivent le contenu des corps des LSA (c'est-à-dire, la partie qui vient après les 20 octets d'en-tête du LSA). Pour des informations concernant la construction de l'en-tête de LSA, voir au paragraphe 12.1.

12.4.1 LSA de routeur

Un routeur génère un LSA de routeur pour chaque zone à laquelle il appartient. Un tel LSA décrit la collection des états de liaison à la zone du routeur. Le LSA est diffusé dans toute la zone en question, et pas plus loin.

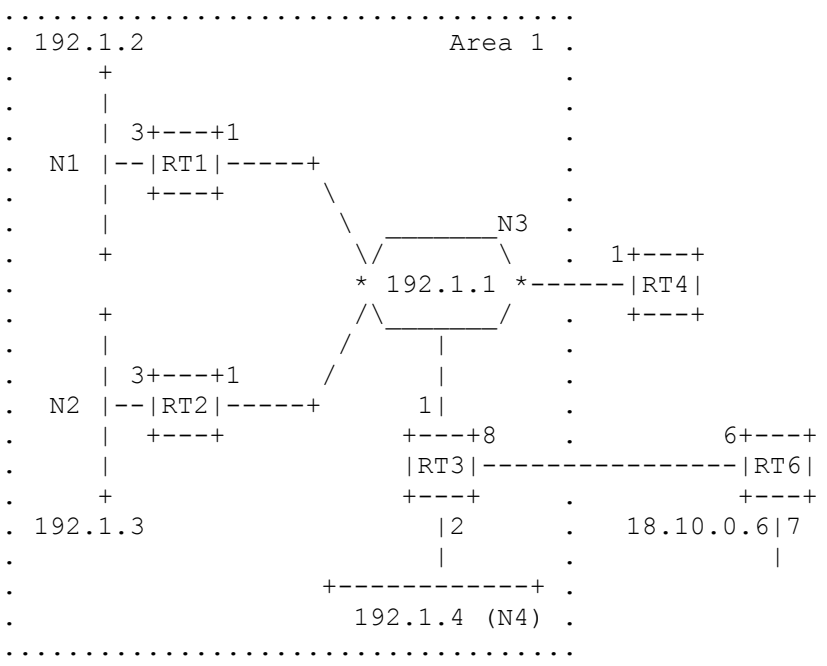


Figure 15 : Zone 1 avec indication des adresses IP

Le format d'un LSA de routeur est indiqué à l'Appendice A (paragraphe A.4.2). Les vingt premiers octets du LSA constituent l'en-tête générique de LSA qui a été exposé au paragraphe 12.1. Les LSA de routeur ont le type LS = 1.

Un routeur indique aussi si il est un routeur frontière de zone ou un routeur frontière de l'AS en réglant les bits appropriés (bit B et bit E, respectivement) dans ses LSA de routeur. Cela permet de sauvegarder les chemins vers ces types de routeurs dans le tableau d'acheminement, pour le traitement ultérieur des LSA de résumé et des LSA externes à l'AS. Le bit B devrait être établi chaque fois que le routeur est rattaché activement à deux zones ou plus, même si le routeur n'est pas actuellement rattaché à la zone cœur de réseau OSPF. Le bit E ne devrait jamais être établi dans un LSA de routeur pour une zone de bout (les zones de bout ne peuvent pas contenir de routeur frontière de l'AS).

De plus, le routeur n'établit le bit V dans son LSA de routeur pour la zone A que si et seulement si le routeur est le point de terminaison d'une ou plusieurs liaisons virtuelles pleinement adjacentes qui ont la zone A comme zone de transit. L'établissement du bit V permet aux autres routeurs de la zone A de découvrir si la zone prend en charge le trafic de transit (voir TransitCapability à la Section 6).

Le LSA de routeur décrit ensuite les connexions actives du routeur (c'est-à-dire, les interfaces ou les liaisons) avec la zone. Chaque liaison a son type conforme au type de réseau de rattachement. Chaque liaison est aussi étiquetée avec son identifiant de liaison. Cet identifiant de liaison donne un nom à l'entité qui est à l'autre extrémité de la liaison. Le Tableau 18 récapitule les valeurs utilisées pour les champs Type et Identifiant de liaison.

Type de liaison	**Description**	**Identifiant de liaison**
1	Point à point	Identifiant de liaison du routeur voisin
2	Liaison à réseau de transit	Adresse d'interface du routeur désigné
3	Liaison à réseau de bout	Numéro de réseau IP
4	Liaison virtuelle	Identifiant du routeur voisin

Tableau 18 : Descriptions de liaison dans le LSA de routeur.

De plus, le champ Données de liaison est spécifié pour chaque liaison. Ce champ donne 32 bits d'informations supplémentaires pour la liaison. Pour les liaisons avec les réseaux de transit, les liaisons point à point numérotées et les liaisons virtuelles, ce champ spécifie l'adresse IP d'interface de l'interface de routeur associée (c'est nécessaire pour le calcul du tableau d'acheminement, voir au paragraphe 16.1.1). Pour les liaisons avec les réseaux d'extrémité, ce champ spécifie le gabarit d'adresse IP du réseau de bout. Pour les liaisons point à point non numérotées, le champ Données de liaison devrait être réglé à la valeur ifIndex du MIB-II [Ref8] de l'interface non numérotée.

Finalement est spécifié le coût d'utilisation de la liaison en sortie. Le coût de sortie d'une liaison est configurable. À l'exception des liaison avec des réseaux d'extrémité, le coût de sortie doit toujours être différent de zéro.

Pour décrire plus avant le processus de construction de la liste des descriptions de liaison, supposons qu'un routeur souhaite construire un LSA de routeur pour la zone A. Le routeur examine sa collection de structures de données d'interface. Pour chaque interface, on suit les étapes suivantes :

- Si le réseau de rattachement n'appartient pas à la zone A, aucune liaison n'est ajoutée au LSA, et l'interface suivante devrait être examinée.

- Si l'état de l'interface est Down, aucune liaison n'est ajoutée.

- Si l'état de l'interface est Bouclage, ajouter une liaison de Type 3 (réseau de bout) pour autant qu'il ne s'agisse pas d'une interface avec un réseau point à point non numéroté. L'identifiant de liaison devrait être réglé à l'adresse IP d'interface, les Données de liaison réglées au gabarit 0xffffffff (qui indique un chemin d'hôte) et le coût réglé à 0.

- Autrement, les descriptions de liaison ajoutées au LSA de routeur dépendent du type d'interface OSPF. Les descriptions de liaison utilisées pour les interfaces point à point sont spécifiées au paragraphe 12.4.1.1, pour les liaisons virtuelles au paragraphe 12.4.1.2, pour les interfaces de diffusion et NBMA au 12.4.1.3, et pour les interfaces point à multipoint en 12.4.1.4.

Après considération de toutes les interfaces de routeur, les liaisons d'hôte sont ajoutées au LSA de routeur en examinant la liste des hôtes rattachés qui appartiennent à la zone A. Un chemin d'hôte est représenté comme une liaison de type 3 (réseau de bout) dont l'identifiant de liaison est l'adresse IP de l'hôte, Données de liaison est le gabarit de tout à uns (0xffffffff), et le coût celui configuré de l'hôte (voir au paragraphe C.7).

12.4.1.1 Description d'interfaces en point à point

Pour les interfaces point à point, une ou plusieurs descriptions de liaison sont ajoutées au LSA de routeur comme suit :

- Si le routeur voisin est pleinement adjacent, ajouter une liaison de type 1 (point à point). L'identifiant de liaison devrait être réglé à l'identifiant de routeur du routeur voisin. Pour les réseaux point à point numérotés, les données de liaison devraient spécifier l'adresse IP d'interface. Pour les réseaux point à point non numérotés, le champ Données de liaison devrait spécifier la valeur ifIndex du MIB-II [Ref8] de l'interface. Le coût devrait être établi au coût de sortie de l'interface point à point.

- De plus, pour autant que l'état de l'interface soit "point à point" (et sans considération de l'état du routeur voisin) une liaison de type 3 (réseau de bout) devrait être ajoutée. Cette liaison de bout peut prendre deux formes :

  Option 1
  En supposant que l'adresse IP du routeur voisin soit connue, régler l'identifiant de liaison de la liaison de type 3 à l'adresse IP du voisin, les Données de liaison au gabarit 0xffffffff (indiquant un chemin d'hôte) et le coût au coût de sortie configuré de l'interface[15].

  Option 2
  Si un sous-réseau a été alloué à la liaison point à point, régler l'identifiant de liaison de la liaison de type 3 à l'adresse IP du sous-réseau, les Données de liaison au gabarit du sous-réseau, et le coût au coût de sortie configuré de l'interface [16].

12.4.1.2 Description d'interfaces de diffusion et de NBMA

Pour les interfaces de diffusion et NBMA opérationnelles, une seule description de liaison est ajoutée au LSA de routeur comme suit :

- Si l'état de l'interface est Attente, ajouter une liaison de type 3 (réseau de bout) avec l'identifiant de liaison réglé au numéro de réseau IP du réseau de rattachement, Données de liaison réglé au gabarit d'adresse du réseau de rattachement, et coût égal au coût de sortie configuré de l'interface.

- Autrement, il y a eu un routeur désigné choisi pour le réseau de rattachement. Si le routeur est pleinement adjacent au

15 C'est la façon dont la RFC1583 spécifie la représentation point à point. Elle a trois avantages : a) elle n'exige pas d'allouer un sous-réseau à la liaison point à point, b) elle tend à biaiser l'acheminement de telle sorte que les paquets destinés à l'interface point à point soient en réalité reçus sur l'interface (ce qui est utile pour les diagnostics) et c) elle permet l'amorçage réseau d'un voisin, sans exiger que le programme d'amorçage contienne une mise en œuvre OSPF.

16 C'est la représentation point à point plus traditionnelle utilisée par des protocoles tels que RIP.

routeur désigné, ou si le routeur lui-même est routeur désigné et est pleinement adjacent à au moins un autre routeur, ajouter une seule liaison de type 2 (réseau de transit) avec Identifiant de liaison réglé à l'adresse IP d'interface du routeur désigné (qui peut être le routeur lui-même) du réseau de rattachement, Données de liaison réglé à la propre adresse IP d'interface du routeur, et Coût égal au coût de sortie configuré de l'interface. Autrement, ajouter une liaison comme si l'état de l'interface était Attente (voir ci-dessus).

12.4.1.3 Description de liaisons virtuelles

Pour les liaisons virtuelles, une description de liaison n'est ajoutée au LSA de routeur que lorsque le voisin virtuel est pleinement adjacent. Dans ce cas, ajouter une liaison de type 4 (liaison virtuelle) avec Identifiant de liaison réglé à l'identifiant de routeur du voisin virtuel, Données de liaison réglé à l'adresse IP d'interface associée à la liaison virtuelle et Coût réglé au coût calculé pour la liaison virtuelle durant le calcul du tableau d'acheminement (voir au paragraphe 15).

12.4.1.4 Description d'interfaces de point à multipoint

Pour les interfaces point à multipoint opérationnelles, une ou plusieurs descriptions de liaison sont ajoutées au LSA de routeur comme suit :

- Une seule liaison de type 3 (réseau de bout) est ajoutée avec Identifiant de liaison réglé à la propre adresse IP d'interface du routeur, Données de liaison réglé au gabarit 0xffffffff (indiquant un chemin d'hôte), et Coût réglé à 0.

- Pour chaque voisin pleinement adjacent associé à l'interface, ajouter une liaison de type 1 supplémentaire (point à point) avec Identifiant de liaison réglé à l'identifiant de routeur du routeur voisin, Données de liaison réglé à l'adresse IP d'interface et Coût égal au coût de sortie configuré de l'interface.

12.4.1.5 Exemples de LSA de routeur

Considérons les LSA de routeur générés par le routeur RT3, comme décrit par la Figure 6. La zone contenant le routeur RT3 (zone 1) a été redessinée, avec de vraies adresses réseau, dans la Figure 15. Supposons que le dernier octet de toutes les adresses d'interface de RT3 soit 3, donnons lui les adresses d'interface 192.1.1.3 et 192.1.4.3, et supposons que les autres routeurs ont des schémas d'adressage similaires. De plus, supposons que toutes les liaisons sont fonctionnelles, et que les identifiants de routeur sont alloués comme la plus petite adresse IP d'interface.

RT3 génère deux LSA de routeur, un pour la zone 1 et un pour le cœur de réseau. Supposons que le routeur RT4 a été choisi comme routeur désigné pour le réseau 192.1.1.0. Le LSA de routeur de RT3 pour la zone 1 est montré ci-dessous. Il indique que RT3 a deux connexions avec la zone 1, la première est une liaison avec le réseau de transit 192.1.1.0 et la seconde, une liaison avec le réseau de bout 192.1.4.0. Noter que le réseau de transit est identifié par l'interface IP de son routeur désigné (c'est-à-dire, l'identifiant de liaison = 192.1.1.4 qui est l'interface IP du routeur désigné RT4 avec 192.1.1.0). Noter aussi que RT3 a indiqué qu'il est un routeur frontière de zone.

; LSA de routeur de RT3 pour la zone 1

Age LS = 0 ; toujours vrai à la création
Options = (bit E) ;
Type LS = 1 ; indique un LSA de routeur
Identifiant d'état de liaison = 192.1.1.3 ; Identifiant de routeur de RT3
Routeur annonceur = 192.1.1.3 ; Identifiant de routeur de RT3
bit E = 0 ; n'est pas un routeur frontière de l'AS

bit B = 1 ; routeur frontière de zone
n° de liaison = 2
Identifiant de liaison = 192.1.1.4 ; adresse IP du routeur désigné
Données de liaison = 192.1.1.3 ; interface IP de RT3 au réseau
Type = 2 ; connecte au réseau de transit
n° de métrique de TOS = 0
métrique = 1

Identifiant de liaison = 192.1.4.0 ; numéro de réseau IP
Données de liaison = 0xffffff00 ; Gabarit de réseau
Type = 3 ; connecte au réseau de bout
n° de métrique de TOS = 0
métrique = 2

Le LSA de routeur suivant de RT3 pour le cœur de réseau est donné. Il indique que RT3 a un seul rattachement au cœur de

réseau. Ce rattachement est via une liaison point à point non numérotée au routeur RT6. RT3 a encore une fois indiqué qu'il est un routeur frontière de zone.

; LSA de routeur de RT3 pour le cœur de réseau

Age LS = 0 ; toujours vrai à la création
Options = (bit E) ;
Type LS = 1 ; indique un LSA de routeur
Identifiant d'état de liaison = 192.1.1.3 ; Identifiant de routeur de RT3
Routeur annonceur = 192.1.1.3 ; Identifiant de routeur de RT3
bit E = 0 ; n'est pas un routeur frontière de l'AS
bit B = 1 ; routeur frontière de zone
n° de liaison = 1
Identifiant de liaison = 18.10.0.6 ; Identifiant de routeur du voisin
Données de liaison = 0.0.0.3 ; ifIndex de MIB-II de liaison point à point
Type = 1 ; connecte au routeur
n° de métrique de TOS = 0
métrique = 8

12.4.2 LSA de réseau

Un LSA de réseau est généré pour chaque réseau de diffusion en transit ou NBMA. (Un réseau de transit est un réseau qui a deux routeurs rattachés ou plus). Le LSA de réseau décrit tous les routeurs qui sont rattachés au réseau.

Le routeur désigné pour le réseau génère le LSA. Le routeur désigné ne génère le LSA que si il est pleinement adjacent à au moins un autre routeur sur le réseau. Le LSA de réseau est diffusé dans toute la zone qui contient le réseau de transit, et pas plus loin. Le LSA de réseau fait la liste des routeurs qui sont pleinement adjacents au routeur désigné ; chaque routeur pleinement adjacent est identifié par son identifiant de routeur OSPF. Le routeur désigné s'inclut lui-même dans cette liste.

L'identifiant d'état de liaison pour un LSA de réseau est l'adresse IP d'interface du routeur désigné. Cette valeur, dont le gabarit est le gabarit d'adresse du réseau (qui est aussi contenue dans le LSA de réseau) donne l'adresse IP du réseau.

Un routeur qui a été le routeur désigné pour un réseau, mais ne l'est plus, devrait éliminer le LSA de réseau qu'il avait précédemment généré. Ce LSA n'est plus utilisé dans le calcul du tableau d'acheminement. Il est éliminé en incrémentant prématurément l'âge du LSA jusqu'à MaxAge et en le rediffusant (voir au paragraphe 14.1). De plus, dans les rares cas où l'identifiant de routeur d'un routeur a changé, tout LSA de réseau qui a été généré avec l'identifiant de routeur précédent du routeur doit être éliminé. Comme le routeur peut n'avoir pas idée de ce que pouvait être le précédent identifiant de routeur, ces LSA de réseau sont indiqués en ayant leur identifiant d'état de liaison égal à une des adresses IP d'interface du routeur et leur Routeur annonceur égal à une valeur autre que l'identifiant de routeur actuel du routeur (voir au paragraphe 13.4 pour des précisions).

12.4.2.1 Exemples de LSA de réseau

Considérons à nouveau la configuration de zone de la Figure 6. Les LSA de réseau sont générés pour le réseau N3 dans la zone1, les réseaux N6 et N8 dans la zone 2, et le réseau N9 dans la zone 3. En supposant que le routeur RT4 a été choisi comme routeur désigné pour le réseau N3, les LSA de réseau suivants sont générés par RT4 au nom du réseau N3 (voir à la Figure 15 les allocations d'adresses) :

; LSA de réseau pour le réseau N3

Age LS = 0 ; toujours vrai à la création
Options = (bit E) ;
Type LS = 2 ; indique un LSA de réseau
identifiant d'état de liaison = 192.1.1.4 ; adresse IP du routeur désigné
Routeur annonceur = 192.1.1.4 ; l'identifiant de routeur de RT4
Gabarit de réseau = 0xffffff00
Routeur rattaché = 192.1.1.4 ; l'identifiant de routeur
Routeur rattaché = 192.1.1.1 ; l'identifiant de routeur
Routeur rattaché = 192.1.1.2 ; l'identifiant de routeur
Routeur rattaché = 192.1.1.3 ; l'identifiant de routeur

12.4.3 LSA de résumé

La destination décrite par un LSA de résumé est un réseau IP, un routeur frontière de l'AS ou une gamme d'adresses IP. Les LSA de résumé sont diffusés seulement dans une seule zone. La destination décrite est externe à la zone, mais appartient encore au système autonome.

Les LSA de résumé sont générés par les routeurs frontières de zone. Les résumés de chemin précis à annoncer dans une zone sont déterminés en examinant la structure du tableau d'acheminement (voir la Section 11) conformément à l'algorithme décrit ci-dessous. Noter que seuls les chemins intra-zone sont annoncés dans le cœur de réseau, alors que les chemins intra-zone et inter-zone sont tous deux annoncés dans les autres zones.

Pour déterminer quels chemins annoncer dans la zone de rattachement A, chaque entrée de tableau d'acheminement est traitée comme suit. Rappelez vous que chaque entrée de tableau d'acheminement décrit un ensemble de meilleurs chemins de coût égal pour une destination particulière :

- Seuls les types de destination de réseau et de routeur frontière de l'AS sont annoncés dans les LSA de résumé. Si le type de destination de l'entrée de tableau d'acheminement est un routeur frontière de zone, examiner l'entrée de tableau d'acheminement suivante.

- Les chemins externes à l'AS ne sont jamais annoncés dans les LSA de résumé. Si l'entrée de tableau d'acheminement a le Type de chemin de externe de type 1 ou externe de type 2, examiner l'entrée de tableau d'acheminement suivante.

- Autrement, si la zone associée à cet ensemble de chemins est la zone A elle-même, ne pas générer de LSA de résumé pour le chemin[17].

- Autrement, si les prochains bonds associés à cet ensemble de chemins appartiennent à la zone A elle-même, ne pas générer de LSA de résumé pour le chemin[18]. Ceci est l'équivalent logique de la logique d'horizon partagé d'un protocole de vecteur distance.

- Autrement, si le coût du tableau d'acheminement égale ou excède la valeur LSInfinity, un LSA de résumé ne peut pas être généré pour ce chemin.

- Autrement, si la destination de ce chemin est un routeur frontière de l'AS, un LSA de résumé devrait être généré si et seulement si l'entrée de tableau d'acheminement décrit le chemin préféré pour le routeur frontière de l'AS (voir l'étape 3 du paragraphe 16.4). S'il en est ainsi, un LSA de résumé de type 4 est généré pour la destination, avec l'identifiant d'état de liaison égal à l'identifiant de routeur du routeur frontière de l'AS et une métrique égale au coût de l'entrée du tableau d'acheminement. Note : ces LSA ne devraient pas être générés si la zone A a été configurée comme zone de bout.

- Autrement, le type de destination est "réseau". Si c'est un chemin inter-zone, générer un LSA de résumé de type 3 pour la destination, avec l'identifiant d'état de liaison égal à l'adresse du réseau (si nécessaire, l'identifiant d'état de liaison peut aussi avoir un ou plusieurs des bits d'hôte du réseau établis ; voir des précisions à l'Appendice E) et la métrique égale au coût du tableau d'acheminement.

- Le seul cas restant est celui d'un chemin intra-zone pour un réseau. Cela signifie que le réseau est contenu dans une des zones directement rattachées au routeur. En général, cette information doit être condensée avant d'apparaître dans des LSA de résumé. Rappelez vous qu'une zone a une liste configurée de gammes d'adresses, chaque gamme comportant une paire [adresse,gabarit] et une indication d'état de Annoncer ou NePasAnnoncer. Au plus un seul LSA de résumé de type 3 est généré pour chaque gamme. Lorsque l'état de la gamme indique Annoncer, un LSA de résumé de type 3 est généré avec l'identifiant d'état de liaison égal à l'adresse de la gamme (si nécessaire, l'identifiant d'état de liaison peut aussi avoir un ou plusieurs bits "hôte" de la gamme mis ; voir les précisions à l'Appendice E) et un coût égal au plus grand coût de tous les réseaux composants. Lorsque l'état de la gamme indique NePasAnnoncer, le LSA de résumé de type 3 est supprimé et les réseaux composants restent cachés aux autres zones.

  Par défaut, si un réseau n'est contenu dans aucune gamme d'adresses explicitement configurée, un LSA de résumé de

17 Cette disposition couvre le cas où les chemins inter-zone ne sont pas résumés au cœur de réseau. Cela parce que les chemins inter-zone sont toujours associés à la zone cœur de réseau.

18 Cette disposition n'est invoquée que quand la zone A non cœur de réseau accepte du trafic de données en transit (c'est-à-dire, a TransitCapability mis à VRAI). Par exemple, dans la configuration de zone de la Figure 6, la zone 2 accepte le trafic de transit du fait de la liaison virtuelle configurée entre les routeurs RT10 et RT11. Il en résulte que le routeur RT11 a seulement besoin de générer un seul LSA de résumé dans la zone 2 (avec la disparition de la destination N9-N11,H1) car tous les autres chemins éligibles du routeur RT11 ont des prochains bonds qui appartiennent à la zone 2 elle-même (et à ce titre doivent seulement avoir des annonces des autres routeurs frontière de zone ; dans ce cas, les routeurs RT10 et RT7).

type 3 est généré avec l'identifiant d'état de liaison égal à l'adresse du réseau (si nécessaire, l'identifiant d'état de liaison peut aussi avoir un ou plusieurs des bits "hôte" du réseau mis ; voir les précisions à l'Appendice E) et la métrique égale au coût du tableau d'acheminement du réseau.

Si une zone est capable de porter du trafic de transit (c'est-à-dire, son TransitCapability est mis à VRAI) les informations d'acheminement qui concernent les réseaux du cœur de réseau ne devraient pas être condensées avant d'être résumées dans la zone. Pas plus que ne devrait être supprimée l'annonce des réseaux de cœur de réseau dans les zones de transit. En d'autres termes, les gammes configurées du cœur de réseau devraient être ignorées lors de la génération de LSA de résumés dans les zones de transit.

Si un routeur annonce un LSA de résumé pour une destination qui devient ensuite injoignable, le routeur doit alors éliminer le LSA du domaine d'acheminement en réglant son âge à MaxAge et en le rediffusant (voir au paragraphe 14.1). Aussi, si la destination est toujours joignable, mais ne peut plus être annoncée selon la procédure ci-dessus (par exemple, c'est maintenant un chemin inter-zone, alors que c'était un chemin intra-zone associé à une zone non cœur de réseau ; il ne serait plus annonçable au cœur de réseau) le LSA devrait aussi être éliminé du domaine d'acheminement.

12.4.3.1 Génération des LSA de résumé dans les zones de bout

L'algorithme du paragraphe 12.4.3 est facultatif lorsque la zone A est une zone de bout OSPF. Les routeurs frontières de zone qui se connectent à une zone de bout peuvent générer des LSA de résumé dans la zone conformément à l'algorithme du paragraphe 12.4.3, ou peuvent choisir de générer seulement un sous-ensemble des LSA de résumé, éventuellement avec un contrôle de configuration. Moins il y a de LSA générés, plus la base de données d'état de liaison de la zone de bout est petite, réduisant d'autant les demandes sur les ressources de ses routeurs. Cependant, omettre des LSA peut aussi conduire à un acheminement inter-zone sous optimal, bien que l'acheminement continue de fonctionner.

Comme spécifié au paragraphe 12.4.3, les LSA de résumé de type 4 (LSA de résumé ASBR) ne sont jamais générés dans les zones de bout.

Dans une zone de bout, au lieu d'importer des chemins externes, chaque routeur frontière de zone génère un "LSA de résumé par défaut" dans la zone. L'identifiant d'état de liaison pour le LSA de résumé par défaut est réglé à DefaultDestination, et la métrique est réglée au paramètre configurable (par zone) de StubDefaultCost. Noter que StubDefaultCost n'a pas besoin d'être configuré de façon identique dans tous les routeurs frontière de zone de la zone de bout.

12.4.3.2 Exemples de LSA de résumé

Considérons à nouveau la configuration de zone de la Figure 6. Les routeurs RT3, RT4, RT7, RT10 et RT11 sont tous des routeurs frontières de zone, et génèrent donc des LSA de résumé. Considérons en particulier le routeur RT4. Son tableau d'acheminement a été calculé comme exemple au paragraphe 11.3. RT4 génère des LSA de résumé à la fois pour le cœur de réseau et pour la zone 1. Dans le cœur de réseau, le routeur RT4 génère des LSA distincts pour chacun des réseaux N1 à N4. Dans la zone 1, le routeur RT4 génère des LSA distincts pour les réseaux N6 à N8 et pour les routeurs frontière de l'AS RT5, RT7. Il concentre aussi les chemins d'hôte Ia et Ib en un seul LSA de résumé. Finalement, les chemins des réseaux N9, N10, N11 et de l'hôte H1 sont annoncés par un seul LSA de résumé. Cette concentration était à l'origine effectuée par le routeur RT11.

Ces LSA sont illustrés graphiquement aux Figures 7 et 8. Deux des LSA de résumé générés par le routeur RT4 suivent. Les adresses IP réelles pour les réseaux et routeurs en question ont été allouées dans la Figure 15.

; LSA de résumé pour le réseau N1, généré par le routeur RT4 dans le cœur de réseau
Age LS = 0 ; toujours vrai à la création
Options = (bit E) ;
Type LS = 3 ; LSA de résumé de type 3
Identifiant d'état de liaison = 192.1.2.0 ; numéro de réseau IP de N1
Routeur annonceur = 192.1.1.4 ; identifiant de RT4
métrique = 4

; LSA de résumé pour routeur frontière de l'AS RT7 généré par le Routeur RT4 dans la zone 1
Age LS = 0 ; toujours vrai à la création
Options = (bit E) ;
Type LS = 4 ; LSA de résumé de type 4
Identifiant d'état de liaison = identifiant du routeur RT7
Routeur annonceur = 192.1.1.4 ; identifiant de RT4
métrique = 14

12.4.4 LSA externes à l'AS

Les LSA externes à l'AS décrivent les chemins vers des destinations externes au système autonome. La plupart des LSA externes à l'AS décrivent des chemins pour des destinations externes spécifiques ; dans ces cas l'identifiant d'état de liaison du LSA est réglé à l'adresse IP du réseau de destination (si nécessaire, l'identifiant d'état de liaison peut aussi avoir un ou plusieurs des bits "hôte" du réseau établis (voir les détails à l'Appendice E). Cependant, un chemin par défaut pour le système autonome peut être décrit dans un LSA externe à l'AS en réglant l'identifiant d'état de liaison du LSA à DefaultDestination (0.0.0.0). Les LSA externes à l'AS sont générés par les routeurs frontière de l'AS. Un routeur frontière de l'AS génère un seul LSA externe à l'AS pour chaque chemin externe qu'il a appris, soit par un autre protocole d'acheminement (tel que BGP) soit par des informations de configuration.

Les LSA externes à l'AS sont le seul type de LSA qui soient diffusés au système autonome tout entier ; tous les autres types de LSA sont spécifiques d'une seule zone. Cependant, les LSA externes à l'AS ne sont pas diffusés dans les zones de bout (voir au paragraphe 3.6). Cela permet une réduction de la taille des bases de données d'état de liaison pour les routeurs internes aux zones de bout.

La métrique qui est annoncée pour un chemin externe peut être de l'un de deux types. Les métriques de type 1 sont comparables à la métrique d'état de la liaison. Les métriques de type 2 sont supposées être supérieures au coût de tout chemin intra-AS.

Si un routeur annonce un LSA externe à l'AS pour une destination qui devient ensuite injoignable, le routeur doit alors sortir le LSA du domaine d'acheminement en réglant son âge à MaxAge et en le rediffusant (voir au paragraphe 14.1).

12.4.4.1 Exemples de LSA externes à l'AS

Considérons une fois encore l'AS décrit à la Figure 6. Il y a deux routeurs frontière de l'AS : RT5 et RT7. Le routeur RT5 génère les trois LSA externes à l'AS, pour les réseaux N12 à N14. Le routeur RT7 génère les deux LSA externes à l'AS, pour les réseaux N12 et N15. Supposons que RT7 ait appris son chemin vers N12 via BGP, et qu'il souhaite annoncer une métrique de type 2 à l'AS. RT7 va alors générer les LSA suivants pour N12 :

```
; LSA externe à l'AS pour le réseau N12, généré par le routeur RT7
Age LS = 0                              ; toujours vrai à la création
Options = (bit E)       ;
LS type = 5     ; LSA externe à l'AS
Identifiant d'état de liaison = numéro de réseau IP de N12
Routeur annonceur = identifiant du routeur RT7
bit E = 1       ; métrique de type 2
Métrique = 2
Adresse de transmission = 0.0.0.0
```

Dans l'exemple ci-dessus, le champ Adresse de transmission a été réglé à 0.0.0.0, indiquant que les paquets pour la destination externe devraient être transmis au routeur OSPF annonceur (RT7). Cela n'est pas toujours souhaitable. Considérons l'exemple décrit par la Figure 16. Il y a trois routeurs OSPF (RTA, RTB et RTC) connectés à un réseau commun. Un seul de ces routeurs, RTA, échange des informations BGP avec le routeur non OSPF RTX. RTA doit donc générer les LSA externes à l'AS pour ces destinations qu'il a apprises de RTX. En utilisant le champ adresse de transmission du LSA externe à l'AS, RTA peut spécifier que les paquets pour ces destinations soient transmis directement à RTX. Sans ce dispositif, les routeurs RTB et RTC prendraient un bond supplémentaire pour atteindre ces destinations.

Noter que quand le champ d'adresse de transmission est différent de zéro, il devrait pointer sur un routeur appartenant à un autre système autonome.

Une adresse de transmission peut aussi être spécifiée pour le chemin par défaut. Par exemple, dans la Figure 16, RTA peut vouloir spécifier que tous les paquets à destination externe devraient être transmis par défaut à son homologue BGP RTX. Le LSA externe à l'AS résultant est décrit ci-dessous. Noter que l'identifiant d'état de liaison est réglé à DefaultDestination.

```
; Chemin par défaut, généré par les du routeur RTA transmis par l'intermédiaire de RTX
Age LS = 0                              ; toujours vrai à la création
Options = (bit E)       ;
Type LS = 5   ; LSA externe à l'AS
Identifiant d'état de liaison = DefaultDestination  ; chemin par défaut
Routeur annonceur = identifiant du routeur RTA
```

bit E = 1 ; métrique de type 2
métrique = 1
Adresse de transmission = adresse IP de RTX

Dans la Figure 16, supposons plutôt que RTA et RTB échangent tous deux des informations BGP avec RTX. Dans ce cas, RTA et RTB génèreront le même ensemble de LSA externes à l'AS. Ces LSA, si ils spécifient la même métrique, seront fonctionnellement équivalents car ils vont spécifier les mêmes destination et adresse de transmission (RTX). Cela conduit clairement à une duplication. Si seulement l'un de RTA ou RTB génère l'ensemble des LSA externes à l'AS, l'acheminement restera le même, et la taille de la base de données d'état de liaison va diminuer. Cependant, il doit être défini sans ambiguïté quel routeur génère les LSA, sinon aucun ne le fera, ou l'identité du générateur peut osciller). Les règles suivantes sont donc établies : si deux routeurs, tous deux joignables l'un par l'autre, génèrent des LSA externes à l'AS fonctionnellement équivalents (c'est-à-dire, même destination, coût et adresse de transmission différente de zéro), le LSA généré par le routeur qui a l'identifiant de routeur OSPF le plus élevé est utilisé. Le routeur qui a l'identifiant de routeur OSPF le plus faible peut alors purger son LSA. La purge des LSA est exposée au paragraphe 14.1.

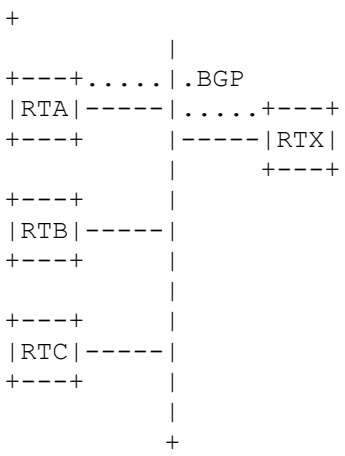


Figure 16 : Exemple d'adresse de transmission

13. Procédure d'arrosage

Les paquets Mise à jour d'état de liaison fournissent le mécanisme d'arrosage des LSA. Un paquet Mise à jour d'état de liaison peut contenir plusieurs LSA distincts, et diffuser chaque LSA un bond plus loin que son point d'origine. Pour rendre fiable la procédure d'arrosage, chaque LSA doit être acquitté séparément. Les accusés de réception sont transmis dans des paquets d'accusé de réception d'état de liaison. De nombreux accusés de réception peuvent aussi être groupés en en seul paquet.

La procédure d'arrosage commence quand un paquet Mise à jour d'état de liaison a été reçu. De nombreuses vérifications de cohérence ont été faites sur le paquet reçu avant d'être passé à la procédure d'arrosage (voir au paragraphe 8.2). En particulier, le paquet Mise à jour d'état de liaison a été associé à un voisin particulier, et une zone particulière. Si le voisin est dans un état inférieur à Échange, le paquet devrait être abandonné sans autre traitement.

Tous les types de LSA, autres que les LSA externes à l'AS, sont associés à une zone spécifique. Cependant, les LSA ne contiennent pas de champ de zone. La zone d'un LSA doit être déduite de l'en-tête du paquet Mise à jour d'état de liaison.

Pour chaque LSA contenu dans un paquet Mise à jour d'état de liaison, on suit les étapes suivantes :

(1) Valider la somme de contrôle LS du LSA. Si la somme de contrôle se révèle invalide, éliminer le LSA et prendre le suivant dans le paquet Mise à jour d'état de liaison.

(2) Examiner le type LS du LSA. Si le type LS est inconnu, éliminer le LSA et obtenir le suivant dans le paquet Mise à jour d'état de liaison. La présente spécification définit les types LS de 1 à 5 (voir au paragraphe 4.3).

(3) Autrement, si c'est un LSA externe à l'AS (type LS = 5), et si la zone a été configurée comme zone de bout, éliminer le LSA et obtenir le suivant dans le paquet Mise à jour d'état de liaison. Les LSA externes à l'AS ne sont pas diffusés dans les zones de bout (voir au paragraphe 3.6).

(4) Autrement, si l'âge LS du LSA est égal à MaxAge, et s'il n'y a actuellement pas d'instance du LSA dans la base de données d'état de liaison du routeur, et si aucun des voisins du routeur n'est dans les états Échange ou Loading, effectuer alors les actions suivantes : a) Accuser réception du LSA en renvoyant un paquet d'accusé de réception d'état de liaison au voisin qui l'a envoyé (voir au paragraphe 13.5) et b) Éliminer le LSA et examiner le LSA suivant (s'il en est) sur la liste du paquet Mise à jour d'état de liaison.

(5) Autrement, trouver l'instance de ce LSA qui est actuellement contenue dans la base de données d'état de liaison du routeur. Si il n'y a pas de copie dans la base de données, ou si le LSA reçu est plus récent que la copie de la base de données (voir au paragraphe 13.1 ci-dessous comment déterminer quel LSA est plus récent) les étapes suivantes doivent être effectuées :

(a) S'il y a déjà une copie dans la base de données, et si la copie de la base de données a été reçue via l'arrosage et installée moins de MinLSArrival secondes auparavant, éliminer le nouveau LSA (sans en accuser réception) et examiner le prochain LSA (s'il en est) sur la liste du paquet Mise à jour d'état de liaison.

(b) Autrement diffuser immédiatement le nouveau LSA sur un sous-ensemble des interfaces du routeur (voir au paragraphe 13.3). Dans certains cas (par exemple, l'état de l'interface receveuse est DR et le LSA a été reçu d'un routeur autre que le routeur désigné de secours) le LSA sera rediffusé sur l'interface receveuse. Cette occurrence devrait être notée pour une utilisation ultérieure par le processus d'accusé de réception (paragraphe 13.5).

(c) Retirer la copie de la base de données actuelle des listes de retransmission d'état de liaison de tous les voisins.

(d) Installer le nouveau LSA dans la base de données d'état de liaison (en remplaçant la copie de la base de données actuelle). Cela peut causer une programmation du calcul du tableau d'acheminement. De plus, le nouveau LSA sera horodaté avec l'heure en cours (c'est-à-dire, l'heure de sa réception). La procédure d'arrosage ne peut pas subroger le LSA qui vient d'être installé jusqu'à ce que MinLSArrival secondes se soient écoulées. Le processus d'installation du LSA est exposé plus en détail au paragraphe 13.2.

(e) Accuser éventuellement réception du LSA en renvoyant un paquet d'accusé de réception d'état de liaison à l'interface receveuse. Ceci est expliqué au paragraphe 13.5.

(f) Si ce nouveau LSA indique qu'il a été généré par le routeur receveur lui-même (c'est-à-dire qu'il est considéré comme un LSA auto généré) le routeur doit prendre des mesures particulières, soit de mise à jour du LSA, soit dans certains cas de sa purge du domaine d'acheminement. Pour une description de la façon dont les LSA auto générés sont détectés et subséquemment traités, voir au paragraphe 13.4.

(6) Autrement, si il y a une instance du LSA sur la liste de demande d'état de liaison du voisin qui envoie, une erreur est survenue dans le processus d'échange de base de données. Dans ce cas, redémarrer le processus d'échange de base de données en générant l'événement de voisin BadLSReq pour le voisin qui envoie et arrêter le traitement du paquet Mise à jour d'état de liaison.

(7) Autrement, si le LSA reçu est la même instance que la copie de la base de données (c'est-à-dire qu'aucun des deux n'est plus récent) les deux étapes suivantes devraient être effectuées :

(a) Si le LSA figure sur la liste de retransmission d'état de liaison pour l'adjacence receveuse, le routeur lui-même attend un accusé de réception pour ce LSA. Le routeur devrait traiter le LSA reçu comme un accusé de réception en retirant le LSA de la liste de retransmission d'état de liaison. C'est ce qu'on appelle un "accusé de réception implicite". Son occurrence devrait être notée pour une utilisation ultérieure par le processus d'accusé de réception (paragraphe 13.5).

(b) Accuser éventuellement réception du LSA en renvoyant un paquet d'accusé de réception d'état de liaison à l'interface receveuse. Ceci est expliqué au paragraphe 13.5.

(8) Autrement, la copie de la base de données est plus récente. Si la copie de la base de données a son âge LS égal à MaxAge et son numéro de séquence LS égal à MaxSequenceNumber, éliminer simplement le LSA reçu sans en accuser réception. (Dans ce cas, le numéro de séquence LS du LSA revient au début, et le LSA MaxSequenceNumber doit être complètement purgé avant qu'aucune nouvelle instance de LSA puisse être introduite). Autrement, pour autant que la copie de la base de données n'ait pas été dans une mise à jour d'état de liaison dans les dernières MinLSArrival secondes, renvoyer la copie de la base de données au voisin qui l'a envoyée, encapsulée au sein d'un paquet Mise à jour d'état de liaison. Le paquet Mise à jour d'état de liaison devrait être envoyé directement au voisin. Ce faisant, ne pas mettre la copie de base de données du LSA sur la liste de retransmission d'état de liaison du voisin, et ne pas accuser réception de l'instance de LSA reçue (moins récente).

13.1 Détermination du plus récent LSA

Lorsqu'un routeur rencontre deux instances d'un LSA, il doit déterminer lequel est le plus récent. Ceci est survenu ci-dessus lors de la comparaison d'un LSA reçu à sa copie dans la base de données. Cette comparaison doit aussi être faite durant la procédure d'échange de base de données qui survient lors de la construction d'une adjacence.

Un LSA est identifié par son type LS, son identifiant d'état de liaison et son routeur annonceur. Pour deux instances du même LSA, les champs Numéro de séquence LS, Age LS, et Somme de contrôle LS sont utilisés pour déterminer quelle instance est plus récente :

o Le LSA qui a le numéro de séquence LS le plus nouveau est plus récent. Voir au paragraphe 12.1.6 une explication de l'espace des numéros de séquence LS. Si les deux instances ont le même numéro de séquence LS, alors :

o Si les deux instances ont des sommes de contrôle LS différentes, l'instance qui a la plus grande somme de contrôle LS (considérée comme un entier non signé de 16 bits) est alors considérée comme plus récente.

o Autrement, si une seule des instances a son champ Age LS réglé à MaxAge, l'instance d'âge MaxAge est considérée comme étant plus récente.

o Autrement, si les champs Age LS des deux instances diffèrent de plus de MaxAgeDiff, l'instance qui a le plus petit âge LS (plus jeune) est considérée comme la plus récente.

o Autrement, les deux instances sont considérées comme étant identiques.

13.2 Installation des LSA dans la base de données

L'installation d'un nouveau LSA dans la base de données, résultant soit d'un arrosage soit d'un LSA nouveau auto généré, peut causer le recalcul de la structure du tableau d'acheminement OSPF. Le contenu du nouveau LSA devrait être comparé à la vieille instance, si elle est présente. S'il n'y a pas de différence, il n'est pas nécessaire de recalculer le tableau d'acheminement. Lors de la comparaison d'un LSA à son instance précédente, tout de qui suit doit être considéré comme différence de contenu :

o Le champ Options du LSA a changé.
o Une des instances du LSA a son âge LS réglé à MaxAge, et pas l'autre.
o Le champ Longueur dans l'en-tête du LSA a changé.
o Le corps du LSA (c'est-à-dire, tout ce qui est en dehors des 20 octets d'en-tête du LSA) a changé. Noter que cela exclut les changements du numéro de séquence LS et de la somme de contrôle LS.

Si les contenus sont différents, les pièces suivantes du tableau d'acheminement doivent être recalculées, selon le champ Type LS du nouveau LSA :

LSA de routeur et LSA de réseau
Le tableau d'acheminement tout entier doit être recalculé, en commençant par les calculs du plus court chemin pour chaque zone (et pas seulement la zone dont la base de données d'états de liaisons a changé). La raison pour laquelle le calcul du plus court chemin ne peut pas se restreindre à la seule zone changée est en rapport avec le fait que les routeurs frontières de l'AS peuvent appartenir à plusieurs zones. Un changement dans la zone qui fournit actuellement le meilleur chemin peut forcer le routeur à utiliser un chemin intra-zone fourni par une zone différente.[19]

LSA de résumé
Le meilleur chemin pour la destination décrite par le LSA de résumé doit être recalculé (voir au paragraphe 16.5). Si cette destination est un routeur frontière de l'AS, il peut aussi être nécessaire de réexaminer tous les LSA externes à l'AS.

LSA externes à l'AS
Le meilleur chemin pour la destination décrit par le LSA externe à l'AS doit être recalculé (voir au paragraphe 16.6).

De plus, toute ancienne instance du LSA doit être retirée de la base de données lorsque le nouveau LSA est installé. Cette ancienne instance doit aussi être retirée de toutes les listes de retransmission d'état de liaison des voisins (voir Section 10).

---

19 En conservant plus d'informations dans le tableau d'acheminement, il est possible à une mise en œuvre de recalculer l'arbre des plus courts chemins pour une seule zone. En fait, il y a des algorithmes d'incrémentation qui permettent à une mise en œuvre de recalculer seulement une portion de l'arbre des plus courts chemins d'une seule zone [Ref1]. Cependant, ces algorithmes sortent du domaine d'application de la présente spécification.

13.3 Étape suivante de la procédure d'arrosage

Lorsqu'un nouveau LSA (plus récent) a été reçu, il doit être diffusé sur un certain ensemble d'interfaces du routeur. Ce paragraphe décrit la seconde partie de la procédure d'arrosage (la première partie étant le traitement qui intervenait à la Section 13) à savoir, de choisir les interfaces de sortie et d'ajouter le LSA aux listes de retransmission d'état de liaison des voisins appropriés. Est aussi incluse dans cette partie de la procédure d'arrosage la maintenance des listes de demande d'état de liaison des voisins.

Ce paragraphe s'applique également à la diffusion d'un LSA que le routeur vient juste de générer lui-même (voir au paragraphe12.4). Pour ces LSA, ce paragraphe donne la procédure d'arrosage complète (c'est-à-dire que le traitement de la Section 13 n'est pas effectué, car par exemple, le LSA n'a pas été reçu d'un voisin et n'a donc pas besoin d'être acquitté).

En fonction du type LS du LSA, le LSA peut être diffusé seulement sur certaines interfaces. Ces interfaces, définies par la suite, sont appelées les interfaces éligibles :
Les LSA externes à l'AS (LS Type = 5)
Les LSA externes à l'AS sont diffusés sur l'AS tout entier, à l'exception des zones de bout (voir au paragraphe 3.6). Les interfaces éligibles sont toutes les interfaces du routeur, à l'exclusion des liaisons virtuelles et des interfaces se rattachant aux zones de bout.
Tous les autres types LS
Tous les autres types sont spécifiques d'une seule zone (la zone A). Les interfaces éligibles sont toutes les interfaces qui se rattachent à la zone A. Si la zone A est le cœur de réseau, cela inclut toutes les liaisons virtuelles.

Les bases de données d'état de liaison doivent rester synchronisées sur toutes les adjacences associées aux interfaces éligibles ci-dessus. Ceci est accompli en exécutant les étapes suivantes sur chaque interface éligible. Il devrait être noté que cette procédure peut décider de ne pas diffuser un LSA sur une interface particulière, si il y a une forte probabilité que les voisins rattachés aient déjà reçu le LSA. Cependant, dans ces cas la procédure d'arrosage doit être absolument sûre que les voisins reçoivent finalement bien le LSA, de sorte que le LSA soit ajouté à chaque liste de retransmission d'état de liaison d'adjacence. Pour chaque interface éligible :

(1) Chacun des voisins rattaché à cette interface est examiné, pour déterminer si il doit recevoir le nouveau LSA. Les étapes suivantes sont exécutées pour chaque voisin :
   (a) Si le voisin est dans un état inférieur à Échange, il ne participe pas à la diffusion, et le prochain voisin devrait être examiné.
   (b) Autrement, si l'adjacence n'est pas encore pleine (l'état du voisin est Échange ou Loading), examiner la liste de demandes d'état de liaison associée à cette adjacence. Si il y a une instance du nouveau LSA sur la liste, cela indique que le routeur voisin a déjà une instance du LSA. Comparer le nouveau LSA à la copie du voisin :
      - Si le nouveau LSA est moins récent, examiner alors le prochain voisin.
      - Si les deux copies sont la même instance, supprimer alors le LSA de la liste de demande d'état de liaison, et examiner le voisin suivant.[20]
      - Autrement, le nouveau LSA est plus récent. Supprimer le LSA de la liste de demande d'état de liaison.
   (c) Si le nouveau LSA a été reçu de ce voisin, examiner le voisin suivant.
   (d) À ce moment, on n'est pas sûr que le voisin ait une instance à jour de ce nouveau LSA. Ajouter le nouveau LSA à la liste de retransmission d'état de liaison pour l'adjacence. Cela assure que la procédure d'arrosage est fiable ; le LSA sera retransmis périodiquement jusqu'à ce que soit vu un accusé de réception du voisin.

(2) Le routeur doit maintenant décider de diffuser ou non le nouveau LSA sur cette interface. Si à l'étape précédente, le LSA N'ÉTAIT PAS ajouté à une des listes de retransmission d'état de liaison, il n'est pas besoin de diffuser le LSA sur l'interface et la prochaine interface devrait être examinée.

(3) Si le nouveau LSA a été reçu sur cette interface, et s'il a été reçu du routeur désigné ou du routeur désigné de secours, il y a des chances que tous les voisins aient déjà reçu le LSA. Donc, on examine la prochaine interface.

(4) Si le nouveau LSA a été reçu sur cette interface, et si l'état de l'interface est Secours (c'est-à-dire que le routeur lui-même est le routeur désigné de secours) examiner l'interface suivante. Le routeur désigné effectuera la diffusion sur cette interface. Cependant, si le routeur désigné échoue, le routeur (c'est-à-dire, le routeur désigné de secours) achèvera la retransmission des mises à jour.

(5) Si cette étape est atteinte, le LSA doit être diffusé sur l'interface. Envoyer un paquet Mise à jour d'état de liaison (y compris le nouveau LSA en tant que contenu) sur l'interface. L'âge LS du LSA doit être incrémenté de InfTransDelay

20 C'est la façon dont la liste de demande d'état de liaison est vidée, qui cause éventuellement le passage de l'état du voisin à Full. Voir au paragraphe 10.9 pour des précisions.

(qui doit être > 0) lorsqu'il est copié dans le paquet Mise à jour d'état de liaison sortant (jusqu'à ce que le champ Age LS atteigne la valeur maximum de MaxAge).

Sur les réseaux de diffusion, les paquets Mise à jour d'état de liaison sont en diffusion groupée. L'adresse IP de destination spécifiée pour le paquet Mise à jour d'état de liaison dépend de l'état de l'interface. Si l'état de l'interface est DR ou Secours, l'adresse AllSPFRouters devrait être utilisée. Autrement, l'adresse AllDRouters devrait être utilisée.

Sur les réseaux qui ne sont pas en diffusion, des paquets Mise à jour d'état de liaison distincts doivent être envoyés, en envoi individuel, à chaque voisin adjacent (c'est-à-dire, ceux qui sont dans l'état Échange ou supérieur). Les adresses IP de destination pour ces paquets sont les adresses IP des voisins.

13.4 Réception de LSA auto générés

Il est fréquent qu'un routeur reçoive des LSA auto générés via la procédure d'arrosage. Un LSA auto généré est détecté lorsque 1) le routeur annonceur du LSA est égal au propre identifiant de routeur du routeur ou 2) le LSA est un LSA de réseau et son identifiant d'état de liaison est égal à une des propres adresses IP d'interface du routeur.

Cependant, si le LSA auto généré reçu est plus récent que la dernière instance que le routeur a généré en réalité, le routeur doit prendre des mesures particulières. La réception d'un tel LSA indique qu'il y a des LSA dans le domaine d'acheminement qui ont été générés par le routeur avant son dernier redémarrage. Dans la plupart des cas, le routeur doit alors avancer le numéro de séquence LS du LSA d'un après le numéro de séquence LS reçu, et générer une nouvelle instance du LSA.

Il peut se trouver que le routeur ne souhaite plus générer le LSA reçu. Parmi les exemples possibles on trouvera : 1) le LSA est un LSA de résumé ou un LSA externe à l'AS et le routeur n'a plus de chemin (annonçable) pour la destination, 2) le LSA est un LSA de réseau mais le routeur n'est plus routeur désigné pour le réseau ou 3) le LSA est un LSA de réseau dont l'identifiant d'état de liaison est une des propres adresses IP d'interface du routeur mais dont le routeur annonceur n'est pas égal au propre identifiant de routeur du routeur (ce dernier cas devrait être rare, et il indique que l'identifiant de routeur du routeur a changé depuis la génération du LSA). Dans tous ces cas, au lieu de mettre à jour le LSA, celui-ci devrait être purgé du domaine d'acheminement en incrémentant l'âge LS du LSA reçu jusqu'à MaxAge et en le rediffusant (voir au paragraphe 14.1).

13.5 Envoi de paquets d'accusé de réception d'état de liaison

Chaque LSA nouvellement reçu doit être acquitté. C'est normalement fait par l'envoi de paquets d'accusé de réception d'état de liaison. Cependant, l'acquittement peut aussi être accompli implicitement par l'envoi de paquets Mise à jour d'état de liaison (voir l'étape 7a de la Section 13).

De nombreux accusés de réception peuvent être groupés en un seul paquet d'accusé de réception d'état de liaison. Un tel paquet est renvoyé à l'interface qui a reçu les LSA. Le paquet peut être envoyé d'une des deux façons suivantes : retardé et envoyé à un intervalle déterminé par un temporisateur, ou envoyé directement à un voisin particulier. La stratégie d'acquittement utilisée dépend des circonstances qui entourent la réception du LSA.

L'envoi d'accusés de réception retardés réalise plusieurs choses : 1) cela facilite l'empaquetage de plusieurs accusés de réception en un seul paquet d'accusés de réception d'état de liaison, 2) cela permet à un seul paquet d'accusé de réception d'état de liaison d'indiquer les accusés de réception à plusieurs voisins en une seule fois (grâce à la diffusion groupée) et 3) cela rend aléatoire les paquets d'accusé de réception d'état de liaison envoyés par les divers routeurs rattachés à un réseau commun. L'intervalle fixé entre les transmissions retardées d'un routeur doit être court (moins que RxmtInterval) sinon il s'en suivra des retransmissions inutiles.

Les accusés de réception directs sont envoyés directement à un voisin particulier en réponse à la réception de LSA dupliqués. Les accusés de réception directs sont envoyés immédiatement lorsque le duplicata est reçu. Sur les réseaux multi accès, ces accusés de réception sont envoyés directement à l'adresse IP du voisin.

La procédure précise d'envoi de paquets d'accusé de réception d'état de liaison est décrite au Tableau 19. Les circonstances entourant la réception du LSA sont énumérées dans la colonne de gauche. L'action d'accusé de réception effectuée figure dans une des deux colonnes de droite. Cette action dépend de l'état de l'interface concernée ; les interfaces dans l'état Secours se comportent différemment des interfaces dans tous les autres états. Les accusés de réception retardés doivent être délivrés à tous les routeurs adjacents associés à l'interface. Sur les réseaux de diffusion, ceci est accompli par l'envoi de paquets d'accusé de réception d'état de liaison retardés en diffusion groupée.

Circonstances	Action prise dans l'état Secours	Dans les autres états
LSA rediffusé par l'interface de réception (voir Section 13, étape 5b).	Pas d'envoi d'accusé de réception.	Pas d'envoi d'accusé de réception.
LSA plus récent que la copie de la base de données, mais non rediffusée à l'interface de réception	Accusé de réception différé envoyé si l'annonce est reçue du routeur désigné, autrement ne rien faire	Accusé de réception différé envoyé
Le LSA est un duplicata, et a été traité comme accusé de réception implicite (voir Section 13, étape 7a).	Accusé de réception différé envoyé si l'annonce est reçue du routeur désigné, autrement ne rien faire	Pas d'envoi d'accusé de réception.
Le LSA est un duplicata, et n'a pas été traité comme accusé de réception implicite.	Accusé de réception direct envoyé.	Accusé de réception direct envoyé.
L'âge LS du LSA est égal à MaxAge, et il n'y a pas d'instance en cours du LSA dans la base de données d'état de liaison, et aucun des voisins du routeur n'est dans les états Échange ou Loading (voir Section 13, étape 4).	Accusé de réception direct envoyé.	Accusé de réception direct envoyé.

Tableau 19 : Envoi des accusés de réception d'état de liaison.

L'adresse IP de destination utilisée dépend de l'état de l'interface. Si l'état de l'interface est DR ou Secours, on utilise la destination AllSPFRouters. Dans tous les autres états, on utilise la destination AllDRouters. Sur les réseaux qui ne sont pas en diffusion, les paquets d'accusé de réception d'état de liaison différés doivent être envoyés individuellement séparément sur chaque adjacence (c'est-à-dire, aux voisins dont l'état est supérieur ou égal à Échange).

Le raisonnement qui sous-tend l'envoi des paquets ci-dessus en diffusion groupée est mieux expliqué par un exemple. Considérons la configuration de réseau décrite à la Figure 15. Supposons que RT4 a été élu routeur désigné, et RT3 comme routeur désigné de secours pour le réseau N3. Lorsque le routeur RT4 diffuse un nouveau LSA au réseau N3, il est reçu par les routeurs RT1, RT2, et RT3. Ces routeurs ne vont pas rediffuser le LSA sur le réseau N3, mais ils doivent quand même s'assurer que leurs bases de données d'états de liaisons restent synchronisées avec celles de leurs voisins adjacents. Aussi RT1, RT2, et RT4 attendent pour voir un accusé de réception provenant de RT3. De même, RT4 et RT3 attendent tous deux de voir un accusé de réception provenant de RT1 et RT2. Le meilleur choix est l'envoi des accusés de réception en diffusion groupée.

La raison pour laquelle la logique d'accusé de réception est légèrement différente pour les DR Secours est qu'ils se comportent différemment durant l'arrosage des LSA (voir au paragraphe 13.3, étape 4).

13.6 Retransmission des LSA

Les LSA en diffusion à partir d'une adjacence sont placés sur la liste de retransmission d'état de liaison de l'adjacence. Afin d'assurer la fiabilité de la diffusion, ces LSA sont retransmis jusqu'à ce qu'ils soient acquittés. L'intervalle entre les retransmissions est une valeur configurable interface par interface, RxmtInterval. Si elle est réglée à une valeur trop faible pour une interface, des retransmissions inutiles vont s'ensuivre. Si la valeur est réglée trop haut, la vitesse de diffusion peut être affectée, en termes de perte de paquets.

Plusieurs LSA retransmis peuvent tenir dans un seul paquet de mise à jour d'état de liaison. Lorsque les LSA sont à retransmettre, seul ceux qui tiennent dans un seul paquet Mise à jour d'état de liaison devrait être envoyés. Un autre paquet de retransmissions peut être envoyé chaque fois que des LSA sont acquittés, ou à la prochaine expiration du temporisateur de retransmissions.

Les paquets Mise à jour d'état de liaison qui portent des retransmissions sont toujours envoyés directement au voisin. Sur les réseaux multi accès, cela signifie que les retransmissions sont envoyées directement à l'adresse IP du voisin. Chaque âge LS de LSA doit être incrémenté de InfTransDelay (qui doit être > 0) lorsqu'il est copié dans le paquet Mise à jour d'état de liaison sortant (jusqu'à ce que le champ Age LS atteigne la valeur maximum de MaxAge).
Si un routeur adjacent a une défaillance, les retransmissions peuvent survenir jusqu'à ce que l'adjacence soit détruite par un protocole Hello d'OSPF. Lorsque l'adjacence est détruite, la liste de retransmission d'état de liaison est vidée.

13.7 Réception des accusés de réception des états de liaison

De nombreuses vérifications de cohérence ont été faites sur un paquet d'accusé de réception d'état de liaison reçu avant qu'il soit passé à la procédure d'arrosage. En particulier, il a été associé à un voisin particulier. Si ce voisin est dans un état inférieur à Échange, le paquet d'accusé de réception d'état de liaison est éliminé.

Autrement, pour chaque accusé de réception dans le paquet d'accusé de réception d'état de liaison, les étapes suivantes sont

effectuées :

- o Le LSA dont il est accusé réception a-t-il une instance sur la liste de retransmission d'état de liaison pour le voisin ? Sinon, examiner le prochain accusé de réception. Autrement :
- o Si l'accusé de réception est pour la même instance que celle contenue dans la liste, retirer l'élément de la liste et examiner l'accusé de réception suivant. Autrement :
- o Enregistrer l'accusé de réception douteux, et examiner le suivant.

14. Vieillissement de la base de données des états de liaison

Chaque LSA a un champ Age LS. L'âge LS est exprimé en secondes. Un champ Age LS de LSA est incrémenté lorsqu'il est contenu dans la base de données d'un routeur. Également, lorsqu'il est copié dans un paquet de mise à jour d'état de liaison pour arroser une interface particulière, l'âge LS du LSA est incrémenté de InfTransDelay.

Un âge LS de LSA n'est jamais incrémenté au delà de la valeur MaxAge. Les LSA qui ont l'âge MaxAge ne sont pas utilisés dans le calcul du tableau d'acheminement. Lorsqu'un routeur vieillit sa base de données d'état de liaison, l'âge LS d'un LSA peut atteindre MaxAge[21]. À ce moment, le routeur doit essayer d'éliminer le LSA du domaine d'acheminement. Cela est fait en rediffusant simplement le LSA de MaxAge comme s'il était un LSA nouvellement généré (voir au paragraphe 13.3).

Lors de la création d'une liste de résumés de base de données pour une adjacence nouvellement formée, tout LSA de MaxAge présent dans la base de données d'état de liaison est ajouté à la liste de retransmission d'état de liaison du voisin au lieu de la liste de résumés de base de données du voisin. Voir au paragraphe 10.3 pour des précisions.

Un LSA de MaxAge doit être immédiatement retiré de la base de données d'état de liaison du routeur aussitôt qu'à la fois a) il n'est plus contenu dans une liste de retransmission d'état de liaison voisine et b) qu'aucun voisin du routeur n'est dans l'état Échange ou Loading.

Lorsque, dans le processus de vieillissement de la base de données d'état de liaison, l'âge LS d'un LSA atteint un multiple de CheckAge, sa somme de contrôle LS devrait être vérifiée. Si la somme de contrôle LS est incorrecte, une erreur de programme ou de mémoire a été détectée, et au minimum, le routeur lui-même devrait être redémarré.

14.1 Vieillissement prématuré des LSA

Un LSA peut être purgé du domaine d'acheminement en réglant son âge LS à MaxAge, tout en laissant son numéro de séquence LS, et en rediffusant le LSA. Cette procédure suit le même cours que la purge d'un LSA dont l'âge LS a naturellement atteint la valeur MaxAge (voir la section 14). En particulier, le LSA de MaxAge est retiré de la base de données d'état de liaison du routeur aussitôt que : a) il n'est plus contenu dans une liste de retransmission d'état de liaison d'aucun voisin, et b) aucun des voisins du routeur n'est dans les états Échange ou Loading. On appelle "vieillissement prématuré" le réglage de l'âge LS d'un LSA à MaxAge.

Le vieillissement prématuré est utilisé lorsqu'il est temps pour un champ numéro de séquence d'un LSA auto généré de revenir à initialisation. À ce moment, l'instance de LSA en cours (qui a le numéro de séquence LS MaxSequenceNumber) doit être vieillie prématurément et purgée du domaine d'acheminement avant qu'une nouvelle instance avec un numéro de séquence égal à InitialSequenceNumber puisse être générée. Voir au paragraphe 12.1.6 des informations complémentaires.

Le vieillissement prématuré peut aussi être utilisé lorsque, par exemple, un des chemins externes précédemment annoncés du routeur n'est plus accessible. Dans ces circonstances, le routeur peut purger son LSA externe à l'AS du domaine d'acheminement via un vieillissement prématuré. Cette procédure est préférable à une autre, qui serait de générer un nouveau LSA pour la destination en spécifiant une métrique de LSInfinity. Le vieillissement prématuré est aussi utilisé lors de la réception inattendue de LSA auto générés durant la procédure d'arrosage (voir au paragraphe 13.4).

Un routeur ne peut vieillir prématurément que ses propres LSA auto générés. Le routeur peut ne pas vieillir prématurément les LSA qui ont été générés par d'autres routeurs. Un LSA est considéré comme auto généré lorsque soit 1) le routeur annonceur du LSA est égal au propre identifiant de routeur du routeur, soit 2) le LSA est un LSA de réseau et son identifiant d'état de liaison est égal à une des propres adresses IP d'interface du routeur.

---

21 Il devrait être assez rare qu'un âge LS d'un LSA atteigne MaxAge de cette façon. Normalement, le LSA sera remplacé par une instance plus récente avant de se périmer.

15. Liaisons virtuelles

La seule zone cœur de réseau (ID de zone = 0.0.0.0) ne peut pas être déconnectée, ou certaines zones du système autonome vont devenir inaccessibles. Pour établir/maintenir la connexité du cœur de réseau, des liaisons virtuelles peuvent être configurées à travers des zones non cœur de réseau. Les liaisons virtuelles servent à connecter physiquement des composants séparés du cœur de réseau. Les deux points d'extrémité d'une liaison virtuelle sont des routeurs frontière de zone. La liaison virtuelle doit être configurée dans les deux routeurs. Les informations de configuration dans chaque routeur comportent l'autre point d'extrémité virtuel (l'autre routeur frontière de zone), et la zone non cœur de réseau que les deux routeurs ont en commun (appelée la zone de transit). Les liaisons virtuelles ne peuvent pas être configurées à travers des zones de bout (voir au paragraphe 3.6).

La liaison virtuelle est traitée comme si il y avait un réseau point à point non numéroté appartenant au cœur de réseau et joignant les deux routeurs frontière de zone. On tente d'établir une adjacence sur la liaison virtuelle. Quand cette adjacence est établie, la liaison virtuelle est incluse dans les LSA de routeur de cœur de réseau, et les paquets OSPF appartenant à la zone cœur de réseau vont s'écouler sur l'adjacence. Une telle adjacence est appelée dans le présent document une "adjacence virtuelle".

Dans chaque routeur de point d'extrémité, le coût et la viabilité de la liaison virtuelle sont découverts en examinant l'entrée de tableau d'acheminement pour l'autre routeur de point d'extrémité. (La zone associée à l'entrée doit être la zone de transit configurée). C'est ce qu'on appelle l'entrée de tableau d'acheminement correspondante de la liaison virtuelle. L'événement InterfaceUp survient pour une liaison virtuelle lorsque son entrée de tableau d'acheminement correspondante devient accessible. À l'inverse, l'événement InterfaceDown survient lorsque son entrée de tableau d'acheminement devient injoignable. En d'autres termes, la viabilité de la liaison virtuelle est déterminée par l'existence d'un chemin intra-zone, à travers la zone de transit, entre les deux points d'extrémité. Noter qu'une liaison virtuelle dont le chemin sous-jacent a un coût supérieur à l'hexadécimal 0xffff (taille maximum d'un coût d'interface dans un LSA de routeur) devrait être considérée comme non opérationnelle (c'est-à-dire, traitée comme si le chemin n'existait pas).

Les autres détails concernant les liaisons virtuelles sont comme suit :

- Les LSA externes à l'AS ne sont JAMAIS diffusés sur des adjacences virtuelles. Ce serait une duplication d'efforts, car les mêmes LSA externes à l'AS sont déjà diffusés dans toute la zone de transit de la liaison virtuelle. Pour cette même raison, les LSA externes à l'AS ne sont pas résumés sur les adjacences virtuelles durant le processus d'échange de base de données.

- Le coût d'une liaison virtuelle N'EST PAS configuré. Il est défini comme le coût du chemin intra-zone entre les deux routeurs frontière de zone qui la définissent. Ce coût apparaît dans l'entrée de tableau d'acheminement correspondante de la liaison virtuelle. Lorsque le coût d'une liaison virtuelle change, un nouveau LSA de routeur devrait être généré pour la zone cœur de réseau.

- Juste comme le coût et la viabilité de la liaison virtuelle sont déterminés par le processus de construction du tableau d'acheminement (par la construction d'une entrée de tableau d'acheminement pour l'autre point d'extrémité) il en est de même de l'adresse IP d'interface pour l'interface virtuelle et l'adresse IP du voisin virtuel. Celles-ci sont utilisées lors de l'envoi des paquets de protocole OSPF sur la liaison virtuelle. Noter que lorsque un (ou les deux) des points d'extrémité de la liaison virtuelle se connecte à la zone de transit via une liaison point à point non numérotée, il peut être impossible de calculer l'adresse IP de l'interface virtuelle et/ou l'adresse IP du voisin virtuel, causant par là l'échec de la liaison virtuelle.

- Dans un LSA de routeur pour le cœur de réseau de chaque point d'extrémité, la liaison virtuelle est représentée comme une liaison de type 4 dont l'identifiant de liaison est réglé à l'identifiant de routeur OSPF du voisin virtuel et dont les données de liaison sont réglées à l'adresse IP de l'interface virtuelle. Voir au paragraphe 12.4.1 des informations complémentaires.

- Une zone non cœur de réseau peut porter du trafic de données de transit (c'est-à-dire, est considérée comme une "zone de transit") si et seulement si elle sert de zone de transit pour une ou plusieurs liaisons virtuelles pleinement adjacentes (voir TransitCapability aux paragraphes 6 et 16.1). Une telle zone requiert un traitement particulier lorsqu'elle comporte des réseaux cœur de réseau en elle (voir au paragraphe 12.4.3) et durant le calcul d'acheminement (voir au paragraphe 16.3).

- L'intervalle entre les retransmissions d'état de liaison, RxmtInterval, est configuré pour une liaison virtuelle. Ce devrait être bien au-delà du délai d'aller retour attendu entre les deux routeurs. Il peut être difficile à estimer pour une liaison virtuelle ; il ne faut pas avoir peur de prévoir trop grand.

16. Calcul du tableau d'acheminement

La présente section détaille le calcul du tableau d'acheminement OSPF. En utilisant la base de données d'état de liaisons de sa zone de rattachement comme entrée, un routeur fait fonctionner l'algorithme suivant, construisant son tableau d'acheminement pas à pas. À chaque étape, le routeur doit accéder aux éléments individuels de la base de données d'états de liaisons (par exemple, un LSA de routeur généré par un certain routeur). Cet accès est effectué par la fonction de recherche exposée au paragraphe 12.2. Le processus de recherche peut retourner un LSA dont l'âge LS est égal à MaxAge. Un tel LSA ne devrait pas être utilisé dans le calcul du tableau d'acheminement et est traité juste comme si le processus de recherche avait échoué. L'organisation du tableau d'acheminement OSPF est expliquée à la Section 11. Deux exemples du processus de construction du tableau d'acheminement sont présentés aux paragraphes 11.2 et 11.3. Ce processus peut être divisé selon les étapes suivantes :

(1) Le présent tableau d'acheminement est invalidé. Le tableau d'acheminement est reconstruit à partir de zéro. L'ancien tableau d'acheminement est sauvegardé de sorte que les changements d'entrées du tableau d'acheminement puissent être identifiés.

(2) Les chemins intra-zone sont calculés par la construction de l'arbre des plus courts chemins pour chaque zone de rattachement. En particulier, toutes les entrées de tableau d'acheminement dont le Type de destination est "routeur frontière de zone" sont calculées dans cette étape. Il est décrit en deux parties. D'abord, l'arbre est construit en ne considérant que les liaisons entre routeurs et réseaux de transit. Puis les réseaux d'extrémité sont incorporés à l'arbre. Durant le calcul de l'arbre des plus courts chemins de la zone, le TransitCapability de la zone est aussi calculé pour être utilisé à l'étape 4.

(3) Les chemins inter-zone sont calculés à travers l'examen des LSA de résumé. Si le routeur est rattaché à plusieurs zones (c'est-à-dire, si c'est un routeur frontière de zone) seuls les LSA de résumé de cœur de réseau sont examinés.

(4) Dans les routeurs frontières de zone qui se connectent à une ou plusieurs zones de transit (c'est-à-dire, les zones non cœur de réseau dont le TransitCapability se trouve être VRAI) les LSA de résumé des zones de transit sont examinés pour voir si de meilleurs chemins existent en utilisant les zones de transit qui ont été trouvées aux étapes 2-3 ci-dessus.

(5) Les chemins pour les destinations externes sont calculés par l'examen des LSA externes à l'AS. Les localisations des routeurs frontière de l'AS (qui génèrent les LSA externes à l'AS) ont été déterminées dans les étapes 2-4.

Les étapes 2-5 sont expliquées plus en détail ci-dessous.

Les changements apportés aux entrées de tableau d'acheminement par suite de ces calculs peuvent causer d'autres actions du protocole OSPF. Par exemple, un changement d'un chemin intra-zone sera cause qu'un routeur frontière de zone génère de nouveaux LSA de résumé (voir au paragraphe 12.4). Voir au paragraphe 16.7 une liste complète des actions du protocole OSPF résultant de changements du tableau d'acheminement.

16.1 Calcul de l'arbre des plus courts chemins pour une zone

Ce calcul donne l'ensemble des chemins intra-zone associés à une zone (appelée ci-après la zone A). Un routeur calcule l'arbre des plus courts chemins en s'utilisant lui-même comme racine[22]. La formation de l'arbre des plus courts chemins est faite ici en deux stades. Au premier stade, seules sont considérées les liaison entre routeurs et réseaux de transit. En utilisant l'algorithme de Dijkstra, on forme un arbre à partir de ce sous-ensemble de la base de données d'état de liaison. Au second stade, les feuilles sont ajoutées à l'arbre en considérant les liaisons aux réseaux d'extrémité.

La procédure sera expliquée en utilisant la terminologie de graphe qui a été introduite à la Section 2. La base de données d'état de liaison de la zone est représentée comme un graphe dirigé. Les vertex du graphe sont les routeurs, réseaux de transit et réseaux d'extrémité. Le premier stade de la procédure concerne seulement les vertex de transit (routeurs et réseaux de transit) et leurs liaisons de connexion. Tout au long du calcul du plus court chemin, les données suivantes sont aussi associées à chaque vertex de transit :

Identifiant de vertex (nœud)
: Nombre de 32 bits qui avec le type de vertex (routeur ou réseau) identifie de façon univoque le vertex. Pour les vertex de routeur l'identifiant de vertex est l'identifiant de routeur OSPF du routeur. Pour les vertex de réseau, c'est l'adresse IP du routeur désigné du réseau.

22 Strictement parlant, à cause des chemins multiples à coût égal, l'algorithme ne crée pas un arbre. On continue d'utiliser la terminologie "arbre" parce que c'est ce qui est fait le plus souvent dans la littérature existante.

Un LSA
Chaque vertex de transit a un LSA associé. Pour les vertex de routeur, c'est un LSA de routeur. Pour les réseaux de transit, c'est un LSA de réseau (qui est en fait généré par le routeur désigné du réseau). Dans tous les cas, l'identifiant d'état de liaison du LSA est toujours égal à l'identifiant de vertex ci-dessus.

Liste des prochains bonds
La liste des prochains bonds pour l'ensemble actuel des plus courts chemins depuis la racine jusqu'à ce vertex. Il peut y avoir plusieurs plus courts chemins du fait de la capacité de plusieurs chemins à coût égal. Chaque prochain bond indique l'interface de routeur sortante à utiliser lors de la transmission de trafic à la destination. Sur les réseaux de diffusion, en point à multipoint et NBMA, le prochain bond inclut aussi l'adresse IP du prochain routeur (s'il en est) sur le chemin vers la destination.

Distance à la racine
Coût de l'état de liaison de l'ensemble actuel de plus courts chemins de la racine au vertex. Le coût d'état de liaison d'un chemin est calculé comme la somme des coûts des liaisons constitutives du chemin (tels qu'annoncés dans les LSA de routeur et les LSA de réseau). Un chemin est dit être "plus court" qu'un autre si il a un coût d'état de liaison plus faible.

Le premier stade de la procédure (c'est-à-dire, l'algorithme de Dijkstra) peut maintenant être résumé comme suit. À chaque itération de l'algorithme, il y a une liste de vertex candidats. Les chemins de la racine à ces vertex ont été trouvés, mais pas nécessairement les plus courts. Cependant, le chemin du vertex candidat qui est le plus proche de la racine est à coup sûr le plus court ; ce vertex est ajouté à l'arbre des plus courts chemins, retiré de la liste des candidats, et ses vertex adjacents sont examinés pour un ajout/modification possible à la liste des candidats. L'itération de l'algorithme reprend. Elle se termine lorsque la liste des candidats devient vide.

Les étapes suivantes décrivent l'algorithme en détail. Rappelez vous que nous calculons l'arbre des plus courts chemins pour la zone A. Toutes les références à la recherche de base de données d'état de liaison ci-dessous sont à partir de la base de données de la zone A.

(1) Initialiser les structures de données de l'algorithme. Nettoyer la liste des vertex candidats. Initialiser l'arbre des plus courts chemins à partir de la seule racine (qui est le routeur qui fait le calcul). Régler le TransitCapability de la zone A à FAUX.

(2) Appelons le vertex qui vient d'être ajouté à l'arbre vertex V. Examiner le LSA associé au vertex V. C'est une recherche dans la base de données d'état de liaison de la zone A fondée sur l'identifiant de vertex. Si c'est un LSA de routeur, et si le bit V du LSA de routeur (voir au paragraphe A.4.2) est mis à 1, régler le TransitCapability de la zone A à VRAI. Dans tous les cas, chaque liaison décrite par le LSA donne le coût pour un vertex adjacent. Pour chaque liaison décrite, (disons qui joint le vertex V au vertex W) :

(a) Si c'est une liaison à un réseau de bout, examiner la liaison suivante dans le LSA de V. Les liaisons aux réseaux d'extrémité seront considérées dans le second stade du calcul du plus court chemin.

(b) Autrement, W est un vertex de transit (routeur ou réseau de transit). Chercher le LSA du vertex W (LSA de routeur ou LSA de réseau) dans la base de données d'état de liaison de la zone A. Si le LSA n'existe pas, ou si son âge LS est égal à MaxAge, ou s'il n'a pas une liaison retournant au vertex V, examiner la liaison suivante dans le LSA de V [23].

(c) Si le vertex W est déjà sur l'arbre des plus courts chemins, examiner la liaison suivante dans le LSA.

(d) Calculer le coût D d'état de la liaison du chemin résultant depuis la racine jusqu'au vertex W. D est égal à la somme du coût d'état du plus court chemin de la liaison (déjà calculé) jusqu'au vertex V et du coût annoncé de la liaison entre les vertex V et W. Si D est :

- Supérieur à la valeur qui apparaît déjà pour le vertex W sur la liste des candidats, examiner alors la liaison suivante.
- Égal à la valeur qui apparaît pour le vertex W sur la liste des candidats, calculer l'ensemble des prochains bonds qui résultent de l'utilisation de la liaison annoncée. Les entrées pour ce calcul sont la destination (W), et son parent (V). Ce calcul est montré au paragraphe 16.1.1. Cet ensemble de bonds devrait être ajouté aux valeurs des prochains bonds qui apparaissent pour W sur la liste des candidats.
- Inférieur à la valeur qui apparaît pour le vertex W sur la liste des candidats, ou si W n'apparaît pas encore sur la

23 Noter que la présence de n'importe quelle liaison de retour vers V est suffisante ; il n'est pas nécessaire que ce soit la moitié correspondante de liaison considérée de V à W. Cela suffit pour s'assurer que, avant que le trafic de données s'écoule entre une paire de routeurs voisins, leurs bases de données d'état de liaison seront synchronisées.

liste des candidats, régler alors l'entrée pour W sur la liste des candidats de façon à indiquer une distance de D de la racine. Calculer aussi la liste des prochains bonds qui résulte de l'utilisation de la liaison annoncée, en réglant les valeurs des prochains bonds pour W en conséquence. Le calcul du prochain bond est décrit au paragraphe 16.1.1 ; il prend en entrée la destination (W) et son parent (V).

(3) Si à cette étape la liste des candidats est vide, l'arbre des plus courts chemins (des vertex de transit) a été entièrement construit et cette étape de la procédure se termine. Autrement, choisir le vertex appartenant à la liste des candidats qui est le plus proche de la racine, et l'ajouter à l'arbre des plus courts chemins (et en le retirant de la liste des candidats). Noter que lorsqu'il y a un choix à faire parmi les vertex les plus proches de la racine, les vertex de réseau doivent être choisis avant les vertex de routeur afin de trouver nécessairement tous les chemins de coût égal. Ceci est cohérent avec les modes de résolution de conflit introduits dans l'algorithme Dijkstra modifié utilisé par les extensions d'acheminement en diffusion groupée d'OSPF (MOSPF, *OSPF Multicast routing extension*).

(4) Modifier éventuellement le tableau d'acheminement. Pour les entrées de tableau d'acheminement modifiées, la zone associée sera réglée à zone A, le type de chemin sera réglé à intra-zone, et le coût sera réglé à la distance calculée du plus court chemin qui vient d'être découvert.

Si le vertex qui vient d'être ajouté est un routeur frontière de zone ou un routeur frontière de l'AS, une entrée de tableau d'acheminement est ajoutée dont le type de destination est "routeur". Le champ Options trouvé dans le LSA de routeur associé est copié dans le champ Capacités facultatives de l'entrée de tableau d'acheminement. Appelons Routeur X le vertex qui vient d'être ajouté. Si le Routeur X est le point d'extrémité d'une des liaisons virtuelles du routeur qui fait le calcul, et si la liaison virtuelle utilise la zone A comme zone de transit : la liaison virtuelle est déclarée active, l'adresse IP de l'interface virtuelle est réglée à l'adresse IP de l'interface sortante calculée ci-dessus pour le Routeur X, et l'adresse IP du voisin virtuel est réglée à l'adresse d'interface du Routeur X (contenue dans le LSA de routeur du routeur X) qui repointe sur la racine de l'arbre des plus courts chemins ; de façon équivalente, c'est l'interface qui repointe sur le vertex parent du Routeur X sur l'arbre des plus courts chemins (semblable au calcul du paragraphe 16.1.1).

Si le vertex qui vient d'être ajouté est un réseau de transit, l'entrée de tableau d'acheminement pour le réseau est localisée. L'identifiant de destination de l'entrée est le numéro de réseau IP, qui peut être obtenu en appliquant à l'identifiant de vertex (identifiant d'état de liaison) le gabarit de son sous-réseau associé (qui se trouve dans le corps du LSA de réseau associé). Si l'entrée de tableau d'acheminement existe déjà (c'est-à-dire, s'il y a déjà un chemin intra-zone pour cette destination installé dans le tableau d'acheminement) plusieurs vertex sont transposés sur le même réseau IP. Par exemple, cela peut arriver quand un nouveau routeur désigné est en cours d'établissement. Dans ce cas, l'entrée actuelle du tableau d'acheminement ne devrait être subrogée que si et seulement si le chemin qui vient d'être trouvé est tout aussi court et si l'origine d'état de liaison de l'entrée actuelle de tableau d'acheminement a un plus petit identifiant d'état de liaison que le LSA du vertex qui vient d'être ajouté.

S'il n'y a pas d'entrée de tableau d'acheminement pour le réseau (le cas normal) une entrée de tableau d'acheminement pour le réseau IP devrait être ajoutée. L'origine d'état de liaison de l'entrée de tableau d'acheminement devrait être réglée au LSA du vertex qui vient d'être ajouté.

(5) Itérer l'algorithme en retournant à l'étape 2.

Les réseaux de bout sont ajoutés à l'arbre dans le second stade de la procédure. Dans ce stade, tous les vertex de routeur sont réexaminés. Ceux dont il a été déterminé qu'ils sont injoignables dans la première phase ci-dessus sont éliminés. Pour chaque vertex de routeur accessible (appelons le V) le LSA de routeur associé est trouvé dans la base de données d'état de liaison. Chaque liaison de réseau de bout qui apparaît dans le LSA est alors examinée, et on effectue les étapes suivantes :

(1) Calculer la distance D du réseau de bout depuis la racine. D est égal à la distance de la racine au vertex de routeur (calculée au stade 1) plus le coût annoncé de la liaison du réseau de bout. Comparer cette distance au meilleur coût actuel jusqu'au réseau de bout. Ceci est fait en cherchant l'entrée actuelle du tableau d'acheminement pour le réseau de bout. Si la distance D calculée est supérieure, aller examiner la liaison de réseau de bout suivante dans le LSA.

(2) Si cette étape est atteinte, l'entrée de tableau d'acheminement du réseau de bout doit être mise à jour. Calculer l'ensemble des prochains bonds qui résulteraient de l'utilisation de la liaison du réseau de bout. Ce calcul est indiqué au paragraphe 16.1.1 ; les entrées de ce calcul sont la destination (le réseau de bout) et le vertex parent (le vertex de routeur). Si la distance D est la même que le coût actuel du tableau d'acheminement, ajouter simplement cet ensemble de prochains bonds à la liste des prochains bonds de l'entrée de tableau d'acheminement. Dans ce cas, le tableau d'acheminement a déjà une Origine d'état de liaison. Si cette origine d'état de liaison est un LSA de routeur dont l'identifiant d'état de liaison est inférieur à l'identifiant de routeur de V, rétablir l'origine d'état de liaison du LSA de routeur de V.

Autrement D est inférieur au coût du tableau d'acheminement. Remplacer l'entrée actuelle de tableau d'acheminement en réglant le coût de l'entrée de tableau d'acheminement à D, et en réglant la liste des prochains bonds de l'entrée à l'ensemble qui vient d'être calculé. Régler l'origine d'état de liaison de l'entrée de tableau d'acheminement au LSA de routeur de V. Puis poursuivre l'examen de la liaison de réseau de bout suivante.

Pour toutes les entrées de tableau d'acheminement ajoutées/modifiées dans le second stade, la zone associée sera réglée à la zone A et le type de chemin sera réglé à intra-zone. Lorsque la liste des LSA de routeur joignables est épuisée, le second stade est terminé. À ce moment, tous les chemins intra-zone associés à la zone A ont été déterminés.

La spécification n'exige pas que la méthode des deux stades ci-dessus soit utilisée pour calculer l'arbre des plus courts chemins. Cependant, si un autre algorithme est utilisé, un arbre identique doit être produit. Pour cette raison, il est important de noter que les liaisons entre vertex de transit doivent être bidirectionnelles afin d'être incluses dans l'arbre ci-dessus. Il devrait aussi être mentionné que des algorithmes plus efficaces existent pour le calcul de l'arbre ; par exemple, l'algorithme SPF par incrémentation décrit dans [Ref1].

16.1.1 Calcul du prochain bond

Ce paragraphe explique comment calculer l'ensemble actuel des prochains bonds à utiliser pour une destination. Chaque prochain bond comporte l'interface sortante à utiliser pour la transmission des paquets pour la destination ainsi que l'adresse IP du routeur du prochain bond (s'il en est). Le calcul du prochain bond est invoqué chaque fois qu'un chemin plus court est découvert pour la destination. Cela peut arriver dans tout stade du calcul de l'arbre des plus courts chemins (voir au paragraphe 16.1). Dans le stade 1 du calcul de l'arbre des plus courts chemins, un chemin plus court est trouvé lorsque sa destination est ajoutée à la liste des candidats, ou lorsque l'entrée de la destination sur la liste des candidats est modifiée (étape 2d du stade 1). Dans le stade 2, un chemin plus court est découvert chaque fois que l'entrée de tableau d'acheminement de la destination est modifiée (étape 2 du stade 2).

L'ensemble des prochains bonds à utiliser pour la destination peut être recalculé plusieurs fois durant le calcul de l'arbre des plus courts chemins, lorsque des chemins de plus en plus courts sont découverts. À la fin, l'entrée de tableau d'acheminement de la destination va toujours refléter les prochains bonds résultant du ou des plus courts chemins absolus.

Les entrées du calcul du prochain bond sont a) la destination et b) son parent dans le plus court chemin actuel entre la racine (le routeur qui fait le calcul) et la destination. Le parent est toujours un vertex de transit (c'est-à-dire, toujours un routeur ou un réseau de transit).

Si il y a au moins un routeur intervenant dans le plus court chemin actuel entre la destination et la racine, la destination hérite simplement du parent l'ensemble des prochains bonds. Autrement, il y a deux cas. Dans le premier cas, le vertex parent est la racine (le routeur qui calcule lui-même). Cela signifie que la destination est soit un réseau directement connecté soit un routeur directement connecté. L'interface de sortie est dans ce cas simplement l'interface OSPF qui connecte au réseau/routeur de destination. Si la destination est un routeur qui se connecte sur le routeur qui fait le calcul via un réseau en point à multipoint, la ou les adresses IP du prochain bond vers la destination peuvent être déterminées en examinant le LSA de routeur de la destination : chaque liaison repointant sur le routeur qui fait le calcul et a un champ Données de liaison qui appartient au réseau en point à multipoint fournit une adresse IP de son routeur de prochain bond. Si la destination est un réseau directement connecté, ou un routeur qui se connecte au routeur qui fait le calcul via une interface point à point, aucune adresse IP de prochain bond n'est exigée. Si la destination est un routeur connecté au routeur qui fait le calcul via une liaison virtuelle, le réglage du prochain bond devrait être différé jusqu'au calcul du paragraphe 16.3.

Dans le second cas, le vertex parent est un réseau qui connecte directement le routeur qui fait le calcul au routeur de destination. La liste des prochains bonds est alors déterminée en examinant le LSA de routeur de la destination. Pour chaque liaison qui dans le LSA de routeur repointe sur le réseau parent, le champ Données de liaison de la liaison donne l'adresse IP d'un routeur de prochain bond. L'interface sortante à utiliser peut alors être déduite de l'adresse IP du prochain bond (ou elle peut être héritée du réseau parent).

16.2 Calcul des chemins inter-zones

Les chemins inter-zone sont calculés en examinant les LSA de résumé. Si le routeur a des rattachements actifs à plusieurs zones, seuls les LSA de résumé de cœur de réseau sont examinés. Les routeurs rattachés à une seule zone examinent les LSA de résumé de cette zone. Dans l'un et l'autre cas, les LSA de résumé examinés ci-dessous font tous partie de la base de données d'état de liaison d'une seule zone (appelons la zone A).

Les LSA de résumé sont générés par les routeurs frontières de zone. Chaque LSA de résumé dans la zone A est considéré tour à tour. Se rappeler que la destination décrite par un LSA de résumé est soit un réseau (LSA de résumé de type 3) soit un routeur frontière de l'AS (LSA de résumé de type 4). Pour chaque LSA de résumé :

(1) Si le coût spécifié par le LSA est LSInfinity, ou si l'âge LS du LSA est égal à MaxAge, examiner alors le LSA suivant.

(2) Si le LSA a été généré par le routeur calculateur lui-même, examiner le LSA suivant.

(3) Si c'est un LSA de résumé de type 3, et si la collection des destinations décrites par le LSA de résumé est égale à une des gammes d'adresses de zone configurées du routeur (voir au paragraphe 3.5) et si la gamme d'adresses de zone particulière est active, le LSA de résumé devrait alors être ignoré. "Active" signifie qu'il y a un ou plusieurs réseaux accessibles (par un chemin intra-zone) contenus dans la gamme de la zone.

(4) Autrement, appelons la destination décrite par le LSA N (pour les LSA de résumé de type 3, l'adresse de N est obtenue en appliquant le gabarit de réseau/sous-réseau contenu dans le corps du LSA à l'identifiant d'état de liaison du LSA) et la bordure de zone qui génère le LSA BR. Cherchons l'entrée de tableau d'acheminement pour BR qui a la zone A comme zone associée. Si une telle entrée n'existe pas pour le routeur BR (c'est-à-dire, BR est injoignable dans la zone A) ne rien faire de ce LSA et considérer le suivant sur la liste. Autrement, ce LSA décrit un chemin inter-zone pour la destination N, dont le coût est la distance à BR plus le coût spécifié dans le LSA. Appelons le coût de ce chemin inter-zone IAC.

(5) Ensuite, cherchons l'entrée de tableau d'acheminement pour la destination N. (Si N est un routeur frontière de l'AS, chercher l'entrée de tableau d'acheminement "routeur" associée à la zone A). S'il n'existe pas d'entrée pour N ou si le type de chemin de l'entrée est "externe type 1" ou "externe type 2", installer alors le chemin inter-zone pour N, avec la zone A comme zone associée, le coût IAC, le prochain bond égal à la liste des prochains bonds pour le routeur BR, et Routeur annonceur égal à BR.

(6) Autrement, si les chemins présents dans le tableau sont des chemins intra-zone, ne rien faire du LSA (les chemins intra-zone sont toujours préférés).

(7) Autrement, les chemins présents dans le tableau d'acheminement sont aussi des chemins inter-zone. Installer le nouveau chemin à travers BR si il est le moins cher, en se substituant aux chemins du tableau d'acheminement. Autrement, si le nouveau chemin a le même coût, l'ajouter à la liste des chemins qui apparaissent dans l'entrée du tableau d'acheminement.

16.3 Examen des LSA de résumé des zones de transit

Cette étape n'est effectuée que par les routeurs frontières de zone rattachés à une ou plusieurs zones non cœur de réseau qui sont capables de porter du trafic de transit (c'est-à-dire, des "zones de transit", ou les zones dont le paramètre TransitCapability a été réglé à VRAI à l'étape 2 de l'algorithme de Dijkstra (voir au paragraphe 16.1)).

L'objet du calcul ci-dessous est d'examiner les zones de transit pour voir si elles fournissent de meilleurs (plus courts) chemins que ceux précédemment calculés aux paragraphes 16.1 et 16.2. Tout chemin trouvé meilleur ou égal aux chemins précédemment découverts est installé dans le tableau d'acheminement.

Le calcul détermine aussi le ou les prochains bonds réels pour les destinations dont le prochain bond a été calculé comme une liaison virtuelle aux paragraphes 16.1 et 16.2. Après achèvement du calcul ci-dessous, tous les chemins calculés aux paragraphes 16.1 et 16.2 qui ont encore des prochains bonds virtuels devraient être éliminés.

Le calcul se déroule comme suit. Tous les LSA de résumé de zones de transit sont examinés tour à tour. Chacun de ces LSA de résumé décrit un chemin à travers une zone de transit A vers un réseau N (l'adresse de N est obtenue en appliquant le gabarit de réseau/sous-réseau contenu dans le corps du LSA à l'identifiant d'état de liaison du LSA) ou dans le cas d'un LSA de résumé de type 4, vers un routeur frontière de l'AS N. Supposons aussi que le LSA de résumé a été généré par un routeur frontière de zone BR.

(1) Si le coût annoncé par le LSA de résumé est LSInfinity, ou si l'âge LS du LSA et égal à MaxAge, examiner alors le LSA suivant.

(2) Si le LSA de résumé a été généré par le routeur calculateur lui-même, examiner le LSA suivant.

(3) Chercher l'entrée de tableau d'acheminement pour N. (Si N est un routeur frontière de l'AS, chercher l'entrée de

tableau d'acheminement "routeur" associée à la zone cœur de réseau). Si elle n'existe pas, ou si le type de chemin est autre que intra-zone ou inter-zone, ou si la zone associée à cette entrée de tableau d'acheminement n'est pas la zone cœur de réseau, examiner alors le LSA suivant. En d'autres termes, ce calcul met seulement à jour les chemins intra-zone de cœur de réseau trouvés au paragraphe 16.1 et les chemins inter-zone trouvés au paragraphe 16.2.

(4) Chercher l'entrée de tableau d'acheminement pour le routeur annonceur BR associé à la zone A. Si il est injoignable, examiner le LSA suivant. Autrement, le coût vers la destination N est la somme du coût dans l'entrée de tableau d'acheminement de la zone A de BR et du coût annoncé dans le LSA. Appelons ce coût IAC.

(5) Si ce coût est inférieur au coût survenant dans l'entrée de tableau d'acheminement de N, remplacer la liste des prochains bonds de N par celle utilisée pour BR, et régler le coût du tableau d'acheminement de N à IAC. Autrement, si IAC est le même que le coût actuel de N, ajouter la liste des prochains bonds de BR à la liste des prochains bonds de N. Dans tous les cas, la zone associée à l'entrée de tableau d'acheminement de N doit rester la zone cœur de réseau, et le type de chemin (intra-zone ou inter-zone) doit aussi rester le même.

Il est important de noter que le calcul ci-dessus ne rend jamais accessibles des destinations injoignables, mais trouve éventuellement de meilleurs chemins pour des destinations déjà accessibles. Le calcul installe tout meilleur coût trouvé dans l'entrée de tableau d'acheminement, à partir duquel il peut être réannoncé dans des LSA de résumé aux autres zones.

À titre d'exemple du calcul, considérons le système autonome décrit à la Figure 17. Il y a une seule zone non cœur de réseau (Zone 1) qui divise physiquement le cœur de réseau en deux parties distinctes. Pour maintenir la connexité du cœur de réseau, une liaison virtuelle a été configurée entre les routeurs RT1 et RT4. Sur la droite de la figure, le réseau N1 appartient au cœur de réseau. Les lignes en pointillés indiquent qu'il y a un chemin de cœur de réseau intra-zone bien plus court entre le routeur RT5 et le réseau N1 (coût 20) que celui entre le routeur RT4 et le réseau N1 (coût 100). Le routeur RT4 et le routeur RT5 vont tous deux injecter des LSA de résumé pour le réseau N1 dans la zone 1.

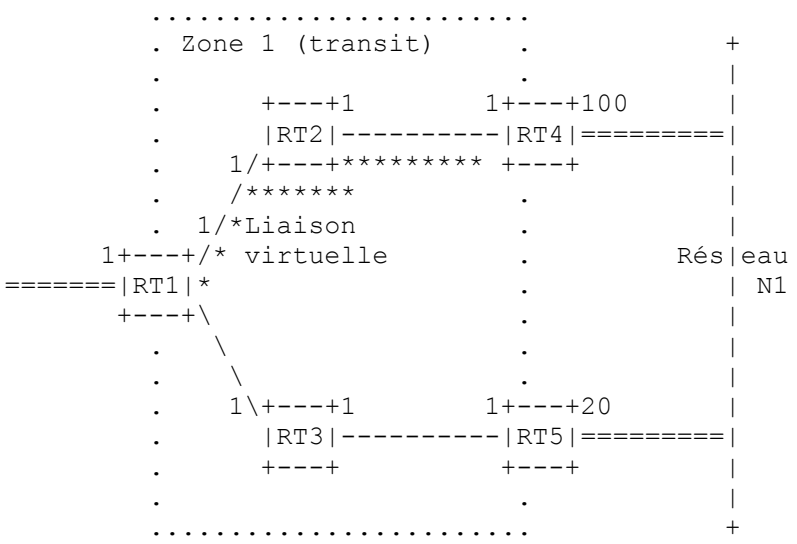


Figure 17 : Acheminement à travers des zones de transit

Après le calcul de l'arbre des plus courts chemins pour le cœur de réseau au paragraphe 16.1, le routeur RT1 (extrémité gauche de la liaison virtuelle) aura calculé un chemin à travers le routeur RT4 pour tout le trafic de données destiné au réseau N1. Cependant, comme le routeur RT5 est si proche du réseau N1, tous les routeurs internes à la zone 1 (par exemple, les routeurs RT2 et RT3) vont transmettre leur trafic de réseau N1 au routeur RT5, au lieu de RT4. Et bien sûr, après avoir examiné les LSA de résumé de la zone 1 par le calcul ci-dessus, le routeur RT1 transmettra aussi le trafic du réseau N1 vers RT5. Noter que dans cet exemple, la liaison virtuelle permet de transmettre le trafic de données de transit à travers la zone 1, mais le chemin réel du trafic de données de transit ne suit pas la liaison virtuelle. En d'autres termes, les liaisons virtuelles permettent de transmettre le trafic de transit à travers une zone, mais ne dictent pas le chemin précis que va emprunter le trafic.

16.4 Calcul des chemins externes à l'AS

Les chemins externes à l'AS sont calculés en examinant les LSA externes à l'AS. Chacun des LSA externes à l'AS est considéré tour à tour. La plupart des LSA externes à l'AS décrivent des chemins pour des destinations IP spécifiques. Un LSA externe à l'AS peut aussi décrire un chemin par défaut pour le système autonome (Destination ID = DefaultDestination, gabarit de réseau/sous-réseau = 0x00000000). Pour chaque LSA externe à l'AS :

(1) Si le coût spécifié par le LSA est LSInfinity, ou si l'âge LS du LSA est égal à MaxAge, examiner le LSA suivant.

(2) Si le LSA a été généré par le routeur calculateur lui-même, examiner le LSA suivant.

(3) Appeler la destination décrite par le LSA N. L'adresse de N est obtenue en appliquant à l'identifiant d'état de liaison du LSA le gabarit de réseau/sous-réseau contenu dans le corps du LSA. Chercher les entrées de tableau d'acheminement (potentiellement une par zone rattachée) pour le routeur frontière de l'AS (ASBR, *AS Boundary Router*) qui a généré le LSA. S'il n'existe pas d'entrée pour le routeur ASBR (c'est-à-dire, l'ASBR est injoignable), ne rien faire du LSA et considérer le suivant de la liste.
Autrement, ce LSA décrit un chemin externe à l'AS pour la destination N. Examiner l'adresse de transmission spécifiée dans le LSA externe à l'AS. Cela indique l'adresse IP à laquelle devraient être transmis les paquets pour la destination.
Si l'adresse de transmission est réglée à 0.0.0.0, les paquets devraient être envoyés à l'ASBR lui-même. Parmi les diverses entrées de tableau d'acheminement pour l'ASBR, choisir l'entrée préférée comme suit. Si RFC1583Compatibility est réglé à "désactivé", élaguer l'ensemble des entrées de tableau d'acheminement pour l'ASBR comme décrit au paragraphe 16.4.1. Dans tous les cas, parmi les entrées de tableau d'acheminement restantes, choisir l'entrée de tableau d'acheminement qui a le moindre coût ; lorsqu'il y a plusieurs entrées de tableau d'acheminement à moindre coût, est choisie l'entrée dont la zone associée a le plus gros identifiant de zone OSPF (considéré comme entier non signé de 32 bits).

Si l'adresse de transmission est différente de zéro, chercher l'adresse de transmission dans le tableau d'acheminement [24]. L'entrée de tableau d'acheminement correspondante doit spécifier un chemin intra-zone ou inter-zone ; s'il n'existe pas de tel chemin, ne rien faire du LSA et considérer le suivant de la liste.

(4) Soit X le coût spécifié par l'entrée de tableau d'acheminement préférée pour l'ASBR/adresse de transmission, et Y le coût spécifié dans le LSA. X est en termes de métrique d'état de liaison, et Y est une métrique externe de type 1 ou 2.

(5) Chercher l'entrée de tableau d'acheminement pour la destination N. Si aucune entrée n'existe pour N, installer le chemin externe à l'AS vers N, avec le prochain bond égal à la liste des prochains bonds pour l'adresse de transmission, et le routeur annonceur égal à l'ASBR. Si le type de métrique externe est 1, le type de chemin est alors réglé au type 1 externe et le coût est égal à X+Y. Si le type de métrique externe est 2, le type de chemin est réglé à type 2 externe, le composant d'état de liaison du coût du chemin est X, et le coût de type 2 est Y.

(6) Comparer le chemin externe à l'AS décrit par le LSA aux chemins existants dans l'entrée de tableau d'acheminement de N comme suit. Si le nouveau chemin est préféré, il remplace les chemins actuels dans l'entrée de tableau d'acheminement de N. Si le nouveau chemin est de préférence égale, il est ajouté à la liste des chemins de l'entrée de tableau d'acheminement de N.
   (a) Les chemins intra-zone et inter-zone sont toujours préférés aux chemins externes à l'AS.
   (b) Les chemins externes de type 1 sont toujours préférés aux chemins externes de type 2. Quand tous les chemins sont des chemins externes de type 2, les chemins avec la plus petite métrique de type 2 annoncée sont toujours préférés.
   (c) Si le nouveau chemin externe à l'AS est toujours indiscernable des chemins actuels dans l'entrée de tableau d'acheminement de N, et si RFC1583Compatibility est réglé à "désactivé", choisir les chemins préférés sur la base des chemins intra-AS pour les ASBR/adresses de transmission, comme spécifié au paragraphe 16.4.1.
   (d) Si le nouveau chemin externe à l'AS est toujours indiscernable des chemins actuels dans l'entrée de tableau d'acheminement de N, choisir le chemin préféré sur la base de la comparaison des moindres coûts. Les chemins externes de type 1 sont comparés en regardant la somme de la distance à l'adresse de transmission et de la métrique de type 1 (X+Y) annoncée. Les chemins externes de type 2 qui annoncent des métriques égales de type 2 sont comparés en regardant la distance aux adresses de transmission.

16.4.1 Préférences de chemin externe

Lorsque plusieurs chemins intra AS sont disponibles vers des ASBR/adresses de transmission, les règles suivantes

24 Lorsque l'adresse de transmission est différente de zéro, elle devrait pointer sur un routeur appartenant à un autre système autonome. Voir au paragraphe 12.4.4 pour des précisions.

indiquent quels chemins sont préférés. Ces règles s'appliquent lorsque le même ASBR est accessible à travers plusieurs zones, ou pour essayer de décider parmi plusieurs LSA externes à l'AS lequel devrait être préféré. Dans le premier cas, les chemins se terminent tous au même ASBR, alors que dans le dernier, les chemins se terminent à des ASBR/adresses de transmission distinctes. Dans l'un et l'autre cas, chaque chemin est représenté par une entrée de tableau d'acheminement distincte, comme défini Section 11.

Ce paragraphe ne s'applique que quand RFC1583Compatibility est réglé à "désactivé".

Les règles de préférence de chemin, établies de la plus grande préférence à la moindre, sont les suivantes. Noter que par suite de ces règles, il peut encore y avoir plusieurs chemins de la plus haute préférence. Dans ce cas, le chemin à utiliser doit être déterminé sur la base du coût, comme décrit au paragraphe 16.4.

- Les chemins intra-zone qui utilisent des zones non cœur de réseau sont toujours préférés.
- Les autres chemins intra-zone cœur de réseau et inter-zones, sont de préférence égale.

16.5 Mises à jour incrémentaires – LSA de résumé

Lorsqu'un nouveau LSA de résumé est reçu, il n'est pas nécessaire de recalculer le tableau d'acheminement entier. Appelons N la destination décrite par le LSA de résumé (l'adresse de N est obtenue en appliquant à l'identifiant d'état de liaison de N le gabarit de réseau/sous-réseau contenu dans le corps du LSA), et soit la zone A la zone à laquelle appartient le LSA. Il y a maintenant deux cas distincts :

Cas 1 : la zone A est le cœur de réseau et/ou le routeur n'est pas un routeur frontière de zone.
Dans ce cas, on doit effectuer les calculs suivants. D'abord, si il y a actuellement un chemin inter-zone pour la destination N, l'entrée de tableau d'acheminement de N est invalidée, en sauvegardant les valeurs de l'entrée pour des comparaisons ultérieures. Ensuite on refait le calcul du paragraphe 16.2 pour la seule destination N. Dans ce calcul, tous les LSA de résumé de la zone A qui décrivent un chemin pour N sont examinés. De plus, si le routeur est un routeur frontière de zone rattaché à une ou plusieurs zones de transit, le calcul du paragraphe 16.3 doit être refait pour cette seule destination. Si le résultat de ces calculs a changé le coût/chemin pour un routeur frontière de l'AS (comme ce serait le cas pour un LSA de résumé de type 4) ou pour toute adresse de transmission, tous les LSA externes à l'AS devront être réexaminés en refaisant le calcul du paragraphe 16.4. Autrement, si N est maintenant devenu inaccessible, le calcul du paragraphe 16.4 doit être refait pour cette seule destination N, au cas où existe un chemin externe de remplacement pour N.

Cas 2 : la zone A est une zone de transit et le routeur est un routeur frontière de zone.
Dans ce cas, on doit effectuer les calculs suivants. D'abord, si l'entrée de tableau d'acheminement de N contient présentement un ou plusieurs chemins inter-zone qui utilisent en zone de transit la zone A, ces chemins devraient être retirés. Si cela retire tous les chemins de l'entrée du tableau d'acheminement, l'entrée devrait être invalidée. Les vieilles valeurs de l'entrée devraient être sauvegardées pour des comparaisons ultérieures. Ensuite, le calcul du paragraphe 16.3 doit être refait pour la seule destination N. Si le résultat de ce calcul a causé l'augmentation du coût pour N, le calcul complet du tableau d'acheminement doit être refait en partant de l'algorithme de Dijkstra spécifié au paragraphe 16.1. Autrement, si a changé le coût/chemin pour un routeur frontière de l'AS (comme ce serait le cas pour un LSA de résumé de type 4) ou pour toutes adresses de transmission, tous les LSA externes à l'AS devront être réexaminés en refaisant le calcul du paragraphe 16.4. Autrement, si N est maintenant devenu inaccessible, le calcul du paragraphe 16.4 doit être refait pour cette seule destination N, au cas où existe un chemin externe de remplacement pour N.

16.6 Mises à jour incrémentaires – LSA externes à l'AS

Lorsque un nouveau LSA externe à l'AS est reçu, il n'est pas nécessaire de recalculer le tableau d'acheminement entier. Appelons N la destination décrite par le LSA externe à l'AS. L'adresse de N est obtenue en appliquant à l'identifiant d'état de liaison du LSA le gabarit de réseau/sous-réseau contenu dans le corps du LSA. Si il y a déjà un chemin intra-zone ou inter-zone pour la destination, aucun recalcul n'est nécessaire (les chemins internes ont la préséance).

Autrement, il faudra effectuer la procédure du paragraphe 16.4, mais seulement pour les LSA externes à l'AS dont la destination est N. Avant d'effectuer cette procédure, la présente entrée du tableau d'acheminement pour N devrait être invalidée.

16.7 Événements générés par suite de changements du tableau d'acheminement

Les changements aux entrées de tableau d'acheminement causent parfois des actions supplémentaires pour les routeurs OSPF frontières de zone. Ces routeurs doivent agir sur les changements suivants du tableau d'acheminement :

o Le type de coût ou de chemin d'une entrée de tableau d'acheminement a changé. Si la destination décrite par cette entrée est un réseau ou routeur frontière de l'AS, et si ce n'est pas simplement un changement de chemins externes à l'AS, de nouveaux LSA de résumé peuvent devoir être générés (potentiellement un pour chaque zone de rattachement, y compris le cœur de réseau). Voir au paragraphe 12.4.3 des informations complémentaires. Si une entrée précédemment annoncée a été supprimée, ou n'est plus annonçable pour une zone particulière, le LSA doit être purgé du domaine d'acheminement en réglant son âge LS à MaxAge et rediffusé (voir au paragraphe 14.1).

o Une entrée de tableau d'acheminement associée à une liaison virtuelle configurée a changée. La destination d'une telle entrée de tableau d'acheminement est un routeur frontière de zone. Le changement indique une modification du coût ou de la viabilité de la liaison virtuelle.

Si l'entrée indique que le routeur frontière de zone est nouvellement accessible, la liaison virtuelle correspondante est maintenant opérationnelle. Un événement InterfaceUp devrait être généré pour la liaison virtuelle, ce qui va causer le commencement de la formation d'une adjacence virtuelle (voir au paragraphe 10.3). À ce moment, l'adresse IP d'interface de la liaison virtuelle et l'adresse IP de voisin du voisin virtuel sont aussi calculées.

Si l'entrée indique que le routeur frontière de zone n'est plus accessible, la liaison virtuelle et son adjacence associée devraient être détruites. Cela signifie qu'un événement InterfaceDown devrait être généré pour la liaison virtuelle associée.

Si le coût de l'entrée a changé, et si il y a une adjacence virtuelle pleinement établie, un nouveau LSA de routeur doit être généré pour le cœur de réseau. Cela peut à son tour causer d'autres changements au tableau d'acheminement.

16.8 Chemins à coût égal

Le protocole OSPF maintient plusieurs chemins à coût égal pour toutes les destinations. Cela peut se voir dans les étapes utilisées ci-dessus pour calculer le tableau d'acheminement, et dans la définition de la structure du tableau d'acheminement.

Chacun des divers chemins sera du même type (intra-zone, inter-zone, externe type 1 ou externe type 2) du même coût, et aura la même zone associée. Cependant, chaque chemin peut spécifier un prochain bond et un routeur annonceur distinct.

Il n'est pas exigé qu'un routeur fonctionnant avec OSPF garde trace de tous les chemins à coût égal possibles pour une destination. Une mise en œuvre peut choisir de ne garder trace que d'un nombre fixé de chemins pour toute destination donnée. Cela n'affecte aucun des algorithmes présentés dans la présente spécification.

Références

[Ref1] J. McQuillan, I. Richer et E. Rosen, "ARPANET Routing Algorithm Improvements", Rapport technique BBN, avril 1978.

[Ref2] Digital Equipment Corporation, "Information processing systems -- Data communications -- Intermediate System to Intermediate System Intra-Domain Routing Protocol", octobre 1987.

[Ref3] J. McQuillan et al., "The New Routing Algorithm for the ARPANET", IEEE Transactions on Communications, mai 1980.

[Ref4] R. Perlman, "Fault-Tolerant Broadcast of Routing Information", Computer Networks, décembre 1983.

[Ref5] J. Postel, éd., "Protocole Internet - Spécification du protocole du programme Internet ", RFC0791 , STD 5, septembre 1981.

[Ref6] Organisation internationale de normalisation, "Spécification du protocole de transport ISO - ISO DP 8073", RFC0905 , avril 1984.

[Ref7] S. Deering, "Extension d'hôte pour la diffusion groupée sur IP", STD 5, RFC1112 , mai 1988. *(Obsolète, voir RFC3376)*

[Ref8] K. McCloghrie et M. Rose, "Base de données d'informations de gestion pour la gestion de réseau des internets fondés sur TCP/IP : MIB-II", RFC1213 , STD 17, mars 1991.

[Ref9] J. Moy, "OSPF version 2", RFC1583, mars 1994. *(Rendue obsolète par la RFC 2178)*

[Ref10] V. Fuller, T. Li, J. Yu et K. Varadhan, "Acheminement inter domaine sans classe (CIDR) : stratégie d'allocation et d'agrégation d'adresses", RFC1519 , septembre 1993. *(D.S., rendue obsolète par la RFC4632)*

[Ref11] J. Reynolds et J. Postel, "Numéros alloués", RFC1700 , STD 2, octobre 1994. *(Historique, voir www.iana.org)*

[Ref12] P. Almquist, "Type de service dans la suite de protocole Internet", RFC1349 , juillet 1992. *(Remplacée par 2474)*

[Ref13] B. Leiner et.al., "The DARPA Internet Protocol Suite", DDN Protocol Handbook, avril 1985.

[Ref14] T. Bradley et C. Brown, "Protocole de résolution inverse d'adresse", RFC1293 , janvier 1992. *(Remplacée par 2390)*

[Ref15] O. deSouza et M. Rodrigues, "Lignes directrices pour OSPF sur les réseaux en relais de trame", RFC1586 , mars 1994. *(Information)*

[Ref16] S. Bellovin, "Problèmes de sécurité dans la suite des protocoles TCP/IP", ACM Computer Communications Review, Volume 19, numéro 2, pp. 32-38, avril 1989.

[Ref17] R. Rivest, "Algorithme de résumé de message MD5", RFC1321, avril 1992. *(Information)*

[Ref18] J. Moy, "Extensions de diffusion groupée à OSPF", RFC1584 , mars 1994. *(Historique, remplacée par RFC 5110)*

[Ref19] R. Coltun et V. Fuller, "L'option NSSA OSPF", RFC1587 , mars 1994. *(P.S., remplacée par RFC 3101)*

[Ref20] D. Ferguson, "LSA d'attribut externe dans OSPF", (*non publiée comme RFC*)

[Ref21] J. Moy, "Extension d'OSPF pour la prise en charge des circuits de demande", RFC1793 , avril 1995. *(Mise à jour par la RFC 3883)*

[Ref22] J. Mogul et S. Deering, "Découverte de la MTU de chemin", RFC1191 , novembre 1990.

[Ref23] Y. Rekhter et T. Li, "Protocole de routeur frontière 4 (BGP- 4)", RFC1771 , mars 1995. (*Obsolète, voir RFC4271)*

[Ref24] R. Hinden, "Critères de normalisation d'un protocole d'acheminement Internet", BBN, octobre 1991.

[Ref25] J. Moy, "OSPF version 2", RFC2178, juillet 1997. *(Rendue obsolète par la présente RFC)*

[Ref26] E. Rosen, "Vulnerabilities of Network Control Protocols: An Example", Computer Communication Review, juillet 1981.

Appendice A. Formats de données OSPF

Le présent appendice décrit les formats des paquets de protocole OSPF et des LSA OSPF. Le protocole OSPF fonctionne directement sur la couche réseau IP. Avant de décrire les formats de données, on explique les détails de l'encapsulation OSPF.

Ensuite sont décrits les champs Options OSPF. Ce champ décrit les diverses capacités qui peuvent être ou non prises en charge par des parties du domaine d'acheminement OSPF. Le champ Options OSPF est contenu dans les paquets Hello d'OSPF, dans les paquets de description de base de données et dans les LSA OSPF.

Les formats de paquet OSPF sont détaillés au paragraphe A.3. La description des LSA d'OSPF figure au paragraphe A.4.

A.1 Encapsulation des paquets OSPF

OSPF fonctionne directement sur la couche réseau du protocole Internet. Les paquets OSPF sont donc uniquement

encapsulés par IP et les en-têtes locaux de liaison des données.

OSPF ne définit pas de moyen pour fragmenter ses paquets de protocole, et dépend de la fragmentation IP lors de la transmission de paquets plus gros que la MTU du réseau. Si nécessaire, la longueur des paquets OSPF peut aller jusqu'à 65 535 octets (y compris l'en-tête IP). Les types de paquet OSPF qui vont vraisemblablement être grands (paquets de description de base de données, de demande d'état de liaison, de mise à jour d'état de liaison, et d'accusé de réception d'état de liaison) peuvent normalement être partagés en plusieurs paquets de protocole séparés, sans perte de fonctionnalités. Voici une recommandation : la fragmentation IP devrait être évitée chaque fois que possible. En utilisant ce raisonnement, on devrait tenter de limiter la taille des paquets OSPF envoyés sur les liaisons virtuelles à 576 octets si on n'a pas effectué de découverte de la MTU du chemin (voir [Ref22]).

Les autres caractéristiques importantes de l'encapsulation IP d'OSPF sont :

o Utilisation de la diffusion groupée IP. Certains messages OSPF sont en diffusion groupée, lorsqu'ils sont envoyés sur des réseaux de diffusion. Deux adresses de diffusion groupée IP distinctes sont utilisées. Les paquets envoyés à ces adresses de diffusion groupée ne devraient jamais être retransmis ; ils sont destinés à ne faire qu'un seul bond. Pour s'assurer que ces paquets ne vont pas voyager sur plusieurs bonds, leur TTL IP doit être réglé à 1.

  AllSPFRouters
  La valeur 224.0.0.5 a été allouée à cette adresse de diffusion groupée. Tous les routeurs qui fonctionnent avec OSPF devraient être prêts à recevoir des paquets envoyés à cette adresse. Les paquets Hello sont toujours envoyés à cette destination. De plus, certains paquets de protocole OSPF sont envoyés à cette adresse durant la procédure d'arrosage.

  AllDRouters
  La valeur 224.0.0.6 a été allouée à cette adresse de diffusion groupée. Le routeur désigné et le routeur désigné de secours doivent tous deux être prêts à recevoir des paquets destinés à cette adresse. Certains paquets de protocole OSPF sont envoyés à cette adresse durant la procédure d'arrosage.

o OSPF a le numéro de protocole IP 89. Ce numéro a été enregistré auprès du Centre des informations du réseau. Les allocations de numéro de protocole IP sont publiées dans le document [Ref11].

o Tous les paquets du protocole d'acheminement OSPF sont envoyés en utilisant la valeur de TOS de service normal de 0000 binaire définie dans [Ref12].

o Les paquets de protocole d'acheminement sont envoyés avec la préséance IP réglée à Contrôle inter-réseaux. Les paquets de protocole OSPF devraient recevoir la préséance sur le trafic IP de données régulier, à la fois en émission et en réception. Régler le champ Préséance IP dans l'en-tête IP à Contrôle inter-réseaux [Ref5] peut aider à mettre en œuvre cet objectif.

A.2 Champ Options

Le champ OSPF Options est présent dans les paquets Hello OSPF, dans les paquets de description de base de données et dans tous les LSA. Le champ Options permet aux routeurs OSPF de prendre (ou non) en charge (les capacités facultatives, et de communiquer leur niveau de capacité aux autres routeurs OSPF. Grâce à ce mécanisme, des routeurs de capacités différentes peuvent être mélangés au sein d'un domaine d'acheminement OSPF.

Lorsqu'il est utilisé dans un paquet Hello, le champ Options permet à un routeur de rejeter un voisin à cause d'une discordance de capacités. Autrement, lorsque les capacités sont échangées dans des paquets de description de base de données, un routeur peut choisir de ne pas transmettre certains LSA à un voisin à cause des ses fonctionnalités réduites. Enfin, faire la liste des capacités dans les LSA permet aux routeurs de transmettre du trafic à des routeurs à fonctionnalités réduites, en les excluant de certaines parties du calcul du tableau d'acheminement.

Cinq bits du champ Options OSPF ont été alloués, quoique un seul (le bit E) soit entièrement décrit dans le présent mémoire. Chaque bit est décrit brièvement ci-dessous. Les routeurs devraient éliminer les bits non reconnus dans le champ Options lors de l'envoi de paquets Hello ou de paquets de description de base de données et lorsqu'ils génèrent des LSA. À l'inverse, les routeurs qui rencontrent des bits Option non reconnus dans les paquets Hello, dans les paquets de description de base de données ou dans les LSA qu'ils reçoivent devraient ignorer la capacité et traiter normalement le paquet/LSA.

*	*	DC	EA	N/P	MC	E	*

Le champ Options

bit E
Ce bit décrit la façon dont les LSA externes à l'AS sont diffusés, comme décrit aux paragraphes 3.6, 9.5, 10.8 et 12.1.2 du présent mémoire.

bit MC
Ce bit décrit si les datagrammes IP en diffusion groupée sont transmis conformément aux spécifications de [Ref18].

bit N/P
Ce bit décrit le traitement des LSA de type-7, comme spécifié dans [Ref19].

bit EA
Ce bit décrit la volonté du routeur de recevoir et transmettre des LSA d'attributs externes, comme spécifié dans [Ref20].

bit DC
Ce bit décrit la façon dont le routeur traite les circuits de demande, comme spécifié dans [Ref21].

A.3 Formats de paquet OSPF

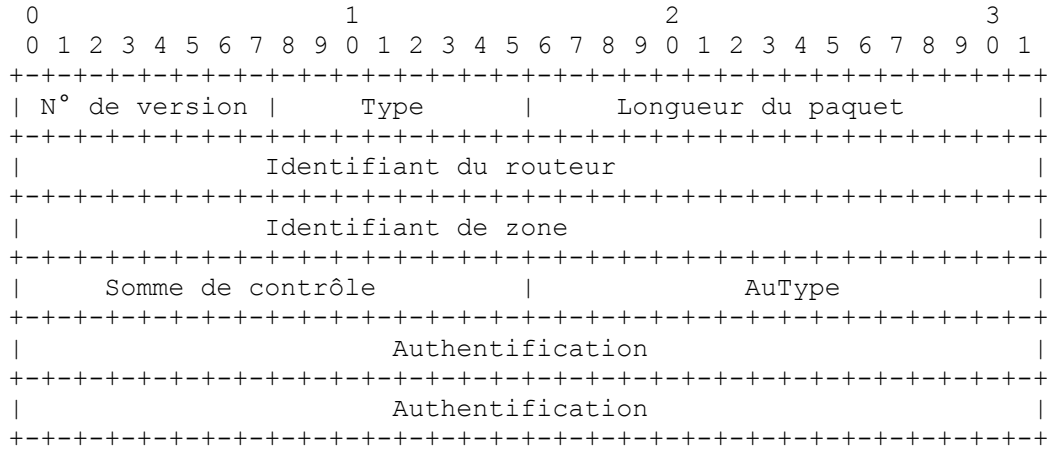
Il y a cinq types distincts de paquet OSPF. Tous les types de paquet OSPF commencent par un en-tête standard de 24 octets. On commencera par décrire cet en-tête. Chaque type de paquet est ensuite décrit dans un des paragraphes qui suivent. Dans ces paragraphes sont affichées les divisions des paquets en champs, puis sont énumérées les définitions des champs.

Tous les types de paquet OSPF (autres que les paquets Hello OSPF) traitent des listes de LSA. Par exemple, les paquets Mise à jour d'état de liaison mettent en œuvre l'arrosage des LSA sur tout le domaine d'acheminement OSPF. À cause de cela, les paquets de protocole OSPF ne peuvent pas être analysés si le format des LSA n'est aussi compris. Le format des LSA est décrit au paragraphe A.4.

Le traitement des paquets OSPF reçus est exposé au paragraphe 8.2. L'envoi des paquets OSPF est expliqué au paragraphe 8.1.

A.3.1 En-tête de paquet OSPF

Tout paquet OSPF débute par un en-tête standard de 24 octets. Cet en-tête contient toutes les informations nécessaires pour déterminer si le paquet devrait être accepté aux étapes ultérieures de traitement. Cette détermination est décrite au paragraphe 8.2 de la présente spécification.



N° de version
Numéro de version OSPF. La présente spécification documente la version 2 du protocole.

Type
Les types de paquet OSPF sont comme suit. Voir les détails aux paragraphes A.3.2 à A.3.6.

Type	Description
1	Hello
2	Description de base de données
3	Demande d'état de liaison
4	Mise à jour d'état de liaison
5	Accusé de réception d'état de liaison

Longueur de paquet
Longueur en octets du paquet de protocole OSPF. Cette longueur inclut l'en-tête OSPF standard.

Identifiant de routeur
L'identifiant de routeur de la source du paquet.

Identifiant de zone
Nombre de 32 bits qui identifie la zone à laquelle appartient le paquet. Tous les paquets OSPF sont associés à une seule zone. La plupart font un voyage d'un seul bond. Les paquets qui voyagent sur une liaison virtuelle sont étiquetés avec l'identifiant de zone du cœur de réseau de 0.0.0.0.

Somme de contrôle
C'est la somme de contrôle IP standard sur le contenu du paquet entier, qui commence avec l'en-tête du paquet OSPF mais exclut les 64 bits du champ Authentification. Cette somme de contrôle est calculée sur 16 bits comme complément à un de la somme des compléments à un de tous les mots de 16 bits du paquet, sauf du champ Authentification. Si la longueur du paquet n'est pas un nombre entier de mots de 16 bits, le paquet est bourré avec un octet de zéros avant d'être soumis à la somme de contrôle. La somme de contrôle est considérée comme faisant partie de la procédure d'authentification du paquet ; pour certains types d'authentification, le calcul de la somme de contrôle est omis.

AuType
Identifie la procédure d'authentification à utiliser pour le paquet. L'authentification est discutée à l'Appendice D de la présente spécification. Consulter à l'Appendice D la liste des types d'authentification actuellement définis.

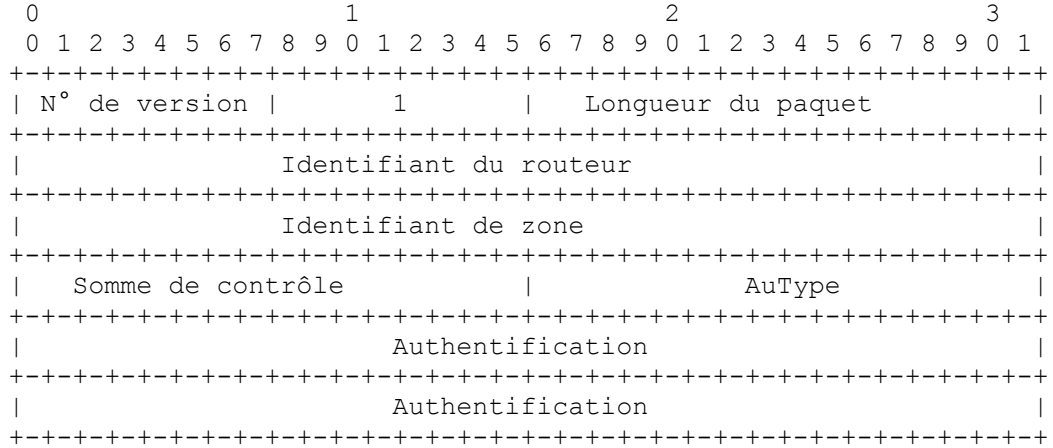
Authentification
Un champ de 64 bits à utiliser par le schéma d'authentification. Voir les détails à l'Appendice D.

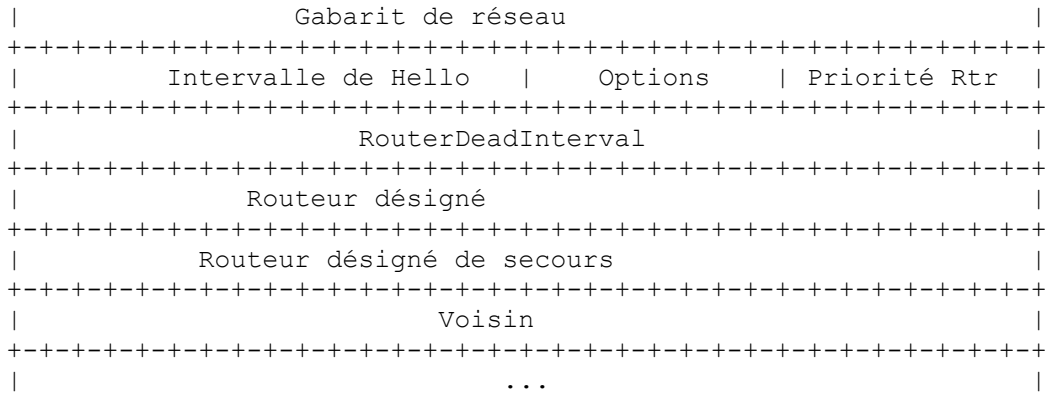
A.3.2 Paquet Hello

Les paquets Hello sont des paquets OSPF de type 1. Ces paquets sont envoyés périodiquement sur tous les interfaces (y compris les liaisons virtuelles) afin d'établir et maintenir les relations de voisinage. De plus, les paquets Hello sont envoyés en diffusion groupée sur les réseaux physiques qui ont une capacité de diffusion ou de diffusion groupée, ce qui permet la découverte dynamique des routeurs voisins.

Tous les routeurs connectés à un réseau commun doivent être d'accord sur certains paramètres (Gabarit de réseau, Intervalle Hello et Intervalle de routeur mort).

Ces paramètres sont inclus dans les paquets Hello, de sorte que des différences peuvent inhiber la formation des relations de voisinage. Un explication détaillée du traitement des paquets Hello en réception est présentée au paragraphe 10.5. L'envoi des paquets Hello est traité au paragraphe 9.5.





Gabarit de réseau
C'est le gabarit de réseau associé à cette interface. Par exemple, si l'interface est avec un réseau de classe B dont le troisième octet est utilisé pour le sous-réseautage, le gabarit de réseau est 0xffffff00.

Options
Ce sont les capacités facultatives prises en charge par le routeur, comme exposé au paragraphe A.2.

Intervalle Hello
Nombre de secondes entre les paquets Hello de ce routeur.

Priorité de routeur
La priorité de routeur de ce routeur. Utilisé pour le choix du routeur désigné (de secours). Réglé à 0, le routeur sera inéligible pour devenir routeur désigné (de secours).

Intervalle de routeur mort
Nombre de secondes avant de déclarer mort un routeur silencieux.

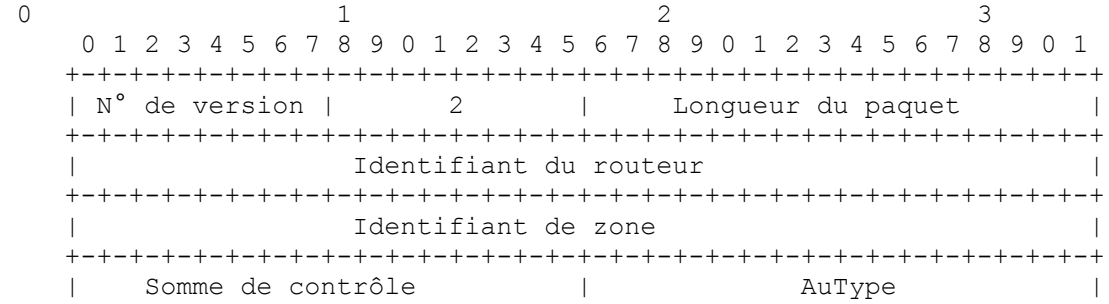
Routeur désigné
Identité du routeur désigné pour ce réseau, du point de vue du routeur émetteur. Le routeur désigné est identifié ici par son adresse IP d'interface sur le réseau. Réglé à 0.0.0.0 s'il n'y a pas de routeur désigné.

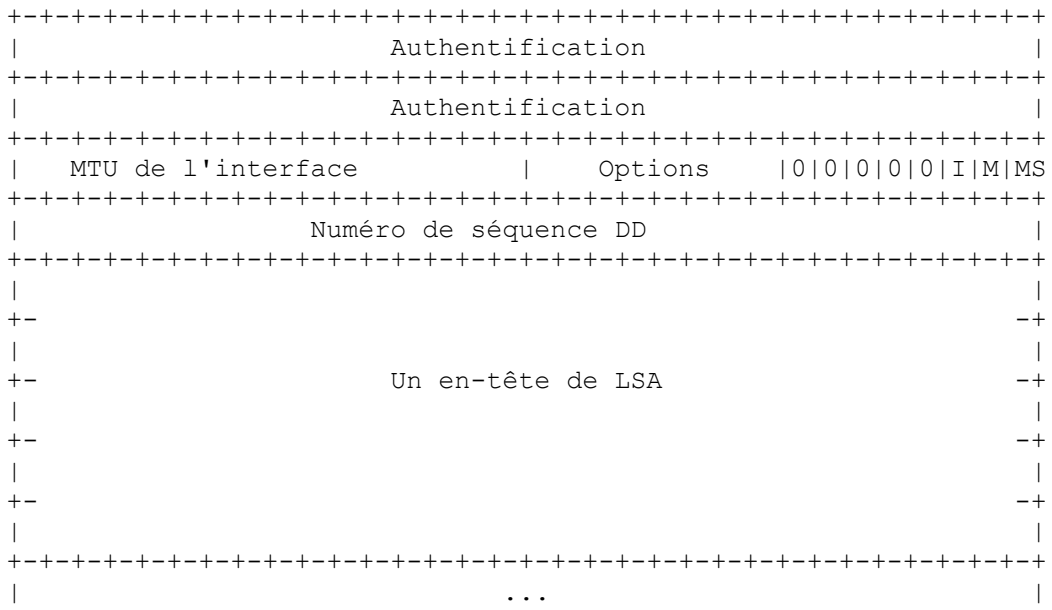
Routeur désigné de secours
Identité du routeur désigné de secours pour ce réseau, du point de vue du routeur émetteur. Le routeur désigné de secours est identifié ici par son adresse IP d'interface sur le réseau. Réglé à 0.0.0.0 si il n'y a pas de routeur désigné de secours.

Voisin
C'est l'identifiant de routeur de chaque routeur dont des paquets Hello valides ont été vus récemment sur le réseau. Récemment signifie dans le dernier Intervalle de routeur mort (en secondes).

A.3.3 Paquet Description de base de données

Les paquets de description de base de données sont des paquets OSPF de type 2. Ces paquets sont échangés lorsqu'une adjacence est initialisée. Ils décrivent les contenus des bases de données d'états de liaison. Plusieurs paquets peuvent être utilisés pour décrire la base de données. Une procédure d'interrogation/réponse est utilisée à cette fin. Un des routeurs est désigné comme étant le maître, l'autre comme l'esclave. Le maître envoie les paquets de description de base de données (interrogations) dont il est accusé réception par les paquets de description de base de données envoyés par l'esclave (réponses). Les réponses sont liées aux interrogations via les numéros de séquence DD des paquets.





Le format du paquet de description de base de données est très similaire aux deux paquets de demande d'état de liaison et d'accusé de réception d'état de liaison. La partie principale de tous les trois est une liste d'éléments, chacun décrivant une partie de la base de données d'états de liaisons. L'envoi des paquets de description de base de données est exposé au paragraphe 10.8. La réception des paquets de description de base de données est exposée au paragraphe 10.6.

MTU d'interface
C'est la taille en octets du plus grand datagramme IP qui peut être envoyé de l'interface associée, sans fragmentation. Les MTU des types de liaison Internet courantes se trouvent au Tableau 7-1 de [Ref22]. La MTU d'interface devrait être réglée à 0 dans les paquets de description de base de données envoyés sur des liaisons virtuelles.

Options
Ce sont les capacités facultatives prises en charge par le routeur, comme exposé au paragraphe A.2.

Bit I
Le bit Init. Lorsqu'il est mis à 1, ce paquet est le premier dans la séquence des paquets de description de base de données.

Bit M
Le bit More *(plus)*. Lorsqu'il est mis à 1, il indique que plus de paquets de description de base de données suivent.

Bit MS
C'est le bit Maître/esclave. Lorsqu'il est mis à 1, il indique que le routeur est le maître durant le processus d'échange de base de données. Autrement, le routeur est l'esclave.

numéro de séquence DD
Utilisé pour mettre en séquence la collection de paquets de description de base de données. La valeur initiale (indiquée par le bit Init à 1) devrait être unique. Le numéro de séquence DD est alors incrémenté jusqu'à ce que toute la description de la base de données ait été envoyée.

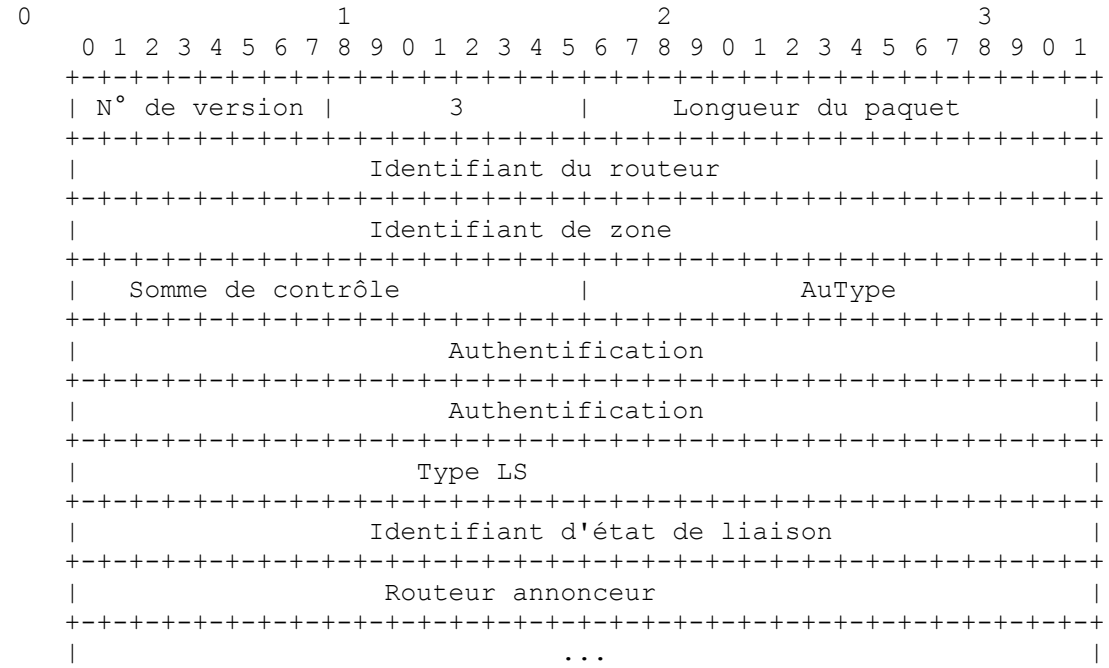
Le reste du paquet consiste en une liste (éventuellement partielle) des éléments de la base de données d'états de liaisons. Chaque LSA de la base de données est décrit par son en-tête de LSA. L'en-tête de LSA est expliqué au paragraphe A.4.1. Il contient toutes les informations nécessaires pour identifier de façon univoque à la fois le LSA et l'instance actuelle du LSA.

A.3.4 Paquet Demande d'état de liaison

Les paquets Demande d'état de liaison sont des paquets OSPF de type 3. Après avoir échangé les paquets de description de base de données avec un routeur voisin, un routeur peut trouver que certaines parties de sa base de données d'états de liaisons sont périmées. Le paquet Demande d'état de liaison est utilisé pour demander les éléments de la base de données du voisin qui sont plus à jour. Plusieurs paquets de demande d'état de liaison peuvent devoir être utilisés.

Un routeur qui envoie un paquet Demande d'état de liaison a en vue l'instance précise de l'élément de la base de données qu'il demande. Chaque instance est définie par son numéro de séquence LS, sa somme de contrôle LS, et son âge LS, bien que ces champs ne soient pas spécifiés dans le paquet de demande d'état de liaison lui-même. Le routeur peut même recevoir en réponse des instances plus récentes.

L'envoi des paquets Demande d'état de liaison est expliqué au paragraphe 10.9. La réception des paquets Demande d'état de liaison est expliquée au paragraphe 10.7.

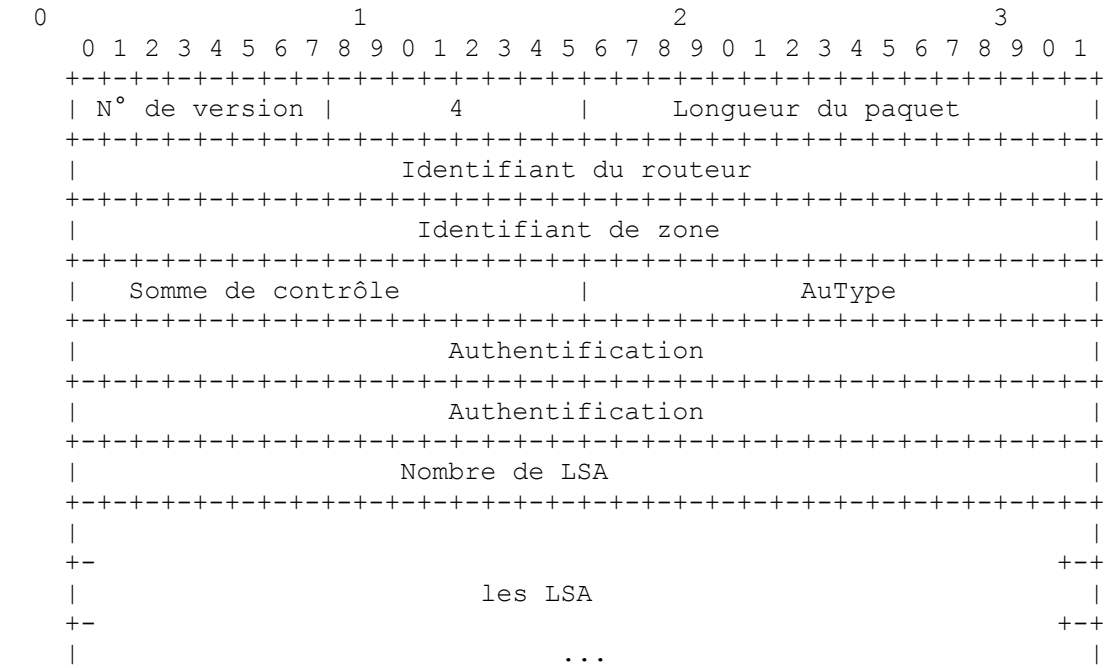


Chaque LSA demandé est spécifié par son type LS, son identifiant d'état de liaison, et le Routeur annonceur. Cela identifie de façon univoque le LSA, mais pas son instance. Les paquets Demande d'état de liaison sont compris comme la demande de l'instance la plus récente (quelle qu'elle puisse être).

A.3.5 Paquet Mise à jour d'état de liaison

Les paquets Mise à jour d'état de liaison sont des paquets OSPF de type 4. Ces paquets mettent en œuvre l'arrosage des LSA. Chaque paquet Mise à jour d'état de liaison porte une collection des LSA qui se trouvent un bond plus loin que leur origine. Plusieurs LSA peuvent être inclus dans un seul paquet.

Les paquets Mise à jour d'état de liaison sont envoyés en diffusion groupée sur les réseaux physiques qui acceptent la diffusion/diffusion groupée. Afin de rendre fiable la procédure d'arrosage, les LSA diffusés sont acquittés dans des paquets Accusé de réception d'état de liaison. Si la retransmission de certains LSA est nécessaire, les LSA retransmis sont toujours envoyés directement au voisin. Pour des informations complémentaires sur la diffusion fiable des LSA, consulter la Section 13.



Nombre de LSA
C'est le nombre de LSA inclus dans cette mise à jour.

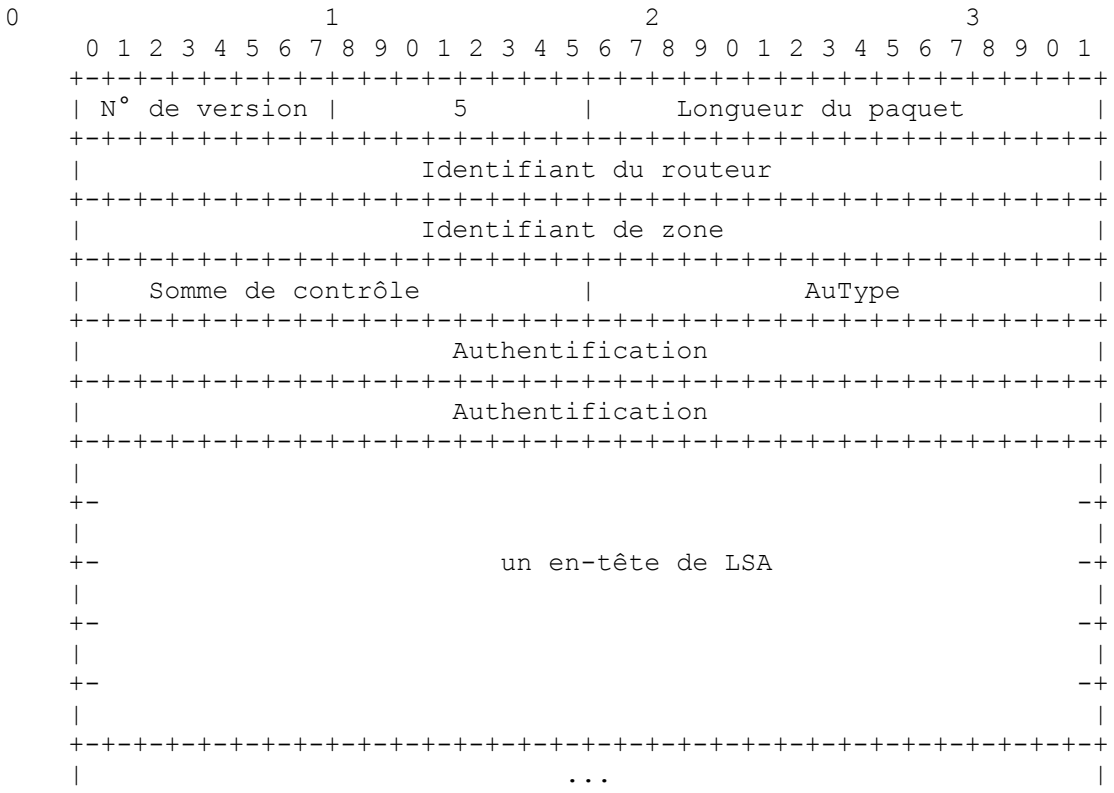
Le corps du paquet Mise à jour d'état de liaison consiste en une liste des LSA. Chaque LSA commence par un en-tête commun de 20 octets, décrit au paragraphe A.4.1. Les formats détaillés des différents types de LSA sont décrits au paragraphe A.4.

A.3.6 Paquet Accusé de réception d'état de liaison

Les paquets Accusé de réception d'état de liaison sont des paquets OSPF de type 5. Pour rendre fiable la diffusion des LSA, il est explicitement accusé réception des LSA. Cet accusé de réception est réalisé par l'envoi et la réception des paquets Accusé de réception d'état de liaison. Il peut en être accusé réception de plusieurs dans un seul paquet Accusé de réception d'état de liaison.

Selon l'état de l'interface d'envoi et l'envoyeur du paquet Mise à jour d'état de liaison correspondant, un paquet d'accusé de réception d'état de liaison est envoyé soit à l'adresse de diffusion groupée AllSPFRouters, soit à l'adresse de diffusion groupée AllDRouters, soit comme envoi individuel. L'envoi des paquets d'accusé de réception d'état de liaison est expliqué au paragraphe 13.5. La réception des paquets d'accusé de réception d'état de liaison est expliquée au paragraphe 13.7.

Le format de ce paquet est similaire à celui du paquet Description des données. Le corps des deux paquets est simplement une liste des en-têtes des LSA.



Chaque LSA acquitté est décrit par son en-tête de LSA. L'en-tête de LSA est exposé au paragraphe A.4.1. Il contient toutes les informations requises pour identifier de façon univoque le LSA et l'instance actuelle du LSA.

A.4 Formats des LSA

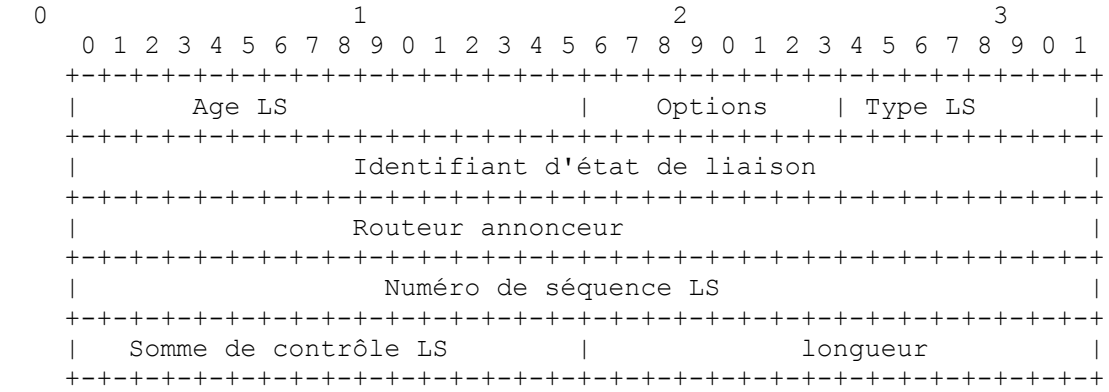
Le présent mémoire définit cinq types distinct de LSA. Chaque LSA commence par un en-tête standard de 20 octets. Cet en-tête est expliqué au paragraphe A.4.1. Les paragraphes suivants donnent les diagrammes des divers types de LSA.

Chaque LSA décrit un élément du domaine d'acheminement OSPF. Chaque routeur génère un LSA de routeur. De plus, chaque fois que le routeur est choisi comme routeur désigné, il génère un LSA de réseau. Les autres types de LSA peuvent aussi être générés (voir au paragraphe 12.4). Tous les LSA sont alors diffusés sur le domaine d'acheminement OSPF. L'algorithme de diffusion est fiable, assurant que tous les routeurs ont la même collection de LSA. (Voir à la Section 13 pour des informations complémentaires concernant l'algorithme de diffusion). Cette collection de LSA est appelée la base de données d'états de liaisons.

À partir de la base de données d'état de liaison, chaque routeur construit un arbre des plus courts chemins avec lui-même comme racine. Cela donne un tableau d'acheminement (voir la Section 11). Pour les détails du processus de construction du tableau d'acheminement, voir la Section 16.

A.4.1 En-tête de LSA

Tous les LSA commencent par un en-tête commun de 20 octets. Cet en-tête contient des informations suffisantes pour identifier de façon univoque le LSA (Type LS, Identifiant d'état de liaison, et Routeur annonceur). Plusieurs instances du LSA peuvent exister en même temps dans le domaine d'acheminement. Il est donc nécessaire de déterminer quelle instance est la plus récente. Ceci est réalisé par l'examen des champs Age LS, Numéro de séquence LS et Somme de contrôle LS qui sont aussi contenus dans l'en-tête de LSA.



Age LS
C'est le temps en secondes depuis la création du LSA.

Options
Capacités facultatives prises en charge par la portion décrite du domaine d'acheminement. Les capacités OSPF facultatives sont exposées au paragraphe A.2.

Type LS
Le type du LSA. Chaque type de LSA a un format d'annonce distinct. Le type de LSA défini dans le présent mémoire est comme suit (voir au paragraphe 12.1.3 des explications complémentaires) :

Type LS	**Description**
1	LSA de routeur
2	LSA de réseau
3	LSA de résumé (réseau IP)
4	LSA de résumé (ASBR)
5	LSA externes à l'AS

Identifiant d'état de liaison
Ce champ identifie la portion de l'environnement internet qui est décrite par le LSA. Le contenu de ce champ dépend du type LS du LSA. Par exemple, dans les LSA de réseau, l'identifiant d'état de liaison est réglé à l'adresse IP d'interface du routeur désigné du réseau (d'où l'adresse IP du réseau peut être déduite). L'identifiant d'état de liaison est exposé plus en détails au paragraphe 12.1.4.

Routeur annonceur
C'est l'identifiant de routeur du routeur qui a généré le LSA. Par exemple, dans les LSA de réseau, ce champ est égal à l'identifiant de routeur du routeur désigné du réseau.

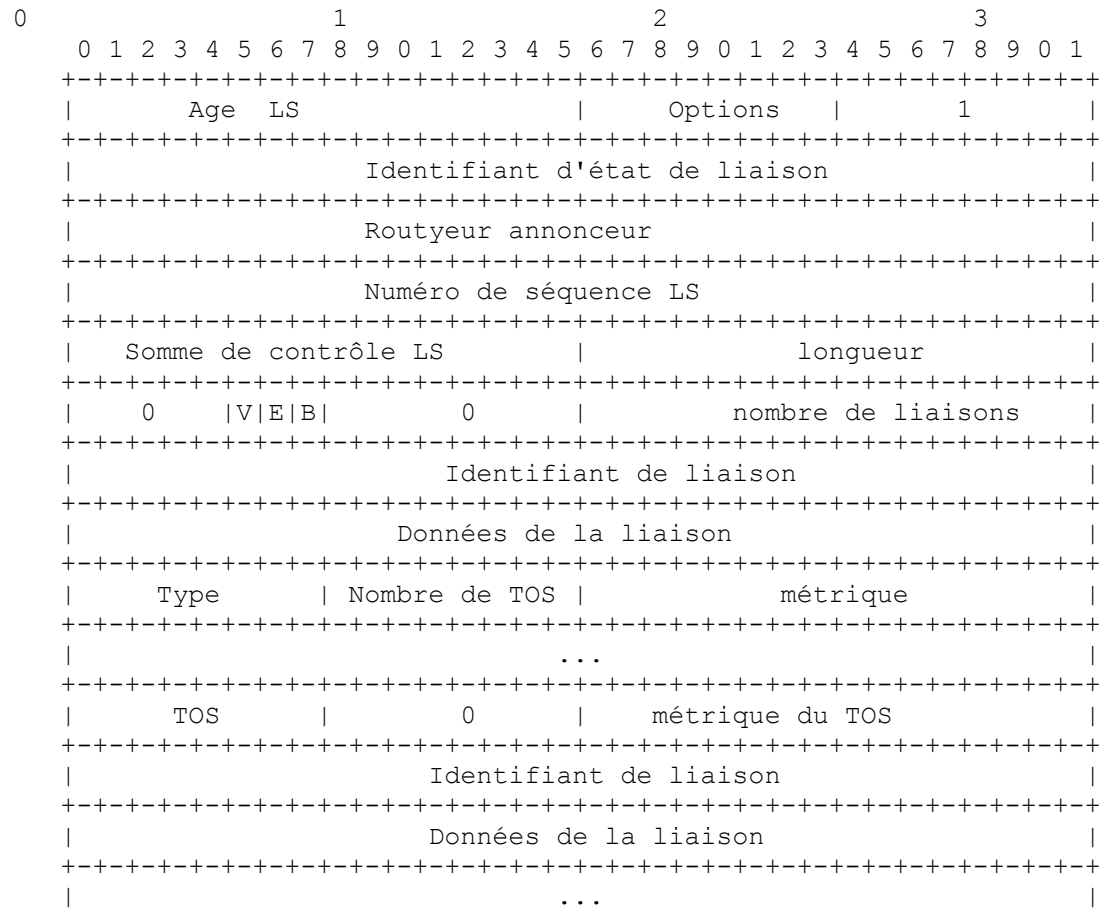
Numéro de séquence LS
Il détecte les LSA périmés ou dupliqués. Les instances successives d'un LSA reçoivent des numéros de séquence LS qui se succèdent. Voir au paragraphe 12.1.6 pour des précisions.

Somme de contrôle LS
C'est la somme de contrôle de Fletcher du contenu complet du LSA, y compris l'en-tête de LSA mais à l'exclusion du champ Age LS. Voir au paragraphe 12.1.7 pour des précisions.

Longueur
C'est la longueur en octets du LSA. Cela inclut les 20 octets de l'en-tête de LSA.

A.4.2 LSA de routeur

Les LSA de routeur sont des LSA de type 1. Chaque routeur dans une zone génère un LSA de routeur. Le LSA décrit l'état et le coût des liaisons du routeur (c'est-à-dire, les interfaces) avec la zone. Toutes les liaisons du routeur avec la zone doivent être décrites dans un seul LSA de routeur. Pour les détails concernant la construction des LSA de routeur, voir au paragraphe 12.4.1.



Dans les LSA de routeur, le champ d'identifiant d'état de liaison est réglé à l'identifiant de routeur OSPF du routeur. Les LSA de routeur ne sont diffusés que dans une seule zone.

Bit V (V pour point d'extrémité de liaison virtuelle)
Lorsqu'il est mis à un, le routeur est un point d'extrémité d'une ou plusieurs liaisons virtuelles pleinement adjacentes dont la zone décrite est une zone de transit.

Bit E (E pour externe)
Lorsqu'il est mis à un, le routeur est un routeur frontière de l'AS.

Bit B (B pour bordure)
Lorsqu'il est mis à un, le routeur est un routeur frontière de zone.

Nombre de liaisons
C'est le nombre de liaisons de routeur décrites dans ce LSA. Cela doit être la collection totale des liaisons de routeur (c'est-à-dire, d'interfaces) avec la zone.

Les champs suivants sont utilisés pour décrire chaque liaison de routeur (c'est-à-dire, d'interface). Chaque liaison de routeur est typée (voir ci-dessous le champ Type). Le champ Type indique quelle sorte de liaison est décrite. Cela peut être une liaison avec un réseau de transit, avec un autre routeur ou avec un réseau de bout. Les valeurs de tous les autres champs qui décrivent une liaison de routeur dépendent du type de la liaison. Par exemple, chaque liaison a un champ Données de liaison associé de 32 bits. Pour les liaisons avec des réseaux de bout, ce champ spécifie le gabarit d'adresse IP du réseau. Pour les autres types de liaison, le champ Données de liaison spécifie l'adresse IP de l'interface du routeur.

Type
Brève description de la liaison de routeur. Une des suivantes. Noter que les chemins d'hôte sont classés comme liaisons

avec des réseaux de bout dont le gabarit de réseau est 0xffffffff.

Type	Description
1	Connexion point à point avec un autre routeur
2	Connexion à un réseau de transit
3	Connexion à un réseau de bout
4	Liaison virtuelle

Identifiant de liaison
Identifie l'objet auquel connecte cette liaison de routeur. Sa valeur dépend du type de la liaison. Lorsqu'elle connecte à un objet qui génère aussi un LSA (c'est-à-dire, un autre routeur ou un réseau de transit) l'identifiant de liaison est égal à l'identifiant d'état de liaison du LSA voisin. Cela donne la clé de la recherche du LSA voisin dans la base de données d'état de liaison durant le calcul du tableau d'acheminement. Voir au paragraphe 12.2 pour des précisions.

Type	Identifiant de liaison
1	Identifiant de routeur du routeur voisin
2	Adresse IP du routeur désigné
3	Numéro IP de réseau/sous-réseau
4	Identifiant de routeur du routeur voisin

Données de liaison
Sa valeur dépend encore une fois du champ Type de la liaison. Pour les connexions avec les réseaux de bout, Données de liaison spécifie le gabarit d'adresse IP du réseau. Pour les connexions point à point non numérotées, il spécifie la valeur ifIndex de MIB-II [Ref8] de l'interface. Pour les autres types de liaison, il spécifie l'adresse IP de l'interface du routeur. Ce dernier élément d'information est nécessaire durant le processus de construction du tableau d'acheminement, lors du calcul de l'adresse IP du prochain bond. Voir au paragraphe 16.1.1 pour des précisions.

Nombre de TOS
Nombre des différentes métriques de TOS données pour cette liaison, sans compter la métrique de liaison requise (appelée la métrique 0 de TOS dans [Ref9]). Par exemple, si aucune métrique de TOS additionnelle n'est donnée, ce champ est à 0.

Métrique
Le coût d'utilisation de cette liaison de routeur.

Des informations spécifiques du type de service supplémentaires peuvent aussi être incluses, pour la rétrocompatibilité avec les versions précédentes de la spécification OSPF ([Ref9]). Pour chaque liaison et pour chaque type de service désiré, les informations de liaison spécifiques du type de service peuvent être codées comme suit :

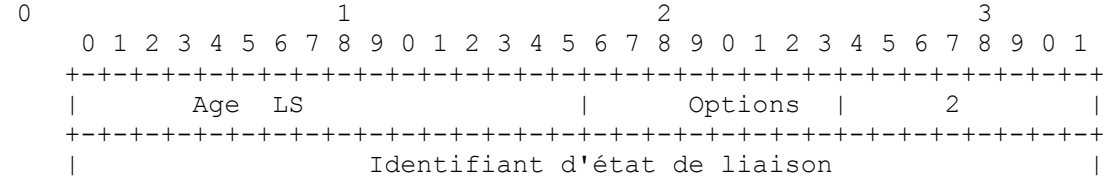
TOS IP
C'est le type de service auquel cette métrique se réfère. Le codage du TOS dans les LSA OSPF est décrit au paragraphe 12.3.

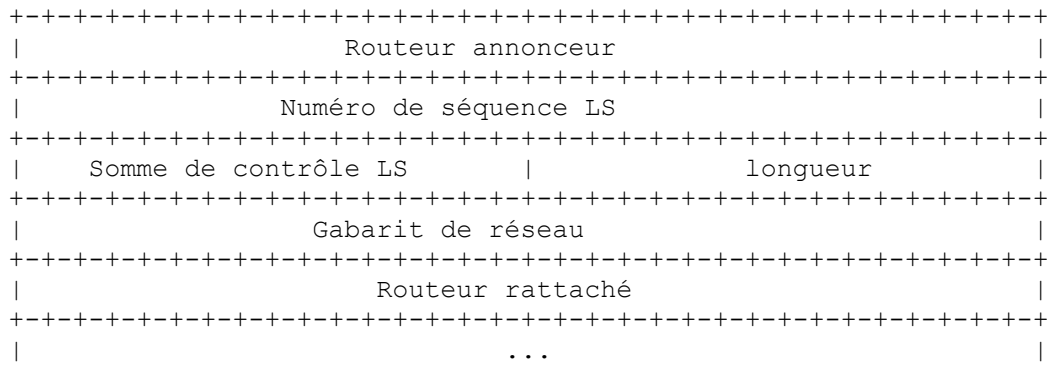
Métrique de TOS
Informations sur la métrique spécifique du type de service.

A.4.3 LSA de réseau

Les LSA de réseau sont des LSA de type 2. Un LSA de réseau est généré pour chaque réseau de diffusion et NBMA qui, dans la zone, prend en charge deux routeurs ou plus. Le LSA de réseau est généré par le routeur désigné du réseau. Le LSA décrit tous les routeurs rattachés au réseau, y compris le routeur désigné lui-même. Le champ d'identifiant d'état de liaison du LSA fait la liste des adresses IP d'interface du routeur désigné.

La distance du réseau à tous les routeurs rattachés est zéro. C'est pourquoi les champs Métrique n'ont pas besoin d'être spécifiés dans le LSA de réseau. Pour les détails concernant la construction des LSA de réseau, voir au paragraphe 12.4.2.





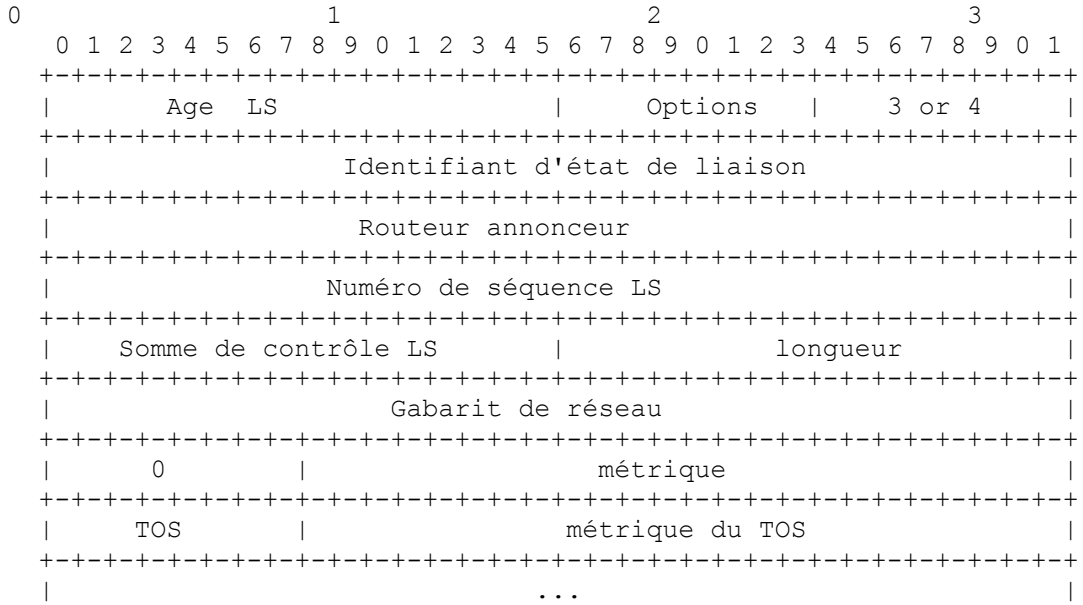
Gabarit de réseau
C'est le gabarit d'adresse IP pour le réseau. Par exemple, un réseau de classe A aurait le gabarit 0xff000000.

Routeur rattaché
Ce sont les identifiants de routeur de chacun des routeurs rattachés au réseau. En fait, seuls les routeurs qui sont pleinement adjacents au routeur désigné figurent sur la liste. Le routeur désigné s'inclut lui-même sur cette liste. Le nombre de routeurs inclus peut se déduire du champ Longueur de l'en-tête du LSA.

A.4.4 LSA de résumé

Les LSA de résumé sont les LSA des types 3 et 4. Ces LSA sont générés par les routeurs frontières de zone. Les LSA de résumé décrivent les destinations inter-zone. Pour les détails concernant la construction des LSA de résumé, voir au paragraphe 12.4.3.

Les LSA de résumé de type 3 sont utilisés lorsque la destination est un réseau IP. Dans ce cas le champ Identifiant d'état de liaison du LSA est un numéro de réseau IP (si nécessaire, l'identifiant d'état de liaison peut aussi avoir un ou plusieurs des bits "d'hôte" du réseau mis à un (voir les détails à l'Appendice E). Lorsque la destination est un routeur frontière de l'AS, on utilise un LSA de résumé de type 4, et le champ d'identifiant d'état de liaison est l'identifiant de routeur OSPF du routeur frontière de l'AS. (Pour voir pourquoi il est nécessaire d'annoncer la localisation de chaque ASBR, consulter le paragraphe 16.4.) À part la différence du champ Identifiant d'état de liaison, le format des LSA de type 3 et 4 est identique.



Pour les zones de bout, les LSA de résumé de type 3 peuvent être aussi utilisés pour décrire un chemin par défaut (zone par zone). Les résumés de chemins par défaut sont utilisés dans les zones de bout à la place de l'arrosage d'un jeu complet de chemins externes. Lorsqu'il décrit un résumé de chemin par défaut, l'identifiant d'état de liaison de LSA de résumé est toujours réglé à DefaultDestination (0.0.0.0) et le gabarit de réseau est réglé à 0.0.0.0.

Gabarit de réseau
Pour les LSA de résumé de type 3, ceci indique le gabarit d'adresse IP du réseau de destination. Par exemple, lors de l'annonce de la localisation d'un réseau de classe A, on utilisera la valeur 0xff000000. Ce champ n'est pas significatif

pour les LSA de résumé de type 4 et doit être à zéro.

Métrique
C’est le coût de ce chemin. Exprimé dans les mêmes unités que les coûts d’interface dans les LSA de routeur.

Des informations supplémentaires spécifiques du type de service peuvent aussi être incluses, pour la rétrocompatibilité avec les versions précédentes de la spécification OSPF ([Ref9]). Pour chaque type de service désiré, les informations spécifiques du TOS sont codées comme suit :

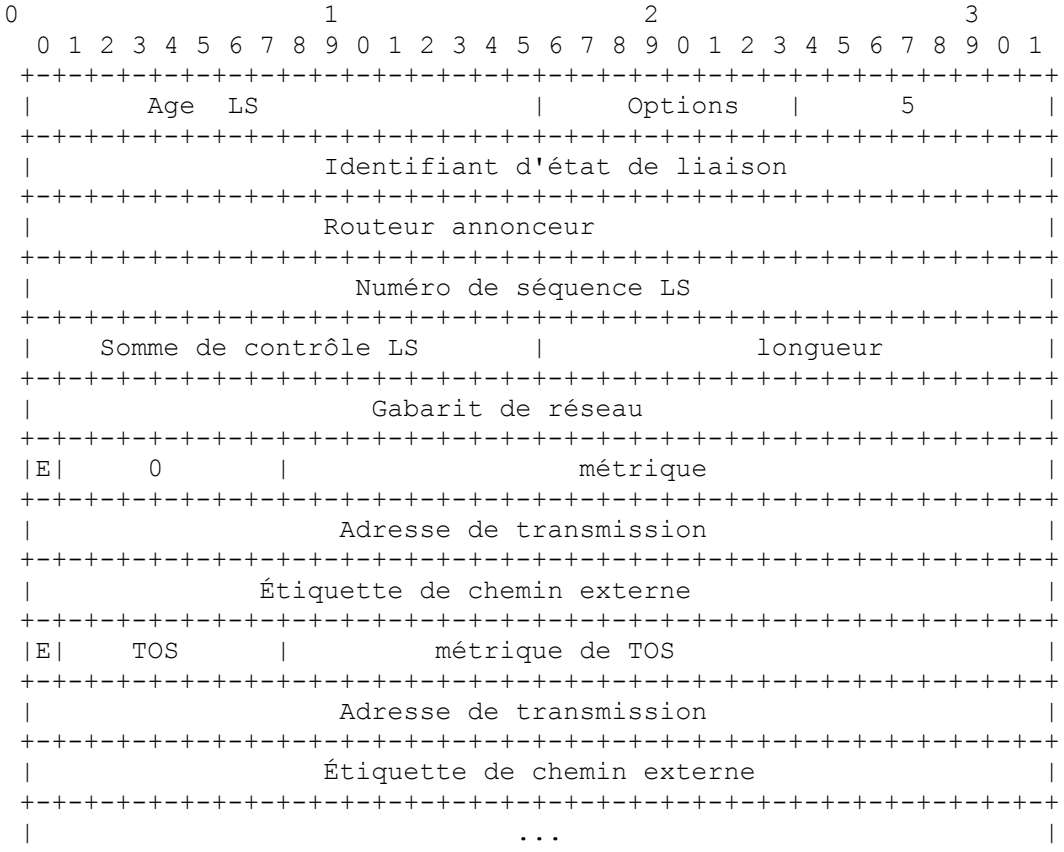
TOS IP
C’est le type de service auquel cette métrique se réfère. Le codage du TOS dans les LSA OSPF est décrit au paragraphe 12.3.

Métrique de TOS
Ce sont les informations sur la métrique spécifique du type de service.

A.4.5 LSA externes à l’AS

Les LSA externes à l’AS sont des LSA de type 5. Ces LSA sont générés par les routeurs frontières de l’AS, et décrivent des destinations externes à l’AS. Pour des détails sur la construction des LSA externes à l’AS, voir au paragraphe 12.4.3.

Les LSA externes à l’AS décrivent normalement une destination externe particulière. Pour ces LSA, le champ d’identifiant d’état de liaison spécifie un numéro de réseau IP (si nécessaire, l’identifiant d’état de liaison peut aussi avoir un ou plusieurs bits "d’hôte" du réseau mis à un ; voir les détails à l’Appendice E). Les LSA externes à l’AS sont aussi utilisés pour décrire un chemin par défaut. Les chemins par défaut sont utilisés lorsqu’aucun chemin spécifique n’existe pour la destination. Quand il décrit un chemin par défaut, l’identifiant d’état de liaison est toujours réglé à DefaultDestination (0.0.0.0) et le gabarit de réseau est mis à 0.0.0.0.



Gabarit de réseau
C’est le gabarit d’adresse IP pour la destination annoncée. Par exemple, lors de l’annonce d’un réseau de classe A, le gabarit 0xff000000 devrait être utilisé.

Bit E
C’est le type de métrique externe. Si le bit E est mis à 1, la métrique spécifiée est une métrique externe de type 2. Cela

signifie que la métrique est considérée comme plus grande que celle de tout chemin d'état de liaison. Si le bit E est à zéro, la métrique spécifiée est une métrique externe de type 1. Cela signifie qu'elle est exprimée dans les mêmes unités que la métrique d'état de liaison (c'est-à-dire, la même unité que le coût de l'interface).

Métrique
C'est le coût de ce chemin. L'interprétation dépend de l'indication du type externe (le bit E ci-dessus).

Adresse de transmission
Le trafic de données pour la destination annoncée sera transmis à cette adresse. Si l'adresse de transmission est réglée à 0.0.0.0, le trafic de données sera alors transmis au générateur du LSA (c'est-à-dire, au routeur frontière de l'AS responsable).

Étiquette de chemin externe
C'est un champ de 32 bits attaché à chaque chemin externe. Il n'est pas utilisé par le protocole OSPF lui-même. Il peut être utilisé pour communiquer des informations entre routeurs frontières de l'AS ; la nature précise de telles informations est en dehors du domaine d'application de la présente spécification.

Des informations spécifiques du type de service supplémentaires peuvent aussi être incluses, pour la rétrocompatibilité avec les versions précédentes de la spécification OSPF ([Ref9]). Pour chaque type de service désiré, les informations spécifiques du TOS sont codées comme suit :

TOS
C'est le type de service du champ suivant. Le codage du TOS dans les LSA OSPF est décrit au paragraphe 12.3.

Bit E
Pour la rétrocompatibilité avec [Ref9].

Métrique de TOS
Les informations de métrique spécifiques du type de service.

Adresse de transmission
Pour la rétrocompatibilité avec [Ref9].

Étiquette de chemin externe
Pour la rétrocompatibilité avec [Ref9].

Appendice B. Constantes architecturales

Plusieurs paramètres de protocole OSPF ont des valeurs architecturales fixes. Ces paramètres ont été appelés dans le texte par des noms tels que LSRefreshTime. La même convention de dénomination est utilisée pour les paramètres configurables du protocole. Ils sont définis dans l'Appendice C.

Le nom de chaque constante architecturale suit, ainsi que sa valeur et une brève description de sa fonction.

LSRefreshTime
Durée maximum entre des générations distinctes de tout LSA particulier. Si le champ Age LS de l'un des LSA auto générés du routeur atteint la valeur de LSRefreshTime, une nouvelle instance du LSA est générée, quand bien même les contenus du LSA (à part l'en-tête de LSA) seraient les mêmes. La valeur de LSRefreshTime est établie à 30 minutes.

MinLSInterval
Durée minimum entre des générations distinctes de tout LSA particulier. La valeur de MinLSInterval est établie à 5 s.

MinLSArrival
Pour tous LSA particulier, la durée minimum qui doit s'écouler entre la réception de nouvelles instances de LSA durant l'arrosage. Les instances de LSA reçues à une fréquence plus élevée sont éliminées. La valeur de MinLSArrival est établie à 1 s.

MaxAge
C'est l'âge maximum qu'un LSA peut atteindre. Lorsque le champ Age LS d'un LSA atteint MaxAge, le LSA est rediffusé afin de tenter de le purger du domaine d'acheminement (voir la Section 14). Les LSA d'âge MaxAge ne sont pas utilisés dans le calcul du tableau d'acheminement. La valeur de MaxAge est établie à une heure.

CheckAge
Lorsque l'âge d'un LSA dans la base de données d'état de liaison se heurte à un multiple de CheckAge, la somme de contrôle du LSA est vérifiée. Une somme de contrôle incorrecte à ce moment indique une erreur sérieuse. La valeur de CheckAge est établie à 5 minutes.

MaxAgeDiff
C'est la dispersion maximum de durée qui peut survenir lors de la diffusion d'un LSA sur l'AS. La plus grande partie de ce temps est passée par le LSA dans les files d'attentes de sortie du routeur (et ne compte donc pas pour la péremption) durant le processus d'arrosage. La valeur de MaxAgeDiff est établie à 15 minutes.

LSInfinity
C'est la valeur de métrique qui indique que la destination décrite par un LSA est inaccessible. Elle est utilisée dans les LSA de résumé et les LSA externes à l'AS comme solution de remplacement à une péremption prématurée (voir au paragraphe 14.1). Elle est définie comme une valeur binaire de 24 bits tous en uns : 0xffffff.

DefaultDestination
C'est l'identifiant de destination qui indique le chemin par défaut. Ce chemin est utilisé lorsqu'aucune autre entrée de tableau d'acheminement correspondante ne peut être trouvée. La destination par défaut ne peut être annoncée que dans les LSA externes à l'AS et dans les LSA de résumé de type 3 des zones de bout. Sa valeur est l'adresse IP 0.0.0.0. Son gabarit de réseau associé est aussi toujours 0.0.0.0.

InitialSequenceNumber
C'est la valeur utilisée pour le numéro de séquence LS lors de la génération de la première instance de tout LSA. Sa valeur est l'entier signé de 32 bits 0x80000001.

MaxSequenceNumber
C'est la valeur maximale que peut atteindre le numéro de séquence LS. Sa valeur est l'entier signé de 32 bits 0x7fffffff.

Appendice C. Constantes configurables

Le protocole OSPF a assez peu de paramètres configurables. La liste de ces paramètres figure ci-dessous. Ils sont groupés en catégories fonctionnelles générales (paramètres de zone, paramètres d'interface, etc.). Des exemples de valeur sont donnés pour certains des paramètres.

Certains réglages de paramètres doivent être cohérents entre les groupes de routeurs. Par exemple, tous les routeurs d'une même zone doivent être en accord avec les paramètres de la zone, et tous les routeurs rattachés à un réseau doivent être conformes au numéro de réseau IP et au gabarit de ce réseau.

Certains paramètres peuvent être déterminés par des algorithmes de routeur figurant en dehors de la présente spécification (par exemple, l'adresse d'un hôte connecté au routeur via une ligne SLIP). Du point de vue d'OSPF, ces éléments sont alors configurables.

C.1 Paramètres globaux

En général, une copie distincte du protocole OSPF fonctionne dans chaque zone. À cause de cela, la plupart des paramètres de configuration sont définis sur la base de la zone. Les quelques paramètres de configuration globaux sont énumérés ci-dessous.

Identifiant de routeur
C'est un nombre de 32 bits qui identifie de façon univoque le routeur dans le système autonome. Un algorithme pour l'allocation de l'identifiant de routeur est de choisir la plus grande ou la plus petite adresse IP allouée au routeur. Si l'identifiant de routeur OSPF d'un routeur est changé, le logiciel OSPF du routeur devrait être redémarré avant que le nouvel identifiant de routeur ne prenne effet. Avant un redémarrage afin de changer son identifiant de routeur, le routeur devrait purger ses LSA auto générés du domaine d'acheminement (voir au paragraphe 14.1) sinon ils vont persister jusqu'à MaxAge minutes.

RFC1583Compatibility
Contrôle les règles de préférence utilisées au paragraphe 16.4 lors du choix entre plusieurs LSA externes à l'AS qui annoncent la même destination. Lorsqu'il est réglé à "activé", les règles de préférence restent celles spécifiées par la

RFC 1583 ([Ref9]). Lorsqu'il est réglé à "désactivé", les règles de préférence sont celles établies au paragraphe 16.4.1, ce qui empêche les acheminements en boucle lorsque les LSA externes à l'AS pour la même destination ont été générés à partir de zones différentes. Réglé à "activé" par défaut.

Afin de minimiser les chances d'acheminement en boucle, tous les routeurs OSPF d'un domaine d'acheminement OSPF devraient avoir un réglage identique de leur RFC1583Compatibility. Quand sont présents des routeurs qui n'ont pas été mis à jour avec la fonctionnalité spécifiée au paragraphe 16.4.1 du présent mémoire, tous les routeurs devraient avoir RFC1583Compatibility réglé à "activé". Autrement, tous les routeurs devraient avoir RFC1583Compatibility réglé à "désactivé", pour empêcher tous les acheminements en boucle.

C.2 Paramètres de zone

Tous les routeurs appartenant à une zone doivent être d'accord sur la configuration de cette zone. Les désaccords entre deux routeurs conduiront à l'incapacité de former les adjacences, avec un empêchement résultant du flux de trafic de protocole d'acheminement et de données. Les éléments suivants doivent être configurés pour une zone :

Identifiant de zone
C'est un nombre de 32 bits qui identifie la zone. L'identifiant de zone 0.0.0.0 est réservé pour le cœur de réseau. Si la zone représente un réseau organisé en sous-réseaux, le numéro de réseau IP du réseau en sous-réseaux peut être utilisé pour l'identifiant de zone.

Liste des gammes d'adresse
Une zone OSPF est définie comme une liste de gammes d'adresses. Chaque gamme d'adresse comporte les éléments suivants :

[adresse IP, gabarit]
Décrit la collection d'adresses IP contenues dans la gamme d'adresse. Les réseaux et les hôtes sont assignés à une zone selon que leurs adresses tombent dans les gammes d'adresses définies pour la zone. Les routeurs sont vus comme appartenant à plusieurs zones, selon l'appartenance de zone de leurs réseaux de rattachement.

Statut
Réglé à Annoncer ou NePasAnnoncer. Les informations d'acheminement sont concentrées aux frontières de la zone. Externe à la zone, un seul chemin au plus est annoncé (via un LSA de résumé) pour chaque gamme d'adresse. Le chemin est annoncé si et seulement si le Statut de la gamme d'adresses est réglé à Annoncer. Les gammes non annoncées permettent de cacher intentionnellement l'existence de certains réseaux aux autres zones. Statut est réglé à Annoncer par défaut.

Par exemple, supposons qu'un réseau IP organisé en sous-réseaux soit sa propre zone OSPF. La zone sera configurée comme une seule gamme d'adresses, dont l'adresse IP est l'adresse du réseau en sous-réseaux, et dont le gabarit est le gabarit d'adresse de la classe A, B, ou C naturelle. Un seul chemin sera annoncé à l'extérieur de la zone, décrivant le réseau en sous-réseaux tout entier.

ExternalRoutingCapability
Indique si les LSA externes à l'AS seront diffusés dans la zone. Si les LSA externes à l'AS sont exclus de la zone, la zone est appelée un "bout". À l'intérieur des zones de bout, l'acheminement vers les destinations externes sera uniquement fondé sur un résumé de chemin par défaut. Le cœur de réseau ne peut être configuré comme une zone de bout. De plus, les liaisons virtuelles ne peuvent pas être configurées à travers des zones de bout. Pour des informations complémentaires, voir au paragraphe 3.6.

StubDefaultCost
Si la zone a été configurée comme zone de bout, et si le routeur lui-même est un routeur frontière de zone, StubDefaultCost indique alors le coût du LSA de résumé par défaut que le routeur devrait annoncer dans la zone.

C.3 Paramètres d'interface de routeur

Certains des paramètres configurables d'interface de routeur (tels que les adresses IP d'interface et le gabarit de sous-réseau) impliquent en fait des propriétés des réseaux de rattachement, et doivent donc être cohérents à travers tous les routeurs rattachés à ce réseau. Les paramètres qui doivent être configurés pour une interface de routeur sont :

Adresse IP d'interface
C'est l'adresse du protocole IP pour cette interface. Elle identifie de façon univoque le routeur sur l'Internet tout entier.

Une adresse IP n'est pas exigée sur les réseaux point à point. Un tel réseau point à point est appelé "non numéroté".

Gabarit d'interface IP

Aussi appelé gabarit de réseau/sous-réseau, il indique la portion de l'adresse IP d'interface qui identifie le réseau de rattachement. L'application du gabarit d'interface IP à l'adresse IP d'interface donne le numéro de réseau IP du réseau de rattachement. Sur les réseaux point à point et les liaisons virtuelles, le gabarit d'interface IP n'est pas défini. Sur ces réseaux, la liaison elle-même n'a pas de numéro de réseau IP alloué, et donc les adresses de chaque côté de la liaison sont allouées de façon indépendante, s'il en est d'allouées.

Identifiant de zone

C'est la zone OSPF à laquelle appartient le réseau de rattachement.

Coût de sortie d'interface

C'est le coût d'envoi d'un paquet sur l'interface, exprimé dans la métrique d'état de liaison. Il est annoncé comme coût de la liaison pour cette interface dans le LSA de routeur du routeur. Le coût de sortie de l'interface doit toujours être supérieur à 0.

RxmtInterval

C'est le nombre de secondes entre les retransmissions de LSA, pour les adjacences qui appartiennent à cette interface. Aussi utilisé lors de la retransmission des paquets Description de base de données et Demande d'état de liaison. Il devrait être bien supérieur au délai d'aller-retour attendu entre deux routeurs quelconques sur le réseau de rattachement. Le réglage de cette valeur devrait être prudent sinon il en résultera des retransmissions inutiles. Un exemple de valeur pour un réseau de zone locale serait 5 secondes.

InfTransDelay

C'est le nombre estimé de secondes que prend la transmission d'un paquet Mise à jour d'état de liaison sur cette interface. Les LSA contenus dans le paquet de mise à jour doivent avoir leur âge incrémenté de cette quantité avant transmission. Cette valeur devrait prendre en compte les délais de transmission et de propagation de l'interface. Elle doit être supérieure à 0. Un exemple de valeur pour un réseau de zone locale serait d'une seconde.

Priorité de routeur

C'est un entier non signé de 8 bits. Lorsque deux routeurs rattachés à un réseau essayent tous deux de devenir routeur désigné, celui qui a la plus forte priorité de routeur prend la préséance. Si il y a toujours conflit, le routeur qui a le plus fort identifiant de routeur prend la préséance. Un routeur dont la priorité de routeur est réglée à 0 est inéligible à devenir routeur désigné sur le réseau de rattachement. La priorité de routeur n'est configurée que pour les interfaces avec des réseaux en diffusion et NBMA.

HelloInterval

C'est la durée, en secondes, entre les paquets Hello que le routeur envoie par l'interface. Cette valeur est annoncée dans les paquets Hello du routeur. Elle doit être la même pour tous les routeurs rattachés à un réseau commun. Plus HelloInterval est petit, plus vite seront détectés les changements topologiques ; cependant, il s'ensuivra plus de trafic d'acheminement de protocole OSPF. Un exemple de valeur pour un réseau PDN X.25 sera de 30 secondes. Un exemple de valeur pour un réseau de zone locale est de 10 secondes.

RouterDeadInterval

C'est le nombre de secondes sans avoir entendu de paquets Hello d'un routeur après lequel ses voisins vont déclarer qu'il est mort. C'est aussi annoncé dans les paquets Hello du routeur dans son champ RouterDeadInterval. Ce devrait être un multiple de HelloInterval (disons 4). Cette valeur doit elle aussi être la même pour tous les routeurs rattachés à un réseau commun.

AuType

Identifie la procédure d'authentification à utiliser sur le réseau de rattachement. Cette valeur doit être la même pour tous les routeurs rattachés au réseau. Voir à l'Appendice D la discussion des types d'authentification définis.

Clé d'authentification

Ces données configurées permettent à la procédure d'authentification de vérifier les paquets de protocole OSPF reçus sur l'interface. Par exemple, si le AuType indique un simple mot de passe, la clé d'authentification serait un mot de passe de 64 bits en clair. Les clés d'authentification associées aux autres types d'authentification OSPF sont exposées à l'Appendice D.

C.4 Paramètres de liaison virtuelle

Les liaisons virtuelles sont utilisées pour restaurer/augmenter la connexité du cœur de réseau. Les liaisons virtuelles peuvent être configurées entre toute paire de routeurs frontières de zone qui ont des interfaces avec une zone commune (non cœur de réseau). La liaison virtuelle apparaît comme une liaison point à point non numérotée dans le graphe de cœur de réseau. La liaison virtuelle doit être configurée dans les deux routeurs frontières de zone.

Une liaison virtuelle apparaît dans les LSA de routeur (pour le cœur de réseau) comme si il y avait une interface de routeur séparée avec le cœur de réseau. Comme telle, elle a tous les paramètres associés à une interface de routeur (voir au paragraphe C.3). Bien qu'une liaison virtuelle agisse comme une liaison point à point non numérotée, elle a une adresse IP d'interface qui lui est associée. Cette adresse est utilisée comme la source IP dans les paquets de protocole OSPF qu'il envoie sur la liaison virtuelle, et elle est établie de façon dynamique durant le processus de construction du tableau d'acheminement. Le coût de sortie de l'interface est aussi établi de façon dynamique sur les liaisons virtuelles comme le coût du chemin intra-zone entre les deux routeurs. Le paramètre RxmtInterval doit être configuré, et devrait être bien au dessus du délai d'aller-retour attendu entre les deux routeurs. Il peut être difficile à estimer pour une liaison virtuelle ; il vaut mieux courir le risque de prévoir trop grand. La priorité de routeur n'est pas utilisée sur les liaisons virtuelles.

Une liaison virtuelle est définie par les deux paramètres configurables suivants : l'identifiant de routeur de l'autre point d'extrémité de la liaison virtuelle, et la zone (non cœur de réseau) à travers laquelle fonctionne la liaison virtuelle (appelée la zone de transit de la liaison virtuelle). Les liaisons virtuelles ne peuvent pas être configurées à travers les zones de bout.

C.5 Paramètres de réseau NBMA

OSPF traite un réseau NBMA de façon assez semblable à celle d'un réseau de diffusion. Comme il peut y avoir de nombreux routeurs rattachés au réseau, un routeur désigné est choisi pour le réseau. Ce routeur désigné génère alors un LSA de réseau, qui fait la liste de tous les routeurs rattachés au réseau NBMA.

Cependant, du fait du manque de capacités de diffusion, il peut être nécessaire d'utiliser des paramètres de configuration dans le choix du routeur désigné. Il ne sera nécessaires de configurer ces paramètres que dans les routeurs qui sont eux-mêmes éligibles pour devenir routeur désigné (c'est-à-dire, les routeurs dont la priorité de routeur pour le réseau est différente de zéro) et ensuite, seulement s'il n'existe pas de procédure automatique pour la découverte des voisins :

Liste de tous les autres routeur rattachés
: C'est la liste de tous les autres routeurs rattachés au réseau NBMA. Chaque routeur figure par son adresse IP d'interface sur le réseau. De plus, pour chaque routeur énuméré, l'éligibilité du routeur à devenir routeur désigné doit être définie. Lorsqu'une interface à un réseau NBMA apparaît, le routeur n'envoie de paquets Hello qu'aux voisins éligibles à devenir routeur désigné, jusqu'à ce que l'identité du routeur désigné soit découverte.

PollInterval
: Si un routeur voisin est devenu inactif (il n'a pas été vu de paquet Hello pendant RouterDeadInterval secondes) il peut encore être nécessaire d'envoyer des paquets Hello au voisin mort. Ces paquets Hello seront envoyés au taux réduit de PollInterval, qui devrait être bien plus grand que HelloInterval. Un exemple de valeur pour un réseau PDN X.25 est de 2 minutes.

C.6 Paramètres de réseau en point à multi point

Sur les réseaux en point à multipoint, il peut être nécessaire de configurer l'ensemble des voisins qui sont directement accessibles sur le réseau en point à multipoint. Chaque voisin est identifié par son adresse IP sur le réseau en point à multipoint. Les routeurs désignés ne sont pas choisis sur les réseaux en point à multipoint, de sorte que l'éligibilité à être routeur désigné des voisins configurés est indéfinie.

Autrement, les voisins sur des réseaux en point à multipoint peuvent être découverts de façon dynamique par des protocoles de niveau inférieur tels que l'ARP inverse ([Ref14]).

C.7 Paramètres des chemins d'hôte

Les chemins d'hôte sont annoncés dans les LSA de routeur comme des réseaux de bout avec un gabarit de 0xffffffff. Ils indiquent des interfaces de routeur avec des réseaux point à point, des interfaces de routeur en boucle, ou des hôtes IP qui sont directement connectés au routeur (par exemple, via une ligne SLIP). Pour chaque hôte directement connecté au routeur, les éléments suivants doivent être configurés :

Adresse IP d'hôte
C'est l'adresse IP de l'hôte.

Coût de la liaison à l'hôte
C'est le coût de l'envoi d'un paquet à l'hôte, en termes de métrique d'état de liaison. Cependant, comme l'hôte a probablement une seule connexion à l'internet, le coût configuré réel est sans importance dans la plupart des cas (c'est-à-dire qu'il n'aura pas d'effet sur l'acheminement).

Identifiant de zone
C'est la zone OSPF à laquelle appartient l'hôte.

Appendice D. Authentification

Tous les échanges de protocole OSPF sont authentifiés. L'en-tête de paquet OSPF (voir au paragraphe A.3.1) comporte un champ Type d'authentification, et 64 bits de données à utiliser par le schéma d'authentification approprié (déterminé par le champ Type).

Le type d'authentification est configurable interface par interface (ou de façon équivalente, par réseau/sous-réseau). Des données d'authentification supplémentaires sont aussi configurables par interface.

Les types d'authentification 0, 1 et 2 sont définis par la présente spécification. Tous les autres types d'authentification sont réservés pour être définis par l'IANA (iana@ISI.EDU). Le Tableau 20 donne la liste actuelle des types d'authentification.

AuType	**Description**
0	Pas d'authentification
1	Simple mot de passe
2	Authentification cryptographique
Tous les autres	Réservé pour allocation par l'IANA (iana@ISI.EDU)

Tableau 20: Types d'authentification OSPF.

D.1 Authentification nulle

L'utilisation de ce type d'authentification signifie que les échanges d'acheminement sur le réseau/sous-réseau ne sont pas authentifiés. Le champ Authentification de 64 bits dans l'en-tête OSPF peut contenir n'importe quoi, il n'est pas examiné à la réception du paquet. Lorsque l'authentification nulle est utilisée, le contenu entier de chaque paquet OSPF (autre que le champ authentification de 64 bits) fait l'objet d'une vérification de somme de contrôle afin de détecter la corruption des données.

D.2 Authentification par simple mot de passe

Quand on utilise ce type d'authentification, un champ de 64 bits est configuré sur la base du réseau. Tous les paquets envoyés sur un réseau particulier doivent avoir cette valeur configurée dans le champ Authentification de 64 bits de leur en-tête OSPF. Cela sert essentiellement de mot de passe en "clair" de 64 bits. De plus, le contenu entier de chaque paquet OSPF (autre que le champ Authentification de 64 bits) est vérifié par somme de contrôle afin de détecter la corruption des données.

L'authentification par simple mot de passe protège contre des routeurs qui se joindraient par inadvertance au domaine d'acheminement ; chaque routeur doit d'abord être configuré avec les mots de passe de ses réseaux de rattachement avant qu'il puisse participer à l'acheminement. Cependant, l'authentification par simple mot de passe est vulnérable aux attaques passives largement répandues actuellement dans l'Internet (voir [Ref16]). Quiconque a un accès physique au réseau peut apprendre le mot de passe et compromettre la sécurité du domaine d'acheminement OSPF.

D.3 Authentification cryptographique

Avec l'utilisation de ce type d'authentification, une clé secrète partagée est configurée dans tous les routeurs rattachés à un réseau/sous-réseau commun. Pour chaque paquet de protocole OSPF, la clé est utilisée pour générer/vérifier un "résumé de message" qui est ajouté à la fin du paquet OSPF. Le résumé de message est une fonction unilatérale du paquet de protocole

OSPF et de la clé secrète. Comme la clé secrète n'est jamais envoyée sur le réseau en clair, la protection est assurée contre les attaques passives.

Les algorithmes utilisés pour générer et vérifier le résumé du message sont spécifiés implicitement par la clé secrète. La présente spécification définit complètement l'utilisation de l'authentification cryptographique OSPF avec l'utilisation de l'algorithme MD5.

De plus, un numéro de séquence non décroissant est inclus dans chaque paquet de protocole OSPF pour le protéger contre les attaques en répétition. Cela procure une protection à long terme ; cependant, il est toujours possible de répéter un paquet OSPF jusqu'à ce que le numéro de séquence change. Pour mettre en œuvre ce dispositif, chaque structure de données de voisin contient un nouveau champ appelé "numéro de séquence cryptographique". Ce champ est initialisé à zéro, et est aussi établi à zéro chaque fois que l'état du voisin passe à "Down". Chaque fois qu'un paquet OSPF est accepté comme authentique, le numéro de séquence cryptographique est réglé au numéro de séquence du paquet reçu.

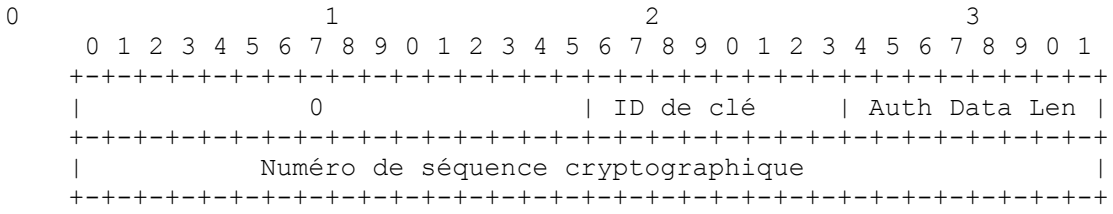


Figure 18 : Usage du champ Authentification dans l'en-tête de paquet OSPF lors de l'emploi de l'authentification cryptographique

La présente spécification ne fournit pas de procédure de débordement pour le numéro de séquence cryptographique. Lorsque le numéro de séquence cryptographique qu'envoie le routeur atteint la valeur maximum, le routeur devrait rétablir le numéro de séquence cryptographique qu'il renvoie à 0. Cela fait, les voisins du routeur vont rejeter les paquets OSPF du routeur pendant une période de RouterDeadInterval, et ensuite le routeur sera forcé de rétablir toutes les adjacences sur l'interface. Cependant, on s'attend à ce que de nombreuses mises en œuvre utilisent les "secondes depuis le réamorçage" (ou "secondes depuis 1960", etc.) comme numéro de séquence cryptographique. Un tel choix va naturellement empêcher le débordement de compteur, dans la mesure où le champ Numéro de séquence cryptographique est long de 32 bits.

L'option OSPF Authentification cryptographique n'assure pas la confidentialité.

Lorsque l'authentification cryptographique est utilisée, le champ Authentification de 64 bits dans l'en-tête de paquet OSPF standard est redéfini comme indiqué à la Figure 18. Les nouvelles définitions de champ sont les suivantes :

ID de clé
Ce champ identifie l'algorithme et la clé secrète utilisés pour créer le résumé de message ajouté au paquet OSPF. Les identifiants de clé sont uniques sur l'interface (ou de façon équivalente, sur le sous réseau).

Longueur de données d'authentification
C'est la longueur en octets du résumé de message ajouté au paquet OSPF.

Numéro de séquence cryptographique
C'est un numéro de séquence non signé de 32 bits non décroissant. Utilisé pour se garder contre les attaques en répétition.

Le résumé de message ajouté au paquet OSPF n'est en fait pas considéré comme faisant partie du paquet de protocole OSPF : le résumé de message n'est pas inclus dans la longueur de paquet de l'en-tête OSPF, bien qu'il soit inclus dans le champ Longueur d'en-tête IP du paquet.

Chaque clé est identifiée par la combinaison de l'interface et de l'identifiant de clé. Une interface peut avoir plusieurs clés actives à tout moment. Cela permet une transition en douceur d'une clé à l'autre. Chaque clé est associée à quatre constantes temporelles. Ces constantes temporelles peuvent être exprimées en termes d'horloge horaire, ou en termes d'horloge locale d'un routeur (par exemple, nombre de secondes depuis le dernier réamorçage) :

KeyStartAccept
C'est l'heure à laquelle le routeur va commencer à accepter les paquets qui ont été créés avec la clé en cause.

KeyStartGenerate
C'est l'heure à laquelle le routeur va commencer à utiliser la clé pour générer des paquets.

KeyStopGenerate
C'est l'heure à laquelle le routeur va arrêter d'utiliser la clé pour générer des paquets.

KeyStopAccept
C'est l'heure à laquelle le routeur va arrêter d'accepter des paquets créés avec la clé en cause.

Afin de réaliser une transition de clé en douceur, KeyStartAccept devrait être inférieur à KeyStartGenerate et KeyStopGenerate devrait être inférieur à KeyStopAccept. Si KeyStopGenerate et KeyStopAccept ne sont pas spécifiés, la durée de vie des clés sera infinie. Lorsqu'une nouvelle clé en remplace une ancienne, l'heure de KeyStartGenerate pour la nouvelle clé doit être inférieure ou égale à l'heure de KeyStopGenerate de l'ancienne clé.

La mémorisation des clés devrait persister à travers un redémarrage système, à chaud ou à froid, pour éviter des problèmes de fonctionnement. Au cas où la dernière clé associée à une interface arrive à expiration, il n'est pas acceptable de revenir à une condition de non authentification, et pas conseillé d'interrompre l'acheminement. Donc, le routeur devrait envoyer une notification "dernière arrivée à expiration de clé d'authentification" au gestionnaire de réseau et traiter la clé comme ayant une durée de vie infinie jusqu'à ce que la durée de vie soit allongée, que la clé soit supprimée par la gestion de réseau, ou qu'une nouvelle clé soit configurée.

D.4 Génération des messages

Après la construction des contenus d'un paquet OSPF, la procédure d'authentification indiquée par l'envoi de la valeur Autype de l'interface est invoquée avant l'envoi du paquet. La procédure d'authentification modifie le paquet OSPF comme suit.

D.4.1 Génération de Authentification nulle

Quand on utilise l'authentification nulle, le paquet est modifié comme suit :

(1) Le champ Autype dans l'en-tête OSPF standard est réglé à 0.

(2) Le champ Somme de contrôle dans l'en-tête OSPF standard est réglé à la somme de contrôle IP standard du contenu entier du paquet, commençant par l'en-tête de paquet OSPF mais excluant le champ authentification de 64 bits. Cette somme de contrôle est calculée comme le complément à un sur 16 bits de la somme des compléments à un de tous les mots de 16 bits du paquet, excepté le champ Authentification. Si la longueur du paquet n'est pas un nombre entier de mots de 16 bits, le paquet est bourré avec un octet de zéros avant de réaliser la somme de contrôle.

D.4.2 Génération de Authentification par simple mot de passe

Lorsque l'authentification par simple mot de passe est utilisée, le paquet est modifié comme suit :

(1) Le champ Autype dans l'en -tête OSPF standard est mis à 1.

(2) Le champ Somme de contrôle dans l'en-tête OSPF standard est réglé à la somme de contrôle IP standard du contenu entier du paquet, commençant par l'en-tête du paquet OSPF mais excluant le champ authentification de 64 bits. Cette somme de contrôle est calculée sur 16 bits comme le complément à un de la somme des compléments à un de tous les mots de 16 bits du paquet, excepté le champ Authentification. Si la longueur du paquet n'est pas un nombre entier de mots de 16 bits, le paquet est bourré avec un octet de zéros avant de réaliser la somme de contrôle.

(3) Le champ Authentification de 64 bits dans l'en-tête du paquet OSPF est réglé au mot de passe de 64 bits (c'est-à-dire, la clé d'authentification) qui a été configuré pour l'interface.

D.4.3 Génération de Authentification cryptographique

Quand on utilise l'authentification cryptographique, plusieurs clés peuvent être configurées pour l'interface. Dans ce cas, parmi les clés qui sont valides pour la génération de message (c'est-à-dire, qui ont KeyStartGenerate ≤ heure actuelle < KeyStopGenerate) choisir celle qui a l'heure KeyStartGenerate la plus récente. En utilisant cette clé, modifier le paquet comme suit :

(1) Le champ Autype dans l'en-tête OSPF standard est mis à 2.
(2) Le champ Somme de contrôle dans l'en-tête OSPF standard n'est pas calculé, mais réglé à 0.
(3) L'identifiant de clé (voir la Figure 18) est réglé à l'identifiant de clé choisi.

(4) Le champ Longueur des données authentifiées est réglé à la longueur en octets du résumé de message qui va être ajouté au paquet OSPF. Quand on utilise l'algorithme d'authentification MD5, Longueur des données authentifiées est réglé à 16.

(5) Le numéro de séquence cryptographique de 32 bits (voir la Figure 18) est réglé à une valeur non décroissante (c'est-à-dire, une valeur au moins aussi élevée que la dernière valeur envoyée de l'interface). Les valeurs précises à utiliser dans le champ Numéro de séquence cryptographique sont spécifiques de la mise en œuvre. Par exemple, il peut être appuyé sur un simple compteur, ou se fonder sur l'horloge du système.

(6) Le résumé du message est alors calculé et ajouté au paquet OSPF. L'algorithme d'authentification à utiliser pour calculer le résumé est indiqué par la clé elle-même. Les entrées de l'algorithme d'authentification comportent le paquet OSPF et la clé secrète. Quand on utilise l'algorithme d'authentification MD5, le calcul du résumé du message se déroule comme suit :
   (a) La clé MD5 de 16 octets est ajoutée au paquet OSPF.
   (b) Les champs Bourrage d'en-queue et Longueur sont ajoutés, comme spécifié dans [Ref17].
   (c) L'algorithme d'authentification MD5 est appliqué sur la concaténation du paquet OSPF, de la clé secrète, des champs Bourrage et Longueur, produisant un résumé de message de 16 octets (voir [Ref17]).
   (d) Le résumé MD5 est écrit sur la clé OSPF (c'est-à-dire, ajouté au paquet OSPF d'origine). Le résumé n'est pas compté dans le champ Longueur du paquet OSPF, mais il est inclus dans le champ Longueur IP du paquet. Aucun champ de bourrage d'en-queue ou de longueur au-delà du résumé n'est compté ni transmis.

D.5 Vérifications de message

Lorsqu'un paquet OSPF a été reçu sur une interface, il doit être authentifié. La procédure d'authentification est indiquée par le réglage de Autype dans l'en-tête standard de paquet OSPF, qui correspond au réglage de Autype pour l'interface OSPF receveuse.

Si un paquet de protocole OSPF est accepté comme authentique, le traitement du paquet continue comme spécifié au paragraphe 8.2. Les paquets qui échouent à l'authentification sont éliminés.

D.5.1 Vérification de Authentification nulle

Lorsqu'on utilise l'authentification nulle, on doit vérifier le champ Somme de contrôle dans l'en-tête OSPF. Il doit être établi au complément à un sur 16 bits de la somme des compléments à un de tous les mots de 16 bits dans le paquet, à l'exception du champ Authentification. (Si la longueur du paquet n'est pas un nombre entier de mots de 16 bits, le paquet est bourré avec un octet de zéros avant d'effectuer la somme de contrôle.)

D.5.2 Vérification de Authentification par simple mot de passe

Lorsqu'on utilise l'authentification par simple mot de passe, le paquet OSPF reçu est authentifié comme suit :

(1) Le champ Somme de contrôle doit être vérifié dans l'en-tête OSPF. Il doit être réglé au complément à un sur 16 bits de la somme des compléments à un des mots de 16 bits du paquet, à l'exception du champ Authentification. (Si la longueur du paquet n'est pas un nombre entier de mots de 16 bits, le paquet est bourré avec un octet de zéros avant d'effectuer la somme de contrôle.)

(2) Les 64 bits du champ Authentification de l'en-tête du paquet OSPF doivent être égaux aux 64 bits du mot de passe (c'est-à-dire, la clé d'authentification) qui a été configuré pour l'interface.

D.5.3 Vérification de Authentification cryptographique

Lorsqu'on utilise l'authentification cryptographique, le paquet OSPF reçu est authentifié comme suit :

(1) Localiser la clé configurée de l'interface receveuse qui a l'identifiant de clé égal à ce qui est spécifié dans le paquet OSPF reçu (voir la Figure 18). Si la clé n'est pas trouvée, ou si la clé n'est pas valide pour la réception (c'est-à-dire, heure actuelle < KeyStartAccept ou heure actuelle ≥ KeyStopAccept) le paquet OSPF est éliminé.

(2) Si le numéro de séquence cryptographique trouvé dans l'en-tête OSPF (voir la Figure 18) est inférieur au numéro de séquence cryptographique enregistré dans la structure de données du voisin expéditeur, le paquet OSPF est éliminé.

(3) Vérifier le résumé de message ajouté selon les étapes suivantes :
   (a) Le résumé reçu est mis de côté.

(b) Un nouveau résumé est calculé, comme spécifié à l'étape 6 du paragraphe D.4.3.

(c) Les résumés, celui calculé et celui reçu, sont comparés. S'ils ne correspondent pas, le paquet OSPF est éliminé. Si ils correspondent, le paquet de protocole OSPF est accepté comme authentique, et le "numéro de séquence cryptographique" dans la structure de données du voisin est réglé au numéro de séquence trouvé dans l'en-tête OSPF du paquet.

Appendice E. Algorithme d'allocation des identifiants d'état de liaison

L'identifiant d'état de liaison dans les LSA externes à l'AS et les LSA de résumé est normalement réglé à l'adresse IP du réseau décrit. Cependant, si nécessaire, un ou plusieurs bits d'hôte du réseau peuvent être établis dans l'identifiant d'état de liaison. Cela permet au routeur de générer des LSA séparés pour les réseaux qui ont la même adresse, mais des gabarits différents. De tels réseaux peuvent survenir en présence de super réseau et de sous-réseau de zéro (voir [Ref10]).

Le présent appendice donne un algorithme possible pour régler les bits d'hôte en identifiants d'état de liaison. Le choix d'un tel algorithme est une décision locale. Des routeurs sont libres d'utiliser des algorithmes différents, car les seuls LSA affectés sont ceux que le routeur génère lui-même. La seule exigence sur les algorithmes utilisés est que l'adresse IP du réseau devrait être utilisée comme l'identifiant d'état de liaison chaque fois que possible ; cela maximise l'interopérabilité avec les mises en œuvre d'OSPF antérieures à la RFC 1583.

L'algorithme ci-dessous est établi pour les LSA externes à l'AS. Ceci est seulement dans un souci de clarté ; le même algorithme peut être utilisé pour les LSA de résumé. Supposons que le routeur souhaite générer un LSA externe à l'AS pour un réseau avec l'adresse NA et le gabarit NM1. Les étapes suivantes seront alors utilisées pour déterminer l'identifiant d'état de liaison du LSA :

(1) Déterminer si le routeur génère déjà un LSA externe à l'AS avec l'identifiant d'état de liaison égal à NA (dans un tel LSA le routeur lui-même sera sur la liste comme Routeur annonceur du LSA). Sinon, l'identifiant d'état de liaison est mis égal à NA et l'algorithme se termine. Autrement,

(2) Obtenir le gabarit de réseau du corps du LSA externe à l'AS déjà existant. Appelons ce gabarit NM2. Il y a maintenant deux cas :

o NM1 est plus long (c'est-à-dire, plus spécifique) que NM2. Dans ce cas, régler l'identifiant d'état de liaison dans le nouveau LSA pour qu'il soit le réseau [NA,NM1] avec tous les bits d'hôte établis (c'est-à-dire, égaux à NA et collés ensemble avec tous les bits qui ne sont pas établis dans NM1, ce qui est l'adresse de diffusion du réseau [NA,NM1]).

o NM2 est plus long que NM1. Dans ce cas, changer le LSA existant (qui a un identifiant d'état de liaison de NA) pour faire référence au nouveau réseau [NA,NM1] en incrémentant le numéro de séquence, en changeant le gabarit dans le corps pour NM1 et en insérant le coût du nouveau réseau. Générer ensuite un nouveau LSA pour le vieux réseau [NA,NM2], avec l'identifiant d'état de liaison égal à NA et collé ensemble avec les bits qui ne sont pas établis dans NM2 (c'est-à-dire, l'adresse de diffusion du réseau [NA,NM2]).

L'algorithme ci-dessus suppose que tous les gabarits sont contigus ; cela assure que lorsque deux réseaux ont la même adresse, un gabarit est plus spécifique que l'autre. L'algorithme suppose aussi que si un des réseaux en conflit est de gabarit d'hôte IP, sa génération de LSA est supprimée. Le choix de l'algorithme de suppression est là encore une décision locale. Cependant, le LSA supprimé DOIT être généré si le réseau en conflit se trouve retiré. Avec ces deux hypothèses, l'algorithme ci-dessus produit toujours un identifiant d'état de liaison univoque. L'algorithme ci-dessus peut aussi être reformulé de la façon suivante : en générant un LSA externe à l'AS, essayer d'utiliser le numéro de réseau comme l'identifiant d'état de liaison. Si cela produit un conflit, examiner les deux réseaux en conflit. L'un sera un sous-ensemble de l'autre. Pour le réseau le moins spécifique, utiliser le numéro de réseau comme identifiant d'état de liaison et pour le plus spécifique utiliser à la place l'adresse de diffusion du réseau (c'est-à-dire, passer tous les bits "hôte" à 1). Si le réseau le plus spécifique a été généré en premier, cela vous amènera à générer deux LSA en une fois.

Comme exemple de l'algorithme, considérer son fonctionnement lorsque survient la séquence d'événements suivante dans un seul routeur (Routeur A).

(1) Le routeur A veut générer un LSA externe à l'AS pour [10.0.0.0,255.255.255.0] :
  (a) On utilise l'identifiant d'état de liaison 10.0.0.0.

(2) Le routeur A veut alors générer un LSA externe à l'AS pour [10.0.0.0,255.255.0.0] :
  (a) Le LSA pour [10.0.0,0,255.255.255.0] est généré à nouveau en utilisant un nouvel identifiant d'état de liaison de 10.0.0.255.
  (b) On utilise l'identifiant d'état de liaison 10.0.0.0 pour [10.0.0.0,255.255.0.0].

(3) Le routeur A veut alors générer un LSA externe à l'AS pour [10.0.0.0,255.0.0.0] :

(a) Le LSA pour [10.0.0.0,255.255.0.0] est généré à nouveau en utilisant un nouvel identifiant d'état de liaison de 10.0.255.255.
(b) On utilise l'identifiant d'état de liaison 10.0.0.0 pour [10.0.0.0,255.0.0.0].
(c) Le réseau [10.0.0.0,255.255.255.0] garde son identifiant d'état de liaison de 10.0.0.255.

Appendice F. Interfaces multiples dans le même réseau/sous-réseau

Il y a au moins deux façons de prendre en charge plusieurs interfaces physiques sur le même sous-réseau IP. Les deux méthodes vont interopérer avec les mises en œuvre de la RFC 1583 (et bien sûr du présent mémoire). Les deux méthodes sont brièvement résumées ci-dessous. On fait l'hypothèse que chaque interface a reçu une adresse IP distincte (autrement, la prise en charge de plusieurs interfaces est plus une question du niveau liaison ou d'ARP que d'OSPF).

Méthode 1 :
Faire fonctionner la pleine fonctionnalité OSPF sur les deux interfaces, en envoyant et recevant des hello, en arrosant, en prenant en charge les différentes interfaces et les FSM voisins pour chaque interface, etc. En faisant cela tous les autres routeurs sur le sous-réseau vont traiter les deux interfaces comme des voisins distincts, car les voisins sont identifiés (sur les réseaux en diffusion et NBMA) par leur adresse IP.

La méthode 1 a les inconvénients suivants :
(1) On augmente le nombre total de voisins et d'adjacences.
(2) On perd l'essai de bidirectionnalité sur les deux interfaces, car la bidirectionnalité est fondée sur l'identifiant de routeur.
(3) On doit considérer les deux interfaces ensemble durant l'élection du routeur désigné, car si on les déclare toutes deux comme étant simultanément le DR on va embrouiller le système de départage (qui est l'identifiant de routeur).

Méthode 2 :
Faire fonctionner OSPF sur une seule interface (appelons la l'interface primaire), mais inclure à la fois l'interface primaire et la secondaire dans le LSA de routeur.

La méthode 2 a les inconvénients suivants :
(1) On perd l'essai de bidirectionnalité sur l'interface secondaire.
(2) En cas de défaillance de l'interface primaire, il faut promouvoir l'interface secondaire au statut de primaire.

Appendice G. Différences avec la RFC 2178

La présente section répertorie les différences entre le présent mémoire et la RFC 2178. Toutes les différences sont rétrocompatibles. Les mises en œuvre du présent mémoire et celles des RFC 2178, 1583, et 1247 interopèrent.

G.1 Modifications de l'écoulement

Trois changements ont été apportés à la procédure d'arrosage de la Section 13.

Le premier changement est à l'étape 4 de la section 13. Maintenant, il est accusé réception des LSA MaxAge et ils ne sont ensuite éliminés que lorsque à la fois a) il n'y a pas de copie du LSA dans la base de données et b) aucun des voisins du routeur n'est dans les états Échange ou Loading. Dans tous les autres cas, le LSA de MaxAge est traité comme tous les autres LSA, on installe le LSA dans la base de données et on le diffuse sur les interfaces appropriées lorsque le LSA est plus récent que celui de la copie de la base de données (étape 5 de la Section 13). Ce changement affecte aussi les contenus du Tableau 19.

Le second changement est à l'étape 5a de la Section 13. La vérification MinLSArrival n'a de sens que pour les LSA reçus durant l'arrosage, et ne devrait pas être effectuée sur les LSA que le routeur génère lui-même.

Le troisième changement est à l'étape 8 de la Section 13. La confusion entre les routeurs au sujet de quelle instance de LSA est plus récente peut causer une inondation désastreuse dans un protocole d'état de liaison (voir [Ref26]). OSPF se garde de deux façons contre ce problème : a) le champ Age LS est utilisé comme un champ TTL dans l'arrosage, pour finalement retirer du réseau les LSA en boucle (voir au paragraphe 13.3), et b) les routeurs refusent d'accepter les mises à jour de LSA plus fréquemment qu'une fois toutes les MinLSArrival secondes (voir la Section 13). Cependant, il y a encore un cas dans la RFC 2178 où des désaccords sur le LSA qui est le plus récent peuvent causer beaucoup de trafic d'arrosage : répondre aux vieux LSA en rediffusant la copie de la base de données. Pour cette raison, l'étape 8 de la Section 13 a été amendée

pour ne répondre par la copie de la base de données que quand cette copie n'a pas été envoyée dans une Mise à jour d'état de liaison dans les dernières MinLSArrival secondes.

G.2 Changements des préférences de chemin externe

Il y a toujours la possibilité d'une boucle d'acheminement dans la RFC 2178 lorsque à la fois a) les liaisons virtuelles sont utilisées et b) le même chemin externe est importé par plusieurs ASBR, chacun étant dans une zone distincte. Pour régler ce problème, le paragraphe 16.4.1 a été révisé. Pour choisir l'ASBR/adresse de transmission correct, les chemins intra-zone à travers les zones non cœur de réseau sont toujours préférés. Cependant, les chemins intra-zone à travers la zone cœur de réseau (Zone 0) et les chemins inter-zones sont maintenant d'égale préférence, et doivent être comparés sur la seule base du coût.

Le raisonnement derrière ce changement est le suivant. Lorsqu'on utilise les liaisons virtuelles, un chemin intra-zone cœur de réseau pour un routeur peut se transformer en chemin inter-zone dans un routeur plusieurs bonds plus près de la destination. Et donc, les chemins intra-zone cœur de réseau et les chemins inter-zones doivent être d'égale préférence. On peut comparer leur coût en toute sûreté, préférer le chemin au plus faible coût, du fait des calculs du paragraphe 16.3.

Merci à Michael Briggs et Jeremy McCooey de UNH InterOperability Lab pour avoir soulevé ce problème.

G.3 Résolution incomplète des prochains bonds virtuels

Une des fonctions du calcul du paragraphe 16.3 est de déterminer le ou les prochains bonds réels pour les destinations dont le prochain bond a été calculé comme liaison virtuelle aux paragraphes 16.1 et 16.2. Après achèvement du calcul du paragraphe 16.3, tout chemin calculé aux paragraphes 16.1 et 16.2 qui a encore des prochains bonds virtuels non résolus devrait être éliminé.

G.4 Recherche de tableau d'acheminement

L'algorithme de recherche de tableau d'acheminement du paragraphe 11.1 a été modifié pour refléter les pratiques actuelles. L'entrée de tableau d'acheminement qui a la "meilleure correspondance" est maintenant toujours choisie pour être celle qui donne la correspondance la plus spécifique (la plus longue). Supposons par exemple qu'un routeur transmette des paquets à la destination 192.9.1.1. Une entrée de tableau d'acheminement pour 192.9.1/24 va toujours être une meilleure correspondance que l'entrée de tableau d'acheminement pour 192.9/16, sans considération des types de chemin des entrées de tableau d'acheminement. Noter cependant que lorsque plusieurs chemins sont disponibles pour une entrée de tableau d'acheminement donnée, les calculs des paragraphes 16.1, 16.2, et 16.4 donnent toujours les chemins qui ont le type de chemin préféré. (Les chemins intra-zone ont la plus grande préférence, suivis dans l'ordre par les chemins inter-zone, type 1 externe et type 2 externe ; voir la Section 11).

Considérations pour la sécurité

Tous les échanges de protocole OSPF sont authentifiés. OSPF prend en charge plusieurs types d'authentification ; le type d'authentification utilisé peut être configuré au niveau du segment de réseau. Un des types d'authentification d'OSPF, à savoir l'option d'authentification cryptographique, est estimé sûr contre les attaques passives et fournit une protection significative contre les attaques actives. Lorsqu'il utilise l'option d'authentification cryptographique, chaque routeur ajoute un "résumé de message" aux paquets OSPF qu'il émet. Le receveur utilise alors la clé secrète partagée et le résumé reçu pour vérifier que chaque paquet OSPF reçu est authentique.

La qualité de la sécurité fournie par l'option d'authentification cryptographique dépend complètement de la force de l'algorithme de résumé de message (MD5 est actuellement le seul algorithme de résumé de message spécifié) de la force de la clé utilisée, et de la mise en œuvre correcte du mécanisme de sécurité dans toutes les mises en œuvre OSPF qui communiquent. Elle exige aussi que toutes les parties maintiennent le secret de la clé secrète partagée.

Aucun des types d'authentification OSPF ne fournit la confidentialité. Pas plus qu'ils ne protègent contre l'analyse de trafic. La gestion des clés n'est pas traitée dans le présent mémoire.

Pour des informations complémentaires, voir aux paragraphes 8.1, 8.2, et à l'Appendice D.

Adresse de l'auteur

John Moy
Ascend Communications, Inc.
1 Robbins Road
Westford, MA 01886
USA
téléléphone : 978-952-1367
fax : 978-392-2075
mél : jmoy@casc.com

Déclaration complète de droits de reproduction