O Protocolo OSPF

Jailton Santos das Neves, Waldeck Ribeiro Torres
Departamento de Engenharia de Telecomunicações – Universidade Federal Fluminense
UFF – Niterói – RJ – Brasil
jaineves@ig.com.br, waldeck@spymac.com

Resumo. *Este trabalho fornece uma descrição simples de como o protocolo de roteamento OSPF trabalha, suas funcionalidades e estrutura, usos e limitações. Faremos também uma breve introdução ao MOSPF e do OSPF no ambiente do IP versão 6.*

1. Introdução

Protocolos são conjuntos de regras que regem a comunicação entre duas ou mais entidades para que seja possível a troca de informações e mensagens. Em redes de computadores, especialmente no tocante a este artigo, os protocolos de roteamento destinam-se à troca de informações entre roteadores, necessárias para a atualização dinâmica de suas tabelas de rotas, implementando um algoritmo específico de roteamento. Utilizando-se destes protocolos, os roteadores conectados que podem 'escolher' o melhor caminho para o destino dos dados, preenchendo suas tabelas de roteamento que acabam por descrever o estado da rede.

Dentre os protocolos de roteamento usados na Internet, podemos distinguir claramente dois tipos de protocolos: os protocolos de roteamento interno e os protocolos de roteamento externo. Os protocolos de roteamento externo são utilizados entre sistemas autônomos[1] da Internet para que se possa permitir a interconexão entre estas redes. Alguns protocolos de roteamento externo utilizam o algoritmo de vetor de distância, como o BGP, ou um protocolo mais simples como o EGP (usado para anunciar os endereços IP das redes internas para um roteador externo).

Dentre os protocolos de roteamento interno, temos o RIP (*Routing Information Protocol*) que utiliza o algoritmo vetor de distância. Este algoritmo é responsável pela construção de uma tabela que informa as rotas possíveis dentro de um AS.

O OSPF (Open Short Path First) é um outro protocolo de roteamento utilizado no interior de sistemas autônomos (Interior Gateway Protocol – IGP) para troca de informações de rotas dos pacotes IP. Ele surgiu em substituição ao protocolo RIP – Routing Information Protocol, mas diferente deste, o OSPF pode obedecer a uma hierarquia. O OSPF é um protocolo *link-state*, isto é, os roteadores rodando este protocolo trocam, entre si, informações sobre os estados dos enlaces de comunicação ligados às suas portas.

---

[1] Um Sistema Autônomo (AS) é um grupo de redes IP que é gerenciado por um ou mais operadores de rede que possuem uma clara e única política de roteamento.

Esse trabalho tem por objetivo mostrar como funciona o protocolo de roteamento OSPF e o MOSPF e suas principais características. Aproveitando a oportunidade falaremos um pouco do OSPF no IPv6.

O restante do texto está estruturado da seguinte maneira. Na seção 2 falaremos sobre o protocolo OSPF especificamente, seu funcionamento e faremos uma breve comparação com outros protocolos. Na seção 3 explicaremos com é realizada a troca de mensagens do protocolo OSPF. Na seção 4 falaremos sobre o protocolo MOSPF e na seção 5 vamos falar do OSPF no IPv6. Em seguida faremos uma conclusão sobre os assuntos abordados.

2. O Open Shortest Path First

O Open Shortest Path First (OSPF) implementa o algoritmo de estado de enlace e, nos dias de hoje, é o mais popular entre os IGPs. Seu surgimento deve-se principalmente a limitações dos demais protocolos tipo IGP, como é o caso do RIP. É chamado de OSPF, pois utiliza o algoritmo Shortest Path First para o cálculo dos melhores caminhos, que também é conhecido como Dijkstra.

Um de seus princípios de funcionamento é a utilização do conceito de ÁREA, ou seja, a definição de um conjunto de *roteadores* e redes em que é implementado o protocolo de *roteamento*. Isso faz com que o projeto de uma rede OSPF divida de forma hierárquica roteadores nas chamadas áreas, com o intuito de diminuir a complexidade e minimizar a comunicação entre roteadores. Necessariamente deve existir uma área central, chamada de Backbone (Área 0), que deverá atuar como elo de ligação com as demais áreas existentes. A comunicação entre as demais áreas deve ser feita obrigatoriamente através do Backbone. Um exemplo de rede OSPF dividida em áreas é ilustrado na figura 1:

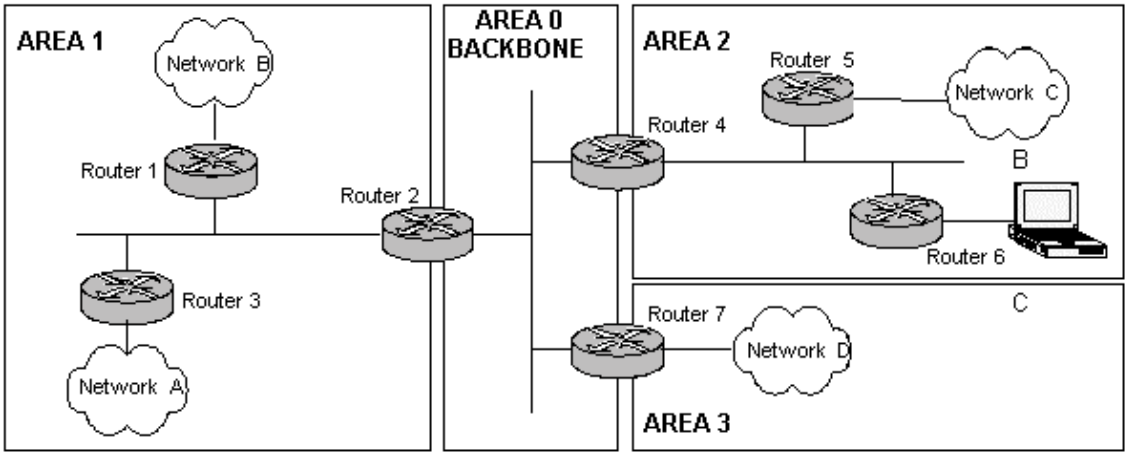

Figura 1: Exemplo de rede OSPF

Como a figura 1 demonstra, uma prática comum principalmente na área 0 é a ocorrência de roteadores com múltiplas interfaces estarem localizados em diferentes áreas, ou seja, cada interface em uma área diferente. Neste caso, o roteador irá manter uma base de dados da topologia para cada área. Esse é o caso dos roteadores 2, 4 e 7.

O protocolo OSPF funciona utilizando um algoritmo do tipo *Link State*, o que aumenta a sua complexidade, mas permite uma fácil e eficiente detecção de falhas. Este tipo de algoritmo caracteriza o estado de um enlace como a descrição da respectiva interface e sua relação com os seus *roteadores* vizinhos, esta descrição inclui o endereço IP da interface em causa, a respectiva máscara de rede, o tipo de rede a que está ligada, os *roteadores* ligados a essa rede etc. Este conjunto de informações constitui a base de dados de *link-state*. Permite ainda a autenticação das mensagens trocadas entre roteadores.

No início, cada *roteador* testa as suas ligações aos respectivos *roteadores* vizinhos, sincronizando em seguida a sua base de dados *link-state*, calculando então o melhor caminho para cada destino. Depois do OSPF em funcionamento, cada *roteador* repete periodicamente o teste às suas ligações, o que implica atualização da base de dados *link-state* e respectiva propagação para os *roteadores* da mesma área, assim como novo cálculo dos melhores caminhos. Com uma periodicidade, cada *roteador* propaga todos os estados dos enlaces (*link-state*) que conhece (e não só os que foram alterados) aos *roteadores* da sua área.

O cálculo do custo de um determinado caminho para um destino é um dos conceitos mais importantes neste tipo de protocolo sendo, aliás, um dos pontos fortes do OSPF. Neste protocolo, o custo de uma interface costuma ser inversamente proporcional à largura de banda da mesma, ou seja, o custo final de cada caminho está relacionado com a qualidade do enlace.

O OSPF possui uma série de proteções contra alguns perigos como erros de memória, falhas nos processos de *flooding* ou mesmo contra introdução voluntária de informação enganosa. São elas:

- Os pacotes de descrição da tabela são enviados de forma segura;
- Cada entrada é protegida por um contador de tempo e é removida da tabela se um pacote de atualização não chegar em um determinado tempo;
- Todas as entradas são protegidas por checksum;
- As mensagens podem ser autenticadas;
- O processo de *flooding* inclui notificação de reconhecimento hop by hop.

2.1. Vantagens do OSPF sobre o RIP

Veremos agora algumas vantagens do protocolo OSPF sobre o RIP, o que explica a preferência pelo OSPF em casos onde os roteadores suportam os dois protocolos.

· *Convergência rápida e sem loop*

Enquanto o RIP converge proporcionalmente ao número de nós da rede, o OSPF converge em uma proporção logarítmica ao número de enlaces. Isto torna a convergência do OSPF muito mais rápida. Além disso, no protocolo RIP, a mensagem é proporcional ao número de destinos, sendo assim se a rede é muito grande, cada mensagem terá de ser subdividida em vários pacotes, diminuindo mais ainda a velocidade de convergência.

· *Caminhos Múltiplos*

Nem sempre a melhor rota entre X e Y deve ser a única utilizada, pois isso pode implicar em sua sobrecarga[Moy95]. Análises matemáticas provaram que a divisão do tráfego em duas rotas é mais eficiente. Por isso o OSPF utiliza esse método de divisão de caminhos. Essa divisão é realizada por um algoritmo muito complexo, pois, como dificilmente uma fonte e um destino têm duas rotas possíveis exatamente iguais, é feita uma análise se as rotas são suficientemente iguais. Além disso, deve-se decidir a fração do tráfego que deve ser enviado em cada uma delas. Para que tenhamos uma melhor compreensão usaremos o exemplo da figura 2:

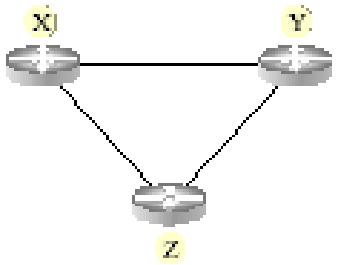

Figura 2: Exemplo de rede com vários caminhos

Em se tratando do tráfego entre X e Z, seria razoável se mandássemos 2/3 do pacote pelo caminho mais curto e 1/3 por Y. Mas isto gera um conflito se levarmos em consideração o tráfego entre X e Z, que ao enviar por Y, seria formado um *loop*. Para evitar isto, foi aplicada a seguinte regra: Um pacote que iria de X para Y, só pode passar por Z se a distância entre Z e Y for menor que a distância entre X e Y. Com isso, determinamos todas as rotas secundárias que alcançarão um determinado nó.

Outras vantagens que o OSPF tem sobre o RIP:

- As rotas calculadas pelo algoritmo SPF são sempre livres de loops.
- O OSPF pode ser dimensionado para interconexões de redes grandes ou muito grandes.
- A reconfiguração para as alterações da topologia de rede é muito rápida, ou seja, o tempo de convergência da rede, após alterações na topologia é muito menor do que o tempo de convergência do protocolo RIP.

- O tráfego de informações do protocolo OSPF é muito menor do que o do protocolo RIP.
- O OSPF permite a utilização de diferentes mecanismos de autenticação entre os roteadores que utilizam OSPF.
- O OSPF envia informações somente quando houver alterações na rede e não periodicamente.

2.2. Especificações do protocolo OSPF

Descreveremos sucintamente a seguir as especificações do protocolo OSPF na sua segunda versão de acordo com as especificações contidas no seu Request For Comments [RFC 2178]

2.2.1. O cabeçalho dos pacotes

Cada pacote OSPF possui um cabeçalho comum de 24 bytes. Este cabeçalho contém todas as informações necessárias para determinar se o pacote deve ser aceito para processamento ou não, a figura 3 detalha o formato deste cabeçalho, indicando os campos que o compõem e mais abaixo as suas descrições.

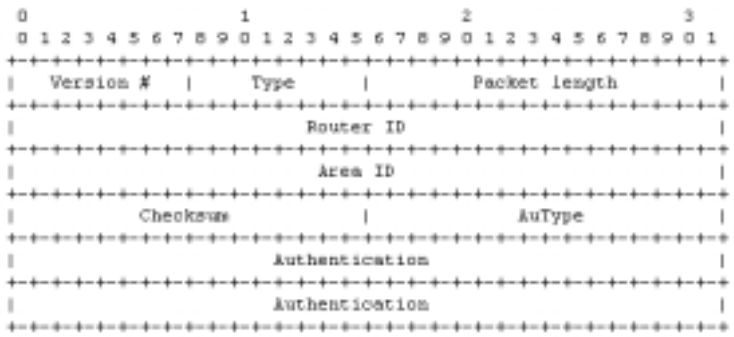

Figura 3: Cabeçalho de um pacote OSPF

Version # : Indica o número de Versão do Protocolo.
Type: Indica o tipo de pacote enviado, o qual pode ser:

Tipo	Descrição
1	Hello
2	Descrição da base de Dados
3	Requisição do estado do link
4	Atualização do estado do link
5	ACK do estado do link

Packet length: Indica o comprimento do pacote, incluindo o cabeçalho OSPF.
Router ID: Indica o ID do roteador de origem do pacote.

Área ID: Identifica a área a qual este pacote pertence – Todos os pacotes OSPF são associados a uma determinada área.
Checksum: Contém o Checksum de todo o conteúdo do pacote excetuando o campo de 64 bits de autenticação. O valor do checksum é calculado como um número de 16 bits complementar da soma de todas as palavras de 16 bits do pacote. Se o comprimento do pacote não for um múltiplo de 16, é feito um preenchimento com bytes zero antes do cálculo.
AuType : Identifica o esquema de autenticação usado no pacote
Authentication: Um campo de 64 bits usado pelo esquema de autenticação.

2.2.2. O pacote HELLO

As mensagens HELLO são pacotes OSPF do tipo 1, estes pacotes são enviados periodicamente em todas as interfaces, para que se possa estabelecer e manter ligações entre a vizinhança. Os pacotes HELLO são multicast nas redes físicas que possuam capacidade de broadcast ou multicast, habilitando com isso o conhecimento dinâmico dos roteadores vizinhos.

Todos estes roteadores conectados em uma rede comum devem compartilhar determinados parâmetros de rede, tais como máscara, intervalo de envio de mensagem HELLO, etc. Estes parâmetros estão incluídos nos pacotes HELLO, de outra forma parâmetros diferentes não possibilitariam a formação de relação entre os roteadores. A figura 4 mostra o formato e os campos do pacote HELLO juntamente com o cabeçalho comum.

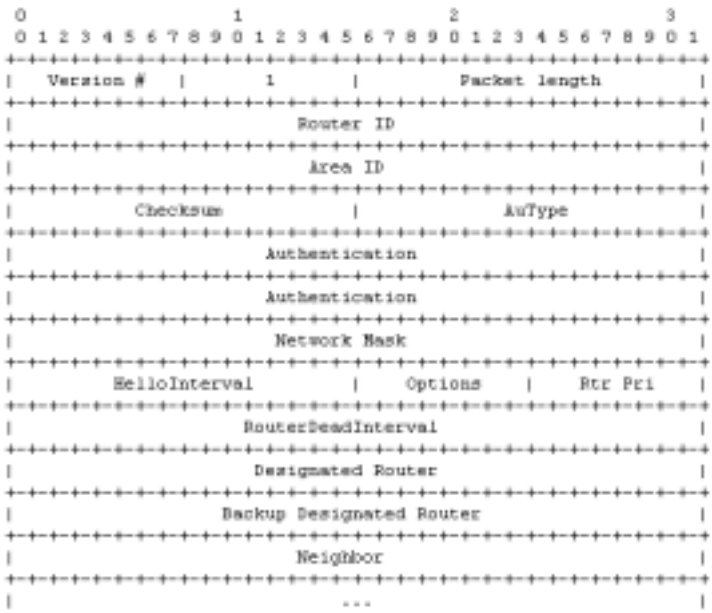

Figura 4: Pacote HELLO

Network mask: Indica a máscara de rede associada à interface.
HelloInterval: Indica o tempo, em segundos, entre os envios dos pacotes HELLO.

Options: Indica as capacidades opcionais suportadas pelo roteador.
Rtr Pri: Indica a prioridade do roteador. Ele é usado na seleção do roteador desejado caso haja um backup. Se setado como zero, o roteador não participa da seleção.
RouterDeadInterval: Indica o tempo, em segundos, antes de declarar o roteador como fora da rede ou desabilitado.
Designated Router: Mostra a identidade (IP) do roteador designado na adjacência. Se setado como 0.0.0.0 significa que não há roteador designado.
Backup Designated Router: Mostra a identidade (IP) do roteador backup designado. Se setado como 0.0.0.0 significa que não há roteador backup designado na adjacência.

2.2.3. O pacote de descrição de base de dados

Os pacotes de descrição de base de dados do protocolo são pacotes “tipo 2”. Estas mensagens são trocadas quando uma adjacência começa a se formar, eles descrevem o conteúdo da topologia. Múltiplos pacotes podem descrever a base de dados, neste caso uma coleta de respostas enviadas por outros roteadores é utilizada: um dos roteadores é designado como mestre e um outro escravo. O roteador mestre envia mensagens de descrição de base de dados (coleta) que são reconhecidas pelas mensagens de descrição enviadas pelo roteador escravo (respostas). Estas respostas são associadas às coletas via número de seqüência DD. A figura 5 exibe o formato desse pacote.

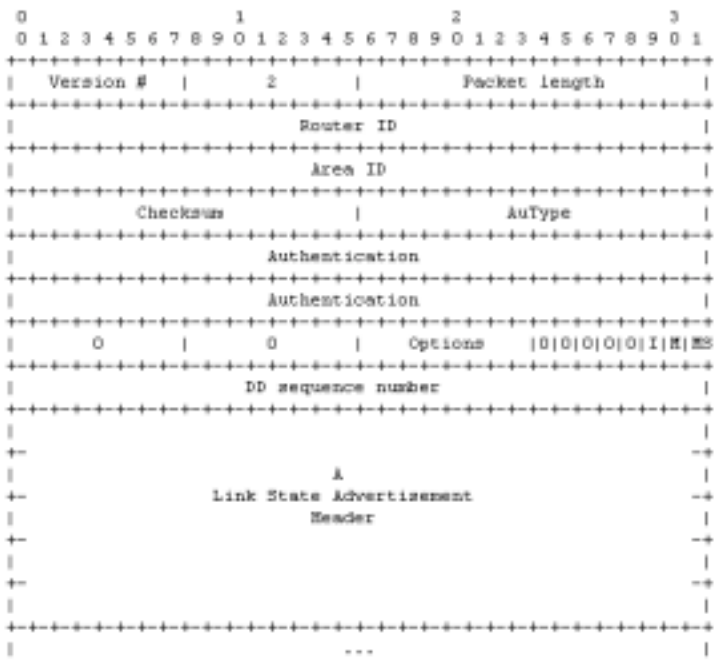

Figura 5: Pacote de descrição da base de dados

O formato do pacote de descrição de base de dados é muito similar aos pacotes de requisição de estado de link e ACK de requisição de estado de link, a parte principal deste pacote é composta pela informação de uma parte da base de dados da topologia de rede. A seguir descrevemos os campos desta mensagem, que inclui o cabeçalho.

0: Este é um campo reservado e seu valor fixo é Zero.
Options: Indica as capacidades opcionais suportadas pelo roteador. (Type of Service)

0	0000 normal service
2	0001 minimize monetary cost
4	0010 maximize reliability
6	0011
8	0100 maximize throughput
10	0101
12	0110
14	0111
16	1000 minimize delay
18	1001
20	1010
22	1011
24	1100
26	1101
28	1110
30	1111

I-bit: O “Bit Init” quando setado para 1 significa que o pacote é o primeiro da seqüência.
M-bit: O “Bit mais” quando setado em 1 indica que mais pacotes na seqüência estão por vir.
MS-bit: Este bit indica se o roteador é mestre (1) ou escravo (0) durante o processo de troca de mensagens.
DD sequence number: Indica o número de seqüência das mensagens enviadas. Ele é incrementado até que toda a descrição da base de dados tenha sido enviada.

O resto do pacote consiste na lista parcial de partes da base de dados, o cabeçalho de divulgação de estado de link (LSA – Link State Advertisement) será discutido mais adiante.

2.2.4. O Pacote de requisição de estado de link

Os pacotes de requisição de estado de link são do tipo 3. Após trocar pacotes de descrição de base de dados com os roteadores adjacentes, o roteador poderá encontrar partes da topologia que estejam desatualizadas. Os quadros de requisição de estado de link são usados para requisitar aos roteadores vizinhos, informações de base de dados para atualizar a sua própria caso esta esteja desatualizada. O envio destes pacotes é o último passo para configurar as adjacências. A figura 6 mostra o formato do pacote de requisição de estado de link.

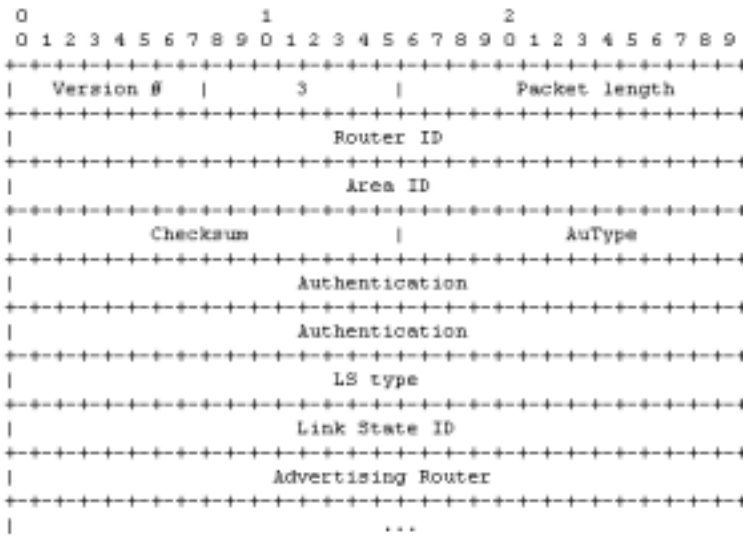

Figura 6: Pacote de requisição de estado de link

Um roteador que solicita um pacote de requisição de estado de link conhece as instâncias das partes da base de dados da topologia que estão sendo necessárias, definidas pelo LS sequence number, LS checksum, e LS age, ainda que estes campos não estejam especificados no pacote. Assim o roteador pode receber instâncias mais recentes em resposta a sua solicitação.

2.2.5. O Pacote de atualização de estado de link

Estes pacotes implementam a distribuição dos estados de links, cada pacote carrega uma coleção de informações de estado de link de um salto além de sua origem. Isto significa que muitas publicações de estado de link podem estar inseridas em um único pacote.

Os pacotes de atualização de estado de link são multicast em seus domínios físicos que suportam multicast/broadcast. Para ter certeza que esta “inundação” de pacotes de atualização seja confiável, os pacotes são confirmados com seus respectivos pacotes de confirmação. A figura 7 exibe o formato desse pacote.

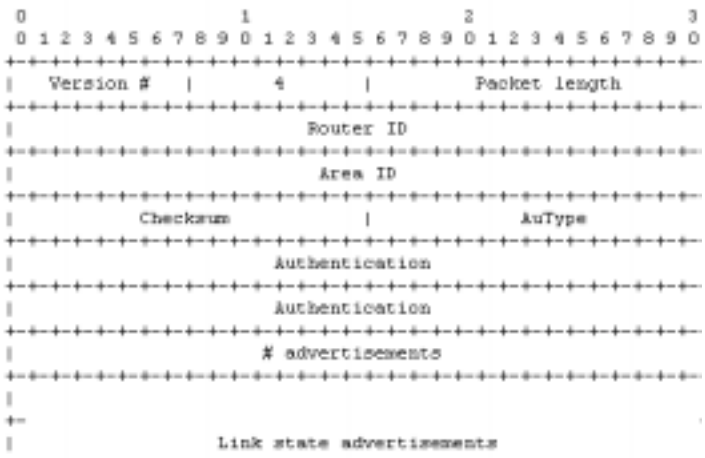

Figura 7: Pacote de atualização de estado de link

2.2.6. O Pacote de ACK do estado de link

Para assegurar a confiabilidade da publicação dos pacotes de estado de link, eles são explicitamente confirmados. Estas confirmações são completadas através da troca dos pacotes de confirmação, mesmo que seja usada uma única confirmação para múltiplos links de um mesmo pacote. Dependendo do estado da interface que enviou e da fonte das informações que estão sendo confirmadas, os pacotes são mandados tanto para o endereço multicast AllSPFRouters e AllDRouters, ou como uma mensagem unicast. A figura 8 exibe o formato desse pacote.

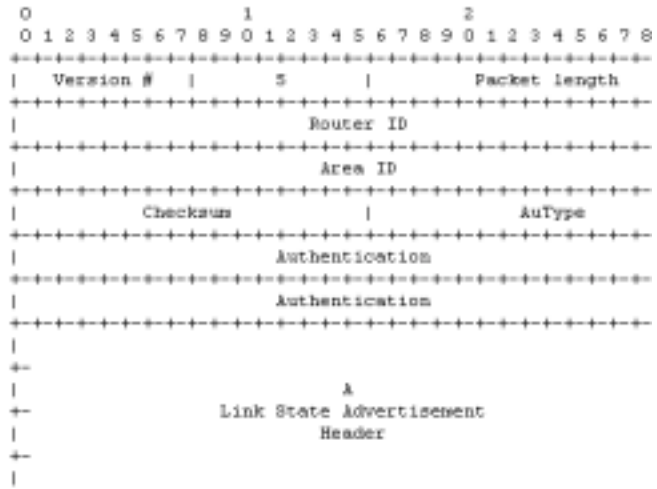

Figura 8: Pacote de ACK do estado de link

3. Troca de Mensagens do Protocolo OSPF

O Fato dos roteadores serem vizinhos não é o suficiente para garantir a troca de atualizações de link states, é necessário que se formem adjacências para as trocas de atualizações de link states. Uma adjacência é uma forma avançada de relacionamento entre roteadores vizinhos de uma mesma área, ele é formado por roteadores que "desejam" trocar informações de roteamento depois de negociar dados para montagem de suas próprias tabela de rotas. Os roteadores atingem o status de Full da adjacência quando eles terminam a sincronização do banco de dados de link-state, conforme descreveremos abaixo.

O Tipo de interface tem papel crucial na maneira como as adjacências são formadas, por exemplo: Vizinhos cujo link é um "ponto-a-ponto" sempre tentarão se tornar adjacentes, enquanto roteadores cujas interface sejam Ethernet somente se tornarão adjacentes apenas se houver um um subsistema de vizinhança ligados naquela interface.

Uma vez que o roteador "decida" formar uma adjacência com um vizinho, ele inicia a troca de uma cópia de seu banco de dados de Link-State. Os vizinhos, um após o outro, trocam cópias de seu banco de dados de Link-State com o roteador que iniciou o processo, e após os passos descritos abaixo ele se torna um roteador adjacente.

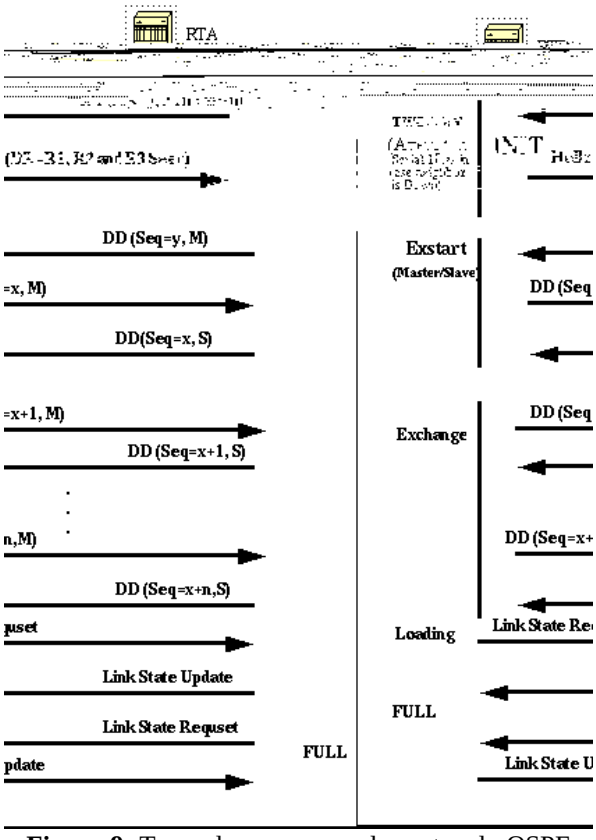

Figura 9: Troca de mensagens do protocolo OSPF

Na Figura 9, roteadores no mesmo segmento passam por uma série de estados antes de formar uma adjacência com sucesso. A eleição do roteador designado (DR) e a sua vizinhança são feitos através dos pacotes HELLO. Toda vez que um roteador vê a si mesmo na troca de mensagens HELLO, o enlace entra no estado "2-Way" e neste ponto a eleição do DR e o Backup DR acontece. O roteador continua formando as adjacências mesmo se estes estiverem conectados via um enlace ponto-a-ponto ou se eles forem um DR e Backup DR respectivamente.

No estado “Exstart”, os dois vizinhos formam um relacionamento mestre/escravo onde eles trocam um número de seqüência. Este número de seqüência é utilizado para detectar LSA´ s velhos ou duplicados.

No estado “Exchange", os “Database Description Packets”(DD) são trocados. Para estes pacotes são utilizados LSA “Abreviados” no formato de cabeçalho link-state, este cabeçalho possui informação suficiente para identificar o link. O nó mestre envia os pacotes DD que são confirmados com os pacotes DD vindos do nó escravo. Todas as adjacências no estado “Exchange” são utilizadas no processo de “flooding”. Estas adjacências são completamente capazes de transmitir e receber todos os tipos de protocolos de roteamento OSPF.

No Estado “Loading”, requisições “link-state” são enviadas para os vizinhos, que solicitam por LSA´s mais recentes que foram “descobertos” e ainda não enviados. Neste momento cada roteador monta uma lista de LSA´s necessários para montar a sua adjacência mais atualizada. Uma lista de retransmissão é mantida para que se tenha certeza que cada LSA seja confirmado.

No estado “FULL” os roteadores vizinhos já são “adjacentes” na sua base de dados, ou seja, os banco de dados internos de uma área comum são exatamente iguais entre roteadores adjacentes. Cada pacote “LSA” possui um tempo de vida que é periodicamente decrementado enquanto seus dados são válidos no banco de dados. Quando este tempo de vida expira, ele é descartado do banco de dados ou descartado também quando ele não está na lista de retransmissão da vizinhança.

4. O Multicast OSPF (MOSPF)

A extensão *multicast* para o protocolo de roteamento *IP Open Shortest Path First* (OSPF) dentro de um mesmo sistema autônomo é denominada *Multicast Open Shortest Path First* (MOSPF). Ele roteia mensagens, através dos caminhos mais curtos, o MOSPF depende do uso do OSPF, além de ser aconselhável para ambientes com poucos pares (origem, grupo destino) ativos, devido a restrições de processamento. Uma rede de roteadores utilizando MOSPF pode enviar pacotes *multicast* diretamente, enviando não mais que uma cópia por cada enlace, e sem a necessidade de túneis. O MOSPF apresenta suporte para *roteamento* hierárquico. Todas as estações da Internet estão particionadas em sistemas autônomos (AS) – conforme figura 10, onde cada AS é ainda dividido em subgrupos denominados áreas.

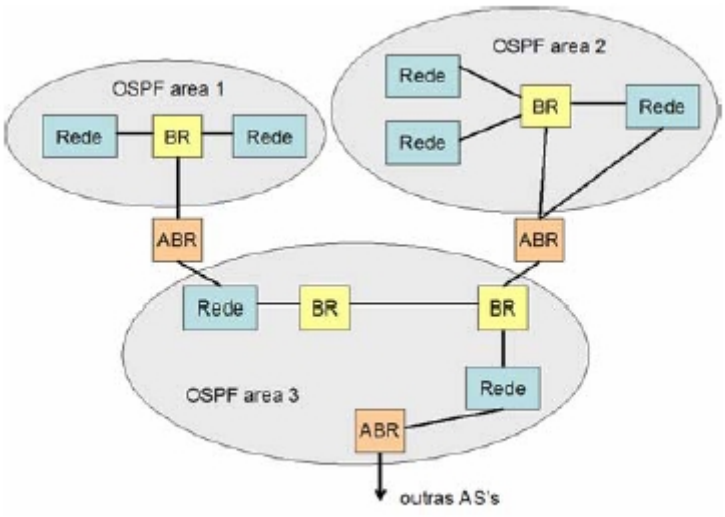

Figura 10: Exemplo de AS´s particionados

O MOSPF transmite os datagramas IP *multicast* da origem para os vários membros do grupo sem formar laços, cada roteador MOSPF, periodicamente, envia informações sobre os componentes dos grupos, para os outros roteadores. Dessa forma, todos os roteadores ficam sabendo da localização dos componentes de cada grupo, formando um mapa completo das ligações nas redes. Tendo as informações sobre os estados das ligações, o roteador constrói, a árvore das distâncias mais curtas de um computador a todos os outros computadores de um dado grupo, através do algoritmo de Dijkstra. Esta árvore tem como raiz o nó origem do datagrama, e todos os “braços” terminam em membros do grupo.

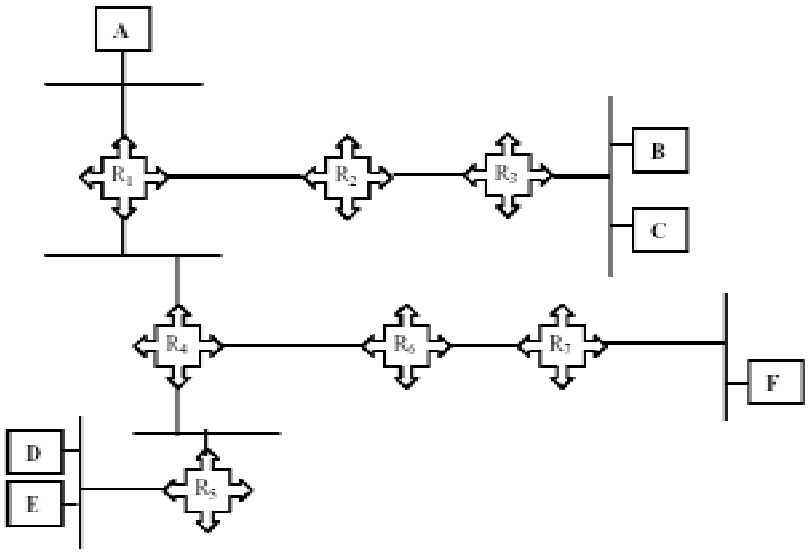

Figura 11: Exemplo de topologia de rede

De acordo com a figura 11, supondo haver um grupo G formado por B, C, D, E e F, o roteador R1 através do IGMP, tem como saber que computadores pertencem ao grupo; um mesmo computador pode participar de um ou mais grupos. Então, R1 calcula a árvore e verifica que atinge R5 via R4, R7 via R4 e R3 via R2. O roteador R4 calcula a sua árvore e nota que atinge R7 via R6.

Similarmente, R2 determina que atinge R3 diretamente. R6 determina que atinge R7 diretamente. Note que cada um dos roteadores calcula a mesma árvore.

Com essa informação sobre os componentes do grupo, o roteador pode remover roteadores da árvore, que não possuam ninguém do grupo, evitando envios de pacotes desnecessários.

Conseqüentemente, a atualização periódica das informações de roteamento (trocadas pelos roteadores), pode resultar em restrições de escala na rede. O estado de cada árvore é mantido em cache. Tais árvores devem ser calculadas novamente, caso ocorram mudanças de topologia na rede.

Seguindo a filosofia *multicast*, o datagrama é replicado apenas quando surge uma divisão, um braço, na árvore. Este esquema de roteamento, onde o caminho dos datagramas depende da origem e dos destinos, já que a árvore possui raiz na origem, é denominado *source/destination routing*. Ele é diferente da maioria dos algoritmos de roteamento *unicast*, incluindo o OSPF, que se baseiam somente no destino do datagrama ao fazer o roteamento. A necessidade de considerar a origem para tomar as decisões do roteamento causa maior quantidade de cálculos de roteamento, porém resulta em melhores caminhos em termos de utilização da rede e atraso para membros individuais do grupo. O protocolo, porém, não necessariamente otimiza o uso da rede como um todo.

A figura 12 apresenta uma rede onde é realizada uma transmissão de um datagrama originado do nó O para os membros do grupo G, onde o caminho dos datagramas está indicado com as flechas. Se fosse, porém utilizado o caminho que otimizasse mais a rede, o datagrama seria transmitido do roteador R4 para o roteador R2, onde seria enviado para a rede local e para o roteador R3, que o transmitiria para as redes locais D e E.

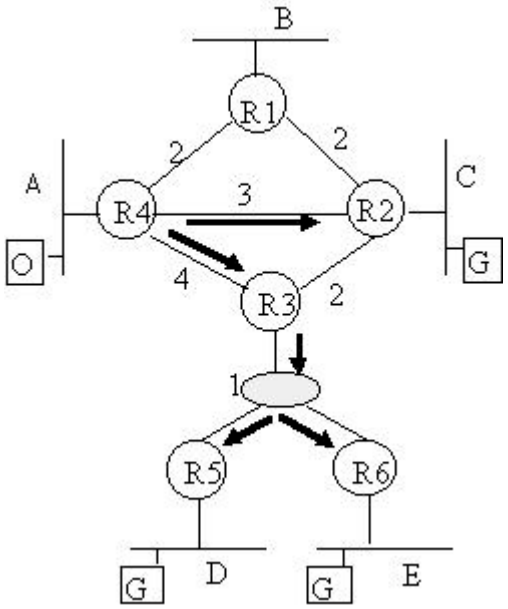

Figura 12 - Transmissão de um datagrama no MOSPF

Como havíamos comentado antes, o roteador MOSPF utiliza o protocolo IGMP (Internet Group Management Protocol) que é o protocolo usado para gerência de grupos multicast, para estabelecer a localização de membros de grupos, enviando mensagens IGMP do tipo Host Membership Query e recebendo mensagens Host Membership Report como resposta. De posse destas informações, o roteador MOSPF as distribui por todo o Sistema Autônomo através do envio de um novo tipo de anúncio de estado de enlace, o *group-membership-LSA*, que indica os pedaços do mapa da rede que possuem membros do grupo.

Utilizando o mapa, o roteador MOSPF calcula, na primeira vez que um datagrama multicast com uma dada origem e destino é recebido, a árvore com raiz na origem de menor caminho para o datagrama. As ramificações da árvore que não possuem membros são eliminadas, de modo que o datagrama não é enviado para onde não é necessário. O resultado deste cálculo da árvore é então armazenado para uso nos datagramas do grupo em questão que forem recebidos posteriormente.

O cálculo de roteamento do MOSPF é muito similar ao cálculo do roteamento *unicast* utilizado no OSPF, ambos utilizando o algoritmo *Dijkstra* para calcular as árvores de menor caminho. No MOSPF, entretanto, existem potencialmente muitas diferentes árvores calculadas, possivelmente uma para cada combinação da origem do datagrama e

destino. Assim, existem mecanismos para garantir que, dado datagrama, todos os roteadores MOSPF calculem a árvore de menor caminho absolutamente iguais, o que é essencial para a correta transmissão de datagramas de difusão seletiva.

O MOSPF possui algoritmos para transmitir datagramas multicast entre áreas OSPF e um algoritmo para importar datagramas multicast de outro Sistema Autônomo. O compartilhamento de carga, enviando datagramas através de múltiplos caminhos com mesmo custo, não é suportado, já que entre a origem de um datagrama e um particular membro do grupo deve existir apenas um caminho. Isto ocorre pela natureza do roteamento da difusão seletiva: a fim de evitar replicação dos datagramas, cada roteador deve conhecer por qual interface um dado datagrama será recebido, e deve descartar os datagramas recebidos por outras interfaces.

Para transmissões além do limite de uma área OSPF, novos mecanismos são necessários. Isto acontece porque um mapa de uma área OSPF não é visível externamente a aquela área, complicando a construção das árvores baseadas na origem, além de que um membro de um grupo não pode ser livremente anunciado além dos limites da área.

As áreas OSPF podem ser vistas como organizadas em uma hierarquia de dois níveis, onde o nível superior corresponde à área do backbone. Para distribuir os *group-membership-LSA*s MOSPF, o grupo é anunciado para a área do backbone, de forma que o backbone possua completo conhecimento dos grupos de todas as áreas. Entretanto, a informação de associação aos grupos não é anunciada de volta para as áreas que não são backbone, que desta forma não possuem conhecimento dos grupos das outras áreas. Isso reduz o tamanho do banco de dados dos estados dos enlaces da área. Para compensar, o conceito de roteadores recebedores de anúncios multicast é introduzido. Com o mecanismo, tais roteadores recebem todos os datagramas de difusão seletiva, independente do destino. Assim, para habilitar a entrega dos datagramas além dos limites da área, todos roteadores MOSPF conectando áreas não-*backbone* ao *backbone* se anunciam como recebedores de anúncios de difusão seletiva para as áreas não-*backbone*.

O cálculo de caminhos para os datagramas que ultrapassam os limites do Sistema Autônomo é realizado de forma análoga. Quando um datagrama é originado de um outro Sistema Autônomo, sua vizinhança é aproximada pelos *AS-external-LSA*s. Adicionalmente, roteadores desejando enviar datagramas para outro Sistema Autônomo se anunciam como recebedores de anúncios de difusão seletiva, e recebem assim os datagramas independentes dos destinos destes.

No MOSPF, assim como no OSPF, os datagramas são marcados com a sua classificação do *Type of Service* (TOS), baseada em um dos cinco valores mutuamente exclusivos *minimize delay*, *maximize throughput*, *maximize reliability*, *minimize monitary cost* e *normal service*. O caminho do datagrama multicast no MOSPF pode variar de acordo com a classificação TOS utilizada. Por exemplo, um tráfego multicast sensitivo ao *delay* (retardo) pode seguir rotas diferentes de uma aplicação multicast de *alto throughput* (alta vazão). A classificação TOS no protocolo MOSPF é, assim como no OSPF

opcional, e roteadores que a suportam podem ser misturados livremente como os que não a suportam.

Quando isso é feito, todos os roteadores irão interoperar no roteamento de datagramas *unicast*, que não é afetado pelos roteadores MOSPF. Esta possibilidade de misturar ambos tipos de roteadores habilita a fase de introdução da capacidade de difusão seletiva em uma rede. O MOSPF suporta todos os tipos de rede que são suportadas pelo protocolo OSPF: redes multicast (como Ethernet), redes ponto-a-ponto e redes de multiacesso que não suportam multicast. Estas últimas, porém, não poderão possuir membros locais.

O OSPF em IPv6

O IPv6 usa um endereçamento de 128 bits. Na realidade antes de se chegar a este valor, algumas entidades defendiam valores de endereçamento que iam de 1 a 20 Bytes, o endereçamento de 128 Bits foi finalmente escolhido por dois motivos. Este valor pode ser utilizado para "manusear" mais facilmente a complexidade da Internet pela adição de camadas lógicas e por que um endereçamento muito longo pode fazer com que desenvolvedores, por facilidade de programação, tendem a optar pelo tamanho máximo de endereçamento [Huit96] tendo por conseqüência algoritmos de rede mais lentos.

De um modo geral o OSPFv3 foi desenvolvido para adicionar suporte para o IPv6, a partir do protocolo OSPF tal como detalhado na sua especificação[RFC 2740], a maioria das configurações e comandos operacionais é essencialmente igual aos utilizados no OSPFv2, dentre eles podemos destacar:

- Todos os comandos operacionais e de configurações do OSPFv3 incluem o identificador "ospf3" no lugar da opção "ospf". Por exemplo: "show ospf database" para OSPFv2 passa a ser: "show ospf3 database" no protocolo OSPFv3.
- OSPFv3 Router ID´s, Área ID´s, e os LSA link-state IDs continuam com o tamanho de 32bits do protocolo OSPFv2 para IPv4.
- Todas as configurações opcionais do protocolo OSPFv2 para IPv4, tal como o "not-so-stubby-areas" (NSSA), são suportadas no OSPFv3 para IPv6.

Contudo existem algumas mudanças significativas que devem ser levadas em consideração quando se trata do protocolo para a versão IPv6, conforme listamos abaixo:

- Os "Router link-state advertisements" (LSA´s) e os LSA´s de rede não carregam mais as informações de prefixo, no OSPFv3 estes LSA´s somente transportam informações de topologia de rede. Com esta remoção de endereçamento o OSPFv3 passa a ser independente de protocolo

- Novos e modificados LSA´s foram criados para gerenciar o fluxo de endereços e prefixos IPv6 na rede do protocolo OSPFv3.

Os LSA´s que foram modificados foram:

- LSA de prefixo Inter Área — Ele substitui o “Network Summary” ou o LSA do tipo 3.
- Roteador-Inter Área — Ele substitui o LSA do tipo 4 (Autonomous System Boundary Router (ASBR)).
- Os “Label-switched” (LSP´s) e o planejamento de tráfego deixam de ser suportados no OSPFv3.
- Os Roteadores vizinhos são sempre identificados por um “Router ID” de 32bits no OSPFv3.

Os LSA´s que foram adicionados para o OSPFv3 foram:

- Link LSA — Este LSA tem ação local e não se estende além do link no qual ele está associado. A idéia do “link LSA” é prover o endereço IPv6 do link local para os roteadores vizinhos, informar os quais os outros roteadores associados estão disponíveis e fornecer informações para os LSA´s de rede (network LSA´s). Em todas as interfaces OSPF, excetuando links virtuais, os pacotes são enviados utilizando o endereço local da interface como o endereço de origem (O endereço de link local é um endereço IPv6 que começa com os primeiros 10 bits setados para 1111111010, ou mais comumente no formato hexa: fe80) [RFC2373].
- LSA Prefixo-Intra-Área - Este LSA transporta toda informação de prefixo IPv6 para todos os roteadores OSPFv3 dentro de uma área (No IPv4 esta informação é transportada pelo LSA de roteamento e de rede).
- O OSPFv3 agora passa a rodar baseado em link e não mais baseado em Subnet IP

Como os endereços de link locais do IPv6 passaram a ser utilizados para as trocas de informações entre vizinhos (exceto sobre links virtuais), o escopo de “flooding” dos LSA´s foram divididos em três categorias para o OSPFv3:

- Escopo Link-local — Os pacotes OSPFv3 são espalhados para os membros do link.
- Escopo de área — Os pacotes OSPFv3 são espalhados para todos os membros de uma mesma área OSPFv3.
- Escopo do Sistema Autônomo — Os pacotes OSPFv3 são espalhados para todos os membros de um mesmo Sistema Autônomo.

Autenticação foi removida do protocolo OSPFv3 que agora passa a confiar no “Authentication Header (AH)” e no “Encapsulating Security Payload” (ESP). Porções (IPSec) “IP Security protocol” para todas as tarefas de autenticação do IPv6.

5. Conclusão

Nessa monografia abordamos os protocolos de roteamento OSPF e MOSPF. Foi visto o funcionamento de seus algoritmos e suas aplicações além deles explicitamos sobre o funcionamento do OSPF no IPv6.

Podemos verificar que o protocolo OSPF tem diversas vantagens sobre o protocolo RIP, entretanto o RIP possui uma fácil implementação, além de utilizar menos processamento para os roteadores, sendo implementado com bons resultados para redes de pequeno porte. Para redes maiores o OSPF leva a vantagem no tempo de convergência e na escolha das rotas, sendo mais vantajoso neste caso.

Ainda existe outro problema para a implementação do protocolo OSPF; alguns roteadores, principalmente os de menor poder de processamento e os mais antigos, não estão aptos a utilizar o protocolo OSPF, enquanto o protocolo RIP é implementado pela grande maioria dos roteadores.

Vimos também que o MOSPF utiliza princípios parecidos com os do OSPF só que para pacotes enviados em multicast, usando o conceito de árvores onde o topo dela é o nó principal de onde é originado o datagrama.

Finalizando, mostramos que, com a chegada do IPv6 os problemas com endereçamento IP na Internet, que cresceu de forma surpreendente, estão com os dias contados. Mostramos que as mudanças que o modo de funcionamento do OSPF terão com seu uso sob IPv6 não afetarão a sua funcionalidade, permanecendo assim como um dos mais eficientes protocolos utilizados.

6. Referências

- **[CISCO]** System, Cisco "**http://www.cisco.com**" Document ID: 13699.
- **[Huit96]** Huitema, Christian "***IPv6, The New Internet Protocol***" 1996, Prentice Hall, ISBN 0-13-241936-X.
- **[Moy95]** J. Moy "***OSPF Version 2***" 11/22/1995, Internet-Draft.
- **[RFC 2740]** RFC 2740 OSPF for IPv6 "**http://www.rfc-archive.org/**", Dec 1999.
- **Tanembaum, A.** Redes de Computadores, 4^{A}. Edição. Ed. Campus, 1998.
- **Kurose, James F.** Redes de Computadores e a Internet: uma nova abordagem – tradução Arlete Simille Marques, primeira edição – SP: Addison Wesley, 2003.