UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ – UTFPR
CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

CLENIO MOSS

PROJETO DE IMPLANTAÇÃO DO PROTOCOLO IPV6 NO PROVEDOR DE ACESSO A INTERNET

TRABALHO DE DIPLOMAÇÃO

MEDIANEIRA
2015

CLENIO MOSS

PROJETO DE IMPLANTAÇÃO DO PROTOCOLO IPV6 NO PROVEDOR DE ACESSO A INTERNET

Trabalho de Conclusão de Curso, apresentado como requisito parcial à obtenção do Grau de Tecnólogo, do Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas – COADS – da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Tecnólogo.

Orientador: Prof. *Dr*. Neylor Michel.

MEDIANEIRA

2015

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Graduação e Educação Profissional
Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas

TERMO DE APROVAÇÃO

PROJETO DE IMPLANTAÇÃO DO PROTOCOLO IPV6 NO PROVEDOR DE ACESSO A INTERNET

Por

CLENIO MOSS

Este Trabalho de Diplomação (TD) foi apresentado às 10:20 h do dia 11 de junho de 2015 como requisito parcial para a obtenção do título de Tecnólogo no Curso Superior de Tecnologia em Análise e Desenvolvimento de Sistemas, da Universidade Tecnológica Federal do Paraná, Câmpus Medianeira. O acadêmico foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

Prof. Neylor Michel
UTFPR – Câmpus Medianeira
(Orientador)

Prof. Paulo Lopez de Menezes
UTFPR – Câmpus Medianeira
(Convidado)

Prof. Hamilton Pereira da Silva
UTFPR – Câmpus Medianeira
(Convidado)

Prof. Juliano Rodrigo Lamb
UTFPR – Câmpus Medianeira
(Responsável pelas atividades de TCC)

“A mente que se abre a uma nova ideia jamais voltará ao seu tamanho original.” – Albert Einstein.

RESUMO

MOSS, Clenio. projeto de implantação do protocolo IPv6 no provedor de acesso a Internet. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas). Universidade Tecnológica Federal do Paraná. Medianeira 2015.

Por tratar-se de uma invenção tão antiga (1969) e ter seu surgimento em um momento tão conturbado (Guerra Fria), a Internet inicialmente tinha o objetivo de criar uma rede mundial de comunicação onde não dependesse somente de um nó central, mas sim que cada nó pudesse se comunicar com qualquer outro nó por qualquer caminho alternativo, assim, destruindo um nó, os outros conseguiriam se comunicar sem nenhum problema. Somente em 1983 o protocolo TCP/IP seria adotado. Um endereço de 32 bits com mais de 4 bilhões de endereços possíveis. Contudo, surgem nos anos 90, estudos sobre o esgotamento dos IP's versão 4 e se não fossem medidas paliativas, o IPv4 já teria se esgotado a algum tempo. O que na época, parecia quase infinito, hoje está esgotado. Com o surgimento do IPv6 (1993), além de solucionar o maior problema, que é o esgotamento de IP's, ele ainda contribui para melhorias significativas na rede. Este trabalho tem por objetivo apresentar esses aspectos positivos do protocolo IPv6 e implementa-lo num provedor de Internet já existente com a versão atual IPv4.

Palavras-chaves: Internet, Endereçamento, Protocolo da Internet.

ABSTRACT

MOSS, Clenio. PROJECT OF IMPLANTATION THE IPV6 PROTOCOL IN PROVIDER THE INTERNET ACCESS. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas). Universidade Tecnológica Federal do Paraná. Medianeira 2015.

Because it is such an old invention (1969) and has its appearance at such a troubled moment (Cold War), the Internet had originally the goal of creating a global communication network where it did not depend on a central node only, but each node could communicate with any other node by any alternative path. Thus destroying one node, the other ones would be able to communicate with each other without any problems. Only in 1983, the TCP/IP protocol would be adopted. A 32-bit address with over 4 billion possible addresses. However, studies on the depletion of IP version 4 arise in the 90s and if it were not for palliative measures, IPv4 would have run out for some time. What at that time seemed almost infinite, is exhausted today. With the emergence of IPv6 (1993), in addition to solving the biggest problem of IP's exhaustion, it still contributes to significant improvements in the network. This project aims to present the positive aspects of the IPv6 protocol and implement them in an existing version current IPv4.

Keywords: Internet, addressing, Internet protocol.

LISTA DE SIGLAS

ARP	*Address Resolution Protocol*
AS	*Autonomy System*
ASN	*Autonomy System Number*
BGP	*Border Gateway Protocol*
CIDR	*Classless Inter-Domain Routing*
DARPA	*Defense Advanced and Projects Agency*
DHCP	*Dynamic Host Configuration Protocol*
DHCPv6	*Dynamic Host Configuration Protocol version 6*
DNS	*Domain Name System*
EIGRP	*Enhanced Interior Gateway Routing Protocol*
EUA	Estados Unidos da América
FTP	*File Transfer Protocol*
IANA	*Internet Assigned Number Authority*
ICMP	*Internet Control Message Protocol*
ICMPv6	*Internet Control Message Protocol version 6*
IESG	*Internet Engineering Steering Group*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*

IPNG	*IP Next Generation*
IPsec	*IP Security Protocol*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ISO	*International Standarts Organization*
HTTP	*Hyper Text Transfer Protocol*
LACNIC	Registro de Endereços da Internet para a América Latina e o Caribe
LAN	*Local Area Network*
MAC	*Media Access Control*
MPLS	*Multi Protocol Label Switching*
NAT	*Network Address Translation*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Patch First*
OUI	*Organizationally Unique Identifier*
RARP	*Reverse Address Resolution Protocol*
RFC	*Request for Comments*
RIP	*Routing Information Protocol*
RNP	Rede Nacional de Ensino e Pesquisa
SA	Sistema Autônomo
SPF	*Shortest Path First*
SRI	Universidade de Stanford

TCP	*Transmission Control Procol*
TI	Tecnologia da Informação
UCLA	Universidade da Califórnia em Los Angeles
UCSB	Universidade da Califórnia em Santa Bárbara
UTFPR	Universidade Tecnológica Federal do Paraná
URSS	União das Repúblicas Socialistas Soviéticas
WAN	*Wide Area Network*
WWW	*World Wide Web*

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Conforme BRITO (2013), a Internet teve seu surgimento na década de 60, mais precisamente 1966, na época da Guerra Fria, partindo de um projeto da agência norte americana *Defense Advanced and Projects Agency* (DARPA), entidade cuja função era liderar as pesquisas de ciência e tecnologia aplicáveis às forças armadas dos EUA (Estados Unidos da América), sendo que um dos objetivos foi o de se ter a possibilidade de desenvolver projetos em conjunto, sem o incomodo da distância física, nem o risco de se perder dados e informações de uma base destruída em caso de combate. Era então necessária a utilização de um protocolo de comunicação que assegurasse tais funcionalidades, foi assim que começou a ser desenvolvida a arquitetura TCP/IP (*Transmission Control Protocol/Internet Protocol*).

Segundo BRITO (2013) ainda na década de 60, foram instalados os primeiros quatro nós de redes que interligava quatro pontos, três localizados no Estado da Califórnia, sendo eles, UCLA (Universidade da Califórnia em Los Angeles), UCSB (Universidade da Califórnia em Santa Bárbara), SRI (Universidade de Stanford) e um localizado no Estado de Utah (Universidade de Utah).

Somente em 1983, surge então a Internet que conhecemos hoje, ou seja, baseada no protocolo IP. Nesse período muitas pesquisas foram realizadas em todo o mundo, o que contribuiu para o aprimoramento do protocolo TCP/IP. Naquele tempo, não havia requisitos de escalabilidade, segurança ou mobilidade, era um momento que ainda existiam dúvidas se as pessoas realmente iriam se interessar em computadores pessoais. (BRITO, 2013).

De acordo com FLORENTINO (2012) a Internet continuou sendo controlada pelo departamento de defesa dos EUA até 1987 e então, o governo americano criou a IANA (*Internet Assigned Number Authority*), que passou a ser responsável pela atribuição de endereços IP’s e de nomes de domínio de todo mundo. A IANA por sua vez, dividiu o mundo em cinco partes, para cada parte foi estabelecido um escritório regional encarregado na alocação de endereços IP, conforme ilustrado na Figura 1.

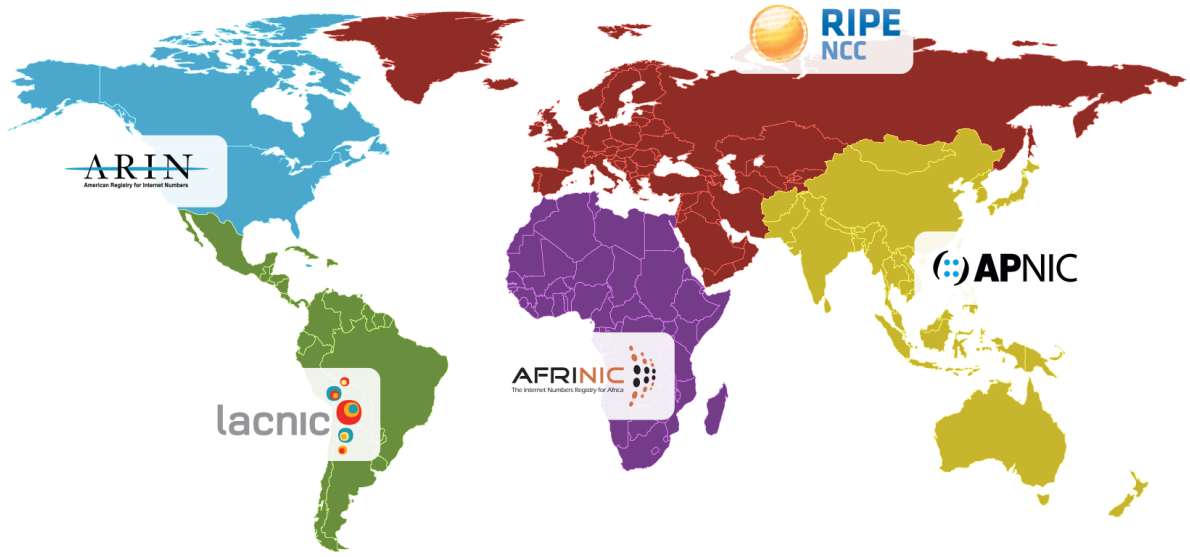


Figura 1 - Escritórios regionais da IANA
Fonte – Adaptado de iana.org

Como podemos ver na Figura 1, a LACNIC (Registro de Endereços da Internet para a América Latina e o Caribe) é um dos cinco Registros Regionais da Internet no mundo. É uma organização não governamental internacional estabelecida no Uruguai em 2002. Ela é responsável pela distribuição e administração dos recursos de numeração da Internet (IPv4, IPv6), entre outros recursos para a região da América Latina e o Caribe. (LACNIC.net).

No Brasil temos a RNP (Rede Nacional de Ensino e Pesquisa), responsável pela infraestrutura básica de interconexão e informação em nível nacional. A Rede Nacional de Pesquisa, como era chamada em seu início, tinha também a função de disseminar o uso das redes no Brasil. (RNP, 1997).

Hoje é possível encontrar Internet em praticamente todos os lugares, conforme GRIPA (2014), numa pesquisa realizada recentemente (Dezembro, 2013), pela consultoria de pesquisas ComScore, o Brasil se tornou o quinto maior país em número de habitantes conectados, possui aproximadamente 67 milhões de usuários. Com 353 milhões de usuários, a China lidera a lista, à frente dos Estados Unidos, onde quase 200 milhões de pessoas acessam a Internet. Na sequência aparece Índia, com 81 milhões, e Japão, em quarto lugar, com 73 milhões de usuários.

O número de usuários no mundo teve um aumento significativo, e segundo FLORENTINO (2012) para dar conta desse crescimento, verificou-se a necessidade de aumentar a quantidade de endereços IP's (*Internet Protocol*), sabendo-se que o IPv4, sendo o protocolo mais popular na Internet, tendo seu surgimento na década de 70, possui seus

endereços de IP’s com 32 bits, em torno de 4.3 bilhões de endereços, dos quais podemos constatar assim como PINTO (2013) que “não existe um para cada habitante do mundo e devido a essa escassez de IP’s e outros problemas que não foram incluídos em seu projeto como mobilidade, segurança e qualidade de serviço, iniciou-se estudos em busca de soluções para tais problemas”.

PINTO (2013) relata que muitos grupos de trabalhos iniciaram pesquisas com a intenção de desenvolver uma solução para os problemas levantados, sendo que no ano de 1993, o IESG (*Internet Engineering Steering Group*) criou uma nova versão do protocolo IP, o IPng (*IP Next Generation*). Com as devidas alterações e protocolos adicionados, originou-se o IPv6, que possui 128 bits, quatro vezes mais que seu antecessor.

De acordo com BRITO (2013), desde junho de 2012 o IPv6 passou a ser considerado o novo protocolo padrão da Internet, substituindo seu antecessor IPv4, o que significa que, a partir desta data, todo novo dispositivo de rede fabricado no mundo deve ter suporte ao IPv6.

Segundo PINTO (2013), “inicialmente o IPv6 era somente discutido em ambiente acadêmico, porém devido a necessidade evidente de atualização do IPv4, com a preocupação da exaustão dos endereços IP, um novo protocolo deveria ser desenvolvido”.

Essa nova versão do protocolo foi desenvolvida para atualizar o IPv4, novas funcionalidades foram adicionadas, outras foram mantidas e até funcionalidades desnecessárias foram removidas, sendo que para FALSARELLA (2010) “é preciso lembrar que o IPv4 não irá sumir de uma hora para outra, os dois protocolos irão coexistir por um bom tempo”.

2 OBJETIVOS

2.1 OBJETIVO GERAL

Realizar um projeto de implantação do protocolo IPv6 na estrutura da rede de um provedor de acesso a Internet.

2.2 OBJETIVOS ESPECÍFICOS

- Fazer a solicitação de um bloco v6 junto a LACNIC e/ou RNP;
- Sumarizar um bloco de IPv6 para a topologia atual;
- Realizar a configuração dos roteadores envolvidos.

2.3 JUSTIFICATIVA

Este estudo foi elaborado a fim de ressaltar a importância da implementação do Protocolo IPv6 como medida para cessar as falhas da antiga e presente versão 4, bem como promover a evolução do mesmo.

De acordo com JAMHOUR (2008), as mudanças realizadas no IPv6 podem ser associadas a cinco categorias, conforme ilustrado na Figura 2.

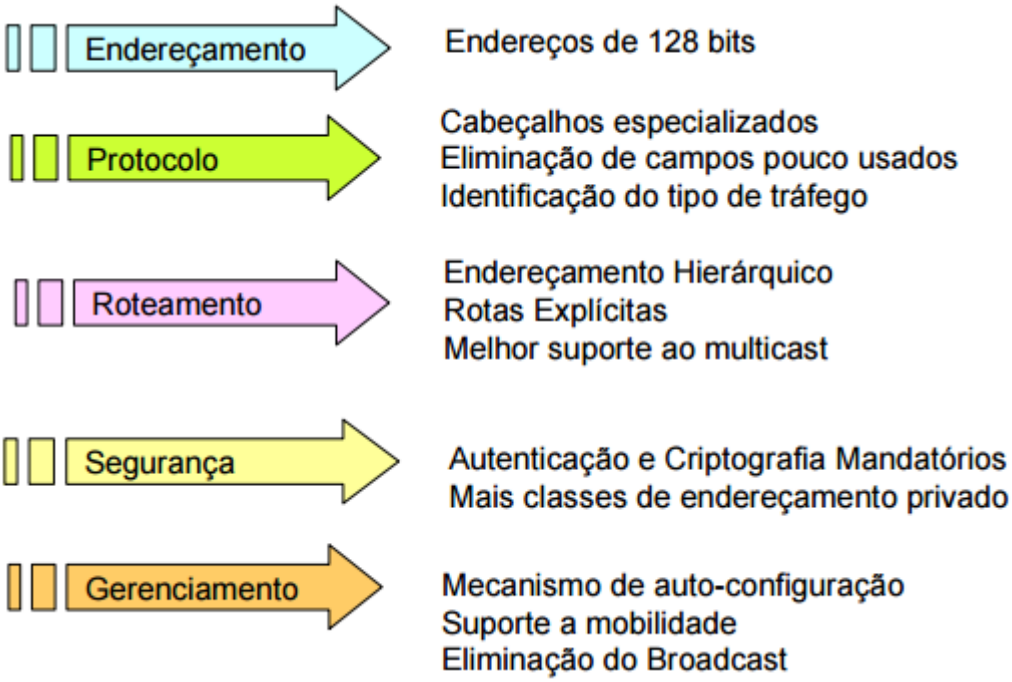


Figura 2 - Melhorias implementadas no protocolo IPv6.
Fonte – Adaptado de JAMHOUR (2008)

- Endereçamento: Os endereços IP versão 6 tiveram uma ampliação para um número possivelmente inesgotável.
- Cabeçalho do Protocolo: O protocolo IP versão 6 permite criar cabeçalhos de diferentes tamanhos, conforme as exigências especificas dos pacotes que estão sendo enviados.
- Roteamento: O protocolo IP versão 6 desenvolveu o conceito de hierarquia de endereçamento que possibilita um conjunto de rotas nas tabelas de roteamento dos roteadores BGP. Foi desenvolvido também a oportunidade de escolha da rota por onde o pacote ira passar.
- Segurança: O IPv6 cria mais classes de endereçamento privado, concedendo mais opções de gerenciamento para a estrutura da rede e maior segurança.
- Gerenciamento: O IPv6 possui um mecanismo de atribuição automática de endereço sem DHCP (auto configuração) e uma melhor mobilidade que faz a troca automática do endereço IP quando o usuário muda de rede.

3 REVISÃO BIBLIOGRÁFICA

Conforme BRITO (2013, p. 19), na época em que a Internet estava sendo elaborada (década de 60), o projeto tinha como finalidade a construção de uma rede experimental que tivesse a arquitetura de uma rede distribuída e não centralizada, tendo como característica principal a resistência a falhas. Essa resistência foi um dos requisitos de projeto mais importantes, afinal, era época em que os EUA (Estados Unidos da América) estavam em guerra contra a URSS (União das Repúblicas Socialistas Soviéticas), com isso, havia uma preocupação constante de que ataques aos meios de comunicação do país resultassem na indisponibilidade nos serviços de telecomunicação, por isso o motivo de a internet ser financiada pelos militares.

Segundo BRITO (2013, p. 21), a Internet é uma rede baseada totalmente em padrões abertos, onde toda tecnologia que a integra é publicada pela IETF *(Internet Engineering Task Force*) em documentos públicos acessíveis a qualquer usuário, que são denominados RFC's (*Request for Comments*). Essa é uma das características fundamentais da rede, afinal, o crescimento da Internet até ela se tornar o que conhecemos hoje só foi possível por causa dos padrões abertos.

De acordo com BRITO (2013), toda a estrutura da internet esta baseada no protocolo IPv4, na RFC 791 (*Request for Comments 791*) que foi pela primeira vez publicada em Setembro de 1981. Este documento descreve o protocolo da camada de rede mais popular e atualmente em uso, o IPv4.

BRITO (2013), ainda ressalta que somente na década de 90 começou a ficar evidente as falhas do IPv4, como exemplo, a escalabilidade comprometida em virtude do endereçamento limitado, falta de suporte nativo á segurança para execução de aplicações sigilosas, falta de suporte á mobilidade para permitir dispositivos móveis acessando á rede etc.

Para MORAIS et al. (2012, p. 42) a Internet é uma rede mundial de computadores ou terminais ligados entre si, que tem em comum um conjunto de protocolos e serviços, de uma maneira que os usuários conectados possam aproveitar os serviços de informação e comunicação de alcance mundial através de linhas telefônicas, linhas de comunicação privadas, satélites e demais serviços de telecomunicações.

Para reduzir a complexidade de um projeto de rede, é aconselhável a organização da mesma em forma de pilha de camadas, colocadas uma sobre a outra. A identificação e função

de cada camada diferem de uma rede para outra, porem o objetivo em todas as redes é que cada camada possa oferecer determinados serviços às camadas superiores, isolando as mesmas dos detalhes de implementação desses recursos, ou seja, cada camada é uma espécie de máquina virtual, oferecendo determinados serviços á camada que esta acima dela. (TANENBAUM, 2002).

Com o surgimento das redes de computadores, ocorreu também a incompatibilidade dos equipamentos, isto é, uma determinada tecnologia só era suportada por seu fabricante. Não havia possibilidades de misturar equipamentos de fabricantes diferentes. Dessa forma, quando se criava uma rede, usavam-se somente tecnologias de um mesmo fabricante, assim, evitando a incompatibilidade dos mesmos. (TORRES, 2007)

Segundo PINHEIRO (2008), o modelo OSI (*Open Systems Interconnection*), criado em 1983 pela ISO (*International Standarts Organization*) e formalizado em 1995, possui a finalidade de padronizar equipamentos para redes de comunicação de dados.

Para TORRES (2007), o conceito básico do modelo OSI é que ele possui sete camadas e cada uma é responsável por algum tipo de processamento comunicando-se apenas com a camada inferior ou superior. Por exemplo, a camada 3 irá comunicar-se somente com as camadas 2 e 4, e nunca diretamente com as demais camadas, conforme ilustrado na Figura 3.

Figura 3 - Estrutura do modelo OSI
Fonte – Adaptado de PINHEIROS (2008)

3.1 CAMADAS DO MODELO OSI

3.1.1 Primeira camada: Física.

A camada Física representa as características mecânicas, elétricas, funcionais e as maneiras para ativar, manter e desativar conexões físicas para a transferência de bits. (PINHEIRO, 2008).

PINHEIRO (2008) ainda afirma que as características mecânicas tratam-se do tamanho e forma de conectores, pinos e cabos que compõem um circuito de transferência. As características elétricas caracterizam os valores dos sinais elétricos (nível de tensão e corrente) usados. As características funcionais esclarecem o significado dado aos sinais transmitidos na camada física (por exemplo, transmissão, recepção, etc.).

Ainda sobre as características mecânicas, podemos citar o cabeamento feito por fibra óptica. Desde a sua existência, as fibras ópticas representaram uma revolução na forma de transmitir informações, servem para transmitir voz, televisão e sinais de dados por ondas de luz, por meio de fios finos e flexíveis, constituídos de vidro ou plástico. (CAMPOS, 2002).

CAMPOS (2002) ainda ressalta que existem dois tipos de fibra óptica, as multimodo, utilizadas em aplicações de rede locais (LAN) e as monomodo, utilizadas para aplicações de redes de longa distância (WAN). Conforme pode ser visto na Figura 4.

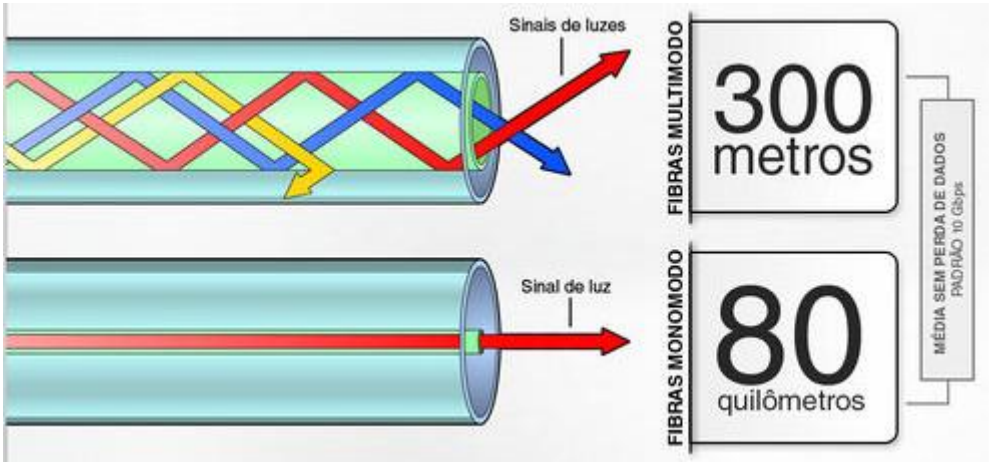


Figura 4 - Diferença entre fibra óptica Multimodo e Monomodo
Fonte – Adaptado de FERREIRA (2013)

3.1.2 Segunda camada: Enlace

Para TANENBAUM (2002), a camada de enlace tem como principal tarefa, transformar um canal de transmissão bruta em uma linha que se mostra livre de erros de transmissão não reconhecidos pela camada de rede. Para a execução dessa tarefa, a camada de enlace de dados faz com que o transmissor separe os dados de entrada em quadros de dados e os transmita sequencialmente. O receptor enviara um aviso de recebimento se o serviço for confiável, assim, confirmando a recepção correta de cada quadro.

Outra característica importante da camada de enlace de dados é a resolução de problemas de danificação, perda e impossibilitar que um transmissor envie uma quantidade excessiva de dados a um receptor mais lento. (TANENBAUM, 2002).

Segundo PINHEIROS (2008), o principal objetivo da camada de enlace é tornar o meio físico mais confiável e sem erros para as camadas superiores, proporcionando mecanismos á ativar, manter e desativar a conexão. Para cumprir seu objetivo, são implementados mecanismos de controle e identificação de possíveis erros e os bits de informação são agregados em unidades chamadas "*frames*".

De acordo com TORRES (2001), o switch é responsável por enviar quadros de origem diretamente para portas de destino, pois o switch é um dispositivo que aprende, ou seja,

quando um computador envia um quadro para a rede, o switch identifica o campo de endereço MAC (*Media Access Control*) de origem do pacote e anota em uma tabela interna o endereço MAC da placa de rede do computador que está conectado a aquela porta. Desta forma, quando o switch recebe um quadro para ser enviado, ele consulta essa sua tabela interna. Caso o endereço MAC de destino esteja nessa tabela, ele consegue identificar para qual porta deve enviar o quadro.

3.1.3 Terceira camada: Rede

Segundo TANENBAUM, (2002), a camada de rede é responsável pelo trafego e roteamento dos dados na rede garantido que os pacotes de origem cheguem até o destino final. Quando um pacote viaja de uma rede para outra, muitos problemas de compatibilidade podem aparecer (endereçamento, tamanho, etc.), sendo que a camada de rede deve resolver essas incompatibilidades.

De acordo com TORRES (2001), o roteador é um dispositivo fundamental na escolha de um caminho para os pacotes chegar até seu destino. Em redes de grande porte pode haver mais de um caminho e o responsável por escolher o melhor caminho é o roteador. Resumidamente, o roteador é um dispositivo encarregado de interligar redes diferentes.

A Internet possui uma ampla variedade de protocolos relacionados à camada de rede. Entre eles, o IP, que é o protocolo de transporte de dados, os protocolos de controle ICMP, ARP e RARP, e os protocolos de roteamento OSPF, BGP, RIP e EIGRP. (TANENBAUM, 2002).

O Protocolo IP (*Internet Protocol*), conforme afirma MORAIS et al. (2012, p. 32), possibilita o roteamento dos pacotes para que os mesmos possam transitar pela rede e conseguir chegar a determinado destino, controlando o fluxo dos dados da grande rede. O Protocolo IP é responsável pela comunicação entre máquinas em uma estrutura de rede TCP/IP. Ele auxilia a capacidade de comunicação entre cada elemento componente da rede para permitir o transporte de uma mensagem de origem até o destino.

No IPv4 os endereços de IP’s são compostos por 4 blocos de 8 bits, também chamados de octetos, totalizando 32 bits cada IP. A sua utilização em “octetos” é apenas para facilitar a visualização, mas quando processados, são apenas números binários. No total são 4.294.967.296 de endereços IP’s no mundo, que são representados através de números de 0 a 255. (MACEDO 2012).

De acordo com FLORENTINO (2012, p. 17), a divisão dos endereços IP’s do protocolo de Internet IPv4 nunca foram iguais, metade dos endereços disponibilizados foram para os EUA, onde o *backbone* ou espinha dorsal da internet fora originado e o restante divididos entre os demais países. Para o protocolo IPv6, o número de IP’s é muito maior, cerca de 340 undecilhões de endereços.

Conforme MACEDO (2012), inicialmente os endereços IP’s foram divididos em cinco classes, sendo elas chamadas de A, B, C, D e E. Dentre elas, apenas as classes A, B e C são realmente utilizadas, pois a D e E são respectivamente para *multicast* e utilização futura. Na Tabela 1 é possível ver a separação de IP’s para cada classe e a quantidade de redes e hosts que cada uma pode ter:

Tabela 1 - Separação das classes e a quantidade de Redes e Hosts para as mesmas

Classe	Endereço mais baixo	Endereço mais alto	Máscara de Sub-Rede	Redes	Host por Rede
A	1.0.0.0	126.0.0.0	255.0.0.0	128	16.777.216
B	127.0.0.0	191.255.0.0	255.255.0.0	16.384	65.536
C	192.0.0.0	223.255.255.0	255.255.255.0	2.097.150	256
D	224.0.0.0	239.255.255.255		Multicast	
E	240.0.0.0	247.255.255.255		Uso Futuro	

Fonte – Adaptado de CRISPIM (2013)

Já com o protocolo IPv6, a principal característica em relação ao IPv4, foi o aumento do endereçamento que passou de 32 para 128 bits, assim, representando aproximadamente 79 octilhões (7,9×1028) de vezes a quantidade de endereços IPv4 e representa também, mais de 56 octilhões (5,6×1028) de endereços por ser humano na Terra, mais precisamente 340.282.366.920.938.463.463.374.607.431.768.211.456 números de endereços IPv6, considerando-se a população mundial estimada em 6 bilhões de habitantes. (PINTO, 2013).

Conforme BRITO (2013) sua leitura é representada no formato hexadecimal de base 16, ou seja, seu sistema numérico utiliza os números de 0 a 9 e as letras de A até F. Este formato foi escolhido por ser uma forma mais simples de representar, tendo a menor notação para o endereço IPv6.

Conforme TELECO (2015), o IPv6 foi projetado para atender as exigências da potencial expansão da Internet e propiciar uma comunicação global, onde as normas de endereçamentos irão novamente ser transparentes para as aplicações, como eram realizadas

anteriormente ao uso do protocolo NAT (existente somente na versão IPv4), por meio da autoconfiguração e suporte *plug and play*, os dispositivos de rede poderão ligar-se à rede sem uma configuração manual. O IPv6 consegue proporcionar isso através das seguintes vantagens ás redes e aos profissionais de TI:

A principio o IPv6 dispõe de muito espaço para endereços, proporcionando uma disponibilidade e escalabilidade global, tendo como resultado um número quase ilimitado de endereços IP e uma arquitetura hierárquica de rede para um eficiente encaminhamento dos dados eliminando os problemas relacionados ao protocolo NAT. A escalabilidade "fim-a-fim" e a consequente gestão de rede mais simples e fácil é possível graças a capacidade de fornecer endereços globais para cada dispositivo de rede. (TELECO 2015).

A segunda vantagem ou beneficio seria um formato simplificado do cabeçalho para um manuseio eficiente dos pacotes. Conforme pode ser visto na figura abaixo, seis dos doze campos do cabeçalho IPv4 foram retirados (campos em verde claro) na versão seis (IPv6), sendo que alguns campos ainda existem, porem com nomenclatura diferenciada (campos em vermelho). Um novo campo (campo em laranja) foi adicionado com o intuito de aumentar a eficiência e introduzir funcionalidades novas. (TELECO 2015).

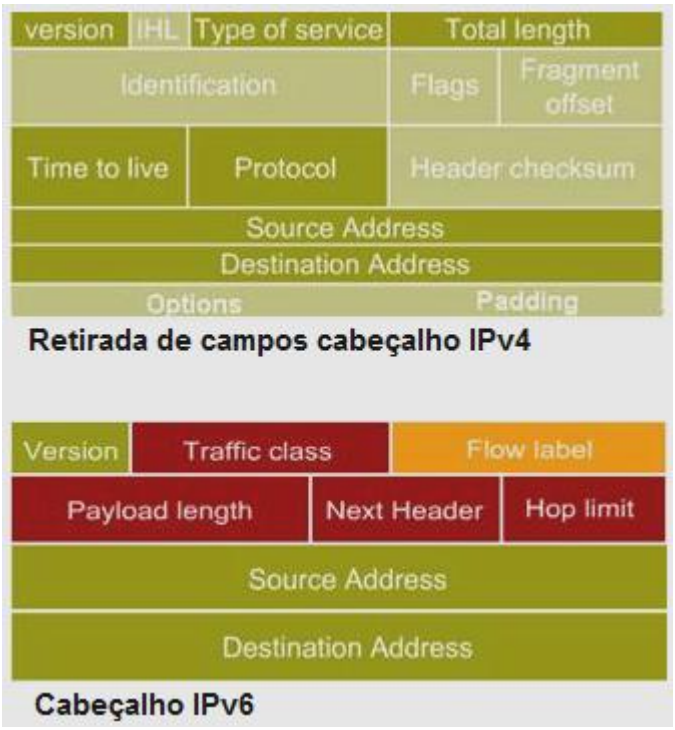


Figura 5 - Comparativo entre o cabeçalho IPv4 e IPv6
Fonte – Adaptado de TELECO (2015)

A terceira vantagem significativa do IPv6, é a segurança integrada com a implementação necessária do IPsec (*IP Security Protocol*), que consiste em aumentar a confiabilidade das informações fornecidas pelo usuário para uma localidade da Internet, como bancos. Diferentemente do IPv4, que a utilização do IPSec é opcional e teve que ser adaptada para o funcionamento.

Tabela 2 - Sistema de numeração hexadecimal

Hexadecimal	Decimal	Binário
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Fonte – Adaptado de BRITO (2013)

O ICMP (*Internet Control Message Protocol*), definido na RFC 792, é um protocolo que relata erros e fornece uma resposta para a fonte original que requisitou um teste de conectividade. Um exemplo de teste é o comando "*ping"*, que exibe se o destino respondeu e quanto tempo demorou a receber uma resposta. Se houver um erro na remessa ao destino, o comando *ping* exibirá uma mensagem de erro. (BRITO 2013).

De acordo com PINTO (2013), todas as mensagens ICMP apresentam o mesmo formato, composto por *type*, que indica o tipo da mensagem, código para diferenciar, *Checksum* que faz a soma de verificação e a variável do corpo. Conforme pode ser visto na Tabela 3.

Tabela 3 - Formato de mensagem ICMP

ICMP	Descrição
Type	Campo com 8 bits, identifica o tipo de mensagem enviada ou de resposta recebida (mensagens de erro ou informação).
Code	Também com 8 bits, serve para diferenciar as mensagens, cada uma tem seu código.
Checksum	Com 16 bits, o *checksum* é calculado somente sobre o cabeçalho ICMP. Para se calculá-lo, faz-se o complemento de um de cada palavra de 16 bits do cabeçalho, soma-se elas e faz o complemento de um da soma total (para efeitos de cálculo, o campo *Checksum* vale 0).
Message body	Contém os dados da mensagem específica.

Fonte – Adaptado de PINTO (2013)

Conforme HAGEN (2006, p. 60), o protocolo de mensagens de controle da Internet ICMP transmite informações importantes sobre o desempenho da rede. Ele informa erros se os pacotes não podem ser processados de forma adequada e envia mensagens de informações sobre o estado da rede. Por exemplo, se um roteador for impedido de encaminhar um pacote, porque ele é muito grande para ser enviado para outra rede, ele envia uma mensagem ICMP de volta ao host de origem. O host de origem pode usar esta mensagem para indicar um pacote de tamanho adequado e envia-lo novamente.

O ICMPv6 é a versão que funciona com o protocolo IPv6, semelhante ao antecessor ICMPv4, porém apresenta mais recursos devido a ter absorvido alguns protocolos como o ARP/RAP. Responsável por tais serviços como descoberta de vizinho e mobilidade IPv6 por exemplo, possui mais mensagens. (PINTO 2013).

Para BRITO (2013), o protocolo IP não foi projetado para ser completamente confiável e por isso o ICMP é muito importante na Arquitetura TCP/IP, para verificação e diagnóstico da conectividade entre dispositivos interligados em redes.

Já os protocolos ARP (*Address Resolution Protocol)* e RARP (*Reverse Address Resolution Protocol*) que foram extintos na versão IPv6, cujas funcionalidades foram agregadas pelo ICMPv6, sendo o ARP responsável em mapear os endereços físicos (*hardware*) através de endereços lógicos (IP) que é previamente gravado nos dispositivos de rede em memória de somente leitura. E o RARP que realiza o inverso do ARP, mapeando os endereços lógicos para endereços físicos. (BRITO 2013).

3.1.4 Quarta camada: Transporte

De acordo com TANENBAUM (2002), a camada de transporte controla as transferências de dados e transmissões tendo como função transportar os dados da camada de sessão, quebra-los em partes menores, caso for necessário, passa-los para a camada de rede e garantir que as partes cheguem em ordem ao outro lado. Essa camada isola as camadas superiores das mudanças inevitáveis na tecnologia de *hardware*.

Segundo BRITO (2013), um exemplo de protocolo que atua na camada de transporte é o DHCPv6 (protocolo específico para IPv6), similar ao seu antecessor (DHCP) no quesito de distribuir endereços IP automático, porém, nessa nova versão a distribuição pode ser feita de duas maneiras:

O modo mais simples de configuração é o *stateless*, que recebe este nome, pois quando a máquina for receber o endereço IPv6, irá receber somente o prefixo que devera ser usado internamente na rede, assim, o computador gerará o endereço de identificação de host, a partir do endereço físico da interface (MAC), porém, esta configuração tem dois inconvenientes, que é o uso relativamente ineficiente do espaço de endereços e falta de controle de acesso à rede. (BRITO, 2013).

BRITO (2013) ainda destaca outro modo de distribuir endereços automaticamente, através da configuração *stateful*, que serve para quando á necessidade de manter o registro dos endereços dinamicamente atribuídos e que precisam determinar o escopo claramente sem restrições. Normalmente essa configuração será utilizada em servidores Linux e Windows Server, somente no IPv6.

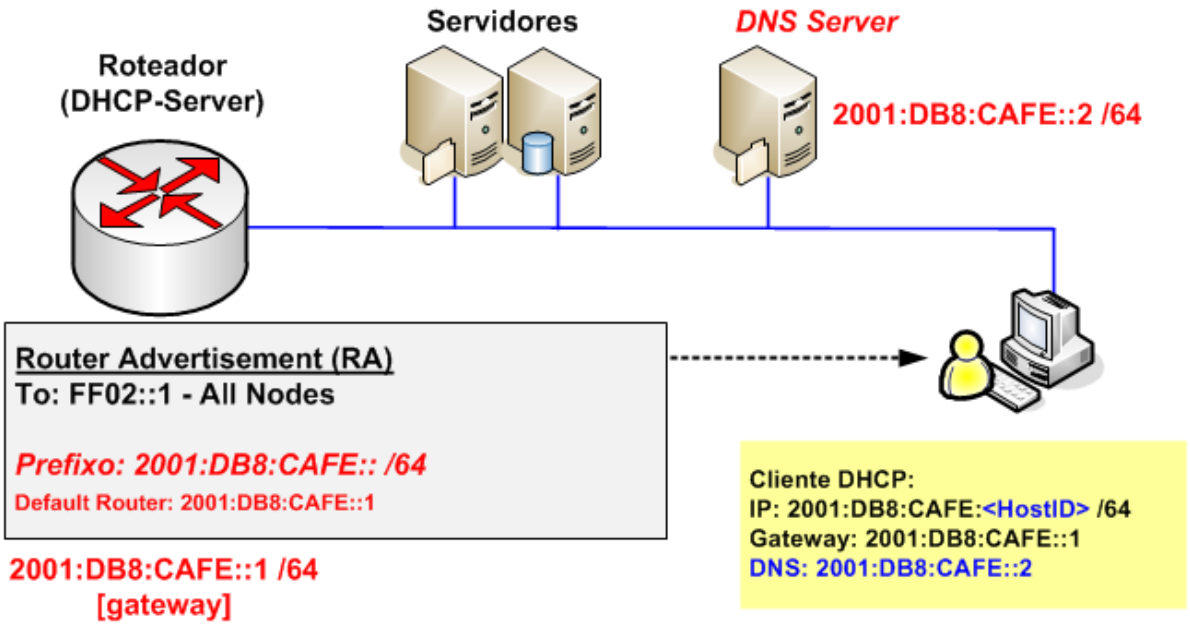


Figura 6 – Funcionamento do DHCPv6
Fonte – Adaptado de BRITO (2013)

A Figura 6 exemplifica o funcionamento do protocolo DHCPv6, onde o cliente esta recebendo a configuração automática (IPv6, Gateway e DNS) através do roteador (DHCP-Server).

Resumidamente para COMER (2014), o objetivo da camada de transporte é fornecer confiabilidade fim a fim, possibilitando que o computador de origem se comunique com o computador de destino. Apesar de as camadas inferiores fornecerem verificações confiáveis, a camada de transporte faz uma verificação adicional para garantir que nenhuma máquina intermediária falhe.

3.1.5 Quinta camada: Sessão

Conforme PINHEIRO (2008), a camada de sessão estabelece uma estrutura de controle para a comunicação entre aplicações, gerencia de maneira organizada a transferência de informação, desde a maneira como se processa o diálogo até a troca de dados entre as entidades de apresentação.

TANENBAUM (2002) cita os diversos serviços da camada de sessão, inclusive o controle de diálogo, que estabelece quem deve transmitir em cada momento, o gerenciamento de símbolos, em que ambos os lados não tentem a mesma operação ao mesmo tempo e a

sincronização que realiza a verificação de transmissões para permitir que elas continuem a partir do ponto em que estavam ao ocorrer uma falha.

3.1.6 Sexta camada: Apresentação

A Camada de Apresentação efetua a conversão do formato de dados de forma padrão, assim, permitindo que eles sejam entendidos por todos os sistemas envolvidos na comunicação. Esta camada também faz a compressão de dados e criptografia para garantir privacidade. (PINHEIRO, 2008).

Segundo TANENBAUM (2002), para suceder a comunicação entre computadores com dados de diferentes representações, as estruturas de dados a serem intercambiadas podem ser estabelecidas de maneira indefinida, simultaneamente com uma codificação padrão que será empregada no decorrer da conexão. A camada de apresentação administra essas estruturas de dados indefinidas e concede a definição e o intercambio de estruturas de dados de nível superior, como por exemplo, registros bancários.

3.1.7 Sétima camada: Aplicação

Conforme TANENBAUM (2002), a camada de aplicação é a camada do modelo OSI mais próxima do usuário, ela possui uma série de protocolos comumente necessários para os usuários, sendo o HTTP (*Hyper Text Transfer Protocol*) um dos mais conhecidos, que constitui a base para a WWW (*World Wide Web*). Quando um navegador deseja uma página da Web, ele envia o endereço da página desejada ao servidor, utilizando o HTTP, então, o servidor retorna a página.

Outros protocolos de aplicação são usados para transferências de arquivos, correio eletrônico e transmissão de notícias pela rede, como exemplo, o FTP (*File Transfer Protocol)*, protocolo de transferência de arquivos. (TANENBAUM, 2002).

3.2 PROTOCOLO TCP/IP

Tendo o seu surgimento na década de 70, para TORRES (2007) o TCP/IP (*Transmission Control Procol/Internet Protocol*) é o protocolo mais utilizado atualmente, sendo na verdade um conjunto de protocolos, cujo nome faz referência a dois protocolos

diferentes, o TCP que é o protocolo de controle de transmissão e o IP que é um protocolo de internet.

O TCP/IP interage com quatro camadas, sendo elas, a aplicação que realiza tarefas diretamente em contato com os usuários, a camada de transporte que oferece suporte a comunicação entre diversos dispositivos de redes distintas, a camada de rede que determina o melhor caminho através da rede e a camada física que controla os dispositivos de *hardware* e meio físico que compõem a rede. (TORRES, 2007).

Tabela 4 - Arquitetura do TCP/IP

Modelo nº	OSI	TCP/IP
7	Aplicação	Aplicação
6	Apresentação	
5	Sessão	
4	Transporte	Transporte
3	Rede	Rede
2	Enlace	Física
1	Física	

Fonte - Adaptado de TORRES (2007)

Observando a tabela 4, pode-se notar que a camada de aplicação do modelo TCP/IP junta as três últimas camadas do modelo OSI, enquanto a camada de acesso á rede do modelo TCP/IP engloba a camada física e de enlace do modelo OSI, deixando somente as camadas de rede e transporte parecidas com o modelo OSI. (TORRES, 2007).

TORRES (2007) ainda destaca que se passaram mais de quatro décadas e a arquitetura de protocolos TCP/IP continua sendo referência no que se diz respeito à conectividade da Internet.

3.3 TIPOS DE ENDEREÇAMENTO PARA O IPV6

De acordo com FLORENTINO (2012), *unicast*, *anycast* e *multicast* são os três tipos de endereçamentos existentes no IPv6. Os endereços de broadcast que havia no IPv4, não existem no IPv6, esta função será realizada pelos endereços *multicast*.

3.3.1 Unicast

Utiliza a técnica um-para-um, ou seja, identificam um host de forma única e exclusiva. Com a quantidade enorme de endereços possíveis, este tipo de endereço possibilita que todos os hosts do planeta consigam ter conectividade fim-a-fim, sem precisar utilizar endereços públicos e privados, como ocorre no IPv4. (FLORENTINO, 2012). A Figura 7 tem por objetivo ilustrar uma configuração entre apenas dois pontos dentro de um grupo.

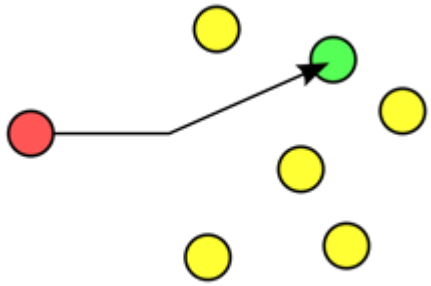


Figura 7 - Modelo *Unicast*.
Fonte – Adaptado de BRITO (2013)

3.3.2 Multicast

Utiliza a técnica um-para-muitos, identificam um grupo de hosts que adquirem o mesmo fluxo de pacotes. Seu uso pode ser encontrado nas transmissões de áudio e vídeo e em alguns protocolos de roteamento. (FLORENTINO, 2012). A Figura 8 ilustra a configuração do modelo *multicast*, onde um host encontra vários grupos de hosts.

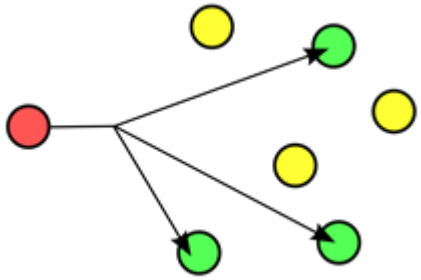


Figura 8 - Modelo *Multicast*
Fonte – Adaptado de BRITO (2013)

3.3.3 Anycast

Utiliza a técnica um-para-um-de-muitos, isto é, quando um endereço é compartilhado por mais de um host com a finalidade de se alcançar o host mais próximo. Sua utilização mais comum pode ser encontrada nos serviços UDP (*User Datagram Protocol*), quando temos vários servidores publicados em variadas localidades com o mesmo número IP. (FLORENTINO, 2012). A Figura 9 mostra a configuração *anycast*, onde um host consegue compartilhar arquivos com vários hosts, buscando alcançar os hosts mais próximos.

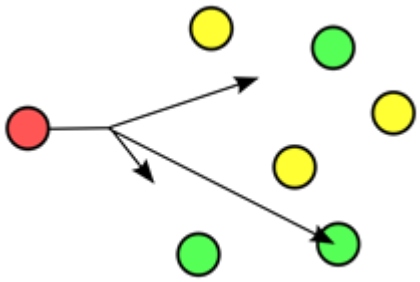


Figura 9 - Modelo *Anycast*.
Fonte – Adaptado de BRITO (2013)

3.4 MEDIDAS PALIATIVAS PARA O IPV4 CONTINUAR ATUANDO:

Para BRITO (2013, p. 27), o esgotamento dos aproximados 4,3 bilhões de endereços IPv4 já era algo previsto pelos especialistas desde o início da década de 1990. Desde então, os mesmos preocuparam-se em criar um novo protocolo com capacidade muito maior de endereços. Enquanto esse novo protocolo, identificado como IPv6 estava em fases de testes, foram desenvolvidos vários mecanismos temporários para economizar o esgotamento dos endereços IPv4.

Conforme FLORENTINO (2012) e BRITO (2013), se não fosse por esses mecanismos paliativos como a separação de endereços públicos e privados (RFC 1918), o uso do NAT para poupar os endereços internos das redes locais, o DHCP para fornecer IP’s dinâmicos durante um determinado período e o CIDR para alocar e especificar blocos de endereços de tamanhos variados de acordo com a necessidade, os blocos de endereço IPv4 já teriam se esgotado há algum tempo.

BRITO (2013, p. 27) ainda ressalta que essas medidas provisórias foram responsáveis por manter a internet funcionando até hoje com uma sobrevida de quase 25 anos para o IPv4,

assim, adiando a adoção do IPv6 durante todos esses anos. Chegou o momento em que essas medidas não são mais suficientes diante do crescimento da Internet.

3.4.1 RFC 1918

Criada em 1996 a RFC (*Request For Comments*) 1918 especifica três faixas de endereços privados, que não circulam na internet, estes endereços são 10/8 (de 10.0.0.0 até 10.255.255.255), 172.16/12 (de 172.16.0.0 até 172.31.255.255) e 192.168/16 (de 192.168.0.0 até 192.168.255.255), conforme podem ser vistos na tabela 5. Essa também foi uma das medidas para a economia dos endereços IPv4 roteáveis na Internet, afinal, por causa desses endereços privados, uma empresa não precisava mais de um endereço publico roteável na Internet para seus hosts internos. (BRITO, 2013).

Tabela 5 - Endereços privados RFC 1918

Classe	Intervalo de endereços internos RFC 1918
A	10.0.0.0 até 10.255.255.255
B	172.16.0.0 até 172.31.255.255
C	192.168.0.0 até 192.168.255.255

Fonte - Adaptado de BRITO (2013)

3.4.2 DHCP (Dynamic Host Configuration Protocol)

DHCP (*Dynamic Host Configuration Protocol*), criado em 1993, onde através dele é possível distribuir automaticamente os endereços para todas as máquinas internas de uma grande rede, o que diminui os esforços de configuração dos nós. (BRITO, 2013).

MOREIRAS *et al* (2010) afirmam que o DHCP esta sendo bastante utilizado por parte dos fornecedores de serviços de Internet por possibilitar a atribuição de endereços IP’s temporários a seus clientes conectados. Assim sendo, é desnecessário obter um endereço para cada cliente, tendo apenas que designar endereços dinamicamente, através de seu servidor DHCP, que terá uma lista de endereços IP disponíveis, e quando um novo cliente se conectar à rede, lhe será apresentado um desses endereços de maneira arbitrária, e no momento que o cliente se desconecta, o endereço é devolvido.

De acordo com BRITO (2013), apesar de a técnica DHCP ser muito usada no mercado, ela é ruim no quesito segurança, porque abrange uma distancia maior na identificação do cliente, pois deixa de existir o endereço exclusivo.

Resumidamente para PEREIRA (2009), quando um computador conecta-se a uma rede, ele envia um pacote ao servidor solicitando o serviço DHCP, o servidor recebe este pacote e gerencia uma faixa fixa de IP's disponíveis juntamente com as informações e parâmetros necessários (*gateway* padrão, nome de domínio, DNS, etc), após esse gerenciamento, o servidor devolve um pacote com estes endereços e configurações para o cliente.

3.4.3 CIDR (Classless Inter-Domain Routing)

O CIDR (*Classless Inter-Domain Routing*) foi descrito na RFC 1519 e para TANENBAUM (2002) ele tem como objetivo o fim de classes de endereçamento, permitindo alocar blocos com o tamanho necessário a cada rede, além desta funcionalidade, pode ser feita a agregação de maneira a permitir uma redução no tamanho da tabela de roteamento. Basicamente o CIDR tem a função de alocar os endereços IP's restantes em blocos de tamanho variável, sem levar em consideração as classes.

De acordo com BRITO (2013), desde o surgimento do IPv4, a divisão entre os bits do prefixo da rede e do sufixo de host foi separado em 3 classes, sendo elas A, B e C onde possuem respectivamente 8, 16 e 24 bits. A finalidade desta divisão era atender variados tipos de redes, sejam elas redes pequenas, médias ou grandes. A classe A é representada por poucas redes de grande porte com muitos hosts; a classe B, redes de médio porte; e a classe C, muitas redes de pequeno porte com poucos hosts. Conforme pode ser visto na figura a seguir.

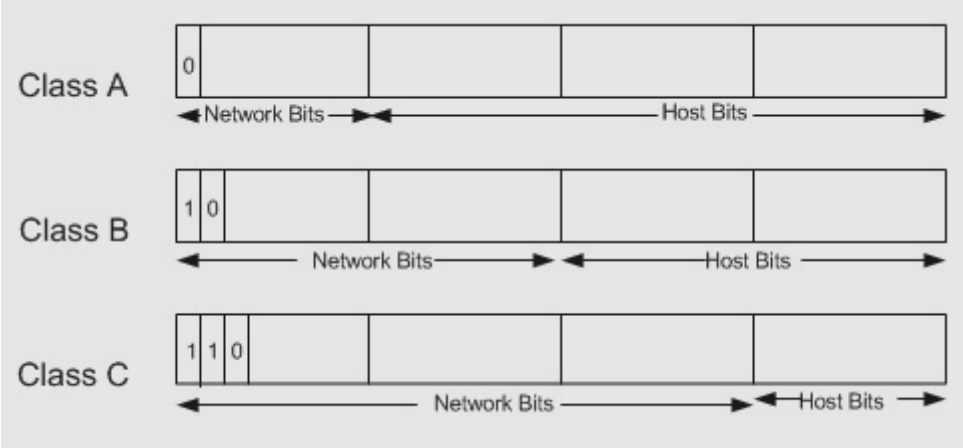


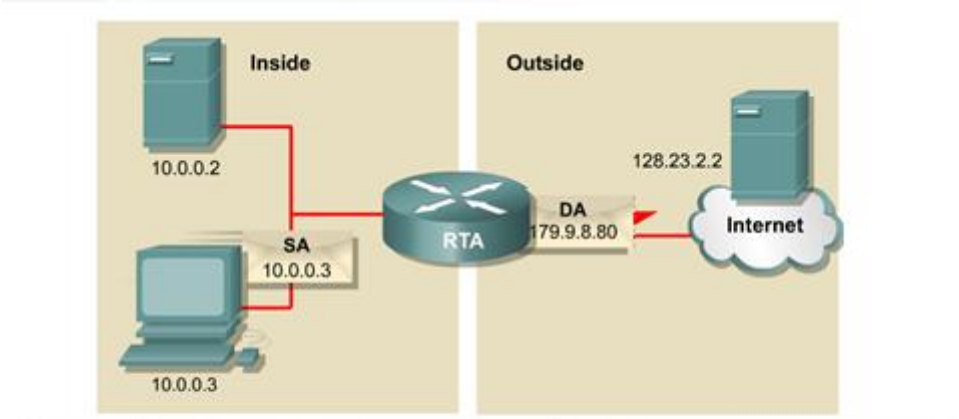
Figura 10 - Classes padrões no IPv4
Fonte – Cisco (2005)

Conforme ilustrado na Figura 10, endereços que começam com 0 são representados na classe A (1 a 127) e são reservados 8 bits para o primeiro octeto (rede) e 24 bits para o restante (hosts); endereços iniciados em 10 são representados na classe B (128 a 191), sendo reservados 16 bits para os dois primeiros octetos (rede) e 16 bits para o restante (hosts); e os endereços começados em 110 são representados na classe C (192 a 223) sendo reservados 24 bits para os três primeiros octetos (rede) e 8 bits para o restante (hosts). (BRITO, 2013).

3.4.4 NAT (Network Address Translation)

A técnica NAT (*Network Address Translation*) foi desenvolvida no intuito de um único endereço IP, ou um pequeno número deles, permita que diversos hosts, de uma rede local (LAN), possam trafegar na Internet (MOREIRAS, 2012).

Segundo BRITO (2013), o NAT foi criado em 1999 e publicado na RFC 2663, sendo o maior responsável pela sobrevida de 25 anos do IPv4. Uma deficiência dessa técnica é que o roteador preserva uma tabela agregando as conexões internas por meio das portas (*socket*). Os números que representam as portas têm 16 bits, permitindo que cada endereço público consiga atender cerca de 65.000 conexões ao mesmo tempo. Apesar do grande número de conexões, pode não ser satisfatório para grandes redes, porque existem aplicações que consomem um grande intervalo de portas.



Class	RFC 1918 Internal Address Range	CIDR Prefix
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

Figura 11 - Protocolo NAT
Fonte – Adaptado de Cisco

Como exemplo, pode-se observar a Figura 11, que ilustra o funcionamento do protocolo NAT, onde possui uma rede interna conforme RFC 1918, através dos IP's (classes A), realizando desta forma a troca de IP (NAT) no roteador para a rede externa.

4 CARACTERIZAÇÃO DA ÁREA DE ESTUDO

Tendo como base o provedor de Internet da empresa KDM Informática, operando em IPv4 e utilizando o protocolo de roteamento OSPF, usado para rotas de rede interna, fazendo a comunicação entre os roteadores e o protocolo BGP para rede externa fazendo a comunicação entre o provedor e a operadora Copel que fornece o bloco de ip's ASN (*Autonomy System Number*).

Esta empresa esta localizada no município de Santa Helena – Pr que tem uma altitude de 258m e na área da cidade não apresenta uma quantidade significativa de relevos, tornando a topologia favorável na utilização via radio, pois o sinal não encontra obstáculos significativos que interferem em sua propagação. Na figura 12 é apresentada a ilustração das torres (A, B, C, D) e da área de cobertura dos clientes da empresa que utilizam os serviços de Internet no município de Santa Helena-Pr.

Figura 12 – Localização das Torres
Fonte - Adaptado de Google Earth (2015)

As torres foram demarcadas em A (altitude de 283m) que faz cobertura de aproximadamente 20% da cidade, B (altitude de 246m) que atende cerca de 40% da cidade, C (altitude de 242m) cobrindo cerca de 25% da cidade e D (altitude de 239m) que faz cobertura em torne de 15% da cidade, sendo a distância entre a A e B de aproximadamente 1.720 metros, da torre B para a C a distancia é cerca de 1.000 metros e da C até a D fica em torno de

1.130 metros. A ligação entre as quatro torres são realizadas por fibra óptica, possibilitando assim uma finita largura de banda para próximas atualizações visto a necessidade crescente por largura de banda.

5 MATERIAL E METODOS

Primeiramente visando aplicar o novo protocolo de redes IPv6, sobre uma rede de um provedor de Internet já existente com o protocolo atual IPv4, será necessário a realização de estudos e comparativos dos mesmos. Haverá a necessidade da utilização de algumas ferramentas e técnicas já existentes nesta rede, visando a compatibilidade dos *hardwares* e *softwares* para assim conseguir implantar o novo protocolo IPv6.

5.1 MATERIAL

- Bloco v6;
- Roteador RB 1100AH;
- Switch 3COM 24 Portas;
- Antena Setorial;
- Torres.

5.2 METODOS

Atualmente existem duas formas de solicitação dos blocos v6, através da LACNIC ou RNP:

Para solicitar um bloco de endereços IPv6 através da LACNIC, a empresa solicitante deve preencher um formulário e envia-lo para hostmaster@lacnic.net. Depois de solicitado, um "ticket" é gerado, identificando a solicitação. Após a solicitação aprovada, um e-mail é enviado para a empresa solicitante com informações sobre o pagamento da alocação inicial e também sobre o Acordo de Serviço de Registro, que é assinado. A alocação somente efetua-se após recebido o pagamento e o acordo assinado.

De acordo com o site da RNP (2015), o registro de blocos IP para as instituições usuárias qualificadas pelo seu Comitê Gestor do Programa Interministerial (PI-RNP), a solicitação de alocação de blocos IP é realizada através de um formulário disponível na extranet da RNP, na última etapa do processo de qualificação das instituições usuárias. As solicitações de blocos IPv6 devem ser enviadas pelos contatos técnicos das instituições usuárias para o e-mail registro@rnp.br, incluindo a descrição detalhada das necessidades e justificativas para o pedido.

Segundo MOREIRAS (2013), os métodos propostos pela RFC 3531 para ordenar e distribuir endereços e blocos IPv6 seria por alocação de um bloco adicional para quem já tenha recebido um, sendo que este pode anunciá-lo de maneira agregada no roteamento, ou então, pode possivelmente alterar a quantidade de blocos previstos para um determinado uso, sem modificar as alocações já efetuadas.

5.3 TOPOLOGIA

A Figura 13 representa a topologia física do provedor KDM Informática da seguinte forma:

A comunicação entre as torres ocorre via fibra óptica, nestas estão os roteadores que recebem o sinal óptico e os convertem em um sinal de rádio frequência distribuindo para os clientes, através dos painéis setoriais. Em cada torre existem quatro Painéis Setoriais, onde cada um desses atende a uma abrangência de 90º, sendo assim, os quatro juntos conseguem alcançar 360º, atendendo uma boa porção do espaço em seu entorno.

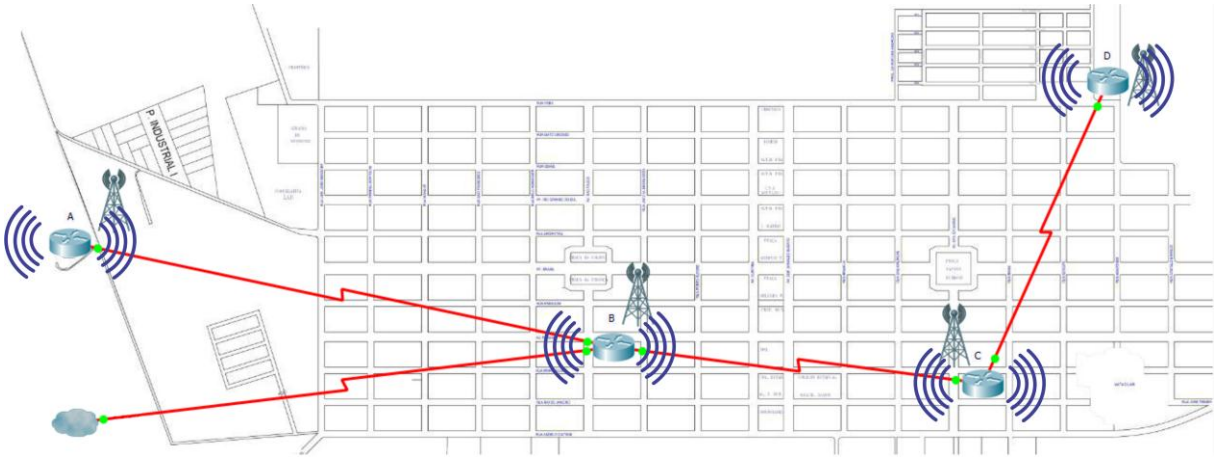


Figura 13 - Topologia do Provedor KDM Informática
Fonte – Adaptado de MS VISIO

Através destas quatro torres é possível fazer a cobertura da área urbana do município em 100% e uma cobertura de 20% aproximadamente da área rural e como mencionado acima, o município de Santa Helena fica em uma região com algumas planícies facilitando desta forma a propagação do sinal. A figura a seguir mostra a topologia do provedor KDM Informática.

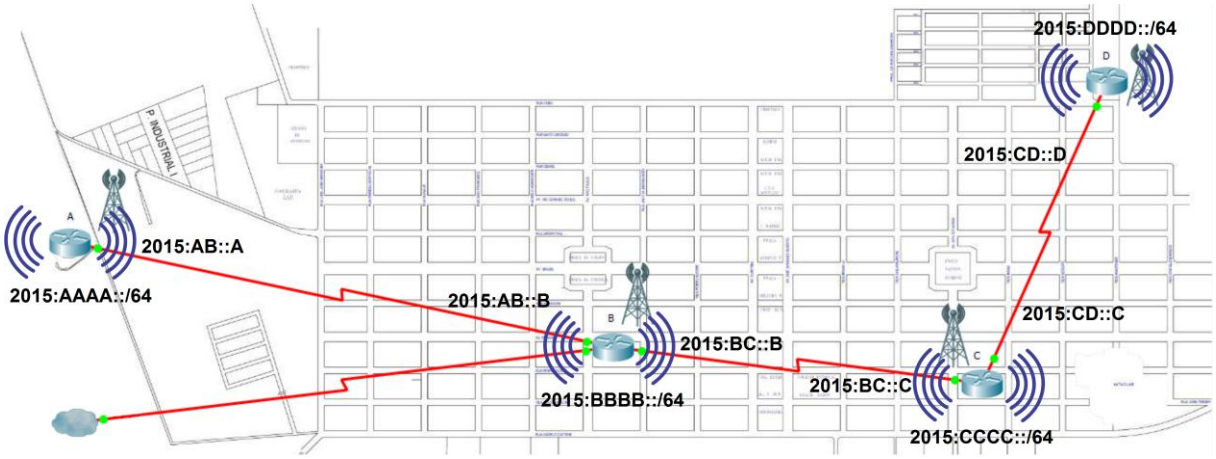


Figura 14 - Topologia lógica do Provedor
Fonte – Adaptado de MS VISIO

A Figura 14 apresenta a visão do todo da topologia lógica utilizada pelo provedor. Observa-se nas redes LAN, as que encaminham os endereços IP´s aos clientes a utilização dos blocos fictício 2015:AAAA::A onde a sequencia das letras A, foi a estratégia aplicada naquela região, isso só é possível devido ao IPv6 aceitar os valores Hexadecimais. Desta forma, como as torres foram identificadas conforme Figura 12 por letras, aproveitamos e marcamos as redes LAN pela mesma letra que identifica a torre. Conforme a Tabela 6 abaixo.

Tabela 6 - Configuração dos endereços LAN através dos blocos v6

ROTEADORES	CONFIGURAÇÃO
LAN ROUTER A	2015:AAAA::/64
LAN ROUTER B	2015:BBBB::/64
LAN ROUTER C	2015:CCCC::/64
LAN ROUTER D	2015:DDDD::/64

Fonte – Autoria própria

Através da Figura 14 é possível observar a sumarização dos blocos aplicados entre as ligações das torres configuradas nas interfaces seriais. Também aproveitamos da facilidade dos valores em hexadecimal para no IP identificar a qual parte da topologia o mesmo será implementado. Desta forma observa-se a facilidade onde entre os roteadores A e B, o bloco de ipv6 aplicado foi 2015:AB::/127. A Tabela 7 na sequencia resume a sumarização aplicada entre os roteadores.

Tabela 7 - Configuração dos endereços WAN através dos blocos v6

Configuração dos endereços WAN utilizados na comunicação entre as torres	
WAN ROUTER A e B	2015:AB::/127
WAN ROUTER B e C	2015:BC::/127
WAN ROUTER C e D	2015:CD::/127

Fonte – Autoria própria

A figura 15 exibe parte da configuração detalhada aplicada no roteador A (R-A) e roteador B (R-B), observa-se o roteador A utilizando o IPv6 na interface serial configurada com o seguinte bloco 2015:AB::A/127. Já a interface que alimenta a torre para os painéis setoriais é uma fast-ethernet, a qual distribui um IPv6 via DHCP. Nesta interface esta atribuído como *gateway* tendo como IPv6 2015:AAAA::1/64.

No roteador B pode-se ver o IPv6 configurado na interface serial A conectada ao B com o seguinte bloco 2015:AB::B/127, sendo a interface fast-ethernet com o endereço de IPv6 2015:BBBB::1/64 responsável pela distribuição aos clientes. Observa-se para ambas a ativação do V6 através do comando *enable*, bem como a divulgação do protocolo de roteamento OSPF com ID 2015 estando todos na área de *backbone* (Espinha Dorsal da Internet).

As residências que forem atendidas por estas torres (A e B), receberão um IP respectivamente dos blocos 2015:AAAA::1/64 e 2015:BBBB::1/64.

R-A

```
interface FastEthernet0/0
 duplex auto
 speed auto
 ipv6 address 2015:AAAA::1/64
 ipv6 enable
 ipv6 ospf 2015 area 0
!
interface Serial0/0/0
 encapsulation ppp
 ipv6 address 2015:AB::A/127
 ipv6 enable
 ipv6 ospf 2015 area 0
!
ipv6 router ospf 2015
 router-id 10.1.1.1
 log-adjacency-changes
!
ipv6 route ::/0 Serial0/0/0
```

R-B

```
interface FastEthernet0/0
 duplex auto
 speed auto
 ipv6 address 2015:BBBB::1/64
 ipv6 enable
 ipv6 ospf 2015 area 0
!
interface Serial0/0/0
 encapsulation ppp
 ipv6 address 2015:AB::B/127
 ipv6 enable
 ipv6 ospf 2015 area 0
 clock rate 1000000
!
interface Serial0/0/1
 encapsulation ppp
 ipv6 address 2015:BC::B/127
 ipv6 enable
 ipv6 ospf 2015 area 1
 clock rate 1000000
!
interface Serial0/1/0
 ipv6 address 2801:82:C00A::B/48
 ipv6 enable
 ipv6 ospf 2015 area 0
 clock rate 2000000
!
ipv6 router ospf 2015
 router-id 10.1.1.2
 log-adjacency-changes
!
ipv6 route ::/0 Serial0/1/0
```

Figura 15 - Configuração dos Roteadores A e B
Fonte – Adaptado de GNS

Na Figura 16 exibe parte da configuração do Roteador B (R-B) entre o roteador C (R-C). Pode-se ver o IPv6 configurado no roteador B, na interface serial com o IPv6 2015:BC::B/127, que esta fazendo ligação ao roteador C através do IPv6 2015:BC::C/127 pertencente a interface serial.

No roteador C, a interface fast-ethernet com o endereço IPv6 2015:BBBB::1/64 é responsável pela distribuição de endereços aos clientes, o qual esta ativo o OSPF com ID 2015.

R-B

```
interface FastEthernet0/0
 duplex auto
 speed auto
 ipv6 address 2015:BBBB::1/64
 ipv6 enable
 ipv6 ospf 2015 area 0
!
interface Serial0/0/0
 encapsulation ppp
 ipv6 address 2015:AB::B/127
 ipv6 enable
 ipv6 ospf 2015 area 0
 clock rate 1000000
!
interface Serial0/0/1
 encapsulation ppp
 ipv6 address 2015:BC::B/127
 ipv6 enable
 ipv6 ospf 2015 area 1
 clock rate 1000000
!
interface Serial0/1/0
 ipv6 address 2801:82:C00A::B/48
 ipv6 enable
 ipv6 ospf 2015 area 0
 clock rate 2000000
!
ipv6 router ospf 2015
 router-id 10.1.1.2
 log-adjacency-changes
!
ipv6 route ::/0 Serial0/1/0
```

R-C

```
interface FastEthernet0/0
 duplex auto
 speed auto
 ipv6 address 2015:CCCC::1/64
 ipv6 enable
 ipv6 ospf 2015 area 1
!
interface Serial0/0/0
 encapsulation ppp
 ipv6 address 2015:BC::C/127
 ipv6 enable
 ipv6 ospf 2015 area 1
!
interface Serial0/0/1
 encapsulation ppp
 ipv6 address 2015:CD::C/127
 ipv6 enable
 ipv6 ospf 2015 area 1
 clock rate 1000000
!
ipv6 router ospf 2015
 router-id 10.1.1.3
 log-adjacency-changes
```

Figura 16 - Configuração dos Roteadores B e C
Fonte – Adaptado de GNS

A Figura 17 apresenta parte da configuração entre o roteador C (R-C) e roteador D (R-D), observa-se o roteador C com o IPv6 na interface serial configurada com o seguinte bloco 2015:CD::C/127, que esta fazendo ligação com o roteador D através da interface serial configurada com o bloco IPv6 2015:CD::D/127.

No roteador D, a interface responsável pela distribuição de endereços aos clientes é a fast-ethernet com o bloco de endereço IPv6 2015:BBBB::1/64, o qual esta ativo o OSPF com ID 2015.

R-C

```
interface FastEthernet0/0
 duplex auto
 speed auto
 ipv6 address 2015:CCCC::1/64
 ipv6 enable
 ipv6 ospf 2015 area 1
!
interface Serial0/0/0
 encapsulation ppp
 ipv6 address 2015:BC::C/127
 ipv6 enable
 ipv6 ospf 2015 area 1
!
interface Serial0/0/1
 encapsulation ppp
 ipv6 address 2015:CD::C/127
 ipv6 enable
 ipv6 ospf 2015 area 1
 clock rate 1000000
!
ipv6 router ospf 2015
 router-id 10.1.1.3
 log-adjacency-changes
```

R-D

```
interface FastEthernet0/0
 duplex auto
 speed auto
 ipv6 address 2015:DDDD::1/64
 ipv6 enable
 ipv6 ospf 2015 area 1
!
interface Serial0/0/0
 encapsulation ppp
 ipv6 address 2015:CD::D/127
 ipv6 enable
 ipv6 ospf 2015 area 1
!
ipv6 router ospf 2015
 router-id 10.1.1.4
 log-adjacency-changes
!
ipv6 route ::/0 Serial0/0/0
```

Figura 17 - Configuração dos Roteadores C e D
Fonte – Adaptado de GNS

A figura na sequencia exibe o esquema de configuração realizado em todos os roteadores para fornecer o endereço IPv6 aos clientes, para tal, foi escolhido a configuração DHCPv6 *statefull*.

```
ipv6 unicast-routing
ipv6 cef
 ipv6 dhcp pool RA
 address prefix 2015:AAAA::/64 lifetime infinite infinite
 dns-server AAAA:BBBB:10FE:100::15
 dns-server 2015:BBBB::1
 domain-name KDM.com
!
interface F0/0
 duplex auto
 speed auto
 ipv6 address 2015:AAAA::1/64
 ipv6 dhcp server RA rapid-commit
!
end
```

Figura 18 - Configuração DHCPv6
Fonte – Adaptado de GNS

Quando um novo cliente conectar-se a rede, o servidor DHCPv6 irá identifica-lo e configurará automaticamente sua máquina, evitando o esforço do administrador da rede ter que configurar manualmente as máquinas dos clientes, assim, poupando tempo e incrementando a mobilidade da rede.

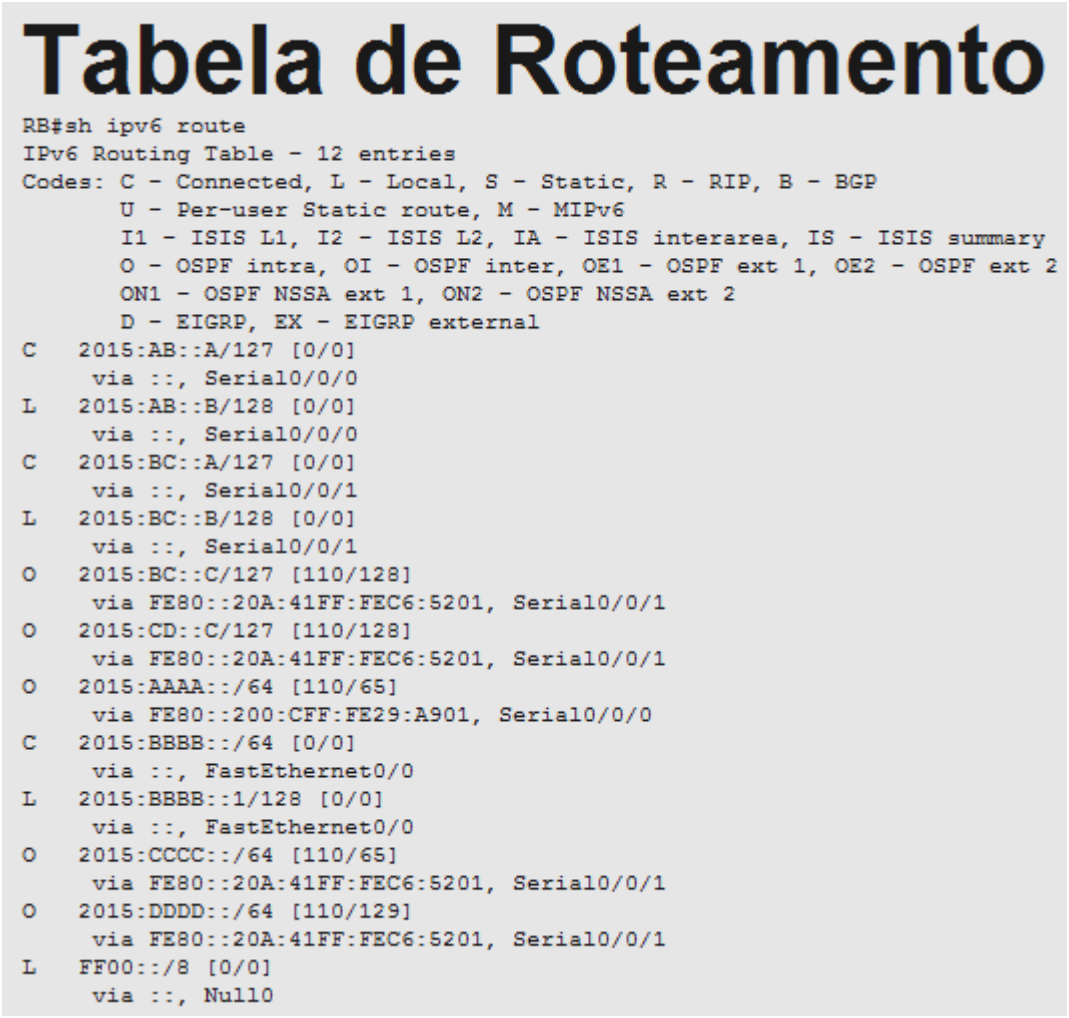


Figura 19 - Tabela de roteamento entre os roteadores que ligam as torres
Fonte – Adaptado de GNS

Na Figura 19 esta exibindo a configuração do roteador B, pode-se observar também a tabela de roteamento entre os roteadores que ligam as torres. Observe que a letra "O" no início da linha apresenta a rota aprendida, que são as redes locais nas torres, como a 2015:AAAA::/64 e as demais rotas, além do link WAN entre os roteadores C e D. A convergência da rede foi total entre os roteadores.

Para realizar um teste de conectividade, utilizamos o comando "*Ping*", que pertence ao protocolo ICMP, pode-se comprovar a comunicação entre os roteadores (A, B, C e D) e saber o tempo de resposta que um roteador terá para comunicar-se com outro.

Na Figura 20 pode-se observar o resultado do "*Ping"* executado no roteador A (2015:AAAA::1), testando a conectividade com o roteador D (2015:DDDD::1), assim, passando sobre toda a rede (roteadores A, B, C e D), sendo o resultado 100% de conectividade e o tempo de resposta de 1 milissegundo.

```
RA#ping 2015:dddd::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2015:dddd::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Figura 20 - Comando *Ping* mostrando a comunicação entre os roteadores
Fonte – Adaptado de GNS

6 CONCLUSÕES

Com a utilização do protocolo de redes IPv6, tem-se muitas melhorias significativas em relação ao protocolo IPv4, oferecendo maior segurança através da autenticação e privacidade, seu cabeçalho de protocolo é mais simplificado, diminuindo o tempo de processamento na análise dos cabeçalhos, por parte de roteadores.

As estações se auto configuram através do *stateless* (número IP, nome do servidor e etc.) ao serem ligados na rede, através do protocolo DHCPv6, o que incrementa a mobilidade, pois utilizamos os blocos de IPv6 com base no número alocado a torre, assim, para resolver um chamado técnico, observado o IPv6 atribuído ao cliente, é possível identificar qual torre forneceu o acesso. Também sua utilização nos roteadores facilitou muito o trabalho realizado nas residências uma vez que a disponibilidade de IP's deixa de ser um problema.

Contudo, é necessário um plano de migração inteligente e planejado, dando aos usuários a liberdade para testar, mover e migrar sua infraestrutura atual em um ritmo controlado e gerenciável. Conclui-se também que os tempos de respostas entre as LAN's são muito baixos, equivalente a 1 milissegundo, isto ocorre devido a utilização da fibra óptica, desta forma a largura de banda não é comprometida.

A opção do protocolo de roteamento OSPF, possibilitou uma rápida configuração, devido a estarem todos a área 0, área do *backbone*, as redes convergiram rapidamente aprendendo todas as rotas. Assim como para o IPv4 no v6, o OSPF atendeu seu proposito.

A evolução tecnológica não deve ser ignorada, pois devemos alcançar os objetivos para a qual ela serve, de forma que o homem entenda o seu funcionamento e utilize-a para facilitar o que antes continha menos recursos ou vantagens, que a utilize para "crescer" e não se "suicidar" criando armas de guerra.

6.1 TRABALHOS FUTUROS/CONTINUAÇÃO DO TRABALHO

Dado a complementação desta etapa, sugere-se sua continuação através de uma comparação de desempenho entre o IPv4 e IPv6 sobre esta estrutura apresentada.

REFERÊNCIAS BIBLIOGRÁFICAS

AMARAL, Allan Francisco Forzza. **Redes de computadores**. 1ª ed. Instituto Federal do Espírito Santo – IFES, 2012.

BRITO, Samuel Henrique Bucke. **IPv6: O Novo Protocolo da Internet.** 1ª ed. Novatec, 2013.

BRITO, Samuel Henrique Bucke. **Servidores DHCPv6 em Redes IPv6**, 2013. Disponível em: <http://labcisco.blogspot.com.br/2013/05/servidores-dhcpv6-em-redes-ipv6.html>. Acesso em: 05 mai. 2015.

CAMPOS, André Luiz Gonçalves. **Fibras ópticas - uma realidade reconhecida e aprovada**, 2002. Disponível em: < https://memoria.rnp.br/newsgen/0203/fibras_opticas.html>. Acesso em: 17 mai. 2015.

CISCO. **TCP/IP Overview,** 2005. Disponível em: <http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13769-5.html>. Acesso em: 07 abr. 2015.

COMER, Douglas E. **Interligação de redes com TCP/IP – Princípios, Protocolos e Arquitetura**. 6ª ed. Campus, 2014.

CRISPIM, José. **Artigos - Redes de Comunicação de Dados**, 2013. Disponível em: <http://www.jose-crispim.pt/artigos/redes/redes_art/03_teoria.html>. Acesso em: 04 dez. 2014.

FALSARELLA, Douglas. **O Futuro do IPv6 e o fim do IPv4**, 2010. Disponível em: <http://imasters.com.br/artigo/18471/redes-e-servidores/o-futuro-do-ipv6-e-o-fim-do-ipv4/>. Acesso em: 17 mar. 2014.

FERREIRA, Cleiton. **Fibras Ópticas**, 2013. Disponível em: < http://www.projetoderedes.com.br/artigos/artigo_fibras_opticas.php>. Acesso em: 17 mai. 2015.

FLORENTINO, Adilson Aparecido. **IPv6 na Prática**. 1ªed. Linux New Media, 2012.

GRIPA, Marcelo. **Brasil supera Rússia e se torna 5º país com mais usuários de internet**, 2014. Disponível em: <http://olhardigital.uol.com.br/noticia/40022/40022>. Acesso em: 17 mar. 2014.

HAGEN, Silvia. **IPv6 Essentials**. Editora O'Reilly Media, 2ª ed. 2006.

IANA. **Number Resources**. Disponível em: < https://www.iana.org/numbers>. Acesso em 14 abr. 2015.

JAMHOUR, Edgard. **IPv6: Internet Protocol – Versão 6 e Mecanismos de Transição**. 2008. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/Pessoal/Mestrado/TARC/IPv6Trans.pdf>. Acesso em: 19 abr. 2015.

LACNIC. **Acerca do LACNIC**. Disponível em: <http://www.lacnic.net/pt/web/lacnic/acerca-lacnic>. Acesso em: 16 abr. 2015.

MACEDO, Diego. **Arquitetura e Protocolos TCP/IP**, 2012. Disponível em: <http://www.diegomacedo.com.br/arquitetura-e-protocolos-tcp-ip/>. Acesso em: 03 dez. 2014.

MORAIS, Carlos Tadeu Queiros de; LIMA, José Valdeni de; FRANCO, Sergio Roberto K. **Conceitos sobre Internet e Web.** 1ª ed. UFRGS, 2012.

MOREIRAS, Antonio M. **Veja na pratica como distribuir suas subredes IPv6, pela RFC 3531**, 2013. Disponível em: <http://ipv6.br/veja-na-pratica-como-distribuir-suas-subredes-ipv6-pela-rfc-3531/>. Acesso em: 23 abr. 2015.

OLIVEIRA, Ivo Rodrigues de. **Implantação de Compartilhamento de Internet em Condomínios Residenciais**. 2013. 32 f. Monografia (Especialização em software livre aplicado a Telemática) - Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná, Curitiba, 2013. Disponível em: < http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1843/1/CT_CESOL_I_2013_06.pdf>. Acesso em: 30 nov. 2014.

PEREIRA, Ana Paula. **O que é DHCP?**. 2009. Disponível em: <http://www.tecmundo.com.br/2079-o-que-e-dhcp-.htm>. Acesso em: 13 abr. 2015

PINHEIRO, José Mauricio Sanos. **OSI: Um Modelo de Referência**. 2008. Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_osi_um_modelo_de_referencia.php>. Acesso em: 13 out. 2014.

PINTO, Clécio Oliveira. **IPv6,** 2013. Disponível em: <http://cleciooliveira.com/academicos/Artigo_IPV6.pdf>. Acesso em: 17 mar. 2014.

RNP. **Nossa História**, 1997. Disponível em: < http://www.rnp.br/institucional/nossa-historia>. Acesso em: 14 abr. 2015.

TANENBAUM, Andrew S. **Computer Networks**. Editora Campus, 4ª ed. 2002.

TELECO. **Sessão: Banda larga,** 2015. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialredeipmig1/pagina_2.asp>. Acesso em: 22 mai. 2015.

TORRES, Gabriel. **Redes de Computadores – Curso Completo**. Editora Axcel Books, 1ª ed. 2001.

TORRES, Gabriel. **Como o Protocolo TCP/IP Funciona**. 2007. Disponível em: <http://www.clubedohardware.com.br/artigos/Como-o-Protocolo-TCP-IP-Funciona-Parte-1/1351/1>. Acesso em: 02 Dez. 2014.