

LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
ESPECIALIZAÇÃO EM REDES DE COMPUTADORES

MORONI NERES VIEIRA

ESTUDO DE IMPLANTAÇÃO DO PROTOCOLO IPv6

NATAL/RN
2013

MORONI NERES VIEIRA

ESTUDO DE IMPLANTAÇÃO DO PROTOCOLO IPv6

Trabalho de conclusão de curso apresentada ao Centro Universitário do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Orientador: Prof. Ms. Aluizio Ferreira da Rocha Neto.

NATAL/RN
2013

MORONI NERES VIEIRA

ESTUDO DE IMPLANTAÇÃO DO PROTOCOLO IPv6

Trabalho de conclusão de curso apresentada ao Centro Universitário do Rio Grande do Norte como requisito parcial para a obtenção do título de Especialista em Redes de Computadores.

Aprovado em: ____ / ____ / ____

BANCA EXAMINADORA

Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador

Membro examinador

Membro examinador

RESUMO

O presente trabalho aborda a implantação do novo protocolo de endereçamento da Internet, o IPv6, em uma rede de computadores. Para isso, foram realizadas algumas análises e testes de configurações em diversos equipamentos que fazem parte da infra-estrutura de uma rede, assim como dos equipamentos finais dos usuários. Foram apresentados alguns conceitos relativos ao cabeçalho da versão 4 do protocolo IP fazendo um comparativo com o cabeçalho da versão 6 do mesmo protocolo. O IPv6 foi desenvolvido para ser um substituto do protocolo IPv4, as mudanças no cabeçalho são bastantes significativas, além de diminuir o tamanho total do cabeçalho, houve mudanças na performance, já que a fragmentação que antes era realizada em cada nó da rede e agora é feita somente na origem e destino. A implantação do protocolo na rede foi feita com a técnica de pilha dupla através de um túnel virtual até um servidor *broker* onde é disponibilizado um endereço IPv6 do tipo global que permite o acesso a outras redes, inclusive permitindo o acesso aos serviços web.

Palavras-chave: Redes de Computadores. IPv4. IPv6.

ABSTRACT

The current work deals with the implementation of a new Internet addressing protocol; the IPv6, in a Computer network. That's why, it was made some analysis and configuration tests in diverse equipments that take part of a network infra-structure, as well as the user's final equipments. It was presented some concepts related to the version 4 header of the IP protocol making a comparison with the version 6 header of the same protocol. The IPv6 was developed to be a substitute of the IPv4 protocol, the changes in the header are quite significant, besides decreasing the total header's length, there were changes in performance, since the fragmentation that was made in each network node and now it's made only in the origin and destiny. The implementation of the protocol in the network was made using the dual stack technique through a virtual tunnel until the *broker* server where is available a kind of global IPv6 which allows access to other networks, also allowing the access to web services.

Keywords: Computer network. IPv4. IPv6.

LISTA DE FIGURAS

Figura 1: Cabeçalho de um datagrama IPv4.....	11
Figura 2: Classes de endereços IPv4.	13
Figura 3: Gráfico de esgotamento dos endereços IPv4.	15
Figura 4: Alocação de endereços no IANA.....	19
Figura 5: Cabeçalho de um datagrama IPv6.....	20
Figura 6: Cabeçalhos de extensão do IPv6.....	22
Figura 7: Esquema de pilha dupla (IPv4 e IPv6).....	27
Figura 8: Estabelecimento de um túnel IPv6.....	28
Figura 9: Roteamento em uma rede IPv6.	29
Figura 10: Rede Local IPv4.....	30
Figura 11: Formulário de cadastro no SIXXS.....	31
Figura 12: Faixa de endereços adquirida para o Túnel.....	32
Figura 13: Configuração do software aiccu.....	33
Figura 14: Teste de conectividade IPv6.	34
Figura 15: Propriedades de rede no Windows XP.....	34
Figura 16: Rede local com endereços IPv6.	35
Figura 17: Arquivo de configuração radvd.conf.	36

SUMÁRIO

1	INTRODUÇÃO	7
1.1	OBJETIVOS	7
1.1.1	Objetivos Específicos.....	8
1.2	MOTIVAÇÃO	8
2	REFERENCIAL TEÓRICO	9
2.1	PROTOCOLO IPV4	9
2.1.1	Cabeçalho IPv4.....	11
2.1.2	Organização do endereçamento IPv4	12
2.1.3	Fragmentação no IPv4	14
2.1.4	Protocolo ICMP	14
2.1.5	Esgotamento dos Endereços IPv4	15
2.1.6	Soluções paliativas para o esgotamento de endereços	16
	2.1.6.1 CIDR (Classless InterDomain Routing).....	16
	2.1.6.2 DHCP (Dynamic Host Configuration Protocol)	17
	2.1.6.3 NAT (Network Address Translation)	17
2.2	PROTOCOLO IPV6	19
2.2.1	Cabeçalho IPv6.....	20
2.2.2	Cabeçalhos de Extensão	21
2.2.3	Endereçamento IPv6	22
2.2.4	ICMPv6.....	25
2.2.5	Planejamento e Implantação	26
2.2.6	Transição	26
2.2.7	Roteamento do IPv6	29
3	ESTUDO DE CASO	30
3.1	TOPOLOGIA DO AMBIENTE	30
3.2	AQUISIÇÃO DO TÚNEL IPV6	31
3.3	HABILITANDO IPV6 NOS SISTEMAS OPERACIONAIS	33
3.4	PARÂMETROS DA REDE IPV6	35
3.5	DISTRIBUINDO ENDEREÇOS IPV6 ATRAVÉS DO RADVD	36
4	CONCLUSÃO	37
	REFERÊNCIAS.....	38

1 INTRODUÇÃO

No momento em que se desenvolvia a pesquisa para criação e adoção de um protocolo responsável pelo endereçamento lógico dos hosts pertencentes a então recém criada *Advanced Research Projects Agency Network* (ARPANET), talvez não se tenha pensando no seu esgotamento. A Internet, em seus primórdios, fora criada com a finalidade de interligação de uma rede de pesquisa entre organizações militares e algumas poucas faculdades dentro do território dos EUA.

Quando essa rede saiu dos centros de pesquisas militares e universidades, ela ganhou instituições de pesquisas espalhados pelo mundo, incluindo universidades, escolas de ensino secundário, lares, empresas, setores públicos e afins.

Em meados do ano de 1993, quando a Internet ficou popular através dos *modems* domésticos, ficou claro que seu crescimento seria imediato e rápido e que os endereços lógicos logo ficariam escassos. Como consequência acabaria tão rápido quanto a Internet pudesse crescer e tomar as proporções que conhecemos hoje.

Ficou claro que o esgotamento de endereços lógicos disponíveis seria iminente e que uma linha de pesquisa seria necessária com o intuito de buscar uma solução para o problema. Em meados de 1993 foi criada a *Request For Comment* (RFC) 1550, a qual formalizou a pesquisa a respeito da nova versão do novo protocolo de endereçamento.

Nesse meio tempo muitas soluções paliativas foram concebidas, mas nenhuma foi suficiente para otimização do protocolo de endereçamento.

As universidades, empresas e centros de pesquisas têm necessidade de crescimento e de demandas cada vez maiores de serviços e recursos computacionais e para que a instituição possa continuar crescendo foi necessário fazer um estudo para adequação ao novo protocolo *Internet Protocol* (IP) em sua versão 6, denominado IPv6.

1.1 OBJETIVOS

O objetivo principal deste trabalho é realizar a implantação do novo protocolo de endereçamento IPv6 em uma rede, de forma transitória, utilizando a técnica de túnel para que esta rede possa trafegar em pilha dupla (IPv4 e IPv6) e acessar os serviços já disponíveis na Internet nestes dois protocolos.

1.1.1 Objetivos Específicos

Para atingir o objetivo geral deste trabalho, as seguintes etapas foram seguidas:

- Foi feito o um histórico do surgimento da Internet e do IPv4 para contextualizar o estudo de caso apresentado, o problema do esgotamento dos endereços, as soluções paliativas que surgiram para retardar o esgotamento dos endereços;
- Análise do protocolo IPv6 como uma solução definitiva para o esgotamento dos endereços IPv4, as mudanças no cabeçalho, o tamanho do campo de endereçamento, e o tamanho total do cabeçalho só aumentou em duas vezes, houve uma melhora de performance considerável em virtude da fragmentação só ser realizada agora no nó inicial e final da transmissão dos pacotes.
- Foi realizado um estudo comparativo entre o protocolo IPv4 e IPv6, a mudança que ocorreu nos campos do cabeçalho, os cabeçalhos de extensão e a performance em virtude da mudança da fragmentação;
- Análise de uma solução que permita a convivência entre os dois protocolos em uma rede física, utilizando a técnica de pilha dupla através de tunelamento até um servidor broker;

1.2 MOTIVAÇÃO

Este trabalho teve como principal motivação o presente esgotamento dos endereços IPv4 disponíveis na Internet e a necessidade de adequação das redes para o novo protocolo de endereçamento IPv6, de uma forma transitória, permitindo a coexistência e compatibilidade entre os dois protocolos de forma transparente para os usuários.

2 REFERENCIAL TEÓRICO

Este capítulo descreve de forma resumida as principais teorias e conceitos abordados neste trabalho, começando pelo histórico de criação do protótipo do protocolo TCP/IP, descreve também o protocolo a *Protocol Data Unit* (PDU) – do protocolo IP versão 4, suas características e seu esgotamento, bem como a descrição das principais soluções paliativas para evitar o fim.

É feita uma abordagem do protocolo IP versão 6, suas principais características, seu funcionamento, bem como uma breve comparação entre os dois protocolos.

É feita uma descrição das ferramenta utilizadas no estudo de caso, o funcionamento do software de divulgação de prefixo, assim como a ferramenta de monitoramento de utilização de link.

2.1 PROTOCOLO IPV4

A primeira rede de computadores nasceu de uma pesquisa iniciada pelo *Defense Advanced Research Projects Agency* (DARPA) no final da década de 1960 e começo da década de 1970 o primeiro protótipo entrou em funcionamento em 1969, conhecido na época como processadores de mensagens de interface (*interface message processors – IMPs*), foram usados para interligar as Universidades da Califórnia em Los Angeles, o Stanford Research Institute (SRI), na universidade da Califórnia em Santa Barbara e a Universidade de Utah.

A ARPANET – rede divulgada publicamente divulgada em 1972 por Robert Kahn – no início conectava somente 15 nós e utilizava o protocolo NCP -*network-control protocol* - um protocolo não escalar para atender uma rede que originalmente começou com poucos hosts.

Em 1976, no laboratório do DARPA, um grupo de pesquisadores norte americano decidiu a quantidade de endereços suficientes para que uma rede de computadores fosse interligada, cada endereço representaria uma máquina conectada.

Após um ano de discussão o prazo para a discussão já tinha chegado ao fim, um dos líderes do projeto Vinton G. Cerf tomou uma decisão importante sobre a quantidade de endereços necessárias que então seria de 4,3 bilhões (2^32 , um número de 32 bits para o endereço IP).

562 hosts passaram a adotar o protocolo TCP/IP, com o novo protocolo o crescimento foi ordenado e eliminou-se as restrições dos protocolos anteriores.

A pesquisa desenvolvida deu início a Internet, e os endereços que foram discutidos pelos pesquisadores da DARPA são os endereços IP em sua versão atual, a 4. Um conjunto de 32 bits divididos em uma sequência de 8 bits usando notação decimal pontilhada, que vão dos valores decimais de 0 a 255 separados pelo “.” ponto.

Atualmente a arquitetura TCP/IP forma a base para que a Internet possa se comunicar e assim conectar aproximadamente 650 milhões de computadores em todo o mundo.

A versão do protocolo IP que atualmente é utilizada é a 4 ou comumente chamado de IPv4, apesar do protocolo ser robusto, fácil de implementar e ter interoperabilidade, seu projeto não teve a previsibilidade de alguns aspectos como:

- O crescimento das redes, tendo como principal característica o esgotamento dos endereços IP;
- Crescimento das tabelas de roteamento;
- Segurança das informações que trafegam na rede;
- Qualidade na saída e entrega de determinados tipos de pacotes.

O Protocolo TCP/IP nasceu de uma pesquisa iniciada pelo DARPA em meados da década de 1970 formando um conjunto de padrões e um conjunto de convenções para interconectar os hosts. Segundo COMER (2007), “A tecnologia de inter-rede revolucionou a comunicação entre os computadores. [...] Além de inter-redes privadas, a tecnologia de TCP/IP possibilitou uma Internet global que alcança escolas, organizações comerciais e sites governamentais e militares em todos os países do mundo.”

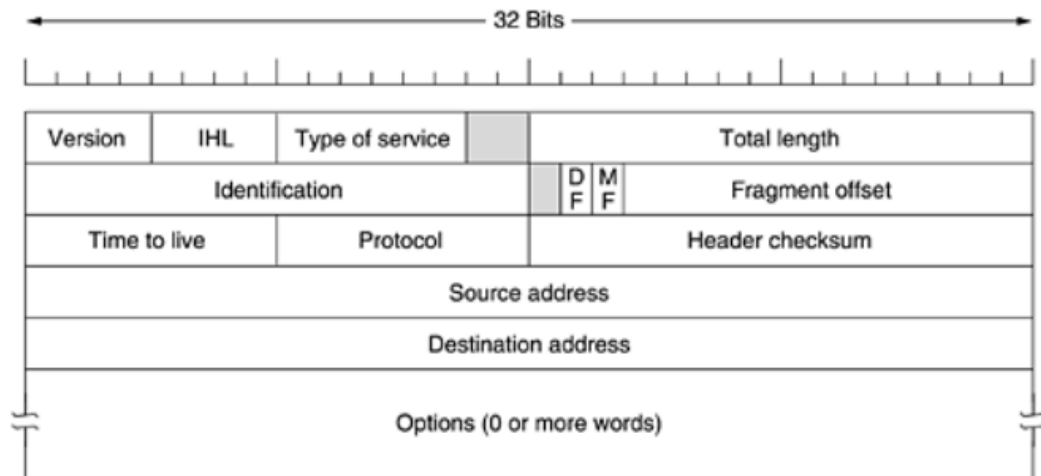
O *Transmission Control Protocol* (TCP) por sua vez é um protocolo que garante a entrega confiável dos pacotes na rede, orientado para conexão, da Internet. Segundo KUROSE (2010), o protocolo IP é o responsável pelo endereçamento e repasse dos pacotes na Internet.

Segundo (SANTOS et al., 2011) A RFC 791 diz que o protocolo IP possui duas funções básicas e são elas: a fragmentação que permite com que a informação possa ser transmitida em diferentes meios de comunicação com diferentes taxas de transmissão, sua função básica é a quebra do pacote em partes menores e o endereçamento, que permite ter um endereço único de origem e outro de destino para que a informação possa chegar ao seu destino e o mesmo possa responder as requisições da origem com o fim de estabelecimento e troca de informações.

2.1.1 Cabeçalho IPv4

O cabeçalho IPv4 é formado por 12 campos fixos, tendo ou não opções e seu tamanho varia entre 20 e 60 Bytes.

Figura 01 – Cabeçalho de um datagrama IPv4.



Fonte: Kurose (2010)

O Campo *Version* controla a versão do protocolo, pode ser IPv4 ou IPv6. O protocolo IPv5 foi um protocolo de fluxo somente experimental, nunca foi implementado.

O campo de *tamanho de cabeçalho* pode variar até porque o tamanho do cabeçalho IP sofre variações.

O campo *Type of Service* é usado para informar o tipo de serviço, pode ser usado por aplicações para ter controle na qualidade de serviço da rede, podem ser implementadas alguns tipos de confiabilidade e velocidade.

O campo *tamanho total* informa todo o tamanho em bytes do cabeçalho e dados, o tamanho máximo chega a ser de 65.536 bytes.

O campo *identification* faz a identificação do fragmento que chega ao host para saber de que datagrama fragmentado ele pertence.

Existe em seguida um campo que não é utilizado, em seguida tem dois campos de tamanho de 1 bit cada, onde o primeiro é identificado por DF, sigla em inglês que significa *Don't Fragment* (Não fragmentar), é compreendido pelos roteadores e informa ao roteador

que não fragmentem o datagrama, em uma rede de dados todas as máquinas são obrigadas a aceitar fragmentos de 576 bytes ou menos.

MF significa *More Fragment* (mais fragmentos), esse campo é configurado com o bit de valor 1 em todos os datagramas fragmentados menos no último que tem como função informar que todos os datagramas chegaram ao destino.

O campo *fragment offset* informa ao destinatário a que parte o datagrama que chegou fragmentado pertence.

O campo *Time to live* é um campo com valor decremental, a cada *hop* o valor é decrementado e esse valor varia de 255 a 0, sendo que quando chega a 0 o pacote é descartado.

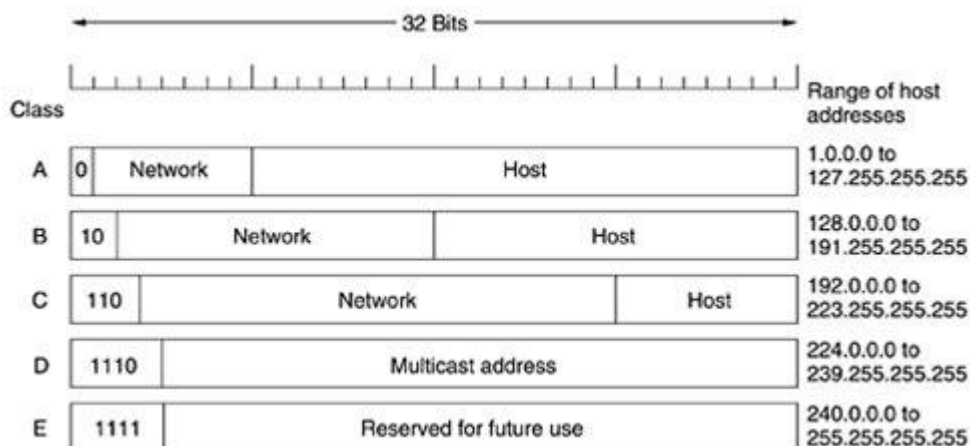
O campo *protocolo* informa qual o protocolo da camada superior, aceita as possibilidades de TCP e UDP.

O campo *checagem de cabeçalho* faz a verificação do cabeçalho e informa se contém erros durante a transmissão dos pacotes.

Os campos *endereço de origem* e *endereço de destino* informam quais os endereços IP dos hosts que enviam o pacote e qual o IP do host que deverá receber o pacote.

2.1.2 Organização do endereçamento IPv4

Conceitualmente os endereços IP são pares e divididos em prefixos, responsáveis pela identificação da rede, também chamado de *netid*, e sufixos, responsável pela identificação do host também chamado de *hostid*.

Figura 02 – Classes de endereços IPv4.

Fonte: – Tanenbaum (2007)

Na figura 2 é mostrado 5 classes de endereços, a primeira começa em 1.0.0.0 e termina em 127.255.255.255, pode-se alocar até 2^{24} (16.777.216) endereços para os hosts, a segunda começa em 128.0.0.0 e termina em 191.255.255.255, pode-se alocar 2^{16} (65.536) endereços para os hosts, a terceira começa em 192.0.0.0 e termina em 223.255.255.255, pode-se alocar 2^8 (256) endereços para o host, a classe D é reservada para aplicações que utilizam multicast, algumas aplicações multimídia fazem uso dessa faixa de endereços, a classe E foi reservada para usos futuros, inicialmente pensou-se em reservar uma faixa de endereços com o objetivo de um futuro uso.

A Internet é uma rede virtual, ela foi pensada por projetistas e implementada diretamente no software, sob essa perspectiva ela pode ser livre para que possa ter regras, parâmetros, tamanhos e formatos para que os protocolos possam ser desenvolvidos.

Os endereços IP seguindo essa perspectiva foi desenvolvido para ser dividido em 4 grupos de 8 bits separados por “.”, a essa organização de endereços dar-se o nome de notação decimal pontilhada.

Atualmente os hospedeiros e roteadores conectados a internet tem um endereço que os identificam e permitem a comunicação entre os nós das redes, sejam elas locais ou geograficamente distribuídas.

2.1.3 Fragmentação no IPv4

Para que os pacotes possam ser transmitidos na rede, eles podem passar por enlaces que divergem capacidade de largura de banda ou poderá ocorrer de encontrar enlaces congestionados.

Quadros ethernet só podem ter no máximo 1500 bytes de dados, e alguns quando usados em longas distâncias só podem ter no máximo 576 bytes, quem define qual o tamanho máximo que pode conter um quadro é a *Maximum Transmission Unit* (MTU).

O datagrama ao trafegar entre roteadores precisa conhecer a MTU deles para que possa ser calculado o tamanho do datagrama que poderá passar pelo meio físico, quando um datagrama é enviado ele passa por diversos roteadores que podem compartilhar protocolo de enlaces diferentes com diferentes MTUs, o datagrama IP é então quebrado em pedaços menores para que possa ser transferido entre os roteadores.

Essa porção menor é chamada de fragmento e recebe algumas identificações no cabeçalho do protocolo IP, e necessita ser remontado no receptor ao chegar na camada de rede.

Na camada de transporte é esperado receber todo o segmento não fragmentado, atualmente os roteadores no meio do caminho não fazem a fragmentação, essa tarefa de fragmentação e remontagem de datagramas é destinada aos equipamentos da ponta da rede.

Se algum fragmento se perder ao longo do caminho o datagrama não será recuperado e se perderá, mas como a camada de transporte é responsável pela entrega confiável dos segmentos ela poderá solicitar a retransmissão das informações perdidas.

2.1.4 Protocolo ICMP

O protocolo de controle de erros e troca de mensagens é o *Internet Control Message Protocol* ICMP, muitas vezes é referenciado na camada de rede apesar de estar na camada acima, é um protocolo que tem como características a divulgação de eventuais erros que podem ocorrer na comunicação entre os hospedeiros e outras informações necessárias

2.1.5 Esgotamento dos Endereços IPv4

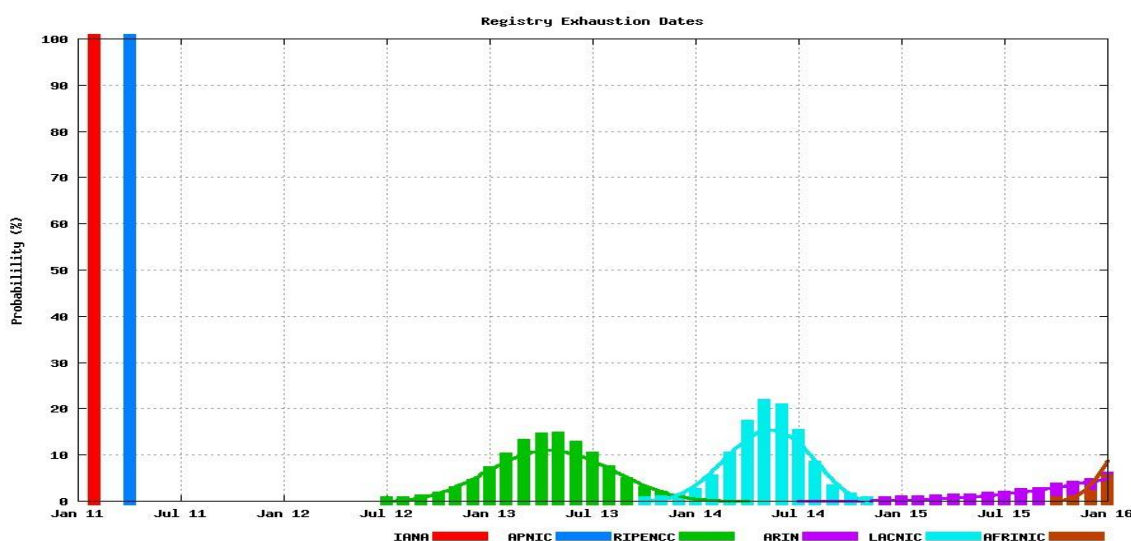
Não era possível imaginar que em 1976 4,3 bilhões de endereços não seriam suficientes, comparado com o que acontece com placas de carro e números de telefones, a quantidade de combinações possíveis de Ips esgotou.

Segundo o *Internet Assigned Numbers Authority* (IANA) – Órgão responsável pela alocação dos endereços mundialmente – o estoque dos endereços esgotou em 06 de fevereiro de 2011, restando apenas estoques em cada órgão regional distribuído geograficamente entre os continentes.

Segundo as projeções a primeira região a ficar sem os blocos IPv4 vai ser a região atendida pelo APNIC

Segundo as previsões do LACNIC, registro regional responsável pela alocação de endereços na América Latina e Caribe nos próximos meses as reservas locais dos endereços IPv4 disponíveis vão acabar isso deverá acontecer até aproximadamente junho de 2014 segundo as projeções realizadas.

Figura 03 – Gráfico de esgotamento dos endereços IPv4.



Fonte: Comitê Gestor da Internet

2.1.6 Soluções paliativas para o esgotamento de endereços

Algumas soluções foram desenvolvidas para que o esgotamento fosse retardado, era necessário algum tempo de pesquisa e estudo para que o novo protocolo estivesse maduro o suficiente para que fosse implementado.

Dentre as soluções desenvolvidas pode-se citar as que são vistas nas seções seguintes.

2.1.6.1 CIDR (Classless InterDomain Routing)

Definido na RFC 4632, o CIDR foi criado com o intuito de acabar com o uso das classes de endereços completas, fazendo com que fosse distribuído tamanho de blocos de acordo com a real necessidade da rede, com essa solução a tabela de roteamento foi reduzida e levou-se em consideração para o roteamento os bits mais significativos para a rede, como mostra tabela abaixo:

Tabela 01 – Possíveis prefixos para sub-rede IPv4.

Nº Bits por sub-rede	Nº Bits por Host	Nº Hosts por sub-rede	Tamanho do prefixo decimal	Máscara de sub-rede equivalente
1	31	2.147.483.648	/1	128.0.0.0
2	30	1.073.741.824	/2	192.0.0.0
3	29	536.870.912	/3	224.0.0.0
4	28	268.435.456	/4	240.0.0.0
5	27	134.217.728	/5	248.0.0.0
6	26	67.108.864	/6	252.0.0.0
7	25	33.554.432	/7	254.0.0.0
8	24	16.777.216	/8	255.0.0.0
9	23	8.388.608	/9	255.128.0.0
10	22	4.194.304	/10	255.192.0.0
11	21	2.097.152	/11	255.224.0.0
12	20	1.048.576	/12	255.240.0.0
13	19	524.288	/13	255.248.0.0
14	18	262.144	/18	255.252.0.0

15	17	131.072	/17	255.254.0.0
16	16	65.536	/16	255.255.0.0
17	15	32.768	/17	255.255.128.0
18	14	16.384	/18	255.255.192.0
19	13	8.192	/19	255.255.224.0
20	12	4.096	/20	255.255.240.0
21	11	2.048	/21	255.255.248.0
22	10	1.024	/22	255.255.252.0
23	9	512	/23	255.255.254.0
24	8	256	/24	255.255.255.0
25	7	128	/25	255.255.255.128
26	6	64	/26	255.255.255.192
27	5	32	/27	255.255.255.224
28	4	16	/28	255.255.255.240
29	3	8	/29	255.255.255.248
30	2	4	/30	255.255.255.252

2.1.6.2 DHCP (Dynamic Host Configuration Protocol)

Outra solução apresentada na RFC 2131 foi o protocolo DHCP que distribui as informações de rede aos hosts automaticamente, ele torna bem eficaz a distribuição temporária de endereços, depois que o cliente desconecta é possível desalocar o endereço arbitrariamente, através de regras de controle dos endereços.

2.1.6.3 NAT (Network Address Translation)

Definido na RFC 3022, permite que vários computadores naveguem na Internet através de um ou mais endereço(s) válido(s), os computadores dentro da rede recebem um endereço único e privado, quando um computador dessa rede precisa de comunicação com a Internet ele é convertido em um endereço que tem roteamento global, para que esse esquema funcione corretamente utiliza-se as classes de endereços definidos na RFC 1918, onde a regra

mais básica é que nenhum dos endereços definidos nessa RFC sejam usados na Internet, as três faixas são:

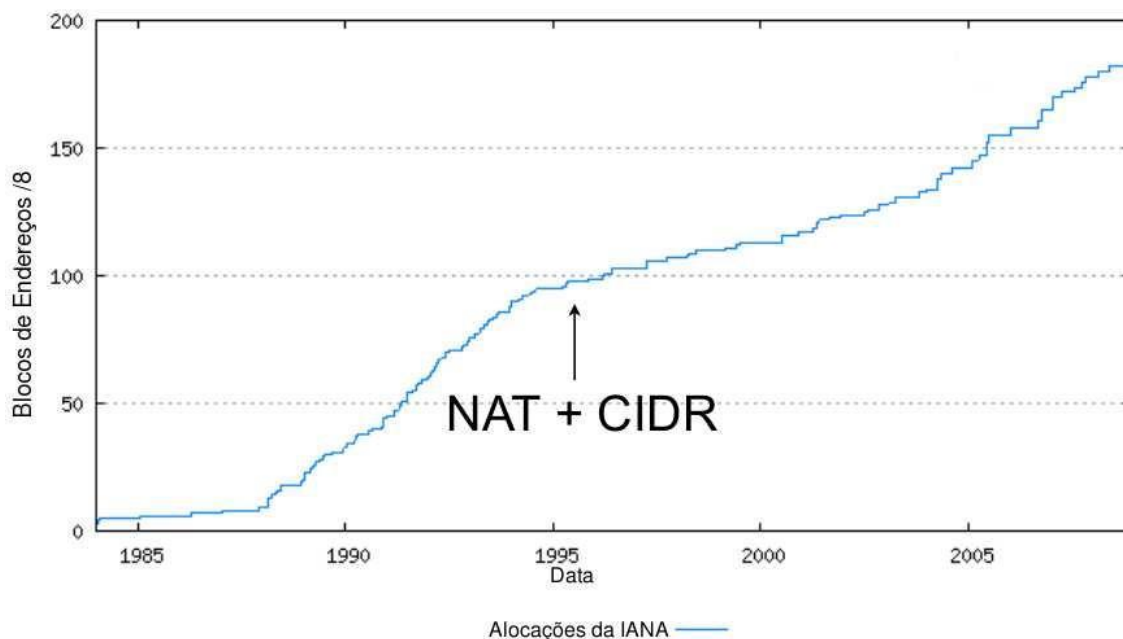
10.0.0.0 a 10.255.255.255/8

172.16.0.0 a 172.31.255.255/12

192.168.0.0 a 192.168.255.255/16

O NAT é muito eficiente quando se trata de economia de endereços, facilidade de gerência dos endereços da rede, oculta a topologia e só permite a entrada de informações que foram solicitadas de dentro da rede.

- Alguns problemas surgiram em contrapartida do uso do NAT, são eles:
- Não escalonável;
- Quebra o modelo fim-a-fim da Internet, não permite a conexão direta entre dois hosts diretamente, dificultando o funcionamento de algumas aplicações, dentre as quais podemos citar: P2P, VoIP e VPNs.
- Impossibilita o rastreamento do caminho do pacote, através de ferramentas como traceroute, mtr dentre outras, que tem como base o protocolo ICMP;
- Dificulta a utilização de técnicas de segurança como IPSec.
- Essas soluções apesar de serem bem eficazes no intuito de diminuir a demanda por Ips, não foram suficientes para resolver diversos problemas decorrentes da expansão da Internet.

Figura 04 – Alocação de endereços no IANA.

Fonte: Comitê Gestor da Internet

Como é visualizado no gráfico acima, mesmo com todas essas soluções, não foram suficientes para resolver o problema da grande demanda de alocação de endereços para que a Internet pudesse continuar crescendo. E consecutivamente o crescimento foi retardado em apenas 14%.

2.2 PROTOCOLO IPV6

O IPv6 foi apresentado inicialmente na RFC 1883 de dezembro de 1995, porém em dezembro de 1998 ela foi substituída pela RFC 2460, como principais mudanças podemos citar: Maior capacidade de endereçamento, simplificação do formato do cabeçalho, suporte a cabeçalhos de extensão, capacidade de identificar fluxo de dados e o suporte a autenticação e privacidade.

Além dessas mudanças houve uma melhoria significativa no tratamento da fragmentação dos pacotes, que passou a ser realizado somente na origem além de permitir o uso de conexões fim-a-fim e facilidade de configuração de redes.

A não adequação e implementação do IPv6 são riscos que terão algumas consequências graves para as redes já que elas não poderão surgir, a inclusão de novos

usuários nas redes existentes ficará comprometida, dificultará o surgimento de novas aplicações e os provedores não poderão disponibilizar novos serviços para seus clientes.

A adoção do protocolo IPv6 por completo possibilitará um novo conceito denominado “Internet das Coisas”, onde não só computadores estarão conectados, mas todo tipo de objeto, como carros, geladeiras, roupas, dispositivos de vigilância poderão se interligar a outros dispositivos em rede.

No início da década de 1990, pesquisadores já tinham propostas para substituição do protocolo IPv4 e em 1992 o *Internet Engineering Task Force* (IETF) criou um grupo chamado *IP Next Generation* (Ipng), em 1993 a pesquisa foi formalizada através da RFC 1550.

O novo protocolo deveria cumprir alguns pré-requisitos na sua elaboração, para que pudesse ser aceito, as questões foram as seguintes: escalabilidade, segurança, configuração e administração de rede, suporte *Quality Of Service* (QoS), mobilidade, políticas de roteamento e transição.

2.2.1 Cabeçalho IPv6

Figura 05 – Cabeçalho de um datagrama IPv6.

Version	Priority	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

Fonte - Comitê gestor da Internet

O cabeçalho IPv6 foi reduzido a 8 campos se tornando mais simples, mais flexível e mais eficiente e tendo tamanho fixo de 40 bytes, ou seja, apesar do aumento do campo de endereçamento ter aumentado em 16 vezes do tamanho original o total do cabeçalho aumentou somente em 2 vezes.

Foram removidos seis campos do cabeçalho sendo eles: Tamanho do cabeçalho, Identificação, Flags, Deslocamento de Fragmento, Soma de Verificação do Cabeçalho e Opções. Quatro campos tiveram seus nomes alterados e seus posicionamentos modificados, foram eles: Tipo de Serviço que mudou pra Classe de Tráfego, Tamanho Total que mudou pra Tamanho de Dados, *Time to Live* (TTL) que mudou pra Limite de Encaminhamento, o campo Protocolo mudou para Próximo Cabeçalho.

Foi adicionado um novo campo chamado Identificador de Fluxo e Três campos foram mantidos, foram eles: Versão, Endereço de Origem e Endereço de Destino.

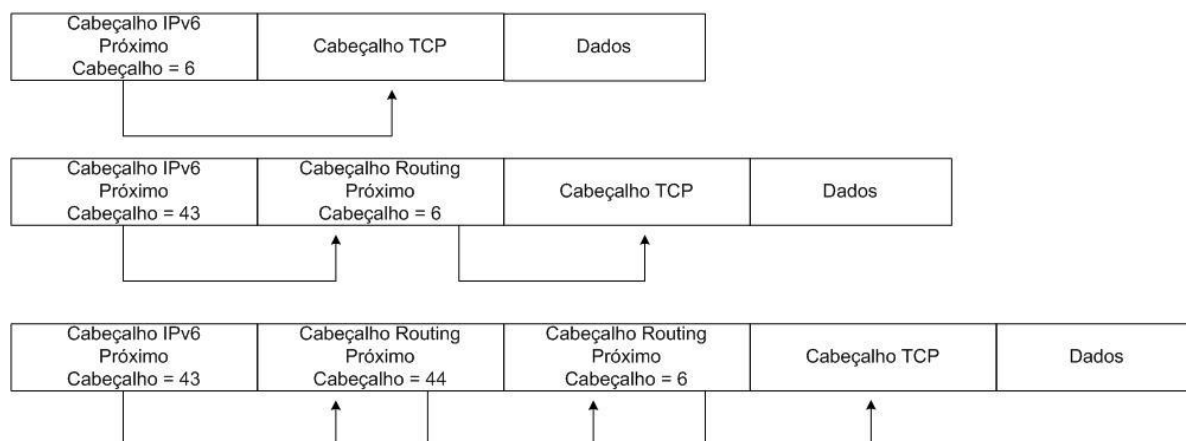
Com essas mudanças o cabeçalho IPv6 tem algumas vantagens sobre o cabeçalho IPv4, são elas:

- Mais simples por ter somente 40 Bytes;
- Mais flexível por ter recursos ampliados pelos cabeçalhos de extensão;
- Mais eficiente por ter diminuído o overhead.

2.2.2 Cabeçalhos de Extensão

No IPv6 as opções não vem mais como um campo no cabeçalho, agora essas informações estão nos cabeçalhos de extensão. Os cabeçalhos de extensão estão localizados entre o cabeçalho base e o cabeçalho imediatamente acima, não temos quantidade nem tamanho fixo para eles.

O Ipv6 tem seis cabeçalhos de extensão: *Hop-by-Hop*, *Options*, *Destination Options*, *Routing*, *Fragmentation*, *Authentication Header* e *Encapsulating Security Payload*.

Figura 06 – Cabeçalhos de extensão do IPv6.

Fonte: Comitê Gestor da Internet

2.2.3 Endereçamento IPv6

No IPv6 o endereço é dividido em oito grupos de 16 bits, separando-os por “:”, escritos com dígitos hexadecimais, por exemplo:

2001:0DB8:CAFE:DAD0:FACA:CA5A:F0CA:DE01

Na representação é possível a utilização de caracteres maiúsculos ou minúsculos, existe a regra de abreviação para facilitar a escrita de alguns endereços extensos. O zero pode ser omitido à esquerda de cada bloco de 16 bits, pode ser substituída uma sequência longa de zeros por “::”. Devemos ter cuidado na abreviação para que não haja ambigüidade, por exemplo, o endereço 2001:0DB8:0000:0000:130F:0000:0000:140B pode ser escrito como 2001:DB8:0:0:130F::140B ou 2001:DB8:::130F:0:0:140B. No exemplo podemos observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, senão poderá gerar ambigüidades na representação do endereço.

A utilização do CIDR está presente no IPv6, continua sendo escrita do mesmo modo que no IPv4, essa notação é representada pela divisão da forma “endereço-IPv6/tamanho do prefixo”, onde o valor do prefixo é um número decimal que representa a quantidade bits contíguos a esquerda do prefixo. Podemos representar um endereço de 128 bits como no exemplo a seguir:

Prefixo 2001:db8:3003:2::/64

Prefixo Global 2001:db8::/32

ID da sub-rede 3003:2

Essa forma de organização do endereço possibilita que sejam identificadas de forma hierárquica, identificando a topologia da rede através de parâmetros como localização geográfica, provedor de acesso, identificação da rede, divisão da sub-rede, etc. Com esse recurso é possível a correta organização e traz a diminuição do tamanho da tabela de rotas e agilizam a entrega dos pacotes.

No IPv6 existem três tipos de endereços definidos:

- **Unicast:** Este tipo de endereço é para identificação de uma única interface, desse modo se um pacote tem como destino um endereço *unicast* ele é entregue a uma única interface;
- **Anycast:** É responsável pela identificação de um conjunto de interfaces. Quando um pacote tiver como destino um endereço *anycast* ele é entregue a interface pertencente ao conjunto mais próxima da origem, ele é especialmente utilizado na comunicação de um-para-um-de-muitos.
- **Multicast:** Também identifica um conjunto de interfaces, porém quando um pacote tem como destino um endereço *multicast* ele é entregue a todas as interfaces associadas a esse endereço. Ele é especialmente usado em comunicações de um-para-muitos.

No IPv6 não tem endereço de broadcast, essa função foi atribuída à tipos específicos de endereços *multicast*.

Existem alguns tipos de endereços *unicast* IPv6: *Global Unicast*; *Unique-Local*; e *Link-Local*.

- **Global Unicast** – São os tipos de endereços roteáveis e acessíveis na Internet IPv6, assim como no IPv4 o IPv6 é constituído para permitir agregações de tamanho flexível da mesma maneira que no IPv4 e ele é constituído de três partes: o prefixo do roteamento global, a identificação da sub-rede e a identificação da interface.
- Para essa faixa de endereços está reservada a faixa 2000::/3 (001), corresponde aos endereços de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff. Representa 13% do total de endereços possíveis com IPv6, e permite criar $2^{(64-3)} = 2.305.843.009.213.693.952$ ($2,3 \times 10^{18}$) sub-redes /64 diferentes ou $2(48-3) = 35.184.372.088.832$ ($3,5 \times 10^{13}$) redes /48.

- **Link Local**- É usado especificamente no enlace onde a interface está conectada, esse tipo de endereço é atribuído automaticamente utilizando prefixo **FE80::/64**. O endereço é formado por um padrão de endereços chamado **IEEE EUI-64**. Nesse caso os roteadores não encaminham os pacotes que tem como destino ou origem um endereço *link-local*.
- O padrão **EUI-64** é obtido da seguinte maneira:
 - Se o MAC da placa de rede for um endereço MAC de 64 bits (padrão EUI-64), faz a inversão do valor do sétimo dígito binário mais a esquerda (denominado de bit U/L – Universal/Local) do endereço MAC, ou seja, se o valor do bit é “0” é alterado para “1”, se for “1” é alterado para “0”.
 - Se a placa de rede tiver o padrão de 48 bits (IEEE 802), adiciona-se os dígitos hexadecimais FF-FE, entre o terceiro e o quarto Byte do endereço MAC, dessa forma ele se torna um endereço no padrão EUI-64, logo após a alteração o bit U/L é complementado. Por exemplo: Se o endereço MAC for: **48-1E-C9-21-85-0C**, o endereço com as alterações ficaria da seguinte forma: **4A-1E-C9-FF-FE-21-85-0C**, logo o endereço de link-local que seria atribuído a Interface de rede seria: **FE80::4A1E:C9FF:FE21:850C**.
- **Unique-Local-Endereço** que pode ser único globalmente, ele é utilizado em comunicações locais, geralmente dentro de um mesmo enlace ou conjunto de enlaces, assim como os endereços Link Local ele não pode ser roteável na Internet Global.

Esse endereço é alocado pseudo-randomicamente, e é composto pelas seguintes partes:

- **Prefixo:** FC00::/7
- **Flag Local (L):** Formado por um bit de dado e quando seu valor for 1 significa que o prefixo é atribuído localmente (**FD**) e quando o bit for 0 (**FC**), o prefixo deve ser atribuído por uma organização central.
- **Identificador Global:** Formado por um campo de 40 bits usados para formação de um prefixo globalmente único.
 - **Identificador da Interface:** Identifica a interface e seu tamanho é de 64 bits.

Deste modo qualquer enlace pode ter um prefixo /48 privado e único globalmente. Caso algum prefixo desse tipo de rede seja anunciado acidentalmente para fora da rede, através de roteador ou via DNS, ele pode ser bloqueado facilmente.

2.2.4 ICMPv6

Os recursos que foram implantados no protocolo IPv6 tem como base o ICMPv6, através dele é possível fazer a divulgação e atribuição de endereços aos hosts automaticamente, outros recursos podem ser o gerenciamento de grupos, a descoberta de vizinhança e o suporte a QOS melhor elaborado.

Os protocolos ARP, RARP e IGMP foram substituídos pelo ICMPv6, é necessário ser cauteloso ao se trabalhar com firewall nas estações de trabalho, se o protocolo for bloqueado a rede não irá funcionar.

A descoberta de vizinhança é fundamental em um segmento de rede que usa o IPv6, quatro mensagens são de extrema importância são elas:

- **RS (*Router Solicitation*)** – A mensagem é enviada por uma estação para aprender sobre informações de um roteador, com as informações adquiridas a estação terá condições de acessar o mundo externo sem a necessidade de um serviço DHCPv6. O endereço da mensagem de origem é unicast, exemplificada por uma comunicação ponto-a-ponto. O endereço de destino é *Multicast All-Routers FF02::2*.
- **RA (*Router Advertisement*)** – As mensagens RA podem ser feitas em duas situações distintas: a primeira é a resposta a uma solicitação do tipo RS. Outra maneira é a possibilidade de envio de anúncios em intervalos de tempo no segmento de rede sem a solicitação de requisição dos clientes, ou seja, de forma automática. Alguns roteadores já vem configurados com esse anúncio de forma padrão, em outros é necessário a ativação desse serviço por meio de algum software, o daemon RADVD é utilizado em máquinas Linux para fazer as divulgações das mensagens. A origem da mensagem é um endereço unicast e o de destino é um endereço *Multicast All-Nodes FF02::1*.
- **NS (*Neighbor Solicitation*)** – Similar ao funcionamento do *ARP Request*, envia uma mensagem ao host para descobrir qual o endereço MAC que corresponde a um determinado endereço IPv6, tem a função de confirmar a unicidade do endereço atribuído ao host de origem (*Deteção de Endereço Duplicado – DAD - Discover Address Duplicate*).

Quando o host pergunta às demais máquinas quem tem o endereço associado ao endereço IPv6, é usado o endereço *IPv6 Multicast Solicited Node*

FF02::1:FFxx:xxxx, sendo que os últimos 24 bits pertencem aos bits finais do endereço IPv6 com o mesmo final.

- **NA (*NeighBor Advertisement*)** – Mensagem enviada em resposta a uma solicitação do tipo NS, ou pode ser enviada automaticamente para todos os hosts do segmento informando a mudança de endereço de um determinado host. Uma mensagem NA tem um endereço de origem e destino unicast quando é a resposta de uma requisição NS, quando é gerada para informar a mudança de endereço, o destino será o endereço *Multicast All Nodes* FF01::2.

2.2.5 Planejamento e Implantação

Para implantação em uma rede do protocolo IPv6 alguns aspectos devem ser considerados para fazer a correta distribuição dos endereços nos diversos departamentos e setores da empresa ou instituição, deve-se avaliar se a quantidade de endereços é suficiente e como será a identificação das redes e hosts.

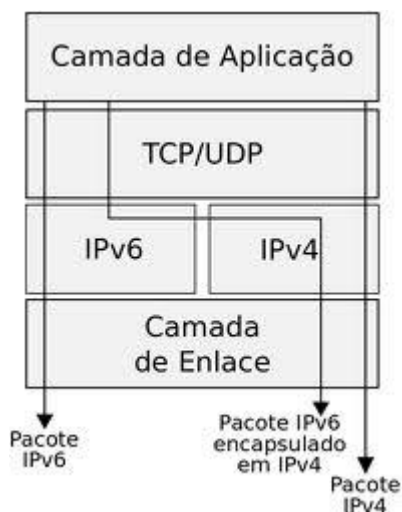
Alguns aspectos devem ser avaliados como:

- A divisão dos endereços;
- Como deve acontecer a transição do IPv4 para o IPv6;
- Gerência dos endereços;
- Quais os serviços irão migrar inicialmente;
- Qual o nível de aderência (Endereçamento, roteamento) dos ativos de rede com relação ao IPv6;
- Compatibilidade dos equipamentos finais dos usuários;
- Adaptação dos serviços para manter a compatibilidade entre os dois protocolos.

2.2.6 Transição

A interoperabilidade e coexistência são fatores determinísticos para que se utilize alguma técnica de transição. Algumas técnicas conhecidas são: Pilha Dupla (figura 8), os túneis ponto a ponto 6over4 e GRE, os Tunnel Brokers, o DS-Lite, o NAT64, o IVI, o 464XLAT, o 6PE, o 6VPE, o 6rd e o 4rd.

Figura 07 – Esquema de pilha dupla (IPv4 e IPv6).



Fonte – Comitê gestor da Internet

A utilização de Túnel Broker é justificada quando se quer testar IPv6, ou fazer a implantação na rede, pode ser utilizada por usuários domésticos e corporativos que queiram trafegar em pilha dupla e onde o *Internet Server Provider* (ISP) não tenha ou ainda não forneçam tráfego IPv6.

Os túneis possibilitam que as redes IPv6 possam trafegar normalmente utilizando a estrutura da rede IPv4, mesmo com uma latência maior do que com redes IPv4 nativas, é uma das melhores alternativas para que se possa trafegar dados na rede IPv6 de forma transparente atualmente.

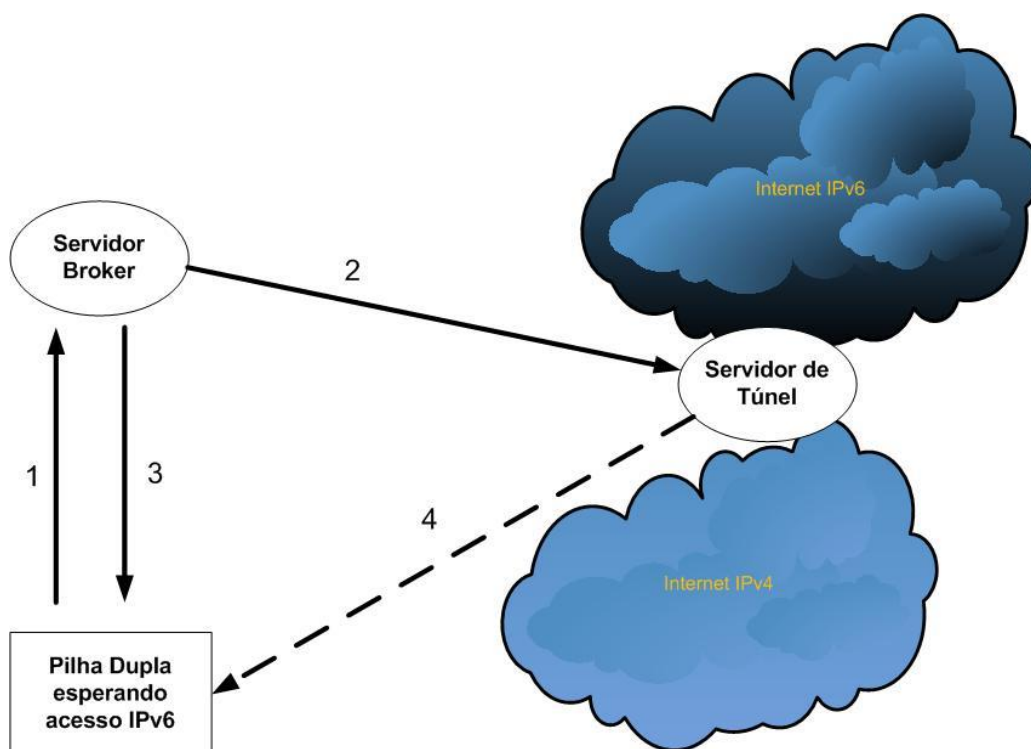
O túnel broker foi definido na RFC 3053, e traz a possibilidade de dispositivos totalmente isolados, ou até mesmo toda uma rede obter conectividade IPv6 por meio do estabelecimento de um túnel com um provedor, tornando-se, na prática, ou uma rede, pilha dupla.

Dentre as opções existentes, recomendam-se:

- **<http://tunnelbroker.net>** - serviço oferecido pela Hurricane Electric, que povê túneis para usuários domésticos ou corporativos, inclusive com a possibilidade de fechar sessões BGP para o provimento de trânsito IPv6 via túnel.
- **<http://www.sixxs.net>** - serviço oferecido de forma colaborativa por um grande número de organizações. Nesse túnel não tem é disponibilizada a possibilidade de fechar sessões BGP, mas tem a vantagem de obter tamanhos fixos de /48 ou /64 roteadas através do túnel. A Algar Telecom/CTBC é responsável por um dos POPs que estão configurados os túneis, no Brasil, de forma que para usuários em

redes brasileiras os túneis funcionam com qualidade e velocidade próximas às de conexões ativas.

Figura 08 – Estabelecimento de um túnel IPv6.



Fonte: própria.

A figura 8 exemplifica os passos para se obter um Túnel Broker e acesso a Internet para trafegar dados em IPv6. A sequência é a seguinte:

- 1- Cliente pilha dupla solicita túnel solicitada via IPv4;
- 2- Broker cadastra usuário no Servidor de túnel;
- 3- Broker informa cliente parâmetros para criação do túnel;
- 4- O túnel é estabelecido.

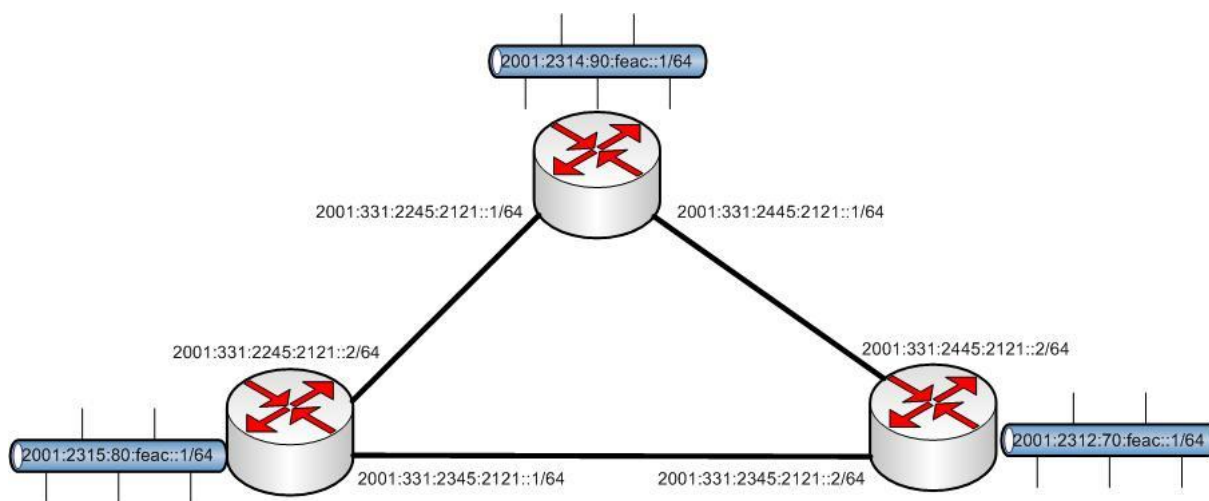
A faixa de endereços disponibilizada pelos provedores de túneis brokers é do tamanho de 64 bits no caso de solicitação de somente um túnel para um dispositivo, seguindo a política de distribuição de endereços IPv6, é aconselhado que se tenha faixas de sub-redes para usos futuros e que o menor valor sugerido é /64 e 48 bits para solicitações de sub-redes sendo que é necessário um prefixo do tamanho de 64 bits para se fazer a distribuição automática dos endereços, leva-se em consideração então que se têm $64-48=16$ bits para endereçar sub-redes.

2.2.7 Roteamento do IPv6

No software do roteador de saída padrão da rede não temos preferência na saída entre os protocolos IPv4 ou IPv6, se um pacote chegar com endereço IPv4 ele simplesmente vai usar a tabela de roteamento IPv4, se um pacote chega com endereço IPv6 ele vai usar a tabela de roteamento IPv6, quem vai determinar se o pacote gerado será IPv4 ou IPv6 é a aplicação e não a rede.

Nesse caso se faz jus a um planejamento detalhado para que se tenha um controle corretos dos endereços de redes e hosts para que se possa alcançar o destinatário e ter a comunicação estabelecida de forma correta, além de se evitar problemas relacionados a segurança.

Figura 09 – Roteamento em uma rede IPv6.



Fonte: própria

Todos os roteadores precisam de uma rota padrão para encaminhar o pacote para um destinatário quando não se sabe o caminho ou o caminho não está listado na tabela de roteamento, uma rota padrão no IPv6 é algo como: ::/0 via eth0 por exemplo.

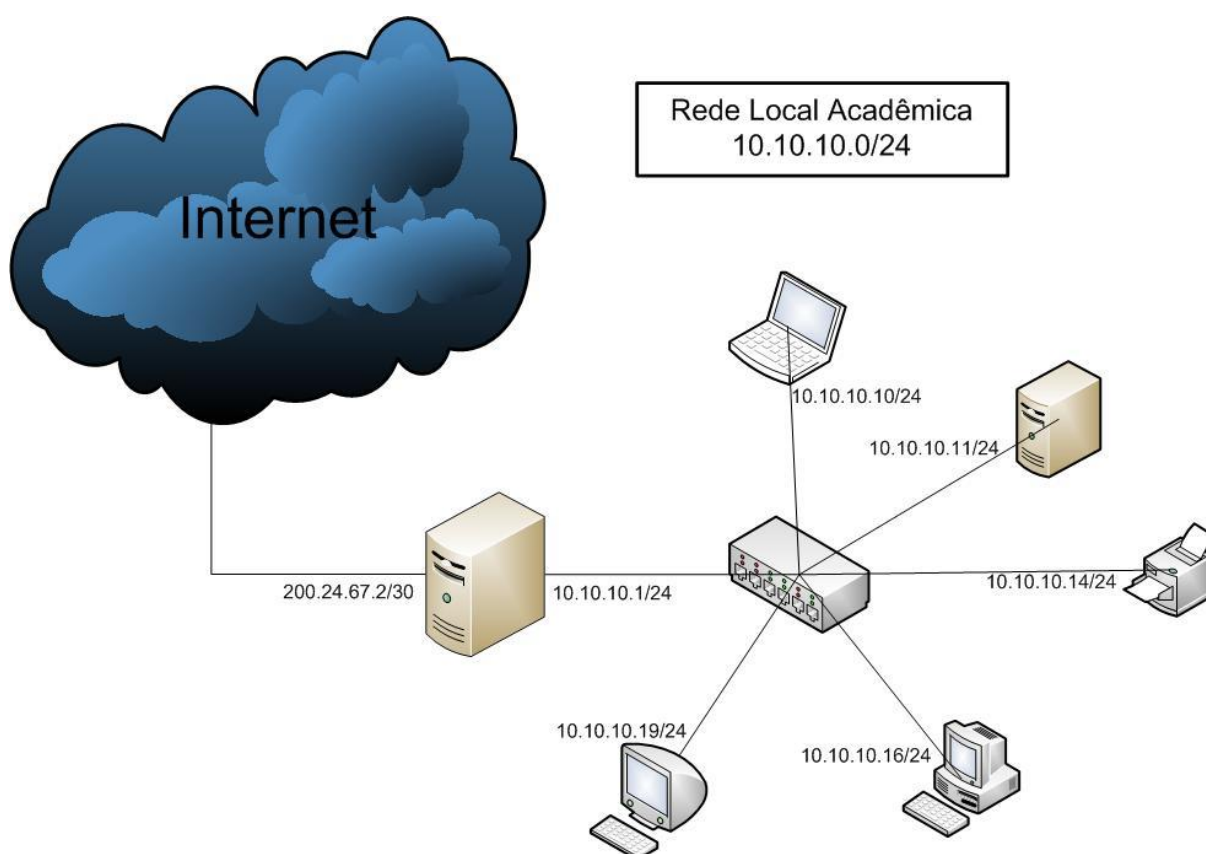
Nos roteadores tem-se dois tipos de rotas: as estáticas que podem ser criadas manualmente e as dinâmicas que são aprendidas através de algum protocolo de roteamento específico.

3 ESTUDO DE CASO

O estudo de caso abordado nesse capítulo refere-se a utilização de um túnel broker para que a rede possa trafegar em pilha dupla com os dois protocolos de endereçamento IPv4 e IPv6, além de conter também algumas aplicações práticas para a distribuição dos endereços na rede e as regras de um simples firewall para prover uma segurança com o objetivo de impedir alguns ataques já disseminados nas redes IPv6.

3.1 TOPOLOGIA DO AMBIENTE

Figura 10 – Rede Local IPv4.



Fonte - Própria

A rede local que será usada, mostrada na figura 10, é formada por diversos dispositivos interligados em rede, dentre eles pode-se citar: Servidor, Firewall, Switch, Notebooks, Impressoras, Computadores de Mesa.

O servidor terá o sistema operacional GNU/Linux Ubuntu Server 11.10, 2 placas de rede gigabit ethernet. A configuração das placas fica da seguinte maneira: uma placa é

conectada diretamente a Internet com um IP Público e a outra na Rede Local com um IP privado da faixa de endereçamento da rede local com o IP 10.10.10.1.

3.2 AQUISIÇÃO DO TÚNEL IPV6

Para aquisição do túnel broker utilizado nesse estudo de caso foi necessário o cadastro no portal do provedor SIXXS através do endereço eletrônico www.sixxs.net, clicando em *signup for new users* e logo depois em *direct signup*.

Em seguida é aberto um formulário de cadastro, como mostrado na figura 11, para solicitação do túnel e escolha do provedor de acesso para conexão com o servidor. O provedor escolhido foi o Provedor CTBC em Uberlândia, Minas Gerais, por ser o único provedor brasileiro com conexão disponível para realização de um túnel nacional, trazendo assim desempenhos satisfatórios relativos a resposta e acesso ao serviços com endereços IPv6 disponíveis atualmente.

Figura 11 – Formulário de cadastro no SIXXS.

Full name:		Examples & Instructions Ernest Xonan Ample (First/Given (Middle) Last/Sur-name', no initials)
Organization:		ACME Corp. (optional)
☐ Hide my details (address, phone, e-mail, url) in whois.		(When selected details will be hidden in whois, otherwise they will be visible there, your name can always be found in whois. See FAQ: Privacy Policy and FAQ: Address)
Address:		Example Lane 42 21PC0D3 City Country (no P.O.Box)
Phone:		+99 123 1234 5678 (International prefix in E.164 format)
Email:		ernest.x.ample@example.com (Your contact email address at your ISP or work, see requirements FAQ)
Website:		http://www.sixxs.net (optional, leave it empty for no website)
Reason:		* = The signup reason should be at least have a minimum 2 lines/20 words. Please specify what you would like to use your account and the connectivity that comes along with it for. We also like to hear how you landed at SixXS (eg friends, search engine, magazine, article etc).
Submit Signup (directly creates an account and sends a verification email)		

Fonte - própria

No processo de aquisição é necessário preencher um campo com a justificativa para aquisição do túnel. Logo após a finalização do cadastro é enviado uma solicitação ao provedor que então é analisado pelo provedor para prover a conexão ou simplesmente ser rejeitado.

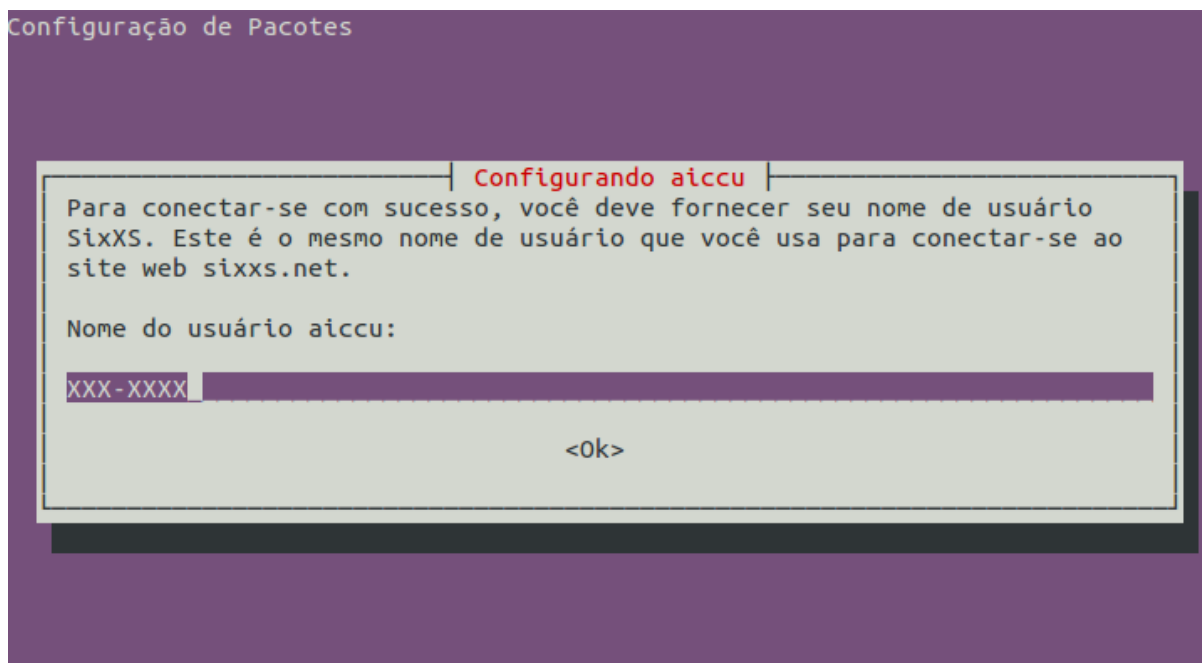
Figura 12 – Faixa de endereços adquirida para o Túnel.

PoP	
brudi01	
Location:	Uberlandia, Brazil 
Hostname:	brudi01.sixxs.net
Established:	2010-02-13
Operational:	2 years, 5 months, 9 days
SixXSd version:	v4
Status:	Up
Heartbeat support:	Yes
AYIYA support:	Yes
Multicast support:	No
m6bone connected:	No
Active Tunnels:	855
Active Subnets ¹ :	169
Available Subnets ¹ :	87
Public:	Yes
Statistics:	Latency/Loss , Traffic
Issue Tracker:	Issues?
This PoP provides tunnels from the following prefixes:	
• 2001:1291:1000::/48 of size /64	
Subnets are allocated out of:	
• 2001:1291:1000::/40 of size /48	
¹ = Default /64 subnets are not included in this number as they equal the number of tunnels.	

Fonte – própria

Em paralelo ao processo de cadastro são enviados e-mails para o solicitante informando todos os passos do cadastro e a positivação ou negação de aceitação do túnel.

Após a aprovação e obtenção dos endereços IPv6 para o túnel, figura 12, é necessário configurar o cliente do túnel. Para isso, é preciso fazer o download do software **aiccu** para fechar a conexão com o túnel. No sistema operacional GNU/Linux Ubuntu Server 12.04, utilizado no estudo de caso, o comando *\$sudo aptitude install aiccu* foi executado para fazer o download e instalar o software a partir do repositório oficial do sistema. No momento da instalação do pacote são solicitadas três informações: o servidor do túnel, o login e a senha que foram cadastradas, conforme figura 13.

Figura 13 – Configuração do software aiccu.

Fonte – Própria

Após a instalação e autenticação no servidor do provedor que provê o túnel, é criada uma interface de rede virtual chamada sixxs, na qual pode ser visualizada com o comando `$ifconfig sixxs`. Pode-se então visualizar o endereço IPv6 atribuído para a Interface e pode-se agora realizar o teste de ping para saber se o computador tem resposta dos hosts que estão prontos para trabalhar com o IPv6, através do comando `$ping6 ipv6.br -n`. Assim como no IPv4 algumas ferramentas que trabalham com testes e diagnósticos na rede já estão prontas para trabalhar com IPv6, dentre elas pode-se citar: *ping6*, *mtr*, *tcpdump*, *nmap*, e *ip*.

3.3 HABILITANDO IPV6 NOS SISTEMAS OPERACIONAIS

A maioria dos sistemas operacionais já estão prontos para trabalhar com o IPv6 nativamente, e os que não estão podem ser habilitados com pequenos ajustes. No sistema operacional GNU/Linux, o IPv6 já está disponível desde o kernel 2.1.8. A configuração do endereço IPv6 em um sistema operacional Linux pode ser visualizada através do comando: `$ip -6 addr show`. Para verificar se foi habilitado, executa-se em uma janela de terminal o comando a seguir:

```
ping6 -c 4 ::1
```

O resultado deve ser o mostrado na figura .

Figura 14 – Teste de conectividade IPv6.

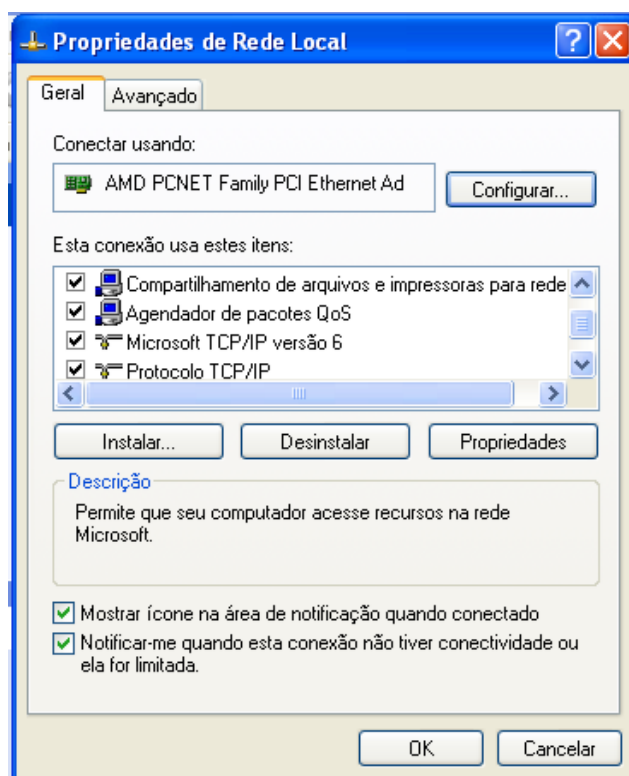
```
# ping6 -c 5 ::1
PING ::1(::1) 56 data bytes
64 bytes from m ::1: icmp_seq=1 ttl=64 time=0.055 ms
64 bytes from m ::1: icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from m ::1: icmp_seq=3 ttl=64 time=0.033 ms
64 bytes from m ::1: icmp_seq=4 ttl=64 time=0.046 ms
64 bytes from m ::1: icmp_seq=5 ttl=64 time=0.039 ms

--- ::1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.020/0.038/0.055/0.013 ms
```

Fonte – Comitê gestor da Internet

No Windows XP é necessário a ativação através de protocolo IPv6 no Painel de Controle – Conexões de Rede - Conexão Local – Propriedades de Conexão Local, e seleciona o item Microsoft TCP/IP versão 6, como mostrado na figura XX.

Figura 15 – Propriedades de rede no Windows XP.



Fonte – própria

No Windows Vista o IPv6 é instalado e habilitado por padrão. No Windows 7 além de instalado e configurando por padrão, novos recursos foram incorporados como:

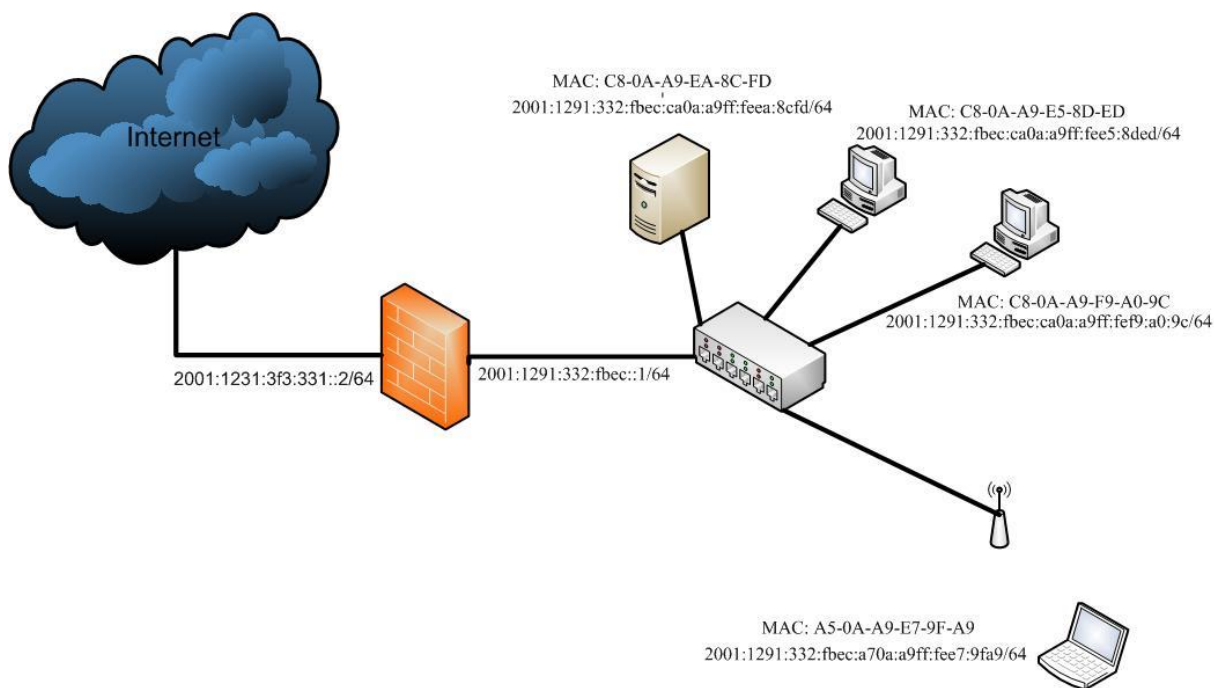
- **DirectAccess**, recurso habilitado no Windows 7 e Windows Server 2008 que permite acesso remoto e transparente aos recursos da rede com o protocolo de criptografia IPSec.
- **IP-HTTPS**: Permite que browsers possam navegar atravessando por proxies e firewall, usando encapsulamento IPv6 sobre IPv4 através de sessões HTTPS.
-

3.4 PARÂMETROS DA REDE IPV6

O endereço IPv6 adquirido para o túnel foi 2001:1291:3f3:331::2/64, o qual foi vinculado à interface virtual sixxs do túnel. A faixa de endereços adquirida para a rede local foi 2001:1291:332::/48.

Para que o serviço de distribuição automática de endereços funcione corretamente foi necessário incluir mais 16 bits na faixa de endereços para a rede local, transformando o prefixo em um /64. A figura 17 mostra o diagrama da rede local após as mudanças.

Figura 16 – Rede local com endereços IPv6.



Fonte - Própria

Foi necessário ativar o roteamento no kernel do GNU/Linux através do seguinte comando:

```
# sysctl -w net.ipv6.conf.all.forwarding=1
```

3.5 DISTRIBUINDO ENDEREÇOS IPV6 ATRAVÉS DO RADVD

O *Router ADvertisement Daemon* (RADVD) é um programa para o Linux que faz a distribuição de prefixo do endereço IPv6 dentro do segmento de rede de forma automática e funciona com mensagens de descoberta de vizinhança RA.

O arquivo de configuração é armazenado no caminho */etc/radvd.conf*. A figura 17 mostra o conteúdo deste arquivo com os parâmetros utilizados.

Figura 17 – Arquivo de configuração radvd.conf.

```
interface eth1{
    AdvSendAdvert on;
    MinRtrAdvInterval 3;
    MaxRtrAdvInterval 30;
    prefix 2001:1291:332:fbec::/64{
        AdvOnLink on;
        AdvAutonomous on;
        AdvRouterAddr on;
        AdvPreferredLifetime 90;
        AdvValidLifetime 120;
    };
};
```

Fonte – Própria

Observando a configuração do RADVD na figura 17, observa-se dois parâmetros principais: a interface de rede na qual o roteador se anunciará para os hosts da rede e o prefixo IPv6 a ser utilizado em tal rede. A partir deste anúncio do prefixo pelo roteador e da elaboração do sufixo no padrão EUI-64, cada host pode definir seu endereço IPv6 e qual o seu gateway para acessar outras redes, incluindo a própria Internet, via IPv6.

Assim, constatou-se que o uso do RADVD evita a necessidade de um servidor DHCPv6 para distribuir os endereços IPv6 na rede aos hosts, papel assumido pelo próprio roteador IPv6.

4 CONCLUSÃO

Conclui-se que o protocolo IPv6 trouxe avanços significativos ao protocolo IP. Através de uma distribuição de endereços IP do tipo *stateless* é possível ter acesso a rede mundial de computadores sem necessitar de configurações avançadas. Após a obtenção da conectividade através de túneis broker com as redes que já estão compatíveis com o IPv6, houve uma contribuição essencial do *daemon* RADVD em um roteador com sistema operacional GNU/Linux para distribuição do prefixo do endereço no segmento da rede e através do padrão EUI-64 foi feita a obtenção do sufixo dos endereços dos hosts.

Alguns roteadores já têm o serviço de distribuição de endereços em modo *stateless* incluídos em seus sistemas, tornando a implantação de uma rede com acesso ao IPv6 simplificada.

REFERÊNCIAS

CENTRO DE ESTUDOS E PESQUISAS EM TECNOLOGIAS DE REDES E OPERAÇÕES. **Habilitando o IPv6 no Linux**. Disponível em: <<http://ipv6.br/habilitando-linux/>>. Acesso em: 26 jul. 2012a.

_____. **Habilitando o IPv6 no Windows**. Disponível em: <<http://ipv6.br/habilitando-windows/>>. Acesso em: 26 jul. 2012b.

COMER, Douglas E. **Redes de computadores e internet**. 4. ed. Porto Alegre: Bookman, 2007. 265 p.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Túneis Teredo**. Disponível em: <<http://www.ipv6.br/IPV6/ArtigoTuneisTeredoParte08>>. Acesso em: 10 maio 2011.

_____. **Programação Sockets BSD Parte 03**. Disponível em: <<http://www.ipv6.br/IPV6/ArtigoProgramacaoSocketsBSDParte03>>. Acesso em: 10 maio 2012.

FLORENTINO, Adilson Aparecido. **Coleção Academy IPv6 na prática**. São Paulo: Linux New Media, 2012.

GUIA Foca GNU/Linux. **Guia online Versão Avançado**: Capítulo 10. Disponível em: <http://www.guiafoca.org/?page_id=14>. Acesso em: 10 jul. 2012.

KUROSE, James F. **Redes de Computadores e a Internet**: uma abordagem top-down. 5. ed. São Paulo: Pearson Addison Wesley, 2010.

MOREIRAS, Antonio Marcos et al. **Técnicas de Transição do IPv4 para o IPv6**. São Paulo: Núcleo de Informação e Coordenação do Ponto BR – NIC.br, 2012. Disponível em: <<ftp://ftp.registro.br/pub/gter/gter33/03-IPv6TecnicasTransicao.pdf>>. Acesso em: 26 abr. 2013.

PONTO DE PRESENÇA DA REDE NACIONAL DE ENSINO E PESQUISA NO ESTADO DO PARANÁ – PoP-PR. Disponível em: <<http://www.pop-pr.rnp.br/tiki-index1ed7.html?page=Roteadores+IPv6>>. Acesso em: 28 jul. 2012.

SANTOS, Rodrigo Regis et al. **Núcleo de Informação e Coordenação do ponto BR**. São Paulo: Curso IPv6 Básico, 2010. Disponível em:
<<http://www.ipv6.br/pub/IPV6/MenuIPv6CursoPresencial/IPv6-apostila.pdf>>. Acesso em: 21 jul. 2012.

TANEMBAUM, Andrew S. **Redes de Computadores**. 4 ed. New Jersey: Prentice Hall PTR, 2003.