FUNDAÇÃO DE ENSINO “EURÍPIDES SOARES DA ROCHA”
CENTRO UNIVERSITÁRIO “EURÍPIDES DE MARÍLIA” – UNIVEM
CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

LUIS FERNANDO CAVALHIERI

ESTUDO DO PADRÃO IPv6 E SUA COMPARAÇÃO COM O IPv4

MARÍLIA
2006

LUIS FERNANDO CAVALHIERI

ESTUDO DO PADRÃO IPv6 E SUA COMPARAÇÃO COM O IPv4

Monografia apresentada ao curso de Bacharelado em Ciência da Computação do Centro Universitário Eurípides de Marília, mantido pela Fundação de Ensino Eurípides Soares da Rocha, como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação.

Orientador:
Prof. Ricardo Petruzza do Prado

MARÍLIA
2006

LUIS FERNANDO CAVALHIERI

ESTUDO DO PADRÃO IPv6 E SUA COMPARAÇÃO COM O IPv4

Banca examinadora da monografia apresentada ao Curso de graduação da UNIVEM, para obtenção do Título de Bacharel em Ciências da Computação.

Resultado: _____

ORIENTADOR: Prof. Ricardo Petruzza do Prado

1º EXAMINADOR: _____

2º EXAMINADOR: _____

Marília, _____ de _____ de 2006.

DEDICATÓRIA

Dedico este trabalho de conclusão de curso a minha namorada Fernanda, por estar sempre me incentivando a vencer os obstáculos da vida, e por ter entendido a importância deste trabalho ajudando-me a chegar até o fim.

AGRADECIMENTOS

Gostaria de prestar esta homenagem aos meus familiares que me acompanharam desde o início.

Aos amigos que ajudavam a resfriar a cabeça nos momentos de lazer.

Ao meu orientador por me ajudar sempre e, principalmente por ter aceitado o pedido de orientação.

CAVALHIERI, Luís Fernando. Estudo do Padrão IPv6 e sua comparação com o IPv4. 2006. Monografia (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2006.

RESUMO

O novo protocolo IPv6 (*Internet Protocol Version)* deverá substituir progressivamente o protocolo atual da Internet, o IPv4 (*Internet Protocol Version 4)*. Nos últimos anos, a Internet demonstrou uma altíssima taxa de crescimento, gerando o aumento da necessidade de endereços IP, que estão tornando-se escassos para atender a crescente demanda. A nova versão do protocolo IP foi desenvolvida pelo Internet Engineering Task Force (IETF), pensando nas melhorias a serem realizadas com base na versão atual (IPv4), prometendo melhorias como: maior espaço de endereços, formato de cabeçalho flexível e segurança que tem por objetivo diminuir os elevados índices de crimes virtuais. Funções desnecessárias foram removidas; funções que trabalhavam bem foram mantidas e novas funcionalidades foram acrescentadas. Este trabalho visa mostrar a estrutura básica do protocolo IPv6, suas características, formas de endereçamento, formato do cabeçalho, além dos mecanismos de transição do IPv4 para o IPv6 e uma comparação entre as duas versões.

Palavra Chave: Internet, Protocolo IP, IPv6.

CAVALHIERI, Luís Fernando. Estudo do Padrão IPv6 e sua comparação com o IPv4. 2006. Monografia (Bacharelado em Ciência da Computação) – Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2006.

ABSTRACT

The new IPv6 protocol (Version Internet Protocol) must gradually substitute the current protocol of the Internet, the IPv4 (Internet Protocol Version 4). For the last years, the Internet demonstrated an enormous growth tax, generating the increase need of IP addresses, that are becoming scarce for the increasing demand. The new version of the protocol IP was developed by the Internet Engineering Task Force (IETF), thinking about improvements to be carried through the basis of the current version (IPv4), promising improvements as: bigger space for addresses, format of flexible heading and security that has for its objective to reduce the high number of virtual crimes. Unnecessary functions were removed; the working well functions were kept and new functionalities were added. This task aims to show the basic structure of the protocol IPv6, its characteristics, addressing forms, format of heading, besides the mechanisms of the transition from the IPv4 to the IPv6 and to compare the two versions

Keywords: Internet, Protocol IP, IPv6.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AH*: Authentication Header*

ARP*: Address Resolution Protocol*

ARPA: *Advanced Research Projects Agency*

ARPANET: *Rede Arpa*

ATM*: Asynchronous Transfer Mode*

CIDR*: Classless Interdomain Routing*

DF*: Don´t Fragment*

DNS*: Domain Name System*

DS*: Differentiated Services*

Hosts: *Equipamentos conectados em rede.*

FP*: Format Prefix*

ICMP*: Internet COntrol Message Protocol*

IDRP*: InterDomain Routing Protocol*

IGMP*: Internet Group Management Protocol*

IHL*: Internet Header Length*

IETF: *Internet Engineering Task Force*

IP: *Internet Protocol*

IPng*: IP Next Generation*

IPv4: *Internet Protocolo versão 4*

IPv6: *Internet Protocolo versão 6*

LAN: *Local Área Network*

MF*: More Fragments*

NAT*: Network Address Translation - Port Translation*

OSI*: Open Systems Interconnection*

RARP*: Reverse Address Resolution Protocol*

RFC*: Request for Comments*

ST*: Stream Protocol*

TCP: *Transmission Control Protocol*

TCP/IP: *Transmition Control Protocol / Internet Protocol*

TTL*: Time to Live*

UDP*: User Datagram Protocol*

WWW - *World Wide Web*

LISTA DE TABELAS

SUMÁRIO

1. INTRODUÇÃO

O crescimento exponencial da Internet gerou aumento da necessidade de endereços IP que estão tornando-se insuficientes para atender a grande demanda. Isto trouxe problemas que não estavam previstos. Com o grande número de *hosts* conectados, os endereços IP (*Internet Protocol*) tornaram-se escassos principalmente pela maneira ineficiente como foram divididos em classes.

Inevitavelmente, o protocolo de rede utilizado, o IPv4 (*Internet Protocol Version* 4) necessita ser substituído. Assim, em 1990, o IETF (*Internet Engineerging Task Force)* iniciou um esforço para desenvolver o sucessor do protocolo IPv4. Uma motivação para esse esforço foi o entendimento de que o espaço de endereços IP estava começando a ficar escasso, com as novas redes e nós IP sendo anexados à Internet a uma velocidade muito rápida. Para atender a essa necessidade de maior endereçamento IP, o IPv6(*Internet Protocol Version* 6) foi desenvolvido. Os projetistas do IPv6 aproveitaram essa oportunidade para melhorar e ampliar outros aspectos do IPv4 com base na experiência operacional acumulada sobre esse protocolo.

Este trabalho de graduação teve como objetivo o estudo, inicialmente, de alguns aspectos históricos e técnicos da evolução do IP, base da pilha de protocolos TCP/IP (*Transmition Control Protocol / Internet Protocol*) e consequentemente o novo protocolo IPv6, destacando suas novas características, melhorias e vantagens em relação ao seu antecessor IPv4.

O tema deste projeto foi escolhido por se tratar de um assunto atual, em que há necessidade do estudo para compreender as diferenças das mudanças no funcionamento de redes de computadores baseadas no conjunto de protocolos TCP/IP, devido ao grande papel que o protocolo desempenha à Internet. A metodologia utilizada vai ser baseada em

simulações e testes, utilizando o Sistema Operacional Windows XP, executando os comandos do IPv6 (*Internet Protocol Version 6*), utilizando o *prompt* do Windows XP.

2. MODELOS DE REFERÊNCIA

A falta de padronização dos modelos de referência sobre as especificações detalhadas e claras das funções dos protocolos e seu inter-relacionamento é um fato verificado ao longo de vários anos na área de redes de computadores.

Dentre muitas vantagens da abordagem de modelos de referência podemos citar uma modularização de funções e a interoperabilidade entre protocolos de diferentes vendedores. Por esta razão, a metodologia atualmente mais aceita é a especificação dos protocolos e sua estruturação em níveis que são chamadas de camadas (Dantas, 2002).

Os modelos de referência dos protocolos são entendidos como uma estrutura onde existe um detalhamento da função de cada nível, das relações entre as interfaces das camadas e dos protocolos. Em outras palavras, o modelo de referência representa uma abstração na qual existem as especificações de como o ambiente deve funcionar. No entanto, não existe a menção de uma implementação de um protocolo específico.

A abordagem funcional das entidades e da estrutura em níveis permite que os modelos de protocolos sejam propostos e que estas especificações possam ser abertas. De outra forma, podemos dizer que os modelos de referências permitem que um fabricante implemente de sua maneira um determinado conjunto protocolos e, ainda assim, podendo ter a interoperabilidade deste pacote de software com outro pacote padronizado desenvolvido por outro fabricante.

O conceito de modelo de referência de protocolo algumas vezes também é apresentado como arquitetura de redes. Nas arquiteturas de protocolos, temos os protocolos já implementados e distribuídos nos níveis de arquitetura. È interessante mencionar que os modelos de protocolos são usualmente dispostos numa forma de pilha.

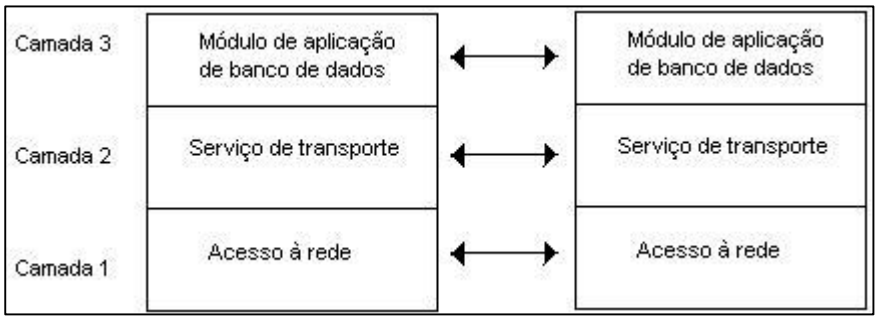

Figura 1 – Modelo genérico para aplicações de banco de dados (Kurose e Ross, 2003).

A Figura 1 ilustra um exemplo de modelo genérico simplificado de protocolo em camadas para suporte de aplicações de banco de dados. Neste exemplo, o modelo de protocolo tem suas funções distribuídas em três camadas. Na primeira camada deverá existir um módulo de acesso à rede, incluindo-se os serviços físicos e de enlace. O próximo nível, denominado de serviço de transporte e rede, é responsável por um serviço confiável orientado à conexão e serviço de roteamento para a Internet. No terceiro nível, o módulo de aplicação de banco de dados tem por função atender as solicitações distribuídas.

2.1 Modelo ISO/OSI

Para o estudo de protocolos, assim como qualquer assunto referente à rede, é importante compreender o Modelo OSI.

Segundo Kurose e Ross (2003), o ISO (*International Organization for Standartization*), em 1994, desenvolveu um modelo chamado RM-OSI (*Referencial Model - Open System International*), que define o fluxo de dados entre a conexão física da rede local e a aplicação do usuário final, sendo amplamente conhecido e bastante utilizado para descrever ambientes de redes. Neste modelo OSI, o propósito de cada camada, que são sete, é prover

serviços para a camada imediatamente superior, somente com uma exceção da camada mais inferior, nenhuma camada pode passar informações diretamente para sua contraparte no outro computador.

O modelo OSI foi proposto devido ao grande sucesso na padronização da arquitetura de protocolos TCP/IP, a idéia foi melhorar o modelo de referência TCP/IP. Como resultado, a ISO propôs seu modelo de referência, constituída em sete camadas e cada qual com sua função que será apresentado, conforme Dantas (2002), uma descrição de cada camada do modelo de referência RM-OSI, ilustrado na Figura 2.

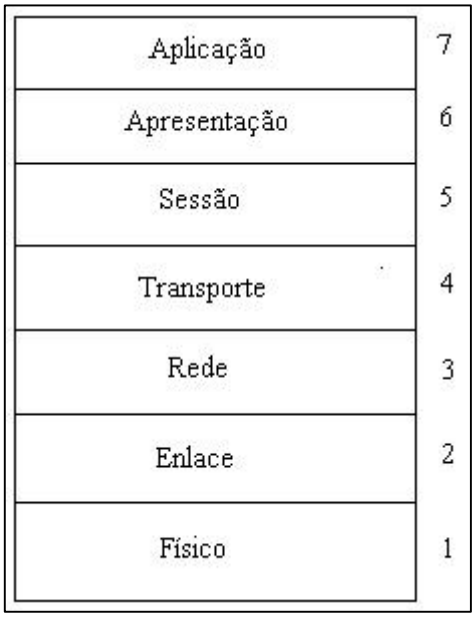

Figura 2 – O modelo de referência RM-OSI (Dantas, 2002).

- Física

É a primeira camada e mais inferior do Modelo OSI. Esta camada endereça a transmissão dos bits para o meio físico, ou seja, o cabo de rede. A camada física manipula os sinais elétricos/ópticos que contém os dados gerados pelas camadas superiores. Essa camada é responsável pelo transporte de bits entre um computador e outro, sem que os bits tenham

qualquer significado para ela e também controla a codificação dos dados e a sincronização dos bits, de forma a garantir que um bit enviado com o nível 0 seja recebido com nível 0, e não com o nível 1.

- Enlace

A segunda camada é denominada enlace de dados, essa camada encapsula os bits provenientes da camada física em blocos de dados, que são pacotes estruturados logicamente onde podem ser armazenados dados. A função primária dessa camada é garantir o envio de dados livre de erros, via camada física, permitindo à camada de rede enviar dados com segurança. Quanto ao mecanismo de envio dos dados, é relevante lembrar que este inclui, também, o processamento dos quadros de controle enviados pelo receptor. Como a função da camada 1 é apenas física (elétrica e mecânica), a camada de enlace é responsável pelo reconhecimento do início e final dos quadros pelo controle de fluxo entre remetente e destinatário e ainda pela forma de acesso ao meio.

- Rede

A terceira camada é responsável pelas tarefas de endereçamento de mensagens, conversão de endereços e nomes lógicos em físicos, determinação do caminho entre o computador origem e destino baseados nas condições de rede, prioridade do serviço, administração de problemas de tráfegos tias como roteamento e controle de números de pacotes na rede.

- Transporte

A quarta camada é responsável por garantir a integridade das mensagens enviadas pela camada de aplicação. De uma maneira geral, exemplos de outras funções encontradas na

camada de transporte são a detecção e correção de erros, o controle de fluxo do transporte, a fragmentação e remontagem.

- Sessão

A quinta camada permite que duas aplicações em diferentes computadores estabeleçam, utilizem e finalizem uma conexão denominada sessão. É responsável pelo reconhecimento de nomes e funções necessárias para permitir que duas aplicações comuniquem-se através da rede.

- Apresentação

A sexta camada fornece um serviço para as aplicações de independência da representação de seus dados. Essa camada converte os dados de um formato enviado pela camada de aplicação, para um formato intermediário, que é reconhecido por ambas as camadas no computador origem. No computador destino, esta camada converte o formato intermediário em um formato utilizável pela camada de aplicação.

- Aplicação

A sétima e última camada encontramos os protocolos que auxiliam os processos dos usuários. Representa a interface com o usuário que permite o acesso aos serviços da rede, como a transferência de arquivos, acesso a banco de dados, correio eletrônico, e etc.

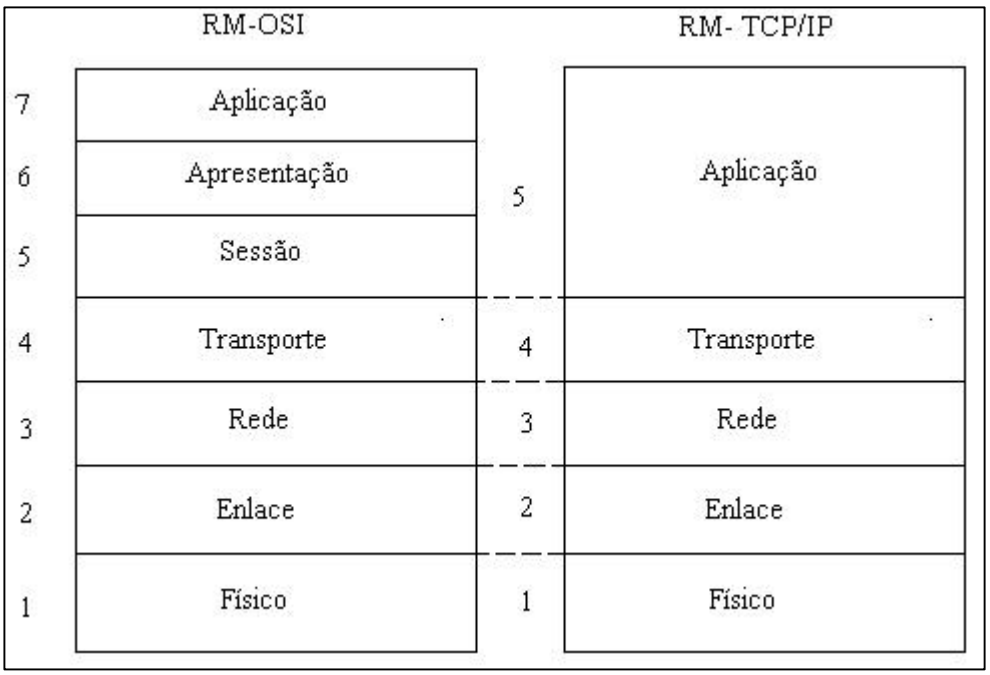

Figura 3 – Comparações dos modelos de referência RM-OSI e TCP/IP (Dantas, 2002).

Na Figura 3, há uma comparação entre os modelos TCP/IP e RM-OSI. Mostrando as camadas dos modelos de referência RM-OSI, que são sete níveis, e do modelo de TCP/IP que são em 5 níveis.

2.2 Modelo IEEE 802

Com a falta de definição observada na camada 1 no modelo TCP/IP inúmeras soluções começaram a surgir no mercado. O objetivo geral era a padronização dessa grande quantidade de soluções que vinham surgindo para as redes locais (LANs), a Sociedade de Computação do Instituto de Engenheiros Elétricos (*Computer Society do IEEE*), nos Estados Unidos, criou um comitê de padronização em 1980 (Dantas, 2002).

O IEEE publicou um conjunto de padrões que foi adotado pelo Instituto Nacional Americano de Padronização (ANSI) e, após uma determinada revisão foi aceito pela ISO. Na ISO, o modelo ficou conhecido como ISO 8802.

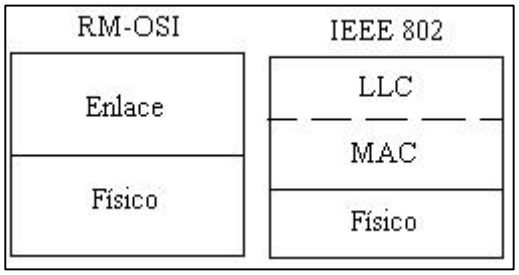

Figura 4 – Comparação IEEE 802 e RM-OSI (Dantas, 2002).

A Figura 4, é uma apresentação do modelo de referência IEEE 802 comparando-o com o modelo de RM-OSI. O modelo IEEE 802 é composto por três camadas, e essas camadas são essenciais para uma rede local. Numa rede local, a maior preocupação de qualquer tecnologia é voltada para implementações eficientes das funções físicas e de enlace. Exemplos de funções importantes na camada de enlace numa rede local são os serviços de acesso concorrentes dos usuários ao meio físico, fragmentação/remontagem em nível de enlace.

2.3 O Protocolo TCP/IP

De acordo com Dantas (2002), o modelo de referência mais conhecido (e um dos mais antigos) é o TCP/IP (*Transmisson Control Protocol/Internet Protocol*). Este modelo surgiu da rede ARPANET, que foi uma rede de pesquisa criada pelo Departamento de Defesa do governo americano que visava à conexão de várias redes e cada rede tinha a sua conexão à ARPANET que era feita através de diferentes tipos de enlace, com isso, vários problemas começaram a surgir e uma necessidade de um modelo ficou visível. O modelo de referência concebido foi o TCP/IP. A Figura 5 apresenta o modelo de referência TCP/IP.

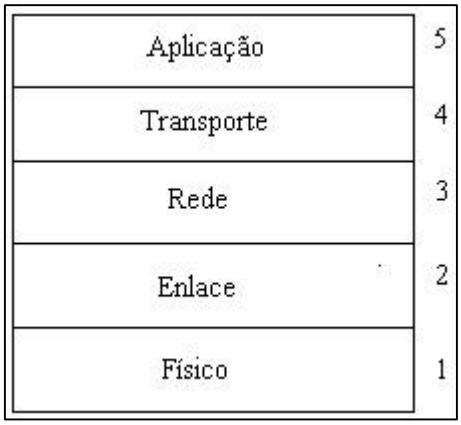

Figura 5 - O modelo de referência TCP/IP (Dantas, 2002).

Conforme Dantas (2002), os níveis do Modelo de referência TCP/IP são explicados da seguinte maneira:

- Inter-rede: este nível é o responsável pelo envio dos datagramas de um computador qualquer para outro computador, independente de suas localizações na rede.
- Transporte: este nível é responsável por prover suporte à camada de aplicação de maneira confiável (ou não), independente dos serviços oferecidos pelas camadas de interface de rede e inter-rede. A função da camada de transporte é garantir uma conexão fim-a-fim com a qualidade solicitada pela camada de aplicação.
- Aplicação: nesta camada estão os protocolos que dão suporte às aplicações dos usuários importante observar que, na camada de aplicação ficam os protocolos que auxiliam, por exemplo, a transferência de dados, o acesso remoto a outros computadores, o protocolo de correio eletrônico, os protocolos que auxiliam na gerência de redes, o protocolo que faz o mapeamento dos nomes dos computadores para seus endereços de rede, e ainda o protocolo que implementa a busca de páginas na WWW (Word Wide Web).

Ainda com relação ao modelo TCP/IP, a Figura 6 ilustra os seus cincos níveis e suas respectivas nomenclaturas que são adotadas quanto às unidades de protocolo. De uma maneira mais simplificada, a Figura 6 indica que em termos de aplicação referem-se às mensagem, que os pacotes são as unidades manipuladas na camada de transporte, que os datagramas são tratados no âmbito de rede e por fim os quadros são as unidades do nível 1.

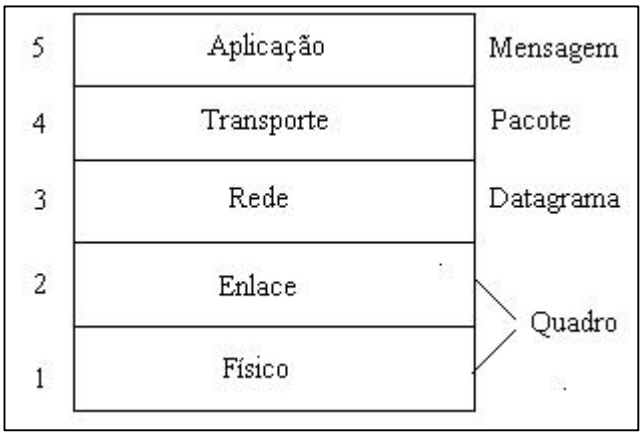

Figura 6 – Níveis e unidades de protocolos (Dantas, 2002).

3. CAMADA DE INTER-REDE

A camada de inter-rede é o segundo nível da arquitetura TCP/IP. Os principais protocolos alocados nesta camada são o IP (*Internet Protocol*), o ICMP (*Internet Control Message Protocol*), IGMP (*Internet Group Management*), o ARP (*Adress Resolution Protocol*) e o RARP (*Reverse Address Resolution Protocol*).

3.1. Internet Protocolo (IP)

Conforme Comer (1998), a camada IP tem que reconstruir o *frame* a partir dos fragmentos que recebe, assegura-se de que não falta nenhum e verificar se eles estão na ordem correta. A camada IP também tem que tratar uma variedade de formatos de endereçamento que são utilizados entre sistemas TCP/IP.

A função do protocolo IP é a transmissão dos pacotes de dados entre dois *hosts*. Estes dados são recebidos da camadas superior, como o TCP, e podem trafegar por diversas redes antes de atingir o seu destino final. O protocolo IP ainda tem um mecanismo de controle de fragmentação dos pacotes de dados, quando são transmitidos para *hosts* onde a janela de recepção é menores que o tamanho do pacote de dados.

No envio de um pacote de dados via IP, ocorre primeiro um processo de multiplexação, onde os dados provenientes da camada de transporte TCP são concatenados através do protocolo IP, que utiliza um cabeçalho próprio e os envia para camadas de enlace e posteriormente para a camada física.

Quando este pacote de dados chega ao seu destino, ocorre o processo de multiplexação, onde o protocolo IP recebe os pacotes de dados provenientes das camadas

física e enlace, e através da leitura do cabeçalho IP, identifica se o pacote de dados deve ser enviado para a camada de transporte TCP (Comer, 1998).

3.2. Endereçamento IP

Segundo Comer (1998), o endereço IP é composto por um campo de 32 bits, numerados de 0 a 31. No campo de endereço IP, estão contidas duas importantes informações: identificação do *host* e identificação da rede à qual o *host* está conectado.

Na implantação inicial do protocolo IP o campo de endereço era de 32 bits, sendo 8 bits designado para identificação da rede, e 24 bits para identificação dos *hosts*.

Esta restrição do protocolo IP tornou-se rapidamente um obstáculo para o seu uso, pois com o crescimento do uso das redes locais, onde se adotou a arquitetura *Ethernet* que utiliza 48 bits para identificação dos *hosts*, torna-se impossível o seu encapsulamento utilizando 24 bits do protocolo IP, além da *Ethernet* ter capacidade bem superior às 256 redes possíveis para o protocolo IP em questão.

Os grupos de endereços relacionados são chamados de endereços Classe A, B ou C.

Um endereço Classe A é aquele que possui cerca de 15 milhões de endereços IP, todos tendo como primeiro componente o mesmo valor e três componentes diferentes no final.

Um endereço Classe B é aquele que possui cerca de 60.000 endereços IP, cada um com os mesmos valores nos dois primeiros componentes. Os dois últimos componentes podem variar. Geralmente, os proprietários de endereços Classe B têm muito menos que 60.000 máquinas em suas redes internas, mas esse número é maior que 250.

Um endereço Classe C é aquele que possui cerca de 250 endereços IP, cada um deles tendo os mesmos valores nos três primeiros componentes. O último componente é diferente em cada máquina da LAN.

3.3. Protocolos da Camada Inter-Rede: ICMP, ARP, RARP.

De acordo com Dantas (2002), “o ICMP (*Internet Control Mesage Protocol*) tem por objetivo prover mensagens na comunicação entre nós num ambiente de rede TCP/IP.” Então, o ICMP permite que roteadores enviem mensagens de erros ou de controle para outros roteadores (ou nós).

O segundo protocolo, o ARP (*Address Resolution Protocol*), tem por função o mapeamento de endereços IP para endereços físicos de rede, ou seja, podemos dizer que o ARP tem por função a resolução de endereços físicos, uma vez fornecidos endereços IPs.

E por fim, temos o protocolo RARP (*Reverse Address Resolution Protocol*), Dantas (2002) afirma que “O paradigma de resolução do protocolo RARP é o inverso do ARP.”. Para a comunicação entre os processos existe a informação do endereço físico, todavia, não está disponível o endereço IP.

3.4. Necessidade de Mudança

Com a “explosão” da Internet e com o surgimento constante de mais e mais serviços e aplicações, os atuais endereços IP (IPv4) estão tornando-se um recurso escasso.

Os protocolos TCP/IP mostram um importante desafio arquitetônico com a contínua expansão da Internet. Com o crescimento anual de 100% no número de redes ligadas à Internet coloca em xeque o sistema de roteamento. As classes B estão paulatinamente sendo esgotadas e o uso das técnicas de CIDR (*Classless InterDomain Routing*) representam uma solução a este problema. Uma nova versão do IP faz-se necessária para suportar um endereçamento muito maior e prover suporte ao problema de escalabilidade. Ao mesmo

tempo, novas e bastante ambiciosas aplicações já sugerem que a Internet precisa suportar pacotes de voz e vídeo em proporções cada vez maiores.

Segurança é também um dos fatores mais importantes, especialmente com a expansão de redes aplicadas ao mundo dos negócios. Procurar uma maneira uniforme de suportar a Internet e ainda lidar com a variedade de tecnologia pelo mundo, algumas das quais sujeitas a restrições de exportação, é um desafio de enormes proporções (TANENBAUN, 2003).

3.5. Internet Protocolo Versão 4 (IPv4)

A versão do protocolo IP que atualmente usada na Internet é o IPv4, que vem sendo substituída pela nova versão IPv6 (*Internet Protocol Version* 6). O IPv4 é um protocolo bastante estável e robusto que existe desde a década de 80, porém devido ao enorme crescimento da Internet, verificou-se que os endereços IPv4 disponíveis não suportariam essa enorme demanda. Na época de desenvolvimento do protocolo IPv4 existiam pouquíssimas redes de computador em operação, por esse motivo o endereçamento foi definido com 32 bits, que era suficiente para a época.

É o protocolo responsável pela comunicação entre máquinas em uma estrutura de rede TCP/IP. As funções mais importantes são as atribuições de um esquema de endereçamento da rede utilizada abaixo e independente da própria topologia de rede utilizada.

3.5.1 Datagrama do IPv4

Um datagrama IP é dividido em cabeçalho e área de dados. O cabeçalho ocupa uma área fixa de 20 bytes e uma área de tamanho variável (correspondente ao campo *options*). A Figura 7 apresenta o formato do cabeçalho IPv4, onde:

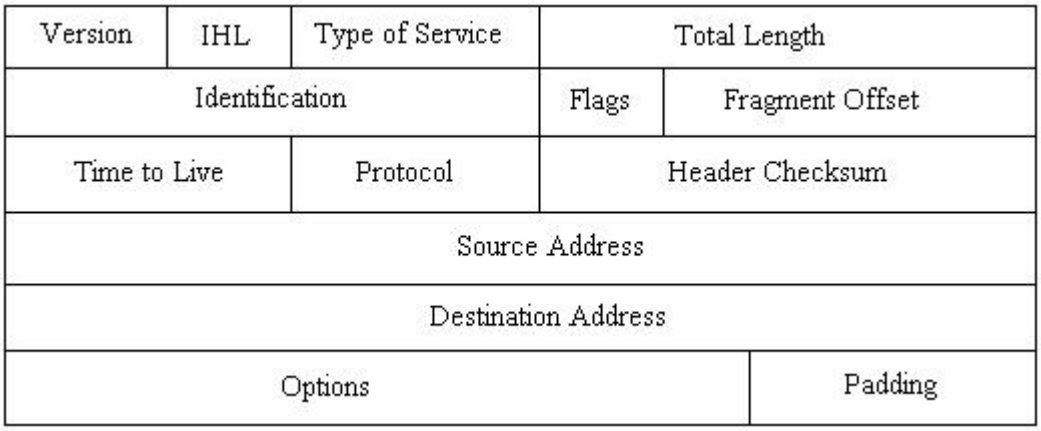

Figura 7 – Cabeçalho do IPv4 (Gupta e Moeta, 2002).

- *Version*

O primeiro campo é *version*, ele define a versão atual do IP implementado pela estação da rede. O roteador através do número da versão pode determinar como interpretar o restante do datagrama IP.

- *IHL - Internet Header Length*

O comprimento do cabeçalho do IP (todos os campos, exceto o campo de dados do IP) pode variar. Nem todos os campos no cabeçalho do IP precisam ser usados. Esses campos são medidos na quantidade de palavras de 32 bits. Como o cabeçalho do IPv4 pode conter um número variável de opções, esses quatro bits são necessários para determinar onde, no datagrama IP, os dados realmente começam. O cabeçalho mais curto do IP terá 20 bytes,

portanto esse campo conteria um 5(20bytes = 160 bits; 160 bits/32 bits = 5). Esse campo é necessário para que o cabeçalho varie de comprimento de acordo com o campo chamado *options*.

- *Type of Service*

O campo de serviço trata de uma entrada que permitiria que os aplicativos indicassem o tipo de percurso de roteamento de que gostariam (o ponto principal é que o aplicativo escolhesse o campo). O tipo de serviço é formado pelos seguintes campos: precedência, retardo, rendimento e confiabilidade.

- *Total Length*

Este campo comprimento total é o comprimento do datagrama IP e não o do pacote, que é medido em bytes alcançando o tamanho máximo de 65.535 bytes.

- *Fragment Identification*

A fragmentação possibilita que um datagrama grande seja encaminhado para o próximo segmento de LAN a ser dividido em segmentos menores para serem remontados no destino. Este campo contém um único inteiro que identifica o datagrama.

- *Identification*

O campo *indentification* indica quais fragmentos de datagrama pertencem a um determinado datagrama, para que não haja confusão entre eles. A camada IP de recebimento usa esse campo e o endereço IP de origem para identificar quais fragmentos pertence a um determinado datagrama.

- *Flags*

Este campo indica se mais fragmentos chegarão ou se serão enviados mais dados para esse datagrama, também indica se o datagrama deve ou não ser fragmentado. Por exemplo, se um roteador receber um pacote que deverá ser fragmentando para ser encaminhado e se o bit de não-fragmentação for definido, ele descartará o pacote e enviará uma mensagem de erro para a estação origem.

- *Fragment Offset*

Indica a que posição do datagrama atual o fragmento pertence. Esse campo indica o offset (em bytes) do datagrama anterior que continua o datagrama completo. No campo Offset todos os cabeçalhos do IP de cada um dos datagramas fragmentados são quase idênticos.

- *Time to Live – TTL*

O campo TTL (*Time to Live*) indica a quantidade de tempo que um datagrama pode permanecer na rede. O tempo máximo que um datagrama pode permanecer na rede é de 255 segundos. Existem duas funções para o campo TTL: finalizar os *loops* de roteamento e limitar o tempo de vida de um segmento TCP (dados transmitidos).

- *Protocol*

O campo protocolo é usado para indicar qual protocolo de nível mais alto deve receber os dados do datagrama, ou seja, indica a que protocolo da camada de transporte esse datagrama está associado.

- *Header Checksun*

Esse campo garante a integridade dos valores do cabeçalho, auxiliando o roteador na detecção de erros de bits em um datagrama IP recebido. Toda vez que o datagrama é recebido por um roteador, esse roteador recalcula a soma de verificação. Por que alterá-la? Porque o campo TTL é alterado por todo roteador que o datagrama atravessa.

- *Source Address*

Indica o endereço IP do *host* origem do datagrama.

- *Destination Address*

Indica o endereço IP do *host* destino do datagrama.

- *Options*

O campo *options* contém informações sobre o roteamento de origem, traçando uma rota, marcando o tempo do pacote à medida que ele atravessa os roteadores e as entradas de segurança. Esses campos podem ou não constar no cabeçalho. Basicamente o campo *options* foi projetado para permitir a evolução do protocolo, possibilitando a experimentação de novas idéias e evitando a alocação de bits de cabeçalho para informações raramente necessárias.

3.5.2. Endereçamento IPv4

O endereço IPv4 tem o tamanho de 32 bits subdivididos em quatro grupos de oito *bits* cada, chamados de octetos. Eles são escritos em notação decimal, separados por ponto (*dotted decimal notation)*, onde cada um dos octetos tem um valor entre 0 a 255. Assim, o endereço IP mais baixo é 0.0.0.0 e o mais alto é 255.255.255.255. Uma parte do endereço

IPv4 indentifica a rede e a outra o *host* dentro dessa rede, servindo tanto para referir-se à rede quanto a um *host* individual (Yokomizo, 2005).

3.5.3. Classes de Endereçamento IPv4

Os endereços IPv4 estão organizados em 5 classes: A, B, C, D e F, como apresentado a Figura 8.

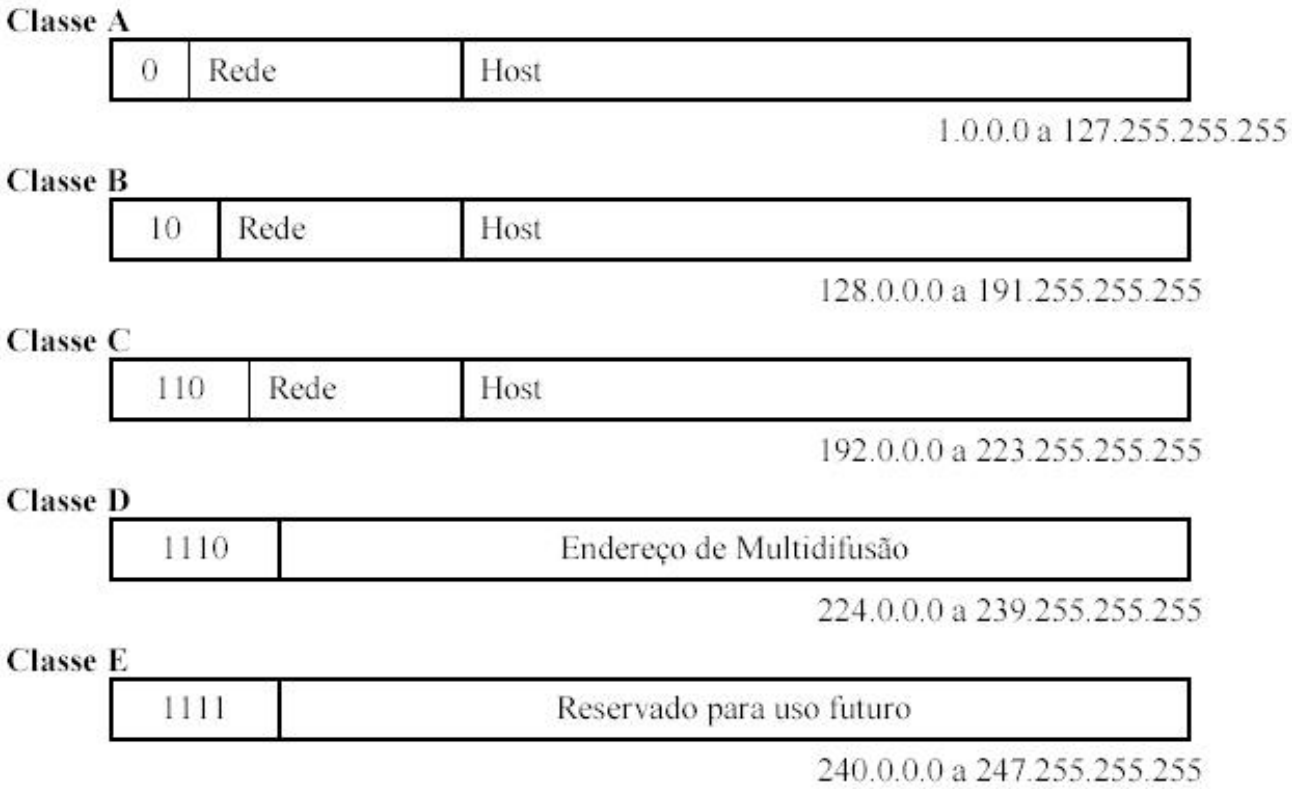

Figura 8 – Classes de Endereços IPv4 (Tanenbaum, 2003).

De acordo com Tanenbaum (2003), nos endereços de classe A, os 8 primeiros bits identificam a rede e os outros 24 bits restantes, identificam o *host* dentro dessa rede. Começam com um número decimal entre 0 a 127.

Os endereços da classe B começam com um número decimal entre 128 a 191, usando *bits* para identificação da rede e os outros 16 *bits* restantes para identificação do *host* na rede.

Os endereços da classe C usam 24 bits para identificação da rede e apenas 8 *bits* para identificação do *host.* Começam com um número decimal entre 192 a 223.

Os endereços de classe D são reservados para os endereços *multicast.* Começam com um número decimal entre 224 a 239.

Os endereços da classe E são reservados para um futuro. Seus 4 primeiros *bits* são 1111, portanto os endereços classe E começam com um número decimal entre 240 a 255.

4. PROTOCOLO IPv6

O IPv6, sigla de *Internet Protocol Version* 6, inclui na realidade uma série de modificações nos protocolos da Arquitetura TCP/IP, que tem como principal objetivo revolver os problemas existentes atualmente no IPv4 e adequá-la aos requisitos de operação das novas tecnologias de redes de alta velocidade, como é o caso das redes ATM (Asynchronous Transfer Mode), e outros tipos de aplicação que envolve voz e vídeo.

Essa nova versão de protocolo mantém as principais características que fizeram do IPv4 um sucesso mundial. Porém, além de ampliar o espaço de endereçamento, o IPv6 oferece outros serviços, como conectividade segura, com maior qualidade de serviço, facilidade de gerenciamento de endereços, simplificação do cabeçalho e aproveitamento das novas arquiteturas de hardware (Santos, 2004).

Neste capítulo são descritas algumas características do IPv6 e uma definição de cada uma delas, e também um detalhamento do datagrama IPv6. Apresenta o formato do cabeçalho básico do IPv6, descrevendo seus respectivos campos que o compõe, bem como uma descrição dos cabeçalhos de extensão. Apresenta também o endereçamento e tipos de endereços IPv6, e a transição do protocolo IPv4 para o IPv6.

4.1. Características do Protocolo IPv6

De acordo com Comer (1998), esse novo protocolo mantém muita das características que contribuíram para o sucesso do IPv4, com algumas modificações. As mudanças introduzidas pelo IPv6 podem ser agrupadas em cinco categorias:

- Endereços Maiores

O novo tamanho de endereço é a mudança mais visível. O IPv6 quadruplica o tamanho do endereçamento em relação ao IPv4, de 32 para 128 bits. Com esse novo tamanho de endereçamento é suficiente para obter 1.564 endereços distintos por m^2 (metro quadrado) do planeta Terra. O espaço de endereçamento do IPv6 é tão grande que dificilmente será consumido em um futuro previsível.

- Formato Flexível de Cabeçalho

Ao contrário do IPv4, que usa um cabeçalho de datagrama de formato fixo, o IPv6 usa um formato de datagrama inteiramente novo, usando um conjunto de cabeçalhos opcionais.

- Opções Aprimoradas

Permite que um datagrama inclua informações de controle opcionais e inclui novas opções que oferecem recursos adicionais não disponíveis no IPv4.

- Suporte para Alocação de Recursos

Substituiu a especificação de tipo de serviço IPv4 por um mecanismo que permite pré-alocação de recursos de rede. Esse novo mecanismo aceita aplicativos tais como vídeo em tempo real, requerendo garantias de largura de banda e retardo de transmissão.

- Provisão para extensão de Protocolo

Acredita-se que a mudança mais significativa no protocolo IPv6, seja uma transição de um protocolo que específica inteiramente todos os detalhes – IPv4, para um protocolo que pode permitir recursos adicionais – IPv6.

4.2. Datagrama do Protocolo IPv6

Conforme Moreira (2004), o IPv6 muda complemente o formato de datagrama, introduzindo um novo e simplificado formato de cabeçalho, que contém menos informações do que o cabeçalho de datagrama IPv4. Esse novo datagrama é constituído por um cabeçalho básico que possui campos de tamanho fixo, que pode ser seguido ou não por cabeçalhos de extensão e finalmente os dados, ilustrado na Figura 9.

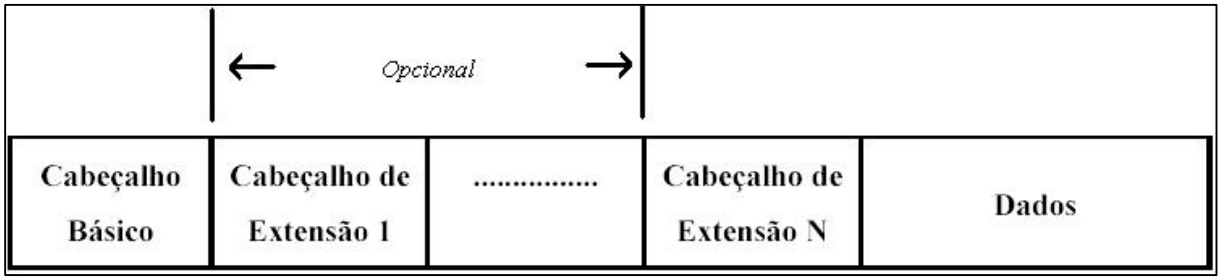

Figura 9 – Formato Geral do Datagrama IPv6 (Comer, 1998).

4.3 Formato do Cabeçalho do IPv6

O cabeçalho do IPv6, curiosamente, possui menos informações do que o datagrama IPv4. Alguns campos dos cabeçalhos são eliminados ou transformados em opções, o número de opções disponíveis é aumentado, incluindo a possibilidade de transmissão em tempo real e segurança. De acordo com Comer (1998), as mudanças no cabeçalho de datagrama refletem mudanças no protocolo:

- O alinhamento foi mudado de múltiplos de 32 bits para múltiplos de 64 bits.
- O campo de comprimento de cabeçalho foi eliminado e o campo de comprimento de datagrama foi substituído por um campo COMPRIMENTO DO PAYLOAD.

- O tamanho dos campos de endereço de origem e de destino foi aumentado para 16 octetos cada.
- As informações de fragmentação foram retiradas de campos fixos do cabeçalho básico, para um cabeçalho de extensão.
- O campo TEMPO DE VIDA foi substituído por um campo LIMITE DE PASSOS DA ROTA.
- O campo TIPO DE SERVIÇO foi substituído por um campo RÓTULO DE FLUXOS.
- O campo PROTOCOLO foi substituído por um campo que específica o tipo do próximo cabeçalho.

Na Figura 10 são apresentados os 5 (cinco) campos e 2 (dois) endereços totalizando em 7 (sete) campos obrigatórios da comunicação IPv6, estes campos apresentam as seguintes características:

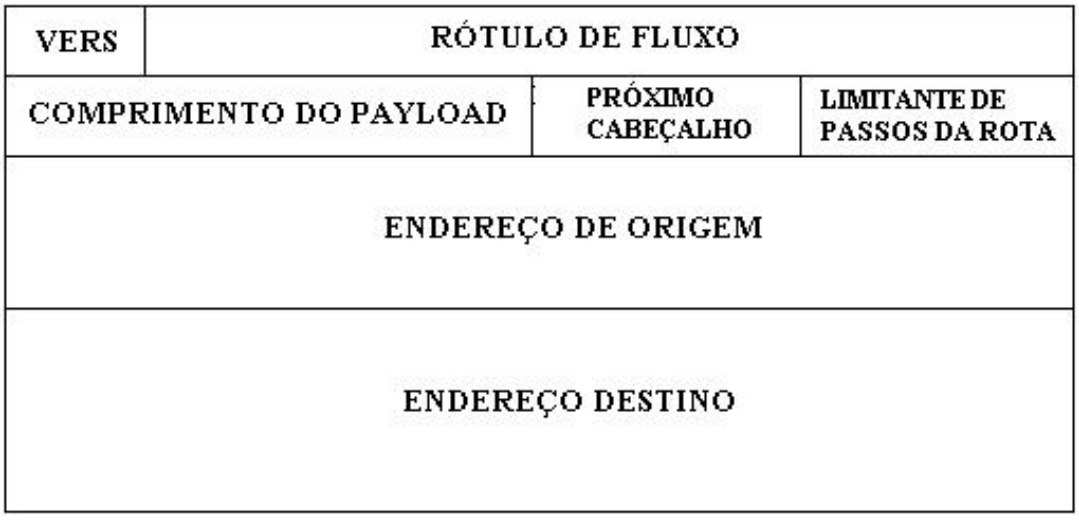

Figura 10 – Formato do Cabeçalho Básico do IPv6. (Comer, 1998)

- Vers (4bits)

Campo destinado a indicar qual a versão do protocolo utilizado, é definido com o valor 6 (seis) indicando que o protocolo utilizado é o IPv6.

- Rótulo de Fluxo (24bits)

Este campo possui a função de ajudar no roteamento dos pacotes na rede. Procura destinguir, entre os pacotes IPv6, a classe ou a prioridade dos pacotes transmitidos pela rede, nesta transmissão podem existir dois tipos de tráfego: com congestionamento ou sem congestionamento.

- Comprimento do Payload (16 bits)

Tem como função indicar o comprimento da carga útil do pacote IPv6, o que inclui os cabeçalhos de extensão e a unidade de dados da camada superior.

- Próximo Cabeçalho (8 bits)

Este campo indica qual é o próximo cabeçalho após o cabeçalho base IPv6, podendo ser tanto os cabeçalhos de extensão como os protocolos da camada superior, como TCP, UDP.

- Limitante de Passos da Rota (8 bits)

Evita que um determinado datagrama permaneça na rede, pois indica o número máximo de saltos que o pacote IPv6 pode dar antes de ser descartado.

- Endereço de Origem (128 bits)

Armazena o endereço que especifica a máquina origem, este endereço origem/destino é formado por 8 campos de 16 bits que são separados por (:) dois pontos.

- Endereço Destino (128 bits)

O campo endereço de destino armazena o endereço que especifica a máquina destina.

4.3.1. Cabeçalho de Extensão

O cabeçalho de extensão do IPv6 foi acrescido de maiores informações sobre o pacote para o seu processamento adequado tanto no destino como nos roteadores onde passa. Para ser totalmente geral, o IPv6 precisa incluir mecanismos de aceitar funções como fragmentação, roteamento de origem e autenticação. Entretanto, a opção por alocar campos fixos no cabeçalho de datagrama para todos os mecanismos não é eficaz, porque a maioria dos datagramas não usa todos os mecanismos e, o grande tamanho de endereço de IPv6 exarceba a ineficiência. (Comer, 1998)

De acordo com Yokomizo (2005), como os cabeçalhos de extensão são opcionais, um pacote IPv6 pode carregar zero, um ou mais cabeçalho de extensão. Eles são identificados por um tipo e carregam no campo *Next Header* a informação do tipo de cabeçalho que o segue e, caso não exista nenhum ou mais nenhum cabeçalho de extensão, o campo *Next Header* é preenchido com o valor 99, identificando o protocolo de nível superior (TCP, UDP, ICMP). Estes cabeçalhos de extensão devem ser processados na mesma ordem em que eles aparecem no pacote.

Conforme a RFC 2460 (Deering e Hinden, 1998), quando ocorre de mais de um cabeçalho de extensão é usado no mesmo pacote, uma ordem de preferência deve ser seguida, essa ordem deve ser:

1. Cabeçalho Básico (IPv6 *Header)*
2. *Hop-by-Hop Options Header*
3. *Destination Options Header*
4. *Routing Header*
5. *Fragment Header*
6. *Authentication Header*
7. *Encapsulating Security Payload Header*
8. *Destionation Options Header*
9. *Upper-layer Header*

Essa ordem não é de uso obrigatório, com a exceção do *Hop-by-Hop Options* que necessariamente deve aparecer logo após o cabeçalho básico do IPv6, quando este for utilizado. Para a maior eficiênica no transporte do pacote essa ordem deve ser seguida, facilitando o processamento dos roteadores, evitando que cada roteador tenha que analisar todos os cabeçalhos até encontrar um cabeçalho que contenha informações úteis para o processamento do pacote no roteador.

4.4. Endereçamento do IPv6

Uma das maiores modificações e mais visíveis para os usuários foi o aumento do espaço de endereçamento e o formato do endereço IPv6. O endereço do IPv4 possui 32 bits de tamanho, enquanto o IPv6 possui 128 bits, porém, esta não é a única diferença em relação ao endereçamento destes protocolos.

Os endereços IPv4 são representados por apenas duas ou três partes variáveis para serem distribuídos e localizados, um identificador de rede, um identificador de conexão e, às

vezes, um identificador de sub-rede. Nesse protocolo, a representação de um endereço IPv4 se da na forma X.X.X.X, em que os pontos separam os campos que são constituídos de até 3 (três) dígitos decimais (Gomes, 2004).

Os endereços IPv6 são quatro vezes maiores que os endereços IPv4 e são representados da seguinte forma X:X:X:X:X:X:X:X, sendo que o X refere-se a quatro dígitos hexadecimais (16 bits). Os endereços IPv6 são praticamente ilimitados (2128 bits) e os estudiosos afirmam que os 128 bits são capazes de acomodar entre nós (Costa, 2000).

Segundo Comer (1998), associando o espaço de endereços IPv6 com quantidade de seres humanos do planeta terra, estima-se que cada ser humano possuiria endereços suficientes para ter sua própria interligação em redes tão grande quanto a Internet atual.

O aumento da quantidade de bits utilizados pelo endereço IPv6 também aumentou a complexidade de representação, que ficou muito longa. Em decimal cada endereço ficaria muito extenso, por isso que não é utilizado. Na Figura 11 pode ser verificado um exemplo de como seria representar um endereço IPv6 em notação decimal.

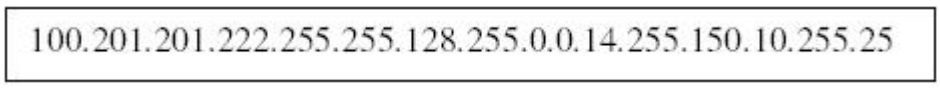

Figura 11 – Exemplo de endereço IPv6 representado em notação decimal

A representação do endereço IPv6 em notação decimal causaria um certo problema de manipulação e seria bastante difícil de memorizar. Assim com a intenção de reduzir a quantidade de dígitos, os endereços IPv6 passaram a ser representados por 8 partes de 16 bits, com os valores em hexadecimal, conforme pode ser verificado na Figura 12.

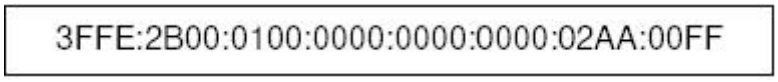

Figura 12 – Exemplo de endereço IPv6

Mesmo assim os endereços estariam grandes, algumas formas de representação simplificadas foram estabelecidas, tais como são descritas abaixo:

- Compreensão de zero: simplificada removendo os zeros à esquerda em cada bloco de 16 bits. Assim, o exemplo da Figura 12 ficaria 3FFE:2B00:100:0:0:0:2AA:FF.
- Emprego de dois pontos duplos: para simplificar ainda mais a representação do endereço IPv6, uma seqüência contígua de blocos de zeros podem ser substituídos por dois pontos duplos (::). Nesse caso o endereço da Figura 12 poderia ser representado como 3FFE:2B00:100::2AA:FF. A ocorrência de dois pontos duplos :: podem ocorrer apenas uma vez em cada endereço (Santos, 2004).

No IPv6 foram especificados apenas três (3) tipos de endereços: anycast, multicast e unicast, os quais serão descritos na sessão seguinte.

4.4.1. Tipos de Endereços

O IPv6 possui 3 (três) tipos de endereços *Unicast, Anycast, Multicast.* Os endereços de Broadcast foram substituídos pelo os endereços Multicast.

De acordo com Godinho (2004). O endereço *Unicast* identifica apenas uma única interface de rede. Um endereço *unicast* é associado a apenas uma interface de rede, enquanto que uma interface de rede pode ter associados a si vários endereços *unicast,* Eles são representados da seguinte forma:

- *Aggregable Global Address* – representa um endereço que será globalmente usado, e especificado por um endereço como este (3ffe:2b00:106::5);

- *Link-Local Address* – pode ser automaticamente conFigurado em qualquer interface pela conjugação do seu prefixo FE80::/10. São utilizados nos processos de conFiguração dinâmica e de reconhecimento de vizinhos (Neighbour Discovery);
- *Site-Local Address* - é identificado pelo prefixo FEC0::/10 (1111111011) e é considerado como privado visto estar restrito a um domínio sem ligação à Internet;
- *Unspecified Address* - representado por 0:0:0:0:0:0:0:0 ou"::", indica ausência de um endereço e nunca deverá ser utilizado em nenhum nó;
- *Loopback Address* - representado por 0:0:0:0:0:0:0:1 ou"::1"e usado quando um nó envia um datagrama a si próprio;
- IPv4 Compatible IPv6 Address - representa um endereço IPv6 cujos últimos 32 bits representam um endereço IPv4. (Ex.: 0:0:0:0:0:0:192.168.67.2 ou no 28 seu formato abreviado ::192.168.67.2;

Os endereços *Anycast* identificam um grupo de interfaces pertencentes a nós diferentes. A idéia é entregar os pacotes a um integrante de um grupo de computadores sem necessariamente saber quem é, e também sem a necessidade de entregar a todos os integrantes e também sem a necessidade de ficar procurando na rede quem é o destinatário correto, pois neste caso o primeiro a receber é o destinatário correto (Godinho,2004).

Deering e Hinden (1998), mencionam a respeito dos endereços *Anycast*:

> (...) são alocados no mesmo espaço de endereçamento *Unicast*, utilizando qualquer um dos formatos dos endereços *Unicast*. Assim, ambos os tipos de endereços não são distinguíveis sintaticamente. Quando um endereço *Unicast* é conFigurado em mais de uma interface num mesmo nó, ele transforma-se em um endereço *Anycast,* e o nó deve ser explicitamente conFigurado para reconhecer este endereço.

Os endereços *anycast* são particularmente úteis para prover certos tipos de serviços, que não requerem relação rígida do tipo cliente-servidor, com um determinado servidor específico. Por exemplo, pode-se conFigurar com classe de servidores de nomes com

endereços de *anycast*; o host cliente acessará o servidor de nomes que estiver mais próximo e o critério para isto é a métrica, isto é, o destino que estiver mais próximo pelo número de salto será o escolhido (Santos, 2004).

Os endereços *Multicast* identificam um grupo de interfaces pertencentes a diferentes nós, porém um pacote destinado a um endereço multicast é enviado para todas as interfaces do grupo. Este endereço corresponde a um conjunto de computadores, possivelmente em muitos locais, que tem por finalidade enviar um único datagrama para todas as interfaces que fazem parte de um determinado grupo de endereços (Pfützenreuter, 2001).

Deering e Hinden (1998), mencionam a respeito dos endereços *Multicast*:

> Cada grupo tem um endereço especialmente atribuído, os emissores para este grupo usam este endereço como endereço de destino para seus pacotes (...). Os *hosts* entram em grupos *multicast* usando um protocolo IGMP (*Internet Group Management Protocol* – Protocolo de gerenciamento de grupo da Internet). Eles usam esse protocolo para notificar um roteador em sua rede local de que desejam receber pacotes enviados para um determinado grupo *multicast.*

4.5. Transição do IPv4 para o IPv6

O *Internet Engineering Task Force* (IETF) trabalha acerca de dez anos no IPv6, e garante que está pronto para ser implantado, porém alguns sistemas operacionais não tem implementado todas as suas funcionalidades ou recomendam o uso apenas para fines de estudo, como é o caso do Microsoft Windows XP.

Em relação ao IPv6, a Microsoft afirma que "O software IPv6, fornecido com esta versão, contém um código de pré-lançamento e não se destina ao uso comercial. Este software está disponível apenas para fins de pesquisa, desenvolvimento e teste; não deve ser utilizado em um ambiente de produção. A Microsoft não é responsável pela utilização do código ou pêlos resultados do uso desse código" (Microsoft, 2001).

Essa transição do protocolo IPv4 para o IPv6 deve ocorrer de forma gradativa para não existir problemas como indisponibilidade de incompatibilidade dos sistemas. Para que ocorra uma

transição sem muitos problemas a melhor forma de difundir IPv6 é o método da coexistência IPv4-IPv6, assim as funcionalidades presentes no IPv4 continuaram funcionando sem a necessidade de interoperabilidade e somados com as novas funcionalidades presentes no IPv6.

Os protocolos IPv4 e IPv6 são inversamente compatíveis, isto é, os sistemas com protocolo IPv6 podem enviar, rotear e receber datagramas IPv4, enquanto os sistemas habilitados para IPv4 não podem manusear datagramas IPv6. Devido a esta e outras restrições, transição levará um certo tempo, assim sistemas IPv6 terão que coexistir com sistemas executando em estrutura IPv4, para que a transição ocorra gradualmente (Martini, 2003).

De acordo com Kurose e Ross (2003), os principais mecanismos para transição dos protocolos podem ser divididos em duas categorias:

- Pilha Dupla;
- Tunelamento.

Começando pelo primeiro mecanismo de pilha dupla, permite encapsular pacotes IPv6 em cima do atual transporte IPv4 permitindo a acessibilidade de nós e serviços IPv6. Chamados de nós “IPv4/IPv6”, possuem a habilidade de enviar e receber pacotes utilizando-se tanto do IPv4 quanto do IPv6 e podem interoperar com nós IPv4 usando pacotes IPv4, o mesmo acontecendo para nós IPv6.

Kurose e Ross (2003), mencionam a respeito dos nós IPV4/IPv6:

> Os nós IPv4/IPv6 devem ter os endereços IPv6 e IPv4. Além disso, devem poder determinar se outro nó é habilitado a IPv6 ou somente a IPv4. Esse problema pode ser resolvido usando o DNS, que poderá devolver um endereço IPv6 se o nome do nó a ser resolvido for habilitado a IPv6. Caso contrário, ele devolverá um endereço IPv4. É claro que, se o nó que estiver emitindo a requisição DNS for habilitado apenas a IPv4, o DNS devolverá apenas um endereço IPv4.

Na abordagem de pilha dupla, se o remetente ou o destinatário forem habilitados apenas ao IPv4, um datagrama IPv4 deverá ser usado e, como resultado é possível que dois

nós habilitados para IPv6 acabem enviando datagramas IPv4 um para outro. Conforme ilustrado na Figura 13.

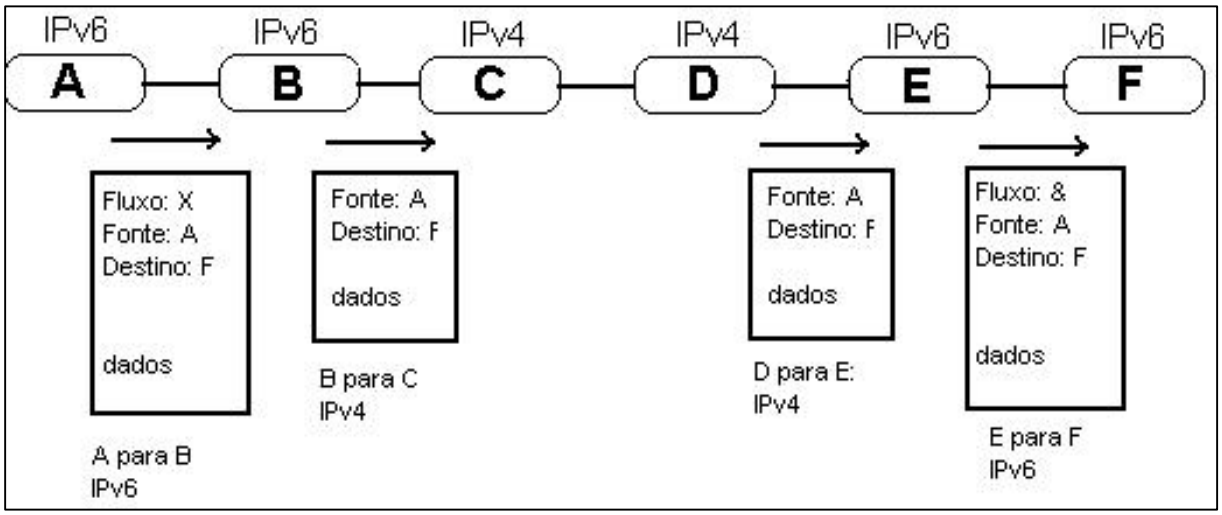

Figura 13 – Abordagem da pilha dupla (Kurose e Ross, 2003).

Conforme Kurose e Ross (2003), essa abordagem da pilha dupla pode ser explicada da seguinte maneira. Suponha que o nó A com IPv6 acabem enviando datagramas IP ao nó F, que também possui IPv6. Os nós A e B podem trocar um pacote IPv6. Desde que o nó B crie um datagrama IPv4 para enviar a C. É certo que o campo de dados do pacote IPv6 pode ser copiado para o campo de dados do datagrama IPv4 e o mapeamento do endereço adequado pode ser feito. No entanto, ao realizar a conversão do IPv6 para o IPv4, haverá campos IPv6 específicos no datagrama IPv6 que não terão contrapartes em IPv4. As informações contidas nesses pacotes serão perdidas. Assim, mesmo que E e F possam trocar datagramas IPv6, os datagramas IPv4 que chegarem a E e D não conterão todos os campos que estavam no datagrama IPv6 original enviado de A. Uma alternativa para resolver esse problema da pilha dupla, é conhecida como tunelamento.

A idéia básica do tunelamento segundo Kurose e Ross (2003), “Suponha que dois nós (IPv6) queiram interoperar usando datagrama IPv6, mas são conectados por roteadores

intervenientes. Referimos-nos ao conjunto de roteadores intervenientes IPv4 entre dois roteadores IPv6, como um túnel", como ilustrado na Figura 14.

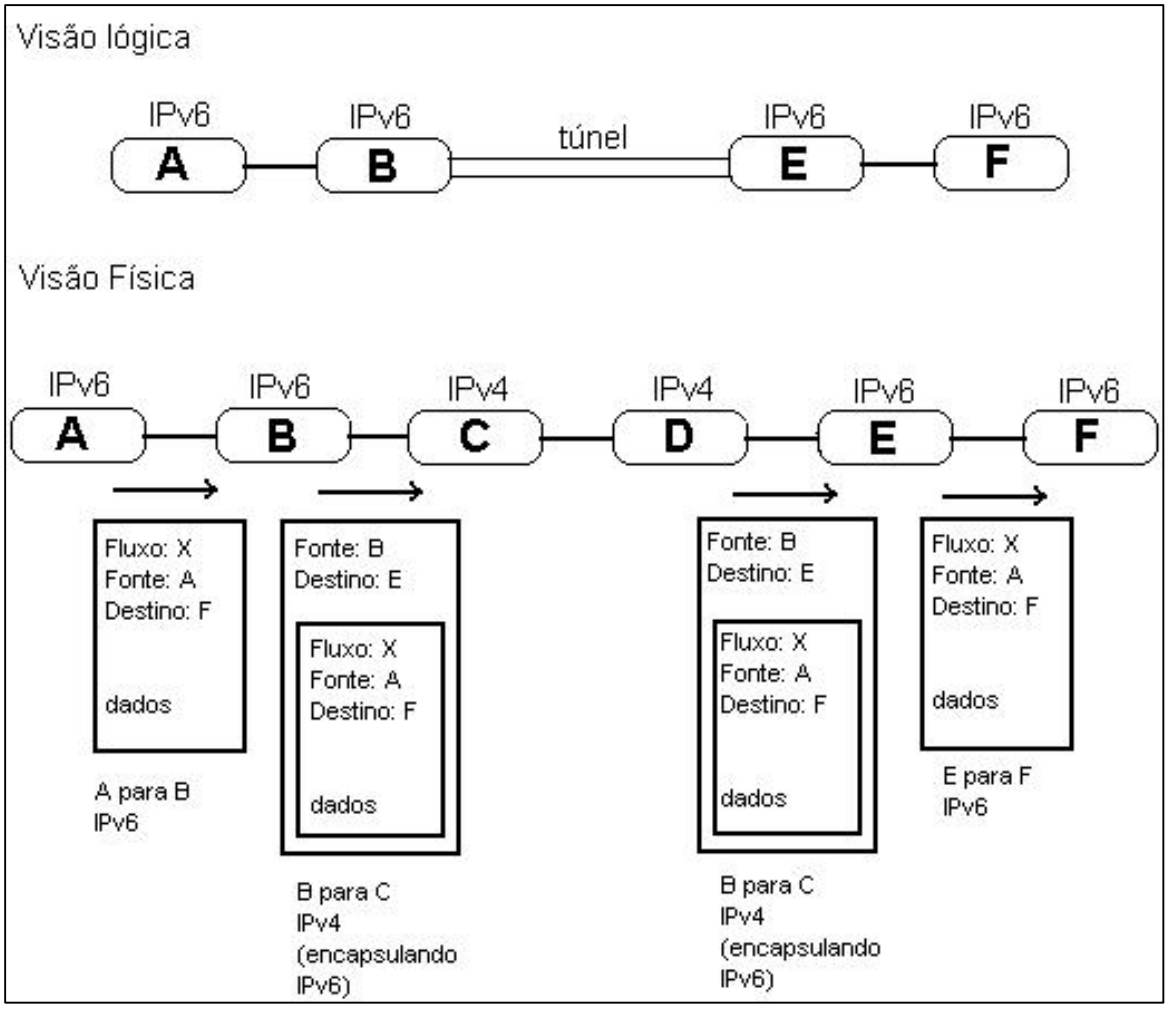

Figura 14 – Implementação do túnel (Kurose e Ross, 2003).

Com a implementação do túnel, o nó IPv6 no lado remetente do túnel (por exemplo, B) pega um datagrama IPv6 integral e o coloca no campo de dados (carga útil) de um datagrama IPv4. Esse datagrama IPv4 é então endereçado ao nó IPv6 no lado receptor do túnel (por exemplo, E) e enviado ao primeiro nó do túnel (por exemplo, C). Os roteadores IPv4 intervenientes no túnel roteiam esse datagrama IPv4 entre eles, exatamente como fariam com qualquer outro datagrama, alheios ao fato de que o datagrama IPv4 contém em si um datagrama IPv6 completo. O nó IPv6 do lado receptor do túnel possivelmente recebe o

datagrama IPv4 (ele é o destino do datagrama IPv4), determina que o datagrama IPv4 contém um datagrama IPv6, extrai o datagrama IPv6 e, em seguida, roteia o datagrama IPv6 do mesmo modo como o faria se tivesse recebido o datagrama IPv6 de um vizinho IPv6 diretamente ligado a ele.

5. COMPARAÇÃO ENTRE IPv4 E IPV6

O IPv6 foi especificado com o objetivo de ser evolucionário em relação ao IPv4. Assim, as funções do IPv4 consideradas válidas foram mantidas e aquelas pouco usadas foram retidas ou tornadas opcionais no IPv6.

O principal problema que o IPv6 tenta resolver é o espaço de endereçamento, que foi expandido de 32 bits para 128 bits, permitindo endereçar um número bem maior de nós e criar mais níveis hierárquicos de endereços. Além disso, não é empregado mais o conceito de classes de endereço, são especificados três tipos de endereços: *unicastt, anycast* e *multicast*.

Outra mudança está no cabeçalho. O IPv6 possui um cabeçalho básico e vários cabeçalhos de extensão. Alguns dos campos do cabeçalho IPv4 foram descartados ou tornados opcionais. Esse cabeçalho básico é bastante simplificado em comparação ao do IPv4, o objetivo de tal simplificação foi garantir que o tempo de processamento dos datagramas nos roteadores não crescesse significativamente, embora o tamanho total do cabeçalho seja duas vezes maior que o cabeçalho do IPv4 em virtude dos campos de endereços serem quatro vezes maior. (Carvalho, 1997).

O campo de opções do cabeçalho do IPv4 foi retirado e substituído pelos cabeçalhos de extensão, permitindo uma maior flexibilidade para suportar características opcionais. Foram especificados seis tipos diferentes de cabeçalhos de extensão. Como nem todos esses cabeçalhos de extensão são processados pelos roteadores, há um aumento de desempenho do processamento dos datagramas IPv6 em comparação aos datagramas IPv4, que os campos de opções devem ser, obrigatoriamente, processados pelos roteadores.

Outra melhoria do IPv6 é o suporte à segurança abaixo do nível de aplicação com a inclusão dos cabeçalhos de extensão *Authtentication Header* (AH) e o *Encapsulation Security Header* (ESP). No IPv6 o emissor dos pacotes tem como identificar um fluxo de pacotes para

um determinado destino (*unicast* ou *multicast)* e pode pedir o tratamento especial desse fluxo por parte do roteador, como QoS (qualidade de serviço) diferenciada e serviço de tempo real. No IPv4 esse tipo de funcionalidade é implementado pelos roteadores e *switches* de camadas 3 ou 4, sobrecarregando seu processamento. O custo desse processamento foi passado para o emissor do pacote e os equipamentos podem utilizar o processamento economizado para outras funções (Yokomizo, 2005).

A função de fragmentação, no IPv4, pode ser realizada pelo nó origem e qualquer roteador intermediário existente no caminho percorrido por um datagrama. Quando ocorre uma fragmentação devem ser atualizadas os campos correspondentes do datagrama. No caso do IPv6, a fragmentação só pode ser efetuada pelo nó origem, o que simplifica a operação dos roteadores intermediários. O nó origem deve incluir, nos datagramas gerados a partir de um mesmo datagrama original, o cabeçalho de extensão de fragmentação.

A previsão para extensão do protocolo é tida por muitos como a maior melhoria no protocolo, existe uma flexibilidade de expansão do protocolo para novas realidades e tecnologias, ao contrário do IPv4, onde existe uma especificação fechada e completa do protocolo.

O roteamento no IPv6 permite, através da utilização do cabeçalho de extensão de roteamento, que o nó origem determine a rota que o datagrama deve seguir na rede. Tal rota pode ser determinada de modo a atender requisitos diversos, como do desempenho e custo. Esse cabeçalho tem a função, também, de informar ao nó destino seu auto-reendereçamento. No Ipv4, poderiam ser implementadas funções análogas de roteamento fonte, empregando-se um protocolo de camada superior.

O IPv4 não provê serviços de segurança. Isso é feito pelo IPv6, empregando-se dois cabeçalhos de extensão diferentes, os cabeçalhos de autenticação e de privacidade.

A Tabela 1 demostra de forma resumida uma comparação entre as duas versões do Protocolo IP, o IPv6 e o IPv4.

Tabela 1 – Comparação das principais características do IPv4 e IPv6 (Carvalho, 1997).

Itens de Comparação	IPv4	IPv6
Endereços IP	• Tamanho do campo de endereços igual a 32 bits. • Definição de cinco classes de endereços (A, B, C, D e F)	• Tamanho máximo do campo de endereços igual a 128 bits. • Definição de três tipos de endereços: *unicast, anycast e multicast*.
Cabeçalho	• Existência de *checksun* do cabeçalho. • Existência de um campo de opções, limitando em 40 bytes. • Inexistência de mecanismo de definição de fluxo de tráfego.	• Inexistência de *checksun* do cabeçalho. • Existência de cabeçalhos de extensão, com tamanho arbitrários. • Possibilidade de vincular vários datagramas ao mesmo fluxo de tráfego.
Fragmentação	• Realização de fragmentação em qualquer roteador, usado na interconexão de sub-redes destintas.	• Realização de fragmentação apenas no nó origem.
Roteamento	• Suporte aos protocolos básicos de roteamento. • Função de roteamento na fonte por exercida por um protocolo de camada superior.	• Suporte aos protocolos básicos de roteamento. • Função de roteamento na fonte implementada utilizando-se o cabeçalho de extensão de roteamento.
Segurança	• Inexistência de mecanismos de segurança.	• Suporte a mecanismos de segurança usados na implementação de serviços de autenticação, não-repudiação, integridade e confidencialidade.
Controle de Erros e Resolução de Endereços	• O controle de erros é efetuado pelo protocolo ICMP, a resolução de endereços IP e físico realizada pelos protocolos ARP e RARP respectivamente e o controle de membros de endereços *multicast* efetuado pelo protocolo IGMP.	• As funções de controle de erro, resolução de endereços e controle de membros de endereços *multicast* é realizada dentro do âmbito de um único protocolo, o ICMP.

6. IMPLEMENTAÇÃO DO IPv6

Atualmente vários sistemas operacionais existentes no mercado possuem suporte ao IPv6. Alguns como o Windows XP, Windows 2003 Server e algumas distribuições Linux (Red Hat Linux 7.3, entre outros) já incluem suporte ao IPv6.

No caso do Windows 95/98 é necessário a instalação de ferramentas como o Trumpet Winsock 5.0 para a implementação do IPv6. Podendo ser encontrada em http://www.trumpet.com.au/ipv6.htm. No Windows 2000 também é necessária à instalação de uma ferramenta adicional, que pode ser encontrada em http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp.

6.1 Instalação do IPv6 no Windows XP

A instalação do IPv6 no Windows XP é de maneira muito simples, é necessário através o *prompt* do DOS, executar o comando ipv6 install ilustrado na Figura 15.

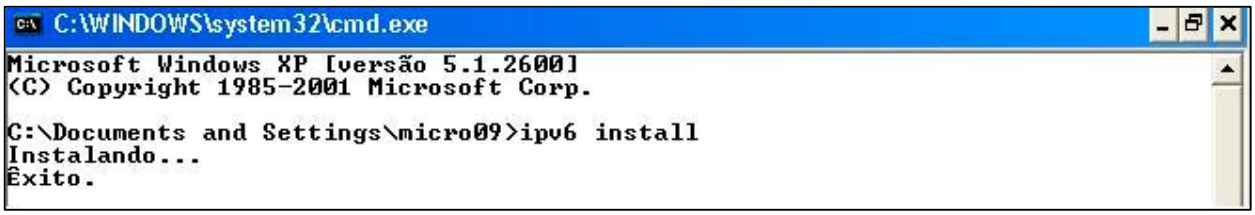

Figura 15 – Instalação do IPv6 no Windows XP

O Windows XP já inclui o protocolo IPv6, então não é necessária à instalação de nenhum módulo adicional.

Por padrão a conFiguração dos endereços IPv6 de *Link-Local* é feita para cada interface IPv6. “Os endereços de *Link-Local* têm o prefixo FE80::/64” (Microsoft, 2002),

onde o /64 indica que no endereço especificado os primeiros 64 bits (os que estão mais a esquerda) dizem respeito à rede, enquanto os últimos 64 bits (os mais à direita) identificam a máquina na rede.

Para visualizar seu endereço IPv6 pode-se utilizar o comando ipconfig ilustrado na Figura 16 e 17.

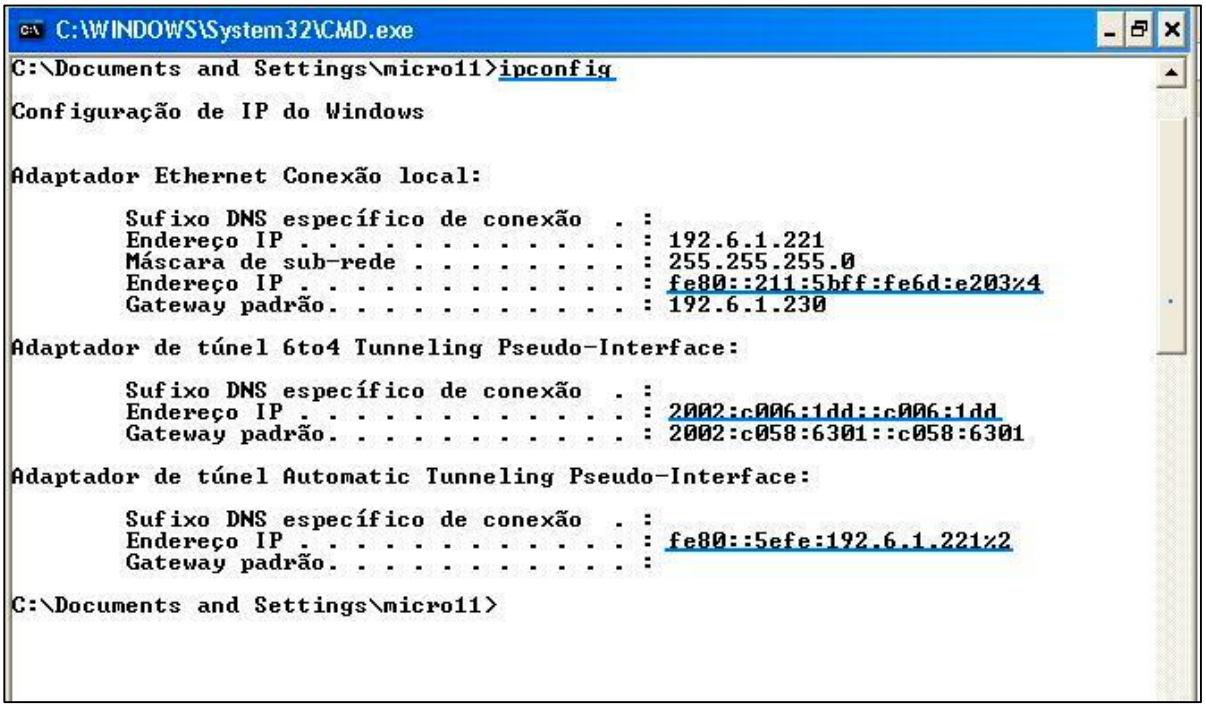

Figura 16 – Comando ipconfig Micro 01

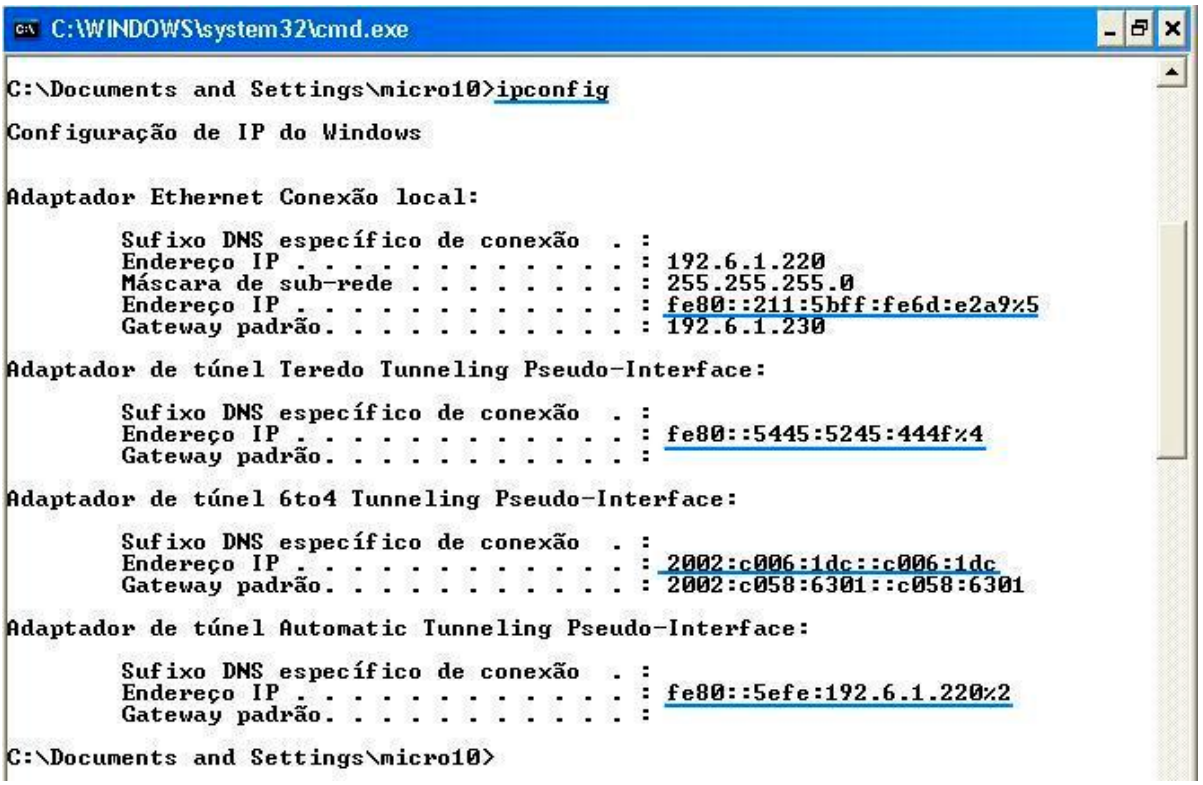

Figura 17 – Comando ipconfig Micro 02

Os comandos netsh interface IPv6 show address (para *Service Pack* 1 ou *Service Pack* 2), ou ipv6 if (caso não possua *Service Pack* instalado) também podem ser usados para visualizar o endereço IPv6 da máquina, ilustrados nas Figuras 18 e 19 respectivamente. Os comandos netsh interface IPv6 show address e ipv6 if mostram também, uma lista com todas as interfaces IPv6 existentes, como por exemplo, a interface 1 chamada *loopback Pseudo-Interface* usada para *loopback*.

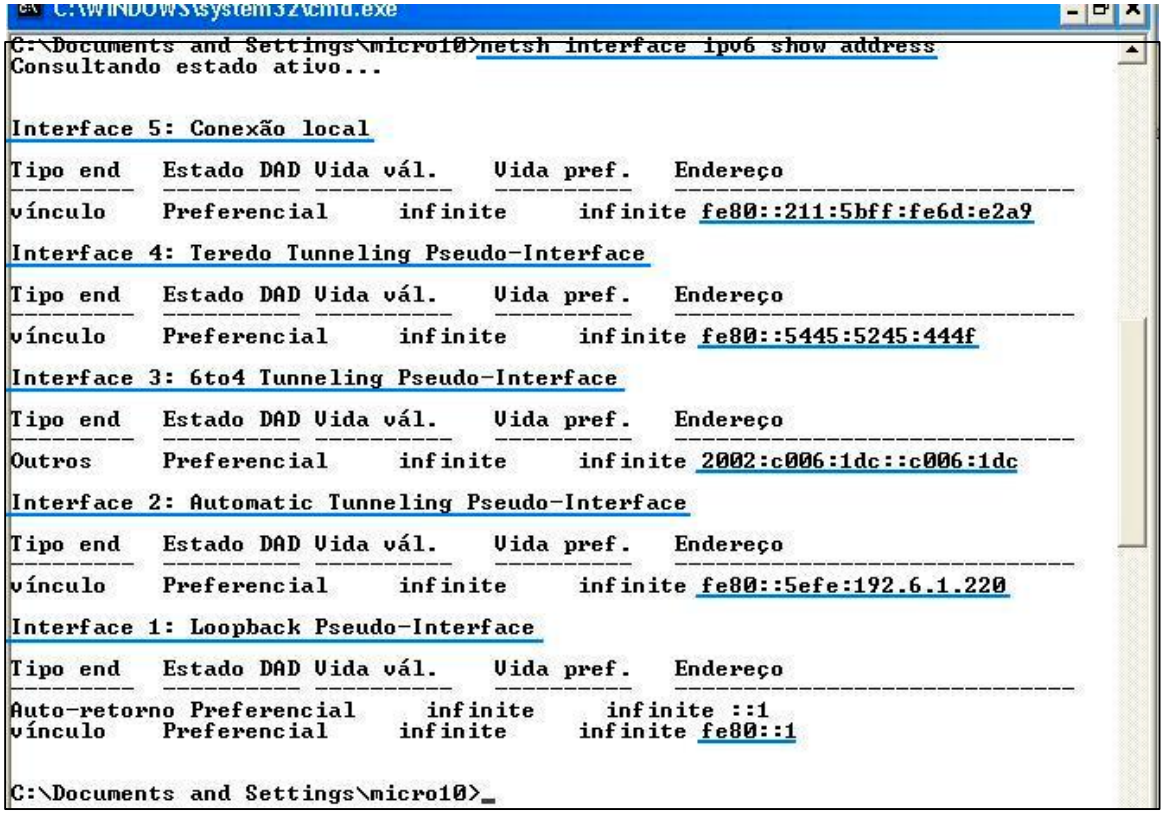

Figura 18 – Comando netsh interface ipv6 show address

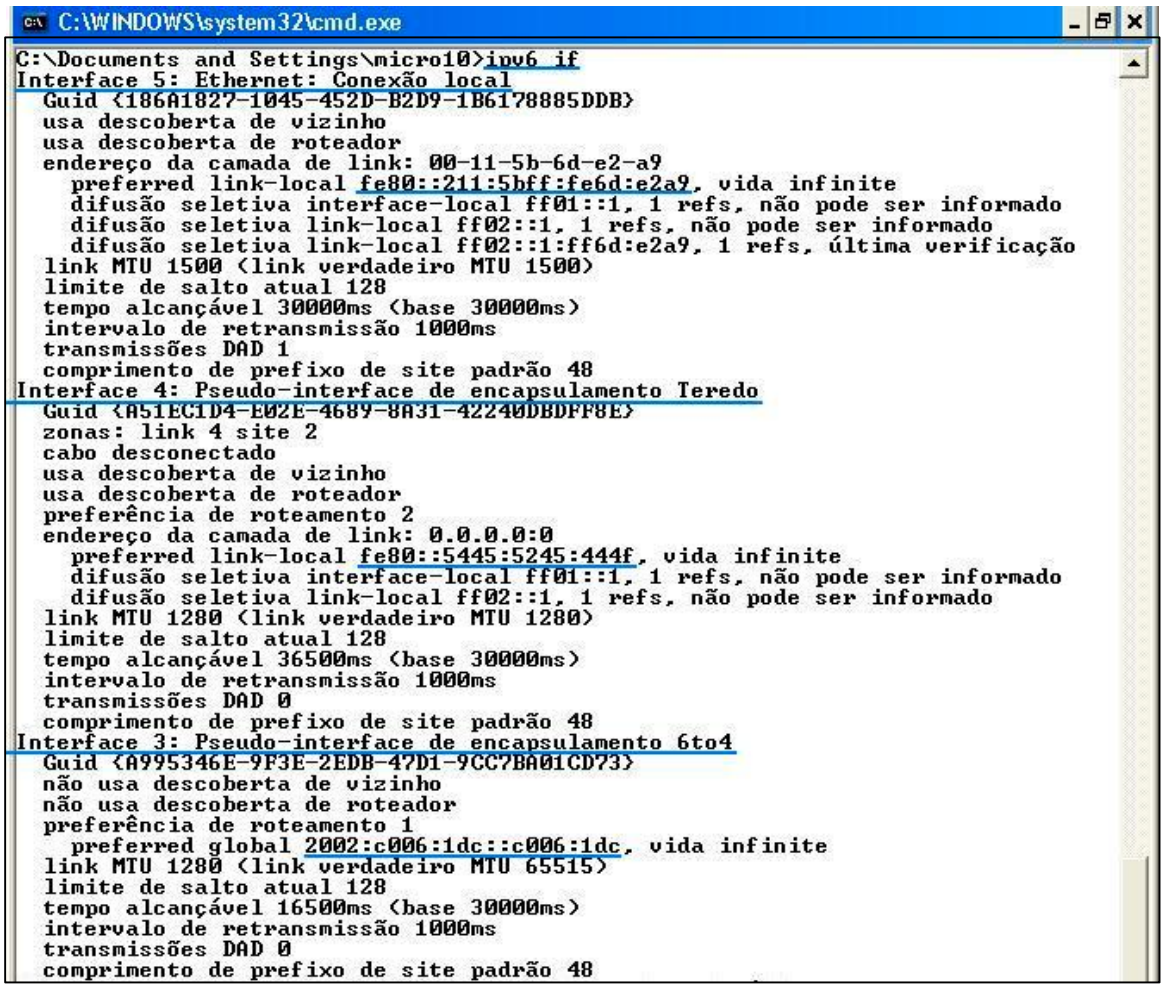

Figura 19 – Comado ipv6 if

O comando netsh interface ipv6 show interface, mostra uma lista de todas as interfaces IPv6 (com *Service Pack* instalado), como apresentada a Figura 20. De acordo com a Microsoft (2002), com exceção da interface *Lookback Pseudo-Interface*, as interfaces mostradas por esse comando podem ser diferentes.

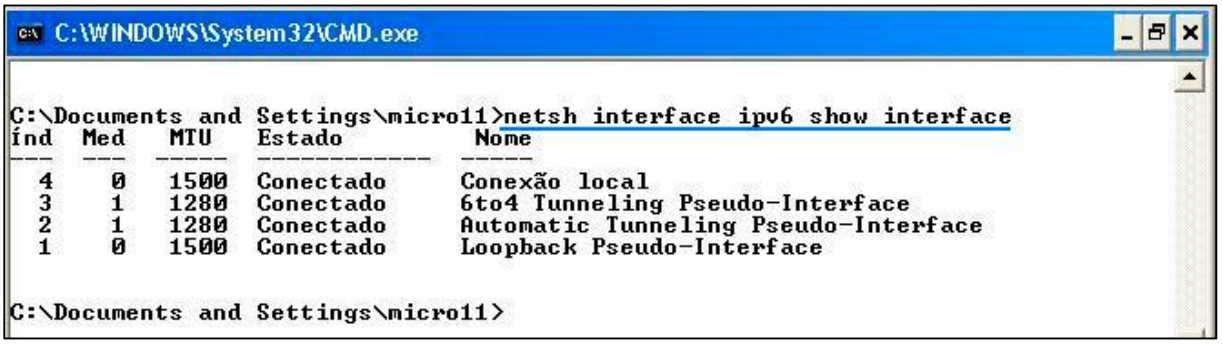

Figura 20 – Comando netsh interface ipv6 show interface micro 01

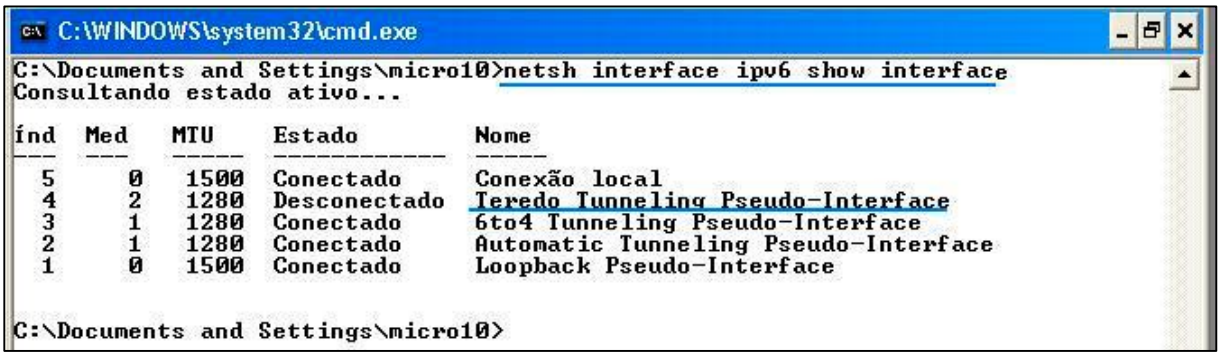

Figura 21 – Comando netsh interface ipv6 show interface micro 02

Para usar o comando ping deve-se, além de especificar o endereço, especificar uma *zone identifier* (índice da interface do endereço), ilustrados nas Figuras 22, 23, 24 e 245.

Figura 22 – Comando ping para Micro 01 Interface 4 (Conexão Local)

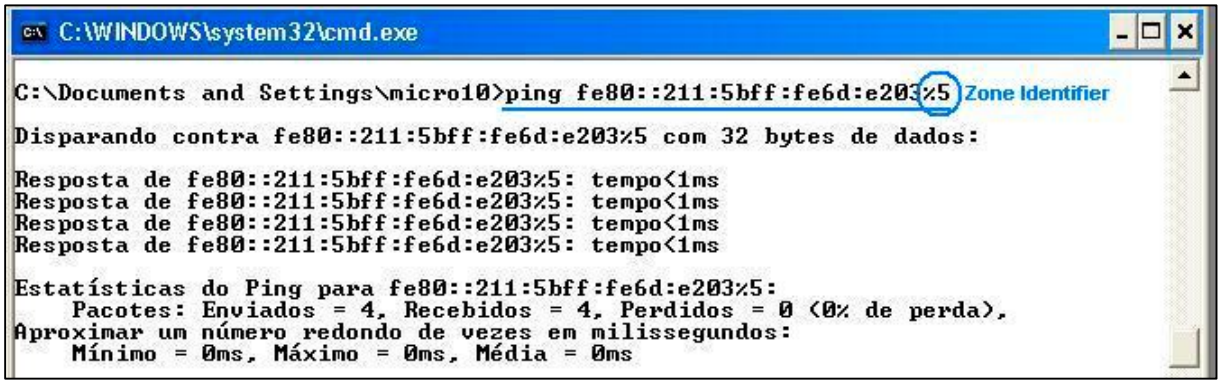

Figura 23 – Comando ping para Micro 02 Interface 5 (Conexão Local)

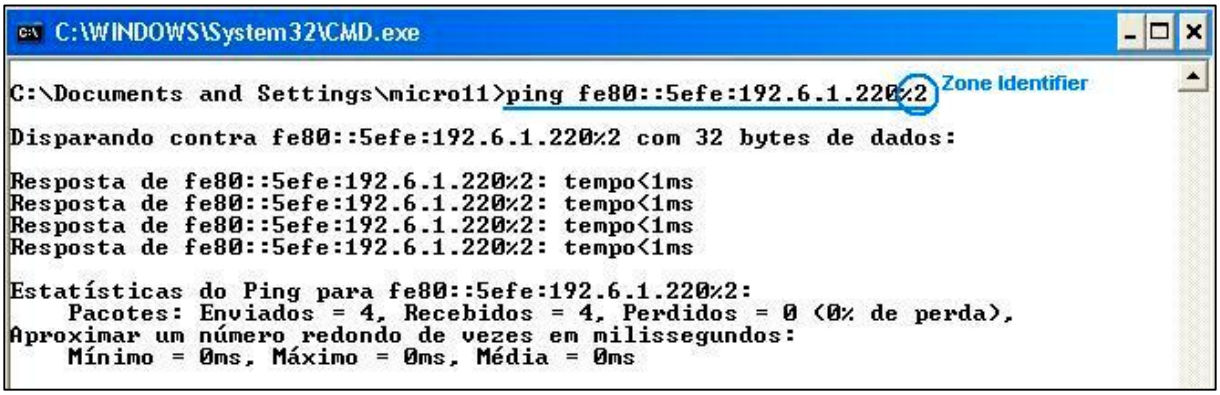

Figura 24 – Comando ping para Micro 01 *Automatic Tunneling Pseudo-Interface*

Figura 25 – Comando ping para Micro 02 *Automatic Tunneling Pseudo-Interface*

Apesar de na maioria das vezes não ser necessário à conFiguração manual do endereço IPv6, ela pode ser executada pelo comando netsh interface ipv6 add address, que adiciona um endereço IPv6 a uma interface. Através do comando netsh interface ipv6 add pode-se ainda adicionar um endereço de servidor DNS estático (netsh interface ipv6 add dns), adicionar uma rota do IPv6 sobre uma interface (netsh interface ipv6 add route), entre outros. Para consultar as opções disponíveis do comando netsh interface ipv6 add, digite netsh interface ipv6 ?.

A Figura 26, apresenta primeiramente o comando ipconfig, mostrando o endereço IP do IPv6, consequentemente executado o comando netsh interface IPv6 add address interface=4 address =fe80::211:5bff:fe6d:e204, neste comando foi adicionado um novo endereço IP, depois foi executado novamente o comando ipconfig mostrando o endereço atribuí

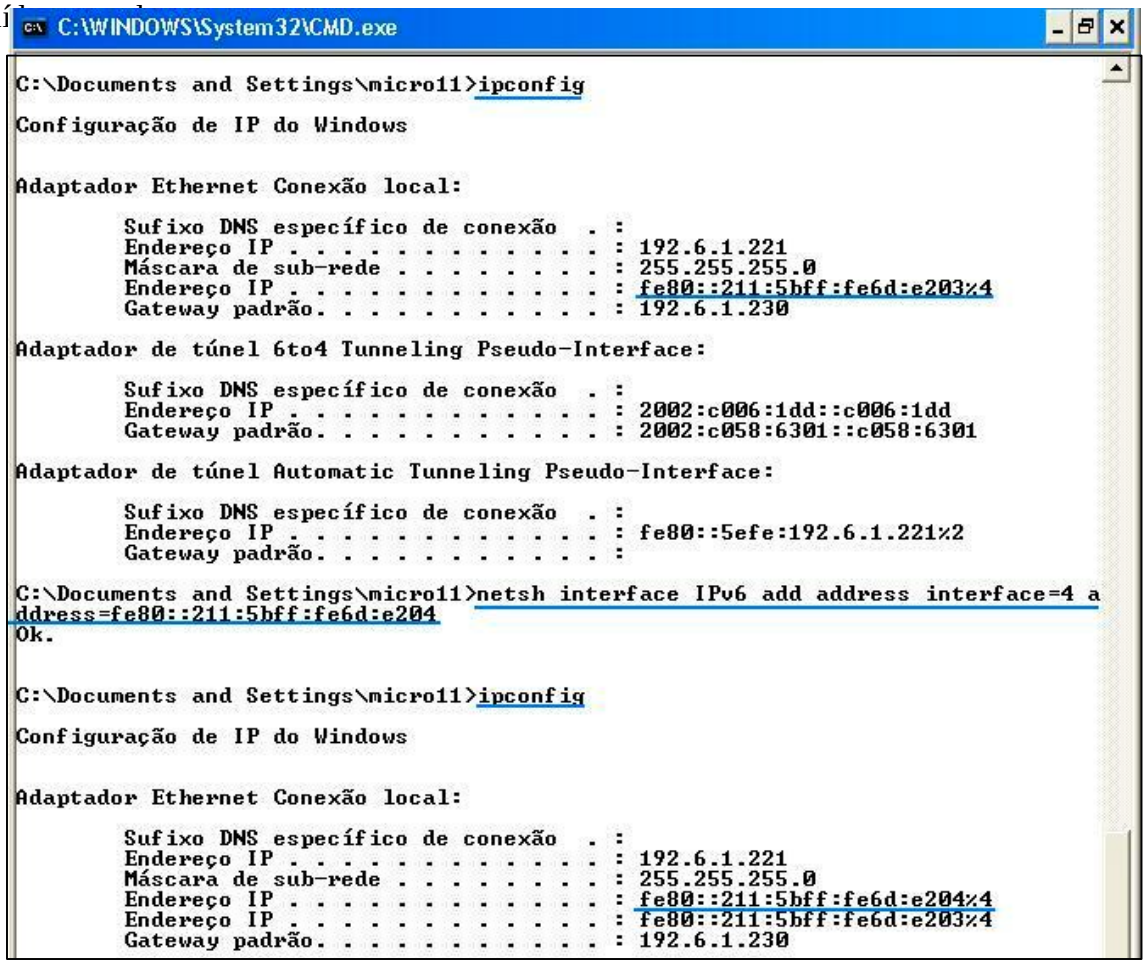

Figura 26- Comando netsh interface ipv6 add address

A lista de opções de comandos disponíveis pode ser consultada através do comando netsh interface ipv6 ou netsh interface ipv6 ?. Ilustrado na Figura 27.

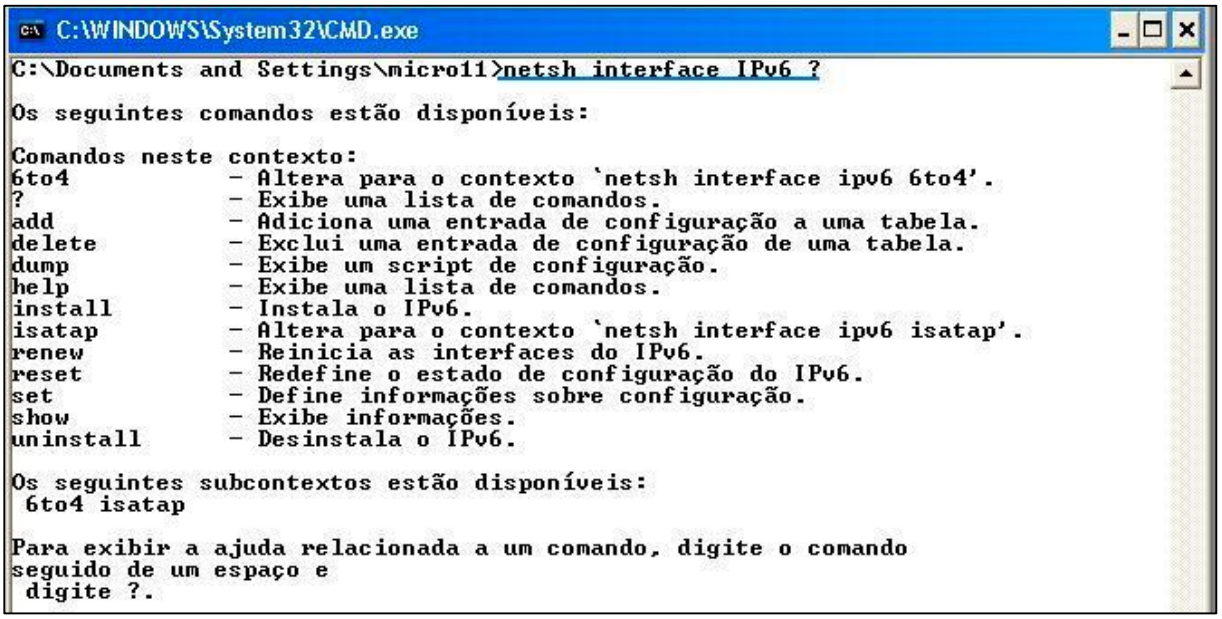

Figura 27 - Comando netsh interface ipv6 ?.

6.2 Coleta de Resultados

De acordo com os testes, a tabela 2 ilustra os resultados obtidos.

Tabela 2 – Coleta de Resultados

IPv4	IPv6
Instalação manual	Instalação Automática
Endereços de 32 bits	Endereços de 128 bits
Possui apenas 1 endereço	Possui 1 ou mais endereços
Possui apenas 1 interface	Possui de 1 até 5 interfaces
Não permiti adicionar endereços	Permiti adicionar mais que um endereço

CONCLUSÃO

Esta monografia apresentou uma descrição dos protocolos IPv4 e IPv6, procurando destacar pontos de transição e comparação, principalmente no que se refere às deficiências apresentas pelo protocolo atual, o IPv4.

O novo protocolo IPv6 vem para solucionar as deficiências apresentadas pelo protocolo IPv4, possuindo um campo de endereços igual a 128 bits, ele soluciona o problema de escassez de endereços IP e provê a diminuição das tabelas de roteamento, com a organização hierárquica dos endereços. Além disso, não é empregado mais o conceito de classes de endereço, são especificados três tipos de endereços: *unicast, anycast e multicast*.

O IPv6 possui um cabeçalho básico, ou seja, possui tamanho fixo que reduz o tempo de processamento dos pacotes e, possui vários cabeçalhos de extensão. Alguns dos campos do cabeçalho IPv4 foram descartados ou tornados opcionais. Os cabeçalhos de extensão (*Extension Headers*) deram flexibilidade ao formato do cabeçalho. Ele gera uma maior flexibilidade para a introdução de novas opções no futuro.

Além disso, uma outra mudança inovadora do IPv6 é a melhora significativa ao suporte de novas tecnologias e das aplicações existentes atualmente. Por meio da identificação do fluxo é possível um tratamento diferenciado para cada tipo de serviço, permitindo que aplicações multimídia possam contar com banda suficiente para transmitir imagens e voz sem interrupções. Esse suporte a aplicações em tempo real e suporte a QoS são garantidos pelos campos *Traffic Class e Flow Label,* que foram desenvolvidos especialmente para o controle desse tipo de tráfego.

Outra melhoria do IPv6 é o suporte à segurança abaixo do nível de aplicação com a inclusão dos cabeçalhos de extensão *Authtentication Header* (AH) e o *Encapsulation Security Header* (ESP), o IPv6 provê autenticação, integridade e confidencialidade aos datagramas. O

receptor de um datagrama pode ter certeza de quem o enviou e que seu conteúdo não foi modificado.

A função de fragmentação, no IPv4, pode ser realizada pelo nó origem e qualquer roteador intermediário existente no caminho percorrido por um datagrama. Quando ocorre uma fragmentação devem ser atualizados os campos correspondentes do datagrama. No caso do IPv6, a fragmentação só pode ser efetuada pelo nó origem, o que simplifica a operação dos roteadores intermediários. O nó origem deve incluir, nos datagramas gerados a partir de um mesmo datagrama original, o cabeçalho de extensão de fragmentação.

Outro ponto importante a ser considerado diz respeito à transição do IPv4 para o IPv6, que pode ser realizada de acordo às necessidades de cada um e mantendo também a "convivência harmoniosa" entre essas duas versões do protocolo IP. As duas técnicas de transição (tunelamento e pilha dupla) combinadas disponibilizarão aos administradores de rede a flexibilidade e interoperabilidade que eles necessitam para implementar o IPv6.

A utilização do protocolo IPv6 deve ser fácil, visto que seu funcionamento é bem parecido com o do IPv4. Além disso, existe também o fato de que os principais sistemas operacionais do mercado já incluem ou possuem mecanismos de suporte ao IPv6.

Essa transição do protocolo IPv4 para o IPv6 deve ocorrer de forma gradativa para não existir problemas como indisponibilidade de incompatibilidade dos sistemas. Para que ocorra uma transição sem muitos problemas a melhor forma de difundir IPv6 é o método da coexistência IPv4-IPv6, assim as funcionalidades presentes no IPv4 continuaram funcionando sem a necessidade de interoperabilidade e somados com as novas funcionalidades presentes no IPv6.

REFERÊNCIAS BIBLIOGRÁFICAS

CARVALHO, T. C. M. B. Arquitetura de redes de computadores OSI e TCP/IP. 2ª Ed. Rev. Ampl. São Paulo: Editora Makron Books, 1997. Volume 1.

COMER, D. E. Interligação em redes com TCP/IP: Princípios, Protocolos e Arquitetura. 3ª Ed. Rio de Janeiro: Editora Campus, 1998. Volume 1.

COSTA, F. H. D. da. A Nova Geração da Internet: IPv6 ou IPng – O Protocolo da Nova Geração. 2000. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – UNIC – Universidade de Cuiabá, Cuiabá, 2000.

DANTAS, M. Tecnologias de Redes Comunicação e Computadores. 1ª Ed. Rio de Janeiro: Editora Axcel Books, 2002.

DEERING, S.; HINDEN, R. RFC 2460 – Internet Protocol, Version 6 (IPv6) Specification. dez.1998.

GODINHO, L. J. Análise de Segurança com Protocolo IPv6: Ambientes Windows e Linux. 2004. Universidade Luterana do Brasil - ULBRA – Centro Universitário Luterano de Palmas.

GOMES, A. P. Introdução ao IPv6. Disponível em: http://www.lsi.usp.br/~ader/introducaoIPv6.pdf .Acessado 05 jul. 2006.

GUPTA, M.; LASALLE, P.; PARIHAR, M; SCRINGER. R. TCP/IP A Bíblia. Tradução: Furmankiewiez, Doweware Traduções. Editora Campus, 2002.

KUROSE, J. F.; ROSS, K. W. Redes de Computadores e a Internet: Uma nova Abordagem. 1ª Ed. São Paulo: Makron Books, 2003.

MARTINI, F. Implantação de um Ambiente de Rede IPv6 utilizando Tunelamento para comunicação. 2003. Universidade Luterana do Brasil – ULBRA - Centro Universitário Luterano de Palmas.

MICROSOFT. Microsoft corporation. 2001. Disponível em: http://www.microsoft.com, Acesso em: 08 ago. 2006.

MOREIRA, A. "Internet Protocol" Versão 6 (IPv6). Disponível em: http://www.dei.isep.ipp.pt/~andre/documentos/ipv6.html. Acesso em: 02 jun. 2006.

PFÜITZENREUTER, E. Migração para IPv6 de aplicações usuárias da interface de programação Sockets BSD. 2003. Monografia de Pós Graduação – UFSC - Universidade Federal de Santa Catarina.

ROSA, M.; VEIGA, P. Bancada de Testes IPv6. Disponível em: http://www.uc.pt/crc98/comfin30/comfin30.html .Acesso em: 16 mai. 2006.

SANTOS, C. R. Integração de IPv6 em um Ambiente Cooperativo Seguro. 2004. Dissertação de Mestrado – UNICAMP - Instituto de Computação da Universidade Estadual de Campinas, Campinas, 2004.

TANENBAUM, A. S. Redes de Computadores. 4ª Ed. Rio de Janeiro: Editora Campus, 2003.

YOKOMIZO, L. A. IPv6: Estrutura Básica do Protocolo. 2005. 70. Monografia (Pós-Graduação em Redes de Computadores e Internet) – Centro Universitário Eurípides de Marília, Fundação de Ensino Eurípides Soares da Rocha, Marília, 2005.