EDUARDO ENIO MARTINS

ESTUDO E AVALIAÇÃO DO PROTOCOLO DE REDE IPv6

Trabalho de conclusão de curso apresentado ao colegiado do Programa de Graduação em Engenharia de Telecomunicações do Centro de Ciências Tecnológicas da Universidade Regional de Blumenau, como requisito parcial para a obtenção do título de Engenheiro de Telecomunicações.

Orientador: Prof.º Francisco Adell Péricas.

BLUMENAU (SC)
2007.

UNIVERSIDADE REGIONAL DE BLUMENAU - FURB

CENTRO DE CIÊNCIAS TECNOLÓGICAS

PROGRAMA DE GRADUAÇÃO EM ENGENHARIA DE TELECOMUNICAÇÕES

ESTUDO E AVALIAÇÃO DO PROTOCOLO DE REDE IPv6

Monografia submetida à

Universidade Regional de Blumenau

como parte dos requisitos para a

obtenção do título de Engenheiro de Telecomunicações

EDUARDO ENIO MARTINS

Blumenau

2007

ESTUDO E AVALIAÇÃO DO PROTOCOLO DE REDE IPv6

EDUARDO ENIO MARTINS

"Esta monografia foi julgada adequada para obtenção do Título de Engenheiro de Telecomunicações e aprovada pela Banca Examinadora."

_____

Francisco Adell Péricas – Orientador

Banca Examinadora:

_____

Fábio Rafael Segundo

Presidente

DEDICATÓRIA

Dedico este trabalho a meus pais, que me deram a vida, a minhas filhas que me deram uma razão, a meu sogro e principalmente sogra que me deram incentivo para começar e minha esposa que me deu apoio, carinho e amor, sem os quais não teria forças para concretizar o meu sonho.

AGRADECIMENTOS

Agradeço a Deus por me permitir chegar até este momento.
A todos que de uma forma ou de outra contribuíram neste trabalho.
Aos colegas de curso que sempre me ajudaram a achar o caminho.
Ao Amílcar Pinheiro que dispôs de seu tempo para me auxiliar a achar um tema para este trabalho.
Ao meu Orientador que com paciência e sabedoria esteve sempre presente, me auxiliando e indicando o caminho a seguir.
A minha esposa e minhas filhas que souberam suportar a minha ausência em muitos momentos em que minha presença se fazia necessária.
E a Cia.Hering que em muitos momentos me permitiu encurtar o horário de trabalho para que eu pudesse me dedicar a este propósito.

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

AAA – Address Allocation Architecture – (Alocação de Endereço para Roteamento Inter-Domínio sem Classe)

ADSL – Assymmetric Digital Subscriber Line

ARPA – Advanced Research and Projects Agency

CIDR – Classless Inter-Domain Routing

CIDR – Classless Inter-Domain Routing – (Roteamento Inter-Domínio sem Classe)

CLNP – ConnectionLess Network Protocol

CLNP – Connection-Less Network Protocol

DARPA – (Defense) Advanced Research Projects Agency– (Agência de Pesquisas de Projetos Avançados de Defesa).

DHCP – Dynamic Host Configuration Protocol

DHCPv6 – Dynamic Host Configuration Protocol – (Protocolo Dinâmico de Configuração de Host)

DNS – Domain Name System – (Sistema de Nomes de Domínios)

DoD – Department of Defense,

FTP – File Transport Protocol

HTTP – Hyper Text Transport Protocol

IAB – Internet Activities Board

IANA – Internet Assigned Numbers Authority – (Autoridade para Atribuição de Números na Internet)

ICMP – Internet Control Message Protocol

IETF – Internet Engineering Task Force – (Força Tarefa de Engenharia da Internet)

IGMP – Internet Group Management Protocol

IMP – Interface Message Processor – (Processador de Mensagens de Interface)

IP – Internet Protocol

IPAE – IP Address Encapsulation

IPng – Internet Protocol Next Generation – (Próxima Geração do Internet Protocol)

IPNGWG – IP Next Generation Working Group

IPTO – Information Processing Techniques Office – (Escritório de Técnicas de Processamento de Informação)

IPX/SPX – Internet Packet Exchange/Sequenced Packet Exchange

ISP – provedores de acesso

LACNIC – Registro de Endereçamento da Internet para América Latina e Caribe

LIR – Local Internet Registry

LLC – Logical Link Control

MCT – Ministério de Ciência e Tecnologia

NAT – Network Address Translation – (Tradução de Endereço de Rede).

NCP – Network Control Protocol

OSI – Open Systems Interconnection – (Sistemas Abertos de Interconexão)

Pip – Paul's internet protocol

PNAD – Pesquisa Nacional Por Amostra de Domicílios

QoS – qualidade de serviço

RFC – Request for Comments

RNP – Rede Nacional de Pesquisa

SIP – Simple IP

SIPP – Simple IP Plus

SMTP – Simple Mail Transport Protocol

SSH – Security Shell

TCP/IP – Transfer Control Protocol/Internet Protocol

TUBA – TCP and UDP over Bigger Address

WINS – Windows Internet Name System

LISTA DE TABELAS

LISTA DE FIGURAS

RESUMO

O crescimento exagerado da internet levou a grande necessidade de endereços IP, não previsto pelos criadores do protocolo de acesso, os problemas que surgiram, como a escassez de endereços e a não possibilidade da implementação de melhorias necessárias para a evolução da rede, levaram a um crescimento das tabelas utilizadas para roteamento, o que tornou o roteamento lento e ineficiente, obrigando os responsáveis a criarem um novo protocolo de comunicação (IPv6) para substituir e suprir todas as implementações necessárias. O IPv6 é uma solução para este problema de escassez de endereços IP e também é provido de novos recursos, tais como o suporte a novas tecnologias de rede (ATM, Gigabit Ethernet, entre outros), novo formato do cabeçalho, infra-estrutura hierárquica e eficiência de roteamento e endereçamento, configuração de endereçamento com ou sem estado, segurança embutida, melhor suporte para a qualidade dos serviços (QoS), novo protocolo para interação entre nós vizinhos e capacidade de extensão. Com o IPv6 haverá um novo protocolo de mensagens de controle da Internet: o ICMPv6. Ele está definido na RFC 2463, "*Internet Control Message Protocol for the Internet Protocol Version 6 Specification*". O ICMPv6 é usado para relatar os erros encontrados no processamento dos pacotes e para mostrar outras funções da camada Internet, como diagnósticos e relato dos membros de endereços *multicast*. O ICMPv6 é parte integral do IPv6, sendo necessário ser implementado em todos os nodos IPv6 de uma rede. A transição do protocolo IPv4 para o IPv6 deverá ser de forma gradual para garantir a funcionalidade da rede. Foram criados dispositivos para que se possa fazer uma transição de modo que os dois protocolos de rede possam coexistir.

ABSTRACT

The exaggerating growth of the internet, took the great need of IP addresses, no foreseen by the creators of the access protocol, the problems that appeared, as the shortage of addresses and the non possibility of the implementation of necessary improvements for the evolution of the net, they took the a growth of the tables used for roteamento, what slow down and become inefficient the routing, forcing to create a new communication protocol (IPv6) to substitute and to supply all of the necessary implementations. IPv6 is a solution for this problem of shortage of addresses IP and it also provides new resources, such as the support to new net technologies (ATM, Gigabit Ethernet, among other), new format of the header, hierarchical infrastructure and routing efficiency and address, address configuration with or without state, safety built-in, better support for the quality of the services (QoS), new protocol for interaction among neighbors and extension capacity. With IPv6 there will be a new protocol of messages of control of Internet: ICMPv6. It is defined in RFC 2463, "Internet Control Message Protocol goes the Internet Protocol Version 6 Specification". ICMPv6 is used to tell the mistakes found in the processing of the packages and to show other functions of the layer Internet, as diagnoses and report of the members of addresses multicast. ICMPv6 is integral part of IPv6, being necessary to be implemented in all of the nodes IPv6 of a net. The transition of the protocol IPv4 for IPv6 should be in a gradual way to guarantee the functionality of the net. They had created devices that can make a transition so that the two protocols can coexist.

1. INTRODUÇÃO

O crescimento acelerado das tecnologias, o número crescente de serviços e o aumento vertiginoso do número de computadores ligados a Internet fez com que o protocolo atual de endereçamento não atendesse de maneira eficiente as necessidades de evolução que a rede necessita. Pensando nisso as pessoas responsáveis pela rede se viram obrigados a trabalhar na busca de alternativas que suprissem todas estas necessidades. Deste trabalho surgiu o IPv6 novo protocolo de endereçamento da Internet. O IPv6 vem trazendo grande expectativa quanto a sua eficiência e funcionalidade. Novos serviços e novas tecnologias tem sido implementadas para teste.

1.1.JUSTIFICATIVA

Percebendo a importância do assunto, da pouca literatura em português e da falta de material didático que auxiliem os acadêmicos nas pesquisas nesta área, fez-se necessário aprofundar o estudo sobre o protocolo IPV6, pois o mesmo está relacionado com um dos tópicos de grande importância do curso de Engenharia de Telecomunicações, a rede mundial de computadores – Internet.

Devido à obrigatoriedade de implantação do IPv6, é necessário conhecer os recursos, as características, vantagens e desvantagens desde protocolo, assim como de seu antecessor, para que possa ser feito um comparativo entre eles para entender todo o processo de migração do IPv4 para o IPv6.

Também se faz necessário o estudo do ICMPv6, para conhecer o sistema de controle de erros.

1.2.DEFINIÇÃO DO PROBLEMA

O maior problema encontrado foi a falta de literaturas em português, que não permitiu que algumas palavras ou títulos pudessem ser traduzidos, fazendo com que alguns deles fossem utilizados na língua inglesa.

1.3. OBJETIVOS

Realizar estudo do protocolo IPv6 e protocolo IPv4 com os seguintes objetivos específicos:

- estudar o protocolo IPv6 e compará-lo com o seu antecessor IPv4.
- vantagens e desvantagens em relação ao IPv4.
- estudar os protocolos de controle necessários ao IPv6 e compara-los com os equivalentes do IPv4.
- demonstrar como adquirir um endereçamento IPv6.

1.4. ESTRUTURA

Este trabalho está subdividido em capítulos que serão citados a seguir.

O primeiro capítulo apresenta a contextualização e a justificativa para o desenvolvimento da proposta do trabalho.

O segundo capítulo aborda a história da internet no Brasil e no mundo, seu crescimento e expectativas para seu futuro.

O terceiro capítulo trata do endereço IP sua definição, tipos e como adquirir.

O quarto capítulo descreve o protocolo TCP/IP e sua configuração.

O quinto capítulo apresenta o IPv4, sua especificação e endereçamento.

O sexto capítulo descreve o IPv6, mudanças em relação ao IPv4, endereçamento, tipos de endereços, roteamento, simplificação do formato de cabeçalho, suporte para campos opcionais, capacidade de identificação de fluxo e especificação.

O sétimo capítulo aborda o ICMP fazendo um comparativo entre o ICMPv4 e o ICMPv6.

O oitavo capítulo detalha a situação atual do IPV6.

O nono capítulo descreve como será feita a transição para o IPv6, estratégias de transição, ferramentas e sistemas que suportam este protocolo.

O décimo capítulo apresenta como adquirir endereços IPv6 através da solicitação de blocos.

O décimo primeiro apresenta a conclusão do trabalho.

2. INTERNET

Desenvolvida pela ARPA (*Advanced Research and Projects Agency*) em 1969, com o objetivo de conectar os departamentos de pesquisa, esta rede foi batizada com o nome de ARPANET. Antes da ARPANET já existia outra rede que ligava estes departamentos de pesquisa e as bases militares, mas como os EUA estavam em plena guerra fria, e toda a comunicação desta rede passava por um computador central que se encontrava no Pentágono, sua comunicação era extremamente vulnerável. Se a antiga URSS resolvesse cortar a comunicação da defesa americana, bastava lançar uma bomba no Pentágono e esta comunicação entrava em colapso, tornando os Estados Unidos extremamente vulnerável a mais ataques. A ARPANET foi desenvolvida exatamente para evitar isto. Com um *Back Bone* que passava por baixo da terra (o que o tornava mais difícil de ser interrompido), ela ligava os militares e pesquisadores sem ter um centro definido ou mesmo uma rota única para as informações, tornando-se quase indestrutível.

Na década de 70, as universidades e outras instituições que faziam trabalhos relativos à defesa tiveram permissão para se conectar à ARPANET e em 1975 já existiam aproximadamente 100 sites.

Os pesquisadores que mantinham a ARPANET estudaram como o crescimento alterou o modo como as pessoas usavam a rede. Anteriormente, os pesquisadores haviam presumido que manter a velocidade da ARPANET alta o suficiente seria o maior problema, mas na realidade a maior dificuldade se tornou a manutenção da comunicação entre os computadores (ou interoperação).

No final dos anos 70, a ARPANET tinha crescido tanto que o seu protocolo de comutação de pacotes original, chamado de *Network Control Protocol* (NCP), tornou-se inadequado.

Em um sistema de comutação de pacotes, os dados a serem comunicados são divididos em pequenas partes. Essas partes são identificadas de forma a mostrar de onde vieram e para onde devem ir, assim como os cartões-postais no sistema postal. Assim também como os cartões-postais, os pacotes possuem um tamanho máximo, e não são necessariamente confiáveis. Os pacotes são enviados de um computador para outro até alcançarem o seu destino. Se algum deles for perdido, ele poderá ser reenviado pelo emissor original. Para eliminar retransmissões desnecessárias, o destinatário confirma o recebimento dos pacotes.

Depois de algumas pesquisas, a ARPANET mudou do NCP para um novo protocolo chamado TCP/IP (*Transfer Control Protocol/Internet Protocol*) desenvolvido no UNIX. A maior vantagem do TCP/IP era que ele permitia (o que parecia ser na época) o crescimento praticamente ilimitado da rede, além de ser fácil de implementar em uma variedade de plataformas diferentes de hardware de computador.

> "No final da década de 80, a Internet era composta de aproximadamente 50.000 redes internacionais, sendo que mais ou menos a metade delas nos Estados Unidos. A partir de julho de 1995, havia mais de 6 milhões de computadores permanentemente conectados à Internet, além de muitos sistemas portáteis e de *desktop* que ficavam *online* por apenas alguns momentos." (BOGO, 2006, internet)

No final de 2005 o mundo chegou a 1 bilhão de usuários de internet, com aproximadamente 845 milhões de pessoas usando a *web* regularmente, de acordo com a pesquisa "Worldwide Online Access: 2004-2010", divulgada em 19/05/06 pela eMarketer.

Os Estados Unidos é o país com a maior população de internet, com 175 milhões de internautas, seguido pela China, com 111 milhões. De acordo com o eMarketer, os norte-americanos devem seguir na frente até o final da década.

Conforme IDG Now (2006), as conexões por banda larga cresceram de 142 milhões de casas em 2004 para 195 milhões em 2005. A região que apresenta a maior taxa de expansão no número de assinantes é a América Latina, com 70,7%. Ela é seguida pelo Leste Europeu, com 42,2%, e pela Ásia-Pacífico, 37,7%. Essa não é a primeira pesquisa a informar que a internet ultrapassou 1 bilhão de usuários. A Internet World Stats divulgou, no começo de 2006, que essa população havia sido alcançada, confirmando os dados agora da eMarketer.

2.1. INTERNET NO BRASIL

A história da Internet no Brasil começou bem mais tarde: só em 1991 com a RNP (Rede Nacional de Pesquisa), uma operação acadêmica subordinada ao MCT (Ministério de Ciência e Tecnologia). Até hoje a RNP é o "*backbone*" principal e envolve instituições e centros de pesquisa (FAPESP, FAPEPJ, FAPEMIG, etc.), universidades, laboratórios, etc.

Em 1994, no dia 20 de dezembro é que a EMBRATEL lança o serviço experimental a fim de conhecer melhor a Internet.

Somente em 1995 é que foi possível, pela iniciativa do Ministério das Telecomunicações e Ministério da Ciência e Tecnologia a abertura ao setor privado da Internet para exploração comercial da população brasileira.

"A RNP é responsável pela infra-estrutura básica de interconexão e informação em nível nacional, tendo controle do *backbone* (Coluna dorsal de uma rede, *backbone* representa a via principal de informações transferidas por uma rede, neste caso, a Internet)". (BOGO, 2006, internet).

O acesso à Internet pode ser feito do domicílio, local de trabalho, escola, centro de acesso gratuito ou pago, ou qualquer outro local.

Conforme TUDE (2006), o IBGE através do PNAD 2005 estimou que em 2005, 21% da população de 10 anos ou mais de idade acessaram a Internet, pelo menos uma vez, por meio de computador, em algum local nos 90 dias que antecederam à entrevista. Este percentual corresponde a uma população de 31.980 milhões de usuários em 2005.

2.1.1. Usuários Domiciliares de Internet

"O IBOPE/Net *ratings* acompanha o número de usuários domiciliares de Internet no Brasil. Segundo esta pesquisa em dezembro de 2005 existiam 18,9 milhões de usuários com acesso em suas residências, sendo que 12,2 milhões haviam efetivamente acessado a Internet em dezembro de 2005". (TUDE, 2006, internet).

Tabela 1 – Usuários Domiciliares de Internet no Brasil.

	Usuários 2005		Usuários 2006	
	Ativos	Com acesso	Ativos	Com acesso
Janeiro	10.656.901	17.945.437	12.035.681	21.227.222
Fevereiro	11.032.316		13.240.648	
Março	11.030.724		14.106.651	
Abril	11.378.029	18.336.044	13.431.424	21.227.222
Maio	11.517.361		13.246.186	
Junho	11.548.170		13.397.404	
Julho	11.434.547	18.336.044	13.392.663	21.241.295
Agosto	11.630.195		13.641.174	
Setembro	11.960.385			
Outubro	11.729.619	18.892.455		
Novembro	12.529.892			
Dezembro	12.208.375			

Fonte: TUDE, 25/09/06, internet.

Tabela 2 – Número de *Hosts* criados por ano.

Ano	2000	2001	2002	2003	2004	2005	Jul/06
Hosts (mil)	877	1.645	2.237,5	3.163,3	3.935	5.095	6.508

Fonte: TUDE, 25/09/06, internet.

Tabela 3 – Número de Domínios criados por ano.

Ano	2000	2001	2002	2003	2004	2005	1T06	2T06	Jul/06
Domínios	359,7	447,9	413,4	539,3	708,9	858,6	899	944,1	958,7

Fonte: TUDE, 25/09/06, internet.

O uso de computadores em rede e, claro, a internet, requer que cada máquina possua um identificador que a diferencie das demais.

É necessário que cada computador tenha um endereço, alguma forma de ser encontrado. Para isso, a tecnologia empregada na internet é o endereço IP.

3. ENDEREÇOS IP (INTERNET PROTOCOL)

O protocolo IP (*Internet Protocol*) trata-se de uma tecnologia que permite a comunicação padronizada entre computadores, mesmo que estes sejam de plataformas diferentes. A comunicação entre computadores é feita através do uso de padrões, ou seja, uma espécie de "idioma" que permite que todas as máquinas se entendam. Em outras palavras, é necessário fazer uso de um protocolo que indique como os computadores devem se comunicar. No caso do IP, o protocolo aplicado é o TCP/IP (*Transmission Control Protocol/Internet Protocol*). Existem outros, mas o TCP/IP é o mais conhecido, além de ser o protocolo usado na internet. O uso do protocolo TCP/IP não é completo se um endereço IP não for utilizado. Se, por exemplo, dados são enviados de um computador para outro, o primeiro precisa saber o endereço IP do destinatário e este precisa saber o IP do emissor, caso a comunicação exija uma resposta. Sem o endereço IP, os computadores não conseguem ser localizados em uma rede.

3.1. ANALISANDO O ENDEREÇO IP

O endereço IP é uma seqüência de números composta de 32 bits. Esse valor consiste num conjunto de quatro grupos de 8 bits. Cada conjunto é separado por um ponto e recebe o nome de octeto ou simplesmente byte, já que um byte é formado por 8 bits. O número 172.31.110.10 é um exemplo. Cada octeto pode ir de 0 a 255.

Como os endereços IP usados em redes locais são semelhantes aos IPs da internet, usa-se o padrão definido pelo IANA (*Internet Assigned Numbers Authority*) para a distribuição de endereços nestas redes. Assim, determinadas faixas de IP são usadas para redes locais, enquanto que outras são usadas na internet. Como uma rede local em um prédio não se comunica a uma rede local em outro lugar (a não ser que ambas sejam interconectadas) não há problemas de um mesmo endereço IP ser utilizado nas duas redes. Já na internet, isso não pode acontecer. Nela, cada computador precisa de um IP exclusivo. O padrão IANA divide a utilização de IPs para redes locais em 3 classes. Essa divisão foi feita de forma a evitar ao máximo o desperdício de IPs que podem ser utilizados em uma rede:

- Classe A: 10.0.0.0 a 10.255.255.255 - Permite até 16 milhões de computadores em cada rede local (máximo de 1 rede);
- Classe B: 172.16.0.0 a 172.31.255.255 - Permite até 65.534 computadores em uma rede local (máximo de 32 redes);
- Classe C: 192.168.0.0 a 192.168.255.255 - Permite até 254 computadores em uma rede local (máximo de 255 redes).

Os IPs são divididos em três classes básicas para atender as seguintes necessidades:

- os endereços IP da classe A são usados em locais onde é necessária uma rede apenas, mas uma grande quantidade de máquinas nela. Para isso, o primeiro byte é usado como identificador da rede e os demais servem como identificador dos computadores;
- os endereços IP da classe B são usados nos casos onde a quantidade de redes é equivalente ou semelhante à quantidade de computadores. Para isso, são usados os dois primeiros bytes do endereço IP para identificar a rede e os restantes para identificar os computadores;
- os endereços IP da classe C são usados em locais que requerem grande quantidade de redes, mas com poucas máquinas em cada uma. Assim, os três primeiros bytes são usados para identificar a rede e o último é utilizado para identificar as máquinas.

3.2. MÁSCARA DE SUB-REDE

A máscara de sub-rede (*subnet mask*) é que define quantos dos quatro números fazem parte da identificação da rede e quantos fazem parte da identificação da máquina. Seja o exemplo:

Número IP: 10.200.150.1
Sub-rede: 255.255.255.0

As três primeiras partes da máscara de sub-rede (subnet) iguais a 255 indicam que os três primeiros números representam à identificação da rede e o último número é a identificação do equipamento dentro da rede. Para o exemplo teríamos a rede: 10.200.150, ou

seja, todos os equipamentos do exemplo fazem parte da rede 10.200.150 ou, em outras palavras, o número IP de todos os equipamentos da rede começa com 10.200.150. Neste exemplo, são utilizados os três primeiros números para identificar a rede e somente o quarto número para identificar o equipamento, há um limite de 254 equipamentos que podem ser ligados nesta rede. São 254 e não 256, pois o primeiro número (10.200.150.0) e o último (10.200.250.255) não podem ser utilizados como números IP de equipamentos de rede. O primeiro é o próprio número da rede: 10.200.150.0 e o último é o endereço de Broadcast: 10.200.150.255. Ao enviar uma mensagem para o endereço de Broadcast, todas as máquinas da rede receberão a mensagem.

Conforme ALECRIM (2006), com base no exposto pode-se apresentar a seguinte definição: "Para se comunicar em uma rede baseada no protocolo TCP/IP, todo equipamento deve ter, pelo menos, um número IP e uma máscara de sub-rede, sendo que todos os equipamentos da rede devem ter a mesma máscara de sub-rede e pertencer ao mesmo endereço de rede. A tabela 4 mostra um exemplo de endereços com mascara de sub rede.

Tabela 4 – Endereços com máscara de sub rede.

Classe	Endereço IP	Identificador de rede	Ident. do computador	Máscara de sub-rede
A	10.2.68.12	10	2.68.12	255.0.0.0
B	172.31.101.25	1721.31	101.25	255.255.255.0
C	192.168.0.10	192.168.0	10	255.255.255.0

Fonte: ALECRIM, 10/08/06, internet.

3.3.OBTENDO UM ENDEREÇO IP

Os endereços IP usados nas placas de rede devem ser únicos, não devendo existir mais de uma placa com um mesmo endereço IP. Os endereços IP a serem usados em uma rede ligada à internet devem ser solicitados a uma instituição responsável pelo registro de endereços IP no país através de um formulário com as seguintes informações:

- Nome da organização que está solicitando os endereços;
- Nome da pessoa para contato;
- Localização geográfica;

- Número estimado de máquinas da rede;
- Finalidade da rede;

Caso não se pretenda ligar a rede à Internet, não é necessário solicitar endereços IP. Os endereços podem ser escolhidos a partir de faixas reservadas pela IANA. As redes que usam endereços nessas faixas são redes privadas e a numeração é chamada de numeração privada. A seguir as faixas reservadas:

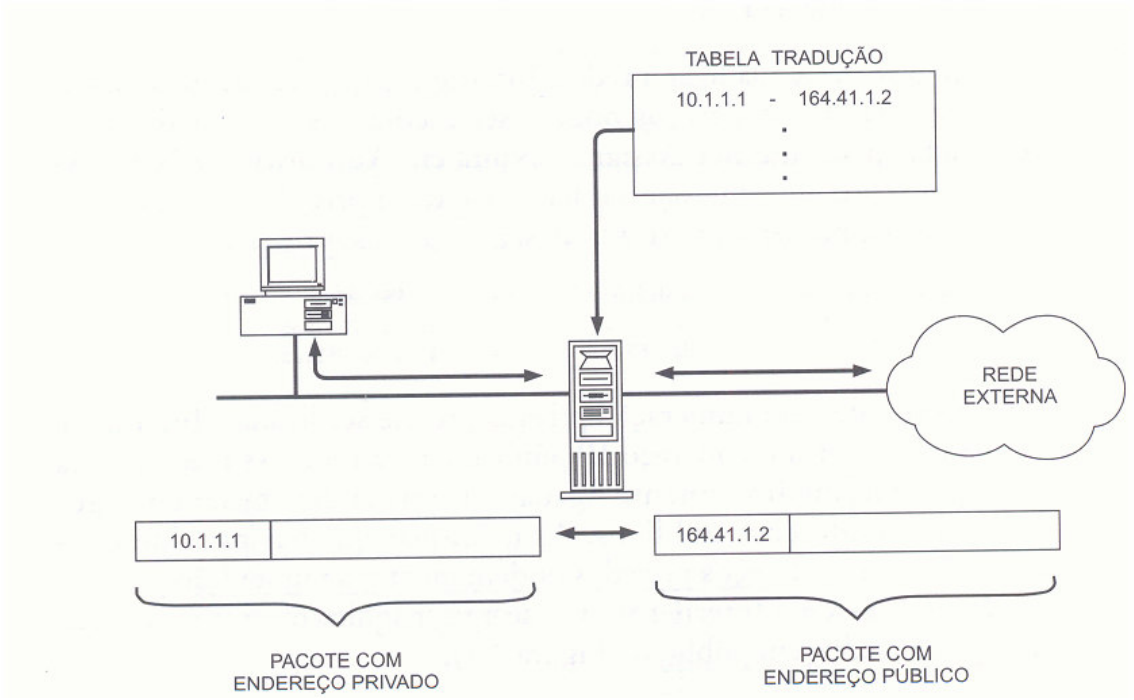
Tabela 5 – Faixas reservadas de Endereços.

Redes classe A	10.0.0.0	10.255.255.255
Redes classe B	172.16.0.0	172.31.255.255
Redes classe C	192.168.0.0	192.168.255.255

Fonte: ALECRIM, 10/08/06, internet.

Caso uma rede com numeração privada precise ser ligada à internet, é necessário obter um endereço IP publico para a rede. As máquinas da rede que estejam diretamente ligadas à internet devem ser configuradas com endereços públicos. As máquinas que haviam sido configuradas com endereços privados podem manter a numeração privada, desde que acessem a Internet através de uma máquina que traduza os endereços privados em públicos.

Figura 1 – Tradução de Endereços



Fonte: ALBUQUERQUE, 2001, p. 58

A tradução entre endereços públicos e privados pode ser estático ou dinâmico.

3.3.1. IP estático

IP estático (ou fixo) é um número IP dado permanentemente a um computador, ou seja, seu IP não muda, exceto se tal ação for feita manualmente. Como exemplo, há casos de assinaturas de acesso à internet via ADSL, onde alguns provedores atribuem um IP estático aos seus assinantes. Assim, sempre que um cliente se conectar, usará o mesmo IP. Essa prática é cada vez mais rara entre os provedores de acesso, por uma série de fatores, que inclui problemas de segurança.

3.3.2. IP dinâmico

O IP dinâmico, por sua vez, é um número que é dado a um computador quando este se conecta a rede, mas que muda toda vez que há conexão. Por exemplo, suponha que alguém conectou seu computador à internet hoje. Quando conectá-lo amanhã, lhe será dado outro IP. Para entender melhor, imagine a seguinte situação: uma empresa tem 80 computadores ligados em rede. Usando IPs dinâmicos, a empresa disponibilizou 90 endereços IP para tais máquinas. Como nenhum IP é fixo, quando um computador "entra" na rede, lhe é atribuído um IP destes 90 que não esteja sendo usado por nenhum outro computador. É assim que os provedores de internet trabalham. Toda vez que se conecta a internet, o provedor fornece um IP dela que esteja livre. O método mais usado para a distribuição de IPs dinâmicos é a protocolo DHCP (*Dynamic Host Configuration Protocol*).

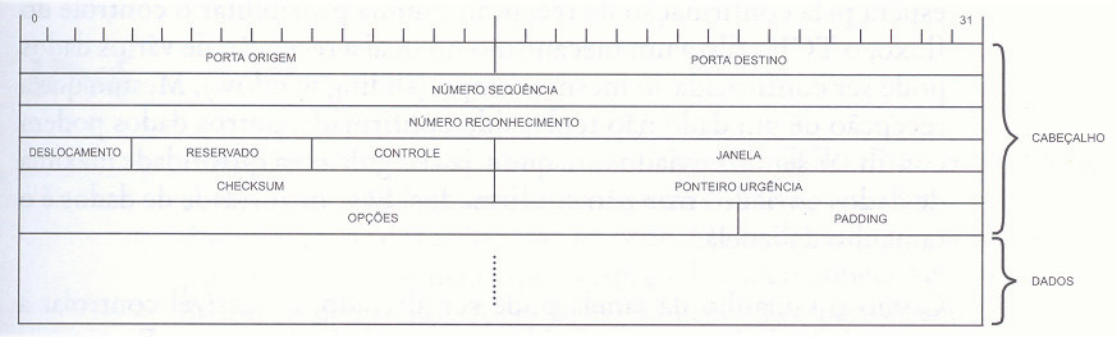
3.4.DOMÍNIO

Conforme ALECRIM (2006), o domínio consiste em uma forma mais fácil de acessar sites do que pelo seu IP. Esse recurso é como um "nome" dado ao IP. Sendo assim, quando se digita em um navegador "www.nomedosite.com.br", um servidor na internet chamado DNS (*Domain Name System* - Sistema de Nomes de Domínios) descobre qual o IP está relacionado ao site que se digitou e direciona o computador a ele. O sistema DNS possui uma hierarquia interessante, semelhante a uma árvore (termo conhecido por programadores). Se, por exemplo, o site www.fulano.com é requisitado, o sistema envia a solicitação a um servidor responsável por terminações".com". Esse servidor vai localizar qual o IP do endereço e responder à solicitação. Se o site solicitado termina com ".br", um servidor responsável por essa terminação é consultado. Assim, fica mais ágil a tarefa de localização de sites e dessa forma, a máquina consegue acessar praticamente qualquer site da internet.

4. TCP/IP

Para que os computadores de uma rede possam trocar informações é necessário que todos adotem as mesmas regras para o envio e o recebimento de informações. Este conjunto de regras é conhecido como Protocolo de comunicação. Falando de outra maneira pode-se afirmar: "Para que os computadores de uma rede possam trocar informações entre si é necessário que todos estejam utilizando o mesmo protocolo". No protocolo de comunicação estão definidas todas as regras necessárias para que o computador de destino "entenda" as informações no formato que foram enviadas pelo computador de origem. Dois computadores com protocolos diferentes instalados não serão capazes de estabelecer uma comunicação e trocar informações.

Figura 2 – Cabeçalho TCP



Fonte: ALBUQUERQUE, 2001, p 33.

Antes da popularização da Internet existiam diferentes protocolos sendo utilizados nas redes das empresas. Os mais utilizados eram os seguintes:

- TCP/IP
- NETBEUI
- IPX/SPX
- Apple Talk

À medida que a Internet cresceu e tornou-se mais popular, com o aumento exponencial do número de usuários, o protocolo TCP/IP passou a ser um padrão de fato, utilizado não só na Internet, como também nas redes internas das empresas, redes estas que

começavam a ser conectadas à Internet. Como as redes internas precisavam conectar-se à Internet, tinham que usar o mesmo protocolo da Internet, ou seja: TCP/IP.

Dos principais Sistemas Operacionais do mercado, o UNIX sempre utilizou o protocolo TCP/IP como padrão. O Windows dá suporte ao protocolo TCP/IP desde as primeiras versões, porém o TCP/IP somente tornou-se o protocolo padrão a partir do Windows 2000. Ser o protocolo padrão significa que o TCP/IP será instalado durante a instalação do Sistema Operacional, a não ser que um protocolo diferente seja selecionado. Até mesmo o Sistema Operacional Novell, que sempre foi baseado no IPX/SPX como protocolo padrão, passou a adotar o TCP/IP como padrão a partir da versão 5.0.

O que há hoje, na prática, é a utilização do protocolo TCP/IP na esmagadora maioria das redes. Sendo a sua adoção cada vez maior. Como não poderia deixar de ser, o TCP/IP é o protocolo padrão do Windows 2000 e também do Windows XP. Se durante a instalação, o Windows detectar a presença de uma placa de rede, automaticamente será sugerida a instalação do protocolo TCP/IP.

Para pequenas redes, não conectadas à Internet, é recomendada a adoção do protocolo NETBEUI, devido a sua simplicidade de configuração. Porém esta é uma situação muito rara, pois dificilmente haverá uma rede isolada, sem conexão com a Internet ou com parceiros de negócios, como clientes e fornecedores.

A arquitetura TCP/IP Internet é o resultado do desenvolvimento de uma filosofia de interligação de redes de computadores cuja característica mais relevante é a total transparência, aos seus usuários, dos detalhes relativos às tecnologias e à forma com a qual essa interligação é feita.

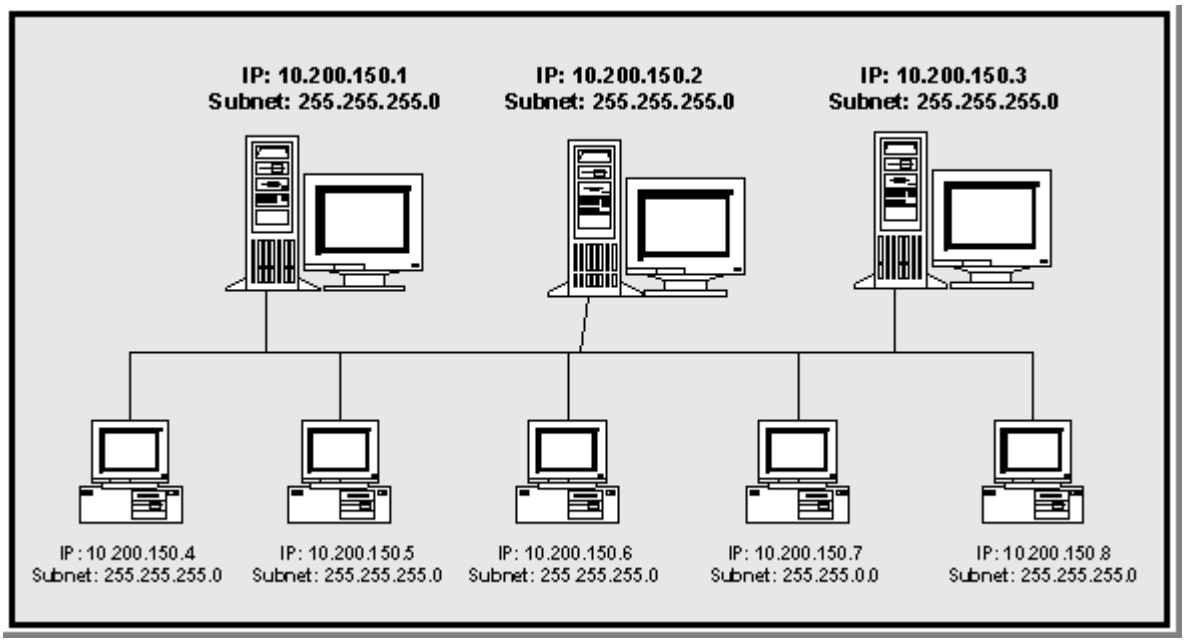
4.1 CONFIGURAÇÕES DO PROTOCOLO TCP/IP PARA UM COMPUTADOR EM REDE

Quando utilizado o protocolo TCP/IP como protocolo de comunicação em uma rede de computadores, há alguns parâmetros que devem ser configurados em todos os equipamentos (computadores, servidores, *hubs*, *switchs*, impressoras de rede, etc) que fazem parte da rede.

Na Figura 3 tem-se uma visão geral de uma pequena rede local não conectada a outras redes ou à Internet para uma pequena empresa baseada no protocolo TCP/IP. Neste caso cada computador da rede precisa de, pelo menos, dois parâmetros configurados:

- Endereço IP
- Máscara de sub-rede

Figura 3 – Rede baseada no protocolo TCP/IP.



Fonte: BATTISTI, 20/08/06, internet.

Caso seja configurado um novo equipamento com o mesmo número IP de uma máquina já existente será gerado um conflito de Número IP e um dos equipamentos, muito provavelmente o novo equipamento que está sendo configurado, não conseguirá se comunicar com a rede. O valor máximo para cada um dos números (que compreendem os 8 bits) é 255. Uma parte do Número IP (1, 2 ou 3 dos 4 números) é a identificação da rede, a outra parte é a identificação da máquina dentro da rede.

Existem configurações mais avançadas onde é possível subdividir uma rede TCP/IP em sub-redes menores. No exemplo da Figura 3 observa-se que o computador com o IP 10.200.150.7, está com uma máscara de sub-rede diferente dos demais: 255.255.0.0. Neste caso é como se o computador com o IP 10.200.150.7 pertencesse à outra rede. Na prática o que irá acontecer é que este computador não conseguirá se comunicar com os demais computadores da rede, por ter uma máscara de sub-rede diferente dos demais. Este é um dos erros de configuração mais comuns. Se a máscara de sub-rede estiver incorreta, ou seja, diferente da máscara dos demais computadores da rede, o computador com a máscara de sub-rede incorreta não conseguirá comunicar-se na rede.

Na Tabela 6 é apresentado alguns exemplos de máscaras de sub-rede e do número máximo de equipamentos em cada uma das respectivas redes.

Tabela 6 – Máscara de sub rede

Máscara	Número do Equipamento na Rede
255.255.255.0	254
255.255.0.0	65.534
255.0.0.0	16.777.214

Fonte: BATTISTI, 20/08/06, internet.

Quando a rede está isolada, ou seja, não está conectada à Internet ou a outras redes externas, através de links de comunicação de dados, apenas o número IP e a máscara de sub-rede são suficientes para que os computadores possam se comunicar e trocar informações. A conexão da rede local com outras redes é feita através de linhas de comunicação de dados. Para que essa comunicação seja possível é necessário um equipamento capaz de enviar informações para outras redes e receber informações destas redes. O equipamento utilizado para este fim é o Roteador. Todo pacote de informações que deve ser enviado para outras redes deve, obrigatoriamente, passar pelo Roteador. Todo pacote de informação que vem de outras redes também deve, obrigatoriamente, passar pelo Roteador. Como o Roteador é um equipamento de rede, este também terá um número IP. O número IP do roteador deve ser informado em todos os demais equipamentos que fazem parte da rede, para que estes equipamentos possam se comunicar com as redes externas. O número IP do Roteador é informado no parâmetro conhecido como *Default Gateway*. Na prática, quando é configurado o parâmetro *Default Gateway*, está se informando o número IP do Roteador.

Quando um computador da rede tenta se comunicar com outros computadores/servidores, o protocolo TCP/IP faz alguns cálculos utilizando o número IP do computador de origem, a máscara de sub-rede e o número IP do computador de destino. Se após feitas as contas, for concluído que os dois computadores fazem parte da mesma rede, os pacotes de informação são enviados para o barramento da rede local e o computador de destino captura e processa as informações que lhe foram enviadas. Se após feitas as contas, for concluído que o computador de origem e o computador de destino fazem parte de redes diferentes, os pacotes de informação são enviados para o Roteador (número IP configurado como *Default Gateway*) e o Roteador é o responsável por achar o caminho (a rota) para a rede

de destino. Com isso, para equipamentos que fazem parte de uma rede, baseada no protocolo TCP/IP e conectada a outras redes ou a Internet, deve-se configurar, no mínimo, os seguintes parâmetros:

- Endereço IP
- Máscara de sub-rede
- *Default Gateway*

Em redes empresarias existem outros parâmetros que precisam ser configurados. Um dos parâmetros que deve ser informado é o número IP de um ou mais servidores DNS – *Domain Name System*. O DNS é o serviço responsável pela resolução de nomes.

Toda a comunicação, em redes baseadas no protocolo TCP/IP é feita através do número IP. Por exemplo, como visto anteriormente, quando se acessa o site: www.furb.br, tem que haver uma maneira de encontrar o número IP do servidor onde fica hospedado o site. O serviço que localiza o número IP associado a um nome é o DNS. Por isso a necessidade de se informar o número IP de pelo menos um servidor DNS, pois sem este serviço de resolução de nomes, muitos recursos da rede estarão indisponíveis.

Existem outros aplicativos que são baseados em um outro serviço de resolução de nomes conhecido como WINS – *Windows Internet Name System*. O Windows NT Server 4.0 utilizava intensamente o serviço WINS para a resolução de nomes. Com o Windows 2000 o serviço utilizado é o DNS, porém podem existir aplicações que ainda dependam do WINS. Nestes casos terá de ser instalado e configurado um servidor WINS na rede e configurado o IP deste servidor em todos os equipamentos da rede.

Conforme BATTISTI (2006), as configurações do protocolo TCP/IP podem ser definidas manualmente, isto é, configurando cada um dos equipamentos necessários. Esta é uma solução razoável para pequenas redes, porém pode ser um problema para redes maiores, com um grande número de equipamentos conectados. Para redes maiores é recomendado o uso do serviço DHCP – *Dynamic Host Configuration Protocol*. O serviço DHCP pode ser instalado em um servidor com o Windows NT Server 4.0 ou o Windows 2000 Server. Uma vez disponível e configurado, o serviço DHCP fornece todos os parâmetros de configuração do protocolo TCP/IP para os equipamentos conectados à rede. Os parâmetros são fornecidos quando o equipamento é inicializado e podem ser renovados em períodos definidos pelo Administrador. Com o uso do DHCP uma série de procedimentos de configuração podem ser automatizados o que facilita a vida do Administrador e elimina uma série de erros. O uso do

DHCP também é muito vantajoso quando são necessárias alterações no número IP dos servidores DNS ou WINS. Vamos imaginar uma rede com 1000 computadores e que não utiliza o DHCP, ou seja, os diversos parâmetros do protocolo TCP/IP são configurados manualmente em cada computador. Agora vamos imaginar que o número IP do servidor DNS foi alterado. Neste caso o Administrador e a sua equipe técnica terão que fazer a alteração do número IP do servidor DNS em todas as estações de trabalho da rede. Um serviço e tanto. Se esta mesma rede estiver utilizando o serviço DHCP, bastará alterar o número do servidor DNS, nas configurações do servidor DHCP. O novo número será fornecido para todas as estações da rede, na próxima vez que a estação for reinicializada. Muito mais simples e prático e, principalmente, com menor probabilidade de erros.

5. IPv4

5.1.INTRODUÇÃO AO IPv4

Embora o IP seja o protocolo de rede mais conhecido, deve ser mencionado que a idéia de se transmitir mensagens por uma rede persegue o homem a milhares de anos. Deixando lendas de lado e atendo-se aos fatos históricos, por volta de 700 aC, já eram utilizados pombos para se transmitir mensagens na Grécia antiga. As comunicações evoluíram muito desde então.

Em 1957, os russos colocaram em órbita o Sputnik, o primeiro satélite artificial, ganhando uma corrida espacial contra os americanos. Como resposta, em 7 de fevereiro de 1958 o Departamento de Defesa dos Estados Unidos (*Department of Defense* – DoD), através da Diretiva 5105.15, decidiu criar a *(Defense) Advanced Research Projects Agency* DARPA – Agência de Pesquisas de Projetos Avançados de Defesa). A DARPA tinha como missão garantir que os Estados Unidos estivessem sempre na dianteira tecnológica militar e antecipar quais seriam os avanços tecnológicos dos "adversários".

Com o passar dos anos, a DARPA teve a necessidade de criar um protocolo de comunicação por comutação de pacotes capaz de interconectar computadores heterogêneos. Então, a DARPA lançou uma licitação para o projeto de um hardware que eles chamaram de "Interface Message Processor" (IMP – Processador de Mensagens de Interface), que deveria ser o nó de comutação de pacotes. Empresas como IBM e AT&T achavam que não era possível realizar tal tarefa. Então, uma pequena empresa, formada por dois professores de Cambridge e um ex-aluno de um deles, chamados Bolt, Beranek e Newman, respectivamente, venceu a concorrência para desenvolver tal tecnologia. A empresa é a renomada Bolt, Beranek & Newman, também conhecida como BBN.

Em 7 de abril de 1969, Steve Crocker criou o primeiro *Request for Comments* (RFC) 1 – *Host Software* – Requisitando Comentários 1 – Software de Host), identificando como deveria ser o software de um host em uma rede, no caso, o software do IMP. A BBN trabalhando em conjunto com o *Information Processing Techniques Office* (Escritório de Técnicas de Processamento de Informação) da DARPA desenvolveu a primeira IMP da ARPANET, entregue em 1971, implementado em um minicomputador da Honeywell.

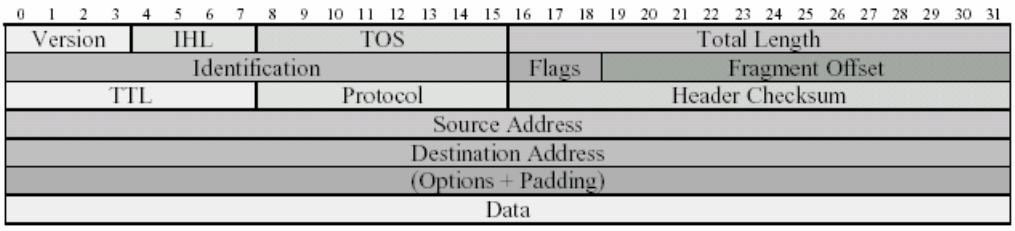
Em maio de 1974, Vint Cerf e Bob Kahn publicaram um *paper* chamado “A Protocol for Packet Network Internetworking” (Um Protocolo para Comunicação entre Redes de Pacotes), que estabelecia o TCP (*Transmission Control Protocol* – Protocolo de Controle de Transmissão). Foi a primeira vez que o termo Internet foi utilizado.

Em 1978, quando Vint Cerf, Steve Crocker e Danny Cohen decidiram passar as funções de roteamento do TCP para um protocolo separado, surgiu o IP. O TCP continuaria com as funções de correção de erro e funções de datagrama. A especificação do IPv4 foi publicada em setembro de 1981, sob o RFC 791, com o auxílio do *Information Sciences Institute – University of Southern California* (Instituto de Ciências da Informação da Universidade do Sul da Califórnia). Em 1982 o TCP e o IP foram adotados como os protocolos oficiais da ARPANET. A popularização do IP veio quando ele passou a ser distribuído pelo Berkeley Software Distribution UNIX (BSD UNIX), versão 4.2c, em 1983.

5.2.ESPECIFICAÇÃO DO IPv4

O Cabeçalho de especificação do IPv4 está representado na Figura 12 (as escalas superiores horizontais se referem a bits).

Figura 4 – Especificação do IPv4 (RFC 791).



Fonte: SMETANA, 17/09/06, internet.

5.2.1. Tradução dos campos:

- Version (Versão): 4 bits. A versão atual é a 4.

- IHL (Internet Header Length – Comprimento do Cabeçalho Internet): 4 bits. Informa o comprimento do cabeçalho Internet em palavras de 32 bits (4 octetos ou 4 bytes). O tamanho mínimo do cabeçalho é de 5 palavras de 32 bits (20 octetos), e o tamanho máximo (o campo Option + Padding tem tamanho variável) é de 15 palavras de 32 bits (60 octetos). Aponta para o campo de dados.

- TOS (Type of Service – Tipo de Serviço): 8 bits. É utilizado para indicar o QoS (*Quality of Service* – Qualidade de Serviço) desejado. Seus bits caracterizam os serviços escolhidos para serem considerados pelos gateways para processar o pacote, como por exemplo, a precedência de um pacote. Um roteador (pode ser chamado de gateway) pode em situações de grande congestionamento, por exemplo, aceitar somente pacotes com um certo nível mínimo de precedência. Geralmente, deseja-se baixo atraso, alta confiabilidade e alto *throughput* (vazão).

Figura 5 – Subdivisão do campo TOS.

Fonte: SMETANA, 17/09/06, internet.

Abaixo temos os significados dos campos da tabela TOS demonstrados na Figura 6.

Figura 6 – Significado do campo TOS

Bits	Descrição	Valores	
0 1 2	Precedence (Precedência)	000: Routine (Rotina) 001: Priority (Prioridade) 010: Immediate (Imediato) 011: Flash ("Relâmpago")	100: Flash Override ("Relâmpago" Precedente) 101: Critic/ECP (Crítico) 110: Internetwork Control (Controle entre Redes) 111: Network Control (Controle de Rede)
3	D (Delay – Atraso)	0: Atraso normal. 1: Atraso baixo.	
4	T (Throughput – Vazão)	0: Vazão normal. 1: Alta vazão.	
5	R (Relibility – Confiabilidade)	0: Confiabilidade normal. 1: Alta confiabilidade.	
6 7	Reservados	Obrigatoriamente 00.	

Fonte: SMETANA, 17/09/06, internet.

O nível de precedência é crescente.

Tradução dos campos:

- Total Length (Comprimento Total): 16 bits. Informa o comprimento do datagrama, em octetos (bytes). O tamanho máximo do datagrama pode ser 65.535 octetos (64 kB). Esse tamanho de octeto é impraticável para a maior parte de hosts e redes. Todos os hosts devem ser capazes de no mínimo aceitar datagramas de até 576 octetos, fragmentados ou não. Esse número foi determinado, partindo-se do pressuposto que 512 octetos seria um número razoável de dados a ser enviado, considerando-se mais 64 bytes de cabeçalho, sendo que o tamanho máximo do cabeçalho Internet é de 60 octetos, mas o tamanho típico é de 20 octetos, dando-se margem para cabeçalhos de outras camadas. Recomenda-se que os hosts só enviem datagramas maiores que 576 bytes se houver a certeza que o endereço destino aceita receber a quantidade de dados enviados.

- Identification (Identificação): 16 bits. Número de identificação do datagrama para permitir que o destino remonte os datagramas.

- Flags (Sinalizadores): 3 bits. Bits que identificam a transmissão de sinais de controle.

Figura 7 – Subdivisão do campo Flags.

Fonte: SMETANA, 17/09/06, internet.

Abaixo temos o cabeçalho de Significado dos bits do campo Flags.

Figura 8 – Significado dos bits do campo Flags.

Bit	Descrição	Valores
0	Reservado	Obrigatoriamente 0.
1	DF (Don't Fragment – Não Fragmente)	0: Esse datagrama pode ser fragmentado. 1: Esse datagrama não pode ser fragmentado.
2	MF (More Fragments – Mais Fragmentos)	0: Esse datagrama é o último fragmento. 1: Há mais fragmentos.

Fonte: SMETANA, 17/09/06, internet.

Tradução dos campos:

- Fragment Offset (Deslocamento do Fragmento): 13 bits. Esse campo indica a posição desse fragmento em relação ao do datagrama original. O valor desse campo é expresso em unidades de 8 octetos (64 bits), portanto o tamanho mínimo do campo de dados de um fragmento é de 64 bits. O primeiro fragmento tem valor 0 (zero) nesse campo.

- TTL (Time to Live – Tempo de Vida): 8 bits. Indica o tempo máximo que o datagrama pode permanecer na rede. Se o valor nesse campo for 0 (zero), o datagrama deve ser destruído. A intenção desse campo é não permitir que datagramas cujo destino seja inalcançável fiquem eternamente circulando pela rede. Inicialmente, a unidade do TTL era segundos mas como cada unidade processadora de datagramas (roteadores, switches de camada 3, etc.) deve diminuir o TTL de uma unidade e o tempo de processamento de pacotes é muito inferior a 1 segundo, o TTL passa a ser somente um limite superior da existência de cada datagrama.

- Protocol (Protocolo): 8 bits. Indica o protocolo da camada superior que está utilizando os serviços da camada IP. Esses valores estão definidos no RFC 790 – Assigned Network Numbers (Números de Redes Designados) de 1981. Esse RFC foi substituído pelo RFC 1700 – Assigned Numbers. O número do TCP, por exemplo, é 6. Quando o IP estiver encapsulado em outra camada IP, como em uma Virtual Private Network, por exemplo, o valor desse campo é 4.

- Header Checksum (Verificação da Soma do Cabeçalho): 16 bits. Esse checksum é calculado somente sobre o cabeçalho IP. Como alguns campos mudam freqüentemente, como o TTL, esse valor tem que ser recalculado. Para se calcular esse checksum, faz-se o complemento de um de cada palavra de 16 bits do cabeçalho, soma-se elas e faz-se o complemento de um da soma total (para efeitos de cálculo, o campo Header Checksum vale 0 (zero)). Embora esse algoritmo seja simples, ele é suficiente e seguro para a maioria das situações.

- Source Address (Endereço de Origem): 32 bits. Informa o endereço de origem.

- Destination Address (Endereço de Destino): 32 bits. Informa o endereço de destino. Essa informação é utilizada pelos roteadores para o encaminhamento (roteamento) do datagrama. Alguns equipamentos podem utilizar os campos IP de origem, de destino e até mesmo informações de protocolos de níveis superiores e o tipo de dado sendo transmitido para realizar o roteamento de pacotes e juntamente realizar algum tipo de priorização ou QoS.

- Options (Opções): Tamanho variável, entre 0 (zero) e 320 bits (40 octetos). O que é opcional é a transmissão ou não desse campo, não a implementação. Todo os roteadores e gateways devem implementar meios de codificação/decodificação desse campo. Pode haver mais de uma opção nesse campo. As opções servem, entre outras coisas, informar se o próprio campo Option deve ou não ser copiado para os fragmentos, caso o pacote venha a ser fragmentado, para embutir um timestamp da rede, adicionar informações relativas ao nível de segurança do pacote (confidencialidade) ou para especificar uma rota para um determinado destino. Mais informações sobre esse campo podem ser encontradas no RFC 791.

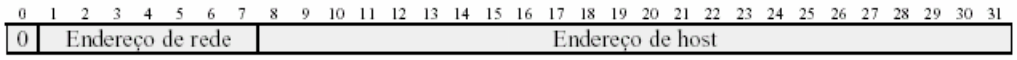
- Padding (Enchimento): Tamanho variável, entre 0 (zero) e 31 bits. O campo Padding serve apenas para que o cabeçalho IP tenha um tamanho múltiplo de 32 bits. Só se faz o enchimento (obrigatoriamente com 0 (zero)), se o tamanho do campo Option não for múltiplo de 32 bits.

5.3.O ENDEREÇAMENTO NO IPv4

Os 32 bits de endereçamento do IPv4 estão separados em duas partes, sendo que a primeira informa o endereço de rede e a segunda, o endereço de host. A representação do endereço IPv4 é feita através da chamada notação decimal pontuada. Nela, cada um dos quatro bytes do endereço IPv4 é representado pelo seu valor decimal separados por um “.”. Originalmente, foram definidas 3 classes de endereço, identificadas pelo valor dos primeiros bits do endereço de rede, para atender às necessidades de redes de diferentes tamanhos. A figura 9 mostra essa divisão.

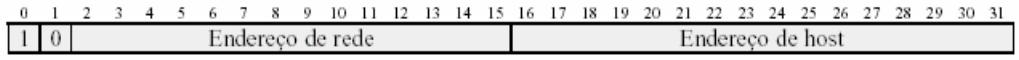
- Classe A: 0.0.0.0 a 127.255.255.255

Aplicação: Para as poucas organizações que possuem redes com número muito grande de hosts.



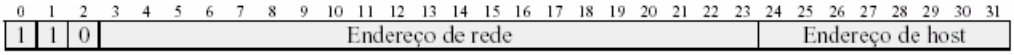
- Classe B: 128.0.0.0 a 191.255.255.255

Aplicação: Para organizações de tamanho médio, com número relativamente grande de hosts.



- Classe C: 192.0.0.0 a 223.255.255.255

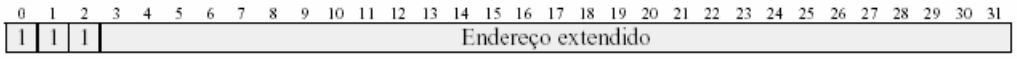
Aplicação: Para organizações pequenas, com número pequeno de hosts.



- Modo de endereçamento estendido: 224.0.0.0 a 255.255.255.255

Aplicação: Uso experimental.

Figura 9 – Formato original dos endereços, suas classes e as faixas de endereços.

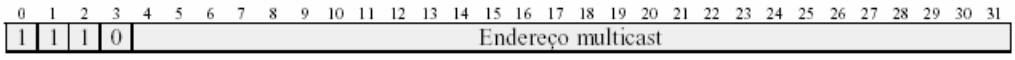


Fonte: SMETANA, 17/09/06, internet.

Depois, foram definidas mais 2 classes de endereços:

- Classe D: 224.0.0.0 a 239.255.255.255

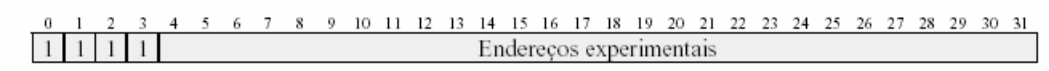
Aplicação: Transmissão de tráfego multicast.



- Classe E: 240.0.0.0 a 255.255.255.255

  Aplicação: Uso experimental.

Figura 10 – Classes de endereço adicionais.



Fonte: SMETANA, 17/09/06, internet.

Tabela 7 – Endereços IPv4 reservados e as faixas de endereços utilizáveis.

Classe	Faixa de endereços	Utilização
A	0.0.0.0 a 0.255.255.255	Não utilizável.
A	10.0.0.0 a 10.255.255.255	Endereço de rede reservado para uso em redes privadas.
A	127.0.0.0 a 127.255.255.255	Não utilizável. Loopback para teste de interfaces.
A	Demais faixas de endereços	Utilizáveis comercialmente.
B	172.16.0.0 a 172.31.255.255	Endereço de rede reservado para uso em redes privadas.
B	Demais faixas de endereços	Utilizáveis comercialmente.
C	192.168.0.0 a 192.168.255.255	Endereço de rede reservado para uso em redes privadas.
C	Demais faixas de endereços	Utilizáveis comercialmente.

Fonte: SMETANA, 17/09/06, internet.

Os endereços de rede reservados para redes privadas estão especificado no RFC 1918 – *Address Allocation for Private Internets* (Alocação de Endereços para Redes Privadas) e foram criados para resolver o problema de endereçamento do IPv4. Assim, uma empresa com um número muito grande de hosts, não precisa receber um endereço classe A da IANA (*Internet Assigned Numbers Authorithy* – Autoridade da Internet dos Números Designados). Ela pode receber qualquer endereço e internamente, utilizar o endereço privado classe A, usando NAT (*Network Address Translation* – Tradução de Endereço de Rede).

Conforme SMETANA (2006), com a publicação do RFC 1518 - Classless Inter-Domain Routing (CIDR) Address Allocation Architecture (Alocação de Endereço para Roteamento Inter-Domínio sem Classe) e do RFC 1519 – Classless Inter-Domain Routing (CIDR – Roteamento Inter-Domínio sem Classe) em setembro de 1993, o endereçamento IPv4 ganhou maior flexibilidade, devido ao uso de máscaras para se criar sub-redes, fazendo com que o endereço de rede não fosse mais expresso somente através dos 8, 16 ou 24 primeiros bits do endereço IPv4. Desde então, o endereço de rede pode ter tamanho variado, de acordo com a necessidade de cada organização.

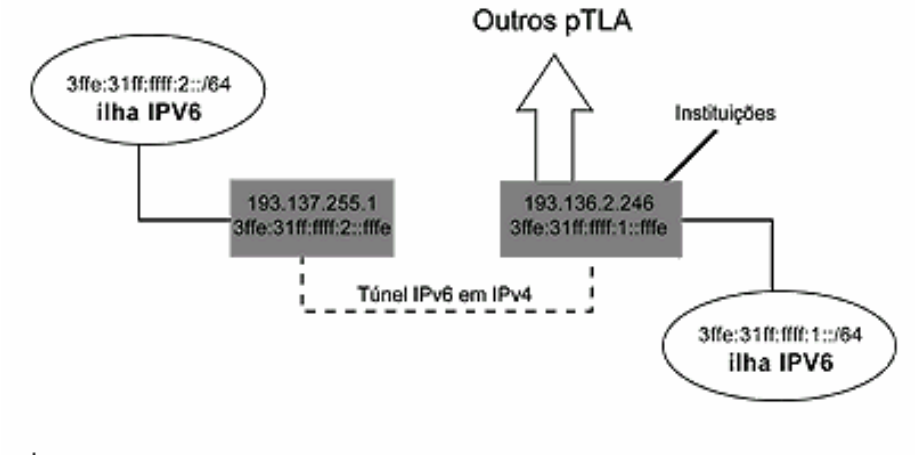
6. IPv6

6.1.INTRODUÇÃO AO PROTOCOLO IPv6

Com a explosão da Internet e com o surgimento constante de mais e mais serviços e aplicações, os atuais endereços IP (IPv4) estão se tornando um recurso escasso. Para solucionar este problema, o IPNGWG (*IP Next Generation Working Group*) da IETF (*Internet Engineering Task Force*), publicou uma série de RFCs descrevendo o protocolo IPv6.

"Em Junho de 1992, acontecia um dos encontros do IAB (*Internet Activities Board*) em paralelo ao congresso da Internet Society. Durante o encontro propuseram, e conseguiram convencer o IAB da adoção do CLNP (Connection-Less Network Protocol) da ISO, como sucessor do IPv4". (NUNES, 2006, internet).

Figura 11 – Esquema da Rede Ipv6



Fonte: FCCN, 27/09/06, internet.

Na Figura 11 temos um exemplo de uma rede Ipv6 sobre a estrutura física de uma rede IPv4.

Com um "*draft*" discutido e revisado, o IAB estava pronto para convencer a comunidade Internet, quando um precipitado anúncio em jornal causou o maior rebuliço, e com isso os membros da comunidade se sentiram traídos.

Achava-se, então, que estavam "vendendo" a Internet para a ISO, uma "inimiga" contra a qual se tinha lutado por vários anos e que já estava vencida, e que o IAB não tinha o direito de tomar essa decisão sozinho.

No mesmo encontro, surgiram três propostas:

- CLNP, que foi chamada de TUBA (TCP and UDP over Bigger Address).

- Uma denominada IP versão 7, de Robert Ullman que, em 1993, propôs outra versão chamada TP/IX e em 1994, propôs uma nova versão chamada CATNIP, como ensaio para compatibilidade entre endereços IP, CLNP e IPX.

- "IP in IP". Em 1993, esta proposta foi modificada e passou a se chamar IPAE (IP Address Encapsulation). O IPAE foi adotado como estratégia de transição para o SIP (Simple IP), proposto por Steve Deering em Novembro de 1992.

- SIP - aumentava o endereço IP para 64 bits, tornava a fragmentação de pacotes opcional e eliminava vários aspectos obsoletos do IP.

Setembro de 1993, Paul Francis propôs uma nova especificação, o Pip (Paul's internet protocol). Propôs uma nova estratégia de roteamento baseada em listas diretivas. Isso permitiria uma implementação eficiente de políticas de roteamento, facilitando, inclusive, a implementação de mobilidade. A união do SIP com o Pip foi chamada de SIPP (Simple IP Plus).

> Em Junho de 1994, a comissão do IPng revisou todas as propostas e publicou sua recomendação. Sugeriu o SIPP como a base para o novo protocolo IP. O novo protocolo teria endereços de 128 bits e se chamaria IPv6. O número 5 havia sido alocado ao protocolo ST (stream), um protocolo experimental para suportar serviços em tempo real em paralelo com o IP. (NUNES, 2006, internet).

Foram considerados os desejos das empresas por redes com arquiteturas mais escaláveis, maior segurança e integridade dos dados, extensões à QoS, autoconfiguração, maior agregação no nível do backbone global e outras necessidades.

Conforme SMETANA (2006), apesar de haver vários backbones com IPv6 em caráter experimental, como o 6Bone, que é o backbone IPv6 do projeto IPng (Internet Protocol Next Generation – Próxima Geração do Internet Protocol) da IETF (Internet Engineering Task Force – Força Tarefa de Engenharia da Internet), a previsão para o início de operação comercial do IPv6 é 2010. Por uns 5 anos, os equipamentos deverão oferecer compatibilidade entre IPv6 e IPv4, seja por encapsulamento, tunelamento, algum protocolo de roteamento capaz de lidar com ambas as versões ou alguma outra técnica. Porém, a migração não será algo simples. Há um grupo de trabalho do IETF, o IPng Transition (ou simplesmente "ngtrans"), exclusivamente ocupado para levantar os problemas e soluções para essa migração.

6.2.MUDANÇAS EM RELAÇÃO AO IPv4

Segundo TAMUSIUNAS (2006), comparando-se o formato do IPv6 com o do IPv4, os mecanismos de opções foram completamente revisados, seis campos foram suprimidos (header length, type of service, identification, flags, fragment offset e header checksum), três foram renomeados e, em alguns casos, ligeiramente modificados (length, protocol type e time to leave), e dois foram criados (trafic class e flow label).

Conforme NUNES (2006), o atual endereço de 32 foi ampliado para 128 bits, acabando definitivamente com as classes de endereços e possibilitando um método mais simples de autoconfiguração. As simplificações mais consideráveis do IPv6 foram a alocação de um formato fixo para todos os cabeçalhos, a remoção do check-sum de cabeçalho e a remoção dos procedimentos de segmentação "hop-by-hop".

A remoção de todos os elementos opcionais não significa que não se possa configurar serviços especiais. Estes poderão ser obtidos através de cabeçalhos denominados "Cabeçalhos de Extensão", que são anexados ao cabeçalho principal. A remoção do check-sum poderia gerar problemas no roteamento dos pacotes, mas o IPv6 pressupõe que as camadas inferiores são confiáveis, com seus respectivos controles de erro como, por exemplo, o 802.2 LLC (*Logical Link Control*) para redes locais, o controle das camadas de adaptação dos circuitos ATM e o controle do PPP para links seriais.

A cada salto de um pacote IPv6, os roteadores não precisarão se preocupar com o cálculo do tamanho do cabeçalho, e nem com as tabelas de fragmentação, que serão realizadas

pelos hosts. Todas estas modificações aumentam substancialmente o desempenho dos roteadores, permitindo melhor desempenho para redes de alta velocidade.

Conforme TAMUSIUNAS (2006), novos recursos para permitir maior segurança na rede foram descritos, assim como uma nova estrutura interna de endereçamento, podendo agora os endereços terem campos em seu conteúdo. Este novo tipo de estrutura afeta de forma direta os novos tipos de roteamento. A tabela a seguir, conforme citada em www.cisco.com.br/ipv6, mostra um quadro comparativo entre os dois protocolos.

Figura 12 – Comparativo entre IPv4 e IPv6

Tipo de Serviço IP	Solução IPv4	Solução IPv6
Segurança	IPSec Disponível	IPSec Obrigatório
Auto-configuração	DHCP para Hosts; Futura Renumeração a Nível de Site	Serverless ou DHCP, Renumeração a Nível de Site
Escalabilidade	Roteamento Hierárquico	Roteamento Hierárquico
Mobilidade	IP Móvel	IP Móvel
IP Multicast	Multicast BGP	Identificador de abrangência, Multicast BGP
Faixa de Endereçamento	32 bits de endereçamento, Tradução de Endereço de Rede (NAT)	128 bits de endereçamento

Fonte: TAMUSIUNAS, 19/09/06, internet.

Há 3 formas de representação do endereço IPv6:

- A notação mais usual é x:x:x:x:x:x:x:x, onde os "x" são números hexadecimais, ou seja, o endereço é dividido em oito partes de 16 bits, como no seguinte exemplo: 1080:0:0:0:8:800:200C:417
- Seqüências de zeros podem ser substituídas pela string "::".
- Esta substituição só pode ser feita uma única vez em cada endereço.

Tabela 8 – Exemplos na forma completa e na forma abreviada de Endereços Ipv6.

Endereço	Forma Completa	Forma Abreviada
Unicast	1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A
Multicast	FF01:0:0:0:0:0:0:43	FF01::43
Loopback	0:0:0:0:0:0:0:1	::1
Unspecified	0:0:0:0:0:0:0:0	::

Fonte: NUNES, 17/09/06, internet.

Conforme BERNAL FILHO (2006), em ambientes mistos com nodos IPv4 e IPv6, é da forma x:x:x:x:x:x:d.d.d.d,

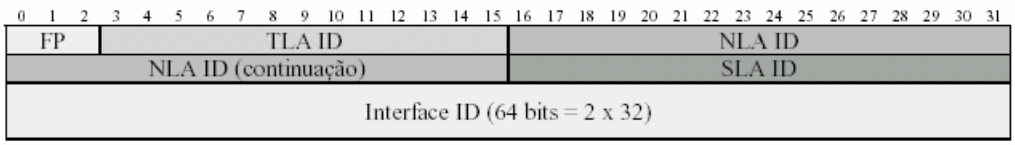
- "x" - são números hexadecimais (16 bits)
- "d" - são valores decimais de 8 bits referentes à representação padrão já bem conhecida do IPv4.

Por exemplo: 0:0:0:0:0:0:192.168.20.30 ou, na forma abreviada: ::192.168.20.30.

6.3. O ENDEREÇAMENTO NO IPv6

> "Em sua reunião de 7 de setembro de 2006, a Diretoria da ICANN ratificou uma política global para que Autoridades para Atribuição de Números na Internet (IANA) possam alocar os endereços IPv6 aos Registros Regionais da Internet", mas como ainda não encontra-se documentos disponíveis analisou-se a RFC 2471 – IPv6 *Testing Address Alocation* (Teste de Alocação de Endereço do IPv6), uma proposta que é a base desta nova política adotada pela IANA, mostrada na figura 13. Embora seja experimental e esteja servindo para testes de implementações do IPv6, ela segue as recomendações definidas para a arquitetura IPv6 e o seu formato é consistente com o *Aggregatable Global Unicast Address Allocation* (Alocação Global Agregável de Endereço Unicast) e com o *Top-Level Aggregation and Next-Level Aggregation Assignment Rules* (Regras de Designação de Agregação *Top-Level* e Agregação *Next-Level*). O endereço IPv6 pode ser definido manualmente, por IPv6 *Auto Address Allocation* (Alocação Automática de Endereço IPv6) ou por DHCPv6 (*Dynamic Host Configuration Protocol* – Protocolo Dinâmico de Configuração de Host). (SMETANA, 2006, internet).

Figura 13 – Proposta do formato do endereçamento IPv6.



Fonte: SMETANA, 17/09/06, internet.

- FP (Format Prefix – Formato do Prefixo): 3 bits. Valor atual binário é 001. Esse valor é utilizado para identificar endereços unicast globais agregáveis.

- TLA ID (Top-Level Aggregation Identifier – Identificador da Agregação Top-Level): 13 bits.O valor desse campo é 0x1FFE e foi designado pela IANA para uso temporário pelo 6bone da IETF. No futuro, todos os usuários desse TLA ID terão que mudá-lo.

- NLA ID (Next-Level Aggregation Identifier – Identificador da Agregação Next-Level): 32 bits. Esse número será designado pelo administrador do NLA ID, em uma hierarquia de endereços suficiente para identificar redes de transitação e sites de usuários finais, de forma consistente com a topologia e arquitetura do 6bone. Isso deverá ser feito para a criação de um serviço de transitação multi-level consistente com os testes de situações de uso real do IPv6 no 6bone.

- SLA ID (Site-Level Aggregation Identifier – Identificador da Agregação Site-Level): 16 bits. Esse número deve ser utilizado por cada organização para criar sua própria hierarquia de endereços e identificar suas sub-redes.

- Interface ID (Interface Identifier – Identificador da Interface): 64 bits. Esse número identifica a interface do nó para a camada de enlace.

6.4.TIPOS DE ENDEREÇOS

Existem três tipos de endereços no IPv6:

- Unicast: identifica uma única interface.
- Anycast: identifica um conjunto de interfaces tais que um pacote enviado a um endereço Anycast seja entregue a qualquer um dos membros desse conjunto.
- Multicast: Identifica um grupo de interfaces, tais que um pacote enviado a um endereço Multicast seja entregue a todas as interfaces do grupo.

Não existe nenhum endereço Broadcast no IPv6, sendo sua função substituída por endereços Multicast.

6.4.1. Endereços Unicast

Existem diversos tipos de endereços Unicast alocados no IPv6, quais sejam: *Provider-based, Neutral-interconnect*, NSAP, IPX , *Site-local-use, Link-local-use*, e IPv4-capable-host. Novos tipos de endereços unicast podem ser definidos no futuro.

Alguns desses tipos de endereços unicast são apresentados a seguir, a título de exemplo:

6.4.1.1. Provider-based

São endereços utilizados para comunicações globais, Seu uso é similar aos endereços IPv4 do tipo CIDR (*Classless Inter-Domain Routing*). Seu formato é:

Figura 14 – Formato endereços Provider-based.

3	n bits	m bits	o bits	p bits	o-p bits
010	REGISTRY ID	PROVIDER ID	SUBSCRIBER ID	SUBNET ID	INTF. ID

Fonte: BERNAL FILHO, 12/08/06, internet.

6.4.1.2. Local-use

É um endereço que tem escopo local para roteamento ou seja, dentro de uma sub-rede ou dentro de uma rede de assinante. Eventualmente pode ter também um escopo global de comunicação.

Existem 2 tipos:

1. Link-local-use: usado num único link ou canal de comunicação. Seu formato é:

Figura 15 – Formato endereço Link-local-use.

10 bits	n bits	118-n bits
1111111010	0	INTERFACE ID

Fonte: BERNAL FILHO, 12/08/06, internet.

2. Site-local-use, usado em um único site. Seu formato é:

Figura 16 – Formato endereço Site-local-use.

10 bits	n bits	m bits	118-n-m bits
1111111011	0	SUBNET ID	INTERFACE ID

Fonte: BERNAL FILHO, 12/08/06, internet.

6.4.1.1 IPv4 Encapsulados

Os mecanismos da transição IPv6 incluem uma técnica para hosts e roteadores enviarem dinamicamente os pacotes IPv6 através da infra-estrutura de roteamento do IPv4. Aos nós IPv6 que utilizam esta técnica são atribuídos os endereços Unicast especiais que carregam um endereço IPv4 no 32-bits de menor ordem. Esse tipo de endereço é denominado IPv4-*compatible* IPv6 *address*, e seu formato é:

Figura 17 – Formato de Endereço IPv4-compatible IPv6 address.

80 bits	16 bits	32 bits
000.....000	0000	ENDEREÇO IPv4

Fonte: BERNAL FILHO, 12/08/06, internet.

Um segundo tipo de endereço IPv6 que encapsula um endereço IPv4 é definido também. Este endereço é usado para representar os endereços de nós exclusivamente IPv4 (aqueles que não suportam o IPv6) como os endereços IPv6. Este tipo de endereço é denominado IPv4-mapped IPv6 address, e seu formato é:

Figura 18 – Endereços IPv4-mapped IPv6 address.

80 bits	16 bits	32 bits
000.....000	FFFF	ENDEREÇO IPv4

Fonte: BERNAL FILHO, 12/08/06, internet.

6.4.2. Endereços Anycast

São tipos de endereços atribuídos a mais de uma interface (tipicamente pertencendo a nós diferentes), com a propriedade que um pacote enviado a um endereço Anycast é roteado para a interface mais próxima que tem esse endereço, de acordo com a medida de distância intrínseca dos protocolos de roteamento. Os endereços de Anycast, quando usados como parte de uma seqüência de rota, permitem a um nó selecionar qual dos diversos provedores existentes deve carregar o seu tráfego. Isto seria executado configurando endereços da anycast para identificar o conjunto de roteadores que pertencem aos provedores selecionados (por exemplo, um endereço do anycast por o provedor). Estes endereços anycast podem ser usados como endereços intermediários em um cabeçalho do IPv6, fazendo com que um pacote seja entregue através de um provedor ou de uma seqüência particular de provedores. Outros usos possíveis de endereços anycast seriam identificar um conjunto de roteadores que fazem parte de uma sub-rede particular, ou o conjunto de roteadores de entrada para um domínio específico. Os endereços Anycast são alocados a partir do espaço de endereço do Unicast, usando alguns dos formatos de endereço definidos para o Unicast. Assim, os endereços Anycast são sinteticamente indistintos dos endereços Unicast. Quando a um endereço Unicast

é atribuído uma ou mais interfaces, gerando assim um endereço do Anycast, os nós a que o endereço é atribuído devem explicitamente ser configurados para identificar que é um endereço Anycast.

6.4.3. Endereços Multicast

Um endereço Multicast é um identificador para um grupo de interfaces. Uma interface pode pertencer a qualquer número de grupos Multicast. Seu formato é:

Figura 19 – Formato endereços Multicast.

8 bits	4 bits	4 bits	112 bits
11111111	FLAGS	SCOPE	GOUP ID

Fonte: BERNAL FILHO, 12/08/06, internet.

6.5.ROTEAMENTO

O roteamento no IPv6 é quase idêntico ao roteamento no IPv4, exceto pelo fato de que os endereços são de 128 bits, ao invés dos 32 bits do IPv4. Com extensões muito claras todos os algoritmos do IPv4 (OSPF, RIP, IDRP, ISIS, etc.) ainda podem ser usados.

O IPv6 inclui extensões de roteamento simplificadas que suportam novas funcionalidades poderosas, quais sejam:

- Provider Selection: seleção de provedor, baseada em políticas, desempenho, custo, etc.
- Host Mobility: roteamento até a localização atual do host, quando este pode se deslocar.
- Auto-Readdressing: roteamento para um novo endereço.

A nova funcionalidade de roteamento é obtida criando seqüências de endereços IPv6 usando a opção Routing. Essa opção é usada por um equipamento de origem para listar um ou mais nós intermediários (ou grupos de nós) a serem visitados no caminho de destino de um

pacote do protocolo. Esta função é muito similar em funcionalidade às opções Loose Source e Record Route do IPv4.

A fim de fazer as seqüências de endereços uma função geral, os hosts IPv6 invertem, na maioria de casos, as rotas de um pacote recebido (se o pacote for autenticado com sucesso usando o cabeçalho de autenticação do IPv6) que contenha seqüências de endereços, a fim retornar o pacote ao equipamento de origem. Esta aproximação é feita para permitir que as implementações do hosts IPv6 suporte, desde o princípio, o tratamento e inversão de rotas de origem. Esta é a chave para permitir que eles interropam com os hosts que contém as novas funcionalidades, tais como a seleção de provedor ou endereços estendidos.

Três exemplos mostram como as seqüências do endereço podem ser usadas. Nestes exemplos, as seqüências do endereço são mostradas numa lista dos endereços individuais separados por vírgulas, quais sejam:

[SRC, I1, I2, I3, DST]

onde:

SRC = endereço de origem
I1, I2, I3 = endereços intermediários
DST = endereço de destino

"No caso hipotético destes exemplos. 2 hosts, H1 e H2, desejam se comunicar. Os locais de H1 e de H2 estão conectados aos provedores P1 e P2. É necessário que P1 e P2 tenham acesso a seqüência SRC.In.DST completa para que seja possível a comunicação entre H1 e H2." (BERNAL FILHO, 2006, internet).

6.6.SIMPLIFICAÇÃO DO FORMATO DO CABEÇALHO

Alguns campos do cabeçalho do IPv4 foram descartados ou tornados opcionais, para simplificar o processamento dos pacotes mais comuns e diminuir o overhead do IPv6, que possui um cabeçalho maior.

6.7.MAIOR SUPORTE PARA CAMPOS OPCIONAIS E EXTENSÕES

Os campos opcionais possuem agora menos restrições quanto ao seu tamanho, há maior flexibilidade para a introdução de novas extensões no futuro, o encaminhamento de pacotes fica mais simplificado e pode ser diferenciado a cada hop.

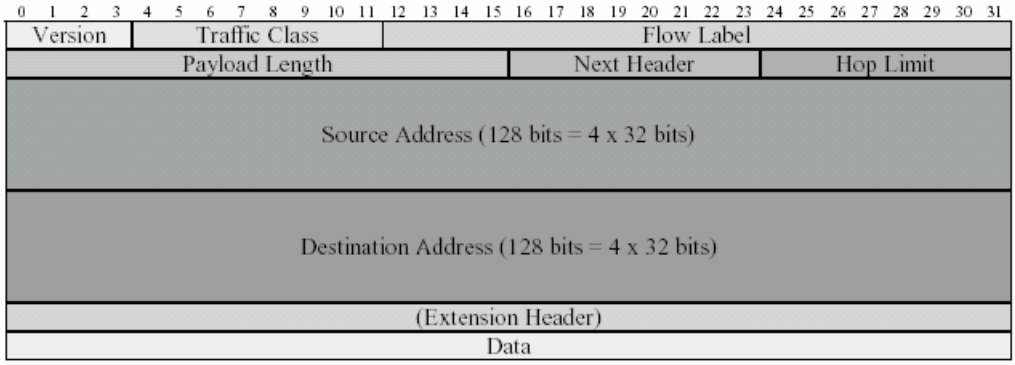
6.8.CAPACIDADE PARA IDENTIFICAÇÃO DE FLUXO

O originador dos pacotes tem como identificar um fluxo de pacotes para um determinado destino (unicast ou multicast) e pedir tratamento especial desse fluxo por parte do roteador, como QoS diferenciado 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 originador do pacote e os equipamentos podem utilizar o processamento economizado para outras funções.

6.9. A ESPECIFICAÇÃO DO IPv6

A figura abaixo foi tirada da especificação do IPv6, documentada sob o RFC 2460.

Figura 20 – Especificação do IPv6 (RFC 2460).



Fonte: SMETANA, 17/09/06, internet.

Tradução do Cabeçalho

- Version (Versão): 4 bits. Para essa versão, o valor é 6.

- Traffic Class (Classe de Tráfego): 8 bits. Esse campo ainda é experimental e pode vir a ser modificado. Na primeira especificação do IPv6, RFC 1883, esse campo não existia. Em seu lugar havia um campo de 4 bits chamado Priority (Prioridade). A função desse campo é permitir diferenciação de tráfego (classes de tráfego) e mecanismos de prioridade, para que os roteadores possam prover tratamento apropriado em cada caso. Algumas idéias do TOS e dos bits Precedence do IPv4 foram aproveitadas. Ainda há muita discussão sobre a divisão mais útil e eficiente dos vários tipos de tráfego em classes. Cabe à camada superior informar a camada IPv6 qual a classe de tráfego a ser utilizada. Um roteador pode alterar os bits do campo Traffic Class da forma que desejar. Por esse motivo, uma estação não deve assumir que um determinado tipo de tráfego que ela associou a uma certa classe será recebido com o campo Traffic Class com o mesmo valor com o qual ela transmitiria.

- Flow Label (Identificação do Fluxo): 20 bits. Um flow é uma seqüência de pacotes enviados a partir de uma determinada origem, para um determinado destino (unicast ou multicast), requerendo um tratamento especial pelos roteadores, como QoS ou reserva de banda (RSVP – Resource Reservation Protocol), por exemplo. O campo Flow Label ainda é experimental e pode vir a ser modificado, como já ocorreu desde a primeira especificação do IPv6, onde ele possuía 24 bits. As mudanças dependem da identificação das características que forem surgindo do tráfego na Internet. A intenção do Flow Label é permitir que a origem possa atribuir uma identificação (padronizada) aos pacotes, para que eles recebam tratamento especial por um roteador (fazer QoS, tráfego de tempo real, etc.). Roteadores e hosts que não

são capazes de identificar o Flow Label de um pacote devem deixar o campo com valor igual a 0 (zero), quando originá-lo, deixá-lo inalterado, quando retransmiti-lo, ou ignorá-lo, quando recebê-lo.

- Payload Length (Comprimento da Carga): 16 bits. Informa o comprimento dos dados, em octetos, encapsulados pela camada de rede, isto é quantos bytes vêm depois do cabeçalho IPv6 (os campos de extensão são contabilizados). Caso esse campo seja 0 (zero), indica que o comprimento do payload é superior a 65.535 octetos e é informado em um Extension Header.

- Next Header (Próximo Cabeçalho): 8 bits. Informa qual o protocolo da camada superior que está utilizando os serviços da camada IP. A numeração também segue o RFC 1700. O UDP, por exemplo, é número 17. No IPv6, pode haver um campo opcional após o cabeçalho. Nesse caso, o valor de Next Header informa qual o tipo de extensão que vem após o cabeçalho IPv6.

- Hop Limit (Limite de Hop): 8 bits. Semelhante ao TTL do IPv4, cada unidade processadora de pacotes (nó) decrementa esse valor de 1 unidade e quando esse valor chegar a 0 (zero), o pacote é descartado.

- Source Address (Endereço de Origem): 128 bits. Informa o endereço de origem do pacote.

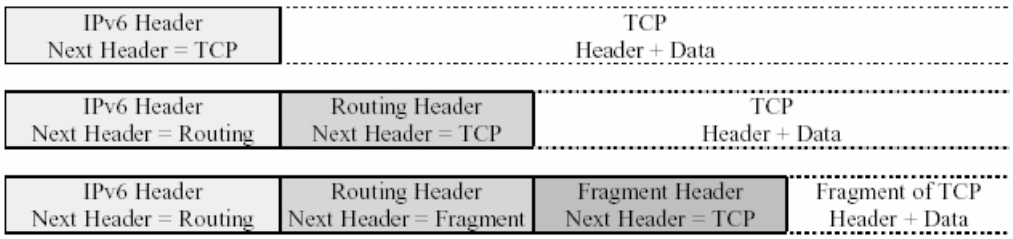
- Destination Address (Endereço de Destino): 128 bits. Informa o endereço de destino. O endereço de destino pode não ser o endereço do host final, porque pode ser um cabeçalho de roteamento.

- Extension Header (Cabeçalho de Extensão): Tamanho variável, mas sempre múltiplo de 8 octetos (64 bits). Pode haver mais de um campo de extensão. A presença de um campo de extensão pode ser determinada pelo valor do campo Next Header. Cada Extension Header tem um campo Next Header informando o próximo protocolo, como pode ser observado na figura 21. Normalmente, somente o nó de destino irá processar os Extension Headers. Os Extension Headers precisam ser processados exatamente na ordem em que eles

aparecem. Uma implementação completa do IPv6 tem de ser capaz de reconhecer e processar os seguintes tipos de Extension Headers: Hop-by-Hop Options (Opções Hop-a-Hop), Routing – Type 0 (Roteamento – Tipo 0), Fragment (Fragmento), Destination Options (Opções de Destino), Authentication (Autenticação) e Encapsulating Security Payload (Encapsulando Carga de Segurança).

Os quatro primeiros tipos de Extension Header podem ser encontrados no RFC 2460 (o da especificação do IPv6), e os dois últimos, nos RFCs 2402 e 2406, respectivamente. O Routing Header pode especificar quais são os próximos destinos depois do destino especificado pelo campo Destination Address. Quando houver mais de um Extension Header presente, recomenda-se que eles estejam na seguinte ordem: cabeçalho IPv6, Hop-by-Hop Options, Destination Options (para o primeiro destino, especificado pelo Destination Address, e pelos próximos destinos, especificados no Routing Header), Routing, Fragment, Authentication, Encapsulating Security Payload, outro Destination Options (para ser processado somente pelo último destino) e depois os cabeçalhos do protocolo da camada superior.

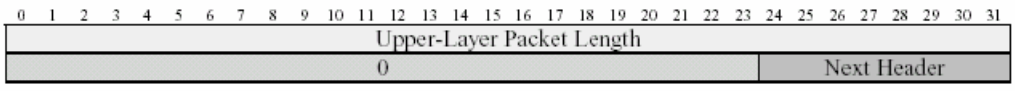
Figura 21 – Exemplo de Extension Headers do IPv6.



Fonte: SMETANA, 17/09/06, internet.

Quando ocorrer a migração para o IPv6, os protocolos da camada superior que incluem o tamanho do campo IP em seus mecanismos de detecção de erro deverão ser alterados. No IPv6, há também um "pseudo-cabeçalho", após os Extension Header, mostrado na figura abaixo.

Figura 22 – Pseudo-cabeçalho que antecede o cabeçalho da camada superior no IPv6.



Fonte: SMETANA, 17/09/06, internet.

- Upper-Layer Packet Length (Comprimento do Pacote da Camada Superior): 32 bits. Corresponde ao comprimento em bytes da camada superior, incluindo o cabeçalho e os dados (PDU e SDU). Para protocolos de camada superior que carregam seu comprimento no próprio cabeçalho, como o UDP, o valor desse campo é o mesmo do presente na camada superior.
- Next Header (Próximo Cabeçalho): O Next Header do pseudo-cabeçalho será diferente do Next Header do cabeçalho IPv6, somente no caso em que houver Extension Headers após o IPv6. Nesse caso, o Next Header do IPv6 informa o valor do Extension Header.

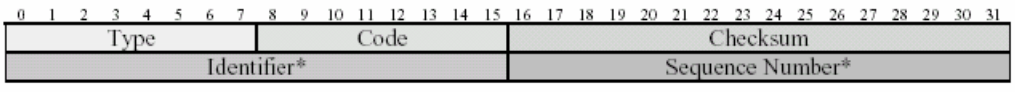
O MTU mínimo do IPv6 é de 1.280 bytes (no IPv4 era 576 bytes), mas o recomendado é que ele seja maior que 1.500 bytes, para que possa ser feita alguma forma de encapsulamento sem que a camada de rede precise fragmentar os dados.

7. ICMP

7.1.ICMPv4

O Internet Control Message Protocol (ICMP) é um protocolo obrigatório da camada de rede da arquitetura TCP/IP e serve para a transmissão de mensagens de erro, controle e obtenção de outras informações relacionadas à rede. Apesar do ICMP ser um protocolo da camada de rede, ele utiliza os serviços do próprio IP para ser transmitido, sendo que no campo Protocol do IPv4, o valor é 1, que é o número do ICMP. Se uma mensagem ICMP não pode ser enviada, não será gerada outra em seu lugar, evitando uma enchente de mensagens ICMP. Sua especificação encontra-se no RFC 792 – Internet Control Message Protocol – DARPA Internet Program Protocol Specification.

Figura 23 – Especificação do ICMP (RFC – 792).



Fonte: SMETANA, 17/09/06, internet.

O formato do cabeçalho ICMP é variável. Os campos marcados com "*" nem sempre estão presentes e pode haver campos adicionais, para informar um timestamp ou o endereço de um gateway, por exemplo.

- Type (Tipo): 8 bits. Identifica o tipo de mensagem enviada ou de resposta recebida (ver tabela mais adiante).

- Code (Código): 8 bits. Identifica a causa do tipo de mensagem recebida (ver tabela mais adiante).

Tabela 9 – Tipo e código de mensagens ICMP.

Type	Code	Significado
0	-	**EEcho Reply (Resposta a Eco)** – Mensagem recebida de um gateway ou de um host. Um Echo Request foi recebido e a mensagem de resposta deve conter os mesmos dados do Echo Request.
3	-	**Destination Unreachable (Destino Inalcançável)** – Mensagem recebida de um gateway. O endereço destino não pode ser alcançado por um dos motivos especificados pelo campo Code.
3	0	**Net Unreachable (Rede Inalcançável)** – Mensagem recebida de um roteador. Causa: O pacote foi descartado, porque o roteador não conseguiu enviar o pacote para a rede destino. Ou o roteador não possui uma rota para a rede destino, ou então o endereço de rede destino não existe.
3	1	**Host Unreachable (Host Inalcançável)** – Mensagem recebida de um roteador. Causa: A rede destino foi alcançada, mas não foi possível entregar o pacote para o host destino, provavelmente por causa de uma sub-máscara configurada erroneamente ou por que o host destino não está acessível.
3	2	**Protocol Unreachable (Protocolo Inalcançável)** – Mensagem recebida de um host. Causa: O host destino provavelmente não suporta o protocolo de camada superior especificado.
3	3	**Port Unreachable (Porta Inalcançável)** – Mensagem recebida de um host. Causa: O socket ou a porta TCP não estão disponíveis.
3	4	**Fragmentation Needed and DF Set (Fragmentação Necessária e Setado)** – Mensagem recebida de um gateway. Causa: O pacote possuía tamanho maior que o MTU (Maximum Transmission Unit – Unidade Máxim Transmissão) de alguma rede por onde ele tentou passar, necessitando e ser fragmentado, porém o bit Don't Fragment do IPv4 estava com valor igu 1, indicando que o pacote não pode ser fragmentado. Como resultado o pa foi descartado.
3	5	**Source Route Failed (Rota da Origem Falhou)** – Mensagem recebida de um roteador. A rota especificada pela origem no campo Options do cabeçalho IP não pôde ser completada.
4	-	**Source Quench (Estrangulamento da Origem)** – Mensagem recebida de um gateway ou de um host. Quando um roteador ou um host está com seus buffers cheios e começa (ou está prestes) a descartar pacotes, essa mensagem é enviada para a origem, pedindo a ela que pare de mandar mais pacotes. É um método de contenção de congestionamento. O roteador ou host continua mandando essa mensagem enquanto estiver com dificuldades em processar pacotes. A origem só volta a transmitir pacotes quando parar de receber essa mensagem.
5	-	**Redirect (Redirecionar)** – Mensagem recebida de um gateway. Nesse tipo de mensagem ICMP há um campo extra, chamado Gateway Internet Address (Endereço Internet do Gateway), que especifica por qual gateway devem passar os datagramas para a rede destino do cabeçalho IP. Esse tipo de mensagem é recebida na situação a seguir. Um host, H1, está diretamente conectado à rede de um gateway, G1. G1 recebe de H1 um datagrama, cujo destino é um outro host, Hx, na rede X. Então, G1 consulta em sua tabela de roteamento e descobre que o próximo gateway na rota para a rede X é o gateway G2. Se G2 estiver na mesma rede que o host que originou o datagrama, G1 manda uma mensagem Redirect para o host, avisando-o que os próximos datagramas para a rede X devem ser encaminhados diretamente para G2. Se o host especificar uma rota para um determinado destino, mesmo que G1 conheça uma rota mais curta, a rota especificada será seguida e não será enviado um Redirect.

5	0	**Redirect Datagrams for the Network (Redirecionar Datagramas para a Rede)** – O host deve encaminhar os datagramas cujo destino é a rede X para um determinado gateway.
5	1	**Redirect Datagrams for the Host(Redirecionar Datagramas para O Host)** – O host deve encaminhar os datagramas cujo destino é o host Hx para um determinado gateway.
5	2	**Redirect Datagrams for the Type of Service and Network (Redirecionar Datagramas para o Tipo de Serviço e Rede)** – O host deve encaminhar os datagramas cujo destino é a rede X e que requerem o Tipo de Serviço T para um determinado gateway.
5	3	**Redirect Datagrams for the Type of Service and Network Redirecionar Datagramas para o Tipo de Serviço e Rede)** – O host deve encaminhar os datagramas cujo destino é a rede X e que requerem o Tipo de Serviço T para um determinado gateway.
8	0	**Redirect Datagrams for the Type of Service and Host (Redirecionar Datagramas para o Tipo de Serviço e Host)** – O host deve encaminhar os datagramas cujo destino é o host Hx e que requerem o Tipo de Serviço T para um determinado gateway.
11	-	**Time Exceeded (Tempo Excedido)** – O tempo de vida de um pacote ou o tempo deremontagem de pacotes fragmentados foi excedido.
11	0	**Time to Live Exceeded in Transit (Tempo de Vida Excedido em Trânsito)** – Mensagem recebida de um gateway. Se o campo TTL de um datagrama chega a 0, ele deve ser descartado e o host que o originou deve ser notificado através de uma mensagem Time Exceeded tipo TTL Exceeded in Transit..
11	1	**Fragment Reassemble Time Exceeded (Tempo de Remontagem do Pacote Excedido)** – Mensagem recebida de um host. Se um host não receber todos os fragmentos necessários para a remontagem de um pacote dentro de um determinado tempo, os fragmentos são descartados e uma mensagem Fragment Reassemble Time Exceeded é enviada para o host de origem. Se o fragmento 0 não está presente, não é enviada a mensagem.
12	-	**Parameter Problem (Problema de Parâmetro)** – Mensagem pode ser recebida de um host ou de um gateway. Se um gateway não conseguir decodificar corretamente os campos de um datagrama e por causa disso ele precisar ser descartado, a origem é notificada através de uma mensagem Parameter Problem, indicando o campo com problema. Esse tipo de problema é mais freqüente nos argumentos do campo Option do cabeçalho IP. Essa mensagem só é enviada caso o pacote precise ser descartado.
13	-	**Timestamp (Marca de Tempo)** – Possui um campo adicional de 32 bits informando o último momento (em ms contados a partir de meia noite de Greenwich) no qual o originador da mensagem mexeu nela. Se não houver sincronismo com o horário de Greenwich, ou se não for possível a precisão com ordem de ms, o bit mais significativo desses 32 bits deve ser setado, indicando o uso de uma base de tempo diferente.
14	-	**Timestamp Reply (Resposta da Marca de Tempo)** – Possui três campos adicionais de 32 bits informando o momento enviado pelo originador da mensagem, o instante no qual a mensagem foi recebida e o instante no qual ela foi enviada.
15	-	**Information Request (Pedido de Informação)** – Mensagem enviada por um host, com os campos origem e destino do cabeçalho IP iguais a 0 (significa “esta rede”). Esse é um modo de um host descobrir a qual rede ele pertence.
16	-	**Information Reply (Resposta ao Pedido de Informação)** – Mensagem enviada por um host ou um gateway, quando eles recebem um Information Request. A mensagem Information Reply deve conter os endereços preenchidos corretamente. Os campos Identifier e Sequence Number são

		utilizados para associar corretamente uma Information Reply a uma Information Request.

Fonte: SMETANA, 17/09/06, internet.

• Checksum (Verificação da Soma): 16 bits. Esse checksum é calculado somente sobre o cabeçalho ICMP. Para se calculá-lo, faz-se o complemento de um de cada palavra de 16 bits do cabeçalho, soma-se elas e faz-se o complemento de um da soma total (para efeitos de cálculo, o campo Checksum vale 0).

• Identifier (Identificador): 16 bits. Serve para associar um Reply a um Request. Pode ser 0.

• Sequence Number (Número de Seqüência): 16 bits. Também serve para associar um Reply a um Request. Pode ser 0.

• Address Mask (Máscara de Endereço): 32 bits.

7.1.1. O comando ping

O comando ping presente em grande parte dos sistemas operacionais e equipamentos de redes nada mais é do que uma mensagem ICMP tipo Echo Request. O campo de dados do Echo Request pode trazer protocolos de camadas superiores e outras informações. O formato geral do comando ping é:

ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] [-r count] [-s count][[-j host-list] | [-k host-list]] [-w timeout] destination-list

Os campos entre “[” e “]” são opcionais e suas funções são apresentadas na tabela 10.

Tabela 10 – Opções do comando ping.

Opção	Função
-t	Pinga o endereço destino até que o processo seja interrompido (CTRL+C no Windows). Exemplo: ping –t 143.107.111.42
-a	Pinga o endereço destino, dado o nome do host. Normalmente, a opção –a é habilitada por default, isto é, não precisa-se digitar o –a para se pingar um host a partir do nome. Exemplo: ping –a www.redes.usp.br.
-n count	Especifica o número de Echo Requests a ser enviado. Exemplo: ping –n 5 143.107.111.42
-l size	Especifica o tamanho em bytes do Echo Request a ser enviado (o campo de dados é preenchido com os bytes). Se o tamanho do ping for maior que o MTU da rede, o ping será fragmentado. Como o campo Total Length tem 16 bits, o valor máximo desse parâmetro é 65.535. Exemplo: ping –l 2000 143.107.111.42
-f	Seta o campo Don't Fragment (DF=1) do cabeçalho IPv4, não deixando que o datagrama seja fragmentado. O MTU da rede Ethernet é 1.518 bytes, mas devido aos cabeçalhos das camadas inferiores (26 bytes da camada de enlace + 20 bytes do cabeçalho IP), não é possível enviar um ping com mais de 1.472 bytes. Exemplo: ping –f –l 1473 143.107.111.42
-i TTL	Define o valor do campo TTL do cabeçalho IPv4. O valor máximo é 255. O valor default do ping do Windows é 32. Exemplo: ping –i 2 www.usp.br
-v TOS	Define o valor (em decimal) do campo TOS, composto pelos sub-campos Precedence, Delay, Throughput, Relibility e bits reservados no cabeçalho IPv4. Exemplo: ping –v 252 143.107.111.42. Campos do TOS (em binário): Precedence = 111 (Network Control) Delay = 1 (Atraso baixo) Throughput = 1 (Alta vazão) Relibility = 1 (Confiabilidade alta) Bits reservados = 00
-r count	Grava a rota para o número de hops especificado. O valor máximo é 9, isto é, no máximo é possível gravar 9 endereços IP. Exemplo: ping –r 9 www.yahoo.com
-s count	Devolve os timestamps (Internet Timestamp) dos hops por onde passou. O valor máximo é 4, isto é, no máximo é possível guardar 4 timestamps. Exemplo: ping –s 4 143.107.111.42
-j host-list	Sugere uma rota para o destino, mas a rota não precisa ser seguida exatamente. Exemplo: ping –j <IP do primeiro hop> [...] [IP do n-ésimo hop] <IP destino>
-k host-list	Especifica uma rota para o destino, que deve ser seguida exatamente. Exemplo: ping –k <IP do primeiro hop> [...] [IP do n-ésimo hop] <IP destino>
-w timeout	Especifica o tempo em milisegundos que o Echo Reply tem para ser recebido antes de dartimeout. Exemplo: ping –w 500 143.107.111.1

Fonte: SMETANA, 17/09/06, internet.

7.1.2. O comando tracert

O comando tracert do Windows (em alguns sistemas, o comando é traceroute) mostra a rota por onde o datagrama passou até chegar ao destino. O formato geral do comando tracert é:

tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Os campos entre "[" e "]" são opcionais e suas funções são apresentadas na tabela 11.

Tabela 11 – Opções do comando tracert.

Opção	Função
-d	Mostra a rota por onde o datagrama passou, mas não descobre o nome dos hosts e gateways por onde ele passou. Exemplo: tracert –d www.yahoo.com. Mostra a rota por onde o datagrama passou, mas não descobre o nome dos hosts e gateways por onde ele passou. Exemplo: tracert –d www.yahoo.com
-h maximum_hops	Especifica um número máximo de hops para tentar alcançar o destino. Exemplo: ping –h 10 www.yahoo.com
-j host-list	Sugere uma rota para o destino, mas a rota não precisa ser seguida exatamente. Exemplo: tracert –j <IP do primeiro hop> [...] [IP do n-ésimo hop] <IP destino>
-w timeout	Especifica o tempo em milisegundos que cada hop tem para enviar a resposta antes de dar timeout. Exemplo: tracert –w 500 143.107.111.1

Fonte: SMETANA, 17/09/06, internet.

7.1.3. O comando netstat

O comando netstat do Windows mostra dados e estatísticas da camada de rede. O formato geral do comando é:

netstat [[-a] | [-r] | [-s]]

Na figura 24 tem-se o cabeçalho de Opções do comando netstat

Figura 24 – Opções do comando netstat

Opção	Função
-a	Mostra as conexões TCP/UDP ativas e os estados delas.
-r	Mostra a tabela de roteamento
-s	Mostra as estatísticas dos protocolos IP, ICMP, TCP e UDP.

Fonte: SMETANA, 17/09/06, internet.

7.1.4. O comando ipconfig

O comando ipconfig do Windows NT mostra as configurações das interfaces de rede do computador. O formato geral do comando é:

ipconfig [/? | /all | /release [adapter] | /renew [adapter]]

Na figura 25 tem-se o cabeçalho de Opções do comando ipconfig

Figura 25 – Opções do comando ipconfig

Opção	Função
/?	Mostra a ajuda para o comando ipconfig.
/all	Mostra todas as informações disponíveis sobre as interfaces de rede e de fax-modem do computador.
/release [adapter]	Quando o endereço IP de uma interface foi obtido através de DHCP, essa opção desassocia o endereço IP à interface.
/renew [adapter]	Associa um endereço IP a uma interface, utilizando o DHCP.

Fonte: SMETANA, 17/09/06, internet.

7.2.ICMPv6

O IPv6 utiliza o ICMP tal como existia para o IPv4, contudo foram necessárias algumas alterações (RFC 1885). O identificador de protocolo 1, usado para o ICMPv4 foi abandonado, um cabeçalho e mensagem ICMPv6 são identificados pelo valor 58 no campo "Next Header" do cabeçalho anterior.

Uma mensagem ICMPv6 possui a seguinte estrutura, semelhante à do ICMPv4:

Tabela 12 – Estrutura de mensagem ICMPv6.

Type	(8 bits)
Code	(8 bits)
Checksum	(16 bits)
Dados da mensagem	(variável)

Fonte: MOREIRA, 13/09/06, internet.

Ao contrário do que acontecia com o ICMPv4, o "checksum" é calculado sobre a mensagem, incluindo também o Pseudo-cabeçalho IPv6.

O campo tipo pode ter um dos seguintes valores:

Tabela 13 – Pseudo-cabeçalho IPv6

1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction

Fonte: MOREIRA, 13/09/06, internet.

Tal como já acontecia para o ICMPv4, as mensagens dividem-se em duas categorias: ERRO ("type" menor do que 128) e INFORMAÇÃO ("type" maior do que 127).

Regras gerais de processamento ICMPv6:

• As mensagens ICMPv6 de erro recebidas, de tipo desconhecido devem ser passadas a camadas superiores.

• As mensagens ICMPv6 de informação recebidas, de tipo desconhecido devem ser ignoradas.

• As mensagens ICMPv6 de erro, contêm parte do "datagrama" original, garantindo que o pacote ICMP não exceda 576 octetos.

• Nos casos em que uma mensagem ICMPv6 de erro exige processamento das camadas superiores, utiliza-se o campo "Next Header" do "datagrama" original para determinar qual a camada apropriada.

• As mensagens ICMPv6 de erro nunca devem ser enviadas em resposta a:
- outras mensagens ICMPv6 de erro

- "datagramas" com destino "multicast" (Excepções: "Packet Too Big" e "Parameter Problem" com código 2)

- "datagramas" com origem "IPv6 Unspecified Address", um endereço "anycast" ou um endereço "multicast"

• As mensagens ICMPv6 de erro não devem sobrecarregar a rede, se um dado nó origina erros sistemáticos, a taxa de envio de mensagens ICMPv6 para esse nó deve ser controlada.

7.2.1. Mensagem "Destination Unreachable"

Esta mensagem é enviada (geralmente por um "router") quando o destino especificado num "datagrama" não pode ser atingido, por razões que não a congestão de um nó, o código indica o tipo de destino não atingido:

Tabela 14 – Tipo de destino não atingido

0	no route to destination
1	communication with destination administratively prohibited
2	not a neighbor
3	address unreachable
4	port unreachable

Fonte: MOREIRA, 13/09/06, internet.

O código zero é gerado quando um "router" não sabe para onde enviar o "datagrama". O código 1 é gerado quando existe um filtro/"firewall" que impede a passagem. O código 2 é gerado quando existe um cabeçalho de extensão "routing" e um dado nó especificado como "strict" não é vizinho do anterior. Outras razões para que não se possa atingir o endereço de destino geram o código 3. O código 4 é gerado quando a porta de destino não tem nenhuma aplicação associada para receber os dados. Seja qual for o tipo de erro a camada superior a que pertence o "datagrama" deve ser notificada.

Após o "checksum" existem 32 bits reservados que devem ser inicializados com zero, segue-se parte do "datagrama" original.

7.2.2. Mensagem "Packet Too Big"

O IPv6 implementa fragmentação apenas entre nós finais e não "router" a "router" como acontecia com o IPv4. Quando um "router" IPv6 recebe um "datagrama" ou fragmento e o MTU correspondente ao "hop" seguinte é demasiado pequeno, esta mensagem é enviada à origem com código 0. O MTU do "hop" no qual se dá a falha é enviado num campo de 32 bits após o "checksum". O envio deste valor facilita uma implementação eficiente do "MTU Path Discovery" (RFC 1191) que permite a determinação do MTU máximo a usar num dado caminho. Quando este erro ocorre, a camada superior a que pertence o "datagrama" deve ser notificada.

7.2.3. Mensagem "Time Exceeded"

Esta mensagem pode ser gerada em duas situações:

- Código 0 - Excesso de saltos (o valor "Hop Limit" do cabeçalho IPv6 chegou a zero)
- Código 1 - Tempo de reagrupamento excedido (o tempo disponível para o nó de destino reconstituir o "datagrama" (60 segundos) foi excedido)

7.2.4. Mensagem "Parameter Problem"

Esta mensagem indica que existe um problema no cabeçalho IPv6 ou cabeçalhos de extensão:

Tabela 15 – Mensagens de Problemas no Cabeçalho.

Código 0	Campo com erro
Código 1	"Next Header" desconhecido
Código 2	"Opção" desconhecida

Fonte: MOREIRA, 13/09/06, internet.

Depois do "checksum" segue-se um campo de 32 bits que indica o "offset" da localização do erro dentro do "datagrama" original.

7.2.5. Mensagens "Echo Request" e "Echo Reply"

Não existem diferenças relevantes relativamente ao ICMPv4.

7.2.6. Mensagens "Group Membership"

Estas mensagens destinam-se à gestão de nós membros de grupos "multicast", junto dos "routers" locais , razão pela qual o "Hop Limit" do respectivo cabeçalho IPv6 é sempre um. No IPv4 os endereços de "multicast" surgiam como uma extensão sendo necessário um protocolo adicional documentado nas RFC 1112 e RFC 2236 (IGMP - "*Internet Group Management Protocol*").

No ICMPv6 deixa de ser necessário o IGMP e as mensagens são integradas no ICMP, o seu formato é o seguinte:

Tabela 16 – Formato de Mensagens ICMP

Type	8 bits	Tipo ICMP (130; 131 ou 132)
Código	8 bits	Sempre ZERO
Checksum	16 bits	ver formato geral ICMPv6

MAX Delay	32 bits	Tempo máximo de resposta
ZERO	32 bits	
Endereço MCAST	128 bits	

Fonte: MOREIRA, 13/09/06, internet.

Tipos de mensagem:

Tabela 17 – Tipos de mensagens

130	"Group Membership Query"
131	"Group Membership Report"
132	"Group Membership Reduction"

Fonte: MOREIRA, 13/09/06, internet.

O campo "MAX Delay" é usado apenas no tipo 130, e define o atraso máximo (em mili segundos) para a obtenção de uma resposta. Os princípios de funcionamento mantêm-se fieis à RFC 1112.

A mensagem "Group Membership Query" é enviada pelos "hosts" aos "routers" para obtenção de informação quanto à existência de grupos locais de "multicast". O campo "Endereço MCAST" pode ser colocado a zero para obtenção de informação sobre qualquer grupo com membros "General Query" ou conter um endereço "multi-cast" para determinar se existem membros nesse grupo "Group-Specific Query".

Os "routers" também enviam periodicamente mensagens "General Query" a que os membros devem responder.

A mensagem "Group Membership Report" é enviada em resposta à anterior, ou em certas situações por iniciativa própria de um membro ou de um "router". Por exemplo, quando um "router" envia uma mensagem "Group-Specific Query" e não obtém resposta num tempo pré-determinado considera que o grupo não possui membros. A mensagem "Group Membership Report" é usada pelos "hosts" para se tornarem membros de um grupo, basta proceder ao seu envio para um "router" local.

A mensagem "Group Membership Reduction" é usada para sair de um grupo de "multi-cast", para tal o membro envia-a ao "router".

Para MOREIRA (2006), existem diversos aspectos de implementação que são atendidos, nomeadamente quanto a temporizações, por exemplo, quando um "router" envia uma mensagem "Group Membership Query" para confirmar o número de membros não é conveniente uma resposta imediata de todos os membros, por esta razão cada membro introduz um atraso aleatório no tempo de resposta.

8. SITUAÇÃO ATUAL DO IPv6

Em 1996 foi iniciado o projeto denominado 6Bone, que é um backbone internacional formado por sites IPv6 conectados através de túneis IPv4, visando servir como suporte a testes de implementação do protocolo IPv6 em diversas plataformas, além de servir como ponto de partida para a implementação do protocolo na internet.

Atualmente, o projeto 6Bone consiste em uma rede virtual que permite o transporte de pacotes IPv6 sobre redes físicas IPv4, formando um cenário composto por ilhas IPv6 que suportam diretamente o protocolo e comunicam-se entre si através de ligações virtuais ponto a ponto (túneis). As máquinas com protocolo IPv4 que compõem os túneis possuem um sistema operacional com suporte para IPv6 e utilizam protocolos de roteamento adequados à nova versão.

O 6Bone foi o ponto inicial para a disseminação do protocolo IPv6, sendo que este projeto é conhecido mundialmente, servindo de referência para pesquisas e informações sobre o novo protocolo.

Apesar do início das pesquisas com o IPv6 terem sido iniciadas há um bom tempo, no Brasil, os projetos utilizando o protocolo ainda estão se consolidando, sendo que a maior parte desses projetos é realizada em laboratórios de instituições de ensino como pesquisas acadêmicas. A quantidade de projetos de pesquisa ainda é relativamente pequena e existe pouca documentação em relação aos mesmos.

A RNP (Rede Nacional de Pesquisa) possui dois projetos relacionados ao IPv6: o backbone RNP2, que interliga alguns pontos de presença da RNP com protocolo IPv6 em modo nativo, atualmente com 8 (oito) pontos de conexão; e o Br6Bone, que conecta instituições que queiram usar o protocolo IPv6 através da estrutura atual em IPv4, através de túneis.

Segundo MARTINI (2006), a disponibilidade destes serviços oferecidos pela RNP abre novas perspectivas para o desenvolvimento do IPv6 no país, na medida em que permite à RNP estabelecer parcerias com instituições, inclusive do setor privado, é possível explorar novos protocolos, serviços e aplicações em ambientes IPv6. Além de que, instituições ligadas a ela podem participar de uma rede de pesquisas com alcance internacional. Diversas universidades como Unicamp, UFRGS e UFBA, além de provedores comerciais, como a Rede Pegasus, participam do projeto.

9. TRANSIÇÃO PARA IPv6

9.1.ESTRATÉGIAS DE TRANSIÇÃO PARA IPv6

Para o IPv6 poder trabalhar plenamente deveriam ser atualizados, pelo menos, todos os hosts de uma rede - uma mudança radical a ser feita por administradores de redes com milhares ou, às vezes, dezenas de milhares de hosts. Entretanto, este não é o caso: as pessoas que trabalham na transição de IPv4 para IPv6 têm trabalhado duro para criar mecanismos que possibilitem a coexistência do IPv4 e IPv6, entre estes podem ser citados, pilha dupla, túnel IPv4/IPv6 e tradução IPv4/IPv6. A atualização das redes atuais pode ser feita com um baixo impacto, caso sejam feitas de forma metodológica e inteligente. A seguir são mostradas estratégias para esta transição.

A transição de IPv4 para IPv6 deve ser feita de forma gradual. Uma atualização de forma radical faria com que administradores de redes tivessem que encontrar e instalar novas versões para softwares de rede para cada host e roteador na internet - nada fácil, imaginando o número de diferentes plataformas rodando IPv4.

Mais realisticamente, a transição para IPv6 continuará a ser feita de maneira mais lenta, com vendedores e desenvolvedores gradualmente introduzindo versões de aplicações IPv6 para as diferentes plataformas, e administradores de redes determinando se são ou não necessários os novos recursos disponíveis para IPv6. É esperado que o IPv4 e o IPv6 devam coexistir por um bom período de tempo, mas não para sempre. Muitas estratégias para transmissão falam em tunelamento, com o intuito de aproximar duas redes distantes, onde pacotes IPv6 são encapsulados dentro de pacotes IPv4. Isto faria com que ilhas IPv6 pudessem se comunicar utilizando oceanos IPv4. Após certo período de tempo, a população IPv6 tenderia a crescer, sendo que cada vez mais as redes começariam a utilizar este protocolo, fazendo com que as ilhas começassem a se juntar, não necessitando mais de tunelamento. Outro ponto da aproximação seria o *dual-stack*, onde hosts e roteadores teriam rodando em uma mesma interface, tanto pilhas IPv4, quanto IPv6. Desta maneira, um nodo *dual-stack* pode receber e transmitir pacotes dos dois protocolos, fazendo com que eles coexistam em uma mesma rede.

A Figura 26 mostra um quadro como exemplo de uma interface ethernet, configurada com *dual-stack*, no sistema operacional Linux. A figura a 27 mostra um quadro como um exemplo da resposta do comando IF CONFIG que traz informações de uma interface também configurada com *dual-stack*, porém com o sistema operacional Solaris.

Figura 26 – Interface Ethernet configurada com dual-stack em Linux

eth0 Link encap:Ethernet HWaddr 00:C0:DF:E9:2B:26
inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
inet6 addr: fe80::2c0:dfff:fee9:2b26/10 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:3580 errors:0 dropped:0 overruns:0 frame:0
TX packets:2065 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
Interrupt:11 Base address:0xde00

Fonte: TAMUSIUNAS, 08/09/06, internet.

Figura 27 – Interface Ethernet configurada com dual-stack em Solaris

lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1 inet 127.0.0.1 netmask ff000000
iprb0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2 inet 192.168.1.1 netmask ffff0000 broadcast 192.168.1.255
lo0: flags=2000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv6> mtu 8252 index 1 inet6 ::1/128

```
iprb0:  flags=2000841<UP,RUNNING,MULTICAST,IPv6>  mtu
1500 index 2 inet6 fe80::2c0:dfff:fee9:2b26/10
```

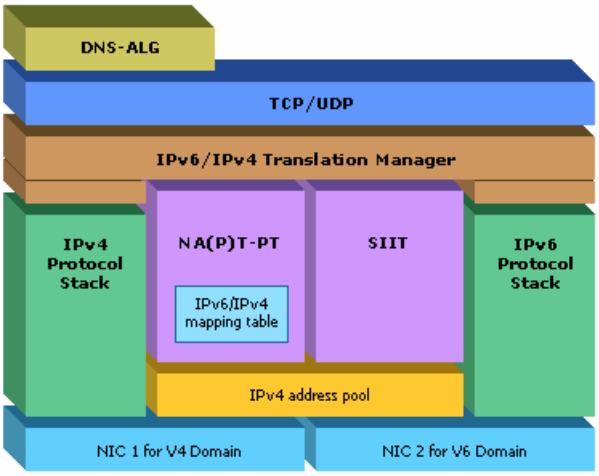
Fonte: TAMUSIUNAS, 08/09/06, internet.

Conforme TAMUSIUNAS (2006), No caso das figuras acima, as interfaces ethernet estão com o endereço IPv4 192.168.1.1 e o endereço IPv6 fe80::2c0:dfff:fee9:2b26, o que caracteriza este nodo como dual-stack.

9.1.1. Pilha Dupla

Segundo MARTINI (2006), através deste mecanismo as máquinas podem suportar os dois protocolos, podendo conectar e acessar recursos da rede IPv4 e IPv6 simultaneamente. Além disso, existe a possibilidade de um dos protocolos estar desabilitado na pilha, assim a máquina irá se comportar como se houvesse somente um protocolo implementado. Os roteadores que tiverem pilha dupla poderão repassar tanto pacotes IPv4 quanto IPv6.

Figura 28 – Pilha do *Gateway* de Protocolo conforme recomendação da RFC2766.

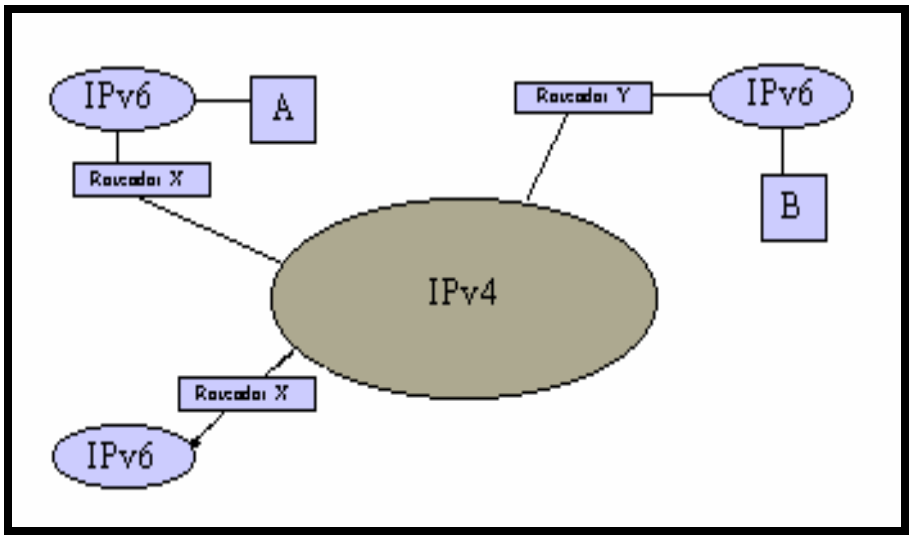


Fonte: COSTA, 27/09/06, internet.

9.1.2. Aproximação de Redes IPv6 Utilizando Túneis

Este tipo de solução é útil quando deseja-se conectar ilhas IPv6 isoladas, no meio de oceanos IPv4, como demonstrado na figura 29.

Figura 29 – Utilização de Túneis Para conexão entre ilhas Ipv6



Fonte: TAMUSIUNAS, 11/09/06, internet.

O tunelamento requer que os nodos IPv6 em ambas as partes do túnel sejam capazes de transmitir pacotes IPv4 (nodos *dual-stack*).

Conforme TAMUSIUNAS (2006), o processo de encapsular IPv6 dentro de IPv4 é similar ao método de encapsulação de outros protocolos: o nodo de um dos lados do túnel pega o datagrama IPv6 e o envia como sendo dados do payload para o nodo que está do outro lado do túnel. O resultado é um stream de datagramas IPv4 que contém datagramas IPv6. Como mostrado na figura 29, os nodos A e B trabalham apenas com IPv6. Para um pacote ser enviado de A para B, o nodo A simplesmente endereça o pacote para o endereço IPv6 do nodo B, passando pelo roteador X. Este roteador encapsula o pacote IPv6 dirigido ao nodo B e o envia para o endereço IPv4 do roteador Y. O roteador Y recebe o pacote e desencapsulá-o, enviando em seguida ao seu destino, utilizando a rede IPv6.

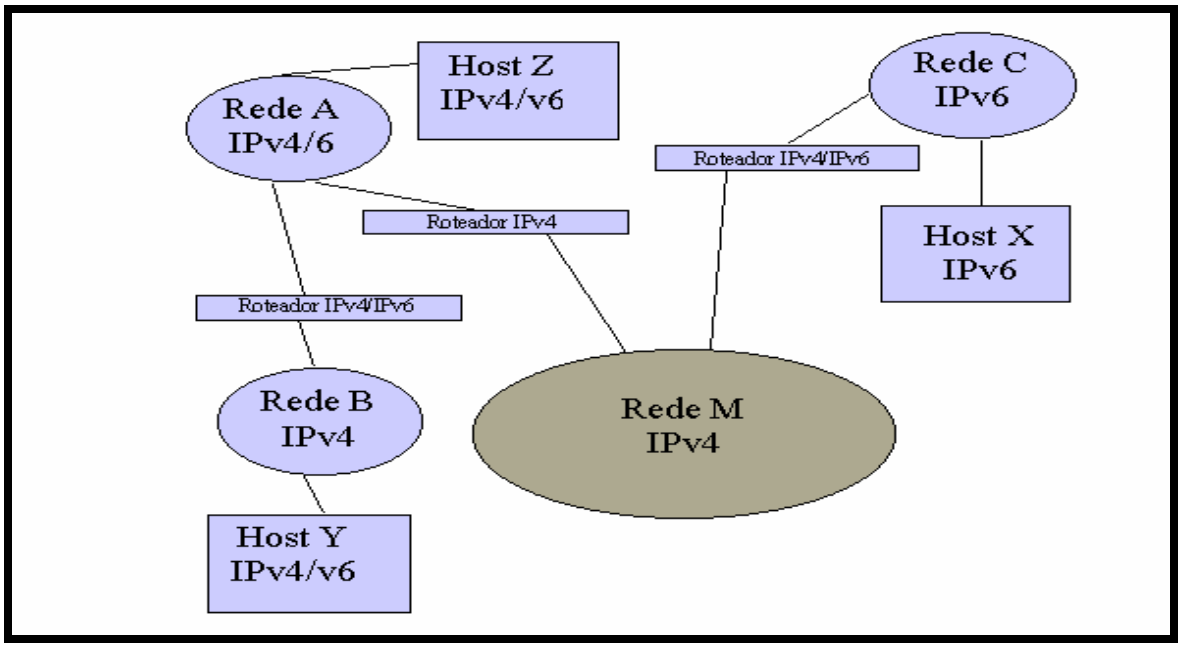
9.1.3. Tunelamento Configurado e Tunelamento Automático

Para TAMUSIUNAS (2006) a diferença entre tunelamento configurado e tunelamento automático está no fato que o tunelamento automático é possível quando os endereços IPv6 dos nodos do túnel são do tipo IPv4 compatível. Os túneis automáticos não requerem configuração para setar os nodos IPv4 do túnel; tunelamento configurado, por sua vez, é utilizado quando algum dos nodos IPv4 das extremidades do túnel recebem o seu endereço IPv4 de alguma maneira dinâmica, como DHCP, sendo necessária uma nova configuração para cada vez que o endereço IPv4 for alterado.

9.1.4. Tipos de Túneis IPv6

Há diferentes tipos de nodos que podem ser a ponta final de um túnel. A Figura 30 será usada como referência para os diferentes tipos de túneis que podem ser estabelecidos.

Figura 30 – Tipos de Túneis



Fonte: TAMUSIUNAS, 11/09/06, internet.

Os diferentes tipos de túneis podem ser:

• Tunelamento roteador a roteador. Na Figura 30, o roteador da rede C e o roteador da rede A trocam pacotes IPv6 utilizando a rede M, que é uma rede que trabalha apenas com IPv4. O host X envia pacotes para o host Z de forma transparente, sendo que nenhum dos hosts precisa saber da existência da rede IPv4 no meio do caminho.

• Tunelamento roteador a host. No caso acima a rede B é uma rede que trabalha apenas com endereços IPv4, porém o host Y utiliza tanto endereços IPv4 quanto endereços IPv6. Este host encontra-se ilhado no meio de uma rede IPv4. Neste caso é feito um túnel deste host em particular, até o roteador *dual-stack*, para que ele possa se comunicar com os demais endereços IPv6 existentes.

• Tunelamento host a host. Supondo que o host Y e o host Z queiram se comunicar, mas que entre eles existam apenas redes IPv4. Neste caso, o tunelamento deve ocorrer apenas entre os hosts Y e Z, para que entre eles sejam transmitidos apenas pacotes IPv4.

9.1.5. Endereços IPv6 do Tipo Compatível-IPv4

Como citado anteriormente, os endereços IPv4 contidos nos endereços IPv6 podem ser de dois tipos: compatível IPv4 e endereço IPv4 mapeado em endereço IPv6. Os endereços do tipo IPv4 compatível têm o objetivo de serem usados em nodos IPv4/IPv6 capazes de fazer tunelamento automático de pacotes IPv6 através de redes IPv4.

Para TAMUSIUNAS (2006) os nodos com *dual-stack* usam o "mesmo" endereço para ambos os pacotes - sejam IPv4 ou IPv6. Nodos que trabalham apenas com IPv4 podem enviar pacotes para nodos *dual-stack* usando endereçamento IPv4, enquanto nodos que trabalham com IPv6 podem enviar pacotes utilizando para isto endereçamento IPv6. Em geral este tipo de nodo poderia ser um roteador conectando redes IPv6 com túneis automáticos, utilizando para isto a rede IPv4. O roteador poderia aceitar endereços IPv6 vindos de sua rede IPv6 local e encapsulá-los em pacotes IPv4 destinado a outro roteador *dual-stack* presente na outra ponta do túnel, também utilizando endereçamento do tipo IPv4 compatível na outra

ponta da rede IPv4. Ao chegarem no outro roteador com *dual-stack*, os pacotes seriam desencapsulados e enviados a rede IPv6 local.

9.1.6. NAT-PT

No caso do IPv4, quando uma organização necessita de vários computadores tendo acesso a internet, ela procura fazer uma requisição de números IP ao órgão responsável pela distribuição destes endereços em um país. Todavia, esta requisição nem sempre é atendida, sendo que às vezes a organização acaba recebendo apenas uma parcela dos endereços que necessita. Para resolver este tipo de problema, foi criada a idéia de NAT (*Network Address Translator*), ou seja, um sistema de tradução de endereços de rede. Na rede interna de cada organização é possível que seja criada uma infra-estrutura de redes utilizando para isto endereços IPv4 privados. Entre a rede interna da organização e a rede Internet, fica uma estação, um firewall, contendo duas interfaces de rede, uma interna, com endereço IPv4 privado, e outra externa, com endereço IPv6 válido. Esta estação é configurada como sendo gateway dos computadores da rede interna, fazendo com que todas as requisições para hosts que se encontrem na internet passem obrigatoriamente por ela. Com isso ela pode enviar as requisições para a Internet, com o seu próprio endereço IP válido, como sendo o originador do pacote. Quando os pacotes chegam são enviados para as estações que o requisitaram. Isto pode ser feito tendo-se uma tabela interna com um endereço IP associado para cada estação, ou tendo-se um endereço IP associado a várias estações. Quando tem-se um endereço IP para cada estação, pode-se acessar esta estação de fora da rede interna caso contrário, com um endereço IP para várias estações, isto não é possível.

Conforme TAMUSIUNAS (2006), em outubro de 1999, foi apresentado na Data Communications, por Pete Loshin, nos Estados Unidos, uma solução para resolver problemas relacionados a estações que poderiam não suportar IPv6 em suas aplicações. Esta solução foi chamada de NAT-PT, ou seja, tradução de endereços de rede - tradução de protocolos. Sua idéia é bem similar a realizada com NAT nas redes IPv4. A rede IPv6 ficaria do lado de fora, enquanto que a rede IPv4 ficaria na rede interna. A interface externa desta *firewall* ficaria com um endereço IPv6 válido, enquanto que a interna ficaria com endereço IPv4. No *firewall* ficaria uma tabela relacionando um endereço IPv6 para cada endereço IPv4 existente na rede interna - desta maneira seria possível mapear todas as estações que trabalhem com IPv4. A tarefa deste *firewall* não seria simplesmente repassar os endereços IPv6 que chegam para os

IPv4 que estão no outro lado, mas convertê-los para este protocolo. O caminho inverso aconteceria também quando os pacotes requisitados retornassem. Este tipo de solução se mostrará extremamente útil no caso de aplicações com dificuldades de serem convertidas para o novo protocolo, ou então no caso de aplicações críticas, que necessitem de mais tempo para serem adaptadas e devidamente testadas, como aplicações militares, científicas e sistemas bancários.

9.2.FERRAMENTAS PARA TRABALHAR COM IPv6

De muito pouco adianta uma rede sem aplicações para que se possa testar seu funcionamento. O Kame Project é um projeto responsável pelo desenvolvimento de aplicações IPv6, sendo estas para os mais diferentes sistemas operacionais.

As aplicações mais básicas de uma rede, como telnet, FTP e HTTP já estão disponíveis para a maioria dos sistemas operacionais com suporte a IPv6, o que permite que haja testes comparativos de desempenho, neste ponto, entre os dois protocolos.

9.2.1. SMTP

O protocolo SMTP (*Simple Mail Transport Protocol*) já foi adaptado para poder trabalhar com o IPv6. O programa que sofreu estas adaptações foi o Sendmail. Este programa, nas suas mais recentes versões (8.10.x), já pode utilizar os recursos de uma rede IPv6, caso ela exista. Este programa já trabalha com a idéia de *dual-stack*, ou seja, quando um programa tenta utilizar uma rede IPv6 utiliza o endereço IPv6 da interface, quando deseja utilizar a rede IPv4, utiliza o endereço IPv4 da interface.

9.2.2. Serviço de Nomes para IPv6

O DNS (*Domain Name Service*), é um serviço importante no que diz respeito a facilidades do uso de aplicações para internet: ele facilita o mapeamento de nomes em endereços IP. O DNS trabalha com a idéia de hierarquia para ajudar a mapear os nomes.

O nome dos hosts pode vir na forma computador.organizacao.com. O host (computador) existe dentro do domínio organização.com. Existem uma série de servidores de nível superior que indicam qual é o servidor responsável pelo domínio organização.com. Quando alguém requisita o endereço host.organizacao.com, o servidor de nomes superior no qual chegou o pedido repassa-o para o servidor responsável, e esse retorna para o requerente o endereço IP deste host, na forma de um endereço de 32 bits. Para que este recurso trabalhe com IPv6 algumas alterações terão que ser feitas. O DNS, como é utilizado hoje, foi projetado para trabalhar com endereços de 32 bits, não podendo por isso, retornar endereços de 128 bits. As alterações descritas em [RFC1886] mostram o que deve ser feito para que o DNS possa suportar o IPv6. As alterações podem ser resumidas da seguinte maneira:

- Criação de um novo tipo de recurso para gravação, chamado de AAAA, para mapear endereços de 128 bits (o tipo de recurso para gravação do IPv4 é o A).
- Criação de um novo domínio (.IP6.int), para permitir que endereços de hosts IPv6 possam servir de base para que chegue ao nome do domínio que responde por eles. Este recurso é parecido com o existente no IPv4 (.in.addr.arpa).

Os servidores de DNS devem ser revisados para localizar ou processar não apenas endereços IPv4, mas endereços IPv4 e IPv6 (caso existam).

9.2.3. HTTP

Um dos servidores adaptado para trabalhar com o protocolo HTTP (*Hyper Text Transport Protocol*), junto com o IPv6, é o Apache. Este programa deve ter um *patch* aplicado para que ele comece a reconhecer o novo protocolo. Assim como o Sendmail, o Apache pode também trabalhar com *dual-stack*.

Para a leitura das páginas existe uma versão adaptada para trabalhar com o IPv6 do Linux, um browser que trabalha em modo terminal.

9.2.4. FTP

O FTP (*File Transport Protocol*) foi um dos primeiros protocolos a serem adaptados para o IPv6. Muitas distribuições de sistemas operacionais já entregam em seus pacotes de atualização para IPv6 um cliente de FTP já adaptado. Como exemplo de servidores já adaptados, pode-se citar o WU-FTP. Este programa possui um *patch* que faz com que ele comece a trabalhar com o novo protocolo, incluindo tecnologias como *dual-stack*.

9.2.5. TELNET

O telnet foi, sem dúvida, uma das principais adaptações, em matéria de ferramentas, para que se pudesse trabalhar com o novo protocolo, o IPv6. Cada sistema operacional se encarregou de produzir o seu próprio telnetd, ou seja, o *daemon* para funcionar como servidor do cliente telnet, que também é produzido de forma exclusiva para sistema operacional.

Segundo TAMUSIUNAS (2006), atualmente já existem adaptadas para o IPv6 uma nova safra de programas que têm a mesma finalidade do telnet, como por exemplo o SSH (*Security Shell*).

9.3.SISTEMAS OPERACIONAIS QUE SUPORTAM IPv6

Hoje em dia, a grande maioria das empresas que fabricam ou distribuem sistemas operacionais se encontram preocupadas em fornecer suporte para que seus produtos trabalhem com o protocolo IPv6. Sistemas operacionais como Linux, FreeBSD, Solaris e AIX se encontram já em uma fase bem adiantada de suporte a IPv6.

Empresas como Microsoft também tem se mostrado interessada em fornecer suporte para que seus sistemas operacionais possam utilizar as vantagens que o protocolo IPv6 proporciona. Os sistemas operacionais Windows 98, Windows NT e Windows 2000 já possuem patches para serem adaptados a trabalhar com IPv6.

9.3.1. Linux

O Linux começou a trabalhar com IPv6 já nas versões 2.1.x do seu *kernel*. Os recursos que ele inicialmente dispunha eram a capacidade de fornecer túneis IPv6 utilizando protocolo IPv4, e reconhecer endereços IPv6 nativos. O Linux possui uma característica que é o fato de não necessitar de *patches* no *kernel* para trabalhar com IPv6, ainda mais quando se utiliza a versão 2.2.x do kernel. Em matéria de alterações, o que necessita ser feito no sistema operacional é a atualização dos arquivos que trabalham com rede, ou seja, os comandos de rede. Os comandos que inicialmente precisam ser atualizados para trabalhar com IPv6 são o ping, route, ifconfig, nslookup e outros.

Uma série de grupos, em muitos lugares do mundo, começaram a desenvolver aplicações para que fosse possível trabalhar com este novo protocolo. Com o lançamento da glibc 2.6, que já vem junto com o RedHat 6.0, começou-se a ter mais recursos para desenvolvimento de aplicações de rede, tendo-se em vista os novos recursos de programação disponibilizados por esta biblioteca.

Entre os países que possuem grupos trabalhado no desenvolvimento de aplicações para o Linux, pode-se citar a Alemanha, os Estados Unidos e o Japão.

9.3.2. Solaris

A Sun, empresa que fabrica o Solaris, lançou, já faz algum tempo, *patches* para que o Solaris7 pudesse trabalhar com o protocolo IPv6. No dia 2 de novembro de 1999, a Sun lançou, nos Estados Unidos, a versão 8 do Solaris, com suporte nativo a IPv6. O Solaris8 é distribuído tanto para plataformas Sparc, como para plataformas x86.

“Muitas das aplicações que rodam em Solaris com suporte a IPv6 são distribuídas pela própria Sun, em pacotes fechados. Estes pacotes já se encontram prontos para a instalação, requerendo apenas a parte de configuração para que possa haver um melhor desempenho dependendo das características da rede que se está utilizando”. (TAMUSIUNAS, 2006).

10. AQUISIÇÃO DE ENDEREÇOS IPv6

Para solicitar um bloco de endereços IPv6 a organização deve preencher o Formulário indicado no ANEXO I e depois enviá-lo para hostmaster@lacnic.net. Depois de verificado e nenhum erro encontrado, um "ticket" será gerado, o qual identificará a solicitação.

Depois de aprovado, um e-mail será enviado com informações sobre o pagamento da alocação inicial e também sobre o Acordo de Serviço de Registro, que precisa ser assinado. A alocação somente será feita uma vez recebido o pagamento e o acordo assinado.

Alocação de blocos adicionais somente serão feitas caso não haja pendências de pagamento ou de documentação.

O bloco mínimo alocado pelo LACNIC é um prefixo de 32 bits e para se qualificar para uma alocação inicial a organização deve:

- Ser um LIR (*Local Internet Registry*), ou seja, organização que designa espaços de endereçamento para usuários dos serviços de rede que ela provê. São, geralmente, os provedores de acesso (ISP), cujos clientes são usuários finais ou outros provedores de acesso;

- Não ser um usuário final;

- Enviar plano detalhado sobre os serviços e conectividade IPv6 a oferecer à outras organizações (clientes);

- Anunciar no sistema de rotas inter-domínios da Internet um único bloco, que agregue toda a alocação de endereços IPv6 recebida, em um prazo não superior a 12 meses.

- Oferecer serviços IPv6 a clientes localizados fisicamente na região do LACNIC em um prazo não superior a 24 meses.

10.1.SOLICITANDO BLOCO ADICIONAL

Alocações adicionais serão concedidas quando a organização (ISP/LIR) alcançar uma boa taxa de utilização do último bloco alocado. A taxa de utilização será calculada em termos de blocos de prefixo /48 designados para usuários finais.

Para calcular a taxa de utilização será utilizado a metodologia HD-Ratio RFC3194 . E segundo essa metodologia, uma taxa de 0.8 é considerada aceitável em termos de utilização de endereçamento e justificaria uma alocação adicional.

LACNIC utilizará as informações sobre designações registradas no WHOIS para calcular o índice utilização HD-Ratio. Caso a organização comprove uma boa utilização do espaço anteriormente alocado, segundo o critério mencionado, essa estará apta a receber um novo espaço de endereçamento de tamanho igual ao alocado anteriormente.

Sempre que for possível, o espaço adicional a ser alocado para uma organização será adjacente ao último espaço alocado. Organizações solicitando blocos de endereços devem estar cientes da existência de uma tarifa de renovação do serviço de registro dos recursos alocados pelo LACNIC.

11. CONCLUSÃO

Os estudos demonstraram que a implantação do protocolo IPv6 é necessária e inevitável.

O IPv4 não supri o número de endereços IP necessários para o crescimento da internet nem mesmo possibilita a implantação de novos serviços.

O Ipv6 com seus 128 bits de endereçamento possibilita aceitar bilhões de hosts através da expansão do espaço de endereçamento e uma hierarquia mais versátil, como também a implantação de vários serviços. Criou um campo que suporta mecanismos de controle de qualidade de serviço, gerando maior sensibilidade ao tipo de serviço, como, por exemplo, serviços de tempo real. Fez melhorias no roteamento, inclusive no que tange a hosts móveis e permite que máquinas móveis (wireless) mudem de lugar sem necessitar de mudanças em seus endereços IP.

A camada do Protocolo de Resolução de Endereços desaparece e esta função é desempenhada pelo Protocolo Neighbor Discovery contido no ICMPv6 através do mecanismo Neighbor Solicitation.

Com o esgotamento dos endereços IP prevista para os próximos anos o maior desafio será conseguir uma forma eficiente e segura para fazer a transição, preparando a rede para a implantação total do IPv6. Com a criação dos dispositivos como Túneis, pilhas duplas e outros tem-se a expectativa que o Ipv6 de forma lenta e gradual conseguirá atingir os objetivos pretendidos, mas somente com uma implantação mais robusta deste protocolo poderá se ter certeza de sua real eficiência.

Sugere-se a implantação de um Host com endereço IPv6 para comprovar seu funcionamento, fazendo testes de segurança, QoS, roteamento entre outros com endereços IPv4 e repetindo os testes com endereços IPv6 comparando os resultados.

ANEXO I - Formulário para solicitar um bloco de endereços IPv6.

```
#   Não remover o numero da versão.
LACNIC IPV6 Template 20060503-2-PT

#   Envie este formulário para hostmaster@lacnic.net

#   Dados da Organização.
#   Se a organização já possui algum recurso registrado com
#   LACNIC, informe somente o "OwnerID" e o nome da Organização
#   assim como esta registrado em nosso sistema. Caso não
#   recorde o "OwnerID", consulte algum recurso alocado a sua
#   organização utilizando o servidor WHOIS de LACNIC:
#   http://whois.lacnic.net

0a. ID. da Organização (OwnerID):
0b. Nome da Organização:
0c. Endereço Postal:
0d. Cidade:
0e. Estado:
0f. Pais:
0g. Código Postal:

#   Pontos de contato na organização.
#   Será necessário informar contato técnico, de cobrança e
#   de membro.
#   Os contatos de cobrança e de membro são internos e por
#   isso não são visíveis nas consultas whois.
#   Informar somente o "UserID" dos ponto de contato.
#   Caso não existam ainda, estes devem ser criados em:
#   http://lacnic.net/newid/PT

1a. ID. contato técnico (UserID):
1b. ID. contato cobrança (UserID):
1c. ID. contato membro (UserID):

#   Fornecer informação sobre a organização que esta'
#   solicitando o bloco IPv6.

2a. Informação da Organização:

#   Conexão Internet.
#   Informar nome do provedor, seu endereço postal, seu ASN
#   e estado da conexão com este provedor.
#   Copie os campos abaixo caso tenha mais de um provedor.

3a. Nome do provedor:
3b. Endereço Postal:
3c. ASN do provedor:
3d. Estado da conexão:

#   Fornecer informação sobre o plano para lançamento da
#   rede IPv6, plano de utilização dos endereços IPv6 e
#   plano de sub alocações dos endereços IPv6 para os
#   clientes.

4a. Data:
4b. Plano de utilização:
4c. Plano de alocação:
```

```
#   Fornecer informação sobre a estrutura da rede IPv6
#   e tipo de serviços a serem oferecidos aos clientes.
#   No caso em que se esta solicitando um prefixo maior que
#   /32, fornecer informação que justifique esta necessidade.

5a.  Informação Adicional:

#   Não remover esta linha.
Fim do formulário
```

REFERÊNCIAS BIBLIOGRÁFICAS

1. ALBUQUERQUE, Fernando. **TCP/IP INTERNET**. Protocolos & Tecnologias. 3 ed. (pg 21 e 58). Rio de Janeiro: Axcelbooks do Brasil, 2001.
2. ALECRIM, Emerson. **Endereços IP (Internet Protocol).** Disponível em: http://www.infowester.com/internetprotocol.php. Acesso em 10/08/06.
3. _____. **IP estático e IP dinâmico**. Disponível em: http://www.infowester.com/internetprotocol.php Acesso em 10/08/06.
4. BATTISTI, Julio. **TCP/IP.** Disponível em : http://www.juliobattisti.com.br/artigos/windows/tcpip_p1.asp. Acesso em: 20/08/06.
5. BERNAL FILHO, Huber. **IPv6: Endereço e Roteamento**. Disponível em: http://www.teleco.com.br/tutoriais/tutorialipv6/pagina_2.asp. Acesso em: 12/08/06.
6. BOGO, Kellen Cristina. **A História da Internet.** Disponível em: http://kplus.cosmo.com.br/materia.asp?co=11&rv=Vivencia. Acesso em: 02/09/06.
7. COSTA, Julio Gustavo Soares Firmo da. Fialho. VIANNA, Sérgio. **Implementação de um mecanismo de tradução de protocolos (IPV4 e IPV6).** Disponível: http://www.rnp.br/newsgen/0303/trad_protocolo.html. Acesso em: 27/09/06.
8. FUNDAÇÃO PARA A COMPUTAÇÃO CIENTÍFICA NACIONAL (FCCN) **. IPv6 – RCTS.** Disponível em: http://www.fccn.pt/index.php?module=pagemaster&PAGE_user_op=view_page&PAGE_id=118. Acesso em: 27/09/06.
9. IDG Now. **Mundo atinge 1 bilhão de usuários de internet**. Disponível em:. http://idgnow.uol.com.br/internet/2006/05/19/idgnoticia.2006-05-19.2158242015/IDGNoticia_view. Acesso em: 15/09/06.
10. LACNIC: Registro de Endereços da Internet para América Latina e Caribe**. Como conseguir endereços IPv6.** Disponível: http://lacnic.net/pt/registro/ipv6.html. Acesso em: 20/09/06.
11. MARTINI, Fernando Zucuni. BOGO, Madianita. **Análise e Proposta de Implantação de um Ambiente de Rede utilizando o Protocolo IPv6.** Disponível em: http://www.ulbra-to.br/ensino/43020/artigos/anais2003/anais/ipv6-encoinfo2003.pdf#search=%22implanta%C3%A7%C3%A3o%20de%20rede%20baseada%20em%20IPv6%22. Acesso em: 27/09/06.

12. MOREIRA, André. **Internet Protocol Versão 6 (IPv6).icmpv6**. Disponível: http://www.dei.isep.ipp.pt/~andre/documentos/ipv6.html. Acesso em: 13/09/06.
13. NUNES, Cristina. **História do Protocolo Ipv6**. Disponível em: http://www.inf.pucrs.br/~cnunes/cdt/aulas/IPv63.pdf#search=%22ICMPv6%20%22 Acesso em: 17/09/06.
14. SMETANA, George Marcel M. A. **IPv4, IPv6 e ICMPv4**. Disponível em: http://www.redes.usp.br/conteudo%5C%5Cdocumentos%5CArtigoIP.pdf#search=%22ICMpv6%22. Acesso em: 17/09/06.
15. TAMUSIUNAS, Fabrício Raupp. **Comparação entre Ipv4 e Ipv6**. Disponível em: http://gtrh.tche.br/ovni/ipv6/modelo2_introducao.htm. Acesso em: 19/09/06.
16. _____. **Estratégias de transição para IPv6**. Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo4_introducao.htm. Acesso em: 08/09/06.
17. _____. **Aproximação de Redes IPv6 Utilizando Túneis.** Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo4_aproximacaoredesipv6utilizandotuneis.htm Acesso em: 11/09/06.
18. _____. **Tunelamento Configurado e Tunelamento Automático** Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo4_tunelamentoconfiguradotunelamentoautomatico.htm. Acesso em: 06/09/06.
19. _____. **Endereços IPv6 do Tipo Compatível-IPv4.** Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo4_enderecosipv6tipocompativel-ipv4.htm. Acesso em: 13/09/06.
20. _____. **NAT-PT** Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo4_napt-pt.htm Acesso em 21/09/06.
21. _____. **Ferramentas para Trabalhar com IPv6** Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo4_ferramentastrabalharipv6.htm. Acesso em: 13/09/06.
22. _____. **Tipos de Túneis IPv6.** Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo4_tipostuneisipv6.htm. Acesso em: 13/09/06.
23. _____. **Sistemas Operacionais que Suportam IPv6** Disponível em: http://gtrh.tche.br/ovni/ipv6/modulo5_conclusao.htm. Acesso em: 14/09/06.
24. TUDE, Eduardo. **Usuários Domiciliares de Internet.** Disponível em: http://www.teleco.com.br/internet.asp. Acesso em: 25/09/06.