



DOUGLAS HENRIQUE SIQUEIRA ABREU

**PROPOSTA DE IMPLANTAÇÃO DO
PROTOCOLO IPV6 NA REDE DA
UNIVERSIDADE FEDERAL DE LAVRAS**

**LAVRAS - MG
2014**

DOUGLAS HENRIQUE SIQUEIRA ABREU

**PROPOSTA DE IMPLANTAÇÃO DO
PROTOCOLO IPV6 NA REDE DA
UNIVERSIDADE FEDERAL DE LAVRAS**

Monografia apresentada ao colegiado do Curso de Sistemas de Informação, como uma das exigências para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador:

Dr. Luiz Henrique Andrade Correa

Coorientador:

MSc. Hermes Pimenta de Moraes Júnior

Anderson Bernardo dos Santos

**LAVRAS - MG
2014**

DOUGLAS HENRIQUE SIQUEIRA ABREU

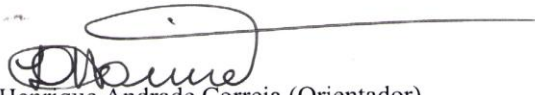
**PROPOSTA DE IMPLANTAÇÃO DO
PROTOCOLO IPV6 NA REDE DA UFLA**

Trabalho de Conclusão de Curso de Graduação apresentado ao Colegiado do Curso de Bacharelado em Sistemas de Informação, para obtenção do título de Bacharel.

APROVADA em 26 de novembro de 2014.

Dr. Neumar Costa Malheiros

Eder Teixeira de Andrade



Dr. Luiz Henrique Andrade Correia (Orientador)

MSc. Hermes Pimenta de Moraes Junior (Coorientador)

Anderson Bernardo dos Santos (Coorientador)

**LAVRAS-MG
Novembro/2014**

RESUMO

A utilização de dispositivos que acessam a internet vem crescendo, com isso um problema que vem se tornando cada vez mais sério é o esgotamento dos endereços de rede (IPv4). O IPv6 foi desenvolvido principalmente para suprir o problema de falta de endereços da rede atual. Este trabalho busca propor uma solução para a implantação do protocolo IPv6, para que este funcione em pilha dupla com IPv4, ambos trabalhando de forma nativa. O projeto de implantação foi planejado de acordo com o cronograma brasileiro de migração para o IPv6.

Palavras-chave: IPv6; Protocolo IP; Redes de Computadores.

LISTA DE FIGURAS

FIGURA 1 MAPA DA ARPANET EM 1969	12
FIGURA 2 ENTIDADES RESPONSÁVEIS PELA DISTRIBUIÇÃO DE IPS NA INTERNET.....	13
FIGURA 3 CABEÇALHO IPV4.....	16
FIGURA 4 CABEÇALHO IPV6.....	17
FIGURA 5 FUNCIONAMENTO DO CABEÇALHO DE EXTENSÃO.....	18
FIGURA 6 ALOCAÇÃO <i>RIGHTMOST</i>	26
FIGURA 7 DIVISÃO DE UMA REDE /32 EM 16 SUBREDES UTILIZANDO <i>RIGHTMOST</i>	26
FIGURA 8 ALOCAÇÃO <i>LEFTMOST</i>	27
FIGURA 9 DIVISÃO DE UMA REDE /32 EM 16 SUBREDES UTILIZANDO <i>LEFTMOST</i>	28
FIGURA 10 CRONOGRAMA BRASILEIRO DE MIGRAÇÃO PARA O IPV6.....	33
FIGURA 11 PORCENTAGEM DE ACESSO AO GOOGLE UTILIZANDO IPV6	34
FIGURA 12 FUNCIONAMENTO DA PILHA DUPLA	35
FIGURA 13 SIMULADOR RFC 3531.....	39
FIGURA 14 DIAGRAMA DA REDE DA UFLA.	42
FIGURA 15 ROTA DE PROPAGAÇÃO DE IPV4 VIA BGP	44
FIGURA 16 ROTA DE PROPAGAÇÃO DE IPV6 VIA BGP	44
FIGURA 17 DIVISÃO DE BITS ENTREGUE A CADA LOCALIDADE.	45
FIGURA 18 DIVISÃO IPV6 NA UFLA.	46
FIGURA 19 REDE DCC	49
FIGURA 20 DIVISÃO DE BITS DENTRO DO DEPARTAMENTO	50
FIGURA 21 PING REALIZADO.....	54

LISTA DE TABELAS

TABELA 1 RENOMEAÇÃO DOS CAMPOS DO PROTOCOLO IPV6 – NIC.BR.....	17
TABELA 2 SALAS DCC.....	47
TABELA 3 SERVIÇOS DE REDE.....	48
TABELA 4 HOSTS COM IPV4 FIXOS.	48
TABELA 5 HOSTS POR LABORATÓRIOS	49
TABELA 6 DIVISÃO IPV6 DCC	51
TABELA 7 SITES MAIS ACESSADOS DO BRASIL	52

SUMÁRIO

1	INTRODUÇÃO.....	8
1.1	Objetivo geral.....	9
1.2	Objetivos específicos	9
1.3	Estrutura do Trabalho.....	10
2	REFERENCIAL TEÓRICO.....	11
2.1	Redes de Internet.....	11
2.2	O protocolo IPv6.....	14
2.2.1	Cabeçalho IPv6.....	15
2.2.2	Endereçamento.....	19
2.2.3	Tipos de endereços.....	20
2.3	Políticas e Métodos de Alocação e Designação de Endereços.....	21
2.3.1	Alocação de faixas de endereços IPv6 de tamanho apropriado	24
2.3.2	Bits para a criação de um plano de endereçamento IPv6.....	25
2.3.2.1	Alocação sequencial (<i>Rightmost</i>).....	25
2.3.2.2	Alocação reservando sempre o maior espaço possível (<i>Leftmost</i>)	27
2.4	Funcionalidades básicas.....	28
2.4.1	<i>Internet Control Message Protocol version 6</i> (ICMPv6)	29
2.4.2	<i>Neighbor Discovery Protocol</i> (NDP).....	29
2.5	Autoconfiguração.....	30
2.5.1	DHCPv6 (<i>Dynamic Host Configuration Protocol</i>)	31
2.6	Transição IPv4 para IPv6.....	32
2.6.1	Pilha dupla: IPv6 e IPv4 em todos os dispositivos	34
3	METODOLOGIA.....	36
3.1	Tipo de Pesquisa	36
3.2	Cenário avaliado	36
3.3	Métricas Avaliadas.....	37
3.4	Implantação do protocolo IPv6.....	38
3.5	Ferramentas utilizadas.....	38
3.5.1	Simulador dos algoritmos apresentados na RFC3531	38
3.5.2	Aplicativo PING	39
4	RESULTADOS E DISCUSSÕES.....	41

4.1	Divisão da rede IPv6 na UFLA.....	45
4.2	Descrição e segmentação do DCC/UFLA.....	47
4.2.1	Rede do DCC.....	47
4.2.2	Política de segmentação da rede IPv6 no DCC.....	50
4.3	Testes de uso do protocolo IPv6.....	51
5	CONCLUSÃO.....	55
	REFERÊNCIAS BIBLIOGRÁFICAS.....	57
	ANEXO I.....	60

1 INTRODUÇÃO

Para que dois *hosts* se comuniquem entre si é necessário que os mesmos estejam conectados em uma rede e possuam um endereço de rede. A Internet é baseada na conexão de computadores que utilizam endereços IPs (Internet Protocol).

Atualmente, a Internet e as inúmeras redes existentes estão passando por mudanças no modo de endereçamento. Os atuais modos de endereçamentos são baseados no protocolo IP versão 4 que possibilita a criação de aproximadamente 4 bilhões de endereços distintos. Mas, diante da grande demanda de hosts que tem a capacidade de se comunicar na rede, essa quantidade de endereços se esgotou, não permitindo novas alocações de endereços.

Para solucionar a falta de endereço para novos acessos à Internet foi projetado o IPv6 que possui uma quantidade muito maior de endereços, esta quantidade representa aproximadamente 79 octilhões ($7,9 \times 10^{28}$) de vezes a quantidade de endereços IPv4, e representa também mais de 56 octilhões ($5,6 \times 10^{28}$) de endereços por ser humano na Terra (NIC.BR, 2012).

Diante do problema de esgotamento de endereços IPv4 e de que o uso de dispositivos que possuem acesso a rede de Internet está aumentando, a resolução CGI.br/RES/2012/007/P (CGI.BR, 2012) cita que as universidades devem implantar o protocolo IPv6 com urgência. A principal motivação do projeto é a frase “A Internet precisa mudar para continuar crescendo” (NIC.BR, 2012).

O ambiente no qual foi aplicado este trabalho é a rede da Universidade Federal de Lavras situado no município de Lavras MG.

1.1 Objetivo geral

O trabalho tem como objetivo propor a implantação de IPv6 na rede da UFLA, já que atualmente a UFLA possui aproximadamente 16 mil endereços IPv4.

Os estudos foram realizados baseados na análise da rede já em funcionamento. A proposta é de conservar a rede IPv4 já existente e implantar o IPv6 de modo que os dois protocolos operem de maneira nativa. O intuito é manter um cenário no qual coexistam os dois protocolos funcionando juntos, até que, em um futuro, não haja mais a necessidade de utilizar o IPv4.

Durante a realização do projeto foram analisados alguns estudos das boas práticas de implantação do IPv6, com a finalidade levantar pontos críticos para que sejam gerenciados, e desenvolver uma transição de forma natural e transparente para que não haja nenhuma contradição com os usuários da rede.

1.2 Objetivos específicos

- Estudo e levantamento bibliográfico do protocolo IPv6, funcionamento e boas práticas de implantação.
- Levantamento da rede que utiliza IPv4 da universidade, com ênfase no DCC/UFLA.
- Planejamento e segmentação da rede IPv6 da universidade, de acordo com a rede atual e com as boas práticas de implantação.
- Implantação parcial do protocolo IPv6.
- Definição de uma ferramenta para análise e verificação do tempo de resposta para realizar testes e coleta de resultados.

- Verificação da disponibilidade de sites *web* e serviços utilizando o IPv6.

1.3 Estrutura do Trabalho

O trabalho foi estruturado da seguinte maneira. O Capítulo 1 apresenta a síntese do trabalho, os objetivos pretendidos. O Capítulo 2 apresenta todos os conceitos abordados no projeto bem como seus referenciais teóricos. O Capítulo 3 apresenta a metodologia utilizada a fim de atender os objetivos propostos. O Capítulo 4 apresenta os resultados, discussões, informações e a proposta de segmentação da rede IPv6 na UFLA e DCC/UFLA. O Capítulo 5 apresenta a conclusão do trabalho.

2 REFERENCIAL TEÓRICO

A Internet não é de modo algum uma rede, ela é um conjunto de redes diferentes que utilizam diversos protocolos comuns e fornecem determinados serviços comuns. É um sistema pouco usual no sentido de não ter seus serviços centralizados (TANENBAUM, 2011).

A internet pública é uma rede de computadores mundial, isto é, uma rede que interconecta milhares de equipamentos de computação em todo o mundo. O termo redes de computadores está começando a ficar ultrapassado, tendo em vista que a rede hoje interliga além de computadores, muitos equipamentos não tradicionais, todos esses equipamentos são denominados sistemas finais ou hospedeiros (KUROSE e ROSS, 2006).

2.1 Redes de Internet

Em 1966 na Agência de Pesquisas e de Projetos Avançados (ARPA¹) do Departamento de Defesa dos Estados Unidos (DoD²) teve início um projeto de pesquisa para interligar computadores militares e de pesquisa, que recebeu o nome de ARPANET, baseada na comutação de pacotes (COMPUTER HISTORY MUSEUM, 2013).

¹ *Advanced Research Projects Agency*

² *Department of Defence*

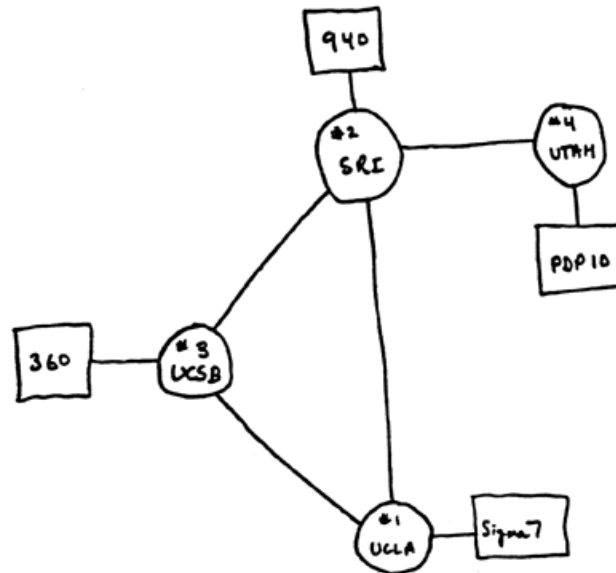


Figura 1 Mapa da ARPANET em 1969

(Fonte: http://www.computerhistory.org/internet_history).

Em 1983, a ARPANET já possuía 562 hosts interligados, trabalhando principalmente sob o protocolo NCP (*Network Control Protocol*), e a partir desta data foi adotado o conjunto de protocolos conhecidos como TCP/IP, o qual permitiu um crescimento ordenado da rede eliminando as restrições dos protocolos anteriores (COMPUTER HISTORY MUSEUM, 2013).

O IP versão 4 definido em setembro de 1981 pela RFC 791 é um dos principais protocolos que sustentam a Internet. A princípio mostrou ser de fácil implantação e interoperabilidade, porém na época de seu projeto, a década de 70, alguns aspectos não foram previstos e que crescentemente vem se tornando problemas, como a necessidade de um número maior de endereços (NIC.BR, 2012). Um desses problemas é o crescimento das redes que gerou o esgotamento dos endereços IP em algumas regiões do mundo (IANA, 2013).

Baseado em um endereçamento de 32 bits, o IPv4 pode gerar mais de 4 bilhões de endereços distintos divididos em três classes principais de tamanho fixo: Classe A, Classe B e Classe C. Ao contrário do que se imaginava, essa classificação mostrou-se muito ineficiente, gerando um grande desperdício de endereços (NIC.BR, 2012).

Para realizar uma distribuição que evite a duplicidade de endereços, existe entidades divididas hierarquicamente conforme ilustrado na Figura 2.

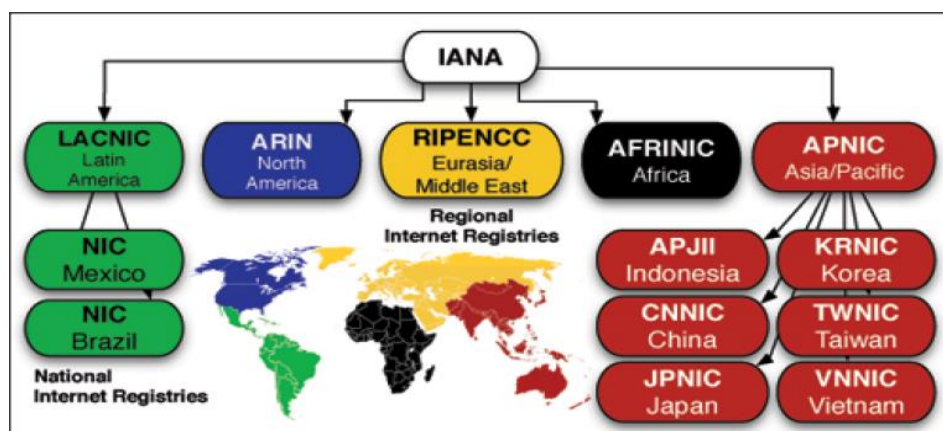


Figura 2 Entidades responsáveis pela distribuição de endereços IP na Internet

(Fonte: <http://caida.org>).

O responsável pela distribuição de endereços na América Latina e Caribe é o LACNIC. Em alguns países há um registro nacional, no Brasil é o NIC.br (Núcleo de informação e Coordenação do Ponto BR).

A seguir são apresentados as características do protocolo IP versão 6 (IPv6).

2.2 O protocolo IPv6

O IPv6 foi desenvolvido principalmente para solucionar o problema do esgotamento do endereçamento da Internet.

Em dezembro de 1993 a IETF (*Internet Engineering Task Force*) definiu a RFC 1550, que consiste na formalização de pesquisas da nova versão do protocolo, requisitando projetos e propostas para o novo protocolo (IETF, 1993). Algumas questões importantes foram definidas durante a elaboração da nova versão do protocolo IP, entre essas questões destacam-se: escalabilidade, segurança, configuração e administração de rede, suporte a QoS (*Quality of Service*), mobilidade, políticas de roteamento e transição (BRADNER e MANKIN, 1993).

Após análises e estudos realizados através de vários projetos, finalmente o IPv6 foi definido em dezembro de 1998 na RFC 2460 pela IETF. O IPv6 traz algumas mudanças importantes como:

- **Maior endereçamento:** O espaço para endereçamento traz agora 128 bits, o IPv4 tem 32 bits de endereçamento, permitindo uma agregação mais específica de endereços.
- **Cabeçalho com formato simplificado:** foi definido um cabeçalho de tamanho único, retirando alguns campos do IPv4, com o intuito de reduzir o processamento nos roteadores.
- **Suporte a cabeçalhos de extensão:** as opções foram retiradas do cabeçalho base e passam a fazer parte de cabeçalhos de extensão, traz uma maior flexibilidade para a introdução de novas opções no futuro.
- **Capacidade de identificar fluxo de dados:** um novo recurso que permite identificar pacotes que pertençam a determinado fluxo,

trazendo a possibilidade de oferecer tratamentos especiais a fluxos específicos.

- **Suporte a autenticação e privacidade:** a partir de cabeçalhos de extensão, o IPv6 pode fornecer suporte a mecanismo de autenticação e garantir a integridade e confiabilidade dos dados transmitidos.

Algumas mudanças são detalhadas a seguir para entendimento do IPv6.

2.2.1 Cabeçalho IPv6

O protocolo IPv4 tem seu cabeçalho com tamanho flexível, podendo ter seu tamanho alterado de 20 bytes até 60 bytes, com a finalidade de fornecer opções, como segurança, roteamento de origem, entre outras. Estas opções tem sido raramente utilizadas e a necessidade de processamento dessas informações pode afetar a performance da rede (HAGEM, 2006).

Algumas mudanças ocorreram no formato do cabeçalho IPv6 retirando alguns campos, e o tornando mais simples. O seu tamanho foi fixado em 40 bytes, e o número de campos foi reduzido para 8 (NIC.BR, 2012). As Figuras 3 e 4 mostram uma comparação entre os cabeçalhos IPv4 e IPv6.

Em relação ao cabeçalho do protocolo anterior, seis campos foram removidos (NIC.BR, 2012):

- **Tamanho do cabeçalho:** como o seu tamanho foi fixado em 40 bytes, este campo perdeu sua função.
- **Identificação, Flags, Deslocamento de Fragmento e Opções e Complementos:** passaram a fazer parte de cabeçalhos de extensão apropriados.

- **Soma de Verificação:** com o objetivo de deixar o protocolo mais eficiente, este campo foi descartado, pois existem outros mecanismos de camadas superiores que realizam outras validações.

Versão (Version)	Tamanho do Cabeçalho (IHL)	Tipo de Serviço (ToS)	Tamanho Total (Total Length)	
Identificação (Identification)		Flags	Deslocamento do Fragmento (Fragment Offset)	
Tempo de Vida (TTL)	Protocolo (Protocol)	Soma de verificação do Cabeçalho (Checksum)		
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				
Opções + Complemento (Options + Padding)				

Figura 3 Cabeçalho IPv4

(Fonte: Apostila IPv6 Básico – NIC.Br).

Versão (Version)	Classe de Tráfego (Traffic Class)	Identificador de Fluxo (Flow Label)		
Tamanho dos Dados (Payload Length)		Próximo Cabeçalho (Next Header)	Limite de Encaminhamento (Hop Limit)	
Endereço de Origem (Source Address)				
Endereço de Destino (Destination Address)				

Figura 4 Cabeçalho IPv6

(Fonte: Apostila IPv6 Básico – NIC.Br).

Alguns campos foram renomeados e reposicionados conforme Tabela 1 (NIC.BR, 2012):

Tabela 1 Renomeação dos campos do protocolo IPv6 – NIC.BR

IPv4	IPv6
Tipo de Serviço	Classe de serviço
Tamanho Total	Tamanho dos Dados
Tempo de Vida (TTL)	Limite de Encaminhamento
Próximo Protocolo	Cabeçalho

O campo “Identificador de Fluxo” foi adicionado, oferecendo suporte ao funcionamento de mecanismos extras de QoS.

Com um cabeçalho mais simples e um processamento mais rápido pelos nós intermediários, o IPv6 possui uma nova capacidade de lidar com as opções chamadas de cabeçalhos de extensão (HAGEM, 2006). Seis destes cabeçalhos foram definidos na especificação do IPv6 (DEERING e HINDEN, 1998):

- **Hop-by-hop:** este cabeçalho se localiza na primeira posição da cadeia de cabeçalhos, sendo analisado por todos os nós intermediários até o destino, tem opções como ignorar e continuar o processamento, e descartar o pacote. Existem dois tipos de *hop-by-hop*: *Router Alert* e *Jumbogram*.
- **Destination Options:** é processado apenas pelo destino do pacote, oferecendo suporte ao mecanismo de mobilidade IPv6 e contém o endereço de destino do nó móvel.

- **Routing:** desenvolvido para listar um ou mais nós intermediários que deveriam ser visitados até o pacote chegar ao destino final. Devido a problemas de segurança, esta função se tornou obsoleta na RFC5095.
- **Fragmentation:** este cabeçalho é utilizado quando o o tamanho do pacote IPv6 é maior que o *MTU* dos roteadores do caminho. Não existe a fragmentação dos pacotes pelos roteadores, os pacotes são fragmentados apenas na origem.
- **Authentication Header e Encapsulating Security Payload:** fazem parte do *IPSec* que tem a finalidade de tentar garantir a segurança em redes de comunicação de dados.

Os cabeçalhos de extensão são adicionados em série, formando uma cadeia de cabeçalhos, a Figura 5 ilustra seu funcionamento.

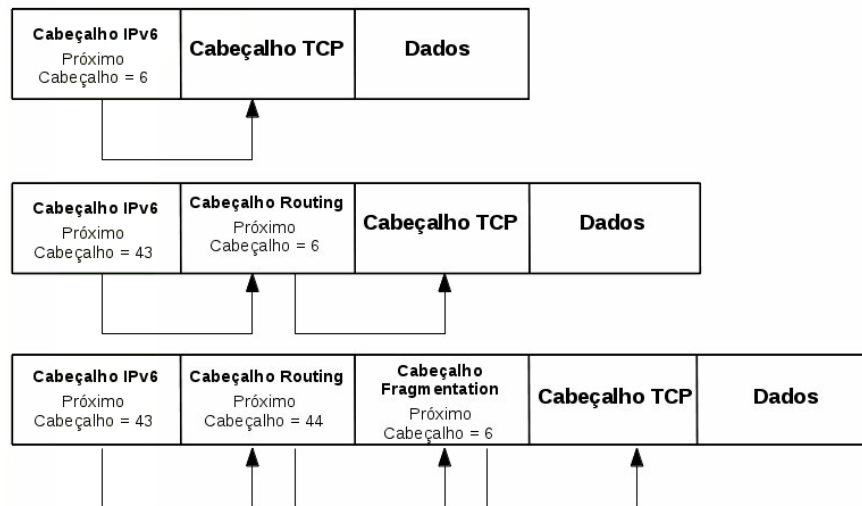


Figura 5 Funcionamento do cabeçalho de extensão

(Fonte: Apostila IPv6 Básico – NIC.Br).

Para o bom funcionamento dos cabeçalhos de extensão, deve-se observar a ordem em que eles são enviados, os cabeçalhos de relevância para todos os nós da rede devem ser enviados antes dos de relevância apenas para o destino final. A vantagem é que os nós intermediários ao localizar um cabeçalho com informações exclusivas do endereço de destino, interrompe a análise dos próximos pacotes, economizando processamento (NIC.BR, 2012).

2.2.2 Endereçamento

Ampliar o espaço de endereçamento e otimizar tabelas de roteamento foram algumas das principais razões para o desenvolvimento do IPv6. A arquitetura de endereçamento IPv6 foi definida na RFC2373 (HAGEM, 2006).

O IPv6 possui um endereçamento de 128 bits, possibilitando um número máximo de 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços, representando aproximadamente 79 octilhões de vezes a quantidade de endereços IPv4, e aproximadamente 56 octilhões de endereços por ser humanos na terra (NIC.BR, 2012).

O endereço IPv6 é representado dividido em 8 grupos de 16 bits, separados pelo caractere “:”, escritos com dígitos hexadecimais (NIC.BR, 2012), como por exemplo:

- 2001:0db8:ca5a:cafe:dad0:face:b00c:0001
- 2001:db8::1.

Definido na RFC 4632, a ideia do CIDR é o fim do uso de classes de endereços, permitindo a alocação de blocos de tamanho apropriado a real necessidade de cada rede. Utilizada atualmente no IPv4, esta representação possibilita a agregação dos endereços de forma hierárquica, permitindo a

identificação da topologia da rede. Com isso, é possível diminuir o tamanho da tabela de roteamento e agilizar o encaminhamento dos pacotes (NIC.BR, 2012).

O IPv6 utiliza a notação CIDR da seguinte forma “endereço ip/tamanho do prefixo”, por exemplo o IP 2001:db8::/32.

É importante ressaltar que endereço 2001:db8::/32 é utilizado para fins de documentação, portanto não deve ser divulgado e nem roteável na Internet global (NIC.BR, 2012).

2.2.3 Tipos de endereços

O IPv4 possui endereços do tipo *unicast*, *broadcast* e *multicast*. O IPv6 não utiliza endereços do tipo *broadcast*, pois esse tipo de endereço apresenta alguns problemas de transmissão na maioria das redes. Um novo tipo de endereço IPv6 foi adicionado, definido na RFC1546, os endereços tipo *anycast* (HAGEM, 2006). Dessa forma os endereços IPv6 são divididos em três categorias (NIC.BR, 2012):

- ***Unicast***: Identifica uma única interface na rede, um pacote encaminhado a um endereço *unicast* é entregue a apenas uma interface na rede.
- ***Anycast***: Identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue a interface pertencente a este conjunto mais próxima da origem.
- ***Multicast***: Identifica um conjunto de interfaces, um pacote enviado a um endereço *multicast* é entregue a todas interfaces associadas a esse endereço. Esses endereços derivam do bloco FF00::/8, e não devem ser utilizados como endereços de origem de um pacote.

O endereço *unicast* pode ser especificado em alguns tipos como: *Global Unicast*, *Unique-Local*, e *Link-Local* (NIC.BR, 2012):

- ***Global Unicast***: Composto por aproximadamente 13% do total de IPv6 possíveis, o global *unicast* são os endereços globalmente roteáveis, acessíveis na Internet IPv6, assim como os IPv4 públicos. Atualmente reservada a faixa de endereços IPv6 2000::/3, corresponde a 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
- ***Link Local***: pode ser utilizado apenas no enlace onde a interface está conectada, utiliza alguns algoritmos para gerar um endereço IPv6 a partir do prefixo FE80::/64, o principal algoritmo utilizado é o IEEE EUI-64.
- ***Unique Local Address (ULA)***: Utilizado apenas para comunicações locais, o ULA não deve ser roteável na internet global. O seu prefixo é FC00::/7. Sua utilização permite que qualquer enlace possua uma rede /48 privada, e único globalmente, assim caso duas redes de empresas distintas sejam interconectadas, provavelmente não haverá conflito de endereços. Um endereço ULA utiliza um algoritmo para sua alocação, com isso possui uma grande possibilidade de ser globalmente único.

2.3 Políticas e Métodos de Alocação e Designação de Endereços

A criação de uma boa política de endereçamento IP é essencial dentro de uma rede, tornando necessário um planejamento para um controle sobre as alocações de blocos apropriados para cada tipo de serviço, ou setor, planejando o uso futuro e eventual expansão da rede. O desperdício inicial na distribuição dos blocos IPv4 é uma das causas do seu esgotamento. Segundo MOREIRAS (2011),

a alocação de grandes blocos IPv6 é vista por muitos como um risco do mesmo esgotamento ocorrer.

Não se pode prever de maneira precisa como a internet vai evoluir, pode ser considerado como conservadorismo entregar e reservar endereços IPv6 com certa abundância (MOREIRAS, 2011).

Um bom plano de alocação de endereços deve seguir quatro princípios básicos: singularidade, registro, agregação e conservação. Isso pode ser chamado de boas práticas de endereçamento IPv6 (NIC.BR, 2012):

- **Singularidade:** cada bloco distribuído e/ou alocado deve ser único globalmente.
- **Registro:** o espaço de endereçamento tem que estar registrado na base de um RIR³ e as informações pertinentes ao registro devem ser acessíveis.
- **Agregação:** sempre que possível distribuir os endereços de maneira hierárquica dentro da topologia. As políticas de endereçamentos devem evitar fragmentação.
- **Conservação:** Mesmo com a grande quantidade de endereços deve-se evitar o uso de práticas que favoreçam o desperdício de endereços.

Algumas medidas se fazem necessárias em uma rede de Internet para evitar que seus usuários, intencionalmente ou não, enviem na rede pacotes com origens inválidas. Esse procedimento, chamado de *Spoofing*, muitas vezes é utilizado para ataque de negação de serviços. A criação de um filtro *antispoofing* é tratada também como boas práticas para Internet

Apenas um filtro é eficaz para manter uma boa administração da rede, deve ser aplicado no roteador, na interface que liga a rede interna da universidade, é eficaz contra isso.

³ *Regional Internet Registry* – Registro Regional da Internet

O Portal de boas práticas para a Internet no Brasil⁴ traz as configurações a serem realizadas em roteadores para configuração com endereçamento IPv6 (NIC.BR). Isso filtra endereços que não são globalmente roteáveis.

O Anexo I traz exemplo de configuração de filtro *antispoofing* a ser realizada em roteadores Juniper, que é o roteador utilizado atualmente pela UFLA.

A RFC2373 designa 2000::/3 como espaço de endereçamento *global unicast* a ser alocado pela IANA para os Registros Internet Regionais.

Os endereços IPv6 são distribuídos hierarquicamente do seguinte modo (NIC.BR, 2012):

- A IANA fornece para um RIR um bloco /12 IPv6.
- O LACNIC, responsável pela América Latina possui o endereço 2800::/12 reservado.
- O Brasil possui um endereço /16 que faz parte do /12 do LACNIC.

O NIC.BR que é responsável pela alocação de endereços IP no Brasil, e segue o padrão de alocação mínima de um bloco /32 para cada ISP⁵ (*Internet Service Provider*), podendo ser feita uma alocação maior, mediante a justificativa de alocação (NIC.BR, 2012).

É importante ressaltar a forma em que a utilização da rede é medida. Diferentemente do IPv4, a utilização de IPv6 é medida em relação ao número de blocos de endereços designado a usuários finais, e não em relação ao número de endereços designados.

⁴ www.bcp.nic.br

⁵ Provedor de Internet

2.3.1 Alocação de faixas de endereços IPv6 de tamanho apropriado

Em setembro de 2001 foi publicada a RFC3177 com recomendações sobre alocações de endereços IPv6. Segundo a RFC deve se designar blocos de endereços /48 nos casos gerais, exceto quando for um cliente muito grande, blocos /64 quando souber que uma e apenas uma sub-rede é necessária, e um endereço /128 quando for absolutamente sabido que um e apenas um equipamento estará conectado (IETF, 2001).

Em maio de 2011 foi publicada a RFC6177, com novas recomendações sobre alocações de endereços IPv6, esta RFC indica que corresponde ao operador da rede decidir qual prefixo designar a seus clientes. Mesmo assim, há uma indicação de que prefixos /64 devem ser designados apenas quando tiver certeza de que não é necessária mais de uma sub-rede. E que para os casos em geral seja designada, por exemplo, um bloco /56. (IETF, 2011).

A RFC3177 teve algumas críticas principalmente em relação ao desperdício dos endereços, já que, segundo sua recomendação, uma empresa grande com muitos trabalhadores poderia receber a mesma quantidade de IP que um usuário residencial (PATARA, 2012). Contudo, o Núcleo de Informação e Coordenação do Ponto BR, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil, faz as seguintes recomendações (MOREIRAS, 2011):

- Blocos /48 ou mais para usuários corporativos, recomenda-se reservar um /44 e alocar um /48.
- Blocos /56 ou mais para usuários SOHO⁶, recomenda-se reservar um /52 e alocar um /56.

⁶ *Small Office/ Home Office* – Redes domésticas e de pequenos escritórios.

- Blocos /64 ou mais para usuários domésticos, recomenda-se reservar um /56 e alocar algo maior ou igual a /64

Sempre que possível, o espaço de endereçamento deve ser alocado de uma forma hierárquica, de acordo com a topologia da infraestrutura da rede. Isto é, necessário para permitir uma agregação de informação de roteamento pelos ISP, e para limitar a expansão da tabela de roteamento da Internet. Políticas de endereçamento IPv6 devem procurar evitar fragmentação dos espaços de endereçamento (LACNIC, 2012).

2.3.2 Bits para a criação de um plano de endereçamento IPv6

A RFC3531 propõe três métodos para ordenar a distribuição de endereços e blocos IP. Este trabalho irá abordar os dois principais, a alocação sequencial (*rightmost*), e a alocação com intuito de reservar sempre o maior espaço disponível (*leftmost*).

2.3.2.1 Alocação sequencial (*Rightmost*)

É o método adequado quando se tem certeza de que não é necessário espaço para expansão, como por exemplo, para enumerar *hosts* de uma rede. O método consiste em variar os bits da direita para criar uma distribuição de endereços sequencial. A Figura 6 mostra a variação de 4 bits para a formação de 16 subredes utilizando a técnica *rightmost* a partir do simulador da RFC3531 (CEPTRO.BR, 2013).

Utilizando a distribuição *rightmost* foi dividido a rede 2001:db8::/32 em 16 subredes, mostrando o resultado de uma alocação sequencial conforme Figura 7. Pode-se notar que as subredes foram alocadas em sequência hexadecimal de 0 a f.

Passo Espaco	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Passo Bits	4	3	2	1
1	1																1	0	0	0	0
2	1	2															2	0	0	0	1
3	1	2	3														3	0	0	1	0
4	1	2	3	4													4	0	0	1	1
5	1	2	3	4	5												5	0	1	0	0
6	1	2	3	4	5	6											6	0	1	0	1
7	1	2	3	4	5	6	7										7	0	1	1	0
8	1	2	3	4	5	6	7	8									8	0	1	1	1
9	1	2	3	4	5	6	7	8	9								9	1	0	0	0
10	1	2	3	4	5	6	7	8	9	10							10	1	0	0	1
11	1	2	3	4	5	6	7	8	9	10	11						11	1	0	1	0
12	1	2	3	4	5	6	7	8	9	10	11	12					12	1	0	1	1
13	1	2	3	4	5	6	7	8	9	10	11	12	13				13	1	1	0	0
14	1	2	3	4	5	6	7	8	9	10	11	12	13	14			14	1	1	0	1
15	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		15	1	1	1	0
16	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	16	1	1	1	1

Figura 6 Alocação *Rightmost*(Fonte: <http://ipv6.br/rfc3531demo/>).

Passo	Endereco IPv6
1	2001:db8:0000::/36
2	2001:db8:1000::/36
3	2001:db8:2000::/36
4	2001:db8:3000::/36
5	2001:db8:4000::/36
6	2001:db8:5000::/36
7	2001:db8:6000::/36
8	2001:db8:7000::/36
9	2001:db8:8000::/36
10	2001:db8:9000::/36
11	2001:db8:a000::/36
12	2001:db8:b000::/36
13	2001:db8:c000::/36
14	2001:db8:d000::/36
15	2001:db8:e000::/36
16	2001:db8:f000::/36

Figura 7 Divisão de uma rede /32 em 16 subredes utilizando *rightmost*(Fonte: <http://ipv6.br/rfc3531demo/>).

2.3.2.2 Alocação reservando sempre o maior espaço possível (Leftmost)

Este método equivale a contar variando os bits mais à esquerda, tendo como propriedade garantir endereços ou blocos livres para expansão, reservando sempre o maior espaço disponível. Além disso permite uma distribuição mais homogênea.

A Figura 8 mostra a variação de 4 bits começando pela esquerda e sequência em que cada subrede é alocada dentro do espaço.

Passo/ Espaco	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	Passo/ Bits	4	3	2	1
1	1																1	0	0	0	0
2	1								2								2	1	0	0	0
3	1				3				2								3	0	1	0	0
4	1				3				2					4			4	1	1	0	0
5	1		5		3				2					4			5	0	0	1	0
6	1		5		3				2		6			4			6	1	0	1	0
7	1		5		3		7		2		6			4			7	0	1	1	0
8	1		5		3		7		2		6			4		8	8	1	1	1	0
9	1	9	5		3		7		2		6			4		8	9	0	0	0	1
10	1	9	5		3		7		2	10	6			4		8	10	1	0	0	1
11	1	9	5		3		11	7		2	10	6			4		11	0	1	0	1
12	1	9	5		3		11	7		2	10	6			4	12	12	1	1	0	1
13	1	9	5	13	3		11	7		2	10	6			4	12	13	0	0	1	1
14	1	9	5	13	3		11	7		2	10	6	14	4		12	14	1	0	1	1
15	1	9	5	13	3		11	7	15	2	10	6	14	4	12	8	15	0	1	1	1
16	1	9	5	13	3		11	7	15	2	10	6	14	4	12	8	16	1	1	1	1

Figura 8 Alocação *Leftmost*

(Fonte: <http://ipv6.br/rfc3531demo/>).

Utilizando a distribuição *leftmost* foi dividido a rede 2001:db8::/32 em 16 subredes, mostrando o resultado de uma alocação reservando sempre o maior

espaço possível conforme Figura 9. Pode-se notar que as subredes foram alocadas reservando o maior espaço quando possível (nas primeiras alocações).

Passo	Endereço IPv6
1	2001:db8:0000::/36
2	2001:db8:8000::/36
3	2001:db8:4000::/36
4	2001:db8:c000::/36
5	2001:db8:2000::/36
6	2001:db8:a000::/36
7	2001:db8:6000::/36
8	2001:db8:e000::/36
9	2001:db8:1000::/36
10	2001:db8:9000::/36
11	2001:db8:5000::/36
12	2001:db8:d000::/36
13	2001:db8:3000::/36
14	2001:db8:b000::/36
15	2001:db8:7000::/36
16	2001:db8:f000::/36

Figura 9 Divisão de uma rede /32 em 16 subredes utilizando *leftmost*

(Fonte: <http://ipv6.br/rfc3531demo/>).

2.4 Funcionalidades básicas

Este tópico abordará algumas funcionalidades básicas do IPv6, como o mecanismo de descoberta de vizinhança, a importância das mensagens ICMPv6, e o mecanismo de autoconfiguração de endereços *stateless* e *stateful*.

2.4.1 *Internet Control Message Protocol version 6 (ICMPv6)*

O ICMPv6 engloba todas as funções de seu antecessor o ICMPv4, como reportar erros no processamento de pacotes, realizar diagnósticos e enviar mensagens com finalidade de informar características da rede. O ICMPv6 também assume o papel de funções isoladas no IPv4, como o ARP (*Address Resolution Protocol*) que tem como objetivo mapear endereços físicos através de endereços lógicos, o RARP (*Reverse Address Resolution Protocol*) faz a função inversa do ARP, o IGMP (*Internet Group Management Protocol*) gerencia membros de grupo *multicast* (NIC.BR, 2012).

Os pacotes ICMPv6 são encapsulados nos pacotes IPv6. Deve-se ter uma atenção extra com os *firewalls* que operam na camada de rede, já que podem bloquear funções básicas como a descoberta de vizinhos e a autoconfiguração. O ICMPv6 é mais importante para o funcionamento do IPv6 do que o ICMP para o IPv4, pois todas as interações (NDP) entre vizinhos são realizadas através dele.

2.4.2 *Neighbor Discovery Protocol (NDP)*

O NDP atua sobre dois aspectos primordiais da comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes. Sua finalidade é resolver problemas de interação de nós vizinhos de uma rede. O NDP foi construído com base nas seguintes mensagens ICMPv6 para a realização de tarefas (NIC.BR, 2012).

- ***Router Solicitation (RS)***: Solicita que roteadores de rede informem sua presença. Esta mensagem é gerada quando se tem

uma necessidade instantânea das informações. A mensagem RS é enviada ao grupo *multicast all routers* (FE02::2).

- **Router Advertisement (RA):** Enviada por roteadores, a mensagem RA é enviada periodicamente ou em resposta a uma mensagem RS, utilizada para um roteador anunciar sua presença dentro de um enlace. O destino da mensagem depende do motivo que originou a mensagem. Quando é enviada periodicamente, o endereço é o grupo *multicast all-nodes* (FF02::1), caso seja em resposta a um RS, o endereço de destino será o endereço de origem do RS que é um *unicast link local*.
- **Neighbor Solicitation (NS):** É uma mensagem para solicitar que um vizinho se apresente imediatamente através de uma resposta *Neighbor advertisement*. Possui três funções básicas: detectar endereços duplicados na vizinhança, ter acessibilidade aos vizinhos do enlace e descobrir um endereço físico através de um endereço lógico.
- **Neighbor advertisement:** Enviada em resposta a um NS, ou para anunciar alguma alteração nas características de algum dispositivos de rede.
- **Redirect:** É utilizada pelo roteador para informar uma rota mais favorável para a comunicação com determinado destino.

2.5 Autoconfiguração

Hoje existe uma grande diversidade de dispositivos de redes, em um futuro breve virá a existir uma quantidade ainda maior. Para facilitar a configuração destes dispositivos, o IPv6 traz mecanismos de autoconfiguração de endereços, podendo facilitar a configuração de endereços para os administradores de rede.

No IPv6, o processo de autoconfiguração é uma das principais características de seu funcionamento básico. É a partir dele que os diversos dispositivos podem adquirir informações da rede (e.g. servidores NTP), do enlace (e.g. prefixos pertencentes ao enlace) e de endereçamento. Isso faz com que a Internet ganhe dinamismo, visto que permite dispositivos se interconectarem sem a necessidade de configurações manuais (NIC.BR, 2012, p. 72).

O IPv6 foi projetado para que não seja mais necessário configurar os hosts manualmente ao conectá-los na rede. Os recursos de autoconfiguração do IPv6 é uma característica chave do protocolo, quando todos os dispositivos como TVs, geladeiras, DVD *players*, telefones móveis, estiverem disponíveis para acesso a rede através do protocolo IP, desfaz a necessidade que os usuários finais tenham que se conectar a um servidor DHCP (HAGEM, 2006).

Existem duas maneiras para a realização de autoconfiguração: não orientada a estado (*stateless*) e orientada a estado (*stateful*) (NIC.BR, 2012). Na configuração *stateless* o dispositivo que fornece as informações para a configuração não mantém registro do estado e das características do nó destinatário. Na configuração *stateful* o dispositivo que fornece as informações para a configuração mantém registro do estado e das características do nó destinatário, um exemplo de mecanismo que atua com configuração *stateful* é o DHCPv6.

2.5.1 DHCPv6 (*Dynamic Host Configuration Protocol*)

O DHCPv6 realiza configuração dinâmica de endereços *stateful*, sua função é tanto distribuir endereços IPv6 quanto divulgar informações da rede. O DHCPv6

é bem parecido com o DHCP da versão IPv4, porém eles não são compatíveis entre si, atuando de maneira independente. Uma diferença a se destacar é o *prefix delegation* essa funcionalidade foi desenvolvida para o DHCPv6, e serve para distribuir prefixos de rede para roteadores (NIC.BR, 2012).

2.6 Transição IPv4 para IPv6

O fato de o IPv4 e o IPv6 não serem diretamente compatíveis entre si, aumenta a importância da escolha de uma técnica de transição adequada. Embora não interoperem, ambos podem funcionar simultaneamente nos mesmos dispositivos, possibilitando uma transição de forma gradual (NIC.BR, 2012).

Várias técnicas de transição foram desenvolvidas e podem ser citadas como: pilha dupla, 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. Existem algumas técnicas já em desuso, como 6to4, Teredo e ISATAP, mas com as quais ainda se convive no ambiente da Internet ou outras redes, principalmente por serem usadas de forma automática por alguns sistemas operacionais e equipamentos (NIC.BR, 2012).

O fato de a UFLA possuir uma quantidade suficiente de endereços IPv4 públicos para suprir suas necessidades, faz com que a técnica de transição abordada e utilizada durante este trabalho seja a pilha dupla.

O Brasil possui um cronograma mostrado na Figura 10 para ser utilizado como referência na implantação do IPv6 no país. Este cronograma foi criado com base no diálogo entre o Comitê Gestor da Internet no Brasil (CGI.br) e vários provedores de acesso, serviços e operadoras de telecomunicações, em diversas reuniões ao longo dos anos de 2011 e 2012 (NIC.BR, 2012).

Em primeiro lugar os provedores de trânsito Internet (as grandes operadoras de telecomunicações e Sistemas Autônomos em geral que oferecem trânsito para outros ASes) devem preparar-se.

“Uma vez que os provedores de serviços e companhias em geral tenham como conseguir conectividade Internet, os serviços (sites em geral, comércio eletrônico, bancos, governos, etc.) devem migrar para IPv6. Essa migração deve ser feita rapidamente. Quanto mais rápida e efetiva for essa migração, melhor será para todos: os sites não terão o risco de perderem audiência, ou terem usuários que os acessarão com potenciais problemas, e os provedores de acesso terão menos motivos para utilizarem o compartilhamento de IPv4 numa fase de transição (NIC.BR, 2012, p. 19).”

“Por fim os provedores de acesso devem fazer chegar o IPv6 aos usuários domésticos. Primeiro aos novos usuários, e depois aqueles já conectados à Internet via IPv4 (NIC.BR, 2012, p. 19).”

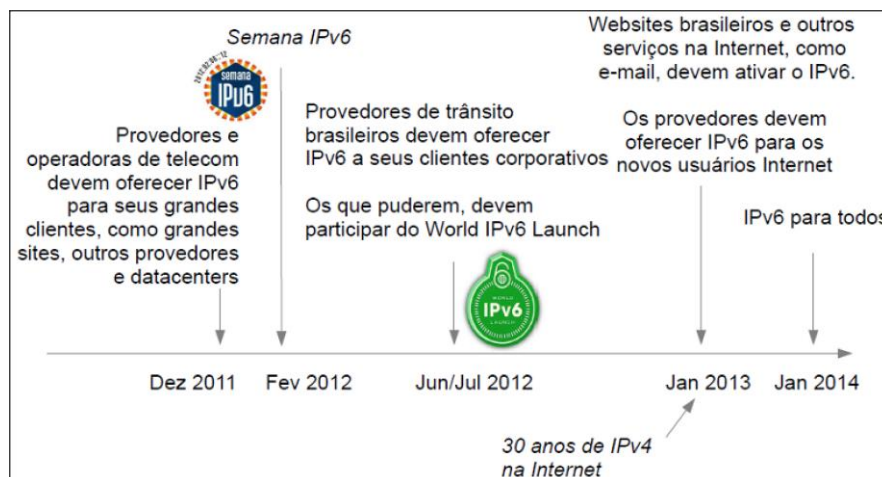


Figura 10 Cronograma Brasileiro de migração para o IPv6

(Fonte: Apostila IPv6 Básico – NIC.Br).

Baseado no cronograma criado, o Comitê Gestor da Internet no Brasil faz várias recomendações, através da “Resolução CGI.br/RES/2012/007/P – Recomendação para Implantação do Protocolo IPv6”. Entre várias recomendações pode-se destacar – “...que as universidades e centros de pesquisa, em especial os relacionados às disciplinas de redes, computação e Internet, implantem o IPv6 em suas redes com urgência.” (CGI.BR, 2012).

A necessidade de transição vem a cada dia mostrando ser de grande importância, e mesmo assim apenas 4,51% da Internet hoje é acessada em IPv6 (GOOGLE, 2014).

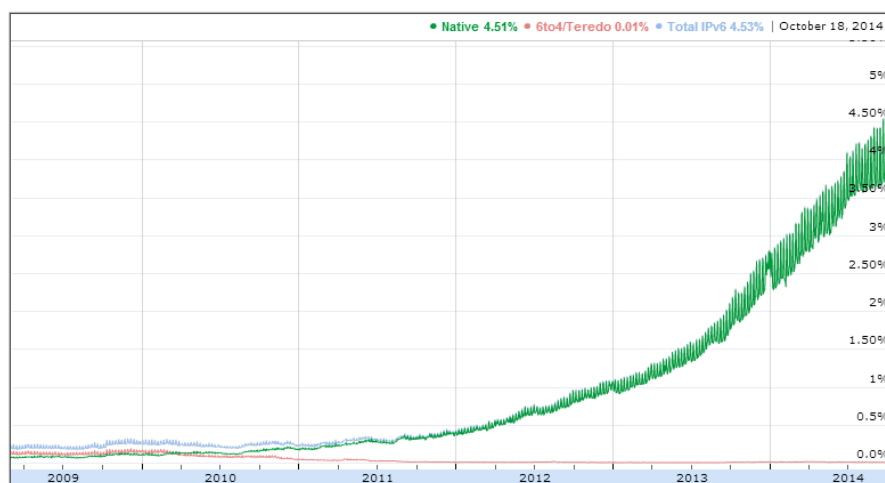


Figura 11 Porcentagem de acesso ao Google utilizando IPv6(Fonte: <http://www.google.com/intl/pt-BR/ipv6/statistics.html>).

2.6.1 Pilha dupla: IPv6 e IPv4 em todos os dispositivos

Visto que muitos serviços e dispositivos na Internet ainda trabalham somente com IPv4, é importante manter o IPv4 já existente funcionando de

maneira estável e implantar nativamente o IPv6. Os equipamentos devem possuir ambos os protocolos em funcionamento. A utilização deste método permite que dispositivos e roteadores tenham a capacidade de se comunicarem utilizando os dois protocolos (NIC.BR, 2012).

Isto faz com que um nó pilha dupla, para se comunicar com um nó IPv6, se comportará como um nó IPv6, para se comunicar com um nó IPv4 se comportará como um nó IPv4 (NIC.BR, 2012).

Uma vantagem de utilizar o método pilha dupla é a possibilidade de realizar uma implementação gradual, podendo configurar pequenas sessões do enlace uma de cada vez (NIC.BR, 2012).

Algumas mudanças na estrutura da rede são necessárias para a utilização deste método, uma estruturação no serviço DNS, configuração dos protocolos de roteamento e de *firewall* (NIC.BR, 2012).

O funcionamento da pilha dupla está ilustrado na Figura 12.

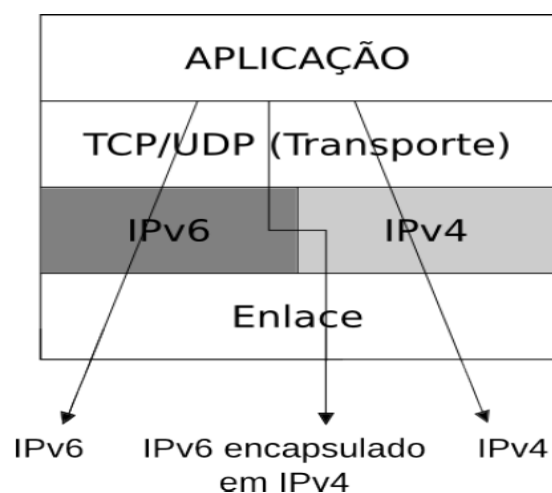


Figura 12 Funcionamento da pilha dupla
(Fonte: Apostila IPv6 Básico – NIC.Br).

3 METODOLOGIA

Este capítulo descreve a metodologia utilizada no trabalho, a fim de possibilitar o alcance dos objetivos da pesquisa. Na primeira seção será apresentada a classificação da pesquisa quanto à natureza, ao objetivo e aos procedimentos. Em seguida serão descritos os procedimentos metodológicos.

3.1 Tipo de Pesquisa

Segundo JUNG (2004) a pesquisa deste trabalho é caracterizada como experimental e qualitativa.

O tipo de pesquisa experimental se faz necessária para a obtenção de resultados relevantes sobre a implantação do novo protocolo IPv6.

As Pesquisas Qualitativas são experimentais e se caracterizam pela manipulação direta do objeto de estudo. O objetivo principal é interferir na realidade com a finalidade de observar o que acontece.

As pesquisas foram aplicadas a fim de seguir as recomendações propostas pelo Comitê Gestor da Internet no Brasil (CGI.BR), e através do entendimento do funcionamento do protocolo IPv6, da análise de técnicas de transição e de endereçamento utilizado como premissas os referenciais citados. Através de um planejamento realizado tendo como base a topologia atual da rede de computadores interna da UFLA.

3.2 Cenário avaliado

Foi realizada uma pesquisa na Diretoria de Gestão de Tecnologia da Informação da UFLA (DGTI – UFLA), a fim de se obter informações sobre dados

da rede interna, políticas de endereçamento, quantidade de sub-redes, disponibilidade de recursos, e disponibilidade para implantação do protocolo IPv6.

Para um estudo mais detalhado da rede, foi analisado a distribuição da rede dentro do Departamento de Ciência da Computação que possui uma estrutura de rede complexa. A análise do DCC irá contribuir para uma análise mais profunda, e pode ser utilizada como exemplo para outros setores.

Como o ambiente onde se deseja implementar o IPv6 é único – a Rede Institucional da Universidade Federal de Lavras, a pesquisa se dará através de um diagnóstico do ambiente, visando a criação de um projeto com maior aderência a este ambiente. De qualquer forma, foram verificados alguns casos de implementação de IPv6, buscando analisar o que as tornou bem sucedidas ou fracassadas. Esse estudo buscou, principalmente, evitar problemas conhecidos que inviabilizem a implementação no ambiente proposto.

Para a realização de testes a DGTI disponibilizou dentro do DCC um ponto de acesso com IPv6 já implantado. Este ponto foi habilitado na sala 02-18, e possui tanto endereço IPv4 e IPv6 funcionando em pilha dupla.

3.3 Métricas Avaliadas

Foram consideradas duas métricas, latência utilizando aplicativo PING e número médio de dispositivos que utilizam a rede simultaneamente através de estatísticas disponível no firewall.

Com IPv6 habilitado em um ponto foi verificado da disponibilidade de acesso dos sites mundiais mais acessados no Brasil, e também o tempo de resposta em milissegundos a uma requisição utilizando tanto o protocolo IPv6 quanto o IPv4 para comparação.

Foi realizado um levantamento no Departamento de Ciência da Computação onde foi verificado a quantidade de pontos de redes disponíveis, e como estes pontos são utilizados, como impressoras, desktops, servidores, etc.

3.4 Implantação do protocolo IPv6

Baseado no projeto este trabalho buscou realizar uma segmentação da rede utilizando IPv6 implantar o protocolo IPv6 funcionando em pilha dupla com o protocolo IPv4, ambos de maneira nativa em um ambiente de testes na rede da UFLA.

Após a análise dos resultados, foi criada uma divisão total da rede da UFLA tomando como base políticas de alocação de endereços, além de boas práticas de endereçamento, para a elaboração da proposta de divisão da rede IPv6 na UFLA.

3.5 Ferramentas utilizadas

Foram utilizadas duas ferramentas para o desenvolvimento do trabalho, um simulador de algoritmos e o aplicativo PING.

3.5.1 Simulador dos algoritmos apresentados na RFC3531

O simulador divide os blocos na quantidade de subredes desejada, e mostra a ordem em que deverá ser alocadas, segundo o algoritmo escolhido. Disponível no site IPv6.br/rfc3531demo/

Simulação RFC 3531

Digite o endereço IPv4:

Digite o endereço IPv6:

Rightmost Leftmost Centermost

Numero de subnets a serem criadas:

Passo	00	01	02	03	04	05	06	07	Passo	3	2	1
1	1								1	0	0	0
2	1				2				2	1	0	0
3	1		3		2				3	0	1	0
4	1		3		2			4	4	1	1	0
5	1	5	3		2			4	5	0	0	1
6	1	5	3		2	6		4	6	1	0	1
7	1	5	3	7	2	6		4	7	0	1	1
8	1	5	3	7	2	6	4	8	8	1	1	1

Passo	Endereço IPv6	Passo	Endereço IPv4
1	2001:db8:0000::/35	1	192.0.2.0/27
2	2001:db8:8000::/35	2	192.0.2.128/27
3	2001:db8:4000::/35	3	192.0.2.64/27
4	2001:db8:c000::/35	4	192.0.2.192/27
5	2001:db8:2000::/35	5	192.0.2.32/27
6	2001:db8:a000::/35	6	192.0.2.160/27
7	2001:db8:6000::/35	7	192.0.2.96/27
8	2001:db8:e000::/35	8	192.0.2.224/27

Figura 13 Simulador RFC 3531

(Fonte: <http://ipv6.br/rfc3531demo/>).

3.5.2 Aplicativo PING

PING é um utilitário que usa o protocolo ICMP para testar a conectividade entre equipamentos. É um comando disponível praticamente em todos os sistemas operacionais. Seu funcionamento consiste no envio de pacotes para o equipamento de destino e na escuta das respostas. Se o equipamento de destino

estiver ativo, uma resposta é devolvida ao computador solicitante. Foi avaliado o tempo de resposta com os dois protocolos.

A rede da Universidade Federal de Lavras foi utilizada como estudo de caso para a segmentação e implantação do IPv6, e para detalhar o trabalho foi aprofundado o trabalho no Departamento de Ciência da Computação. A Seção a seguir apresenta resultados e discussões do levantamento, segmentação e testes realizados.

4 RESULTADOS E DISCUSSÕES

A rede institucional da UFLA é ligada ao POP MG (Ponto de Presença da RNP em Minas Gerais) através de dois *links* de 160 Mbps totalizando 320 Mbps. A universidade possui aproximadamente 12.000 dispositivos que utilizam a internet, e em média, possui cerca de 5.500 usuários simultâneos durante os turnos da manhã e tarde.

A UFLA possui a faixa de endereços IPv4 177.105.0.0/18 e a faixa de endereços IPv6 2801:a6::/32, além de utilizar a faixa IPv4 200.131.250.0/24 pertencente ao AS1916 Rede Nacional de Pesquisa (RNP). A rede funciona nativamente em IPv4, entregando um endereço público para todos os dispositivos, com exceção da rede sem fio. De todos endereços IPv4 que a UFLA possui (16.256 endereços) apenas 23% ainda não estão alocados.

A universidade estabeleceu que sua topologia seja do tipo estrela como mostra a Figura 14. Essa topologia utiliza um nó central para gerenciar a comunicação entre as máquinas. A existência de um nó central pode causar falha em todos os elementos da rede, os demais nós em falhas não prejudicam os outros. Por esse motivo, nessa posição geralmente são utilizados processadores em duplicidade, redundância, para garantir confiabilidade para o sistema (MORAES e CASTRUCCI, 2007).

Adotando a tecnologia de VLAN (Virtual Local Area Network), a rede da universidade é separada virtualmente por Zonas denominadas Servidores, Departamentos, Administrativa, Terceiros, Multimídia e Faixa Livre. Cada departamento tem sua rede local, mas existe uma subdivisão interna separando em rede acadêmica e rede administrativa.

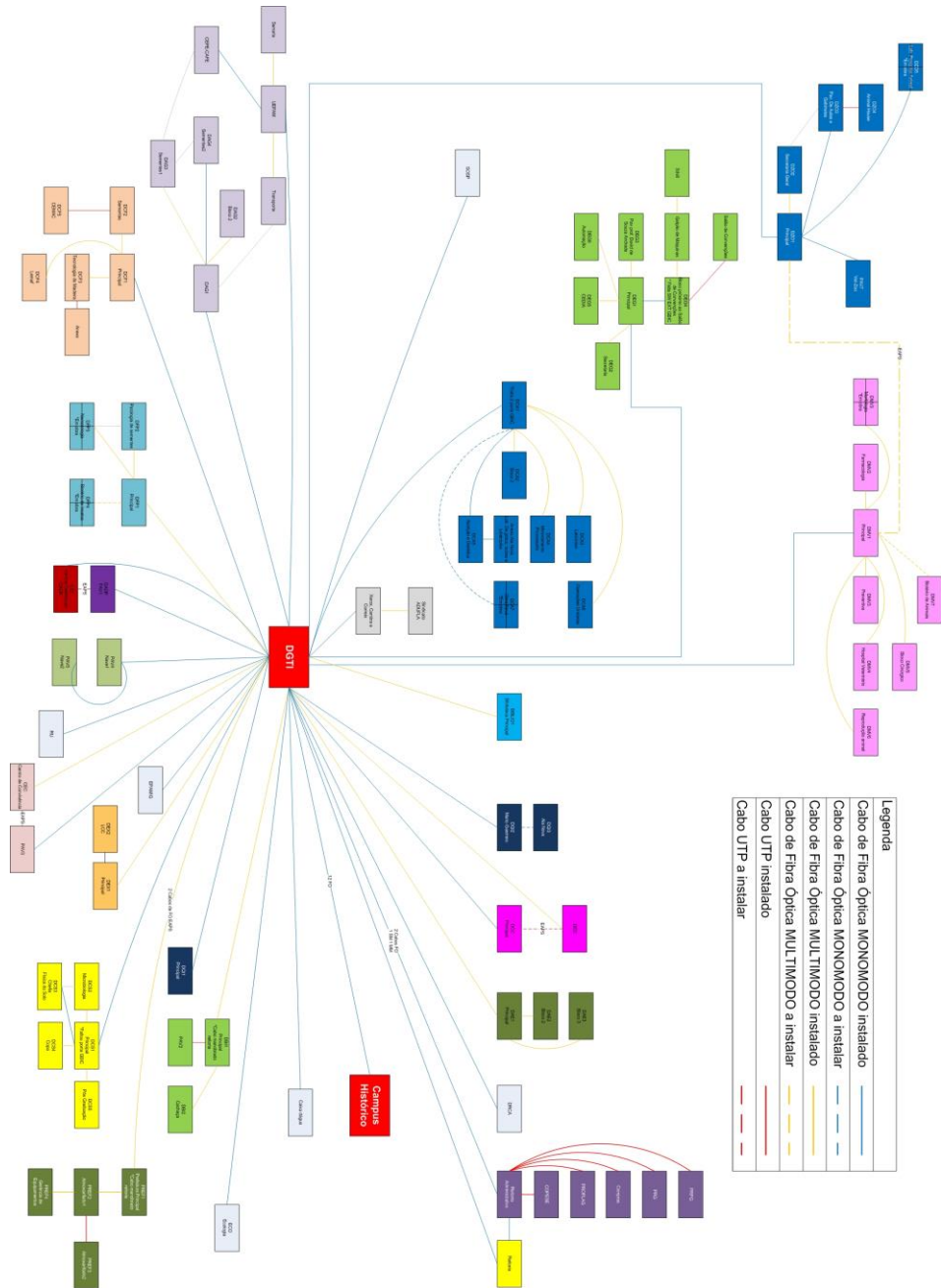


Figura 14 Diagrama da rede da UFLA.

Atualmente o IPv6 já se encontra implantado nos servidores DNS e no servidor da página principal.

Para permitir a conexão da rede da UFLA com as redes externas, ou acesso à Internet são utilizados roteadores de borda configurados com o protocolo BGP (Border Gateway Protocol). O BGP, definido na RFC 1771, permite criar roteamentos de interdomínio sem loop entre sistemas autônomos (AS) (IETF, 1995). Um AS é um conjunto de roteadores em uma única administração técnica. Roteadores em um AS podem usar vários protocolos de gateway interior (IGPs) para trocar informações de roteamento dentro do AS e podem usar um protocolo de gateway exterior (BGP) para rotear pacotes fora do AS (CISCO, 2008).

O BGP em particular foi projetado para permitir a imposição de políticas de roteamento no tráfego entre AS (TANENBAUM, 2011). Essa políticas envolvem fatores de segurança, economia e política.

A UFLA é proprietária do AS 52853, um AS pode ser definido como uma rede, ou um conjunto de redes que possuem características e políticas de roteamento comuns, e se encontram sob uma gestão comum.

As faixas de endereços IPv4 e IPv6 de propriedade da Universidade Federal de Lavras são anunciadas para um *peer*, o AS10417 Fundação de Desenvolvimento da Pesquisa (FUNDEP-UFMG), e posteriormente são anunciadas a Rede Nacional de Pesquisa AS1916 (HE, 2014).

As Figuras 15 e 16 mostram respectivamente as rotas BGP IPv4 e IPv6 o qual a UFLA se conecta.

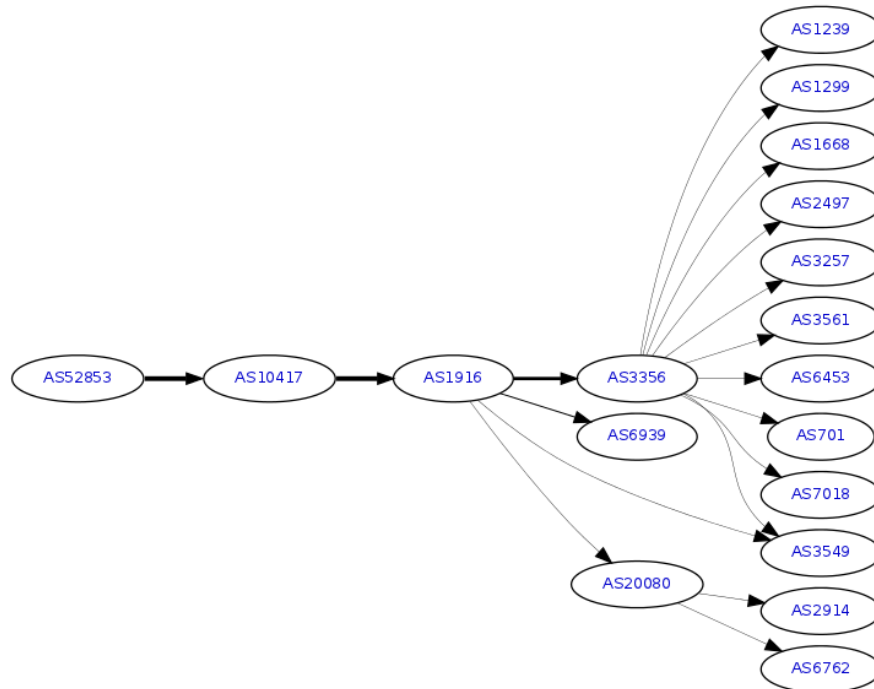


Figura 15 Rota de propagação de IPv4 via BGP

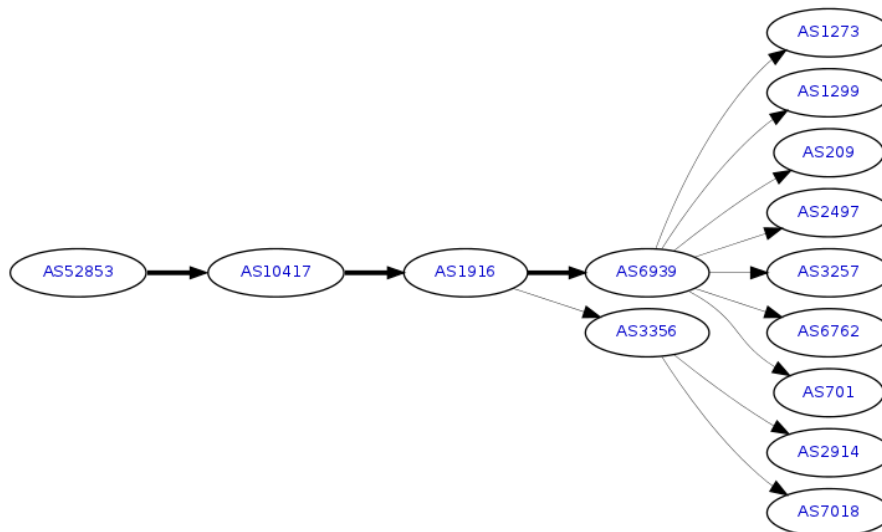


Figura 16 Rota de propagação de IPv6 via BGP.

4.1 Divisão da rede IPv6 na UFLA

Esta proposta segue as mesmas políticas de divisão de endereçamento IPv4 e também seguir as recomendações do NIC.BR, que propõe que a rede seja dividida seguindo pelo menos um dos três tipos básicos de distribuição, geográfica, topológica e/ou funcional.

De acordo com as necessidade da rede propõe-se utilizar uma distribuição funcional, separando inicialmente serviços e funcionalidades, com intenção de facilitar a gestão dos serviços e configuração de firewall. Posteriormente, será separado os locais.

A Figura 17 apresenta a divisão de bits do endereço para cada localidade. Após o prefixo, os 4 primeiros bits define o tipo de serviço. Os tipos de serviços definidos e já em uso são *desktops*, Wlan, Voip, multimídia, câmera (segurança), servidores internos, servidores externos, catraca, (Foram reservados 8 tipos diferente de serviços para uso futuro) conforme apresenta a tabela na Figura 18. Os próximos 8 bits foram reservados para localidades possibilitando um total de 256 localidades para cada tipo de uso. Após esta alocação cada uma das localidades terá reservado uma faixa de endereços /44 para cada tipo de uso.

Com uma faixa de endereços /44 reservada para cada localidade, a mesma receberá uma faixa de endereços /48 para uso imediato, mais 15 faixas /48 para uso futuro.

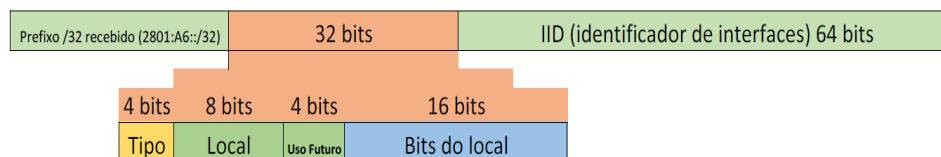


Figura 17 Divisão de bits entregue a cada localidade.

Para um estudo mais detalhado da divisão da rede, propõe-se utilizar o Departamento de Ciência da Computação (DCC) que possui uma estrutura de rede complexa. O DCC Será utilizado como protótipo para experimentos de implantação do protocolo IPv6.

Proposta de divisão de endereços IPv6 - UFPA							
Preho Ufa 2001:06::/32	Localis	Faixa de endereço reservado	Faixa de endereço Entregue	Localis	Faixa de endereço reservado	Faixa de endereço Entregue	
0 Desktops	Administrativa	2801:06:0000::/44	2801:06:0000::/48	Departamentos	idap	2801:06:0000::/44	2801:06:0000::/48
8 WLAN	Departamentos	2801:06:8000::/44	2801:06:8000::/48	Terceros	inbalec	2801:06:8000::/44	2801:06:8000::/48
4 Vop	Departamentos	2801:06:4000::/44	2801:06:4000::/48	Departamentos	uepan	2801:06:4000::/44	2801:06:4000::/48
c Multimidia	Departamentos	2801:06:0000::/36	2801:06:0000::/48	Administrativa	transporte	2801:06:0000::/44	2801:06:0000::/48
2 Camera (Seguranca)	Departamentos	2801:06:2000::/36	2801:06:2000::/48	Departamentos	cepacale	2801:06:2000::/44	2801:06:2000::/48
a Servidores Internos	Departamentos	2801:06:0000::/36	2801:06:0000::/48	Administrativa	auditoria	2801:06:0000::/44	2801:06:0000::/48
6 Servidores Externos	Departamentos	2801:06:6000::/36	2801:06:6000::/48	Administrativa	dicon	2801:06:6000::/44	2801:06:6000::/48
e Caixa	Departamentos	2801:06:0000::/36	2801:06:0000::/48	Administrativa	domng	2801:06:6000::/44	2801:06:6000::/48
	Departamentos			Terceros	emalter	2801:06:1400::/44	2801:06:1400::/48
	Departamentos			Terceros	emaf	2801:06:1400::/44	2801:06:1400::/48
	Departamentos			Terceros	sepanig	2801:06:1400::/44	2801:06:1400::/48
	Departamentos			Administrativa	alogramento	2801:06:1400::/44	2801:06:1400::/48
	Departamentos			Administrativa	ibcnst	2801:06:1400::/44	2801:06:1400::/48
	Departamentos			Departamentos	deg	2801:06:1400::/44	2801:06:1400::/48
	Departamentos			Terceros	abndiomss	2801:06:1400::/44	2801:06:1400::/48
	Departamentos			Administrativa	centro-com (setor2/cre)	2801:06:0000::/44	2801:06:0000::/48
	Departamentos			Administrativa	prefeitura	2801:06:8000::/44	2801:06:8000::/48
	Departamentos			Administrativa	almox-patri (setor3)	2801:06:4000::/44	2801:06:4000::/48
	Departamentos			Terceros	ivu (setor4)	2801:06:0000::/44	2801:06:0000::/48
	Departamentos			Administrativa	centro-medico (setor5)	2801:06:0000::/44	2801:06:0000::/48
	Departamentos			Administrativa	setor6	2801:06:0000::/44	2801:06:0000::/48
	Departamentos			Departamentos	biblioteca-adm	2801:06:6000::/44	2801:06:6000::/48
	Departamentos			Administrativa	navaz	2801:06:6000::/44	2801:06:6000::/48
	Departamentos			Administrativa	teste	2801:06:1000::/44	2801:06:1000::/48
	Departamentos			Terceros	sinidulla	2801:06:9000::/44	2801:06:9000::/48
	Departamentos			Terceros	bni	2801:06:5000::/44	2801:06:5000::/48
	Departamentos			Departamentos	dic	2801:06:0000::/44	2801:06:0000::/48
	Departamentos			Administrativa	radio	2801:06:3000::/44	2801:06:3000::/48
	Departamentos			Terceros	xerox	2801:06:0000::/44	2801:06:0000::/48
	Departamentos			Departamentos	direto	2801:06:7000::/44	2801:06:7000::/48
	Departamentos			Servidores	WAN	2801:06:1000::/44	2801:06:1000::/48

Figura 18 Divisão IPv6 na UFPA.

4.2 Descrição e segmentação do DCC/UFLA

O DCC/UFLA é responsável por dois cursos de graduação, são eles Bacharelado em Ciência da Computação e Bacharelado em Sistemas de Informação. Além de oferecer também cursos de Pós-Graduação.

O Departamento possui diversos laboratórios de pesquisa, dentre eles laboratório de Computação, Laboratório de Eletrônica e Sistemas Digitais. Além desses, Centro Tecnológico de Informática, Empresa Júnior de Computação, Centro de Computação de Alto Desempenho e Laboratório de Computação Avançada.

O Departamento é composto de 2 pavimentos em funcionamento, primeiro andar e térreo, e um pavimento em expansão, subsolo. O térreo é composto de salas de professores, salas de seminários, laboratórios de computadores, laboratórios de pesquisa e anfiteatro. O primeiro andar é composto de salas professores, laboratórios de pesquisas, secretaria e copa, conforme Tabela 2.

Tabela 2 Salas DCC

Copa	01
Salas de Professores e Secretaria	33
Salas de Seminários	02
Laboratórios Diversos	12
Anfiteatro	01

4.2.1 Rede do DCC

O DCC está ligado ao *backbone* da DGTI, a ligação é realizada através de fibra óptica. No departamento estão disponíveis 618 pontos de acesso à Internet através de cabo UTP com conector RJ45. A DGTI disponibiliza uma faixa de

endereços IPv4 /24 (total de 254 hosts) para o DCC. Para que todos os pontos disponíveis sejam acessíveis através de IPv4 público, a quantidade não é suficiente.

O DCC oferece diversos tipos de serviços como hospedagem web, servidores diversos e também pontos de acesso a rede sem fio para alunos e professores, conforme Tabela 3.

Tabela 3 Serviços de Rede

Serviços	Quantidade
Websites	03
Servidores DNS	02
Servidores Diversos	64
Pontos de acesso a rede sem fio	12

As políticas de endereçamento dentro do DCC seguem as regras vindas da DGTI. Existem alguns casos especiais como computadores de alguns professores e impressoras com endereços IPv4 públicos utilizando atribuição fixa, os demais recebem endereços IPv4 atribuídos automaticamente por DHCP direto da DGTI.

Tabela 4 Hosts com IPv4 fixos.

Tipo de Host	Quantidade
Impressoras de Rede	07
Computadores de Professores	04

Estão disponíveis 4 laboratórios de computação, denominados laboratórios 1, 2, 3, 4, dos quais os laboratórios 1 e 2 sua rede passa por um

gateway onde é realizado a distribuição dos IPv4 por NAT. Os laboratórios 3 e 4 estão ligados a um sistema de autenticação de usuário por *login* e senha oferecido diretamente pela DGTI, onde os endereços IPv4 entregues também são privados através de NAT.

Tabela 5 Hosts por laboratórios

Laboratórios	Quantidade
Hosts nos laboratórios de computação 1 e 2	71
Hosts nos laboratórios de computação 3 e 4	70

A Figura 19 exemplifica a distribuição de rede no Departamento de Ciência de Computação.

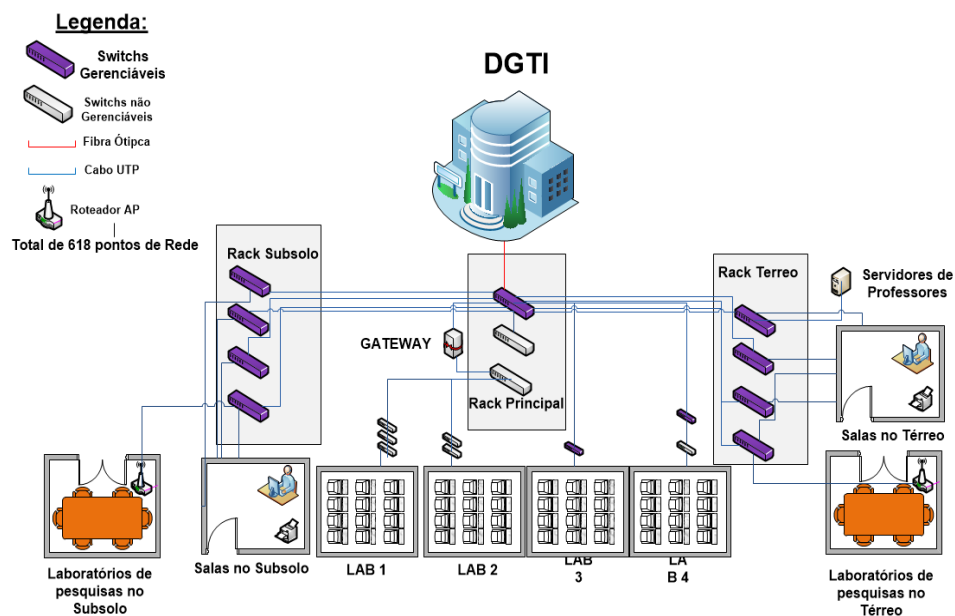


Figura 19 Rede DCC

4.2.2 Política de segmentação da rede IPv6 no DCC

Conforme estabelecido na Seção 4.1, o Departamento de Ciência da Computação receberá a faixa de endereços IPv6 2801:a6:*dcc::/48, no qual * representa o tipo de serviço utilizado, como por exemplo o uso de Desktops, Multimídia, Câmeras de segurança, etc.

Esta proposta também estabelece subdividir a rede IPv6 do DCC em locais, como área administrativa, sala de professores, laboratórios de pesquisa e laboratórios de alunos.

Para cada local é recomendado alocar uma faixa de endereços /56, e reservar para uso futuro uma faixa /52. Como o DCC possui uma faixa de endereços /48, permite-se dividir 16 faixas /52, dentro de cada /52 pode-se obter 16 faixas /56 que seria o tamanho de faixa apropriado para cada local dentro do departamento.

Para cada *host* é recomendável alocar uma faixa de endereço /64, possibilitando um total de 256 *hosts* dentro de cada faixa /56, e um total 4096 *hosts* em uma faixa /52, que é a faixa indicada para reservar para cada local. A Figura 20 ilustra o planejamento de alocação desde a faixa recebida pela UFLA até o *host* final.

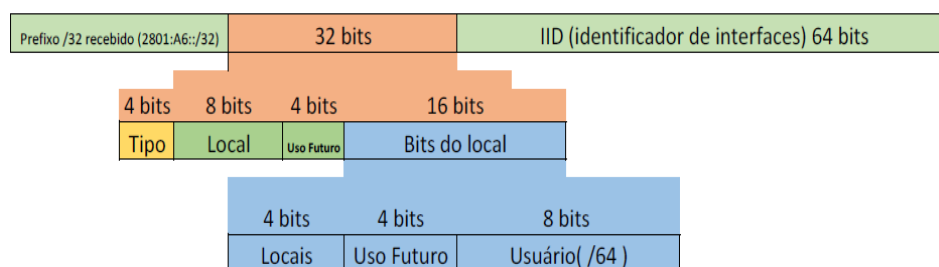


Figura 20 Divisão de bits dentro do Departamento

Utilizando a faixa de endereço entregue ao DCC, a Tabela 6 propõe uma divisão para a rede, separando os locais, utilizando o algoritmo *left most*.

Tabela 6 Divisão IPv6 DCC

Local	Endereço Reservado	Endereço Entregue
Sala de Professores	2801:a6:*dcc:0000::/52	2801:a6:*dcc:0000::/56
Área Administrativa	2801:a6:*dcc:8000::/52	2801:a6:*dcc:8000::/56
Laboratórios de Pesquisas	2801:a6:*dcc:4000::/52	2801:a6:*dcc:4000::/56
Laboratórios de Alunos	2801:a6:*dcc:c000::/52	2801:a6:*dcc:c000::/56

A alocação de faixas de endereços /64 para os *hosts* deverá ser feita de forma sequencial através de um servidor DHCP.

Com a proposta de divisão realizada a DGTI disponibilizou dentro do DCC um ponto de acesso com redes IPv6 e IPv4 em pilha dupla. Este ponto foi habilitado na sala 02-18. A Seção a seguir apresenta os resultados e discussões do uso e testes de tempo de resposta.

4.3 Testes de uso do protocolo IPv6

Foi verificado a disponibilidade de acesso em IPv6 de diversos sites e também o tempo de latência. Com esta verificação, o computador é capaz de medir quantos milissegundos um pacote de informações leva para ir até um destino e voltar caso esteja disponível e habilitado.

Para realizar testes foram extraídos alguns dados do site alexa⁷, através de consulta em um navegador web. O site é um serviço de internet pertencente a

⁷ www.alexa.com

Amazon⁸. Este foi fundado em 1996 e mede a quantidade de usuários de internet visitam um site na *web* (AMAZON, 2014).

O primeiro teste realizado teve a pretensão de mostrar a disponibilidade de acesso a sites utilizando apenas o protocolo IPv6. Foi tomado como base os 20 sites mais acessados do Brasil. Os resultados mostram que entre os 10 primeiros 30% não é acessível em IPv6, são eles globo.com, live.com, mercadolivre.com.br. Ao analisar os 20 mais acessados, o resultado é mais alarmante, onde 60% ainda não estão acessíveis.

Um ponto a se destacar é a acessibilidade de sites e serviços pertencentes a empresa Google, os resultados mostram que a maioria de seus serviços são acessíveis em IPv6. O mesmo não ocorre com a Microsoft, onde nem o seu principal site⁹ está acessível.

Dois dos principais serviços utilizados também foram testados, são eles Skype e Dropbox e os resultados também mostram que estão indisponíveis na rede IPV6.

Tabela 7 Sites mais acessados do Brasil

Posição	Site	IPv6	Descrição
1°	Google.com.br	SIM	Buscador que foca seus resultados para o Brasil
2°	Facebook.com	SIM	Rede social mais acessada do mundo
3°	Google.com	SIM	Buscador a nível mundial
4°	Youtube.com	SIM	Repositório de vídeos
5°	Uol.com.br	SIM	Portal de acesso à internet e serviços agregados

⁸ Empresa multinacional de comércio eletrônico dos Estados Unidos com sede em Seattle

⁹ www.microsoft.com

6°	Globo.com	NÃO	Portal de conteúdo da Rede Globo de Televisão
7°	Yahoo.com	SIM	Maior portal da internet com diversos serviços
8°	Live.com	NÃO	Mecanismo de busca da Microsoft
9°	Mercadolivre.com.br	NÃO	Site para comprar e vender de tudo
10°	Wikipedia.org	SIM	A enciclopédia livre construída de forma colaborativa utilizando o software wiki

Durante testes de acessibilidade foram verificados sites brasileiros e o resultado foi alarmante. Ao analisar os 20 primeiros, apenas 15% é acessível em IPv6, ou seja apenas 3, sendo que 2 deles pertence a empresas estrangeiras.

O teste de PING foi realizado nos dois sites mais acessados, google.com e facebook.com. Conforme mostra a Figura 21 o site google.com obteve uma resposta mais rápida utilizando o protocolo IPv4 com média de 69ms utilizando IPv4 e 141ms utilizando IPv6. O teste realizado com o site facebook.com não mostrou uma diferença considerável, com 167ms e 168ms para IPv4 e Ipv6 respectivamente.

```
Prompt de Comando
C:\Users\Douglas Henrique>ping facebook.com
Disparando facebook.com [2a03:2880:2110:df07:face:b00c:0:1] com 32 bytes de dados:
Resposta de 2a03:2880:2110:df07:face:b00c:0:1: tempo=168ms
Resposta de 2a03:2880:2110:df07:face:b00c:0:1: tempo=168ms
Resposta de 2a03:2880:2110:df07:face:b00c:0:1: tempo=168ms
Resposta de 2a03:2880:2110:df07:face:b00c:0:1: tempo=168ms
Estatísticas do Ping para 2a03:2880:2110:df07:face:b00c:0:1:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (<0% de perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 168ms, Máximo = 168ms, Média = 168ms
C:\Users\Douglas Henrique>ping -4 facebook.com
Disparando facebook.com [173.252.110.27] com 32 bytes de dados:
Resposta de 173.252.110.27: bytes=32 tempo=167ms TTL=84
Resposta de 173.252.110.27: bytes=32 tempo=169ms TTL=84
Resposta de 173.252.110.27: bytes=32 tempo=167ms TTL=84
Resposta de 173.252.110.27: bytes=32 tempo=168ms TTL=84
Estatísticas do Ping para 173.252.110.27:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (<0% de perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 167ms, Máximo = 169ms, Média = 167ms
C:\Users\Douglas Henrique>ping google.com
Disparando google.com [2800:3f0:4003:801::1004] com 32 bytes de dados:
Resposta de 2800:3f0:4003:801::1004: tempo=143ms
Resposta de 2800:3f0:4003:801::1004: tempo=141ms
Resposta de 2800:3f0:4003:801::1004: tempo=141ms
Resposta de 2800:3f0:4003:801::1004: tempo=141ms
Estatísticas do Ping para 2800:3f0:4003:801::1004:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (<0% de perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 141ms, Máximo = 143ms, Média = 141ms
C:\Users\Douglas Henrique>ping -4 google.com
Disparando google.com [173.194.42.226] com 32 bytes de dados:
Resposta de 173.194.42.226: bytes=32 tempo=69ms TTL=56
Resposta de 173.194.42.226: bytes=32 tempo=70ms TTL=56
Resposta de 173.194.42.226: bytes=32 tempo=69ms TTL=56
Resposta de 173.194.42.226: bytes=32 tempo=70ms TTL=56
Estatísticas do Ping para 173.194.42.226:
  Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (<0% de perda),
Aproximar um número redondo de vezes em milissegundos:
  Mínimo = 69ms, Máximo = 70ms, Média = 69ms
```

Figura 21 PING realizado

5 CONCLUSÃO

A Universidade Federal de Lavras tem se destacado em suas funções de ensino, pesquisa e extensão, e tem aumentado a quantidade de cursos e alunos. Isso impacta diretamente na quantidade de dispositivos computacionais conectados a Internet.

Atualmente, a rede mundial de computadores é um dos principais meios de comunicação, a transferindo a responsabilidade de estar preparada para atender uma quantidade cada vez maior de cliente (*hosts*). Como a comunicação com a Internet se dá através de alguns protocolos, sendo o protocolo mais importante nesta comunicação é o IP, que atualmente está na versão 4. Os endereços disponíveis nesta versão vem se esgotando rapidamente, o que pode comprometer o crescimento da rede. O IPv6 foi desenvolvido principalmente com a finalidade de resolver o problema de esgotamento, que possibilitará que a Internet mantenha o incremento em sua taxa de crescimento, tornando o acesso às informações cada vez mais amplo.

Este trabalho teve como principal objetivo a análise da rede atual da UFLA com ênfase no DCC/UFLA, e propor uma segmentação da rede IPv6 obedecendo as políticas estabelecidas pela DGTI adotando boas práticas de implantação do protocolo IPv6 propostas principalmente pelo NIC.BR e CGI.BR.

O uso do protocolo IPv6 pela UFLA se torna viável pois a mesma possui uma quantidade de endereços IPv4 e IPv6 disponível para suprir suas necessidades atuais que não traz a necessidade de adotar medidas paliativas para crescimento da rede. Durante a realização deste trabalho foi verificado que a Internet atual ainda não está preparada para o uso somente do protocolo IPv6, poucos sites e serviços estão disponíveis. Foi constatado que apenas 4,5% dos acessos atuais ao site google.com são realizados através de IPv6, um número relativamente pequeno se considerado que os endereços IPv4 de atribuição da IANA se esgotaram, assim

como nas maiorias dos RIRs pelo mundo. É importante considerar que em um ano este número de acesso ao Google cresceu consideravelmente em torno de 400%. Outro fator é que os atuais Sistemas Operacionais suportam o endereçamento IPv6.

Em 2011 foi criado um cronograma brasileiro para migração para IPv6 o que foi deixado de lado pela maioria dos provedores de trânsito de Internet. Este cronograma previa que em janeiro de 2014 todos na rede utilizariam IPv6, mesmo que o IPv4 ainda se mantivesse ativado. Não foi o que aconteceu, praticamente quase nada na Internet ainda é acessível. Além do cronograma, o CGI.br fez algumas recomendações na resolução CGI.br/RES/2012/007/P em 18 de maio de 2012 o que destaca que provedores de acesso Internet ofereçam suporte ao IPv6 para todos os usuários antes de 01 de Janeiro de 2014, e que as universidades e centros de pesquisa, em especial os relacionados às disciplinas de redes, computação e Internet, implantem o IPv6 em suas redes com urgência. Pouco do que foi recomendado foi cumprido pelas instituições, isso serviu de inspiração para a realização deste trabalho, que depois dos estudos e proposta de segmentação total da rede da UFLA não foi possível a implantação total do IPv6 por questão de *hardware*, especialmente o *firewall* da rede que ainda não tem suporte para o protocolo, isso acarretaria em uma falha de segurança na rede. É esperado que em um futuro breve seja possível a implantação total do IPv6 na rede da universidade.

REFERÊNCIAS BIBLIOGRÁFICAS

- AMAZON. Alexa.com. **Alexa**, 02 jul. 2014. Disponível em: <www.alexacom.com>. Acesso em: 02 jul. 2014.
- BRADNER, S.; MANKIN, A. IP: Next Generation (IPng) White Paper Solicitation. **Request for Comments: 1550**, p. 6, 1993.
- CEPTRO.BR. Simulação RFC 3531. **IPV6.BR - A nova geração do Potocolo Internet**, 2013. Disponível em: <<http://ipv6.br/rfc3531demo/>>. Acesso em: 07 out. 2014.
- CGI.BR. Resolução CGI.br/RES/2012/007/P – Recomendação para Implantação do Protocolo IPv6. **CGI.BR**, 18 maio 2012. Disponível em: <<http://www.cgi.br/regulamentacao/resolucao2012-007>>. Acesso em: 22 maio 2014.
- CISCO. Estudos de caso do BGP. **Cisco.com**, 03 Abril 2008. Disponível em: <http://www.cisco.com/cisco/web/support/BR/8/85/85732_bgp-toc.pdf>. Acesso em: 03 Julho 2014.
- COMPUTER HISTORY MUSEUM. Computer History Museum. **Computer History**, 03 set. 2013. Disponível em: <<http://www.computerhistory.org/>>.
- DEERING, S.; HINDEN, R. Request for Comments: 2460 - Internet Protocol, Version 6 (IPv6) - Specification. **The Internet Engineering Task Force (IETF)**, p. 39, 1998.
- GOOGLE. A adoção do IPv6. **google.com**, 20 out. 2014. Disponível em: <<http://www.google.com/intl/pt-BR/ipv6/statistics.html#tab=ipv6-adoption>>.
- HAGEM, S. **IPv6 Essentials**. Sebastopol: O'Reilly Media, 2006.
- HE. INFO - AS52853 UFLA - UNIVERSIDADE FEDERAL DE LAVRAS. **Hurricane Electric Internet Services**, 03 Julho 2014. Disponível em: <http://bgp.he.net/AS52853#_asinfo>. Acesso em: 03 Julho 2014.

IANA. IANA. **Internet Assigned Numbers Authority**, 03 set. 2013. Disponível em: <<http://www.iana.org/>>.

IETF. IP: Next Generation (IPng) White Paper Solicitation. **Internet Engineering Task Force**, 08 dezembro 1993. Disponível em: <<https://tools.ietf.org/rfc/rfc1550.txt>>. Acesso em: 03 set. 2013.

IETF. A Border Gateway Protocol 4. **Internet Engineering Task Force**, mar. 1995. Disponível em: <<http://www.ietf.org/rfc/rfc1771.txt>>. Acesso em: 03 Julho 2014.

IETF. Internet Engineering Task Force - Internet Architecture Board, Internet Engineering Steering Group. **IAB/IESG Recommendations on IPv6 Address Allocations to Sites**, 2001. Disponível em: <<http://tools.ietf.org/rfc/rfc3177.txt>>. Acesso em: 05 abr. 2014.

IETF. IPv6 Address Assignment to End Sites. **Internet Engineering Task Force - Request for Comments: 6177**, mar. 2011. Disponível em: <<http://tools.ietf.org/search/rfc6177>>. Acesso em: 04 abr. 2014.

JUNG, C. F. **Metodologia para pesquisa & desenvolvimento**: aplicada a novas tecnologias, produtos e processos. Rio de Janeiro: Axcel Books, 2004.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**: Uma abordagem top-down. Tradução de Arlete Smille Marques. São Paulo: Pearson Education do Brasil, v. 3, 2006.

LACNIC. MANUAL DE POLÍTICAS DE LACNIC v1.10. **lacnic.net**, 13 ago. 2012. Disponível em: <<https://lacnic.net/documentos/politicas/manual-politicas-pt-1.10.pdf>>. Acesso em: 16 maio 2014.

MORAES, C. C. D.; CASTRUCCHI, P. L. **Engenharia de Automação Industrial**. [S.l.]: LTC, v. 2.ed., 2007.

MOREIRAS, A. M. Qual é o tamanho de bloco apropriado? **ipv6.br**, 15 set. 2011. Disponível em: <<http://ipv6.br/qual-e-o-tamanho-de-bloco-apropriado/>>. Acesso em: 13 mar. 2014.

NIC.BR. **Apostila IPv6 Básico**. São Paulo: Núcleo de Informação e Coordenação do Ponto BR - NIC.br, 2012.

NIC.BR. Portal de boas práticas para a Internet no Brasi. **BCP**. Disponível em: <<http://bcp.nic.br/>>. Acesso em: 12 abr. 2014.

PATARA, R. Atualização RIRs-on-48. **Políticas LACNIC**, p. 2, 2012.

TANENBAUM, A. S. **Computer Networks**. Amsterdam: Editora Campus, 2011.

ANEXO I

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet6 {
        filter {
          input FILTRO-BOGONS-V6;
        }
        /* Endereço da interface do roteador */
        /* Precisa trocar */
        address 2001:DB8:CAFE:FACA::1/64;
        /* habilitando Strict uRPF */
        rpf-check;
      }
    }
  }
}

policy-options {
  prefix-list LISTA-BOGONS-V6-DENY{
    2001:db8::/32;
  }
  prefix-list LISTA-BOGONS-V6-ACCEPT{
    2001:500::/30;
    2001::/32;
    2001::/16;
    2001:0678::/29;
```

```
2001:0c00::/23;
2001:13c7:6000::/36;
2001:13c7:7000::/36;
2001:43f8::/29;
2002::/16;
2003::/16;
2400::/12;
2600::/12;
2610::/23;
2620::/23;
2800::/12;
2a00::/12;
2801:0000::/24;
2c00::/12;
fe80::/64;
::/128;
}
}
firewall {
  family inet6 {
    filter FILTRO-BOGONS-V6 {
      term 1 {
        from {
          source-prefix-list {
            LISTA-BOGONS-V6-DENY;
          }
        }
      }
      then {
```

```
        discard;
    }
}
term 2 {
    from {
        source-prefix-list {
            LISTA-BOGONS-V6-ACCEPT;
        }
    }
    then {
        accept;
    }
}
term DEFAULT{
    then {
        discard;
    }
}
}
}
```