CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Analise de Sistemas e Segurança da Informação

IPv6

Um estudo comparativo entre os protocolos IPv4 e IPv6.

Aline da Silva Mendes

Americana, SP

2011

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

Faculdade de Tecnologia de Americana
Curso Superior de Tecnologia em Analise de Sistemas e Segurança da Informação

IPv6

Um estudo comparativo entre os protocolos IPv4 e IPv6.

Aline da Silva Mendes
aline.silva.mendes@hotmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Analise de Sistemas e Segurança da Informação da Fatec-Americana, sob orientação do Prof. Jose Luis Zem.

Área: Redes

Americana, SP
2011

BANCA EXAMINADORA

Prof. Dr. José Luis Zem
(Orientador)

Prof. Rafael Fernando Diório
(Convidado)

Prof. Rogério Nunes de Freitas
(Convidado)

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela força e sabedoria que me concedeu principalmente durante o período da minha formação acadêmica.

Agradeço a todos que me auxiliaram para elaboração desta monografia, em especial ao meu orientador José Luis Zem e ao meu namorado Lucas Marzura que colaboraram no desenvolvimento e a todos os outros que me ajudaram de forma direta ou indiretamente a desenvolver este trabalho acadêmico.

DEDICATÓRIA

Aos meus pais, minha irmã e ao meu namorado, pelo incentivo, colaboração e paciência. Em especial aos meus pais por me auxiliar e não medirem esforços durante todo período da minha vida até a formação e também por compreenderem a importância dos meus estudos para o meu futuro.

RESUMO

Este trabalho tem por objetivo apresentar informações referentes ao novo protocolo de Internet IPv6 (*Internet Protocol Version* 6), definindo e abordando pontos como nova estrutura, diferenças entre a versão anterior, segurança, transmissão e o real motivo para implantação. Além disso, também existe a proposta de mostrar uma rede utilizando o novo protocolo para verificar as mudanças e melhorias do IPv6. Outro objetivo é auxiliar como objeto de estudo para compreensão e entendimento do assunto abordado, mostrando fontes, responsáveis e diferentes opiniões referentes ao novo protocolo (IPv6).

Palavras Chaves: Protocolo, IPv6, Segurança.

ABSTRACT

This paper aims to present information regarding the new Internet protocol IPv6 (Internet Protocol Version 6), defining and addressing issues such as new structure, differences between the previous version, security, broadcasting and the real reason for deployment. Moreover, there is also the proposal to show a network using the new protocol to check the changes and improvements in IPv6. Another objective is to assist the object of study for comprehension and understanding of the subject, showing sources, responsible and different opinions regarding the new protocol (IPv6).

Keywords: Protocol, IPv6, Security.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS (ORDEM ALFABÉTICA)

AH (*Authentication Header*)

ARP (*Address Resolution Protocol*)

ARPANET (*Advanced Research Projects Agency Network*)

DARPA (*Defense Advanced Research Projects Agency*)

DES (*Data Encryption Security*)

DF (*Don't Fragment*):

DHCP (*Dynamic Host Configuration Protocol*)

ESP (*Encrypted Security Payload*)

FTP (*File Transfer Protocol*)

HTTP (*HyperText Transfer Protocol*)

IAB (*Internet Activities Board*)

IANA (*Internet Assigned Numbers Authority*)

ICANN (*Internet Corporation for Assigned Names and Numbers*)

ICMP *(Internet Control Message Protocol)*

ICMPv6 *(Internet Control Message Protocol version 6)*

IGMP *(Internet Group Management Protocol*)

IP (*Internet Protocol*)

IPSec (*Internet Protocol Security*)

IPv4 (*Internet Protocol Version 4*)

IPv6 (*Internet Protocol Version 6)*

ISAKMP (*Internet Security Association and Key Management Protocol*).

MAC (*Media Access Control*)

MD5 (*Message-Digest 5*)

MF (*More Fragments*)

MTU (*Maximum Transfer Unit*)

NAT (*Network Address Translation*)

NIC.br (Núcleo de Informação e Coordenação)

QoS (*Quality of Service)*

SMTP (*Simple Mail Transfer Protocol*)

SNMP (*Simple Network Management Protocol*)

UDP (*User Datagrama Protocol*)

WWW (*World Wide Web*)

RIR (*Regional Internet Registry*)

SUMÁRIO

1 INTRODUÇÃO

Este estudo aborda informações referentes ao IPv6 e o IPv4 bem como, a utilização dos mesmos em redes de computadores, trabalhando-se uma abordagem comparativa entre eles.

1.1 Objetivos

O objetivo principal deste trabalho reside em apresentar os protocolos IPv4 e IPv6, abordando suas histórias, evoluções, características, formas de utilização e situação atual do protocolo.

Como objetivos complementares têm-se a identificação dos responsáveis pela pesquisa e elaboração do novo protocolo, a situação atual no Brasil e as atualizações necessárias de compatibilidade com os equipamentos, programas e sistemas operacionais para ativação do protocolo.

Além disso, existe o objetivo de apresentar o desenvolvimento de testes de desempenho e compatibilidade do protocolo IPv6, para aplicar os conceitos teóricos e identificar características.

Esta monografia, realizada para conclusão do curso de Segurança da Informação, também tem o objetivo de contribuir como referência para estudantes, pesquisadores ou curiosos sobre o funcionamento do protocolo de comunicação, IPv6.

1.2 Justificativas

O tema desta monografia foi escolhido por ser um assunto de pesquisa atual e também pelo fato que irá contribuir com o aprendizado teórico e prático referente

ao assunto. Este tema também irá colaborar para o entendimento do assunto, uma vez que esta nova estrutura logo será implantada.

Outro motivo que contribuiu para a escolha do tema é o de que, atualmente, não existem muitas fontes de informações disponíveis sobre o assunto, assim este material de estudo pode colaborar para esclarecer dúvidas e explicar, de uma forma clara e simplificada, a estrutura do protocolo IPv6.

1.3 Metodologia

A metodologia utilizada neste trabalho está voltada ao levantamento bibliográfico realizado através de pesquisas em fontes literárias e ao desenvolvimento realizado a partir da análise, testes e apresentação dos resultados.

Para a realização deste trabalho acadêmico, foi identificada a necessidade de dividir o estudo em etapas, constituídas pelo levantamento bibliográfico e pelo desenvolvimento.

A primeira etapa deste trabalho acadêmico buscou qualificar o levantamento bibliográfico que permitiu o entendimento das principais características, estrutura atual e informações do protocolo IPv6. Para facilitar o entendimento, o levantamento bibliográfico foi dividido nas sub-etapas: o levantamento teórico e a situação atual.

O levantamento teórico tem o objetivo de explicar a Arquitetura TCP/IP, o funcionamento e apontando as características das versões do protocolo IP (IPv4 e IPv6). Através deste levantamento foi possível compreender os conceitos do protocolo IPv6.

Na situação atual foi enfatizado o andamento para implantação do protocolo IPv6 e os principais sistemas operacionais e sites que o suportam.

A segunda etapa contribuiu para um melhor entendimento referente ao protocolo IPv6 e também para aplicar os conceitos estudados, identificar características e atingir resultados dos testes feito no protocolo em questão.

Nesta etapa foi desenvolvido uma simples rede contendo uma máquina local e uma máquina virtual utilizando o sistema operacional Windows com o protocolo IPv6 habilitado, foi realizada a análise, mostrando a configuração realizada e a medição de testes de comunicação entre as duas.

2 LEVANTAMENTO TEÓRICO

O levantamento teórico deste trabalho aborda os protocolos IPv4 e IPv6, apresentando a história dos protocolos, o funcionamento e a comparação entre os dois.

2.1 Arquitetura TCP/IP

A arquitetura TCP/IP (*Internet Protocol*) foi criada pelo Departamento de Defesa Americano (DoD) buscando garantir a preservação da integridade dos dados, assim como manter a comunicação na ocorrência de uma guerra.

De acordo com (Filippetti, 2008):

> "se bem planejada e corretamente implementada, uma rede baseada na combinação de protocolos (suíte) TCP/IP pode ser independente, confiável e muito eficiente."

A arquitetura TCP/IP, ou simplesmente TCP/IP, é um resultado da pesquisa e desenvolvimento de protocolos realizados na rede experimental de comutação de pacotes ARPANET, patrocinada pela *Defense Advanced Research Project* Agency (DARPA), e geralmente é referenciada como conjunto de protocolos TCP/IP. Esse conjunto de protocolos consiste em uma grande coleção de protocolos que foram definidos como padrões da Internet pelo *Internet Activities Board* (IAB) (STALLINGS, 2005).

2.2 Camadas do TCP/IP

O protocolo TCP/IP (*Internet Protocol*) não possui um modelo padrão, mas pode ser organizado em cinco camadas, conforme Figura 1 (TANENBAUM, 2003).

5	Camada de Aplicação
4	Camada de Transporte (Host a Host)
3	Camada de rede
2	Camada de Enlace (Inter-redes)
1	Camada Física

Figura 1: Camada de Redes (TANENBAUM, 2003).

A **Camada Física** é responsável pelo meio de transmissão, trata o nível de sinais, taxa de dados e da transmissão. Cuida da interface física entre um dispositivo de transmissão de dados e um meio de transmissão de rede.

A **Camada de Enlace (Inter-redes)** trata da troca de dados na rede, fornecendo informações de envio para que possa chegar ao endereço de destino, ou seja, ao computador e/ou servidor.

A **Camada de Rede** é responsável pelo transporte de pacotes, a transmissão é realizada de um *host* remetente a um *host* destinatário. Também é responsável pelo repasse e roteamento dos pacotes, ou seja, datagramas.

A **Camada de Transporte (host a host)** é implementada em sistemas finais, faz a comunicação lógica entre processos de aplicação que rodam em locais diferentes.

A **Camada de Aplicação** é responsável pelo suporte às diversas aplicações do usuário, programas que utilizam o acesso à rede e é nela que roda diversos protocolos como o HTTP (*HyperText Transfer Protocol*), FTP (*File Transfer Protocol*), SMTP (*Simple Mail Transfer Protocol*) e outros.

2.3 Aplicações TCP/IP

Muitas aplicações foram feitas para utilizar o protocolo TCP/IP, ferramentas de transferência e outras para acesso remoto. Alguns protocolos que utilizam a camada de aplicação são:

SMTP (*Simple Mail Transfer Protocol*) transfere mensagens entre hosts, protocolo de envio de emails, utilizado nos correios eletrônicos.

HTTP (*HyperText Transfer Protocol*) protocolo de comunicação para acesso a internet, recurso usado pelo WWW (*World Wide Web*).

FTP (*File Transfer Protocol*) utilizado para transferir arquivos; é estabelecida uma conexão e armazenado o arquivo em um local, depois pode ser compartilhado.

TELNET aplicação de utilização remota, através dele é possível acesso remoto a um servidor ou computador. É um terminal simples que interage diretamente com a entrada e saída das informações.

SNMP (*Simple Network Management Protocol*) é uma ferramenta utilizada para gerenciamento de rede, é possível efetuar análise do desempenho e identificar problemas.

2.4 NAT

Para resolver os problemas de insuficiência de endereços IP foi criado o serviço de NAT (*Network Address Translation*) que tem por objetivo traduzir endereços de IP.

O NAT possibilitou que as máquinas de redes internas conseguissem acessar a rede externa, utilizando um único número de IP válido. Essa característica do NAT

elimina a obrigatoriedade de todos os computadores em uma rede terem um endereço IP válido.

O NAT pode ser estático ou dinâmico, a modalidade estática sempre realiza a mesma tradução, uma vez que utiliza um mesmo número IP, normalmente já estabelecido. A forma dinâmica pode receber endereços de IP de forma aleatória em um determinado período de tempo, é feita então a tradução de um endereço IP de redes locais para um endereço global, para que se obtenha o acesso a rede global.

A princípio, o NAT foi desenvolvido apenas para solucionar os problemas de escassez de IP, mas atualmente pode ser utilizado para balancear cargas de rede e backup de servidores.

2.5 Tabela ARP

O ARP (*Address Resolution Protocol*) é um protocolo utilizado para encontrar endereços de rede. Basicamente a tabela ARP possui um IP na rede e tenta descobrir o MAC (*Media Access Control*).

O processo para descobrir o endereço MAC funciona conforme a Figura 2: Tabela ARP.

O computador 1, para descobrir o endereço MAC do computador 2, deve, inicialmente, conhecer o endereço IP da referenciada máquina com a deseja interagir.

O computador 1, utilizando esse endereço IP envia um broadcast ao computador 2 solicitando o seu endereço MAC. O computador 2, por sua vez, responderá, também com um broadcast a informação solicitada. Conforme Figura 2: Tabela ARP (UFGRS).

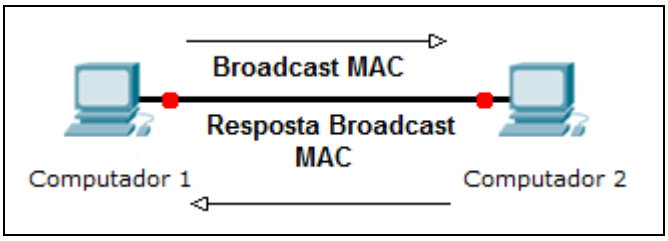

Figura 2: Tabela ARP (UFGRS).

2.6 IPv4

O protocolo IPv4 (*Internet Protocol Version 4*) como o próprio nome diz é o protocolo de internet versão 4 e segue os princípios da arquitetura TCP/IP. Atualmente é utilizado por todos os dispositivos de acesso a rede.

O endereço IP possui largura de 32 bits e serve para identificar cada dispositivo na rede, facilitando a transmissão dos dados e entrega de mensagens.

2.6.1 Estrutura do IPv4

Um datagrama IP consiste em uma parte de cabeçalho e uma parte de texto. O cabeçalho tem uma parte fixa de 20 bytes e uma parte opcional de tamanho variável. Ele é transmitido em uma ordem *big endian*: da esquerda para a direita, com o bit de mais alta ordem do campo *Version* aparecendo primeiro (TANENBAUM, 2003). Conforme Figura 3: O cabeçalho IPv4 (TANENBAUM, 2003).

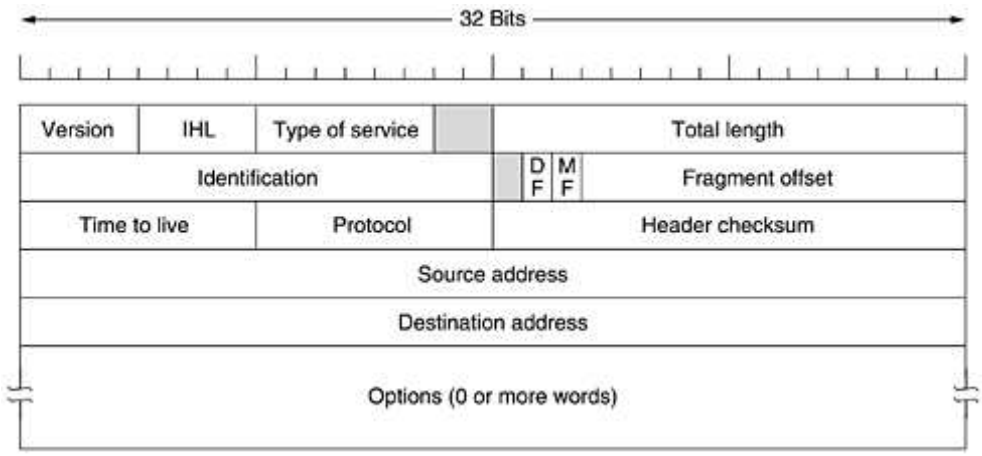

Figura 3: O cabeçalho IPv4 (TANENBAUM, 2003).

O cabeçalho do protocolo IPv4 é dividido nos seguintes campos:

***Version**:* Gerencia e controla as versões do datagrama, é possível também identificar a transição entre as versões.

IHL: Controla o tamanho do cabeçalho, informa o tamanho, porque o cabeçalho não possui um tamanho constante.

Type of service: Distingue as classes de serviço, por exemplo, no pacote de voz é adicionado prioridade e velocidade na entrega.

Total length: Adiciona todas as informações no datagrama (cabeçalho e dados) e também controla o datagrama, mostra o número total de bytes. O tamanho máximo é 65.535 bytes.

Identification: Identifica o *host* que enviou o datagrama.

DF (*Don't Fragment*): É um campo que identifica para não fragmentar os datagramas, isso significa que os roteadores não devem fragmentar os pacotes, porque o destino será incapaz de fragmentar novamente. (não fragmentar).

MF (*More Fragments*): Identifica os fragmentos, exceto o último para saber a ordem dos fragmentos.

Fragment offset: Controla a divisão do datagrama e mostra em que ponto está, são múltiplos de 8 bytes, apenas o ultimo que não. O tamanho do datagrama é 65.536 bytes.

Time to live: Parte do cabeçalho usada para limitar o tempo útil do pacote, conta o tempo em segundos, máximo de 255 segundos, pode ser decrementado várias vezes.

Protocol: Indica onde o datagrama deve ser entregue.

Header checksum: Verifica o cabeçalho, identifica erros gerados pelo caminho que o pacote percorreu.

Source address e ***Destination address***: Indica o número da rede e o número do host.

Options: Permite que seja adicionada informação quando se trata de versões posteriores do protocolo, as opções de tamanho variam.

2.6.2 Divisão endereços IP

O endereço IP identifica um equipamento na rede e deve obrigatoriamente ser exclusivos. Além disso, os endereços de rede são representados em decimal, divididos em quatro octetos separados por pontos.

O endereço IP mais baixo é 0.0.0.0 e o mais alto é 255.255.255.255, para dividir esses endereços foram criadas cinco classes de rede: A, B, C, D e E.

Os endereços da classe de rede A variam de 1 até 127, porém os endereços iniciados em 127 são utilizados para identificar a máquina local, assim os endereços válidos da classe A são de 1 até 126.

As redes classe B possuem os endereços divididos de 128 até 191 formando um total de 16.382 redes, já as redes classe C estão divididas entre 192 e 223 (os endereços 192 são utilizados nas redes internas).

As redes classes D são reservadas para endereços *Multicast* que fazem a entrega para um determinado grupo de usuários e as redes classe E são reservadas para utilização de testes futuros.

A distribuição dos endereços de IP é realizada pela ICANN (*Internet Corporation for Assigned Names and Numbers*), com essa atividade centralizada evitam-se conflitos na liberação dos endereços. Conforme Figura 4: Divisão classes IP (TANENBAUM, 2003).

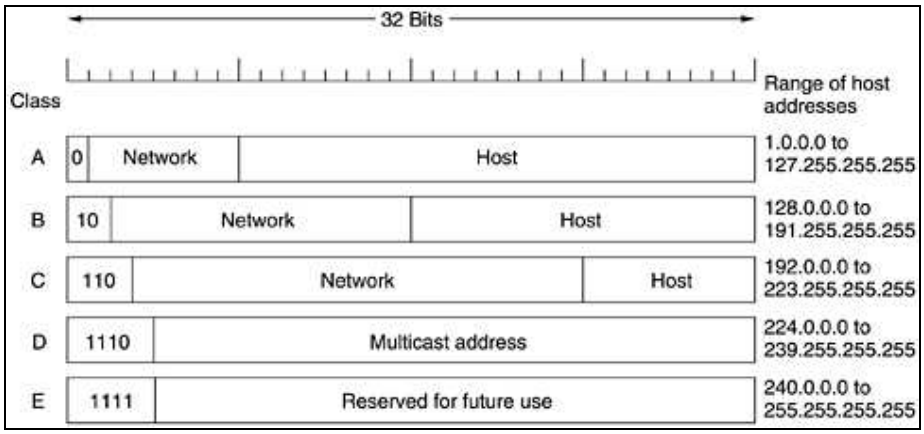

Figura 4: Divisão classes IP (TANENBAUM, 2003).

2.6.3 Endereços especiais IP

O endereço de IP possui divisões para utilização. Os valores 0 e 1 possuem significados especiais sendo que o valor 0 identifica a rede ou host, já o valor 1 identifica todos os hosts.

O endereço de IP 0.0.0.0 é usado nas inicializações dos hosts e onde possui o número 0 referenciam a rede atual.

O endereço de IP 1.1.1.1 permite que uma LAN, que possui valores 1 enviem pacotes de difusão para LANs distantes.

Os endereços iniciados com 127 são reservados para teste de *loopback*, por exemplo, 127.0.0.1, os pacotes enviados para este IP não são transmitidos, é normalmente utilizado para testes locais. Conforme mostra a Figura 5: Divisão endereços IP (TANENBAUM, 2003).

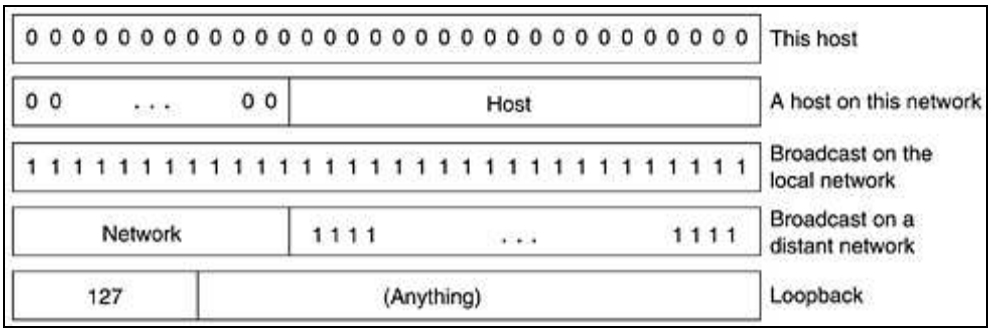

Figura 5: Divisão endereços IP (TANENBAUM, 2003).

2.6.4 Endereçamento IPv4

Segundo (KUROSE, 2005):

> " há cerca de 4 bilhões de endereços IP possíveis. Esses endereços são escritos em notação decimal separada por **pontos**, na qual cada byte do endereço é escrito em sua forma decimal e separado dos outros bytes do endereço por um ponto. Por exemplo, considere o endereço IP 193.32.216.9. O 193 é o número decimal equivalente aos primeiros 8 bits do endereço; o 32 é o decimal equivalente ao segundo conjunto de 8 bits do endereço e assim por diante. Por conseguinte, o endereço 193.32.216.9, em notação binária seria: 11000001 00100000 11011000 00001001."

Cada interface ou nó possui um endereço de IP exclusivo e uma parte do endereço IP determina a sub-rede. A sub-rede pode ser definida como uma parte de uma rede maior e normalmente é dividida em várias redes menores. Para a sub-rede é passado um endereço de IP, com uma notação /24 (máscara de rede), essa máscara com 32 bits reserva 24 bits para definir o endereço de IP.

2.7 IPv6

No início da década de 1990, a IETF iniciou um esforço para desenvolver o sucessor do protocolo IPv4. Uma motivação primária para esse esforço foi o entendimento de que o espaço de endereços IP de 32 bits estava começando a escassear, com novas sub-redes e nós IPs sendo anexados à Internet (e ainda

recebendo endereços IP exclusivos) a uma velocidade considerável. Para atender a essa necessidade de maior quantidade de endereços IP, um novo protocolo IP, o IPv6, foi desenvolvido. Os projetistas do IPv6 também aproveitaram essa oportunidade para ajustar e ampliar outros aspectos do IPv4 com base na experiência operacional acumulada sobre esse protocolo (KUROSE, 2005).

O momento em que todos os endereços IPv4 estariam alocados (e, por conseguinte, mais nenhuma sub-rede poderia ser ligada à Internet) foi objeto de considerável debate ocorrido em 1995. Com base nas tendências correntes sobre alocação de endereços existentes na época, estimou-se que os endereços se esgotariam entre 2008 e 2018 (Solensky, 1996).

Em 1996, o Registro Americano para Números da Internet (*American Registry for Internet Numbers* – Arin) informou que já tinham sido alocados todos os endereços da classe A do IPv4, 62 por cento dos endereços da classe B e 37 por cento dos endereços da classe C (Arin, 1996).

Embora essas estimativas e números sugerissem que havia um tempo considerável até que o espaço de endereços IPv4 fosse exaurido, ficou claro que seria necessário um tempo expressivo para disponibilizar uma nova tecnologia em escala tão gigantesca. Assim, foi dado início ao esforço denominado Próxima Geração do IP (*Next Generation* IP – IPng) (Bradner, 1996; RFC 1752) (KUROSE, 2005).

O resultado desse esforço foi a especificação IP versão 6 (IPv6) (RFC 2460). Foi proposto inicialmente que o protocolo ST-2 se tornasse o IPv5, porém, mais tarde, este protocolo foi descartado em favor do RSVP (KUROSE, 2005).

2.7.1 Estrutura do IPv6

Muitas alterações e inclusões foram realizadas neste novo protocolo IPv6, isso ocorreu pelo fato do IPv4 ter sido projetado para uma estrutura bem menor que a atual.

A nova estrutura do IPv6 possui alguns aspectos diferentes se comparada a do IPv4; uma das principais alterações reside no cabeçalho que contém informações para transferência do pacote na rede como versão do protocolo, tipo de dados de origem e de destino, além de que vários campos foram alterados ou removidos.

O IPv4 é composto de 12 campos fixos, variando o tamanho entre 20 e 60 bytes. Além disso, seis campos do IPv4 foram retirados por não serem utilizados ou foram adicionados para o cabeçalho de extensão. Conforme mostra a Figura 6: Estrutura cabeçalho IPv6 (IPv6.br).

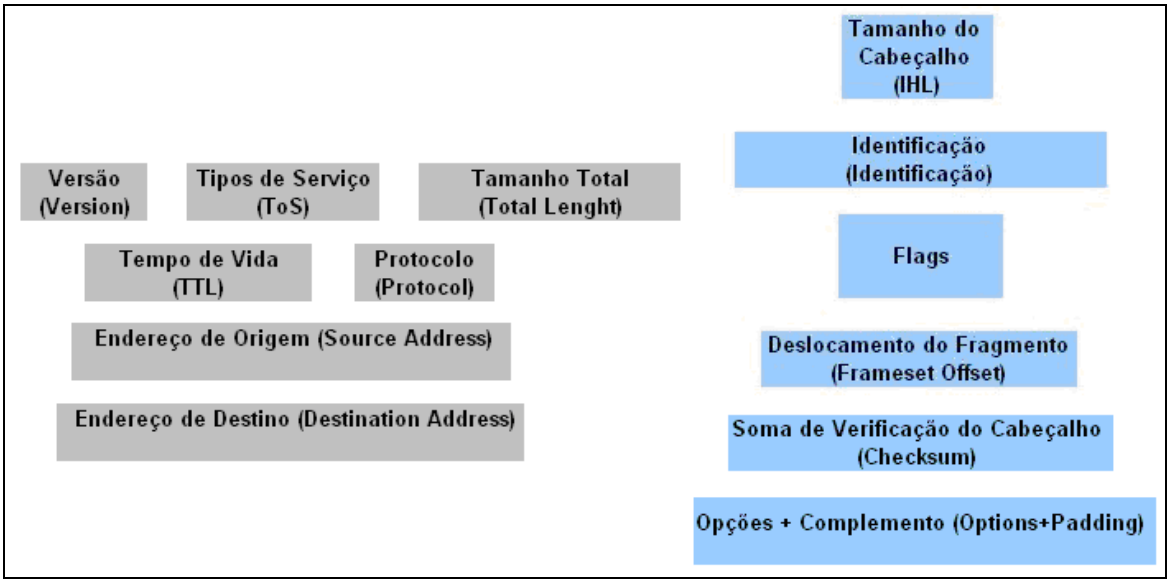

Figura 6: Estrutura cabeçalho IPv6 (IPv6.br).

Os campos removidos foram o Tamanho do Cabeçalho, Identificação, *Flags*, Deslocamento do Fragmento, Soma de Verificação do Cabeçalho, Opções e Complemento.

Para os roteadores entenderem e processarem a informação de forma rápida, foram modificados os nomes e o posicionamento dos campos Classe de tráfego *(Traffic Class)*, Tamanho dos dados (*Payload Length*), Limite de Encaminhamento (*Hop Limit*) e Próximo Cabeçalho (*Next Header*). Também foi adicionado o campo

Identificador de Fluxo (*Flow label*) com suporte à QoS (*Quality of Service*), conforme a Figura 7: Cabeçalho IPv6.

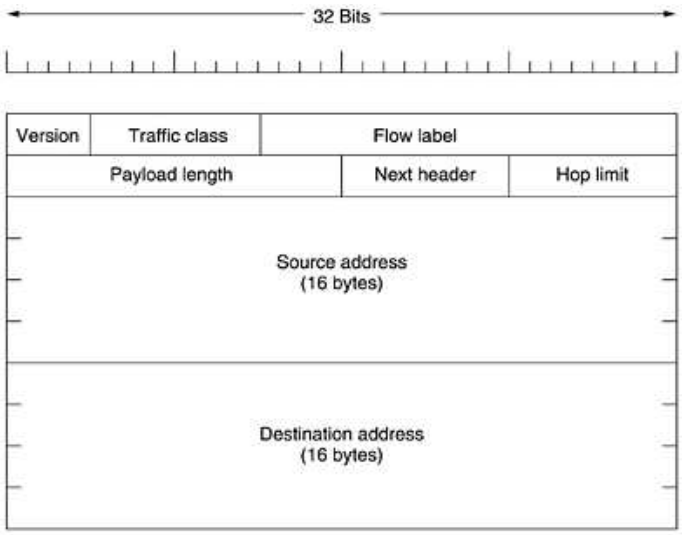

Figura 7: Cabeçalho IPv6 (TANENBAUM, 2003).

Os campos e sua função são apresentados a seguir:

Version – Atual versão do IP.

Priority – Prioriza pacotes, por exemplo, dar preferência aos pacotes de voz.

Flow label – Controla e identifica o fluxo do pacote.

Payload Length – Complemento ao tamanho do pacote, após o cabeçalho utiliza os octetos restantes do pacote.

Next Header – Possui duas funções, primeiramente indicar se é um cabeçalho de extensão, caso não seja mostra o protocolo de transporte.

Hop Limit – Controla a quantidade de roteamentos do pacote, é adicionado informações a cada ponto que o protocolo passa, porém se o valor chegar a zero o pacote é descartado.

Source Address – Identifica o remetente.

Destination Address – Identifica o destino.

Existe também o cabeçalho de extensão que foi criado para alocar alguns campos que são utilizados no IPv4 e fornecer informações adicionais. O cabeçalho de extensão esta incluído entre o cabeçalho do IPv6 e os dados a serem transmitidos. Abaixo, Figura 8: Cabeçalho de extensão.

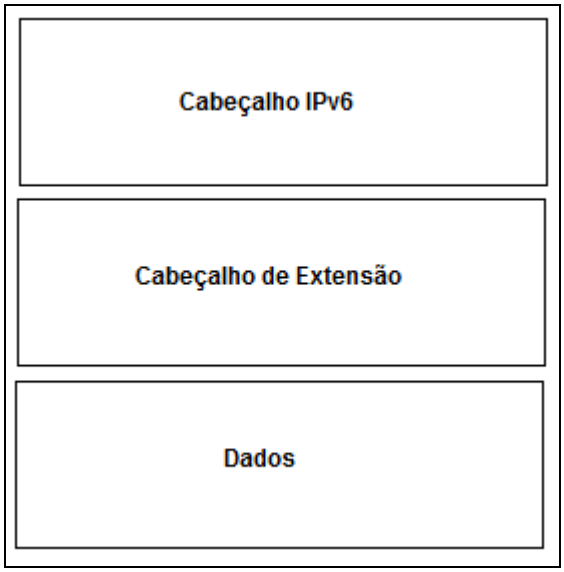

Figura 8: Cabeçalho de extensão (Adaptado de IPv6.br)

2.7.2 Divisão endereços IP

O tamanho de endereçamento do protocolo IPv6 é de 128 bits, sendo que o endereço IP é representado no formato hexadecimal, dividido em octetos de 16 bits e separados por ":". Outra alteração realizada no protocolo IPv6 foi retirar a divisão de classes, pois a quantidade de IPs (2^{128}) chega a octilhões de endereços.

O IPv6 utiliza formato hexadecimal representado por: 2001:0db8:85a3:08d3: 1319:8a2e:0370:7344.

Caso seja feita interação entre duas redes, sendo uma com o IPv4 e outra com IPv6, o endereço IP ficaria dividido em dez partes sendo 96 bits + 32 bits em decimal, conforme: 0:0:0:0:0:0:192.168.20.30.

Além disso, é possível abreviar o grupo que contém zeros com os caracteres "::", mas só pode ser feito uma única vez, conforme Figura 9: Endereçamento IPv6.

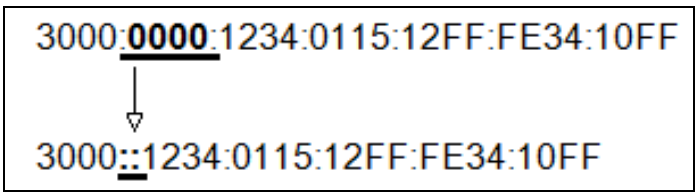

Figura 9: Endereçamento IPv6 (SIVASUBRAMANIAN, 2005).

Os endereços de IPs são divididos nos seguintes grupos:

- ***Unicast* (Ponto-a-Ponto)**: O endereço identificado é enviado para um *host* na mesma rede.
- ***Global Unicast***: Endereço global e público que será utilizado por todos na internet. Como exemplo 2000::/3 e 2002::/16 (reservado para Túnel Ponto-Multiponto 6to4).
- ***Unique Local***: É identificado através do padrão: FC00::/8 e é acrescentado um ID global de 40 bits, não é redirecionado na internet.
- ***Link Local***: Definido automaticamente, mas só é válido dentro da mesma rede (enlace), é identificado através: FE80::/64.
- ***Loopback***: Utilizado para testes de rede, identifica a rede local ::1/128.
- ***Unspecified***: Identifica quando não possui endereço alocado **::** .
- ***Multicast***: Substituto do *broadcast* utilizado no IPv4. O endereço é enviado a um grupo de *hosts* que compartilham uma mesma função FF00::/8.

- ***Anycast***: O endereço é enviado a um grupo de *hosts* que realizam a mesma função.

2.7.3 Tipos de configuração IPv6

Para configuração e utilização dos *hosts* e nós no IPv6 foram criado novas funcionalidades de configuração, podendo ser configuradas exclusivamente ou utilizados dois mecanismos simultaneamente: o *stateless* e o *stateful*.

O ***Stateless*** faz a configuração automática dos nós sem a necessidade do DHCP (*Dynamic Host Configuration Protocol*), não mantém informações de "*leases*" entregues, fornece informações da rede (2000:1234:abcd::/64), configurações de DNS (*Domain Name System*) e *Default Gateway*.

Através do *stateless* é possível fazer a configuração *unicast* sem a necessidade de configuração manual de servidores, gerando automaticamente únicos endereços *link-local*. Esses endereços utilizam o padrão FE80::/64, o MAC da interface de rede e quando possui apenas 48 bits, acrescenta FFFE no centro e altera o 7° *bit* do *byte* mais significativo do IPv4, conforme Figura 10: Endereços *Stateless*.

Endereço de Rede: (3000:0000:1234:/64)
MAC da interface: (0015:1234:10FF)

Endereço de Rede	1ª parte do MAC	Complemento	2ª parte do MAC
3000:0000:1234	115:12:00	FF:FE	34:10FF

Figura 10: Endereços com *Stateless* (SIVASUBRAMANIAN, 2005).

IP: 3000:0000: 0015:1234:12FF:FE34
IP: 3000:0010: 0015:1234:12FF:FE34 (Invertido 7º bit).

Total de *Bits* do IPv6 = 128, dividido em 64 bits de Rede, 48 bits de MAC e 16 bits de complemento (FF:FE).

O serviço DHCP no IPv6 “DHCPv6” utiliza o protocolo de transmissão UDP (*User Datagrama Protocol*) possui várias vantagens para a autoconfiguração *stateless*, porque fornece configurações de rede, como por exemplo o DNS, é também possível criar políticas de acesso e compartilhamento entre os *hosts*.

No ***stateful***, a autoconfiguração é uma possível configuração para o *stateless*, para isso é necessário que sejam passadas informações da rede; esta tarefa necessita da participação de servidores, sendo que os mesmos utilizam o endereço: (FF02::1:2 ou FF05::1:3) para recebimento de todas as mensagens dos *hosts*. Além disso, o serviço DHCP mantém informações de todas as "*leases*" entregues e fornece configurações da rede, DNS e *Default Gateway*.

2.7.4 Serviços IPv6

Atualmente o número de aplicações que suportam o protocolo IPv6 tem aumentado, em alguns casos suportando até as duas versões (IPv4 e IPv6), mas as mais atualizadas suportam apenas o IPv6.

2.7.4.1 ICMPv6

Muitos serviços foram alterados comparado ao IPv4, uma das principais mudanças foi no protocolo ICMP *(Internet Control Message Protocol)* utilizado para passar informações da rede, emitir relatórios com diagnósticos e erros dos pacotes.

Essas informações são obtidas através das trocas de mensagens, resultando nas Mensagens de Erro e Mensagens de Informação. Além disso, o ICMP assume as funções do ARP (*Address Resolution Protocol*) e IGMP *(Internet Group Management Protocol*) protocolo que gerencia os grupos *multicast*. O ICMPv6 faz a descoberta de vizinhança e gerência de grupos.

O cabeçalho do ICMPv6 possui a seguinte estrutura:

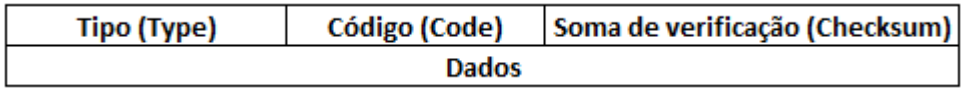

Figura 11: Cabeçalho ICMPv6 (IPv6.br).

Tipo: Formato da mensagem.

Código: Utilizado para acrescentar informações adicionais em alguns tipos de mensagens.

Soma de Verificação: Faz a verificação do cabeçalho, testa se os dados estão corrompidos.

Dados: Mostra informações da mensagem como erros e identificação da mensagem.

O ICMPv6 trabalha com cinco mensagens:

- ***Router Solicitation***: Usado para solicitar mensagens *Router Adversitements* aos roteadores na rede;
- ***Router Advertisements***: Utilizada para responder a *Router Solicitation*, envia mensagens seqüencialmente e anuncia localidade em um enlace;
- ***Neighbor Solicitation***: É uma mensagem *multicast*, ou seja, envia a informação para um grupo de destinatários, através desta mensagem determina o endereço MAC e mostra se existe IPs duplicados;
- ***Neighbor Adversitements***: É uma resposta a *Neighbor Solicitation* e identifica alterações de endereços MACs;
- ***Redirect***: Redireciona os *hosts* ao roteador mais próximo para chegar ao destino;

2.7.4.2 Descoberta de vizinhança

Outro serviço para o IPv6 é o protocolo *Neighbor Discovery* (Descoberta de Vizinhança) que interage com o IPCMPv6 utilizando as cinco mensagens citada na seção anterior. A descoberta de vizinhança é utilizada pelos equipamentos (*hosts e routers*) para identificar os endereços MAC da rede, encontrar roteadores mais próximos, mostrar endereços duplicados, redirecionar pacotes, determinar e configurar os endereços da rede. Este serviço substitui a função da tabela ARP utilizada no protocolo IPv4.

2.7.4.3 Fragmentação

A fragmentação implementada no protocolo IPv6 é bem diferente do protocolo IPv4, antes de mostrar as principais mudanças é necessário entender o processo de fragmentar, que significa dividir em várias parte ou fragmentos.

Para fragmentar pacotes de dados é utilizado o protocolo "*Path MTU Discovery*", este protocolo tenta descobrir qual o maior tamanho de pacote que se indica para a transferência, faz a identificação dos dados do pacote como o tamanho máximo, identificando os MTUs (*Maximum Transfer Unit*) durante o caminho, desde a origem até o destino. No IPv6 faz-se a fragmentação apenas na origem diminuindo o processamento e armazenamento do cabeçalho durante a transmissão.

O *Path MTU Discovery* define o tamanho máximo do pacote desde o primeiro salto, porém se o roteador não suportar essa funcionalidade, este pacote será descartado retornando uma mensagem (*packet too big*); através dessa mensagem o emissor identifica o tamanho que o roteador suporta e retransmite o pacote.

No protocolo IPv4 o processo é diferente, o próprio roteador fragmenta durante o caminho dividindo em pacotes menores, esse processo pode ser realizado diversas vezes dependendo da rede.

2.7.4.4 *Quality of Service* (QoS)

O serviço QoS (*Quality of Service)* tem o mesmo objetivo para as duas versões do protocolo IP, garantindo controle e priorização dos pacotes, principalmente de pacotes de voz, dados e jogos *online*. A única mudança no IPv6, é a inclusão de campos Classe de Tráfego e o Indicador de Fluxo no Cabeçalho.

O campo Classe de Tráfego mostra informações de identificação do tipo do pacote (classes e prioridades) e o campo Indicador de Fluxo de Cabeçalho faz a identificação do fluxo; durante a transmissão este campo é preenchido com valores de 00001 e FFFFF, sendo que pacotes que não pertencem ao fluxo são identificados com 00000 e pacotes de mesmo fluxo são todos identificados com um mesmo valor.

Caso o campo contenha *Hop-by-Hop* todos os nós da rede deverão incluir esta mesma opção.

Com o serviço de QoS é possível definir um padrão, desde a origem estendendo a todos da rota até chegar ao destino.

2.7.4.5 Mobilidade

Uma das melhorias do protocolo IPv6 é o suporte à mobilidade que já vem ativado no protocolo, procedimento que não foi implantado no IPv4, pois não foi previsto o grande crescimento da rede Internet.

A mobilidade foi publicada na (RFC 2002) (IP *Mobility Support*) desde 1996 e contém informações para ativação e suporte, mas já existem diversos documentos com atualizações e melhorias.

Além disso, no cabeçalho de extensão foi acrescentada também a opção *Mobility,* que é utilizada nas trocas de mensagens entre Agente Remoto e Nó Correspondente, nela estão às informações dos endereços. Conforme Figura 12: Cabeçalho Mobilidade.

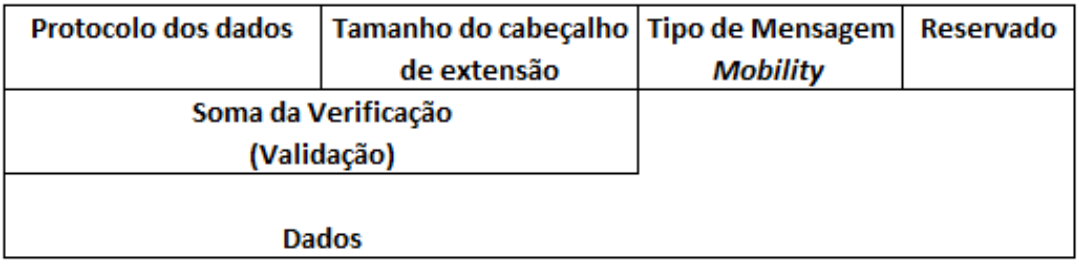

Figura 12: Cabeçalho Mobilidade (IPv6.br).

- **Protocolo de dados**: Mostra se existe o Próximo Cabeçalho;
- **Tamanho do cabeçalho de extensão**: Mostra o tamanho máximo do cabeçalho *Mobility*;
- **Tipo de Mensagem *Mobility***: – Identifica qual é o tipo da mensagem transmitida;
- **Soma de Verificação**: Faz a validação do cabeçalho, garante a integridade e autenticidade das informações;
- **Dados**: Contêm os dados do cabeçalho o tamanho pode variar de acordo com as informações enviadas;

Através da técnica de mobilidade é possível que um dispositivo móvel mude de uma rede para outra sem perder as informações originais, sem a necessidade de trocar o endereço de IP, isso torna o processo mais fácil, porque não perde informações enviadas para o dispositivo e também porque a mudança de local acaba sendo invisível para os protocolos. Para que este processo funcione é feita a associação dos dois endereços através do Agente de Origem.

Basicamente o Agente de Origem mantém os dois endereços e faz o registro do endereço remoto, após isso, para que as informações cheguem ao dispositivo, são enviadas as mensagens: *Binding Update* (solicitação) e *Binding Acknowledgement* (resposta), conforme a Figura 13: Troca de Mensagem.

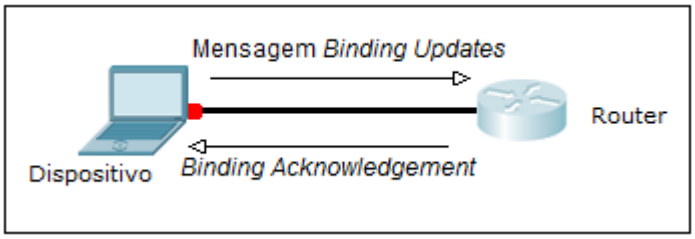

Figura 13: Troca de Mensagem (IPv6.br).

Para que os dispositivos funcionem com a técnica da mobilidade, primeiramente o IPv6 requisita o endereço de IP original chamado de *home address*; durante o processo de deslocamento o dispositivo requisita um novo endereço denominado “endereço remoto” através das configurações *stateless* ou *stateful*, o dispositivo então envia uma mensagem para a rede original informando o IP remoto e todos os pacotes enviados para a rede original, são roteados automaticamente para a nova rede, conforme a Figura 14: Comunicação Mobilidade.

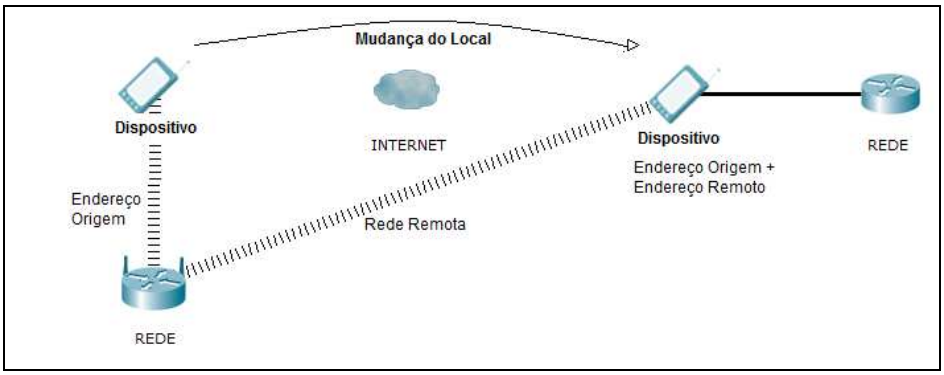

Figura 14: Comunicação Mobilidade (IPv6.br).

Após manter a autenticação do dispositivo na rede de origem sem perder as informações, são então transportados os pacotes através de duas maneiras de comunicação.

No **Tunelamento Bidirecional**: os pacotes enviados para o *home address* passam pelo Agente de Origem, que transmite para um túnel até o nó móvel, identificando através do endereço remoto. Após receber os pacotes, responde para

o Agente de Origem que envia novamente para o túnel até chegar ao nó correspondente, neste processo não é necessário ter suporte ao IPv6.

Já na **Otimização de Rota** faz-se a comunicação direta entre o nó móvel e o nó correspondente, o Agente de Origem não possui controle. A comunicação é feita após o nó móvel cadastrar o endereço remoto ao nó correspondente, os dados ficam armazenados em *cache* e é feita a união do endereço de origem e do endereço remoto.

Para realizar a comunicação e trocar informações, a mobilidade do IPv6 utiliza mensagens criadas para o protocolo ICMPv6, as mais utilizadas são:

Binding Refresh Request: Solicitação de atualização de endereços do Nó Correspondente para o Nó Móvel;

Binding Update: Mensagem enviada para informar a atualização do Endereço Remoto, do Nó Móvel ao Agente de Origem ou Nó Correspondente;

Binding Ack: Mensagem de resposta ao *Binding Update*, confirmação de recebimento;

Binding Error: Nó Correspondente envia mensagem de erro, para mostrar falhas;

2.7.4.6 DNS

O DNS (*Domain Name System*) faz a resolução dos nomes de domínios para endereços de IP e o processo reverso, possui uma estrutura hierárquica distribuída em uma árvore invertida, buscando os dados mais próximos e armazenando em *cache*, porém para funcionar no IPv6 foram necessário fazer algumas alterações. Essas mudanças foram acrescentadas na (RFC3596).

Foi acrescentado ao DNS um novo registro para armazenar os endereços IPv6 e também foi criado um novo modelo no formato AAAA ou quad-A, para realizar a conversão de domínios ou endereços IPv4 em endereços IPv6.

2.7.4.7 Segurança

Para adicionar segurança ao IPv6 foi criado o IPSec, protocolo que atua na camada de rede e também pode ser utilizado no IPv4, desde que não possua estrutura NAT, pois não é possível identificar o real emissor dos dados. O IPSec (*IP Security Protocol*) tem por objetivo proteger o pacote de dados, ou seja, proteger as informações do cabeçalho e das chaves criptografadas, ser compatível com outras aplicações de segurança e evitar problemas de criptografia. Além disso, o IPSec mantém a privacidade do usuário, como por exemplo, guardando as informações passadas pelos usuários em pontos de acesso aos dados bancários (*Internet Banking*).

O IPSec foi desenvolvido pelo IETF, para resolver os problemas de segurança do protocolo IPv4, e está descrito em (RFCs 2401), (2402) e (2406). Para a IETF a segurança tem que começar desde a camada de aplicação e se estender as demais.

A estrutura do IPSec possui diversos algoritmos, os principais serviços não são divulgados para garantir integridade dos dados e baseia-se na criptografia de chave simétrica. Tal estrutura é dividida em duas partes principais, uma que descreve os novos cabeçalhos que controlam o transporte do pacote e a outra que cuida da integridade e compartilhamento das chaves é denominado ISAKMP (*Internet Security Association and Key Management Protocol*).

O IPsec atua na camada de rede, desta forma é possível proteger os dados, aplicativos e serviços, garantido a integridade das informações. Conforme Figura 15: Localização IPsec.

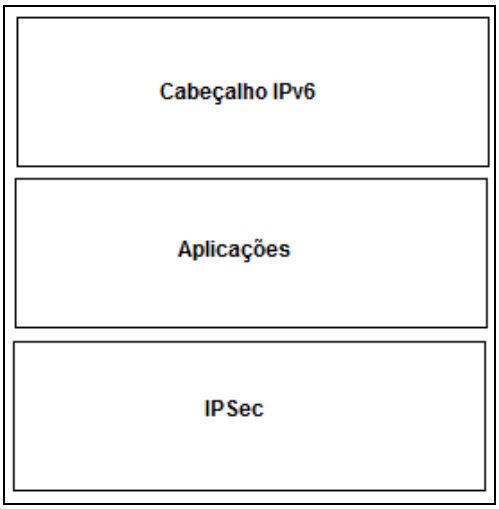

Figura 15: Localização IPSec (IPv6.br).

O IPSec é constituído pelos cabeçalhos AH (*Authentication Header*) e ESP (*Encrypted Security Payload*).

AH (*Authentication Header*) – Parte do cabeçalho de extensão criado para o IPv6, armazena e controla a autenticação através do cabeçalho e do datagrama IP, assegurando informações da origem e garantido que o pacote não foi alterado durante o tráfego das informações. Este mecanismo utiliza a criptografia MD5 (*Message-Digest 5*), algoritmo criado para verificar a integridade dos dados, através de mensagens com 128 bits.

Possui cabeçalho de autenticação com a seguinte estrutura:

Próximo Cabeçalho	Tamanho do Módulo	Reservado
Segurança SPI		
Número de seqüência		
Dados de Autenticação		

Figura 16: Cabeçalho de Autenticação (IPv6.br).

ESP (*Encrypted Security Payload*) – este cabeçalho oferece confidencialidade e integridade. Os dados são cifrados através de uma chave,

compartilhada entre o receptor e o transmissor, assim caso os dados sejam interceptados, por pessoas não autorizadas, estas não terão acesso ao conteúdo.

Além disso, o ESP possui o algoritmo de criptografia DES (*Data Encryption Security*) criado para criptografar e fazer a análise dos dados distribuídos na rede, reforçando a segurança. Através do DES, a origem e o destino concordam com uma chave secreta de autenticação; após validado, os dados são compartilhados.

O ESP possui cabeçalho com a seguinte estrutura:

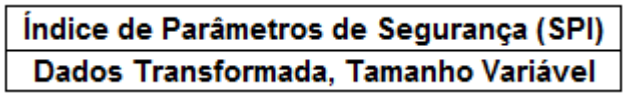

Figura 17: Cabeçalho de Encapsulamento de Dados (MIRANDA, JÚNIOR).

Além disso, o ESP pode ser utilizado de duas maneiras, uma através de transporte (*transport-mode*) ou então através de túnel (*tunnel-mode*) e tem por objetivo proteger os pacotes IP de formas diferentes, o ***transport-mode*** protege as camadas superiores, codifica os dados da camada de transporte e acrescenta um novo cabeçalho, este modelo é ideal para redes pequenas; já o ***tunnel-mode****,* por sua vez, também protege o pacote IP e codifica os dados, mas estabelece conexão e transmite os dados através de um túnel.

Com a criação do IPv6 foi eliminado o uso do NAT permitindo que o IPSec funcione corretamente e identificando a real origem dos dados, mas é importante acrescentar que para utilização com segurança é obrigatório que esteja habilitado em toda a rede de comunicação.

No entanto, o IPSec não consegue evitar algumas falhas de segurança como: A Engenharia Social, Desastres Naturais, Ataques Físicos, Pragas da Internet (Vírus) e Ataques ICMPv6.

Outra melhoria de segurança no IPv6 é a inviabilidade de varredura de endereços de IP na rede; esta técnica é muito utilizada em ataques, com o protocolo

IPv6 não é viável pela grande quantidade de endereços disponíveis na rede. Para realizar este processo, dependendo o número de IPs, demoraria muito, podendo chegar a anos.

É importante acrescentar que apenas o IPSec não irá resolver todos os problemas de segurança, é necessário utilizar outros mecanismos de proteção como, por exemplo, o *firewall* e ferramentas de bloqueio de portas.

Além disso, com o novo modelo hexadecimal alguns endereços de IP serão mais visados para ataques, principalmente os IPs fáceis de memorizar, como por exemplo, terminados com ::10, ::30, ::DADO, ::CAFE.

2.7.5 Transição IPv4 e IPv6

Durante a implantação do IPv6, o IPv4 ainda ficará ativo até a migração de todas as aplicações e os dois trabalharão juntos, ainda alguns anos. O IPv6 e IPv4 não são diretamente compatíveis, portanto uma rede com IPv4 não se comunica diretamente com redes IPv6. Para resolver este problema foram criadas algumas técnicas para a transição.

Para a comunicação entre redes IPv6, passando por uma rede IPv4 é necessário utilizar a técnica de tunelamento e para a comunicação direta entre os dois protocolos pode ser usado o método de pilha dupla e de tradução com NAT-PT.

2.7.5.1 Pilha Dupla (*Dual-Stack*)

Esta técnica foi criada para ser utilizada durante a transição e tem suporte para as duas versões do protocolo IP. A Pilha Dupla tem por objetivo suportar aplicações e serviços dos protocolos, consegue enviar e receber mensagens, são adicionadas no mesmo local e durante uma comunicação IPv4 uma das pilhas mantém o formato IPv4, se a comunicação for IPv6 é feito da mesma maneira.

Através dessa técnica o protocolo IPv6 consegue comunicar com o IPv4, retirando a incompatibilidade entre as versões, para que este método funcione são habilitados dois endereços, o IPv6 é configurado através dos métodos de autoconfiguração (*stateless* e *stateful*) e também existe duas tabelas de roteamento para os protocolos, conforme a Figura 18: Estrutura Pilha Dupla.

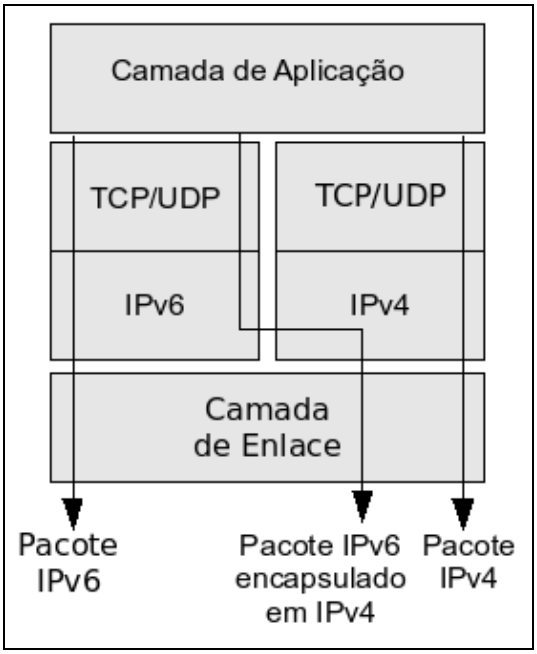

Figura 18: Estrutura Pilha Dupla (SANTOS, 2008).

2.7.5.2 Tunelamento (*Tunnel*)

A técnica de tunelamento foi criada principalmente para tornar a comunicação entre redes IPv6, utilizando recursos IPv4. Para que o processo de transmissão funcione corretamente é necessário que a origem e o destino suportem a comunicação com os dois protocolos.

Segundo (Comer, 2001):

> "A técnica de tunelamento consiste em encapsular um pacote de um protocolo dentro de outro permitindo assim que a informação seja transportada sobre o segundo protocolo garantindo a entrega do pacote."

Os tuneis IPv6 seguem o modelo de configuração abaixo:

Estático: Sempre ponto-a-ponto, redes interligadas diretamente, sem dispositivos de divisão.

Dinâmicos: A configuração é feita baseada em multipontos e requerem mais processamento.

2.7.5.3 Tradução (*Translation*)

Outro método criado para a transição e comunicação entre os protocolos é a tradução, que transforma os dados no formato IPv4 em IPv6 e IPv6 em IPv4. Esta técnica é rápida, porém possui falhas de segurança e conexão ponto-a-ponto.

2.8 Situação Atual

A previsão para implantação do protocolo IPv6 anteriormente era até o final de 2010, mas como muitos locais ainda não estão preparados, a nova previsão é que será implantado até o final de 2012.

As grandes operadoras ainda não possuem estrutura e suporte para atualização, mas os endereços de IPv4 disponíveis controlados pelo IANA (*Internet Assigned Numbers Authority*) praticamente esgotaram.

Os únicos IPs disponíveis estão divididos entre as RIRs (*Regional Internet Registry*), para controlar e liberar os endereços IP, somente através das prioridades.

O IANA órgão responsável pela divisão dos endereços, fará a distribuição dos endereços no formato IPV6, seguindo o procedimento da Figura 19: Estrutura Liberação IP.

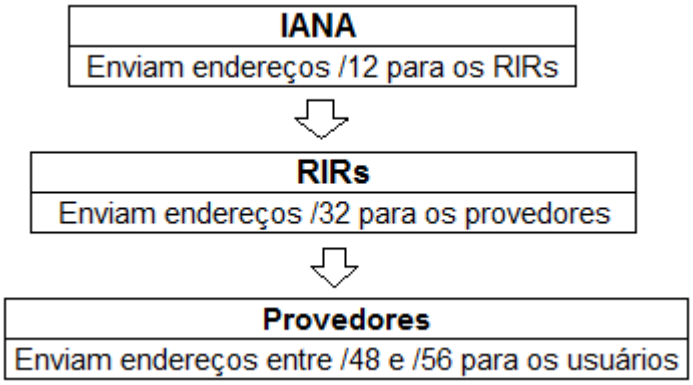

Figura 19: Estrutura Liberação IP (IPv6.br).

2.8.1 Suporte IPv6

Atualmente muitas aplicações incluindo sistemas operacionais suportam a estrutura do IPv6, sendo que possuem o protocolo habilitado por padrão. Os sistemas operacionais que possuem o suporte são:

Windows: As versões do Vista e Seven vem configuradas por padrão, sem a necessidade de instalação, o XP desde a versão SP1 (*Service Pack*), SP2 e SP3 e as versões 2003, 2008 e SE para servidores estão com as versões habilitadas.

MAC OS X: Habilitado desde a versão 10.2 - Jaguar.

BSD: O Unix também possuem compatibilidade com o protocolo IPv6. As distribuições FreeBSD desde a versão 4.0, NetBSD versão 1.5 e OpenBSD versão 2.7.

Linux: Todas as distribuições possuem suporte desde a versão 2.2.x.

Além das aplicações, a Cisco, 3com, Juniper e Alcatel-Lucent, principais empresas fabricantes dos equipamentos de rede como roteadores e *switches*, também estão se adequando para suportar o novo protocolo IPv6 e já possuem o hardware e software devidamente atualizado.

2.8.2 Sites na Internet

Atualmente os sites ainda estão se atualizando para que os usuários que utilizem o IPv6 consigam acessar o conteúdo das páginas.

Segundo a ISOC (*Internet Society*), o dia 08 de junho de 2011, será considerado o DIA D para o IPv6, pois os grandes provedores e redes sociais disponibilizarão as páginas no formato IPv6. Alguns dos participantes são: Google, Facebook, Yahoo, IG e Terra, as páginas ficaram disponíveis por 24 horas para os usuários que estejam em redes IPv6. Além de ser utilizado para testes este dia também incentivará para que todos se adéqüem a nova estrutura de rede. A ISOC disponibilizou no link: http://www.worldipv6day.org/participants/index.html os principais participantes do (World IPv6 Day).

Existe o site: http://validador.ipv6.br/ que foi criado para testar se a página da web esta no formato IPv6.

3 DESENVOLVIMENTO

A realização do desenvolvimento partiu da necessidade de aplicar os conceitos adquiridos e conhecer a nova estrutura do protocolo. A idéia inicial tinha por objetivo criar duas máquinas virtuais com o sistema operacional Windows XP, uma delas executando o protocolo IPv4 e outra o protocolo IPv6 e realizar testes de comunicação entre as duas versões.

Durante a realização deste desenvolvimento foi identificada a necessidade de aplicar técnica de tunelamento para fazer com que as duas se comuniquem; isto ocorreu devido os protocolos IPv4 e IPv6 não serem diretamente compatíveis.

Abaixo é ilustrada na Figura 20: A Estrutura das máquinas.

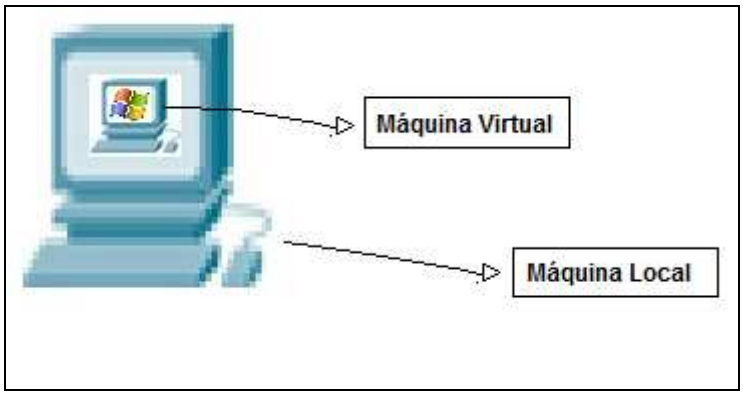

Figura 20: A Estrutura das Máquinas.

Máquina local: Sistema operacional Windows 7 Starter.

Máquina virtual: Configurada utilizando o VirtualBox Manager e com o sistema operacional Windows XP Professional – SP1.

3.1 Configuração

O primeiro passo é habilitar o protocolo IPv6, para isto é necessário seguir o seguinte caminho na maquina virtual utilizado o Windows XP.

Clicar no botão Iniciar, Configurações, Conexões de Rede, Abrir conexão local, clicar em propriedades e selecionar a opção instalar, Conforme Figura 21: Configurando IPv6.

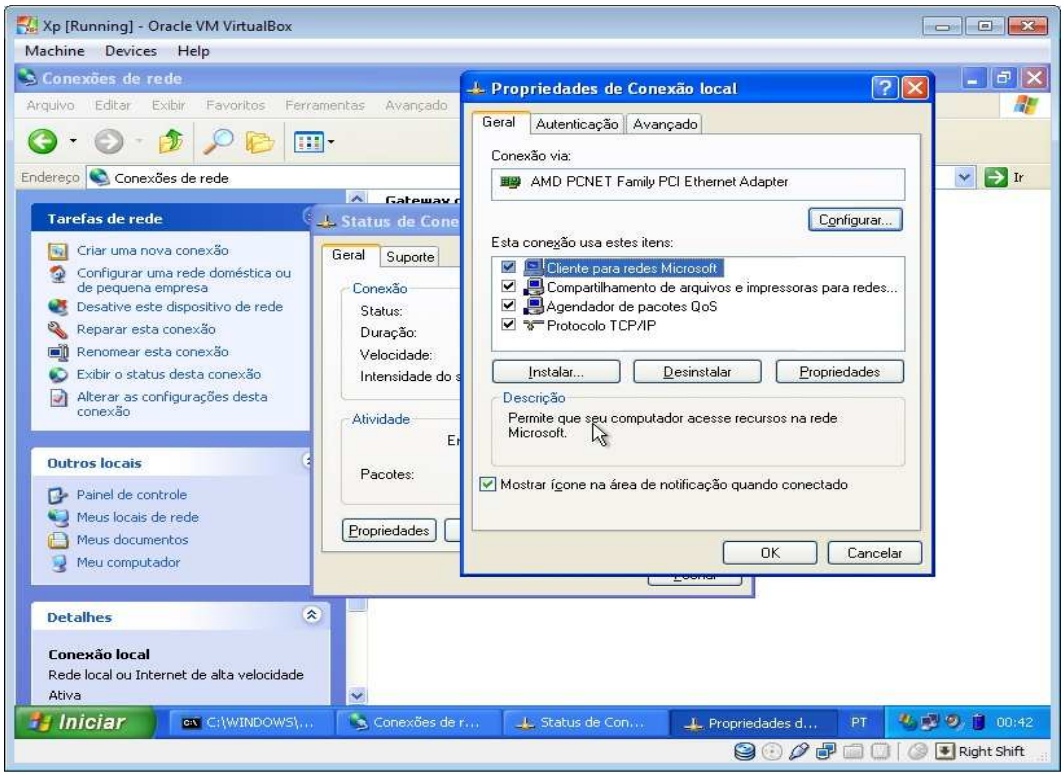

Figura 21: Configurando IPv6.

Após clicar em instalar, deve-se selecionar a opção Protocolo e escolher o item *Microsoft IPv6 Developer Edition*. Conforme Figura 22: Habilitando IPv6.

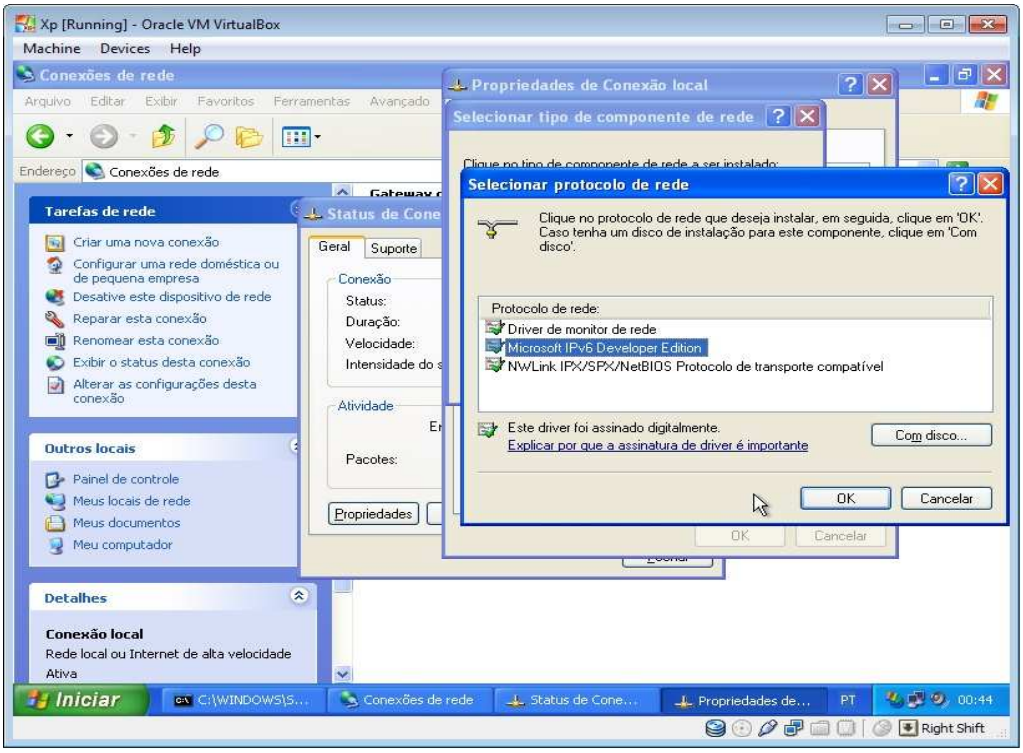

Figura 22: Habilitando IPv6.

Feito este processo será instalado o protocolo IPv6 na máquina e aparecerá o protocolo IPv6 habilitado, conforme Figura 23: IPv6 habilitado.

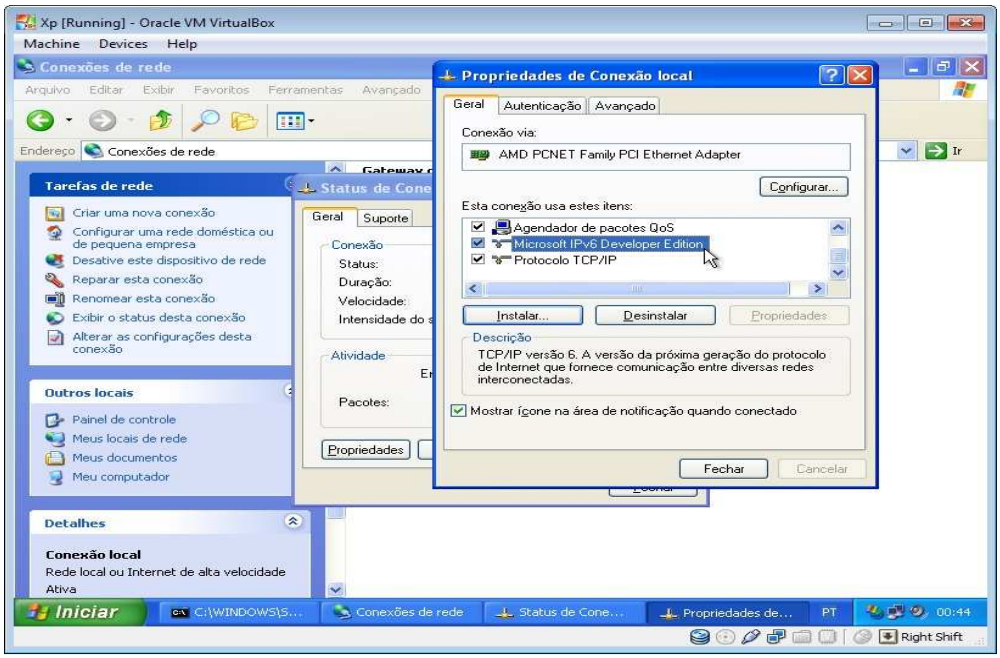

Figura 23: IPv6 habilitado.

Para testar se a instalação foi realizada corretamente é possível testar através do comando ipv6 ?. Este comando deve ser executado seguindo o procedimento: Abrir o *prompt* de comando (Iniciar, Executar, cmd) e digitar o comando ipv6 ?. Este comando mostrará caso esteja instalado as opções de comando que contém no protocolo, conforme Figura 24: Comando IPv6.

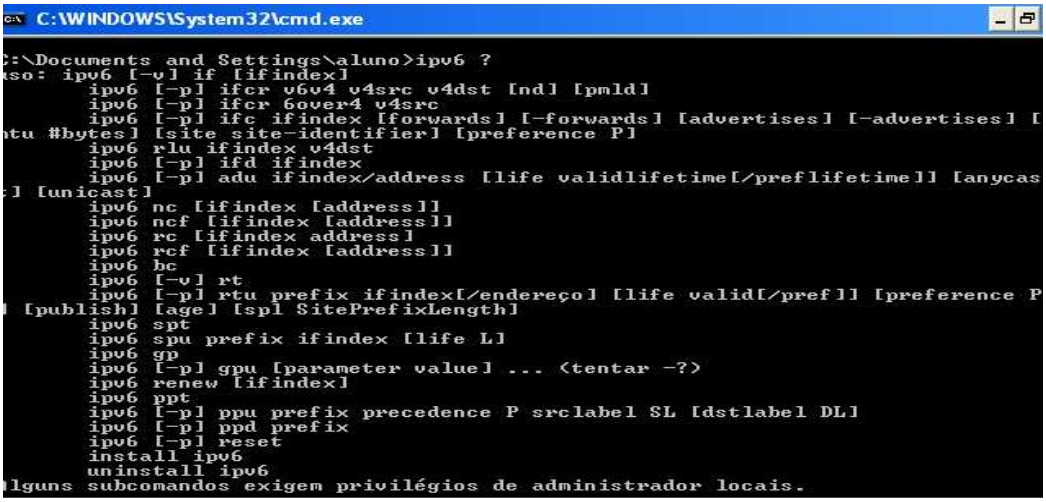

Figura 24: Comando IPv6.

Para identificar o endereço de IPv6 é necessário executar o comando: *ipconfig /all*.

Este comando apresentará o resultado, conforme Figura 25: Informações IP.

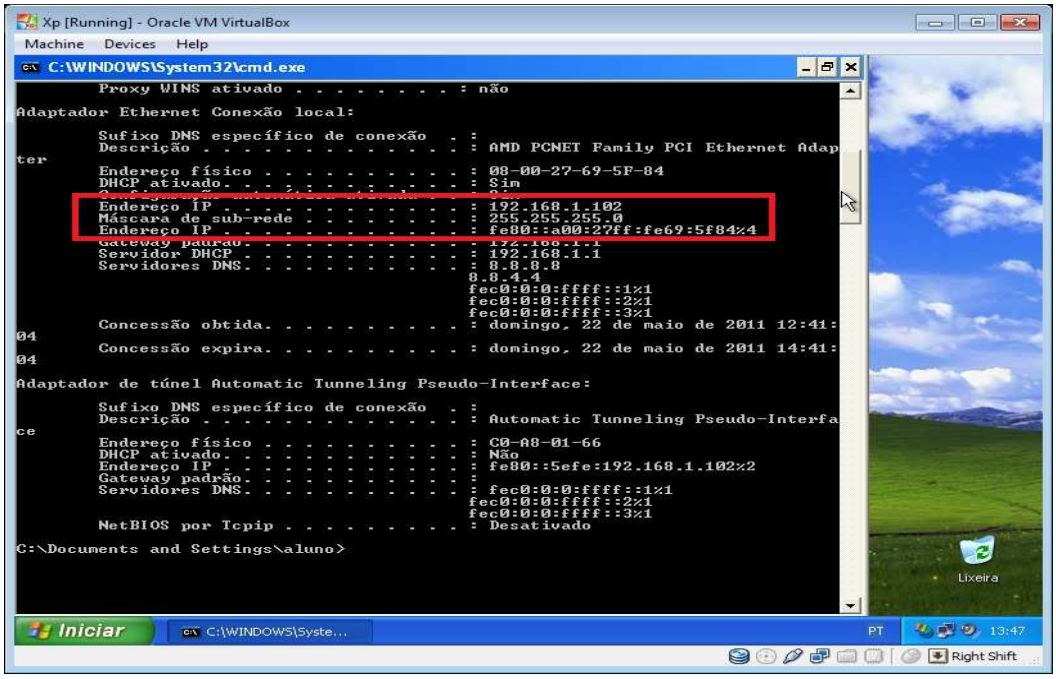

Figura 25: Informações IP.

Depois de identificar o endereço de IPv6 é necessário fazer o teste de *ping* para verificar a comunicação entre a máquina local e a máquina virtual. Neste caso, a máquina local realizará o comando conforme Figura 26: Endereços IP das máquinas.

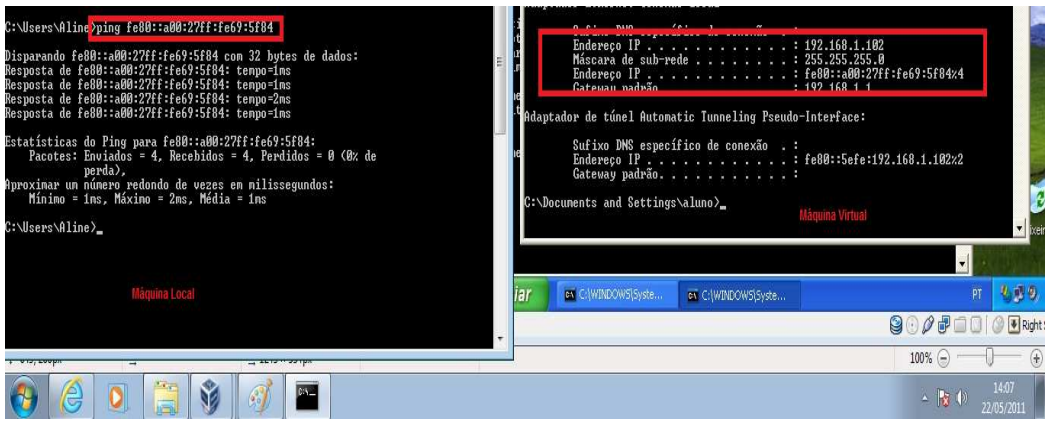

Figura 26: IP das máquinas.

Além disso, também foi efetuado teste de comunicação. Primeiramente foi compartilhada uma pasta com o nome Hi no Desktop, utilizando o endereço de IPv4 (192.168.1.102), foi possível o acesso a pasta, conforme Figura 27: Compartilhamento de pasta IPv6.

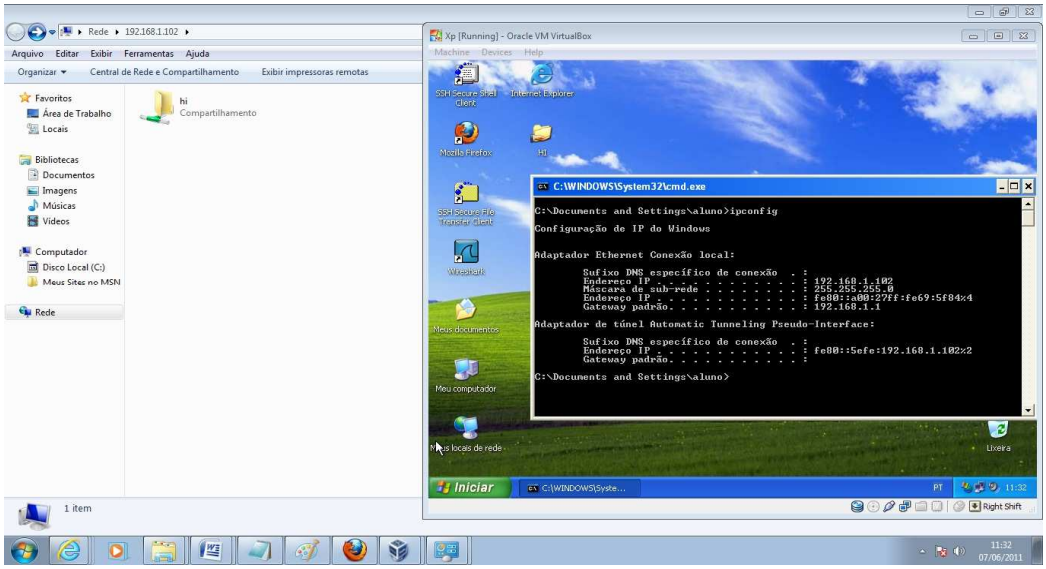

Figura 27: Compartilhamento de pasta - IPv4.

Ao efetuar teste com o endereço de IPv6 e o endereço de tunelamento, não foi possível o acesso a pasta compartilhada, conforme mostra a Figura 28: Compartilhamento de pasta – IPv6.

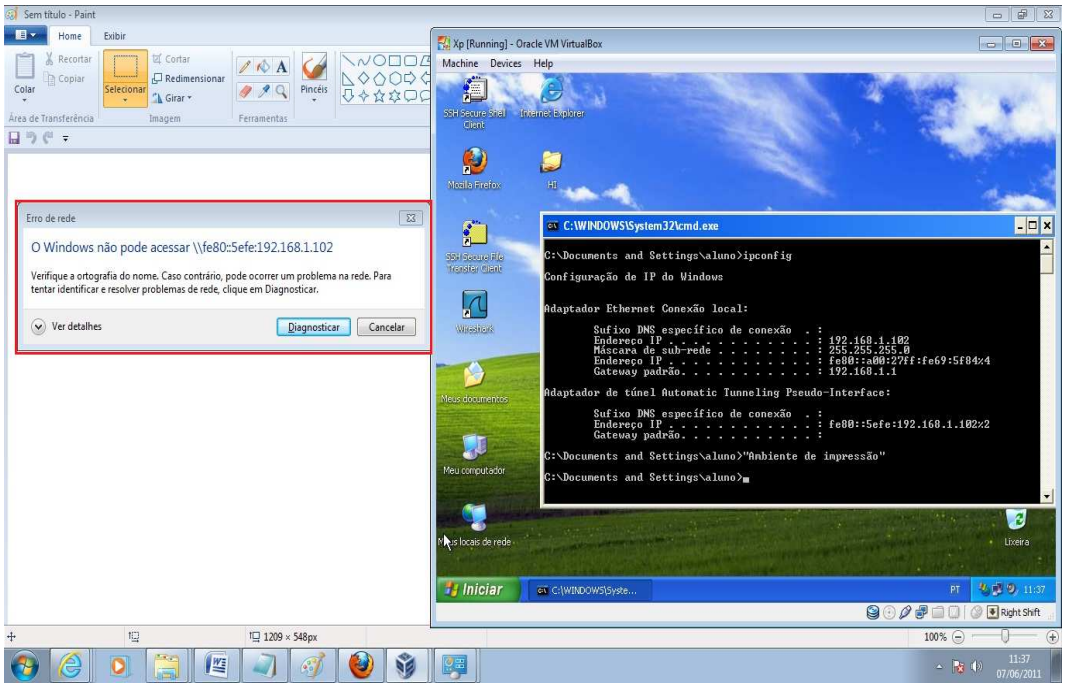

Figura 28: Compartilhamento de pasta - IPv6.

3.2 Discussão dos Resultados

Através da realização do desenvolvimento, foram obtidos os seguintes resultados:

1. A comunicação entre IPv4 e IPv6 é possível apenas se existir técnica de tunelamento devidamente configurada, pois os dois protocolos não são diretamente compatíveis.
2. Para acessar a internet, também é necessária a técnica de tunelamento, porque atualmente a rede e os sites ainda utilizam o protocolo IPv4;
3. O teste de *ping* foi possível devido ao Windows 7, possuir habilitado o protocolo IPv6 por padrão;
4. Utilizando os endereços IPv4 e IPv6, o desempenho do comando *ping* não foi alterado, mesmo estabelecendo tamanho para o pacote;
5. O compartilhamento de pasta é possível, caso as duas máquina estejam habilitadas somente com o protocolo IPv6;

Foram identificadas algumas necessidades durante a configuração do desenvolvimento, como a aplicação da técnica de tunelamento, que não foi possível executá-la, devido ao tempo para estudo, mas este item pode ser utilizado como um possível projeto futuro.

4 CONCLUSÃO

Algumas considerações que se pode fazer a partir deste trabalho é que o novo protocolo IPv6 é projetado para atender a demanda e a evolução da rede, diferentemente do protocolo IPv4 que foi projetado para atender um número menor de redes e de equipamentos.

Outro item importante é que o IPv6 possui diversas melhorias como: aumento dos números de IP, diminuição e organização do cabeçalho, habilitada segurança com o IPSec, garantia de QoS, excluído o uso da Tabela ARP e do NAT e criação das técnicas de transição Pilha Dupla, Tunelamento e Tradução.

Após estudar a estrutura do novo protocolo IP, é possível entender o funcionamento, as melhorias e atualizações. Mas também é importante ressaltar que ainda possuirá novas atualizações necessitando de estudos e novas informações sobre o assunto.

Além disso, é importante ressaltar que o projeto prático também colaborou para a realização e aplicação dos conceitos teóricos, mas acrescentaram e fizeram com que conseguisse chegar aos resultados esperados.

Para finalizar, este trabalho acadêmico proporcionou conhecimento estrutural do protocolo IPv6, contendo desde o protocolo TCP/IP, o histórico e características das duas versões do protocolo IP o IPv4 e o IPv6. Este tema é inovador e pode ser objeto de estudo desde usuários iniciantes até pesquisadores do assunto, é muito útil e auxilia para entender o funcionamento, o formato que será implantado e também pela necessidade de compreender e posteriormente ser capaz de aplicar o conhecimento quando estiver ativo para todos.

5 REFERÊNCIAS BIBLIOGRÁFICAS

COMER, Douglas E. **Redes de Computadores e Internet** 2. ed. Porto Alegre: Bookman, 2001.

.

FILIPPETTI, M. A. **CCNA 4.1**: guia completo de estudo. Florianópolis: Visual Books, 2008.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet**: uma abordagem top-down. 3. ed.: Pearson, 2005.

SIVASUBRAMANIAN, B.; FROOM, R.; FRAHIM, E. **CCNP Self-Study**: building cisco multilayer switched networks (BCMSN). 2. ed.: Cisco Systems, 2005.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**: teoria e aplicações corporativas. 5 ª ed.: Campus, 2005.

TANENBAUM, A. S. **Redes de Computadores**. 4. ed.: Campus, 2003.

BATTISTI, J. **Endereçamento IP**: Classes de Endereços. Disponível em: <http://www.juliobattisti.com.br/artigos/windows/tcpip_p3.asp> Acesso em: 01/06/2011, 11:54.

BATTISTI, J. **Tutorial de TCP/IP**: NAT - Network Address Translation. Disponível em: <http://www.juliobattisti.com.br/artigos/windows/tcpip_p20.asp> Acesso em: 01/05/2011, 16:15.

BASSI FILHO, D. L. Bassi Filho, **Mobilidade sobre IPv6**. Disponível em: <http://www.ipv6.br/IPV6/ArtigoMobilidadeIPv6> Acesso em: 18/05/2011, 10:05.

FAQ, RFC2406: **IP Encapsulating Security Payload (ESP)**. Disponível em: <http http://www.faqs.org/rfcs/rfc2406.html> Acesso em: 11/05/2011, 23:00.

FAQ, RFC2463: **Internet Control Message Protocol** (ICMPv6). Disponível em: <http://www.faqs.org/rfcs/rfc2463.html> Acesso em: 08/05/2011, 23:29.

Gross Doug, The **internet has (kind of) run out of space**. Disponível em: <http://edition.cnn.com/2011/TECH/web/02/03/internet.addresses.gone/index.html?iref=allsearch> Acesso em: 17/05/2011, 23:40.

IETF, RFC1752: **Recommendation for IPng**. Disponível em: < http://www.ietf.org/rfc/rfc1752.txt> Acesso em: 09/05/2011, 09:00.

IETF, RFC2002: **IP Mobility Support**. Disponível em: <http://www.ietf.org/rfc/rfc2002.txt> Acesso em: 17/05/2011, 08:00.

IETF, RFC2401: **Security Architecture for the Internet Protocol**. Disponível em: <http://www.ietf.org/rfc/rfc2401.txt> Acesso em: 20/05/2011, 11:00.

IETF, RFC2402: **IP Authentication Header**. Disponível em: <http://www.ietf.org/rfc/rfc2402.txt> Acesso em: 20/05/2011, 11:00.

IETF, RFC2460: **Internet Protocol, Version 6 (IPv6) Specification**. Disponível em: <http://www.ietf.org/rfc/rfc2460.txt> Acesso em: 20/05/2011, 11:00.

IETF, RFC2463: **Internet Control Message Protocol** (ICMPv6). Disponível em: <http://www.ietf.org/rfc/rfc2463.txt> Acesso em: 08/05/2011, 23:40.

IETF, RFC3596: **DNS Extensions to Support IP Version 6**.. Disponível em: < http://www.ietf.org/rfc/rfc3596.txt> Acesso em: 17/05/2011, 08:00.

IPNEWS, **Órgãos públicos migram ambiente para IPv6**. Disponível em: <http://www.ipnews.com.br/telefoniaip/index.php?option=com_content&id=19431&task=view> Acesso em: 22/05/2011, 18:49.

IPv6.br, **Curso IPv6**: a nova geração do protocolo Internet. Disponível em: <http://curso.ipv6.br/> Acesso em: 25/02/2011, 10:00.

IPv6.br, **FAQ**: Já há provedores fornecendo trânsito IPv6 comercialmente no Brasil?. Disponível em: <http://www.ipv6.br/IPV6/MenuIPV6FAQ#J_h_provedores_fornecendo_tr_nsi> Acesso em: 22/05/11, 19:00.

ISC, **Solutions From ISC**. Disponível em: <http://www.isc.org/solutions/ipv6> Acesso em: 19/05/2011 ás 09:40

ISOC, **LIST OF PARTICIPANTS**. Disponível em <http://www.worldipv6day.org/participants/index.html> Acesso em: 08/06/2011, 19:00.

MICROSOFT, MSDN. **Neighbor Discovery (ND)**. Disponível em: <http://msdn.microsoft.com/pt-br/library/aa916049.aspx> Acesso em: 08/05/2011, 15:34.

MIRANDA JÚNIOR, W. IPv6**: A Nova Geração de Comunicação:** serviços IPv6. Disponível em: <http://www.ipv6.br/IPV6/ArtigoNovaGeracaoComunicacaoParte05> Acesso em: 07/05/2011, 23:17.

MIRANDA JÚNIOR, W. IPv6: **A Nova Geração de Comunicação:** segurança Disponível em: <http://www.ipv6.br/IPV6/ArtigoNovaGeracaoComunicacaoParte07> Acesso em: 07/05/2011, 23:30.

NEVES, M. A., **IPv6 Móvel**. Disponível em: <http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/mipv6/> Acesso em: 19/05/2011, 08:26.

TCP/IP GUIDE, **IPv6 Address Space Allocation**. Disponível em: <http://www.tcpipguide.com/free/t_IPv6AddressSpaceAllocation.htm> Acesso em: 15/05/2011, 14:26.

SANTOS, Rodrigo Regis Dos et al. **Curso IPv6 básico:** Funcionalidades do IPv6. Disponível em: <http://www.ipv6.br/pub/IPV6/MenuIPv6CursoPresencial/IPv6-apostila.pdf>. Acesso em: 18 maio 2011.

SANTOS, R. R. dos **Serviços disponíveis em IPv6**. Disponível em: <http://www.ipv6.br/IPV6/ArtigoServicosIPV6> Acesso em: 07/05/2011, 23:09.

SANTOS, R. R. dos **Técnica de transição**: introdução. Disponível em: <http://www.ipv6.br/IPV6/ArtigoTecnicasTransicao> Acesso em: 10/05/2011, 22:00.

SANTOS, R. R. dos **Técnica de transição**: pilha. Disponível em: <http://www.ipv6.br/IPV6/ArtigoTecnicasTransicaoParte01> Acesso em: 10/05/2011, 22:00.

SILVA, A. J.S.; FARIA, M. R. **Hierarquia de Endereços IPv6**. Disponível em: <http://www.rnp.br/newsgen/0103/end_ipv6.html> Acesso em: 01/05/2011, 11:00.

SUN, **IP Version 6 (IPv6)**. Disponível em: <http://playground.sun.com/ipv6/> Acesso em: 17/05/2011, 23:46.

UFRGS, **Transição IPv4 / IPv6**. Disponível em: <http://penta2.ufrgs.br/redes296/ipv6/transi.htm> Acesso em: 19/05/2011, 08:50.

UFRGS, **Comando ARP**. Disponível em: <http://penta.ufrgs.br/uel/douglas/dotrab1_2.html> Acesso em: 09/05/2011, 11:00.

VALIDADOR, **Validador Experimental**. Disponível em: <http://validador.ipv6.br/> - Acesso em: 22/05/11, 19:05.

6 GLOSSÁRIO

Aplicação: podem ser programas que executam serviços ou camada do modelo TCP/IP.

Arpanet: (*Advanced Research and Projects Agency*) rede de computadores criada em 69 interligando instituições militares.

Bit: dígito binário (0 ou 1), armazenado no computador.

Byte: é um conjunto de oito bits, mostrando o armazenamento.

Backup: cópia de segurança, normalmente alocada em pendrives, fitas e HDs, que permitem a recuperação das informações.

Conexão: ligação de um equipamento a outro podendo ser em uma rede.

Cache: é uma cópia arquivada de um determinado conteúdo, como por exemplo, uma página da Internet.

Hardware: é todo o conjunto físico do computador (peças).

Endereço IP: número para identificar um computador ou uma rede.

Firewall: é uma ferramenta de segurança utilizado para controlar o acesso a uma rede.

Gateway: identifica e interliga redes, podem ser equipamentos como: roteadores.

Host: é um computador interligado à rede, armazena arquivos e permite o acesso de usuários.

HTTP (*HyperText Transfer Protocol*): protocolo de comunicação para acesso as páginas da Web.

IETF (*Internet Engeneering Task Force*): é uma comunidade internacional voltada para o crescimento da Internet.

Internet: é um conjunto de redes que interliga os computadores à escala mundial, permite a transferência e compartilhamento de dados.

Keywords: são palavras chave, basicamente são as palavras principais de um texto.

***Online*:** termo utilizado para definir que um que um computador está ligado à Internet.

LAN (***Local Area Network*)**: é uma rede de computadores, usada para transferência de dados, limitada a um prédio.

Multicast: é um endereço que faz a entrega de mensagens para um determinado grupo na rede.

Pacote: é um conjunto de informações transmitidas pela Internet.

Protocolo: é um conjunto de regras e padrões que especifica o formato de troca de informações.

Ping (*Packet Internet Group*): é usado para testar o alcance de uma rede, envia uma requisição e aguarda uma resposta.

Roteador: equipamento responsável pelo encaminhamento de pacotes em uma rede.

RFC (Request For Comments): são documentos que descrevem como funcionam padrões, protocolos, serviços.

SMTP (*Simple Mail Transfer Protocol*): é o protocolo de Internet usado para correio eletrônico.
SNMP (*Simple Network Management Protocol*): é um protocolo de rede utilizado para monitorar e gerenciar serviços de rede.

UDP (User Datagram Protocol): é um protocolo de transporte não orientado a conexão.

Web (*World Wide Web ou* WWW): é a área da Internet que contém documentos no formato de hipermídia, uma combinação de hipertexto com multimídia.