UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
ESPECIALIZAÇÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

BRUNO LEONARDO VITÓRIA

ANÁLISE E SIMULAÇÃO DE UMA REDE IPv6 COM ROTEAMENTO OSPFv3

MONOGRAFIA

CURITIBA

2013

BRUNO LEONARDO VITÓRIA

ANÁLISE E SIMULAÇÃO DE UMA REDE IPv6 COM ROTEAMENTO OSPFv3

Monografia apresentada como requisito parcial para obtenção do grau de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná - UTFPR.

Orientador: Prof. Dr. Augusto Foronda

CURITIBA

2013

Este trabalho é dedicado aos meus pais, Roberto e Marlene
cujo amor e sabedoria me inspiram
a melhorar dia após dia.

AGRADECIMENTOS

– Dedico este trabalho primeiramente a Deus, pois sem Ele, nada seria possível e não estaríamos aqui reunidos, desfrutando, juntos, destes momentos que nos são tão importantes;

– A minha família, pelo incentivo e segurança que me passaram durante todo esse período;

– A minha namorada Marina Alves de Quadras, pela compreensão e carinho durante esse momento de esforço contínuo;

– Ao Prof. Dr. Augusto Foronda, por toda dedicação, paciência e estímulo em sua orientação;

– A todos os professores do Curso de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes da UTFPR;

– Aos amigos de curso, pelo agradável convívio nesse período de especialização;

– Ao amigo Felipe Dri Ficagna, pela valiosa amizade que permanece desde longa data;

– Ao amigo Glauber Elicker, pela valiosa amizade e caronas gratuitas para Curitiba;

– A todos que direta ou indiretamente contribuíram para a realização deste trabalho.

" *Não tentes ser bem sucedido, tenta antes ser um homem de valor.*"
Albert Einstein.

RESUMO

VITÓRIA, Bruno Leonardo. ANÁLISE E SIMULAÇÃO DE UMA REDE IPv6 COM ROTEAMENTO OSPFv3. 39 f. Monografia – Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

O presente trabalho trata de uma análise e simulação de uma rede IPv6 com roteamento OSPFv3. Apresenta uma análise do protocolo IPv6, contendo uma descrição de funcionamento e os principais motivos para sua utilização. Ainda sobre IPv6, apresenta o cabeçalho do protocolo, os cabeçalhos de extensão e o endereçamento utilizado nesse protocolo. Sobre o protocolo OSPFv3, apresenta a descrição de funcionamento, a estrutura de dados, o processamento de pacotes, a tabela de roteamento e as *Link State Advertisements* (LSAs) desse protocolo. Finaliza com uma simulação prática, utilizando os dois protocolos analisados.

Palavras-chave: IPv6, OSPFv3, análise, simulação.

ABSTRACT

VITÓRIA, Bruno Leonardo. ANALYSIS AND SIMULATION OF AN IPv6 NETWORK WITH ROUTING OSPFv3. 39 f. Monografia – Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Universidade Tecnológica Federal do Paraná. Curitiba, 2013.

This study is about an analysis and simulation of an IPv6 network with routing OSPFv3. It shows an analysis of the protocol IPv6, with a description of its functioning and the main reason for its uses. Still about IPv6, it shows the header of protocol, the extension headers and the addressing used in this protocol. About the protocol OSPFv3, it shows the description of functioning, data extructure, the processing of packets, the table of routing and the Link State Advertisements of this protocol. The study ends up with a practical simulation, using the two analysed protocols.

Keywords: IPv6, OSPFv3, analysis, simulation.

LISTA DE FIGURAS

LISTA DE SIGLAS

AfriNIC - *African Network Information Centre*;

APNIC - *Asia-Pacific Network Information Centre*;

ARIN - *American Registry for Internet Numbers*;

BDR - *Backup Designated Router*;

BGP-4 - *Border Gateway Protocol*-4;

CIDR - *Classless Inter-Domain Routing*;

DCE - *Data Communication Equipment*;

DNS - *Domain Name System*;

DR - *Designated Router*;

EGP - *Exterior Gateway Protocol*;

EIGRP - *Enhanced Interior Gateway Routing Protocol*;

EUI-64 - *Extended Unique Identifier*-64;

IANA - *Internet Assigned Numbers Authority*;

ID - *Identification*;

IEEE - *Institute of Electrical and Electronics Engineers*;

IGP - *Interior Gateway Protocol*;

IP - *Internet Protocol*;

IPSec - *Internet Protocol Security*;

IPv4 - *Internet Protocol version*4;

IPv6 - *Internet Protocol version*6;

ISATAP - *Intra-Site Automatic Tunnel Addressing Protocol*;

IS-IS - *Intermediate System to Intermediate System*;

ISOC - *Internet Society*;

ISPs - *Internet Service Providers*;

LACNIC - *Latin American and Caribbean Internet Addresses Registry*;

LS - *Link State*;

LSAs - *Link State Advertisements*;

MAC - *Media Access Control*;

MTU - *Maximum Transmission Unit*;

NIC.br - Núcleo de Informação e Coordenação do Ponto BR;

NIR - *National Internet Registry*;

NSSA - *Not-So-Stubby Area*;

OSI - *Open Systems Interconnection*;

OSPFv2 - *Open Shortest Path First version*2;

OSPFv3 - *Open Shortest Path First version*3;

QoS - *Quality of Service*;

RFC - *Request for Comments*;

RIPE NCC - *Reseaux IP Europeens Network Coordination Centre*;

RIPng - *Routing Information Protocol next generation*;

RIR - *Regional Internet Registries*;

SPF - *Short Path First*;

TCP/IP - *Transmission Control Protocol/Internet Protocol*;

URL - *Uniform Resource Locators*;

UTFPR - Universidade Tecnológica Federal do Paraná.

SUMÁRIO

1 INTRODUÇÃO

1.1 Motivação

A motivação para o desenvolvimento desse trabalho se deve ao desafio de compreender o protocolo IPv6, cada dia mais presente nas redes de computadores. Para uma melhor aplicação e demonstração do IPv6, foi optado pela integração com um protocolo de roteamento. Para isso, foi escolhido o protocolo OSPFv3, aproveitando de suas relevantes características de funcionamento com o IPv6. Para dar uma ênfase mais prática ao trabalho, foi optado por desenvolver uma simulação prática utilizando os dois protocolos em questão.

1.2 Objetivos

1.2.1 Objetivo Geral

Demonstrar, por meio de pesquisas e simulação prática, os conceitos e aplicações dos protocolos IPv6 e OSPFv3.

1.2.2 Objetivos Específicos

- Demonstrar os conceitos do protocolo IPv6;
- Demonstrar os conceitos do protocolo OSPFv3;
- Demonstrar uma aplicação prática de ambos os protocolos através de uma simulação prática.

2 DESENVOLVIMENTO

2.1 *Internet Protocol version* 6 - IPv6

2.1.1 O que é IPv6

O *Internet Protocol version* 6 (IPv6) é a mais nova versão do protocolo de Internet. Seu objetivo é, ao longo do tempo, substituir e suprir algumas deficiências do *Internet Protocol version* 4 (IPv4). Apesar de ser chamado de novo, o IPv6 não é tão novo assim. Foi especificado inicialmente em dezembro de 1995 pela *Request for Comments* (RFC) 1883, no entanto, foi substituída pela RFC 2460 em dezembro de 1998.

O IPv6 é um endereço composto por 128 bits, diferentemente do IPv4, que possui apenas 32 bits. Com toda essa diferença, o IPv6 possui 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços disponíveis, uma quantidade extremamente alta de endereços. Com isso observa-se que o IPv6 já está preparado para uma adoção inicial, suprindo a demanda atual e também para a demanda futura, onde diversos dispositivos necessitarão de endereçamento na Internet.

2.1.1.1 Por que utilizar IPv6

O crescimento exponencial da Internet nos últimos anos tem mostrado para o mundo uma nova forma de agir com situações cotidianas. Vários serviços que antes necessitavam de deslocamento físico, agora podem ser feitos via Internet. Todo esse crescimento, traz consigo, a necessidade de diversos recursos em equipamentos que farão um papel fundamental na comunicação. Devido aos serviços disponíveis na Internet e a necessidade de recursos em equipamentos, vejamos alguns ítens que mostram o porquê da utilização do IPv6.

- Esgotamento do IPv4: apesar de seus 4.294.967.296 endereços possíveis, o IPv4 está chegando no seu limite de endereçamento. Diversas foram as situações que levaram a isso, por exemplo, o não planejamento da Internet para uma rede do tamanho atual, o

crescimento exponencial da Internet, a má distribuição inicial do endereçamento IPv4, entre outros;

- Internet das Coisas: estamos entrando em uma fase conhecida como Internet das Coisas. Essa fase representa a integração da Internet com diversos dispositivos eletroeletrônicos que fazem parte da vida cotidiana, como por exemplo: televisores, geladeiras, automóveis e diversos outros. O endereçamento IP desses dispositivos é fundamental para que eles se comuniquem, é aí que entra o papel do IPv6;

- Expansão das redes: diversas tecnologias estão utilizando o IP como seu protocolo de endereçamento, com isso, a necessidade de endereços IP torna-se cada vez mais necessária. Um exemplo disso é a tecnologia 4G, que está baseada totalmente em IP;

- Qualidade de serviço: para obter sucesso em determinados tipos de comunicação, principalmente voz e vídeo, é necessária a implantação da Qualidade de serviço, que prioriza esse tipo de tráfego pelo canal de comunicação. O IPv6 possui suporte melhorado para essas configurações;

- Mobilidade: a mobilidade já é e cada vez mais tornar-se-á um fator de extrema importância para as atividades cotidianas. Com o advento, por exemplo, do 4G, a necessidade de endereçamento IPv6 em rede móveis será fundamental.

2.1.1.2 Utilização do IPv6

Inicialmente, imaginava-se que o IPv6 seria utilizado de forma massiva após sua definição e que, em um prazo de 10 anos, a maioria da Internet utilizaria o novo protocolo, porém, não foi isso que aconteceu. Conforme Florentino (FLORENTINO, 2012):

> Entretanto, essa previsão não se concretizou. A Internet cresceu mais de 400% neste período - talvez até mais do que se tenha imaginado - e, ainda estamos engatinhando na implementação de redes IPv6 na Internet.

Os motivos pelos quais isso aconteceu possui razões técnicas e comerciais. Entre elas, podemos citar:

- Indiferente para o usuário final: inicialmente, o novo protocolo não traz nenhum benefício relevante para o usuário final, o que ele quer, é acessar seus serviços *Web*, email, entre outros, indiferente do protocolo utilizado por trás dessa comunicação;

- Atualização de infra-estrutura: diversos equipamentos precisariam ser substituídos para atenderem ao novo protocolo, gerando assim, custos relevantes para operadoras, provedores de Internet, usuário final, entre outros;
- Atualização de mão-de-obra: a falta de mão de obra especializada é outro fator relevante para a baixa adoção do IPv6 até o momento. Para o novo protocolo ser utilizado de forma massiva, seria necessário qualificação do corpo técnico.

O gerenciamento de todo o endereçamento IPv4 e IPv6 possível, é feito por uma organização e seus escritórios regionais. Essa organização é chamada de *Internet Assigned Numbers Authority* (IANA), que foi constituída em 1987 pelo governo norte-americano. Seus escritórios regionais são conhecidos como Registros Regionais de Internet (*Regional Internet Registries* - RIR) e representam uma grande área geográfica. A principal função de um RIR é distribuir e gerenciar endereços IP públicos em suas respectivas regiões geográficas.

Existem no total cinco RIRs, que são:

- *African Network Information Centre* (AfriNIC), que atua na região da África;
- *Asia-Pacific Network Information Centre* (APNIC), que atua na região da Ásia e do Pacífico;
- *American Registry for Internet Numbers* (ARIN), que atua na região da América do Norte;
- *Latin American and Caribbean Internet Addresses Registry* (LACNIC), que atua na região da América Latina e em algumas ilhas do Caribe;
- *Reseaux IP Europeens Network Coordination Centre* (RIPE NCC), que atua na região da Europa e países da Ásia Central.

Existem, em alguns países, um Registro Nacional de Internet (*National Internet Registry* - NIR), que responde a nível nacional por esse gerenciamento e distribuição de endereçamento IP público que, por sua vez, distruibui IPs para os *Internet Service Providers* (ISPs), servindo então aos usuários finais. No Brasil, o NIR responsável chama-se Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

2.1.2 Cabeçalho IPv6

Algumas mudanças ocorreram no cabeçalho do IPv6 em relação ao seu antecessor, o IPv4. Essas mudanças deixaram o cabeçalho mais simples, com apenas oito campos e um

tamanho fixo de 40 bytes. Uma novidade no cabeçalho do IPv6, é a criação de cabeçalhos de extensão, os quais comentaremos melhor adiante. Podemos verificar na figura 1 o cabeçalho do IPv6 e seus respectivos campos. Logo abaixo, segue uma explicação da função de cada campo.

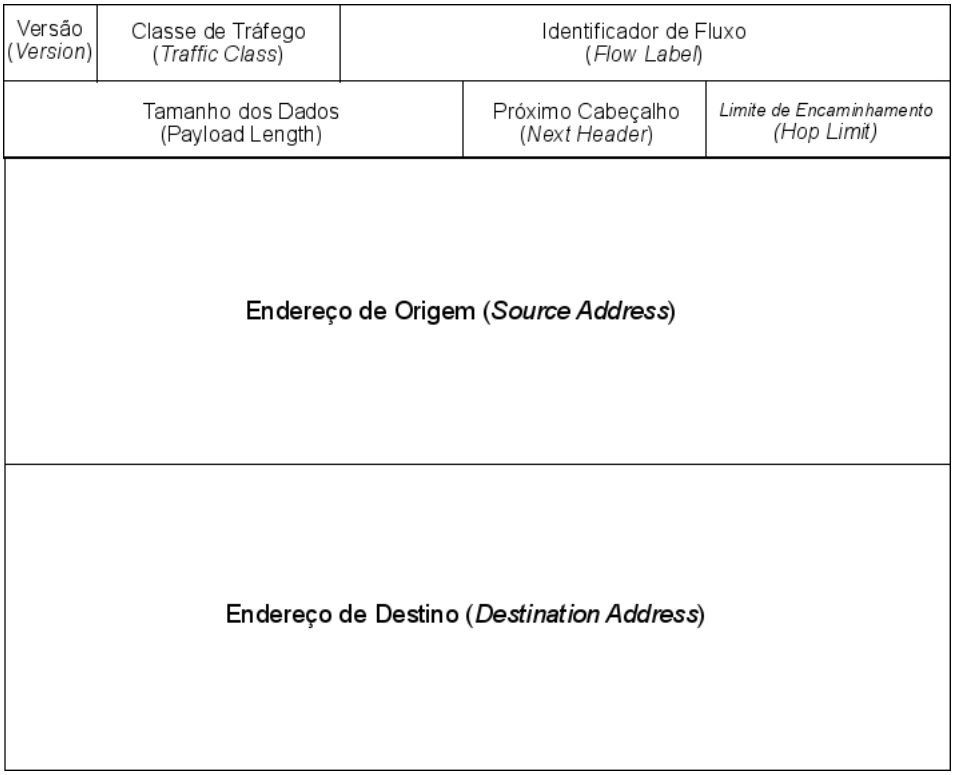

Figura 1: Cabeçalho IPv6.

Fonte: (IPV6.BR, 2012a)

- *Version* (Versão): possui um tamanho de 4 bits. Identifica a versão do protocolo IP utilizado. No caso do IPv6 esse valor é 6;
- *Traffic Class* (Classe de Tráfego): possui um tamanho de 8 bits. Diferencia e identifica os pacotes por classes de serviços ou prioridade. Juntamente com o campo Identificador de Fluxo (*Flow Label*), provê funções de Qualidade de Serviço (*Quality of Service* - QoS);
- *Flow Label* (Identificador de Fluxo): possui um tamanho de 20 bits. Diferencia e identifica pacote do mesmo fluxo na camada de rede. Através desse campo, o roteador consegue identificar o tipo de fluxo de cada pacote, sem a necessidade de verificar sua aplicação;
- *Payload Length* (Tamanho dos Dados): possui um tamanho de 16 bits. Indica o tamanho, em Bytes, somente dos dados transmitidos junto ao cabeçalho IPv6. Os cabeçalhos de extensão também são incluídos no cálculo do tamanho;

- *Next Header* (Próximo Cabeçalho): possui um tamanho de 8 bits. Identifica um cabeçalho de extensão ou protocolo de camada superior que segue ao cabeçalho IPv6 atual;
- *Hop Limit* (Limite de Encaminhamento): possui um tamanho de 8 bits. Indica o número máximo de saltos que o pacote IPv6 pode fazer antes de ser descartado, sendo decrementado em 1 a cada salto. Cada salto representa cada roteador por onde a informação trafega;
- *Source Address* (Endereço de Origem): possui um tamanho de 128 bits. Indica o endereço de origem do pacote;
- *Destination Address* (Endereço de Destino): possui um tamanho de 128 bits. Indica o endereço de destino do pacote;

2.1.2.1 Cabeçalhos de extensão

Uma novidade no IPv6 é a existência de cabeçalhos de extensão, que possuem a função de tratar informações opcionais. Diferentemente do IPv4, que tratava essas informações opcionais em seu cabeçalho base. Os cabeçalhos de extensão estão localizados entre o cabeçalho base e o cabeçalho da camada imediatamente superior. Outro detalhe, é que os cabeçalhos de extensão do IPv6 não possuem nem quantidade, nem tamanho fixo e, caso existam diversos cabeçalhos de extensão no mesmo pacote, eles são adicionados em série, formando uma fila de cabeçalhos.

Um dos objetivos do IPv6 com a criação de cabeçalhos de extensão para tratar informações opcionais é aumentar a velocidade de processamento nos roteadores, pois, o único cabeçalho de extensão processado pelos roteadores é o *Hop-by-Hop*, os demais são tratados apenas no dispositivo de destino. Outra vantagem, é que novos cabeçalhos de extensão podem ser utilizados sem alterar o cabeçalho base. São seis os cabeçalhos de extensão no IPv6 e abaixo, seguem seus nomes e respectivas funções:

- *Hop-by-Hop Options*: possui a função de carregar as informações que devem ser processadas por todos os nós ao longo do caminho do pacote até o destino. O cabeçalho de extensão *Hop-by-Hop Options* deve ser colocado logo após o cabeçalho base do IPv6. Quando o roteador não localiza esse cabeçalho de extensão, ele entende que não precisa processar nenhuma informação adicional e assim encaminha o pacote para o destino final imediatamente;

- *Destination Options*: possui a função de carregar as informações que devem ser processadas pelo nó de destino do pacote, indicado no campo *Destination Address* (Endereço de Destino) do cabeçalho base. Esse cabeçalho também é utilizado quando o recurso de mobilidade é aplicado sobre IPv6;

- *Routing*: teve como objetivo inicial relacionar um ou mais nós intermediários por onde o pacote deveria atravessar até chegar ao seu destino. Devido a problemas de segurança, a RFC 5095 tornou esse cabeçalho de extensão obsoleto. Um novo cabeçalho foi definido e atualmente, serve para funções de suporte à mobilidade no IPv6;

- *Fragmentation*: possui a função de carregar as informações sobre fragmentação de pacotes IPv6. Isso se dá quando o pacote IPv6 a ser enviado é maior que o *Path MTU*;

- *Authentication Header*: possui a função de prover autenticação e garantia de integridade aos pacotes IPv6. É utilizado pelo *Internet Protocol Security* (IPSec), pois é um protocolo que permite a criptografia e autenticação de pacotes na camada de rede. O IPSec é parte integrante do IPv6;

- *Encapsulating Security Payload*: possui a função de prover a garantia de integridade e confidencialidade dos pacotes. O *Encapsulating Security Payload* também é utilizado pelo IPSec.

Um detalhe importante quando trata-se dos cabeçalhos de extensão do IPv6 é a ordem em que eles se encontram. Por questões de melhorias significativas no processamento dos pacotes, deve-se seguir a seguinte sequência:

1. *Hop-by-Hop Options*;
2. *Routing*;
3. *Fragmentation*;
4. *Authentication Header*;
5. *Encapsulating Security Payload*;
6. *Destination Options*.

2.1.3 Endereçamento IPv6

O endereçamento IPv6 é algo de extrema importância para quem deseja aprender sobre o novo protocolo de Internet. Seu espaço de endereçamento possui 128 bits, comportando, com isso, 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços possíveis, chegando assim, no seu maior objetivo, aumentar o espaço de endereçamento.

Um endereço IPv6 possui 8 blocos de 16 bits cada um, separados pelo caractere dois pontos (:). Cada bloco, chamado de duocteto, possui 4 caracteres hexadecimais que podem variar de 0000 à FFFF. Os caracteres de um endereço IPv6 podem ser tanto maiúsculos quanto minúsculos. Eis um exemplo de endereço IPv6: 2001:0DB8:AD1F:25E2:CADE:CAFE:F0CA:84C1.

Conforme pode-se observar, a representação de endereços IPv6 não é algo simples. Sua escrita é longa e possui caracteres hexadecimais. Contudo, existem algumas regras de nomenclatura que podem auxiliar nessa questão. De acordo com Florentino (FLORENTINO, 2012):

> Para facilitar sua representação, algumas regras de nomenclatura foram definidas:
>
> - Zeros à esquerda em cada duocteto podem ser omitidos. Assim, 2001:0DB8:00AD:000F:0000:0000:0000:0001 pode ser representado por: 2001:DB8:AD:F:0:0:0:1.
> - Blocos vazios contínuos podem ser representados pelos caracteres :: (quatro pontos) **uma única vez** dentro do endereço (o valor que vem antes do primeiro sinal de dois pontos representa os primeiros bits, e o que vem após o segundo sinal de dois pontos representa os últimos bits do endereço). Assim, 2001:0DB8:00AD:000F:0000:0000:0000:0001 pode ser representado por: 2001:DB8:AD:F::1.

Pode-se observar que apenas com essas duas regras, a representação de um endereço IPv6 foi facilitada, onde 2001:0DB8:00AD:000F:0000:0000:0000:0001 é o mesmo que 2001:DB8:AD:F::1. Para um maior entendimento, podemos observar no Anexo A um "Guia didático de Endereçamento IPv6".

A representação dos prefixos de sub-rede de endereços IPv6 continua da mesma forma que são feitas no IPv4, utilizando a notação *Classless Inter-Domain Routing* (CIDR). Essa notação é feita utilizando a seguinte estrutura: Endereço IPv6/Tamanho do prefixo de sub-rede. O Tamanho do prefixo de sub-rede indica a quantidade de bits que estão à esquerda do endereço IPv6. Por exemplo: 2001:0DB8::/32.

Outra representação importante no IPv6 é em relação aos endereços *Uniform Resource*

Locators (URL). Os endereços URL em IPv6 são representados entre colchetes. Com isso, não existem problemas de acessar um endereço juntamente com o número de porta daquela comunicação. Por exemplo: http://[2001:0DB8::1]:8080.

2.1.3.1 Classificação de endereços IPv6

No endereçamento IPv6, existem 3 tipos de endereços definidos, que são:

- *Unicast*: esses endereços servem para identificar um host de forma única e exclusiva, sendo que, um pacote enviado a um endereço *unicast* é entregue a uma única interface. Através desses endereços, é possível criar uma topologia de comunicação fim-a-fim. Os endereços *unicast* ainda são divididos em 3 grupos, que são:
  - *Global Unicast*: possuem a mesma função dos Endereços Públicos do IPv4, ou seja, são globalmente roteáveis e acessáveis na Internet IPv6. Existe uma faixa reservada para esse endereçamento que representa apenas 13% do total de endereços possíveis com IPv6. Sua faixa de endereçamento vai de 2000::/3 até 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF;
  - *Link Local*: possuem a função de identificar um host apenas em sua rede local, não sendo roteáveis na Internet IPv6. A faixa reservada para esse endereçamento é FE80::/64. Os outros 64 bits, que identificam o host, são criados a partir do endereço físico *Media Access Control Address - MAC Address* da interface de rede. Essa técnica está padronizada no formato IEEE EUI-64;
  - *Unique Local Address*: possuem a função parecida com os Endereços Privados do IPv4, ou seja, servem para o endereçamento dos hosts na rede local. Apesar de possuírem uma grande probabilidade de serem globalmente únicos, não devem ser publicados na Internet IPv6. A faixa reservada para esse endereçamento é FC00::/7;
- *Multicast*: esses endereços servem para identificarem um grupo de hosts que receberão o mesmo pacote de informação. Quando determinado pacote é enviado para um endereço *multicast*, todas as interfaces associadas a esse endereço receberão o pacote. Tipos específicos de endereços *multicast* fazem a função dos endereços *broadcast* do IPv4, ou seja, enviar as informações para todos os hosts de um determinado domínio. Os endereços *multicast* não devem ser utilizados como endereço de origem de um pacote. Sua faixa reservada de endereçamento deriva do bloco FF00::/8;

- *Anycast*: esses endereços também servem para identificarem um grupo de hosts, entretanto, o host mais próximo da origem é quem receberá a informação. A proximidade entre a origem e o destino é medida pelos protocolos de roteamento. Como aplicações para esses endereços, podemos citar: descoberta de serviços de rede *Domain Name System - DNS*, balanceamento de carga, entre outros. Os endereços *anycast* são atribuídos a partir da faixa de endereçamento *unicast*, não existindo diferenciação entre eles, ou seja, um endereço *unicast* atribuído em mais de uma interface de rede, torna-se um endereço *anycast*.

2.1.3.2 Endereços especiais do IPv6

Da mesma forma que acontece no IPv4, no IPv6 também existem algumas faixas de endereços reservadas para fins especiais. São eles:

- *Unspecified*: esse endereço não deve ser atribuído a um dispositivo pois, ele serve apenas, para indicar a ausência de endereçamento. Da mesma forma, não deve ser utilizado como Endereço de Destino de um pacote IPv6. O endereço *unspecified* é representado por: 0:0:0:0:0:0:0:0 ou ::0;

- *Loopback*: esse endereço serve para o dispositivo referenciar-se a si próprio, sendo muito utilizado para testes internos de aplicativos e protocolos. Da mesma forma que o endereço *unspecified*, o endereço de *loopback* não deve ser atribuído a nenhuma interface física do dispositivo, nem utilizado como Endereço de Origem de pacotes IPv6. O endereço de *loopback* é representado por 0:0:0:0:0:0:0:1 ou ::1;

- Endereços de transição: para auxiliar no processo de transição dos endereços IPv4 com os endereços IPv6, algumas faixas de endereçamento foram reservadas para serem utilizadas com os diversos mecanismos de transição IPv4/IPv6. Essas faixas reservadas são:

  - *IPv4-compatible address*: é representado por 0:0:0:0:0:0:w.x.y.z ou ::w.x.y.z, onde w.x.y.z significa um Endereço Público IPv4 na forma decimal;
  - *IPv4-mapped address*: é representado por 0:0:0:0:0:FFFF:w.x.y.z ou ::FFFF:w.x.y.z, onde w.x.y.z significa um Endereço IPv4 na forma decimal;
  - *6to4 address*: é representado por 2002::/16;
  - *ISATAP address*: é representado por prefixo:0:5EFE:w.x.y.z, onde prefixo significa qualquer prefixo *unicast* (*link-local* ou global) válido em IPv6 e, w.x.y.z significa um Endereço Privado IPv4 na forma decimal;

  - *Teredo address*: é representado por 2001::/32.

2.1.4 Roteamento IPv6

Para que seja possível diferentes redes de computadores se comunicarem, é necessário um sistema de roteamento entre elas. Um sistema de roteamento compreende uma tabela de rotas que indica por onde um pacote de informação pode seguir para alcançar determinado destino. Essas rotas podem ser criadas de duas formas em um roteador:

- Manualmente: essas rotas são criadas manualmente pelo administrador da rede. Também são conhecidas como Rotas Estáticas;
- Dinamicamente: essas rotas são criadas dinamicamente, para isso, necessitam do trabalho dos Protocolos de Roteamento.

Os protocolos de roteamento efetuam um papel fundamental para diferentes redes se comunicarem, pois eles tornam mais fácil a conectividade entre elas, diminuindo a necessidade de configuração pelo administrador da rede. Os protocolos de roteamento são responsáveis por preencherem as tabelas de roteamento, adicionando informações relevantes para o roteador encaminhar os pacotes. Possuem níveis de abrangência e formas de funcionamento diferenciadas, conforme são classificados abaixo:

- Quanto ao nível de abrangência: refere-se à área de abrangência que o protocolo atua. Eles são classificados em:
  - *Interior Gateway Protocol* (IGP): são protocolos de roteamento que distribuem as informações dos roteadores dentro de Sistemas Autônomos. Como exemplo desses protocolos para IPv6, podemos citar: *Open Shortest Path First version 3* (OSPFv3), *Intermediate System to Intermediate System* (IS-IS), *Enhanced Interior Gateway Routing Protocol* (EIGRP) e *Routing Information Protocol next generation* (RIPng);
  - *Exterior Gateway Protocol* (EGP): são protocolos de roteamento que distribuem as informações dos roteadores entre Sistemas Autônomos. Como exemplo desses protocolos para IPv6, podemos citar: *Border Gateway Protocol 4* (BGP-4).
- Quanto à forma de funcionamento: refere-se à forma como o protocolo aprende e distribui informações sobre rotas. Eles são classificados em:

- *Link State*: os protocolos de roteamento *Link State* verificam o estado dos enlaces para determinar as rotas de encaminhamento. Possuem um algoritmo mais inteligente quando comparados aos protocolos *Distance Vector*. Suas atualizações ocorrem apenas quando existem alterações na topologia. Como exemplos de protocolos para IPv6 com essa característica, podemos citar: OSPFv3 e IS-IS;
- *Distance Vector*: o protocolo de roteamento *Distance Vector* aprende e ensina rotas divulgando e recebendo toda a tabela de roteamento dos roteadores vizinhos diretamente conectados. As atualizações são periódicas e consistem em toda a tabela de roteamento. Suas rotas levam em consideração a distância para alcançar o destino. Como exemplo de protocolo para IPv6 com essa característica, podemos citar: RIPng;
- *Path Vector*: o protocolo de roteamento *Path Vector* possui funcionamento parecido ao *Distance Vector*, porém, é utilizado para roteamento entre Sistemas Autônomos. Como exemplo de protocolo para IPv6 com essa característica, podemos citar: BGP-4.

O EIGRP é considerado um protocolo de roteamento híbrido, pois possui características *Link State* e *Distance Vector*, não sendo classificado exclusivamente em nenhuma das formas descritas acima.

2.2 *Open Shortest Path First version* 3 - OSPFv3

2.2.1 O que é OSPFv3

O OSPFv3, também conhecido como OSPF para IPv6, é um protocolo de roteamento utilizado para redes IPv6. Ele foi especificado inicialmente na RFC 2740, em Dezembro de 1999, mas em Julho de 2008, entrou em vigor a RFC 5340, tornando a RFC 2740 obsoleta. Essas RFCs descrevem as modificações do OSPF para prover suporte ao IPv6. Apesar do OSPFv3 ser um protocolo de roteamento para redes IPv6, a partir da RFC 5838, de Abril de 2010, o mesmo passou a ter suporte a redes IPv4. Algumas mudanças foram necessárias no OSPF para prover suporte ao IPv6, porém, alguns mecanismos fundamentais do OSPF continuam inalterados, eis os principais: o algoritmo *Short Path First* (SPF), o conceito de inundação (*flooding*), a eleição de *Designated Router* (DR), o escopo de áreas e os temporizadores e métricas.

Conforme descrito anteriormente, o OSPFv3 é um protocolo de roteamento do tipo *link-state*, ou seja, ele verifica o estado dos enlaces para determinar as rotas de encaminhamento.

Além de *link-state*, o OSPFv3 é também um protocolo IGP, ou seja, distribui as informações de roteamento dentro de seu Sistema Autônomo.

Da mesma forma que no OSPFv2, o OSPFv3 utiliza o conceito de áreas. Cada área é composta por seus próprios roteadores. A área 0 é chamada de área *backbone*, sendo a área central da topologia, e todas as outras áreas devem se conectar a ela, seja por conexão direta ou por *links* virtuais, sendo esse último, um caminho lógico entre uma área e a área *backbone*.

Quanto à entrega de atualizações do OSPFv3, ela pode ocorrer entre conexões ponto-a-ponto entre roteadores como também em redes que suportem *broadcast*, nesse caso, ocorrendo o processo de eleição de um roteador designado (*Designated Router* - DR) e um roteador designado de *backup* (*Backup Designated Router* - BDR).

O protocolo OSPFv3 é baseado em um algoritmo chamado *Shortest Path First* (SPF). Esse algoritmo é responsável pelos cálculos de melhores caminhos até o destino de determinado pacote de informação. Os roteadores que executam o algoritmo SPF possuem duas tarefas fundamentais para o funcionamento do protocolo, são elas:

- Verificar se os roteadores vizinhos estão ativos, realizando testes de status de conexão, através de pacotes *Hello*;
- Anunciar periodicamente o estado dos enlaces para os demais roteadores, com o auxílio das *Link State Advertisements* (LSAs). As LSAs serão vistas com maiores detalhes posteriormente.

De acordo com Albuquerque (ALBUQUERQUE, 1999):

> Os roteadores OSPF se comunicam através de protocolos implementados acima do IP chamados de *Hello*, *Exchange* e *Flooding*. O *Hello* é responsável por verificar se os canais de comunicação estão operacionais. O *Exchange* é responsável pela sincronização inicial das bases de dados. O *Flooding* é responsável por manter as bases de dados sincronizadas.

2.2.2 A estrutura de dados OSPFv3

No OSPF, as estruturas de dados são as mesmas, tanto para o IPv4 quanto para o IPv6. Essas estruturas são: áreas, interfaces, vizinhos, o banco de dados de estado de enlace e a tabela de roteamento. As estruturas de dados de áreas, interfaces e vizinhos são vistas em seguida. Já o banco de dados de estado de enlace e a tabela de roteamento serão vistos posteriormente.

- A estrutura de dados de áreas: essa estrutura possui todos os elementos definidos para a estrutura de dados de áreas IPv4, conforme descritos na RFC 2328, e possui também todos os tipos de LSAs conhecidos que possuem escopo de inundação de área. Essas LSAs são: *router-LSAs*, *network-LSAs*, *inter-area-prefix-LSAs*, *inter-area-router-LSAs*, e *intra-area-prefix-LSAs*;

- A estrutura de dados de interface: essa estrutura possui modificações em relação à estrutura de dados de interface IPv4, descritos na RFC 2328. Essas modificações acontecem nos seguintes ítens: identificação da interface, identificação de instância, lista de LSAs com escopo de *link-local*, endereço IP da interface e lista de prefixos de *link*;

- A estrutura de dados de vizinhos: essa estrutura tem a função de coletar todas as informações necessárias para formar uma adjacência entre dois roteadores, quando necessário. Cada estrutura está vinculada a uma única interface que esteja executando o OSPF. Existem algumas modificações nas estruturas para IPv6 e IPv4. Essas modificações acontecem nos seguintes ítens: identificação da interface do vizinho, endereço IP do vizinho, roteador designado (*Designated Router* - DR) do vizinho e roteador designado de *backup* (*Backup Designated Router* - BDR) do vizinho.

2.2.3 O processamento de pacotes OSPFv3

O OSPFv3, por ser um protocolo de roteamento, é executado na camada de rede do modelo OSI (*Open Systems Interconnection*), juntamente com o IPv6. Quando o IPv6 precisa referenciar-se ao OSPFv3, ele configura o valor 89 no seu campo *Next Header*. Os pacotes enviados pelo OSPFv3 são encaminhados apenas para suas adjacências, com exceção dos pacotes *Hello*, que são utilizados para descobrir as adjacências. Podemos verificar na figura 2 o cabeçalho do OSPFv3 e seus respectivos campos. Logo abaixo, segue uma explicação da função de cada campo.

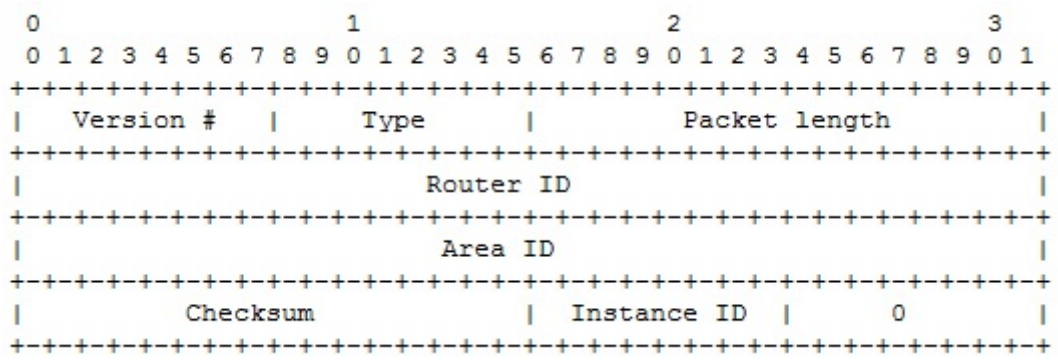

Figura 2: Cabeçalho OSPFv3.

Fonte: (INTERNET SOCIETY - ISOC, 2008)

- *Version* (Versão): possui o valor 3, indicando a versão do protocolo OSPF;
- *Type* (Tipo): existem 5 tipos de pacotes OSPF. Através do valor indicado nesse campo, o tipo correspondente é acionado. São eles:
  1. *Hello Message*;
  2. *Database Description message*;
  3. *Link State Request*;
  4. *Link State Update*;
  5. *Link State Acknowledgement*;
- *Packet Length* (Comprimento do pacote): comprimento do pacote OSPF em Bytes. Esse comprimento inclui o cabeçalho padrão do OSPF;
- *Router ID* (ID do roteador): possui um tamanho de 32 bits. Identifica o *Router ID* de origem do pacote;
- *Area ID* (ID de área): possui um tamanho de 32 bits. Identifica a área a que esse pacote pertence. Cada pacote pertence a uma única área;
- *Checksum* (Soma de verificação): possui um tamanho de 16 bits. Consiste em uma soma de verificação para identificar a integridade do pacote;
- *Instance ID* (ID de instância): permite várias instâncias do OSPF para ser executado em um único link. Para cada instância do protocolo seria atribuído um ID de instância separada;

- 0: é um campo reservado.

2.2.4 A estrutura da tabela de roteamento OSPFv3

Uma tabela de roteamento contém todas as informações necessárias para encaminhar um pacote de dados até seu destino. Quando encaminha um pacote de dados, a entrada da tabela de roteamento proporciona o melhor caminho até o destino para esse pacote. Após um pacote localizar uma rota correspondente na tabela de roteamento, ele então verifica qual interface aquela rota está utilizando e segue por essa interface.

A tabela de roteamento do OSPFv3 possui entradas para os prefixos de endereços IPv6 e também o número de Sistema Autônomo dos roteadores de borda. As últimas entradas da tabela de roteamento são usadas somente para manter os resultados durante o processo de construção da tabela de roteamento. Para manter os resultados durante o cálculo de caminho mais curto (*shortest-path*) para cada área, existe uma tabela de roteamento separada para cada área mantendo as seguintes entradas:

- Uma entrada para cada roteador na área: os roteadores são identificados pelo seu ID de roteador (*Router ID*). Essas entradas na tabela de roteamento mantêm o conjunto de caminhos mais curtos através de uma determinada área para um determinado roteador, que por sua vez permite o cálculo de caminhos para os prefixos IPv6 anunciados por esse roteador;

- Uma entrada para cada enlace na área: os enlaces são associados com as *network-LSAs*, que serão explicadas posteriormente. Essas entradas na tabela de roteamento permitem o cálculo de caminhos para os prefixos IPv6 anunciados para o enlace na *intra-area-prefix-LSAs*.

Alguns campos da tabela de roteamento do OSPFv2 permanecem válidas no OSPFv3, são elas: recursos opcionais (*optional capabilities*), tipo de caminho (*path type*), custo (*cost*), custo tipo 2 (*type 2 cost*), estado do enlace de origem (*link state origin*), próximo salto (*next-hop*) e roteadores de anúncio (*advertising routers*).

Podemos observar na sequência, a tabela de roteamento do roteador RT1 utilizado na simulação prática desse trabalho. A topologia completa, bem como sua configuração, serão demonstradas adiante.

```
RT1#show ipv6 route
IPv6 Routing Table – 16 entries
Codes: C – Connected, L – Local, S – Static, R – RIP, B – BGP
       U – Per-user Static route, M – MIPv6
       I1 – ISIS L1, I2 – ISIS L2, IA – ISIS interarea, IS – IS
       IS summary
       O – OSPF intra, OI – OSPF inter, OE1 – OSPF ext 1, OE2 –
       OSPF ext 2
       ON1 – OSPF NSSA ext 1, ON2 – OSPF NSSA ext 2
       D – EIGRP, EX – EIGRP external
C   2000::/127 [0/0]
     via ::, Serial0/0/0
L   2000::/128 [0/0]
     via ::, Serial0/0/0
O   2001::/127 [110/128]
     via FE80::201:C9FF:FEB1:8B02, Serial0/0/0
O   2002::/127 [110/128]
     via FE80::20A:F3FF:FEC5:2C01, Serial0/0/1
C   2003::/127 [0/0]
     via ::, Serial0/0/1
L   2003::1/128 [0/0]
     via ::, Serial0/0/1
C   2004::/127 [0/0]
     via ::, Serial0/1/0
L   2004::/128 [0/0]
     via ::, Serial0/1/0
O   2005::/127 [110/128]
     via FE80::201:C9FF:FEB1:8B02, Serial0/0/0
O   2006::/127 [110/192]
     via FE80::201:C9FF:FEB1:8B02, Serial0/0/0
     via FE80::20A:F3FF:FEC5:2C01, Serial0/0/1
O   2007::/127 [110/128]
     via FE80::20A:F3FF:FEC5:2C01, Serial0/0/1
O   FD00:0:0:1::/64 [110/65]
     via FE80::20B:BEFF:FECA:2601, Serial0/1/0
O   FD00:0:0:2::/64 [110/129]
     via FE80::201:C9FF:FEB1:8B02, Serial0/0/0
O   FD00:0:0:3::/64 [110/193]
```

```
     via FE80::201:C9FF:FEB1:8B02, Serial0/0/0
     via FE80::20A:F3FF:FEC5:2C01, Serial0/0/1
O   FD00:0:0:4::/64 [110/129]
     via FE80::20A:F3FF:FEC5:2C01, Serial0/0/1
L   FF00::/8 [0/0]
     via ::, Null0
RT1#
```

Através da tabela de roteamento mostrada acima, podemos observar que o RT1 possui 16 entradas. Essas entradas são dos tipos: diretamente conectada (C), conexão local (L) e com roteamento OSPFv3 (O). Em relação as rotas com OSPFv3, como todos os enlaces seriais possuem a mesma largura de banda (1,544 Mbps), as entradas na tabela de roteamento para essas rotas serão criadas a partir da menor distância (menor número de saltos) até a rede de destino. Podemos observar que para o roteador RT1 alcançar a rede 2005::0/127, ele utiliza a interface serial 0/0/0. Já para alcançar a rede 2006::0/127, existem dois caminhos possíveis, via interface serial 0/0/0 ou serial 0/0/1, pois o número de saltos até essa rede é o mesmo, tanto via serial 0/0/0 quanto serial 0/0/1.

2.2.5 *Link State Advertisements*

Os Anúncios de Estado do Enlace (*Link State Advertisements* - LSAs) são pacotes de atualizações utilizados pelos protocolos de roteamento do tipo *Link-State*. É através das LSAs que os roteadores informam aos outros roteadores de mesma área, informações sobre o estado dos enlaces. Essas informações incluem estado das interfaces, métricas utilizadas e outras variáveis.

No OSPFv3, todas as LSAs começam com um cabeçalho padrão de 20 Bytes. Esse cabeçalho possui informações suficientes para identificar a LSA que será utilizada. Múltiplas ocorrências da LSA podem existir em um domínio de roteamento ao mesmo tempo. Em seguida é necessário determinar qual ocorrência é a mais recente. Isso é feito examinando-se os campos *LS age*, *LS sequence number* e *LS checksum* que estão contidos no cabeçalho padrão das LSAs. Esse cabeçalho pode ser visto na figura 3, posteriormente pode ser observada a função de cada campo do cabeçalho.

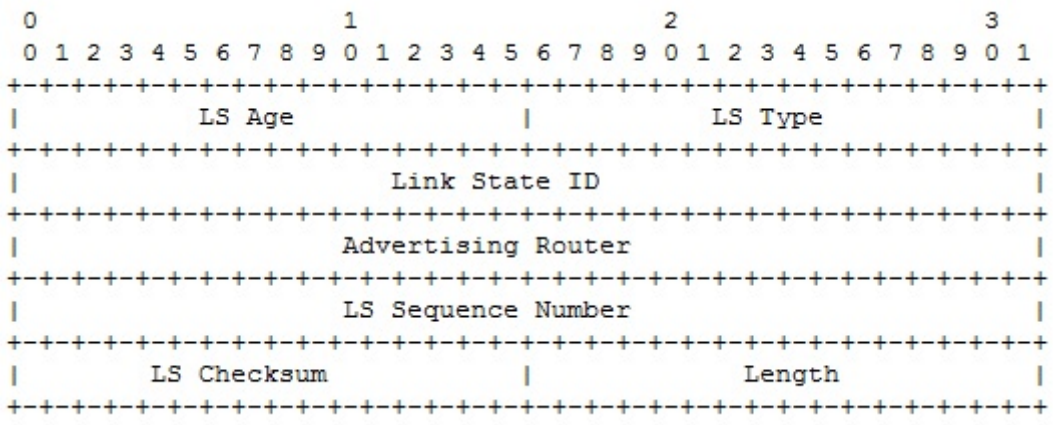

Figura 3: Cabeçalho padrão de LSA do OSPFv3.

Fonte: (INTERNET SOCIETY - ISOC, 2008)

- *LS Age*: o tempo, em segundos, desde que o LSA foi gerado;
- *LS Type*: indica a função desempenhada pela LSA;
- *Link State ID*: identificados do roteador de origem da LSA. A combinação dos campos *Link State ID*, *LS type*, e *Advertising Router* identificam a LSA na Base de Dados de Estado de Enlace (*Link State Database*);
- *Advertising Router*: possui o *Router ID* do roteador que originou a LSA;
- *LS sequence number*: é usado para detectar LSAs velhas ou duplicadas.
- *LS checksum*: é uma soma de verificação do conteúdo da LSA. Essa verificação inclui todo o cabeçalho LSA, exceto o campo *LS age*;
- *Length*: o comprimento, em Bytes, do LSA. Isto inclui os 20 Bytes do cabeçalho do LSA.

Pode-se observar na figura 4, os códigos de função de cada LSA do OSPFv3. Logo abaixo, segue uma breve descrição da função de cada LSA.

LSA Function Code	LS Type	Description
1	0x2001	Router-LSA
2	0x2002	Network-LSA
3	0x2003	Inter-Area-Prefix-LSA
4	0x2004	Inter-Area-Router-LSA
5	0x4005	AS-External-LSA
6	0x2006	Deprecated (may be reassigned)
7	0x2007	NSSA-LSA
8	0x0008	Link-LSA
9	0x2009	Intra-Area-Prefix-LSA

Figura 4: Códigos de função de cada LSA do OSPFv3.

Fonte: (INTERNET SOCIETY - ISOC, 2008)

- *Router LSA*: possui a função de identificar o roteador de origem e seus enlaces com os vizinhos, para ser utilizado nos cálculos do algoritmo SPF;
- *Network LSA*: é originada no Roteador Designado (*Designated Router* - DR) e tem a função de listar todos os roteadores no enlace com o qual é totalmente adjacente;
- *Inter-Area Prefix LSA*: possui a função de realizar o anúncio de redes que estão em outra área, mas dentro do mesmo Sistema Autônomo;
- *Inter-Area Router LSA*: possui a função de anunciar um caminho de destino para um roteador OSPF que é de uma área externa, mas do mesmo Sistema Autônomo;
- *AS-External LSA*: possui a função de anunciar um caminho para os prefixos externos a um Sistema Autônomo;
- *Group Membership LSA*: obsoleto. Pode ser realocado;
- *NSSA LSA*: possui a função de anunciar um caminho para um prefixo externo ao Sistema Autônomo cujo escopo de inundação é restrito a uma única área NSSA;
- *Link LSA*: é usado para transferir informações que são relevantes apenas para dois roteadores vizinhos diretamente conectados;
- *Intra-Area Prefix LSA*: é usado para anunciar prefixos IPv6 que são associados com: o próprio roteador, um segmento de rede *stub* ou um segmento de rede em trânsito.

3 SIMULAÇÃO PRÁTICA

A simulação prática desse trabalho, foi realizada em um aplicativo específico para simulação de topologias de rede, chamado *Cisco Packet Tracer*, em sua versão 6.0.1.0011. A topologia montada conta com os seguintes equipamentos: 8 roteadores Cisco 2911, 4 *switches* Cisco Catalyst 2960 e 4 computadores com interface de rede *FastEthernet*. As conexões entre os roteadores, foram realizadas através de enlaces seriais com largura de banda de 1,544 Mbps. As conexões entre os roteadores e *switches* foram realizadas nas interfaces *GigabitEthernet* de ambos os equipamentos e as conexões entre os *switches* e os computadores, foram realizadas através das interfaces *FastEthernet*. Na sequência, pode-se observar a topologia montada, bem como o plano de endereçamento IPv6 utilizado.

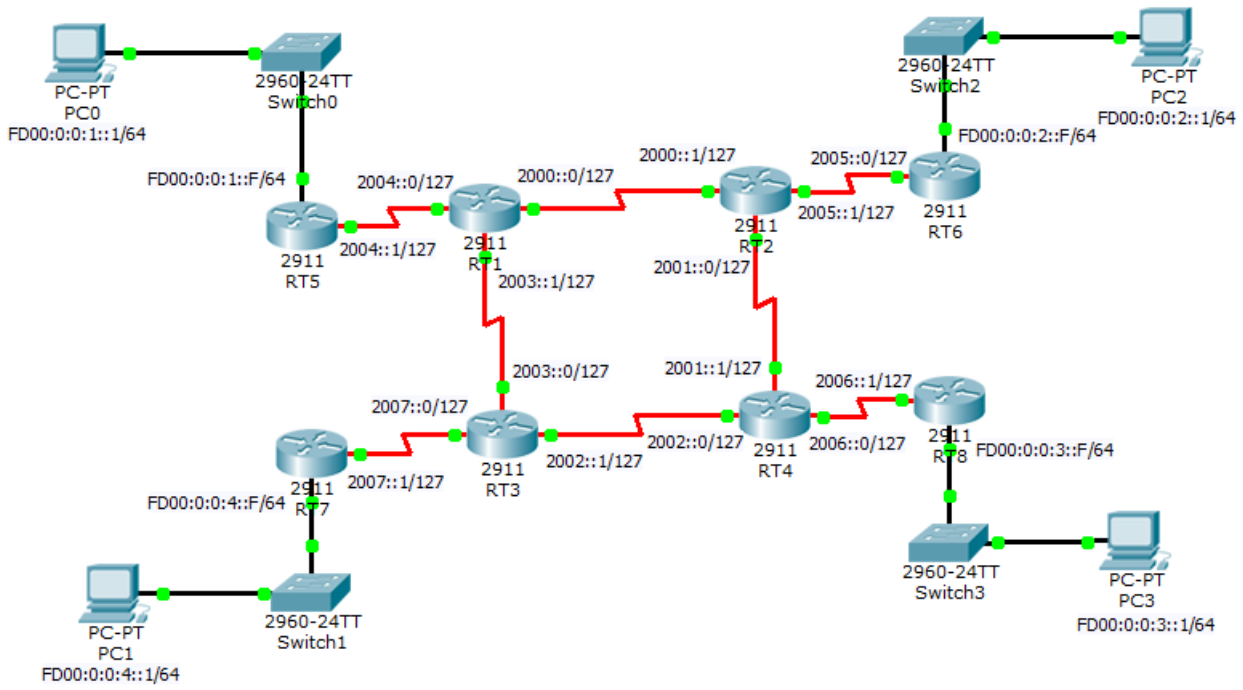

Figura 5: Topologia de rede com IPv6 e OSPFv3.

Fonte: Autoria Própria

Essa topologia, conforme proposto inicialmente, foi realizada utilizando os dois protocolos analisados, o IPv6 e OSPFv3. No IPv6, foram utilizadas máscaras de sub-rede /127 nos enlaces seriais, pois são conexões ponto a ponto, não necessitando mais que dois endereços IPv6. Já para as redes locais, foram utilizadas máscaras de sub-rede /64, conforme recomendado pelo IPv6.br, como pode ser visto no Anexo A - "Guia didático de Endereçamento IPv6". Já para o OSPFv3, foi utilizado o Identificador de Processo (*Process ID*) com valor 1. Referente a área do OSPFv3, a topologia teve uma única área, sendo área 0. O endereço do Identificador de Roteador (*Router-ID*) seguiu a seguinte lógica: 1.1.1.1 para o RT1, 2.2.2.2 para o RT2 e assim sucessivamente.

Questões de segurança, como: senhas, tempo de conexão, e outras, não foram implementadas nessa topologia, pois não era o objetivo do trabalho, mas vale lembrar que, em equipamentos em produção, questões de segurança são fundamentais. A seguir, pode-se observar o processo de configuração do roteador RT1. Vale ressaltar que o processo é o mesmo para os outros roteadores, alterando-se apenas endereçamento IPv6, endereço do *router-id* e ativação do comando *clock rate* nas interfaces seriais DCE.

```
         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: no

Press RETURN to get started!

Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname RT1
RT1(config)#ipv6 unicast-routing
RT1(config)#ipv6 router ospf 1
%OSPFv3-4-NORTRID: OSPFv3 process 1 could not pick a router-id,please
configure manually
RT1(config-rtr)#router-id 1.1.1.1
RT1(config-rtr)#exit
RT1(config)#interface serial 0/0/0
RT1(config-if)#ipv6 address 2000::0/127
RT1(config-if)#clock rate 64000
RT1(config-if)#ipv6 ospf 1 area 0
RT1(config-if)#no shutdown
```

```
RT1(config-if)#exit
RT1(config)#interface serial 0/0/1
RT1(config-if)#ipv6 address 2003::1/127
RT1(config-if)#ipv6 ospf 1 area 0
RT1(config-if)#no shutdown
RT1(config-if)#exit
RT1(config)#interface serial 0/1/0
RT1(config-if)#ipv6 address 2004::0/127
RT1(config-if)#ipv6 ospf 1 area 0
RT1(config-if)#no shutdown
RT1(config-if)#end
RT1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
RT1#
```

Através da configuração executada acima, teremos o resultado mostrado na sequência. Esse resultado é obtido a partir do comando *show running-config*, o qual serve para mostrar as configurações em execução no roteador.

```
RT1#show running-config
Building configuration...

Current configuration : 1032 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RT1
!
ipv6 unicast-routing
!
license udi pid CISCO2911/K9 sn FTX1524RZQ3
!
spanning-tree mode pvst
```

```
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 no ip address
 ipv6 address 2000::/127
 ipv6 ospf 1 area 0
 clock rate 64000
!
interface Serial0/0/1
 no ip address
 ipv6 address 2003::1/127
 ipv6 ospf 1 area 0
!
interface Serial0/1/0
 no ip address
 ipv6 address 2004::/127
 ipv6 ospf 1 area 0
!
interface Serial0/1/1
 no ip address
!
```

```
interface Vlan1
 no ip address
 shutdown
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
!
ip classless
!
no cdp run
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
RT1#
```

Após a configuração executada acima e a total convergência da topologia, podemos avaliar alguns resultados. Com o comando *show ipv6 ospf neighbor* no roteador RT1, podemos visualizar quem são seus roteadores vizinhos. Os vizinhos são identificados pelo endereço *router-id* configurado em cada roteador. Conforme a saída mostrada abaixo, comprovamos que o RT1 possui como vizinhos os roteadores RT2 (*router-id* 2.2.2.2), o RT3 (*router-id* 3.3.3.3) e o RT5 (*router-id* 5.5.5.5). Além disso, outras informações relevantes são: estado da conexão (*State*), intervalo de tempo até o vizinho ser removido da tabela caso o roteador não receba um pacote *hello* (*Dead Time*) e a interface de conexão com cada vizinho.

```
RT1#show ipv6 ospf neighbor

Neighbor ID  Pri  State    Dead Time   Interface ID    Interface
2.2.2.2        0  FULL/  - 00:00:32    5               Serial0/0/0
3.3.3.3        0  FULL/  - 00:00:37    4               Serial0/0/1
5.5.5.5        0  FULL/  - 00:00:37    4               Serial0/1/0
RT1#
```

Outro resultado que podemos avaliar, é através do comando *show ipv6 ospf interface serial 0/0/0* no roteador RT1. Esse comando permite visualizar informações do OSPFv3 na interface serial 0/0/0, conforme pode ser visto abaixo. As principais informações que podemos visualizar com esse comando são: o estado de conexão da interface (*Serial0/0/0 is up, line protocol is up*), a área do OSPFv3 (*Area 0*), o Identificador de Processo (*Process ID 1*), o Identificador do Roteador (*Router ID 1.1.1.1*), os intervalos de tempo do OSPFv3 (*Timer intervals*) e o vizinho com o qual essa interface faz conexão (*Adjacent with neighbor 2.2.2.2*).

```
RT1#show ipv6 ospf interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Link Local Address FE80::20D:BDFF:FE7D:E201 , Interface ID 4
  Area 0, Process ID 1, Instance ID 0, Router ID 1.1.1.1
  Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
RT1#
```

4 CONCLUSÃO

Com a realização desse trabalho, foi possível aprofundar os conhecimentos sobre o protocolo IPv6, obtendo assim, maiores informações sobre as características gerais de funcionamento, o seu cabeçalho padrão e cabeçalhos de extensão, sua estrutura de endereçamento e detalhes sobre roteamento nesse protocolo.

Foi possível também, conhecer o protocolo de roteamento OSPFv3, sua estrutura de dados, sua forma de processamento dos pacotes, a tabela de roteamento nesse protocolo e as *Link State Advertisements* (LSAs) do OSPFv3.

Conclui-se ainda, com a realização da simulação prática, que os dois protocolos são completamente compatíveis, sendo possíveis suas implementações em redes em produção. E, finalmente, podemos concluir que alcançamos o objetivo geral proposto nesse trabalho, conseguindo demonstrar, por meio de pesquisas e simulação prática, os conceitos e aplicações dos protocolos IPv6 e OSPFv3.

REFERÊNCIAS

ALBUQUERQUE, F. **TCP/IP Internet Protocolos e Tecnologias**. 2ª. ed. [S.l.]: Axcel Book, 1999.

FLORENTINO, A. A. **IPv6 na prática**. [S.l.]: Linux New Media, 2012.

INTERNET SOCIETY - ISOC. **RFC 5340 - OSPF for IPv6**. 2008. Disponível em: <http://www.rfc-editor.org/rfc/rfc5340.txt>.

IPV6.BR. **Cabeçalho IPv6**. 2012. Disponível em: <http://ipv6.br/entenda/cabecalho/>.

IPV6.BR. **Guia didático de Endereçamento IPv6**. 2012. Disponível em: <http://ipv6.br/entenda/enderecamento/>.

ANEXO A – GUIA DIDÁTICO DE ENDEREÇAMENTO IPV6

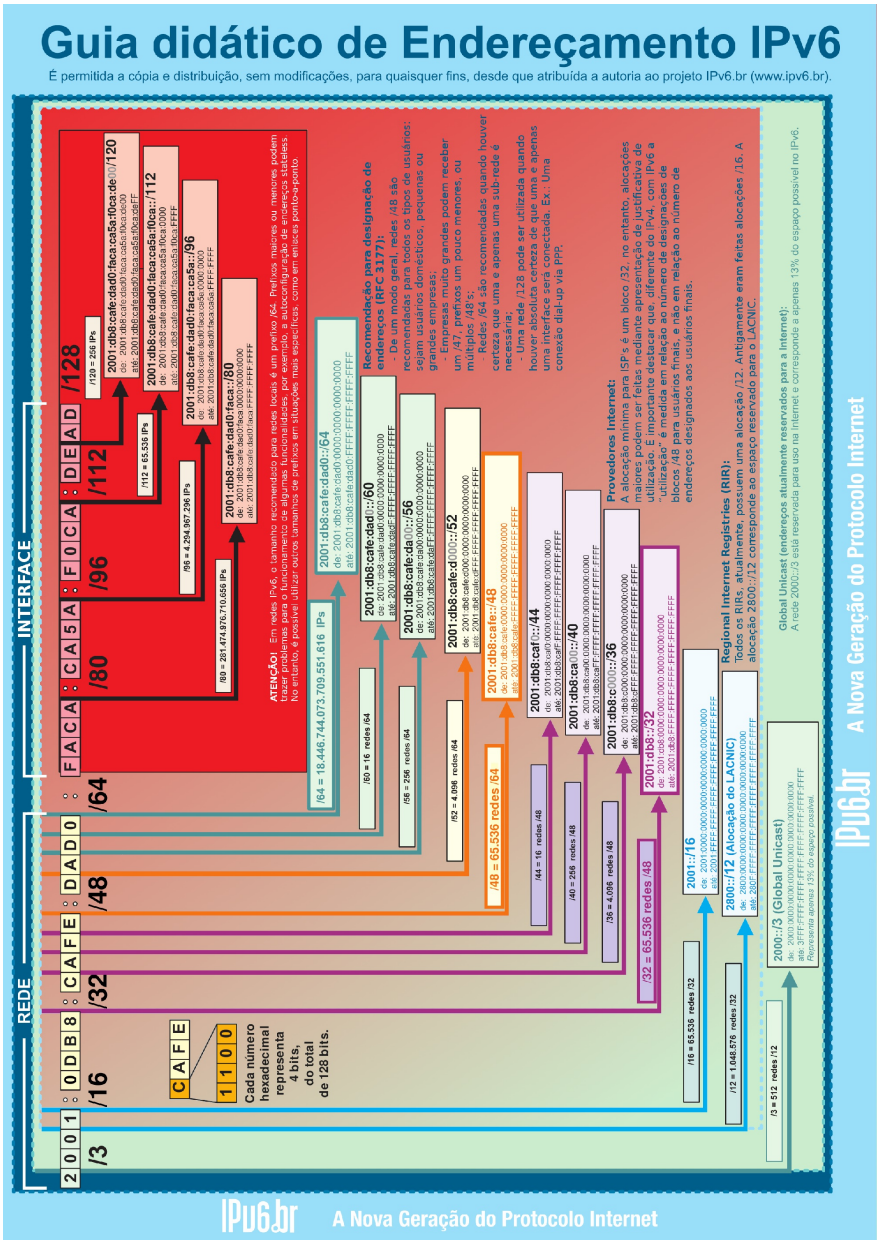

Figura 6: Guia didático de Endereçamento IPv6.

Fonte: (IPV6.BR, 2012b)