

**UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DEPARTAMENTO ACADÊMICO DE INFORMÁTICA
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES**

LUCAS LOSS STOLFO

**IMPLANTAÇÃO DO PROTOCOLO IPV6 EM UM PROVEDOR DE ACESSO A
INTERNET**

TRABALHO DE CONCLUSÃO DE CURSO

PATO BRANCO

2015

LUCAS LOSS STOLFO

**IMPLANTAÇÃO DO PROTOCOLO IPV6 EM UM PROVEDOR DE ACESSO A
INTERNET**

Trabalho de Conclusão de Curso, apresentado ao II Curso de Especialização em Redes de Computadores, da Universidade Tecnológica Federal do Paraná, câmpus Pato Branco, como requisito parcial para obtenção do título de Especialista.

Orientador(a): Prof(a). Adriano Serckumecka

PATO BRANCO

2015

TERMO DE APROVAÇÃO

Implantação do Protocolo IPV6 em um Provedor de Acesso a Internet

por

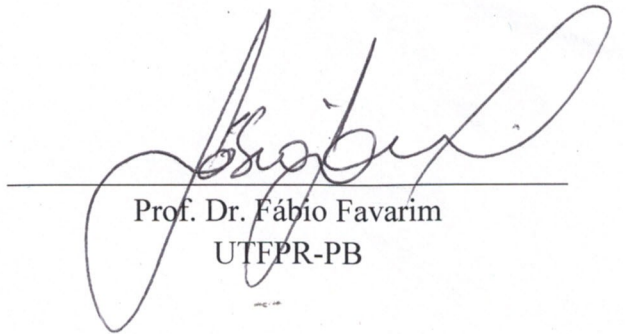
Lucas Loss Stolfo

Esta monografia foi apresentada às 21h10min do dia 27 de outubro de 2015, como requisito parcial para obtenção do título de ESPECIALISTA, no II Curso de Especialização em Redes de Computadores – Configuração e Gerenciamento de Servidores e Equipamentos de Redes, da Universidade Tecnológica Federal do Paraná, Câmpus Pato Branco. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho **aprovado**.

Banca Examinadora



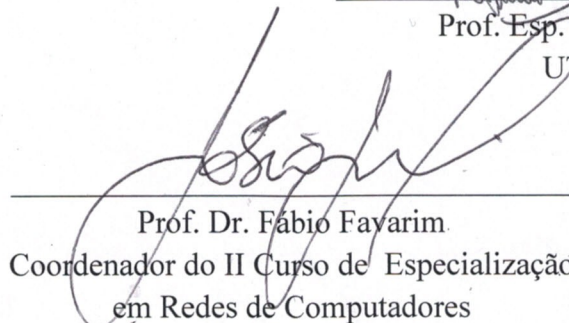
Prof. M.Sc. Adriano Serckumecka
Orientador / UTFPR-PB



Prof. Dr. Fábio Favarim
UTFPR-PB



Prof. Esp. Rudinei Silvestro
UTFPR-PB



Prof. Dr. Fábio Favarim
Coordenador do II Curso de Especialização
em Redes de Computadores

AGRADECIMENTOS

Primeiramente gostaria de agradecer a UTFPR Câmpus Pato Branco pelo esforço realizado para que este curso de pós-graduação fosse realizado.

Agradeço ao professor Adriano Serckumecka por sua honrosa orientação e sua dedicação a este trabalho.

Agradeço a minha esposa Tahis Baú pela compreensão nos dias em que não estive presente para que eu pudesse fazer parte desta turma.

*“O insucesso é apenas uma
oportunidade para recomeçar de novo
com mais inteligência”.*
Henry Ford

RESUMO

STOLFO, Lucas Loss. Implantação do Protocolo IPv6 em um Provedor de Acesso a Internet. 47 Monografia (II Curso de Especialização em Redes de Computadores) - Universidade Tecnológica Federal do Paraná. Pato Branco, 2015.

É evidente a escassez dos endereços IPv4, em 2011 definitivamente esgotou-se no estoque central pertencente a IANA (*Internet Assigned Numbers Authority*), isso quer dizer que cada região do planeta pode contar apenas com seu estoque local. A primeira região a ter seu estoque zerado foi a Ásia, gerida pela APNIC (*Asia-Pacific Network Information Center*). Com a criação de um novo protocolo o IPv6, imaginava-se que a implementação aconteceria de forma gradual e que em poucos anos as maiores entidades estariam utilizando somente o novo protocolo. Porém o crescimento da Internet se deu de uma forma muito maior do que o que se esperava e essa implementação acabou não acontecendo e hoje apenas aproximadamente 10% dos sites disponíveis na Internet estão configurados para serem acessados via IPv6. Neste trabalho tem-se o intuito de implementar o protocolo dentro do provedor e preparar a estrutura para que os clientes possam começar a receber os novos IPs.

Palavras-chave: Endereçamento IP. Protocolos. Dispositivos de Rede. IPv6.

ABSTRACT

STOLFO, Lucas Loss. IPv6 Protocol Implementation in a Internet Access Provider. 47 Monografia (II Curso de Especialização em Redes de Computadores) - Universidade Tecnológica Federal do Paraná. Pato Branco, 2015.

The shortage of IPv4 addresses in 2011 finally ran out in the middle stock clearly owned by IANA (Internet Assigned Numbers Authority), this means that each region of the world be can rely on your stock. The fist region to heve its stock was reset to asia, managed by APNIC (Asia-Pacific Network Information Center). By creation of the new protocol IPv6, it was thought that the implementation happen gradually and in a few yeats the lager entities would be using only the new protocol. But the growth of the Internet occurred in a much greater way than what we expected and this implementation did not happen and today only about 10% of websites available on the Internet are configured to be accessed through IPv6. This work has the aim to implement the protocol within the provider and prepare the framework to allow customers to start receiving new IP.

Keywords: IP Address. Protocols. Network Devices. IPv6.

LISTA DE FIGURAS

Figura 1 – Arvore DNS.....	26
Figura 2 – Topologia da rede em que foi implantado o protocolo IPV6.....	28

LISTA DE QUADROS

Quadro 1 – Configuração da interface GigabitEthernet1/1 roteador cisco	31
Quadro 2 – Interfaces do roteador cisco devidamente configuradas.....	32
Quadro 3 – Teste de comunicação IPv4 e IPv6.....	32
Quadro 4 – Configuração do BGP roteador Cisco.....	33
Quadro 5 – ASNs designados pelo Registro BR para as entidades	33
Quadro 6 – Filtros de permissão.....	34
Quadro 7 – Address-family ipv6.....	34
Quadro 8 – route-map (mapa de rota).....	34
Quadro 9 – Mostragem dos testes de sessão BGP.....	35
Quadro 10 – configuração de IPv6 de forma permanente em um servidor linux	34
Quadro 11 – Testando a configuração.....	36
Quadro 12 – Configuração do firewall em um dos servidores.....	37
Quadro 13 – Configuração do radvd.conf.....	41
Quadro 14 – Configuração do dhcpd.conf.....	41
Quadro 15 – Configuração do named.conf.....	43
Quadro 16 – Configuração dos arquivos 2804:1C30:0000:0001.ip6.int e 2804:1C30:0000:0001.ip6.arpa.....	43

LISTA DE TABELAS

Tabela1. Subdivisão dos endereçamentos IPV4.....	18
Tabela 2. Planejamento da estrutura em IPv6.....	30

LISTA DE ABREVIATURAS, SIGLAS E ACRÔNIMOS

APNIC	Asia Pacific Network Information Center
ARPA	Advanced Research and Projects Agency
AS	Autonomous System
BGP	Border Gateway Protocol
CGI	Comitê Gestor da Internet
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EGP	Exterior Gateway Protocol
IANA	Internet Assigned Numbers Authority
IBOPE	Instituto Brasileiro De Opinião Pública E Estatística
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
LACNIC	Latin American and Caribbean Internet Addresses Registry
MAC	Media Access Control Address
MBGP	Multiprotocol Border Gateway Protocol
NAT	Network Address Translation
RADVD	Router Advertisement Daemon
RFC	Request for Comments
TCP	Transmission Control Protocol

SUMÁRIO

1 INTRODUÇÃO.....	14
1.2 OBJETIVOS.....	16
1.2.1 Objetivo Geral.....	16
1.2.2 Objetivos Específicos.....	16
1.3 JUSTIFICATIVA.....	16
2 REFERENCIAL TEÓRICO.....	17
2.1 Protocolo IPV4.....	17
2.2 Protocolo IPv6.....	18
2.3 Protocolo BGP.....	19
2.4 Protocolo DHCP.....	20
2.5 DHCPv6.....	21
2.6 Protocolo RADVD.....	22
2.7 Firewall ou Filtragem de pacotes (Iptables e Ip6tables).....	22
2.8 Serviço de nomes e domínios (DNS).....	24
2.9 Sistemas Autônomos (AS).....	26
3 DESENVOLVIMENTO.....	28
4 MATERIAIS E MÉTODOS.....	29
5 RESULTADOS.....	31
5.1 Configuração das Interfaces.....	31
5.2 Configuração do protocolo BGP.....	32
5.3 Configuração dos demais dispositivos da rede.....	35
5.3.1 – Configurando o firewall de entrada em servidores linux.....	37
5.3.2 – Instalação e configuração do RADVD.....	40
5.3.3 – Configuração do DHCPv6.....	41
5.4 Configuração do DNS e Zona reversa.....	42
5.4.1 Instalação dos serviços.....	42
5.4.2 Configuração.....	42
6 CONCLUSÃO.....	44
6.1 TRABALHOS FUTUROS.....	44
REFERÊNCIAS.....	45

1 INTRODUÇÃO

Devido a um fator conhecido como Internet das coisas e um crescimento populacional voltado as sistemas de comunicação que somente no Brasil atingiu cerca de 83,4 milhões de pessoas pesquisa realizada em 2012 pelo IBOPE (Instituto Brasileiro De Opinião Pública E Estatística, 2012), o protocolo IPv4 (*Internet Protocol version 4*) praticamente se esgotou. Surgindo então a necessidade da utilização de uma outra versão deste protocolo que teve inicio em 1993 o IPv6 (*Internet Protocol version 6*).

O endereço IP é a identidade que todo computador ou dispositivo precisa para se conectar à Internet. Esta identificação deve ser única. No protocolo IPv4 mais utilizado ainda nos dias atuais, possui endereçamento de 32 bits, totalizando um estoque de 4.294.967.296 de endereços. Diferentemente do IPV4 o IPV6 possui endereçamento de 128 bits, isso significa que há 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços, o que representa cerca de 79 trilhões de trilhões de vezes o espaço disponível no IPv4. Esse número equivale a cerca de $5,6 \times 10^{28}$ (5,6 vezes 10 elevado a 28) endereços IP por ser humano, ou ainda, aproximadamente, 66.557.079.334.886.694.389 de endereços por centímetro quadrado na superfície da Terra.

Comumente ficou conhecido como implantação do IPv6, e não de migração. Na verdade, a médio ou longo prazo se terá realmente uma migração. Mas a curto prazo, tem-se a implantação do IPv6 e de técnicas de transição. O termo técnico utilizado para a nova situação da Internet e das redes em geral é pilha dupla, em que IPv6 e IPv4 funcionarão em conjunto por alguns anos, talvez por muitos, antes do IPv4 ser desativado.

Devido a complexidade e a extensão do protocolo IPV6 se faz necessário, assim como no protocolo IPV4 mas com mais intensidade, a utilização de serviços de resolução de nome **DNS** (*Domain Name System* – Sistema de Nomes de Domínios) que tem por objetivo básico identificar máquinas através de nomes em vez de endereços de IP.

Portanto, este trabalho foi dividido em etapas, sendo a primeira delas a configuração do IPv6 através do protocolo BGP (*Border Gateway Protocol*) em que faz a interligação com as operadoras que fornecem as rotas de Internet ao provedor. Por conseguinte distribuiu-se os endereços IPv6 a todas as máquinas diretamente conectadas ao roteador e também os *workstations* ligados através de um *proxy* pelo sistema DHCP (*Dynamic Host Configuration Protocol*) ou RADVD (*Router Advertisement Daemon*). Ainda houve a necessidade de criar as zonas reversas do DNS e a atribuição de nomes aos endereços IPs que necessitavam de acessos por outros dispositivos.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Implantação do Protocolo IPV6 em um Provedor de Acesso a Internet.

1.1.2 Objetivos Específicos

Devido ao grande volume de utilização e da escassez do IPV4 tem-se a necessidade da utilização do protocolo IPV6, este projeto tem como principais objetivos:

- 1 - Implementar o protocolo IPV6 do Provedor para com as Operadoras;
- 2 - Implementar o protocolo IPV6 em todos os dispositivos da rede interna do provedor;
- 3 – Implementar o serviços de DNS para os endereços IPV6;

1.2 JUSTIFICATIVA

O protocolo IPV6 se fez necessário devido ao esgotamento de endereços IPV4. Eles esgotaram-se na IANA (*Internet Assigned Numbers Authority*, organização mundial que funciona como a máxima autoridade na atribuição dos "números" na Internet - entre os quais estão os números das portas e os endereços **IP**), que é considerada o estoque central no ano de 2011. Ela redistribui os números para entidades regionais, que por sua vez fazem o mesmo para entidades nacionais, ou os designam para os ISPs (*Internet Services Provider*, entidade provedora do acesso a Internet), e estes os designam para os usuários.

Ao contrário do que acontece no protocolo IPV4, no IPV6 a quantidade de endereços disponível é considerado abundante, dessa forma deixando de ser considerado um recurso crítico e também não sendo mais necessário recursos de mediação como é o caso da utilização do NAT (*Network Address Translation*. É um recurso que permite converter endereços da rede interna em endereços da Internet).

Por sua vez, tem se a dificuldade de se memorizar cada endereço, assim, sendo fundamental a resolução desses endereços em nomes comuns através do DNS.

2 REFERENCIAL TEÓRICO

2.1 Protocolo IPV4

O Protocolo IP teve sua origem em meados dos anos 60 pelas universidades norte americanas com o intuito de interligar sistemas computacionais, mas foi a partir do *Department of Defence* (Departamento de Defesas) dos Estados Unidos que o protocolo começou a se espalhar. O maior problema encontrado nesta etapa foi a diversidade dos sistemas operacionais, para isso foi atribuído a ARPA (*Advanced Research Projects Agency*) a tarefa de organizar o modelo e torná-lo compatível com todos os sistemas, foi então criada uma aliança entre as universidades e os desenvolvedores de sistemas operacionais, essa aliança teve nome de ARPANET, que deu origem a Internet de hoje (TANENBAUM, 2003).

A designação IPV4 (Internet Protocol Version 4) significa que esta é a quarta versão do protocolo de Internet. É a tecnologia que permite que os aparelhos eletrônicos como computadores, smartphones, televisores entre outros naveguem na Internet (TANENBAUM, 2003).

Definido como conjunto de endereços compostos por 4 blocos de 8 bits cada, totalizando 32 bits. Estes são representados por números decimais e com um formato em que se permite trabalhar em uma faixa de 0 a 255 (TANENBAUM, 2003).

Estes blocos de IPs foram divididos entre todos os responsáveis pelo gerenciamento de IPs no mundo, como o LACNIC (América Latina e Caribe) que rege pelos IPs entregues ao CGI.br (Comite Gestor Internet do Brasil). Também para fins de organização e priorização foram subdivididos em classes Públicas, Privadas e Reservadas como visto na tabela 1.

Tabela1. Subdivisão dos endereçamentos IPV4.

CIDR Bloco de Endereços	Descrição	Referência
0.0.0.0/8	Rede corrente (só funciona como endereço de origem)	RFC 1700
10.0.0.0/8	Rede Privada	RFC 1918
14.0.0.0/8	Rede Pública	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	Localhost	RFC 3330
128.0.0.0/16	Reservado (IANA)	RFC 3330
169.254.0.0/16	Zeroconf	RFC 3927
172.16.0.0/12	Rede privada	RFC 1918
191.255.0.0/16	Reservado (IANA)	RFC 3330
192.0.2.0/24	Documentação	RFC 3330
192.88.99.0/24	IPv6 para IPv4	RFC 3068
192.168.0.0/16	Rede Privada	RFC 1918
198.18.0.0/15	Teste de benchmark de redes	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	Multicasts (antiga rede Classe D)	RFC 3171
240.0.0.0/4	Reservado (antiga rede Classe E)	RFC 1700
255.255.255.255	Broadcast	

2.2 Protocolo IPv6

Sucessor do IPv4, a “nova” versão do protocolo chamada de IPv6, ou seja, sexta versão do protocolo IP que vem sendo estudada desde a década de 1990 com o objetivo de consertar as falhas do antigo protocolo e o mais claro é suprir a escassez de endereços IPs disponíveis (HERTZOG E MAS 2014).

A principal diferença entre os protocolos é a quantidade de endereços possíveis. O IPv4 é composto por 4 blocos de 8 bits cada, totalizando 32 bits, já no protocolo IPv6 a composição se torna em 8 blocos de 16 bits cada e assim tendo um total de 128 bits por endereço IP.

Os números de cada bloco passa ser hexadecimal de 16 bits. Exemplo:

2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Se um grupo de vários dígitos seguidos for 0000, pode ser omitido. Por exemplo, **2001:0db8:85a3:0000:0000:0000:7344** é o mesmo endereço IPv6 que: **2001:0db8:85a3::7344**

2.3 Protocolo BGP

Considerado um dos protocolos de Internet mais complexos, em que livros inteiros são dedicados a ele e ainda assim nem todas as suas funcionalidades ficam claras apenas com base na leitura (KUROSE, 2010). Segundo Yannuzzi e Masip-Bruin (2005) que mesmo após ler livros e todas as RFCs, talvez seja difícil dominar este protocolo, e que para entender ao menos como ele funciona é necessário meses ou até anos trabalhando como um administrador de um ISP. Além de complexo o BGP é um dos protocolos mais críticos para que o sistema chamado Internet funcione perfeitamente.

O BGP é um protocolo de roteamento dividido em duas categorias: IGP (*Interior Gateway Protocol*) e EGP (*Exterior Gateway Protocol*). Os IGPs são utilizados para interligações entre roteadores pertencente a um mesmo AS, já os EGPs são utilizados para interligações e troca de informações entre roteadores pertencentes a ASs distintos (COMER 1995).

O BGP (*Border gateway protocol*) é um protocolo que permite as entidades denominadas ASN ou AS (sistemas autônomos) trocarem informações de roteamentos entre si. Segundo Tanenbaum (2003) os roteadores se comunicam entre si através de conexões tcp (*transmission control protocol*), o que possibilita uma comunicação confiável e ao mesmo tempo oculta o que se está transmitindo nesta conexão.

As informações de roteamento BGP são divulgadas por meio de conexões denominadas *peers* (Vizinhança), trabalhando em forma de pares também conhecidos como *peerings*. Para haver essa troca, são necessários que dois ou mais roteadores estejam diretamente conectados (ANDREOLI E RODRIGUES, 2002).

O BGP possui seis etapas antes de oficialmente conectar-se ao seu *neighbor* (vizinho) de destino: A primeira etapa é conhecida como **Idle** (inativo), neste o protocolo fica aguardando uma conexão do peer remoto. A próxima etapa é a **Connect** (associar) em que o BGP aguarda o recebimento da mensagem de **Open**

do peer remoto e passa para a etapa **Opensent**, caso a conexão seja mal sucedida o BGP vai para o estado **Active**, no que o BGP tenta novamente uma conexão com o peer remoto, conseguindo esta conexão passa novamente a ficar **Opensent** e com a conexão “fechada” (bem sucedida entre os roteadores) o protocolo passa para a etapa **Established** (estabelecida), em que os roteadores começam a trocar mensagens, caso haja uma intervenção ou desconexão detectada o protocolo volta ao estado inicial **Idle** (ANDREOLI E RODRIGUES, 2002).

Com o crescimento da Internet cresce também a necessidade de novas tecnologias e funcionalidades como o MBGP (*Multiprotocol BGP*), que tem como intuito permitir trocas de informações por múltiplos protocolos como IPv4 e IPv6 (ANDREOLI E RODRIGUES, 2002).

2.4 Protocolo DHCP

É possível realizar atribuições de endereçamento IP dinamicamente, onde destacam-se duas formas distintas que são *stateless* e *statefull*. O *Stateless* atua quando não há nenhum servidor fazendo a moderação dos IPs na rede, onde os dispositivos devem obter informações de configuração de forma automática assim sendo atribuído um endereço IP provisório. No *Statefull* usa-se de um servidor moderador para que esses endereços seja distribuídos dentre os dispositivos. Este servidor utiliza de um protocolo o DHCP (CISCO, 2014) .

Segundo Comer (1995) o DHCP (*Dynamic Host Configuration Protocol*) é um serviço destinado a facilitar redes com recursos de endereçamento IP limitados, tornando a locação dinâmica destes endereços fácil e rápida. O DHCP permite três formas de atribuição: Manual, Automática e dinâmica. Segundo a Microsoft (2015) o protocolo DHCP é um padrão destinado a reduzir a complexidade das configurações de endereçamento IP em máquinas clientes, usando de um servidor para gerenciar e centralizar os endereços IPs. Como todos os dispositivos conectados a uma rede necessitam de um endereço IP único e caso seja necessário alterar este dispositivo de rede a configuração do endereço IP também deverá ser alterado, ai entra o servidor DHCP que atribuirá automaticamente um novo endereço para este dispositivo.

- Atribuição de endereço IP Manual:

Neste modelo de atribuição o endereço IP é fixado ao endereço MAC do dispositivo, desta forma o endereço atrelado a este MAC o servidor não o atribuirá para outro dispositivo.

- Atribuição de endereço Automático

O servidor atribuirá um endereço IP ao dispositivo automaticamente na primeira conexão, fixando este endereço ao MAC do dispositivo por um determinado tempo, a diferença entre o modo automático e o modo manual é que neste não se faz necessário fixar o MAC, o próprio servidor se encarrega de capturá-lo.

- Atribuição de endereço Dinâmico

Este modo é o que traz a principal característica e funcionalidade do DHCP, ele atribui dinamicamente os endereços aos dispositivos e os renova periodicamente, tornando possível a utilização de um mesmo endereço de IP por vários dispositivos em tempos diferentes.

As funcionalidades e formas de configuração do DHCPv4 são definidas pela RFC 2131 que diz respeito a distribuição automática de endereços TCP/IP na versão 4 através de um servidor que seja responsável pela execução do protocolo DHCP.

Na versão 6 do DHCP as configurações e definições são impostas pela RFC 3315, nesta tem-se que o DHCPv6 se tornou dispensável em redes IPv6, porém, manteve-se o protocolo com suas devidas atualizações e adequações. O DHCPv6 continua sendo disponibilizado nas duas modalidades *Stateless* e *Statefull* da mesma forma que ocorre na versão 4 do protocolo.

Vantagens de utilizar o DHCP

Configuração confiável e segura evita erros de configuração causada pela digitação manual do endereçamento IP em cada dispositivo. O DHCP também previne conflitos de endereços em dois ou mais dispositivos de uma mesma rede. Reduz o tempo de configuração de uma rede, já que por padrão todos os dispositivos veem de fábrica aptos a receber um endereço dinamicamente (MICROSOFT, 2015).

2.5 DHCPv6

Uma das principais vantagens do protocolo IPv6 perante o protocolo IPv4 é a autoconfiguração, em que um dispositivo conectado em uma rede disposta de IPv6 automaticamente receberá um endereço, que no seu antecessor o IPv4, esse processo era feito de forma estática e individual, conforme descrito pela RFC 3315, o protocolo DHCPv6 continuou sendo disponibilizado nas duas versões:

- Stateful: em que os dispositivos conectados a rede recebem um endereço automaticamente de um servidor e este o mantém em uma base de dados, da mesma forma que ocorre na versão 4 deste protocolo.
- Stateless: O endereço é gerado a partir de uma combinação de informações locais em cada dispositivo. Essas combinações tem com principio base o prefixo da rede informada pelos roteadores. Então os dispositivos juntam esse prefixo e concatenam com o MAC address formando um endereço denominado *Global*, ou seja é um endereço único na Internet.

2.6 Protocolo RADVD

O RADVD (*Router Advertisement Daemon*) é um software open-source que implementa endereços *Globais* a dispositivos conectados a um servidor, utilizando do NDP (*Neighbor Discovery Protocol*) e da forma *stateless* de configuração do DHCPv6 (RFC 3315).

Devido ao DHCPv6 não divulgar o *gateway default* se faz necessário a utilização do RADVD em servidores Linux, ele é um *daemon* que faz os *routers advertisements* e pode também ter a função de autoconfiguração (RFC 3315).

2.7 Firewall ou Filtragem de pacotes (Iptables e Ip6tables)

Faz parte de um pacote de serviços instalados em um hardware que tem por finalidade filtragem de pacotes ou de conteúdo, ou seja, só permite a passagem de pacotes pré estabelecidos em condições. Em dispositivos Linux o firewall incorpora o *Netfilter*. Ele pode ser controlado pelo administrador do sistema através dos comandos *Iptables* e *Ip6tables*. O que difere os dois comandos é a versão do

protocolo, no *Iptables* é gerenciado a filtragem de pacotes e conteúdos IPv4, e no *Ip6tables* a filtragem é gerida sob o protocolo IPv6 (HERTZOG, R.; MAS, R., 2014).

Funcionamento do Netfilter

Conforme descrito por Hertzog e Mas (2014), quatro tabelas são utilizadas para armazenarem as regras, e três tipos de operações são permitidas.

- Filtro: Como o nome já diz traz as regras de filtragem. (aceita, recusa ou ignora o pacote).
- NAT: Tabela existente apenas para IPv4 esta traduz endereços ips para origens e destinos.
- *Mangle*: Rege alterações nos pacotes como tipos de serviços e encaminhamentos.
- *Raw*: Ester permite fazer modificações manuais nos pacotes antes que estes sejam rastreados pelo sistema.

Cada tabela possui listas de regras denominadas *cadeias*. Estas cadeias podem ser pré-definidas pelo administrador do sistema.

Por padrão a tabela *filtro* possui três cadeias:

- 1 - *INPUT* (Entrada): Filtragem de pacotes cujo destino seja o próprio firewall.
- 2 – *OUTPUT* (Saída): Filtragem de pacotes originados pelo Firewall.
- 3 – *FORWARD* (Passar a diante): Filtragem de pacotes que passam pelo firewall mas que nem a origem e nem o destino seja ele mesmo.

Na tabela NAT também possui três cadeias:

- 1- *PREROUTING* (Pré Roteamento): Faz as alterações cabíveis assim que o pacote chega ao firewall.
- 2 – *POSTROUTING* (Pós Roteamento): Faz as alterações cabíveis sempre que os pacotes estiverem prontos para deixarem o firewall.
- 3 – *OUTPUT* (Saída): Faz alterações nos pacotes de saída gerados pelo próprio firewall.

Segundo Hertzog e Mas (2014), cada cadeia consiste de uma lista de regras e condições com ações a serem executadas quando as condições forem satisfatórias. O *firewall* examina cada pacote que passa, chega ou se origina nele. Estas regras podem ser:

- *Accept*: Aceita o pacote e o permite passar pelo *firewall*.

- *Reject*: Rejeita o pacote gerando uma mensagem de erro.
- *Drop*: Apaga e ignora o pacote
- *Log*: Gera uma mensagem com uma descrição do pacote e da ação tomada nas regras antes dele.
- *Ulog*: Também gera uma mensagem mas que pode ser melhorada e da mesma forma que o *Log* retorna o processamento do *firewall* para a regra da próxima cadeia a ser chamada.
- *Return*: Interrompe o processamento da cadeia atual e retorna a cadeia chamada anteriormente.
- *Snat*: Disponível somente em IPv4 aplica o *Nat* de Origem.
- *Dnat*: Da mesma forma que o *Snat* porém aplicando regra de *Nat* de destino.
- *Masquerade*: Também disponibilizado somente no IPv4 este mascara o endereço ip de rede privado a ter sua saída pelo endereço do *firewall*.
- *Redirect* – Direciona uma porta especificada pela regra para um outro dispositivo da rede, também disposto somente em IPv4.

2.8 Serviço de nomes e domínios (DNS)

Segundo relatado pela Microsoft o DNS surgiu com a própria evolução da Internet, quando ainda estava sob domínio do Departamento de Defesa dos Estados Unidos da América, os nomes dos sites eram armazenados em um arquivo chamado *Hosts* e armazenado em um servidor central. Com o número de dispositivos crescendo este arquivo *Hosts* também cresceu, surgindo assim a necessidade de um sistema mais eficiente. Esse novo sistema tem sua origem em 1984 denominado *Domain Name Server*. O DNS é regido por quatro Request for Comment (RFC), são elas: RFC 882 (Nomes de domínios: Conceitos e instalação), RFC 883 (Nomes: Implementação de domínios e especificações), RFC 1034 (Nomes: Conceitos de domínios e instalações) e RFC 1035 (Nomes: Implantação de domínios e implementação). A essência do DNS é a criação de um sistema hierárquico de atribuição de nomes baseado em um sistema de domínios em um banco de dados (TANENBAUM, 2003).

O *Domain Name Service* (DNS) é responsável pela tradução de endereços IPs em nomes e vice-versa. Diferentemente da maioria dos demais protocolos, o

DNS manteve-se o mesmo tanto para IPv4 quanto para IPv6, mudando apenas a forma de escrita em cada um deles (HERTZOG E MAS, 2014).

Segundo Couto (2012) este é o protocolo mais usado no dia a dia, toda vez que fizemos acesso a Internet ele irá transformar o nome do host digitado no *web browser* para um endereço de IP correspondente. Mas esta não é a única função do protocolo e sim um exemplo simplificado de como seria difícil o cotidiano sem ele.

Os registros de DNS são armazenados em zonas sendo que cada uma delas coincide com um domínio ou subdomínios ou ainda pode representar um intervalo de um endereçamento IP. Estas zonas ficam armazenadas em um servidor denominado *Primário*, é ele que possui a autoridade de regir o conteúdo de cada zona, os demais servidores são denominados *Secundários* e geralmente reapresentam uma cópia da zona configurada no primário (HERTZOG E MAS, 2014). Cada zona pode conter diversos tipos de registros, dentre eles destacam-se:

- **A**: Associa um *hostname* a um endereçamento IPv4.
- **AAAA**: Associa um *hostname* a um endereçamento IPv6.
- **PTR**: Associa um endereço IP a um *hostname* para resolução de DNS Reverso.
- **NS**: Informa os endereços IPs dos servidores de domínios autoritativos.
- **MX**: Informa os endereços IPs dos servidores de SMTP de um domínio.
- **CNAME**: Utilizado para criar subnomes (alias) de um endereçamento IP para outro.
- **TXT**: Armazena informações do tipo texto, criado inicialmente com o intuito de armazenar comentários ou informações sobre os domínios, hoje em dia é mais utilizado como anti-spam como o *SPF (Sender Policy Framework)*.

O sistema do protocolo DNS é criado em formato de árvore como visto na figura 1, e o seu entendimento é tão importante quanto o fundamento do próprio protocolo. O banco de dados do DNS é indexado pela faixa de domínios, cada um deles pode possuir até 127 ramificações, a árvore pode ramificar em qualquer parte do nó do DNS que é separado por um ponto (.) (ALBITZ E LIU, 2006).

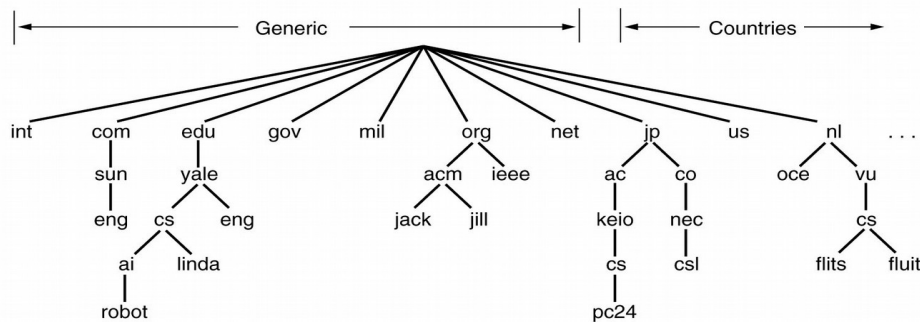


Figura 1 – Arvore DNS
Fonte: (ALBITZ E LIU, 2006)

Servidor autoritativo

Nome dado ao servidor que possui autoridade sobre qualquer domínio, isto é, ao responder requisições de DNS informa ter autoridades sobre aquele domínio e possui as zonas com os recursos solicitados (NEMETH, et al, 2005)

Servidor Recursivo

É o servidor responsável pela consulta aos DNS autoritativos até conseguir uma resposta desejável e entregar ao dispositivo solicitante. Ao receber requisições de resolução de nomes o servidor solicita aos autoritativos e conforme a resposta obtida continua a fazer perguntas para outros servidores até chegar ao servidor autoritativo do domínio requisitado, em que o servidor recursivo se torna obrigado a entregar uma resposta DNS ao dispositivo solicitante, seja ela positiva ou negativa. (CAMPOS E JUSTO, 2008).

2.9 Sistemas Autônomos (AS)

Um provedor de acesso a Internet (ISP) pode ser capaz de gerenciar sua própria rede, escolhendo o melhor caminho para os destinos dos seus ips é torná-lo autônomo. Em outras palavras, o provedor após obter o *AS Number* passa a fazer

parte de um grupo de redes IP, mas sob uma gerencia dentro de uma politica de roteamento encontrado na RFC-1930 de 1996.

Para ser tornar um AS o provedor deve ser *multi-homed* (possuir 2 ou mais conexões independentes à Internet ou uma conexão com uma operadora e uma conexão com um PTT (Ponto de Troca de Tráfego). Atendendo aos pré-requisitos a entidade então entra com o pedido ao gestor da Internet em sua região, no Brasil quem gerencia é o Registro.br, entidade que faz parte do CGI.br (Comite Gestor da Internet no Brasil).

3 DESENVOLVIMENTO

O respectivo trabalho tem como base a matriz do Provedor de Acesso à Internet, localizado na cidade de Francisco Beltrão - PR, que possui como principal preocupação o bom atendimento e melhor qualidade no acesso a Internet com seus clientes. Para isso viu-se a necessidade da utilização do IPV6, tornando o acesso de seus clientes mais ágil e seguro perante as grandes telecoms.

Este projeto será dividido em etapas, sendo a primeira delas a interligação com a operadora, por meio do protocolo de roteamento BGP, sendo utiliza do um roteador de borda da marca Cisco (WS-C6506) e com velocidade de 1Gbit.

Posteriormente será feita a implementação do IPV6 para os demais dispositivos da rede, em que a maioria consiste de servidores que utilizam de sistemas operacionais Linux. Um destes tem por função *firewall*, *proxy* e DHCP (*Dynamic Host Configuration Protocol*), protocolo responsável pela distribuição dos Ips dinamicamente a todos os *Hosts* a ele conectados. Também utilizou-se do protocolo RADVD (*Router Advertisement Daemon*) e o DHCPv6, semelhante ao DHCPv4 ele distribui os endereços IPV6 aos *hosts* a ele conectados. Neste projeto utilizou-se das duas formas de DHCP disponível pela RFC 3315, sendo a primeira delas da forma *stateless* em que cada dispositivo da rede possui um endereço denominado *Global* e o *statefull* em que estes mesmos dispositivos recebem um endereço pré definido pelo DHCPv6 e armazenado no banco de dados do servidor.

Representado pela Figura 2 tem-se a topologia, na qual foi submetida a implantação do protocolo IPV6.

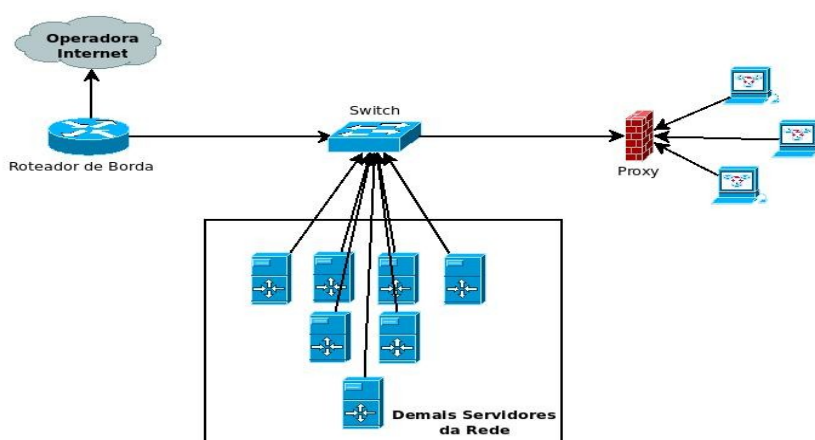


Figura 2 – Topologia da rede em que foi implantado o protocolo IPV6.

Fonte própria.

4 MATERIAIS E MÉTODOS

4.1 Materiais

Durante a implantação do protocolo IPv6 utilizou-se da estrutura existente no provedor, dispondo de um *switch layer 3 Cisco Catalyst 6509*, vários servidores de arquiteturas diferentes e utilizando sistemas operacionais *Linux*, podendo destacar os principais envolvidos neste projeto:

- Switch Cisco Catalyst 6505: Trabalha em *Layer 3* fazendo roteamento avançado (BGP) utilizando da versão 12.2(33)SX14a do *Cisco IOS Software*.
- Servidor Dell R720xd: Virtualizador *Xen Server*, em que rodam os serviços de DNS, Cacti, hospedagens de domínios, entre outros.
- Servidor Dell R420: Servidor com sistema operacional linux distribuição *CentOS 6.7 release (Final)*, responsável pelo sistema de firewall e proxy.

4.2 Métodos

O primeiro processo foi o planejamento da rede, onde definiu-se a divisão do prefixo /32 IPv6 delegado pelo Registro.br ao provedor. Essa divisão ocorreu da seguinte maneira:

Primeiramente subdividiu-se o prefixo /32 em 4 prefixos /34 para facilitar posteriormente a redistribuição dos prefixos menores. Destes, o primeiro /34 foi subdividido em 2 /35 onde o primeiro foi novamente subdividido agora em 32 prefixos /40 de onde utilizou-se o primeiro /40 para uso na rede interna do provedor, e que poderá ser subdividido em diversos outros prefixos menores até chegar ao /64 definido como prefixo padrão para uso na rede interna do provedor, os demais prefixos /40 ficaram cadastrados para uso futuro. Para cada sub-rede criada utilizou-se um /64 como visto na tabela:

Tabela 2. Planejamento da estrutura em IPv6.

2804:1c30::/34	FRANCISCO BELTRÃO
2804:1c30::/35	Francisco Beltrão - Subdividido em /40
2804:1c30::/40	Rede Francisco Beltrão
2804:1c30::/64	Loopback
2804:1c30:0:1::/64	DMZ
2804:1c30:0:2::/64	LAN Interna
2804:1c30:2000::/35	Reserva
2804:1c30:4000::/34	PATO BRANCO
2804:1c30:8000::/34	DOIS VIZINHOS
2804:1c30:c000::/34	RESERVA

Com o planejamento finalizado iniciou-se o processo de implantação que decorreu de forma paralela a rede IPv4, tornando o trabalho mais flexível, sem que prejudicasse o desenvolvimento de nenhum servidor ou cliente.

Para que o provedor pudesse dispor do protocolo IPv6 houve a necessidade de configurar uma sessão BGP com as operadoras. O provedor em questão possui sessão com duas operadoras sendo que uma delas não dispõe do protocolo IPv6, sendo assim foi configurado apenas uma sessão e assim podendo divulgar o prefixo 2804:1c30::/32 pertencente a seu AS, desta forma tornando a rede apta a receber o IPv6.

Devido a alta complexidade do protocolo IPv6 por ser hexadecimal, a utilização dele se torna facilitada com a utilização do serviço de DNS. Perante os sistemas operacionais o fato de ser IPv4 ou IPv6 não possui muita dificuldade. A principal e mais perceptível mudança é para o usuário. Com a utilização de serviços para resolução destes complexos endereços em nomes, torna mais simplificado o acesso a sistemas como câmeras, configurações de clientes de e-mail ou até mesmo o acesso aos próprios servidores, seja este via *telnet*, *ssh* ou ainda área de trabalho remota de um sistema *windows*. Segue abaixo um exemplo de quão grande é a facilidade com o serviço de DNS.

Acesso ao servidor de gerenciamento/monitoramento de rede com o sistema *Cacti*:

Acesso via IPv6 via RADVD: 2804:1c30:0:1::100

Acesso via IPv6 via endereço global: 2804:1c30:0:1:219:bbff:fec6:7174

Acesso via DNS: cacti.provedor.com.br

5 RESULTADOS

5.1 Configuração das Interfaces

Antes de iniciar a configuração do BGP, foi necessário a configuração do roteamento interno, através da configuração de endereço IP na interface que liga o roteador a rede interna do provedor e também na interface que faz a comunicação com a operadora, fazendo com que os roteadores possam se conhecer e com isso tornando possível fechar sessão entre eles. Essa configuração tornou-se possível com a ativação do protocolo IPv6 em suas respectivas interfaces de comunicação. Foi utilizado um roteador Cisco, portanto o comando *ipv6 enable* para permitir tráfego IPv6 na interface fez-se necessário. Após permitir o tráfego fez-se a configuração de um endereço ipv6 (2804:7F4:0:9::2/126), fornecido pela própria operadora (processo ocorre da mesma forma que ocorre com o endereçamento ipv4) na interface *GigabitEthernet1/1* (interface escolhida para a comunicação). Na interface *GigabitEthernet6/2* foi configurado um endereço IPv6 2804:1C30:0:1::1/64, o qual é o *gateway* da rede interna do provedor. Também houve a necessidade de realizar as rotas de distribuição interna através do comando *ipv6 route*. O descritivo desta configuração pode ser visto através dos Quadros 1 e 2.

```
interface GigabitEthernet1/1
description CONEXAO_GVT
ip address 189.26.120.254 255.255.255.252
ipv6 address 2804:7F4:0:9::2/126
ipv6 enable

interface GigabitEthernet6/2
description CONEXAO_REDE_LOCAL_FNB
ipv6 address 2804:1C30:0:1::1/64
ipv6 enable
```

Quadro 1 – Configuração da interface GigabitEthernet1/1 roteador cisco

Fonte própria.

```

core-fnb#configure terminal
core-fnb(config)#interface GigabitEthernet1/1
core-fnb(config-if)#description CONEXAO_OPERADORA
core-fnb(config-if)#ipv6 enable
core-fnb(config-if)#ipv6 address 2804:7F4:0:9::2/126
core-fnb(config-if)#exit
core-fnb(config)#interface GigabitEthernet6/2
core-fnb(config-if)#description CONEXAO_REDE_LOCAL_FNB
core-fnb(config-if)#ipv6 enable
core-fnb(config-if)#ipv6 address 2804:1C30:0:1::1/64
core-fnb(config-if)#exit
core-fnb(config)#ipv6 route 2804:1C30:0:2::/64
2804:1C30:0:1::35
core-fnb(config)#ipv6 route 2804:1C30::/34 Null0 250
core-fnb(config)#ipv6 route 2804:1C30::/32 Null0 250
core-fnb(config-if)#end

```

Quadro 2 – Interfaces do roteador cisco devidamente configuradas.

Fonte própria.

Para confirmar se a configuração apresentada no Quadro 1 teve sucesso utilizados do comando “*ping + ipv6 + ip de destino*” para testar a comunicação IPv6, o resultado deste ping está descrito no Quadro 3.

```

core-fnb#ping ipv6 2804:7F4:0:9::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2804:7F4:0:9::1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
4/4/4 ms

```

Quadro 3 – Teste de comunicação IPv4 e IPv6.

Fonte própria.

5.2 Configuração do protocolo BGP

A configuração do protocolo BGP em IPv6 dar-se-á da mesma maneira do IPv4, diferenciando apenas no protocolo IP. A configuração básica realizada está demonstrada pelo Quadro 4.

```
router bgp 28285
neighbor 2804:7F4:0:9::1 remote-as 18881
  neighbor 2804:7F4:0:9::1 description CONEXAO_AS_OPERADORA_V6
```

Quadro 4 – Configuração do BGP roteador Cisco.

Fonte própria.

Router bgp 28285 simboliza a chamada do protocolo bgp para o AS (*autonomous system* ou sistema autônomo) 28285 que representa o provedor de acesso a Internet, enquanto o *remote-as* 18881 representa a comunicação com o AS que representa a operadora, como vista no Quadro 5.

```
aut-num:      AS28285
owner:        Provedor de Acesso a Internet
ownerid:      001.***.817/0001-**
responsible:  Lucas Loss Stolfo
country:      BR

aut-num:      AS18881
owner:        Operadora
ownerid:      003.**.926/0002-**
responsible:  Eng&Op Dados
country:      BR
```

Quadro 5 – ASNs designados pelo Registro BR para as entidades

Fonte Própria.

No parâmetro *address-family ipv6* fez-se a ativação do neighbor (permite que o vizinho conecte-se ao roteador) e também é implementado os filtros de entrada e saída, os quais estão descritos no Quadro 6. É neles que se permite o recebimento de todas as rotas vindas da operadora pelo filtro *in* e anunciamos somente os prefixos desejados através do filtro *out*. Esses filtros são importantes para que não haja vazamento de rotas indesejadas para a “Internet”. Também é no *address-family* que se indica os *networks* (redes) a serem anunciados. A configuração deste pode ser verificada através do Quadro 7.


```

ipv6 prefix-list BLOCOS-V6 seq 5 permit 2804:1C30::/32
ipv6 prefix-list BLOCOS-V6 seq 10 permit 2804:1C30::/34

```

Quadro 6 – Filtros de permissão

Fonte própria.

```

address-family ipv6
  neighbor 2804:7F4:0:9::1 activate
  neighbor 2804:7F4:0:9::1 route-map ANUNCIO_V6_IN in
  neighbor 2804:7F4:0:9::1 route-map ANUNCIO_V6_OUT out
  network 2804:1C30::/32
  network 2804:1C30::/34
Exit-address-family4

```

Quadro 7 – Address-family ipv6

Fonte Própria.

Com essa configuração descrita já é possível ter conexão entre os roteadores, mas para que haja comunicação dos prefixos do provedor com o restante da Internet, tem-se a necessidade da criação dos *route-maps*, são neles que informamos a operadora qual prefixo irá ser anunciado para a Internet. Esses prefixos foram definidos no *ipv6 prefix-list* (lista de prefixos ipv6) demonstrado no Quadro 8. O *route-map* funciona baseado nos filtros *in/out* relatados no *address-family ipv6*, em que no *route-map in* (entrada), não se tem a necessidade de fazer a aplicação de nenhum filtro, faz-se apenas uma regra permitindo tudo o que vier da operadora. Já no *route-map out* (saída), aplica-se a lista de prefixos de anuncio desejado. Esta configuração pode ser vista através do Quadro 8.

```

route-map ANUNCIO_V6_IN permit5
!
route-map ANUNCIO_V6_OUT permit 5
  match ipv6 address prefix-list BLOCOS-V6
!

```

Quadro 8 – route-map (mapa de rota)

Fonte Própria.

Para confirmar se sessão está funcionando, utiliza-se do comando *show bgp ipv6 unicast summary* para ver a sumarização das sessões, *show bgp ipv6 unicast neighbors + ip neighbor + advertised-routes* para ver todas as rotas anunciadas para a operadora e *show bgp ipv6 unicast neighbors 2804:7F4:0:9::1 routes* para ver todas as 24748 rotas ipv6 recebidas. Os testes de conexão realizados estão descrito no Quadro 9.

```

core-fnb#show bgp ipv6 unicast summary
Neighbor          V          AS MsgRcvd MsgSent   TblVer   InQ
OutQ Up/Down  State/PfxRcd
2804:7F4:0:9::1  4          18881 4880060 300030   5782819   0
0 11:11:39      24748

core-fnb#show bgp ipv6 unicast neighbors 2804:7F4:0:9::1
advertised-routes
BGP table version is 5782819, local router ID is
201.33.228.148
Status codes: s suppressed, d damped, h history, * valid, >
best, i - internal,
                r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf
Weight Path
*> 2804:1C30::/34   ::                0
    32768 i
*> 2804:1C30::/32   ::                0
    32768 i

```

Quadro 9 – Mostragem dos testes de sessão BGP

Fonte própria.

5.3 Configuração dos demais dispositivos da rede

Uma das vantagens do IPv6 é a auto propagação em rede local, uma vez configurado um IP na interface do roteador Cisco, todos os demais dispositivos ativos ligados na rede receberão automaticamente e de forma aleatória um endereço de IP da classe definida. No exemplo deste trabalho, todos os dispositivos receberam um IP de prefixo /64. Além do endereço recebido automaticamente foi fixado um IP para cada servidor, para que possibilite a sua administração remotamente.

A configuração do IPv6 em servidores linux (neste estudo utilizou-se da distribuição CentOS, a qual é uma distribuição baseada no RedHat) decorre de forma considerada simples, inicialmente torna-se ativo o protocolo em `/etc/sysconfig/network`, alterando o parâmetro `NETWORKING_IPV6=no` para `NETWORKING_IPV6=yes`. Após feito isso foi necessário alterar o arquivo `ifcfg-eth0` em que fica guardado as informações da placa de rede denominada `eth0` para que em caso de uma reinicialização do sistema ele volte com as mesmas configurações. Editando o arquivo `ifcfg-eth0`, que fica localizado em `/etc/sysconfig/network-scripts/ifcfg-eth0`, adiciona-se os parâmetros aceitos pelo IPv6: `IPV6INIT` – Ativa o IPv6 na inicialização do sistema, semelhante ao `ONBOOT=yes` do protocolo IPv4. `IPV6ADDR` – Insere-se o endereço IPv6 que se deseja fixar na placa (este não substitui o endereço recebido automaticamente, o sistema mantém os dois endereços). `IPV6_DEFAULTGW` – Endereço de *gateway* para a rede IPv6.

No Quadro 10, pode-se observar um exemplo desta configuração realizada em um dos servidores disponíveis em IPv6 na rede.

```
[root@Links ~]#nano /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=Links
NETWORKING_IPV6=yes
[root@Links ~]# nano /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
BROADCAST=201.33.224.127
DNS1=201.33.224.2
GATEWAY=201.33.224.1
HWADDR=00:19:bb:c6:71:74
IPADDR=201.33.224.100
NETMASK=255.255.255.128
ONBOOT=yes
TYPE=Ethernet
DNS2=201.33.224.3
IPV6INIT=yes
IPV6_AUTOCONF="yes"
IPV6ADDR=2804:1c30:0:1::100/64
IPV6_DEFAULTGW=2804:1c30:0:1::1
```

Quadro 10 – configuração de IPv6 de forma permanente em um servidor linux

Fonte própria.

Também pode se inserir um endereço provisório comumente conhecido como teste de rede, este endereço é utilizado para testar a comunicação entre os

dispositivos sem que haja a necessidade de alterar os arquivos antes mencionados. Utiliza-se do comando “*ip -6 addr add 2804:1c30:0:1::100/64 dev eth0*” para inserir o endereço IPv6 que será posteriormente fixado na interface, porém feito desta forma se a interface de rede ou mesmo o servidor seja reiniciado a configuração se perde.

Para certificar a funcionalidade desta configuração utiliza-se da versão 6 do protocolo ICMP (ping6). No Quadro 11 tem-se os exemplos de comunicação, primeiramente executou-se o teste para o *gateway*, com o resultando sendo positivo, ou seja, o servidor obteve resposta do roteador, em seguida executa-se um teste padrão em que destina-se um pacote ICMP para um destino público.

```
[root@Links ~]# ping6 2804:1c30:0:1::1
PING 2804:1c30:0:1::1(2804:1c30:0:1::1) 56 data bytes
64 bytes from 2804:1c30:0:1::1: icmp_seq=1 ttl=64 time=2.96 ms
64 bytes from 2804:1c30:0:1::1: icmp_seq=2 ttl=64 time=0.467
ms
64 bytes from 2804:1c30:0:1::1: icmp_seq=3 ttl=64 time=0.442
ms
64 bytes from 2804:1c30:0:1::1: icmp_seq=4 ttl=64 time=0.437
ms
64 bytes from 2804:1c30:0:1::1: icmp_seq=5 ttl=64 time=0.412
ms

[root@Links ~]# ping6 ipv6.google.com
PING ipv6.google.com(2800:3f0:4001:812::1005) 56 data bytes
64 bytes from 2800:3f0:4001:812::1005: icmp_seq=1 ttl=58
time=16.7 ms
64 bytes from 2800:3f0:4001:812::1005: icmp_seq=2 ttl=58
time=16.8 ms
64 bytes from 2800:3f0:4001:812::1005: icmp_seq=3 ttl=58
time=16.8 ms
64 bytes from 2800:3f0:4001:812::1005: icmp_seq=4 ttl=58
time=16.7 ms
64 bytes from 2800:3f0:4001:812::1005: icmp_seq=5 ttl=58
time=17.0 ms
```

Quadro 11 – Testando a configuração

Fonte própria.

5.3.1 – Configurando o firewall de entrada em servidores linux

Existe diversas formas de se proteger um servidor, o deixando menos vulnerável a tentativas de invasões e fraudes. Neste trabalho optou-se pela utilização da versão 6 do *iptables* (*ip6tables*), também muito semelhante a versão 4.

O primeiro passo a ser dado antes de criar as regras de *firewall* é dar permissão para que o *ip6tables* inicialize junto com o sistema operacional. Utiliza-se do comando “*chkconfig --level 345 ip6tables on*” para fazer com que o *ip6tables* inicialize com nível privilegiado durante a inicialização do sistema operacional

Com o *ip6tables* já em execução pode-se criar as regras de *firewall*. Essas regras podem ser executadas de diferentes formas, uma delas é editar o arquivo padrão do sistema, neste caso utilizando do CentOS encontrado em */etc/sysconfig/ip6tables*, ou então criar um arquivo de regras que será chamado na inicialização do sistema operacional e ignorando as regras denominadas de *padrão (default)*. Neste trabalho optou-se pela segunda maneira, em que foi criado um arquivo chamado de *rc6.firewall* indexado na pasta */etc/init.d*, em que ficam alguns arquivos de inicialização automática do sistema.

Através do comando *touch rc6.firewall* dentro do diretório */etc/init.d* cria-se um arquivo editável vazio, em seguida é necessário dar permissão de execução a este arquivo (*chmod +x rc6.firewall*). Feito isso dar-se-a inicio a criação das regras.

Definindo variáveis

Antes de definir as variáveis é necessário limpar as regras existentes no servidor através do comando “*ip6tables -F*”. Desta forma inicia-se a configuração do firewall sem nenhuma sujeira de outras configurações antigas ou mesmo configurações que já pertencem por padrão ao servidor.

Para facilitar as configurações utiliza-se de variáveis, neste exemplo adotou-se apenas duas em que é definido quem é a interface de entrada do servidor, denominada de *WAN*, e qual é a interface de saída para a rede interna, denominada de *LAN*. Pode-se ter inúmeras variáveis, dependendo do propósito e da extensão da configuração do arquivo de *firewall*.

- *WAN=eth0*
- *LAN=eth1*

Definindo políticas

Através deste define-se qual a política de execução padrão. Neste servidor adotou-se como política padrão bloquear tudo o que chegar na entrada do servidor

(*INPUT*) e de regras avançadas (*FORWARD*) e permitir tudo o que for sair do servidor (*OUTPUT*).

Regras de entrada permitida (exceções)

Através das regras de *INPUT* pode-se permitir acessos locais em ambas as interfaces (*WAN* e *LAN*), como pode-se observar na regra abaixo:

```
"ip6tables -A INPUT -i $LAN -j ACCEPT"
```

```
"ip6tables -A INPUT -i $WAN -j ACCEPT"
```

A regra a seguir permite acesso vindo da rede interna, definida pelo prefixo de subrede *2804:1c30:0:2::/64* com destino a qualquer lugar saindo pela interface *WAN* na porta 22 do protocolo *tcp*.

```
"ip6tables -A FORWARD -s 2804:1c30:0:2::/64 -i $WAN -p tcp -m tcp --dport 22 -j ACCEPT"
```

Tem-se também uma segunda regra permitindo o acesso de uma determinada rede com destino a interface *WAN* também na porta 22 do protocolo *tcp*. Neste caso optou-se por liberar todo o prefixo */32*, ou seja, de qualquer parte da rede que receba um ip pertencente ao prefixo */32* conseguirá ter acesso a este na porta 22.

```
"ip6tables -A INPUT -s 2804:1c30::/32 -p tcp --dport 22 -j ACCEPT"
```

No Quadro 12 tem-se o modelo de firewall aplicado em um dos servidores que já estão alocados por IPv6.

```

# IPv6 firewall (ip6tables)
WAN=eth0
LAN=eth1
ip6tables -F
# Define Policy
ip6tables -P INPUT DROP
ip6tables -P FORWARD DROP
ip6tables -P OUTPUT ACCEPT
# Allow unrestricted access on internal network
ip6tables -A INPUT -i $LAN -j ACCEPT
ip6tables -A INPUT -i $WAN -j ACCEPT
# allow SSH in
ip6tables -A FORWARD -s 2804:1c30:0:2::/64 -i $WAN -p tcp -m
tcp --dport 22 -j ACCEPT
# Drop everything else
ip6tables -A FORWARD -i $WAN -j DROP
# allow everything to our router/server.
ip6tables -A INPUT -s 2804:1c30::/32 -p tcp --dport 22 -j
ACCEPT
# Drop everything else
ip6tables -A INPUT -i $WAN -j DROP
# Print
echo "IPV6 Firewall OK!!!![ OK ]"

```

Quadro 12 – Configuração do firewall em um dos servidores

Fonte própria.

5.3.2 – Instalação e configuração do RADVD

Este pacote é considerado padrão em todas as distribuições linux, portanto, no CentOS basta instalar através do comando *“yum install radvd”*. Em seguida é necessário editar o arquivo *radvd.conf* encontrado dentro do diretório */etc*. Neste arquivo define-se a interface a qual os demais dispositivos serão conectados, e também o prefixo de subrede destinado a estas dispositivos. As demais regras como definição do tempo mínimo e máximo de atribuição não se alteram. O Quadro 13 mostra a configuração realizada no radvd para este servidor.

```

interface eth1
{
    AdvSendAdvert on;
    MinRtrAdvInterval 30;
    MaxRtrAdvInterval 100;
    prefix 2804:1c30:0:2::/64
    {
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr off;
    };
};

```

Quadro 13 – Configuração do radvd.conf

Fonte própria.

5.3.3 – Configuração do DHCPD6

Para uso dinâmico do IPv6 não se tem a extrema necessidade da utilização do DHCPD6 (*Dynamic Host Configuration Protocol daemon version 6*), em servidores linux basta apenas a utilização do RADVD para que prefixo desejado seja alocado dinamicamente entre os hosts da rede. Porém, caso tenha-se a necessidade de alocar fixas distintas do prefixo IPv6 para a rede utiliza-se do DHCPD6. A configuração do DHCPD6 é dada através da edição do arquivo *dhcpd.conf* encontrado no diretório */etc/dhcp/*, no Quadro 14 tem-se o exemplo utilizado neste projeto em que delimitou-se uma pequena faixa de um prefixo de IPv6 /64. Através da configuração do DHCPD6 pode-se também fixar um endereço IPv6 para um determinado host através de seu endereçamento MAC (*Media Access Control*).

```

option domain-name-server 2804:1c30:0:2::/64;
option domain-name        "ipv6.provedor.com.br";
interface eth1 {
    address-pool-pool1 3600;
};
pool pool1 {
    range 2804:1c30:0:2::100 to2804:1c30:0:2::200;
};

```

Quadro 14 – Configuração do dhcpd.conf

Fonte própria.

5.4 Configuração do DNS e Zona reversa

As entradas de DNS são definidas pelas suas *Resources Records*, estas normalmente são escritas em letras maiúsculas e são definidas na primeira coluna. Abaixo breve descritivo sobre estas entradas:

- SOA – Autoridade sobre o domínio
- NS – Responsável por listar um servidor de nomes para o domínio
- A – Mapeia os nomes para os determinados endereços
- PTR – Mapeamento reverso
- CNAMEs – Mapeia os aliases de sub-domínios
- MX – Gateway de e-mail ou *Mail Exchange*

5.4.1 Instalação dos serviços

Com o surgimento deste novo protocolo, necessitou-se também de uma nova entrada para os registros de DNS em IPv6 o **AAAA**, além do novo domínio criado o .ipv6.int. As formas de atribuição e delegação de reverso continua a mesma.

Neste projeto utilizou-se o sistema operacional CentOS, a instalação do pacote para o DNS é bem simples, utilizei do *BIND (Berkeley Internet Name Domain)* através do comando “*yum install bind bind-utils -y*”.

5.4.2 Configuração

Com a instalação do *BIND* concluída é necessário realizar a configuração do arquivo *named.conf (/etc/named.conf)* para que se possa criar as zonas reversas do prefixo requerido, no exemplo visto no Quadro 15 utilizou-se o prefixo 2801:1C30:0:1::/64.

6 CONCLUSÃO

Este estudo abordou diferentes tipos de protocolos e conceitos, levado por uma necessidade global, a implantação do IPv6, aplicou-se como pré requisito o funcionamento do protocolo internamente dentro de um provedor, para que assim possa se ter continuidade e levar esse a todos os dispositivos da rede.

A primeira impressão que se teve era de uma configuração simples, pelo fato de a configuração dos dois protocolos IPv4 e IPv6 serem parecidos, porém existem algumas particularidades do IPv6 que tornou o projeto mais complexo, porém, com o auxílio de estudos realizados em sala de aula tornou-se possível a realização deste.

Também foram apresentadas brevemente em forma de passo a passo algumas configurações necessárias para que este protocolo pudesse ser implementado.

As informações expostas neste trabalho mostra que os objetivos foram alcançados com sucesso, internamente o provedor já possui estrutura para o IPv6, sendo que seus principais servidores já estão respondendo a ele

6.1 TRABALHOS FUTUROS

Neste trabalho concluiu-se a configuração da rede interna do provedor e ainda deixa como opção de trabalhos futuros prosseguir com a implantação do protocolo IPv6 no modelo autenticação usuário/senha para atender os clientes.

REFERENCIAS

ALBITZ, Paul.; LIU, **Cricket. DNS and BIND**. 5th Edition. United States of América: O'Reilly Media, 2006.

ALEXANDRE, C. M. e REIS, E. A. **Sistemas Autônomos (AS) Brasileiros Introdução**. Disponível em: <<ftp://ftp.registro.br/pub/gter/gter28/07-Asbr.pdf>> . Acesso em 08 de Outubro de 2015.

ANDREOLI, A. V.; RODRIGUES, F. F. **Gerenciamento de Roteamento BGP em Pontos de Troca de Tráfego**. Porto Alegre – 2002

ARIOVALDO GRIESI. **Revisão técnica Mario Olimpio de Menezes**. São Paulo. Pearson Makron Books, 2004.

CAMPOS, D. R. C de ;JUSTO, R. D. **Tutorial DNSSEC**. Disponível em: <<ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>>. Acesso em: 18 de outubro 2015.

CISCO SYSTEMS, INC. **IP Addressing: DHCP Configuration Guide, Cisco IOS XE Release**. Capitulo 1. 170 West Tasman Drive, 2014.

COMER E. D. - **Interligação em Redes com TCP/IP vol. 1 - Princípios, protocolos e arquitetura** - 3a. ed. Ed. Câmpus – 1995

COUTO, B. R. **O protocolo DNS - Entendendo como funciona a resolução de nomes de domínio**. Junho de 2012. Disponível em http://www.ibm.com/developerworks/br/local/opensource/dns_protocol/. Acesso em 18 de Outubro de 2015.

HERTZOG, R.; MAS, R. **O Manual do Administrador Debian**. 1 ed. Freexian SARL. Junho de 2014.

IBOPE. **Acesso a Internet em domicílios continua a crescer no Brasil**. Disponível em: <<http://www.ibope.com.br/pt-br/noticias/Paginas/Acesso-a-Internet-em-domicilios-continua-a-crescer-no-Brasil.aspx>>. Acesso em 26 de Setembro de 2015.

KUROSE, J. F. **Redes de computadores e a Internet**. 5 ed. São Paulo: 2010.

MICROSOFT. **DHCP**. Disponível em: <[https://technet.microsoft.com/pt-br/library/cc778368\(v=ws.10\).aspx](https://technet.microsoft.com/pt-br/library/cc778368(v=ws.10).aspx)>. Acesso em 17 de Outubro de 2015.

NEMETH, Evi.; SNYDER, Garth.; HEIN, Trent R. **Manual Completo do Linux - Guia do Administrador**. Makron Books, 2004.

RFC 1930. Guidelines for creation, selection, and registration of an Autonomous System (AS). Disponível em: <<http://www.ietf.org/rfc/rfc1930.txt>>. Acesso em 08 de Outubro de 2015.

RFC 2461. Neighbor Discovery for IP Version 6 (IPv6). Disponível em: <<https://tools.ietf.org/html/rfc2461.txt>>. Acesso em 08 de Outubro de 2015.

RFC 2462. IPv6 Stateless Address Autoconfiguration. Network Working Group. Disponível em: <<http://www.ietf.org/rfc/rfc2462.txt>>. Acesso em 08 de Outubro de 2015

RFC 6106. IPv6 Router Advertisement Options for DNS Configuration. Disponível em: <<https://tools.ietf.org/html/rfc6106.txt>>. Acesso em 17 de Outubro de 2015.

RFC2131. Dynamic Host Configuration Protocol. Disponível em: <<https://www.ietf.org/rfc/rfc2131.txt>>. Acesso em 17 de Outubro de 2015.

RFC3315. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Disponível em: <<https://www.ietf.org/rfc/rfc3315.txt>>. Acesso em 17 de Outubro de 2015.

TANENBAUM, A. S. – **Redes de Computadores** – 4ª Ed., Editora Campus (Elsevier), 2003.

YANNUZZI, M. MASIP-BRUIN, X. O. Bonaventure, "Open issues in interdomain routing: a survey," **IEEE Network Magazine, Special issue on Interdomain Routing**. Nov-Dec 2005.