UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

LUIZ HENRIQUE ALMEIDA DE ARAÚJO

ANÁLISE E SIMULAÇÃO DA TÉCNICA DE PILHA DUPLA PARA IPV6

MONOGRAFIA

CURITIBA
2014

LUIZ HENRIQUE ALMEIDA DE ARAÚJO

ANÁLISE E SIMULAÇÃO DA TÉCNICA DE PILHA DUPLA PARA IPV6

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.
Orientador: Prof. Augusto Foronda

CURITIBA

2014

AGRADECIMENTOS

- A Deus por ter me dado saúde e força para superar as dificuldades.
- Ao meu orientador Augusto Foronda, pelo suporte no pouco tempo que lhe coube, pelas suas correções e incentivos.
- Aos meus pais, pelo amor, incentivo e apoio incondicional.
- A minha esposa e filho, motivo pelo qual continuo buscando melhorar a cada dia.

RESUMO

ALMEIDA DE ARAUJO, Luiz H. **Análise e Simulação da Técnica de Pilha Dupla para IPv6.** 2014. 42 f. Monografia (Especialização em Gerenciamento de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

Este trabalho tem como tema central à análise e simulação da técnica de Pilha Dupla para IPv6. Estipular um método de convergência entre redes IPv4 e IPv6 é o objetivo principal deste trabalho. Uma análise do protocolo IPv6, contendo uma descrição de funcionamento e os principais serviços, tais como: ICMPv6, Descoberta de Vizinhança, PATH MTU Discovery e QoS. Finaliza com uma simulação prática, utilizando os protocolos IPv4 e IPv6 em uma mesma rede.

Palavra-chave: IPv6, Pilha Dupla, análise, simulação.

ABSTRACT

ALMEIDA DE ARAUJO, Luiz H. **Análise e Simulação da Técnica de Pilha Dupla para IPv6.** 2014. 42 f. Monografia (Especialização em Gerenciamento de Redes) – Programa de Pós-Graduação em Tecnologia, Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

This work is focused on the analysis and simulation technique for Dual Stack IPv6. Stipulate a method of convergence between IPv4 and IPv6 networks is the main objective of this work. An analysis of the IPv6 protocol, containing a description of operation and key services such as: ICMPv6, Discovery Neighbourhood, PATH MTU Discovery and QoS. Ends with a practical simulation using the IPv4 and IPv6 protocols on the same network.

Keyword: IPv6, Dual Stack, analysis, simulation.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

IP - *Internet Protocol;*
ARP - *Address Resolution Protocol;*
RARP - *Reverse Address Resolution Protocol;*
CIDR - *Classless InterDomain Routing;*
Cisco IOS - *Internetworking Operacional System;*
DHCP - *Dynamic Host Configuration Protocol;*
DNS - *Domain Name System;*
DoD - *U.S. Department of Defense;*
DVD - *Digital Versatile Disc;*
e-PING - Padrões de Interoperabilidade de Governo Eletrônico;
IANA - *Internet Assigned Numbers Authority;*
ICMP - *Internet Control Message Protocol;*
ICMPv4 - *Internet Control Message Protocol for IPv4;*
ICMPv6 - *Internet Control Message Protocol for IPv6;*
IESG - *Internet Engineering Steering Group;*
IGMP - *Internet Group Management Protocol;*
IPngWG - *Internet Protocol Next Generation Working Group;*
IpngWG - *IP Next Generation Working Group;*
IPv4 - *Internet Protocol version 4;*
IPv6 - *Internet Protocol version 6;*
IPX - *Internal Packet eXchange;*
IS-IS - *Intermediate System to Intermediate System;*
LACNIC - *Latin American and Caribbean Internet Addresses Registry;*
MAC - *Media Access Control;*
MTU - *Maximum Transmission Unit;*
NIC.br - Núcleo de Informação e Coordenação do Ponto BR;
NSAP - *Network Service Access Point;*
OMB – *Office of Management and Budget;*
OSI - *Open Systems Interconnection;*
OSPFV2 - *Open Shortest Path First version2;*
OSPFv3 - *Open Shortest Path First version3;*
QoS - *Class of Services*;
RFC - *Request for Comments;*
RIPv2 - *Routing Information Protocol – Version 2*;
RIRs - *Regional Intenet Registres;*
RNP - Rede Nacional de Pesquisa;
SIPP - *Simple Internet Protocol Plus*;
TCP - *Internet Protocol;*
TCP/IP - *Transmission Control Protocol/Internet Protocol;*
UDP - *User Datagram Protocol;*

SUMÁRIO

1 INTRODUÇÃO

1.1 Motivação

A motivação para elaboração deste trabalho consiste em uma melhor compreensão do funcionamento do protocolo IPv6, o qual oferece uma série de vantagens em relação ao seu antecessor o IPv4. Para demonstrar o funcionamento do IPv6 será utilizado um método de transição denominado de Pilha Dupla. Para a simulação prática foi elaborado um cenário o qual demostrará a possibilidade de convergência entre IPv4 e IPv6.

1.2 Objetivos

1.2.1 Objetivo Geral

Demonstrar, por meio de pesquisas e simulação prática, os conceitos e aplicação do protocolo IPv6 e o mecanismo de transição Pilha Dupla.

1.2.2 Objetivos Específicos

- Demonstrar os conceitos do protocolo IPv6;
- Demonstrar os conceitos do mecanismo de transição Pilha Dupla;
- Demonstrar uma aplicação prática do protocolo IPv6 e do mecanismo de transição através de uma simulação prática;

2 DESENVOLVIMENTO

2.1 O Protocolo IPv6

Em 1993, o IESG (*Internet Engineering Steering Group*) criou um grupo de trabalho para uma nova versão do protocolo IP, o IpngWG (*IP Next Generation Working Group*), com base em alguns objetivos que deveriam ser alcançados. O grupo de trabalho, então, selecionou protocolos “candidatos” para a camada de rede da arquitetura TCP/IP. O vencedor foi o SIPP (*Simple Internet Protocol Plus*), por deferir menos do IPv4 e ter um plano de transição melhor. Mas uma combinação de aspectos positivos dos três protocolos candidatos foi feito e com isso gerou-se a recomendação para a versão 6 do IP em novembro de 1994.

A nova versão do protocolo IP foi desenvolvido com alguns objetivos, tendo em mente que deveria ser um passo evolucionário em relação à versão 4, mas não um passo radicalmente revolucionário. Funções desnecessárias foram removidas; funções que trabalhavam bem foram mantidas, e novas funcionalidades foram acrescidas.

O novo protocolo IP aumenta o espaço de endereçamento de 32 para 128 bits, suportando mais níveis de hierarquia de endereçamento, um número muito maior de nodos endereçáveis, e permitindo a autoconfiguração de nodos.

2.2 Implantação do IPv6

A implantação do IPv6 é necessária e inevitável. Embora o esgotamento dos endereços IPv4 não faça a Internet acabar, nem mesmo que ela deixe de funcionar, prevê-se que haverá uma diminuição na taxa de crescimento da rede e que algumas novas aplicações, que poderiam ser criadas, não serão. É possível também, que as conexões Internet fiquem mais caras.

No entanto, a implantação do IPv6 não será algo rápido. Também não haverá uma "data da virada" para a troca de protocolo. A migração do IPv4 para IPv6 acontecerá de forma gradual, com o IPv4 ainda em funcionamento. Desde modo, haverá incialmente um período de coexistência entre os dois protocolos.

E neste primeiro momento, manter a compatibilidade entre as versões do protocolo IP torna-se essencial para o sucesso da transição para o IPv6. Isto poderá ser obtido com a utilização dos mecanismos de transição, Tunelamento, Tradução e principalmente Pilha Dupla. O funcionamento desses mecanismos será apresentado no decorrer deste trabalho, porem o foco será o mecanismo de Pilha Dupla.

Entretanto, é importante que as redes estejam preparadas para o novo protocolo desde já. Quanto mais cedo q questão for entendida, e a implantação planejada, menores serão os gastos no processo, É para que essa implantação seja eficaz, é necessário que:

- As empresas e demais entidades tomem consciência da necessidade de implantar o IPv6;
- Técnicos busquem conhecimento sobre o IPv6 e realizem experiências com o novo protocolo;
- Na compra de novos equipamentos, software, ou na contratação de serviços, o suporte ao IPv6 seja exigido;
- Seja feito um planejamento detalhado sobre como será feito a implantação do novo protocolo;

É importante destacar que todos os RIRs (*Regional Intenet Registres*) já distribuem endereços IPv6 em suas regiões. O NIC.br é responsável pela distribuição de blocos no Brasil. Desde modo, provedores Internet e outras entidades que administrem Sistemas Autônomos (AS –*Autonomous System*) podem solicitar ao NIC.br blocos IPv6. Para isso, é preciso acessar o sítio web http://registro.br/info/cidr.html e preencher o formulário correspondente.

A distribuição de endereços é feita de forma hierárquica. Com os blocos IPv6 esta divisão acontece do seguinte modo:

– Cada RIR recebe da IANA um bloco um bloco /12;

– Os provedores recebem dos RIRs bloco /32;

Os provedores devem entregar aos seus cliente blocos variando entre /48 e /56 dependendo de suas necessidades:

– Um bloco /48 pode ser dividido em até 65.536 redes diferentes, cada uma com 18.446.744.073.709.551.616 endereços diferentes;

– Um bloco /56 pode ser dividido em até 256 redes diferentes, cada uma com 18.446.744.073.709.552.616 endereços diferentes.

Um /64 podes ser designado a um usuário se houver certeza de que apenas uma rede atende às suas necessidades. Isso pode ser o caso, por exemplo, de alguns usuários domésticos.

Outro fator que pode facilitar a transição entre os protocolos IP é o fato de já ser possível encontrar diversos aplicativos adaptados ao novo protocolo, e que os principais Sistemas Operacionais lançados nos últimos anos já estão preparados para suporte IPv6.

- **Microsoft Windows** - A primeira versão oficial de suporte ao IPv6 foi lançado junto com o Service Pack 1 para o Windows XP. Atualmente, as versões XP e SP3, Vista, 2003 Server, 2008 Server e CE apresentam uma versão mais aprimorada.
- **Linux** - O primeiro código relacionado ao IPv6 foi adicionado ao *Kernel* do Linux na versão 2.1.8, ainda com muitas limitações. Um suporte estável passou a ser complicado junto ao *Kernel* a partir da versão 2.2.x.
- **MAC OS X** - O suporte ao IPv6 acompanha o MAC OS X desde a versão 10.2 Jaguar e, por padrão, o IPv6 já vem habilitado.
- **BSD** - O FreeBSD apresenta suporte ao IPv6 desde a versão 4.0. Já com o NetBSD este é utilizado desde dezembro de 2000 na versão 1.5. No OpenBSD, a versão 2.7 já apresentava suporte ao IPv6.

Seguindo a mesma tendência, os principais modelos de equipamentos de rede também estão aptos a tratar o novo protocolo. Tão importante quanto o suporte nos softwares, o suporte em roteadores e switches é necessário para que estes estejam aptos a tratar o tamanho do endereçamento IPv6, seu impacto na tabela de rotas, além das mudanças nos protocolos de roteamento.

- **CISCO Systems** - Introduziu o suporte ao IPv6 a partir da versão 12,0(21) ST do Cisco IOS (*Internetworking Operacional System*), provendo o suporte ao IPv6 nos roteadores Cisco a partir das séries 12000 e 10720.
- **Juniper Networks** - Seus principais roteadores, T-Series e M-Series, apresentam suporte ao IPv6 desde a versão 5.1 do Sistema Operacional JUNOS, lançado em novembro de 2001.
- **Alcatel-Lucent** - Seu Sistema Operacional SR-OS, utilizado nos roteadores 7750SR e 7710SR, apresenta suporte a diversas funcionalidade do IPv6.
- **Hitachi** - Operando a pilha IPv6 desenvolvida pelo projeto KAME desde 2001, os roteadores GR2000 da família Gigabit *Router* oferecem entrega de pacotes IPv6 em alto-desempenho, além de suporte a QoS, túneis e filtros.
- **3Com Corporation** - Desde o final de 1997, os softwares para roteadores *NETBuilder*, desde a versão 11.0, e os *Switches PathBuilder* S500, possuem suporte ao IPv6.

Também podemos destacar diversas iniciativas que buscam incentivar io uso do IPv6. Todos os RIRs possuem políticas de estimulo e fomento a adoção do novo protocolo IP nas regiões por eles administradas.

O LACNIC, RIR que atua na América Latina e CARIBE, tem e destacado coordenando diversas inciativas para a adoção do IPv6 com atividades de divulgação e educação como:

- Desenvolvimento de um sítio *web* sobre o tema;
- Grupo de Trabalho LAC TF IPv6 (*IPv6 Task Force for Latin America and the Caribbean*);
- O Fórum Latino-Americano de IPv6 (FLIP-6);
- O IPv6 *Tour*;

No âmbito acadêmico existem diversos grupos de pesquisa pelo mundo, que trabalham no desenvolvimento de projetos relacionados ao protocolo IPv6, destacando-se os projetos:

- Rede CLARA (Cooperação Latino-Americana de Redes Avançadas);
- GÉANT2
- Internet2
- KAME

– USAGI(*Universal playground for IPv6*);

No Brasil, A RNP (Rede Nacional de Pesquisa) tem se destacado desde o projeto Br6Bone. Atualmente, toda a rede RNP está apta a operar com o protocolo IPv6 em modo nativo, além de poder fornecer conexão IPv6 a instituições localizadas nos estados servidos por sua rede. A RNP também possui conexão IPv6 nativa com outras redes acadêmicas e comerciais.

Órgãos governamentais também têm lançado ações para a implantação do IPv6 em alguns países. Seja através da recomendação do uso em suas repartições, ou mesmo ações mandatórias como correu nos EUA, existe em incentivo global por parte dos Governos no que diz respeito à utilização dessa nova versão do protocolo IP.

Segue abaixo alguns países que já adotaram ações para implementação do IPv6:

- **EUA -** Em setembro de 2003, o Departamento de Defesa estadunidense (*DoD – U.S. Department of Defense*) publicou um memorando determinando metas e o planejamento para a realização, até 2008, da transição para o IPv6 de toda a infraestrutura de sua rede. Baseados neste memorando, foram criados documentos definindo um conjunto de padrões técnicos e requisitos de interoperabilidade que devem ser seguidos por equipamentos e *softwares* utilizados nas redes do DoD. O Gabinete de Gestão e Orçamento dos EUA (*OMB – Office of Management and Budget*) também emitiu, em agosto de 2005, um memorando estabelecendo metas semelhantes às do DoD referentes às redes das Agências Governamentais Federais estadunidenses.
- **Brasil -** Em relação ao Governo Brasileiro, há a recomendação da arquitetura e-PING (Padrões de Interoperabilidade de Governo Eletrônico), que define um conjunto de premissas, políticas e especificações técnicas que visam regulamentar a utilização da Tecnologia de Informação Comunicação no Governo Federal. Esta recomendação expressa que os órgãos das Administrações Públicas Federais deverão se planejar para uma futura migração para IPv6 e prever suporte à coexistência dos protocolos IPv4 e IPv6 em novas contratações, compra de produtos de redes.

- **União Europeia** - A União Europeia já investiu, desde 2002, mais de €90 milhões em pesquisas relacionadas ao IPv6, podendo chegar a um total €300 milhões até 2013. Outro passo foi dado em 27 de maio de 2008, quando foi estabelecido como objetivo para a Europa que, em 2010, 25% das empresas, administrações públicas e usuários particulares já utilizem o IPv6. Também foi sugerido que os Estados-Membros exijam a utilização do IPv6 como condição para os contatos públicos e lancem campanhas de incentivo junto as empresas e organizações, além de ajuda-las na transição.
- **China** - O Governo Chinês iniciou a implantação de uma rede IPv6 chamada de *China Net Generation Internet*, investiu cerca de US$170 milhões, e envolvendo oito ministérios, cinco grandes companhias nacionais e várias redes nacionais de pesquisa. Também utilizou os jogos Olímpicos de Pequim 2008 para testar dispositivos moveis e sistemas inteligentes de transporte e de segurança operando sobre IPv6.
- **Japão** - O governo japonês oferece, desde 2000, incentivos fiscais para a adoção do IPv6, além de apoiar, criar e financiar projetos como o *IPv6 Promotion Council*, WIDE, KAME, USAGI, entre outros.

2.3 Cabeçalho do Protocolo IPv6

O IPngWG, grupo responsável pela implementação do IPv6, verificou que alguns campos e funções do protocolo IPv4, executavam tarefas que não eram necessárias, tornando o trabalho do protocolo lento. O IPv6 introduz um novo formato de cabeçalho (cabeçalho IPv6). Em oposição ao anterior (cabeçalho IPv4), todos os campos deste novo processamento dos pacotes pelos roteadores, visto que não há necessidade de calcular a extensão de certos campos, e nem o tamanho do cabeçalho como um todo. Alguns campos foram removidos, outros renomeados e movidos de lugar e outro adicionado. A redução ocorreu nas informações pelos roteadores.

O cabeçalho IPv6 é constituído por 8 campos, num total de 230 *bits*. A fragmentação é assegurada pela origem do pacote IPv6 e as verificações são efetuadas ao nível das camadas de *link* transporte. Adicionalmente, o pacote referente ao cabeçalho IPv6 e o campo de opções estão alinhados para 64 *bits* facilitando o processamento dos pacotes IPv6. Todas estas modificações irão aumentar substancialmente o desempenho do roteadores.

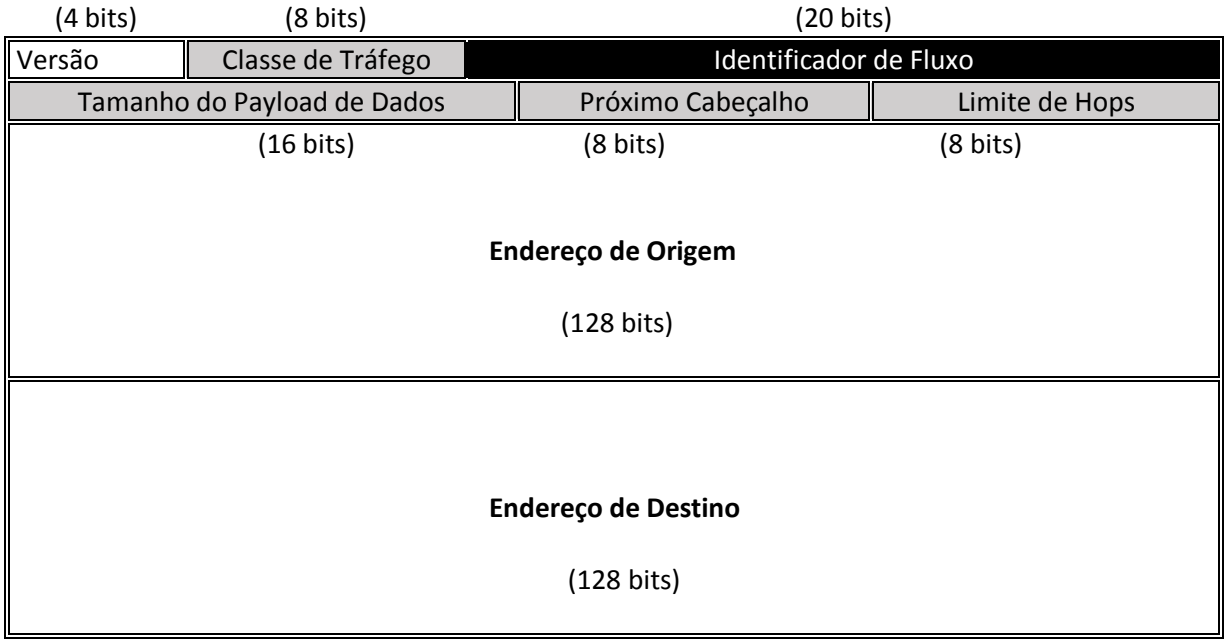

Figura 1: Cabeçalho do protocolo IPv6.

Fonte: Fonte: BUCKE BRITO (2013)

2.3.1 Campos do Cabeçalho

Versão (*Version*) – 4 bits – O campo versão é sempre seis para o IPv6 e quatro para o IPv4. Esse campo serve para os roteadores (camada de rede) identificarem qual é o protocolo do pacote. Porém, é possível que no futuro essa identificação seja feita no *Protocol Data Unit* da camada de enlace para maior rapidez, entretanto o *Service Data Unit* para seu manipulador correto na camada de rede. Isso viola o modelo de camadas ISSO/OSI, pois atribui uma função de uma camada mais acima para uma outra mais baixo.

Classe de Tráfego (*Traffic Class*) – 8 bits – Serve para identificar se o dado no pacote é de uma mídia contínua, como vídeo ou som, ou se é de outro tipo. Embora esse campo já exista no protocolo IP desde o seu início, ele é pouco utilizado pelos roteadores, e vários estudos para descobrir a melhor forma de uso deste campo ainda estão sendo realizados.

Identificação de Fluxo (*Flow Label*) – 20 bits – O campo de identificação de fluxo permite a criação de um "pseudocanal de conexão" entre uma fonte e um destino, que possui requerimentos e propriedades particulares.

Por exemplo: quando um roteador recebe um pacote com esse campo sendo não zero, ele identifica a qual fluxo de pacotes ele pertence. Se for um fluxo um *streaming* de vídeo pertencente a uma determinada aplicação, o roteador pode atribuir maior prioridade para esses

pacotes. Quando um outro pacote com o mesmo número de identificação de fluxo chegar, o roteador poderia enviá-lo diretamente para seu destino, sem precisar ler os campos de endereço. O valor desse campo deve receber um valor aleatório para cada "pseudocanal de conexão", para reduzir a possibilidade de existirem dois canais com o mesmo código, fazendo com que o roteador pense que é só um canal e envie os dados erroneamente pela mesma rota.

Tamanho dos Dados (*Playload Length*) – 16 bits – O campo de tamanho de dados diz quantos dos bytes do pacote acompanham o cabeçalho. É algo parecido com o campo "tamanho total" do IPv4, mas tem nome diferente porque os bytes do cabeçalho não são mais contados.

Próximo Cabeçalho (*Next Header*) – 8 bits – Esse é o campo que permite dizer quais das seis extensões de cabeçalho estão presentes, caso haja alguma. Foi ele quem permitiu transformar alguns campos do cabeçalho do IPv6 em campos opcionais.

Limite de Saltos (*Hop Limit*) – 8 bits – Esse é o campo utilizado para evitar que os pacotes tenham uma vida muito alta. Ele recebe um número, e cada salto entre roteadores, este é decrementado de uma unidade. O campo equivalente no cabeçalho IPv4 é o campo "tempo de vida", que determinava quantos segundos o pacote deveria existir.

2.3.2 Cabeçalhos de extensão

Diferente do IPv4, que inclui no cabeçalho base todas as informações opcionais, o IPv6 trata essas informações através de cabeçalhos de extensão. Estes, localizam-se entre o cabeçalho base e o cabeçalho da camada de imediatamente acima e, não possuem quantidade ou tamanho fixo. Caso existam múltiplos cabeçalhos de extensão no mesmo pacote, eles serão adicionados em série formando uma "cadeia de cabeçalhos. A figura abaixo exemplifica essa situação.

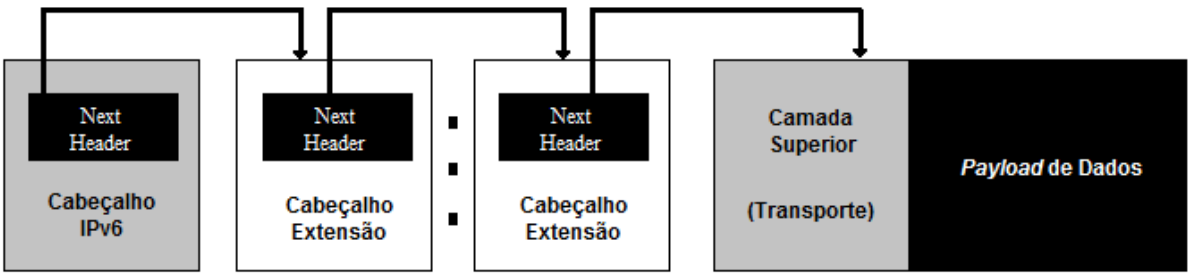

Figura 2: Encadeamento de cabeçalhos de extensão IPv6.

Fonte: BUCKE BRITO (2013)

Um ou mais cabeçalho de extensão são anexados ao cabeçalho IPv6 de maneira encadeada por meio dos seus respectivos códigos de próximo cabeçalho, o que provê flexibilidade para que sejam implementados diferentes funcionalidades. É recomendado que os cabeçalhos de extensão sigam a sequência de encadeamento detalhada com os códigos da tabela abaixo.

Tabela 1: Encadeamento dos cabeçalhos de extensão no IPv6.

Ordem	Nome do cabeçalho	Código no campo "Next Header"
01	Cabeçalho IPv6 convencional	-
02	*Hop-by-hop*	0
03	*Destination Options*	60
04	*Routing Header*	42
5	*Fragment Header*	44
06	*Authentication Header (AH)*	51
07	*Encapsulation Security Payload (ESP)*	50
08	*Destination Options*	60
09	*Mobility*	135
-	Ausência de próximo cabeçalho	59
Camada superior	ICMPv6	58
Camada superior	UDP	17
Camada superior	TCP	6

Fonte: BUCKE BRITO (2013)

Cabeçalho de extensão: *Hop-by-Hop*

Como o próprio nome já diz, esse é o único cabeçalho de extensão que é analisado por todos os roteadores intermediários no caminho entre a origem e o destino (salto a salto), motivo pelo qual é obrigatório que ele seja o primeiro cabeçalho de extensão depois do cabeçalho IPv6.

Assim que a extração do cabeçalho convencional e feito pelos roteadores, o código do campo "*Next Header*" equivale a 0, isso significa que um cabeçalho de extensão "Hop-by-Hop", deverá ser analisado. Contudo existe algumas diferenças. De acordo com Bucke Brito (BUCKE BRITO,2013):

> Caso o código do campo "*Next Header*" no cabeçalho IPv6 seja diferente de 0, esse cabeçalho de extensão não existe. Logo, os roteadores não analisam nenhum cabeçalho de extensão adicional.

Cabeçalho de extensão: *Destination Opitions*

Este cabeçalho é identificado pelo valor 60 no campo "*Next Header*", este cabeçalho dever ser processado apenas pelo host de destino. Ele é utilizado no suporte ao mecanismo de mobilidade ao IPv6, através da opção "Home Address" que contém o IP de origem do host móvel, quando está em trânsito.

Cabeçalho de extensão: *Routing*

Este cabeçalho lista um ou mais roteadores que devem ser visitado durante o percurso do pacote. Pode-se utilizar os dois tipos de roteamento, assim como no IPv4, *Strict e Loose*, com variação de poderem ser combinados. A figura abaixo indica seu formato.

0	8	16	24 31
NEXT HEADER	ROUTING TYPE	NUMBER ADDRESS	NEXT ADDRESS
RESERVED	BIT MAP		
1 – 24 ADDRESS			

Figura 3: Cabeçalho de extensão: Routing

Fonte: (IPV6.BR, 2012a)

O campo *Next Header* possui a mesma função de todos os outros cabeçalhos, ou seja, indica o próximo tipo de cabeçalho.

O campo *Routing Type* indica o tipo de roteamento, atualmente está definido como 0.

O campo *Number Address* indica o número de endereços presentes neste cabeçalho de 1 a 24.

O campo *Next Adress* indica o próximo endereço para o qual o pacote poderia ser enviado. Este campo inicia com 0 e é incrementado cada vez que um endereço é visitado.

O campo *Bit Map* é um mapa de bits que serve para indicar qual dos tipos de tratamento deve ser tomado a cada um dos roteadores. O endereço pode ser visitado diretamente depois do que o antecede (Strict) ou fazê-lo indiretamente, podendo existir roteadores intermediários (Loose).

Cabeçalho de extensão: Fragmentation

O IPv6, assim como o IPv4, implementa a fragmentação do pacote. A grande diferença se dá na maneira com que isto ocorre. No IPv4 cada roteador intermediário deveria fragmentar e reorganizar pacotes. No IPv6, a fragmentação é feita na origem, antes de enviar um pacote, e não ocorre nos roteadores intermediários. Caso haja a necessidade de uma fragmentação não esperada nos roteadores intermediários (mudança de rotas) eles encapsulam o datagrama em um novo e o fragmenta.

2.4 Endereçamento IPv6

A quantidade de endereços possíveis com um protocolo roteável de 128 bits chega a ser assustadora e muitas vezes torna-se difícil até mesmo conseguir visualizar o tamanho dos blocos de endereço a serem criados.

Enquanto no IPV4 temos 32 bits que nos possibilitam cerca de 4 bilhões de combinações (2^{32}), no IPV6 temos mais de 340 undecilhões de endereços possíveis. Para ter uma ideia do que isto representa, se convertêssemos cada IPv6 possível em um cm^2, poderíamos envolver toda a superfície do planeta Terra com 7 camadas de endereço.

Esta fartura de endereços muda o conceito de alocação de blocos IP de forma radical. Hoje os administradores de rede estão acostumados a calcular a quantidades de endereços IPs necessários para suprir as suas demandas baseados na quantidade de máquinas que irão possuir um endereço IP. Com o IPV6, pensa-se na quantidade de redes que podem ser oferecida ao usuário final.

Notação do Endereço

O endereço IPv6 de 128 bits é escrito em formato hexadecimal (base 16), dividindo-se em 8 grupos de 16 bits cada um e separando-se pelo caractere ":". Um exemplo comum de endereço seria:

2001:0bd8:cafe:0000:8e70:5aff:feee:10ac

Na representação dos Endereços IPv6, é indiferente utilizar letras maiúsculas ou minúsculas para escrever os algarismos alfanuméricos em hexadecimal, ou seja, o endereço anterior é a mesma que:

2001:0DB8:CAFÉ:0000:8E70:5AFF:FEEE:10AC

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:0:0:1.

– 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.

2.4.1 Tipos de Endereçamento IPv6

Tradicionalmente, há diferentes tipos de endereços que são associados à natureza da comunicação em redes de computadores. No IPv4, os endereços podiam ser de três tipos, a saber: *unicast, multicast e anycastt*. A comunicação de natureza *unicast* é aquela destinada a um único no especifico (um para um); a comunicação de natureza *multicast* é aquela destinada para vários nós de um grupo (um para muitos); e a comunicação *anycast* é aquela destinada a todos os nós (um para todos).

Endereços *Unicast*

Identifica apenas uma interface. Um pacote destinado a um endereço *unicast* é enviado diretamente para a interface associada ao endereço. Foram definidos vários tipos de endereços *unicast*, que são:

– *Global Provider-based*, ou baseado o Provedor: é o endereço unicast que será globalmente utilizado. Seu plano inicial de alocação baseia-se no mesmo esquema utilizado no CIDR (*Classless InterDomain Routing*, [RFC1519]) definido em [RFC1887]. Seu formato possui um prefixo de 3 bits (010) e cinco campos: registry ID, para registro da parte alocada ao provedor; *provider ID*, que identifica um

provedor especifico; *subscriber ID*, que identifica os assinantes conectados a um provedor; e infra-subscribe, parte utilizada por cada assinante.

- *Unspecified*: definido como 0:0:0:0:0:0:0:0 ou "::", indica a ausência de um endereço e nunca deverá ser utilizado em nenhum node. Este endereço só poderá ser utilizado como endereço de origem (*source address*) de estações ainda não inicializadas, ou seja, que ainda não tenha aprendido seus próprios endereços.
- *Loopback*: representado por 0:0:0:0:0:0:0:1 ou "::1". Pode ser utilizado apenas quando um node envia um pacote para sim mesmo. Não pode ser associado a nenhuma interface.
- *IPv4-based*, ou baseado em IPv4: um endereço IPv6 com um endereço IPv4 embutido. Formado anexando-se um prefixo nulo (96 bits zeros) a um endereço IPv4 como, por exemplo, ::172.16.25.32. Este tipo de endereço foi incluído como mecanismo de transição para hosts e roteadores tunelarem pacotes IPv6 sobre roteamento IPv4. Para hosts sem suporte a IPv6, foi definido um outro tipo de endereço (*IPv4-mapped IPv6*) da seguinte forma: ::FFFF:172.16.25.32.
- NSAP: endereço de 121 bits a ser definido pelo prefixo 0000001. Endereços NSAP (*Network Service Access Point*) são utilizados em sistema OSI.
- IPX: endereço de 121 bits a ser definido, identificado pelo prefixo 0000010. Endereços IPX(*Internal Packet eXchange*) são utilizados em redes Netware/Novell.
- Link-local: endereço identificado pelo prefixo de 10 bits (1111111010), definido para uso interno num único link. Estações ainda não configuradas, ou com um endereço *provider-based* ou com um site-local, poderão utilizar um endereço link-local.
- Site-local: endereço identificado pelo prefixo de 10 bits (1111111011), definido para uso interno uma organização que não se conectará à Internet. Os roteadores não devem repassar pacotes cujos endereços origem sejam endereços site-local.

Também está reservado 12,5% de todo espaço de endereçamento IPv6 para endereços a serem distribuídos geograficamente (*geographic-based*).

Endereços Multicast

Os endereços de *multcast* não são uma novidade do IPv6. Eles já existiam no IPV4 por meio dos endereços de Classe D (de 224.0.0.0 até 239.0.0.0) utilizados por aplicações com

comunicação de natureza “um para muitos”, como, por exemplo, serviços multimídia de teleconferência, serviços de monitoramento distribuído etc.

Há detalhes técnicos envolvidos na formação do prefixo *multicast* que o leitor pode consultar na RFC 3306. Conforme Bucke Brito (BUCKE BRITO,2013):

> Uma observação é que os endereços *multicast* jamais devem ser utilizados na origem de uma comunicação, uma vez que ele representa um grupo compostos por múltiplos nós.

Tabela 2: Endereços multicast do IPv6.

Endereço	Escopo	Descrição
FF01 : : 1	Interface	Todas as interfaces
FF02 : : 1	Enlace	Todos os hosts no link
FF02 : : 2	Enlace	Todos os roteadores no link
FF02 : : 5	Enlace	Protocolo OSPFv3 (roteadores)
FF02 : : 6	Enlace	Protocolo OSPFv3 (roteadores designados)
FF02 : : 9	Enlace	Protocolo RIPng
FF02 : : A	Enlace	Protocolo Cisco®/EIGRP
FF02 : : 1 : FFXX:XXXX	Enlace	*Solicited-Node*
FF02 : : 1:2	Enlace	Todos os servidores DHCP e *relay-agents*
FF05 : : 1:3	Site	Todos os servidores DHCP
FF0X : : 101	Variável	Todos os servidores NTP

Fonte: BUCKE BRITO (2013)

Endereços Anycast

Identifica um grupo de interfaces de nodes diferentes. Um pacote destinado a um endereço *anycast* é enviado para uma das interfaces identificadas pelo endereço. Especificamente, o pacote é enviado para a interface mais próxima de acordo com a medida de distância do protocolo de roteamento.

Devido à pouca experiência na Internet com esse tipo de endereço, incialmente seu uso será limitado:

– Um endereço *anycast* não pode ser configurado como endereço de origem (*source address*) de um pacote IPv6;

– Um endereço *anycast* não pode ser configurado num host IPv6, ou seja, ele deverá ser associado a roteadores apenas.

Este tipo de endereçamento será útil na busca mais rápida de um determinado servidor ou serviço. Por exemplo, pode-se definir um grupo de servidores de nomes configurados com um endereço *anycast*; o host acessará o servidor de nomes mais próximo utilizando este endereço.

2.5 Serviços Básicos IPv6

2.5.1 ICMPv6

Além de exercer algumas funções desempenhadas pelos protocolos ARP, RARP e IGMP, o protocolo ICMPv6, traz consigo todas as funções do seu antecessor ICMPv4, e uma série de novos recurso. Conforme Florentino (FLORENTINO, 2012):

> Para que possamos ter exata noção de sua importância, se deixarmos o firewall das estações de trabalho bloquearem toda e qualquer mensagem ICMPv6, a rede simplesmente irá parar, pois são mensagens deste tipo as responsáveis pela descoberta de vizinhança, atribuição de endereços *Stateless* e pela descoberta de roteadores e gateways em redes IPv6.

O ICMPv6 é integrado ao IPv6 por meio da sinalização do código 58 no campo "Próximo Cabeçalho" do cabeçalho convencional do IPv6, o que implica na inserção de um novo cabeçalho do ICMPv6 com suas funcionalidades adicionais. O Cabeçalho ICMPv6 é bastante simples. Ele contém dois campos de tipo/código para representar o formato das mensagens de controle, um campo de verificação de erros para checar a integridade das mensagens de controle e um campo de tamanho varável com a mensagem propriamente dita.

O ICMPv6, para o IPv6, tem basicamente as mesmas funções do ICMP, para o IPv4. Ou seja, é utilizado para:

– Informar características da rede;
– Realizar diagnósticos;
– Relatar erros no processamento de pacotes;

Estas informações são obtidas através da troca de mensagens ICMPv6, que são divididas em duas classes:

- Mensagem de Erro;
- Mensagem de Informação

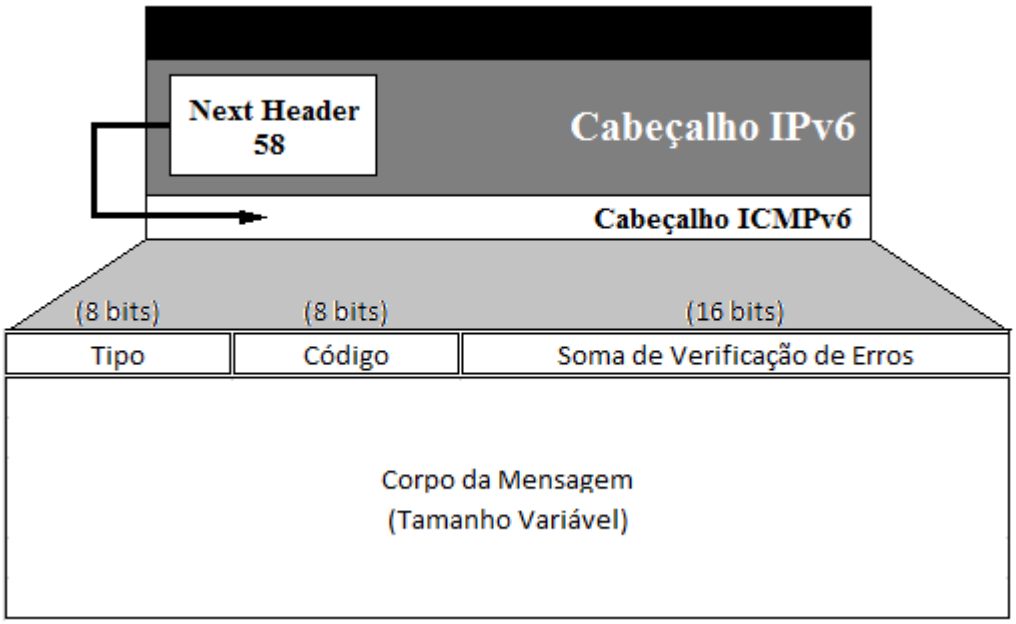

Figura 4: Cabeçalho do ICMPv6.

Fonte: BUCKE BRITO (2013)

O ICMPv6 apresenta uma quantidade maior de mensagens que a versão utilizada com o IPv4. Isto ocorre, porque além das funções básicas atribuídas ao ICMP, o ICMPv6 também passa a incorporar as funções de outros protocolos com ARP/RARP (*Address Resolution Protocol – Reverse Address Resolution Protocol*) e IGMP (*Internet Group Management Protocol*) por exemplo, sendo essencial em serviços do IPv6 como:

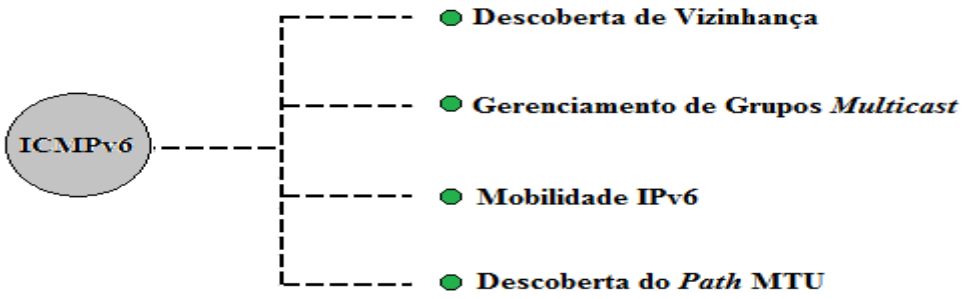

Figura 5: Serviços IPv6 onde o ICMPv6 é essencial.

Fonte: (IPV6.BR, 2012a)

Tabela 3: Mensagens de erro ICMPv6.

Tipo	Grupo	Código	Descrição
1	Destino inalcançável	0	Sem rota para o destino
		1	Comunicação com destino administrativamente proibida
		2	Além do escopo do endereço da origem
		3	Endereço inalcançável
		4	Porta inalcançável
		5	Falha na política de ingresso/egresso
		6	Destino rejeitado
2	Pacote muito grande	0	Pacote ultrapassou o MTU
3	Tempo excedido	0	Limite de saltos excedido
		1	Limite de remontagem de fragmentação excedido
4	Problema de parâmetro	0	Campo inválido no cabeçalho IPv6
		1	Próximo cabeçalho inválido
		2	Opções inválidas
127	-	-	Reservado para novas mensagens de erro

Fonte: BUCKE BRITO (2013)

Tabela 4: Mensagens de informação do ICMPv6.

Tipo	Grupo	Código	Descrição
128	*Echo Request*	0	Utilizado no ping
129	*EchoReply*	0	Utilizado no ping
255	-	-	Reservado para novas mensagens de informação

Fonte: BUCKE BRITO (2013)

2.5.2 DESCOBERTA DE VIZINHAÇA

O IPv6 utiliza o protocolo de Descoberta de Vizinhança, que já era utilizada no IPv4, que foi replanejado, aprimorado e expandido. Esse protocolo é utilizado por hosts e roteadores para os seguintes fins:

- Divulgar o endereço MAC dos nós a rede;
- Encontrar roteadores vizinhos;
- Determinar prefixos e outras informações de configuração de rede;

- Detectar endereços duplicados;
- Determinar a acessibilidade dos roteadores;
- Redirecionamento de pacotes;
- Autoconfiguração de endereços;

Podemos ver que estão listados ai em cima funções dos protocolos ARP, ICMP e DHCP. Para desempenhar essas funções o protocolo de descoberta de vizinhança se utiliza das mensagens ICMP. Abaixo está a lista das cinco mensagens utilizadas por ele:

- ***Router Advertisement*** – Enviadas periodicamente, ou em resposta a uma *Router Solicitation*, pelos roteadores da rede para anunciar sua presença em um enlace e na internet.
- ***Router Solicitation*** – Utilizada por hosts para requisitar aos roteadores mensagens *Router Advertisements* imediatamente;
- ***Neighbor Solicitation*** – Mensagem *multicast* enviada por um nó para determinar o endereço MAC e a acessibilidade de um vizinho, além de detectar a existência de endereços duplicados;
- ***Neighbor Advertisement*** – Enviada como resposta a uma *Neighbor Solicitation*, pode também ser enviada para anunciar a mudança de algum endereço MAC dentro do enlace;
- ***Redirect*** – Utilizada por roteadores para informar ao host um roteador mais indicado para se alcançar um destino.

Todas essas mensagens possuem o campo “Máximo de saltos” no cabeçalho IPv6 setado como 255. Dessa forma essa mensagem fica restrita a um único enlace pois, como está configurado o limite de saltos, esse pacote não será encaminhado pelos roteadores. Essas mensagens que possuam um valor máximo de saltos diferente de 255 serão descartado pelos roteadores.

2.5.3 PATH MTU Discovery

MTU (*Maximum Transmission Unit*, que significa Unidade Máxima de Transmissão, e refere-se ao tamanho do maior datagrama que uma camada de um protocolo de comunicação pode transmitir) menor que o definido no host de origem é encontrado no meio do caminho, este pacote é descartado e uma mensagem *ICMPv6 Packet Too Big* é enviada para a origem, a fim de que este diminua a tamanho do MTU para que os dados possam passar por aquele roteador remoto.

Como em uma transmissão TCP/IP o caminho pode ser alterado várias vezes durante uma transmissão, o MTU vai sendo moldado de acordo com a necessidade. O tamanho mínimo de MTU em uma rede IPv6 é 1280. Não é recomendável alterá-lo para um valor menor.

O IPv6 traz em si uma promessa de poder manipular pacotes bem maiores, de até 4 gigabytes de tamanho, algo equivalente a um DVD inteiro nos dias de hoje. Isso é muito atraente para redes de alta confiabilidade e desempenho que precisam rotear grandes volumes de dados como nos data centers modernos. Esses valores extrapolam inclusive a capacidade máxima de transmissão dos protocolos da camada de transporte (TCP e UDP) e são necessárias modificações nesses protocolos para que o suporte a *jumbo frames* (frames ethernet com mais de 1500 bytes de Payload) possa se tornar realidade.

2.5.4 DNS

O DNS é tradicional serviço de resolução de nomes, responsável por tornar a complexidade dos endereços IP na Internet (ou mesmo em redes internas) em algo totalmente transparente para seus usuários. Isso somente é possível porque existem vários servidores raízes espalhados pelo mundo quem mantêm registros, contendo o mapeamento entre endereços e seus respectivos nomes, de forma que para o usuário basta fazer o acesso por meio dos nomes de domínio. Cabe ao serviço de DNS fazer a tradução dos nomes de domínio para o respectivo endereço IP de host.

Ao contrário do DHCP, em que existem serviços distintos para se trabalhar com IPv4 e Ipv6, um servidor DNS pode conter registros de nomes tanto do tipo A (Ipv4) quanto do tipo AAAA (Ipv6). Na verdade, não é preciso nem mesmo que o servidor esteja em pilha dupla com

endereços das duas famílias. Ou seja, é possível fazer pesquisas Ipv6 que são processadas apenas através de um endereço Ipv4 e vice-versa.

Nos próximos anos a adoção do Ipv6 tende a crescer significativamente, isso quer dizer que teremos cada vez mais hosts Ipv6 na Internet e também nas redes internas. Apesar de a estrutura do Ipv6 apresentar várias mudanças vistas até agora, a transição deve ser totalmente transparente para o usuário, afinal, para ele, o que existe é a internet, independente da sua arquitetura ser baseada em Ipv4 ou Ipv6. Os usuários estão habituados a realizar os acessos por meio dos nomes de domínio. Por isso, é importante a configuração de novos registros nos servidores DNS apontando para endereços Ipv6 dos hosts.

2.5.5 QoS

Qualidade de serviço (QoS), também conhecido como CoS em ambientes Cisco (*Class of Services*) desempenha um papel crucial nas redes modernas, com o objetivo de classificação da banda através de sua priorização, garantindo assim que aplicações sensíveis a atraso, como atividades em tempo real, estejam protegidas.

A classificação de tráfego pode ser feira manualmente, onde pode-se dividir por aplicações, porta, endereço IP ou até mesmo por equipamento conectado à rede. Tal flexibilidade de operação faz do QoS hoje, uma ferramenta indispensável principalmente em meios corporativos.

2.6 MECANISMO DE TRANSIÇÃO IPv6

2.6.1 Pilha-dupla

Técnica que consiste em instalar é operacionalizar ambos os protocolos IPv4 e IPv6 nas máquinas da rede e demais dispositivos da infraestrutura, de maneira gradativa, que implica na existência de duas redes em paralelo. Ao fazê-lo, um nó que esteja operando em pilha-dupla pode conversar com os nós que estejam operando apenas com o IPv4 ou apenas com oIPv6.

Essa estratégia facilita o processo de transição até o resultado seja um ambiente operacional totalmente baseado no IPv6.

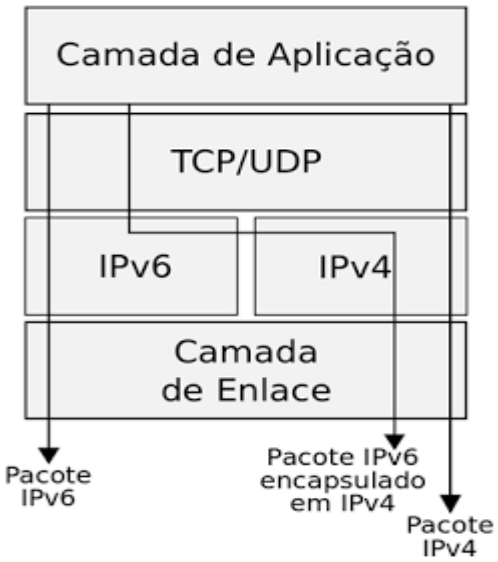

Figura 6: Funcionamento da pilha dupla.

Fonte: BUCKE BRITO (2013)

Alguns aspectos referentes à infraestrutura da rede devem ser considerados ao se implementar a técnica de pilha dupla: a estrutura do serviço de DNS e a configuração dos protocolos de roteamento e de firewalls.

Quando existem ambos os protocolos IPv6 e IPv4 em operação na maquinas da rede, as buscas por nomes do DNS podem retornar apenas A (IPv4), apenas registos AAAA (IPv6) ou ambos os registros A e AAAA. A forma de tratar essa situação varia em função da aplicação utilizada pelo usuário, e essa característica pode influenciar na percepção do usuário em relação ao desempenho da rede.

A configuração do roteamento IPv6 normalmente é independente da configuração do roteamento IPv4. Isto implica no fato de que, se antes de implementar-se o IPv6 a rede utiliza apenas o protocolo de roteamento interno OSPFV2 (com suporte apenas ao IPv4), será necessário migrar para um protocolo de roteamento que suporte tanto IPv6 quanto IPv4 (como ISIS por exemplo) ou forçar a execução do OSPFv3 paralelamente ao OSPFv2.

A filtragem do pacotes que trafegam na rede, pode depender da plataforma que se estiver utilizando. Em um ambiente Linux, por exemplo, os filtros de pacotes são totalmente

independentes um dos outros, de modo que o iptables filtra apenas pacotes IPv4 e o ip6tables apenas IPv6, não compartilhando nenhuma configuração.

3 SIMULAÇÃO PRÁTICA

A simulação da técnica de Pilha-dupla será realizada através do aplicativo de simulação de topologias de rede, chamado *Cisco Packet Tracer* – versão 6.0.1.0011, desenvolvido pela Cisco *Systems*®. A topologia é constituída pelos seguintes equipamentos: 2 roteadores Cisco 2911, 4 *switches* Cisco 2960 -24TT e 8 computadores com interface de rede *FastEthernet.* Na sequência, pode-se observar a topologia montada, bem como o plano de endereçamento IPv6 e IPv4 utilizado.

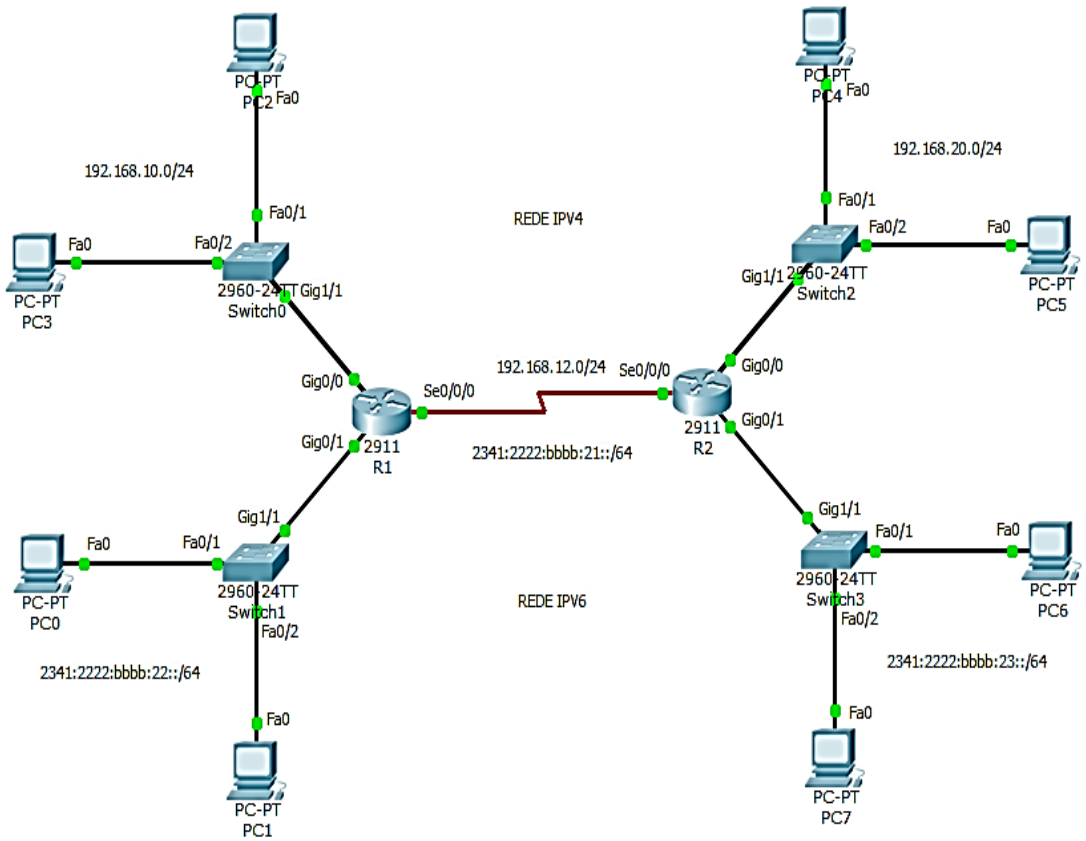

Figura 7: Topologia Pilha Dupla.

Fonte: Autoria Própria

Abaixo segue de forma detalhada o plano de endereçamento de todos os dispositivos e suas respectivas interfaces utilizadas na topologia de rede em Pilha-dupla.

Tabela 5: Endereçamento dos dispositivos.

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	Gig0/0	192.168.10.1	255.255.255.0	N/A
	Gig1/0	2341:2222:bbbb:22::1	/64	N/A
	Se0/0/0	192.168.12.1	255.255.255.0	N/A
R2	Gig0/0	192.168.20.1	255.255.255.0	N/A
	Gig1/0	2341:2222:bbbb:23::1	/64	N/A
	Se0/0/0	192.168.12.2	255.255.255.0	N/A
PC0	NIC	2341:2222:bbbb:22::10	/64	2341:2222:bbbb:22::1
PC1	NIC	2341:2222:bbbb:22::20	/64	2341:2222:bbbb:22::1
PC2	NIC	192.168.10.10	255.255.255.0	192.168.10.1
PC3	NIC	192.168.10.20	255.255.255.0	192.168.10.1
PC4	NIC	192.168.20.10	255.255.255.0	192.168.20.1
PC5	NIC	192.168.20.20	255.255.255.0	192.168.20.1
PC6	NIC	2341:2222:bbbb:23::10	/64	2341:2222:bbbb:23::1
PC7	NIC	2341:2222:bbbb:23::20	/64	2341:2222:bbbb:23::1

Fonte: [Autoria própria].

O proposito inicial desse trabalho consiste em simular o processo de funcionamento do mecanismo de transição *Dual Stack* ou Pilha-dupla. Na conexão dos roteadores, as interfaces seriais foram utilizadas máscaras de sub-rede /24 para rede IPv4 e /64 para rede IPv6. Para as redes locais, foram utilizadas mascaras de sub-rede /24 para rede IPv4 e /64 para rede IPv6.

Nessa topologia foram implementadas apenas as configurações das interfaces de comunicação entre os roteadores R1 e R2, assim como as interfaces da rede local. Os seguintes protocolos foram utilizados: RIPv2 - *Routing Information Protocol – Version 2 e Unicast.* O processo de configuração foi adotado apenas no roteador R1, porem o processo será o mesmo para o roteador R2.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#interface g0/0
```

```
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown

R1(config-if)#exit
R1(config)#
R1(config)#interface s0/0/0
R1(config-if)#ip address 192.168.12.1 255.255.255.0
R1(config-if)#no shutdown

R1(config)#interface g0/1
R1(config-if)#ipv6 address 2341:2222:bbbb:22::1/64
R1(config-if)#no shutdown

R1(config)#interface s0/0/0
R1(config-if)#ipv6 address 2341:2222:bbbb:21::/64 eui-64
R1(config-if)#^Z
```

Configuração do RIP v2 no roteador R1.

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#no auto-summary
R1(config-router)#network 192.168.10.0
R1(config-router)#network 192.168.12.0
R1(config-router)#^Z
```

Configuração Unicast no roteador R1.

```
R1(config)#ipv6 unicast-routing
R1(config)#ipv6 router rip CISCO
R1(config-rtr)#exit
R1(config)#interface g0/1
R1(config-if)#ipv6 rip CISCO
R1(config-if)#ipv6 rip CISCO enable
R1(config-if)#exit
R1(config)#interface s0/0/0
R1(config-if)#ipv6 rip CISCO enable
R1(config-if)#^Z
```

O comando **show ipv6 interface brief** mostra um resumo das interfaces configuradas com IPv4 em R1.

```
R1>show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

GigabitEthernet0/0     192.168.10.1    YES manual up                    up

GigabitEthernet0/1     unassigned      YES unset  up                    up

GigabitEthernet0/2     unassigned      YES unset  administratively down down

Serial0/0/0            192.168.12.1    YES manual up                    up

Serial0/0/1            unassigned      YES unset  administratively down down

Vlan1                  unassigned      YES unset  administratively down down
R1>
```

O comando **show ipv6 interface brief** mostra um resumo das interfaces configuradas com IPv6 em R1.

```
R1#show ipv6 interface brief
GigabitEthernet0/0        [up/up]
GigabitEthernet0/1        [up/up]
   FE80::201:43FF:FE40:2102
   2341:2222:BBBB:22::1
GigabitEthernet0/2        [administratively down/down]
Serial0/0/0               [up/up]
   FE80::203:E4FF:FE93:8401
   2341:2222:BBBB:21:203:E4FF:FE93:8401
Serial0/0/1               [administratively down/down]
Vlan1                     [administratively down/down]
```

O comando **show ip route** mostra as melhores rotas para as redes conhecidas pelo roteamento IPv4 em R1.

```
R1>show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
```

```
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
    192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/24 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
R    192.168.20.0/24 [120/1] via 192.168.12.2, 00:00:18, Serial0/0/0
R1>
```

O comando **show ipv6 route** mostra as melhores rotas para as redes conhecidas pelo roteamento IPv6 em R1.

```
R1#show ipv6 route
IPv6 Routing Table - 6 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 - ISIS 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   2341:2222:BBBB:21::/64 [0/0]
     via ::, Serial0/0/0
L   2341:2222:BBBB:21:203:E4FF:FE93:8401/128 [0/0]
     via ::, Serial0/0/0
C   2341:2222:BBBB:22::/64 [0/0]
     via ::, GigabitEthernet0/1
L   2341:2222:BBBB:22::1/128 [0/0]
     via ::, GigabitEthernet0/1
R   2341:2222:BBBB:23::/64 [120/2]
     via FE80::2D0:97FF:FE01:4201, Serial0/0/0
L   FF00::/8 [0/0]
     via ::, Null0
```

O comando **show running-config** mostra as configurações em execução no roteador R1.

```
R1#show running-config

Building configuration...

Current configuration : 1000 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname R1
!
ipv6 unicast-routing
!
license udi pid CISCO2911/K9 sn FTX152418V1
!
spanning-tree mode pvst
!
interface GigabitEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2341:2222:BBBB:22::1/64
```

```
 ipv6 rip CISCO enable
!
interface GigabitEthernet0/2
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface Serial0/0/0
 ip address 192.168.12.1 255.255.255.0
 ipv6 address 2341:2222:BBBB:21::/64 eui-64
 ipv6 rip CISCO enable
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 network 192.168.10.0
 network 192.168.12.0
 no auto-summary
!
ipv6 router rip CISCO
!
ip classless
```

```
!
line con 0
!
line aux 0
!
line vty 0 4
 login
!
end
R1#
```

4 CONCLUSÃO

A estratégia da Pilha Dupla é bem-vista do ponto de vista de desenvolvimento da Internet, porque é considerada uma estratégia evolucionista no sentido em que o IPv6 está inserindo na rede de forma gradativa, o que implica em maior maturidade no processo de aprendizado da operação do novo protocolo. Espera-se que, por meio desse esforço, as empresas entendam que o IPv6 é o substituto natural e sintam confiança até que haja maturidade para desligar o IPv4.

O referencial teórico neste trabalho aliado a simulação prática, nos proporcionou analisar a técnica de Pilha Dupla, e mostrou que através de algumas configurações especificas é possível que os dois protocolos IPv4 e IPv6, possam coexistir em uma mesma rede.

REFERÊNCIAS

BUCKE BRITO, S.H. O Novo Protocolo da Internet. [S.l.]: Novatec Editora, 2013.

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

IPV6.BR. Cursos IPv6. Disponível <http://douglassilva.com.br/cursos/ipv6/ipv6_mod3.htm/>.

TÉCNOLOGIA, REDES E SEGURANÇA. Método de Transição Pilha Dupla IPv4/IPv6. Disponível <http://tecnologiaredeseseguranca.blogspot.com.br/2011/10/metodo-de-transicao-pilha-dupla.html/>.