UNIVERSIDADE PRESBITERIANA MACKENZIE

ALESSANDRO NUCCI DE SIQUEIRA

REDES IPv6 E ESTRATÉGIA DE IMPLEMENTAÇÃO

São Paulo

2011

ALESSANDRO NUCCI DE SIQUEIRA

REDES IPv6 E ESTRATÉGIAS DE IMPLEMENTAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Especialização em Engenharia de Telecomunicações da Universidade Presbiteriana Mackenzie, como requisito parcial para a obtenção do grau de Especialista.

ORIENTADOR: Prof. Esp. Gerson Estevão

São Paulo

2011

AGRADECIMENTOS

Aos meus pais José Expedito de Siqueira e Ana Lucia Nucci os meus profundos agradecimentos pelo apoio, incentivo para realização de mais esta etapa da minha vida.

Às minhas irmãs Agnes Aparecida Pereira e Juliana Nucci de Siqueira e ao meu sobrinho Christian Pereira de Godoi pelo apoio.

À todos os amigos do curso de Especialização em Engenharia de Telecomunicações em especial Maurício Lomba, Paulo Leite, Thiago Praconi e Victor Arroio.

À Prof.ª. Dra. Melanie, por me ajudar com o desenvolvimento deste trabalho na disciplina de Metodologia.

Ao meu orientador Prof. Esp. Gerson Estevão, pelo apoio, dedicação e compreensão durante todas as etapas deste trabalho.

E principalmente à Deus, fonte de toda sabedoria, pela força e pela coragem que me concedeu, permanecendo ao meu lado em todo o percurso desta caminhada.

Nós somos o que repetidamente fazemos, excelência portanto, não é um ato, mas um hábito (Aristóteles).

RESUMO

A Internet teve um crescimento muito acelerado nos últimos anos, fatores como surgimento de novas tecnologias, a popularização dos dispositivos móveis, e a disseminação das redes sócias contribuíram muito para esse aumento e com isso a necessidade por endereçamento IP (*Internet Protocol*). Esse crescimento não era previsto no projeto original, já que na época a Internet foi desenvolvida para uso militar e acadêmico. Contudo na década de 90, já era previsto o esgotamento do endereçamento IPv4, onde soluções paliativas foram desenvolvidas e aplicadas com intuito de diminuir a necessidade por endereçamento IP público e tendo como principal tarefa não impactar no crescimento da Internet e de novas tecnologias. Mediante a esta situação projetos foram iniciados paralelamente buscando desenvolver o novo protocolo, esses projetos deram resultado e em pouco tempo surgia à nova versão do protocolo IP, mas conhecida como IPv6. Devido a esse crescimento, é ao esgotamento do endereçamento IPv4, a adoção do novo protocolo IPv6 passou a fazer parte da nossa realidade. Além de produzir um bom material de estudo sobre os protocolos abordados, outro objetivo deste trabalho foi ressaltar as técnicas de migração. Assim, por meio de pesquisa e estudo (leitura de livros, tutoriais, sites e RFC), foram apresentados neste trabalho um estudo introdutório sobre o protocolo TCP/IP e o protocolo IPv4 e um estudo detalhado do protocolo IPv6, apresenta suas características técnicas, serviços oferecidos e realiza uma análise comparativa das vantagens e desvantagens da adoção entre os dois protocolos e as estratégias de migração para o IPv6.

Palavra chave: Protocolos de Internet. Evolução. Protocolo IPv6. Migração. Redes de computadores.

ABSTRACT

Internet has shown a very fast growing rate in the past years, the factor that new Technologies, mobile devices and the dissemination of social networks arrived to the market, contributed quite a lot with the growth and the necessity for the IP address came along. Such development was not expected in the original project, since the internet was developed for military and academic purposes. However, they predicted the IPv4 would be running out of new addresses during the 90's, when new solutions came up and were applied to try to reduce the need for public IP addresses, so that it wouldn't impact the internet growth as well as upcoming technologies. Due to this situation, new projects started to be developed in parallel to create a new protocol. These projects were very successful and in a short period of time they generated a new IP protocol, also known as IPv6. With the unstoppable progress and the lack of IPv4, the acceptance of the new protocol turned into reality. The goal of this project was not only to provide a good study about the protocols, but also to point out migration techniques. Thus, through researches and studies (reading books, tutorials, websites and RFC), an introductory presentation over the TCP/IP, IPv4 and also a very detailed IPv6 research to present its technical characteristics, available services and performing an analysis of advantages and disadvantages between the two protocols and the migration strategies to the IPv6.

Keywords: Internet protocols. Progress. IPv6 Protocol. Migration. Computer networks.

LISTA DE GRÁFICOS

LISTA DE ESQUEMAS

SUMÁRIO

1 INTRODUÇÃO

No final da década de 60, o governo dos Estados Unidos se deparou com a necessidade interligar centros militares e de pesquisas, já que a tensão criada pela Guerra Fria era conturbadora. Com isso torna-se real a necessidade de ter um modelo de rede de comunicação, que proporciona-se mais segurança, eficiência e redundância.

Tendo como principal tarefa, na década de 70, centros de pesquisas e o Departamento de Defesa, começaram a trabalhar em projetos de comunicação e interligação dos computadores dos centros militares e de pesquisa, posteriormente essa rede recebeu o nome de ARPANET, tudo isso era possível com a utilização e combinação de vários protocolos de comunicação.

Porém para garantir o futuro da ARPANET, foi necessário realizar algumas mudanças e planejar um crescimento ordenado e escalável para rede, com isso o protocolo TCP/IP torna-se o único protocolo utilizado já que ele oferecia um modelo hierárquico e totalmente flexível (ATAKAN et al., 2000; FILIPPETTI, 2006).

Nos anos seguintes a ARPANET cresceu e se dividiu em duas frentes sendo uma voltada para o seguimento militar e outra para o segmento acadêmico, e no início dos anos 90 o segmento acadêmico foi desativado e no seu lugar surgia a Internet.

Já na década de 90, o crescimento alcançado pela Internet era espantoso e com isso possibilitou a identificação de problemas na pilha de protocolo TCP/IP, já que o projeto original previa o uso incialmente militar e acadêmico, e não a utilização em escala global. O principal problema mapeado foi o esgotamento do endereçamento IPv4, onde foi necessário a adoção de soluções paliativas que amenizaram o problema, porém ficou aparente a necessidade de uma nova versão do protocolo para corrigir falhas do seu antecessor e com plano um novo plano de endereçamento.

Com isso os principais órgãos responsáveis pela regulamentação da Internet no mundo, iniciaram paralelamente vários projetos de pesquisa onde tempos depois surgia a nova versão do protocolo IP, mas conhecida como IPv6. Conforme observado nos parágrafos anteriores, torna-se necessário a utilização da nova geração do protocolo IP, para melhorar requisitos de desempenho, segurança e permitindo o crescimento da Internet e o desenvolvimento de novas tecnologias.

Praticamente todas as redes e dispositivos móveis disponíveis atualmente oferecem suporte ao protocolo IPv4, porém apenas uma pequena fatia desse mercado já traz suporte nativo a nova versão do protocolo o IPv6, com isso não e possível a agregação em

grande escala, faz-se necessário efetuar a transição em etapas adotando técnicas e estratégias para manter as redes IPv4 operacionais paralelamente com as redes IPv6 e naturalmente irá ocorrer a substituição o futuro acontecerá a substituição (DEERING; HINDEN, 1998, tradução nossa; HANGEN, 2002, tradução nossa).

O objetivo geral deste trabalho é analisar o principal protocolo de comunicação utilizado atualmente na Internet, o protocolo IP, apresentar de forma clara e objetiva suas limitações, a nova versão, e realizado um comparativo entre versões e descrevendo as principais técnicas de implantação da nova versão disponíveis no mercado.

A metodologia escolhida para realização deste trabalho foi à pesquisa de normas e documentações técnicas, disponibilizado por órgãos nacionais, internacionais e governamentais e o estudo de materiais (livros, fóruns, sites), que disponibilizavam conceitos básicos de redes de comunicação, computadores e detalhados de cada protocolo de Internet.

A presente monografia foi estruturada em seis capítulos, tendo como primeiro capítulo a introdução do estudo, aonde e descrito o objetivo, a justificativa e a metodologia utilizada para desenvolvimento do trabalho.

A história do protocolo TCP/IP e o modelo de comunicação utilizado são brevemente tratados no segundo capítulo, O Protocolo TCP/IP.

No terceiro capítulo, Protocolo IPv4, e descritivo as versões do protocolo, as características, as funcionalidades e o maior problema do IPv4, o esgotamento de endereçamento IP.

O quarto capítulo, O Protocolo IPv6, traz um estudo mais detalho da nova versão do protocolo IP, descrevendo suas características e as novas funcionalidades.

Uma análise evolutiva entre as versões do protocolo e as estratégias de migração para nova versão são descritas, no quinto capítulo, Análise e estratégias de migração para IPv6.

Finalmente, o capítulo seis é composta pela conclusão e considerações finais.

2 PROTOCOLO TCP/IP

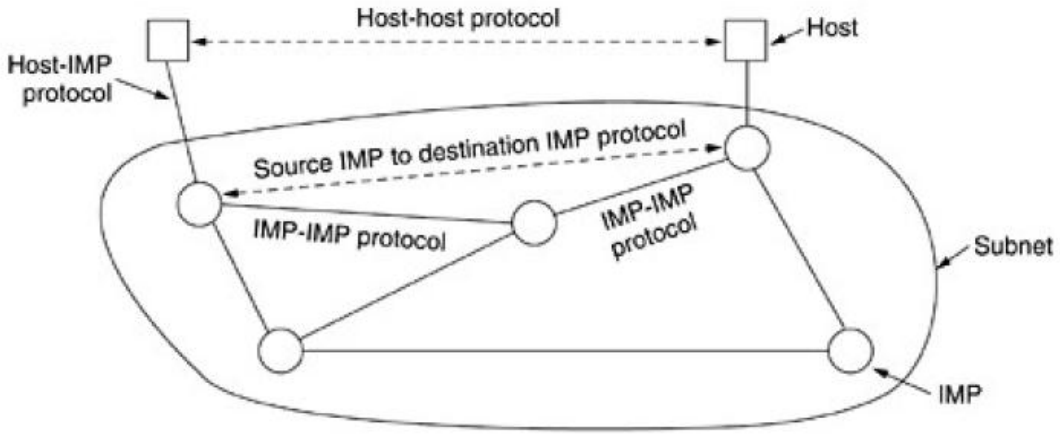
O Protocolo de Controle de Transmissão (TCP – *Transmission Control Protocol*) e o Protocolo de Internet (IP – *Internet Protocol*) fazem parte de uma família de protocolos utilizados na Internet. Onde a principal função e a especificação de padrões que permitem a comunicação de computadores, compartilhamento de arquivos e a interconexão de redes de computadores através de técnicas de roteamento (STARLIN, 2001).

2.1 HISTÓRIA DO TCP/IP

Na década de 60, Agência de Projetos de Pesquisas Avançadas (ARPA - *Advanced Research Projects Agency*) dos EUA iniciou um projeto para o desenvolvimento de uma rede de comutação de pacotes que fosse confiável, redundante, robusta e independente até certo ponto de falhas e totalmente de fabricante (HUNT, 2002, tradução nossa).

Na década seguinte o Departamento de Defesa (DOD – *Departament of Defense*) dos EUA financiou um projeto de interligação dos computadores dos centros militares e de pesquisa, recebendo o nome de ARPANET. Para que o projeto pudesse progredir era necessário um modelo de protocolo que tivesse a garantia de funcionalidades esperadas, sendo flexível e de fácil escalabilidade (SANTOS; MOREIRAS; ROCHA, 2010). No esquema 1 e apresentando o projeto original da ARPANET (TANENBAUM, 2003).

O Projeto Original da ARPANET



Esquema 1: O Projeto Original da ARPANET.

Fonte: Tanenbaum, 2003.

Segundo Starlin (2001), o DOD em parceria com universidades, agências e pesquisadores civis e militares desenvolveram um conjunto de programas que padronizam um sistema de comunicação esse denominado como protocolo e chamado de TCP/IP. Porém no início a ARPANET trabalhava com diversos protocolos, porém quando chegou à marca de 562 hosts o protocolo TCP/IP foi adotado como padrão, permitindo o crescimento ordenado da rede e eliminando limitações apresentadas por protocolos anteriores (SANTOS; MOREIRAS; ROCHA, 2010).

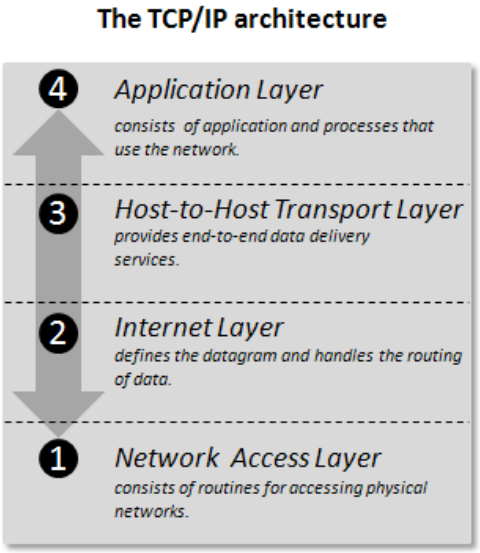
Durante a década de 80, o TCP/IP começou a ser usado em larga escala e o termo Internet entrou em uso comum. A ARPANET foi dividida em MILNET para órgãos militares, sendo a parte sem classificação para Rede de Defesa de Dados (DDN – *Defense Data Network*) e uma nova ARPANET com proporções menores. O Termo "Internet" passou referenciar toda rede.

Em 1985, a Fundação Nacional de Ciência (NSF – *National Science Foundation*) criou NSFNet e a conectou a internet existente. Logo depois interligou cinco centros de supercomputadores da NSF, mesmo sendo uma rede menor que a ARPANET. O principal papel era estender os serviços oferecidos para cientistas e engenheiros de todo território americano e para isso adotou uma topologia de rede em três níveis, que incluiu o *backbone*, redes regionais e redes locais. Em 1990, a ARPANET formalmente desativada para o surgimento da Internet (HUNT, 2002, tradução nossa).

2.2 MODELO TCP/IP

Uma característica bastante importante do TCP/IP é a sua flexibilidade. Ele permite fácil adaptação às tecnologias de redes existentes e futuras. Tudo isso e possível porque o modelo do TCP/IP foi concebido em camadas que trabalham de forma independente (STARLIN, 2001).

O esquema 2 apresenta arquitetura TCP/IP também conhecido como modelo TCP/IP ou DOD (HUNT, 2002, tradução nossa).



Esquema 2: *The* TCP/IP *architecture*.
Fonte: Hunt, 2002.

Para Filippetti (2006), o modelo TCP/IP está constituída, de forma geral, por quatro camadas, cujas funções principais são:

- **Camada de Aplicação** *(Application Layer)***:** Está camada inclui as particularidades e funções das camadas de Aplicação, Apresentação e de Sessão do modelo OSI e trabalha com os protocolos de mais alto nível, fornecendo serviço que permitem a comunicação estação a estação pelas aplicações e o controle específico por parte do desenvolvedor ou usuário. Protocolos como Telnet, FTP, TFTP, NFS, SMTP, LDP, X Window, SNMP e DNS, são exemplos de algumas aplicações.
- **Camada de Transporte** *(Host-to-Hots Transport Layer)***:** Está camada tem as mesmas particularidades e funções da camada de Transporte do modelo OSI, dispondo de protocolos que permite a transmissão confiável com sequenciamento de pacotes de dados transmitidos ou simplesmente a transmissão não confiável de dados para as aplicações. O Protocolo de Controle de Transmissão (TCP – *Transmission Control Protocol*) permite a transmissão orientada a conexão, multiplexação de portas, confiabilidade, controle de fluxo e recuperação de erros. Porém todas essas tarefas fazem com que aplicações que utilizem o TCP demandem de

mais processamento e com isso aumenta sensivelmente o tempo transmissão de dados na rede; Protocolo de Datagrama do Usuário (UDP – *User Datagram Protocol*) permite a transmissão não orientada a conexão e multiplexação de portas. Isso e uma vantagem com relação ao TCP, pois não demanda de tanto processamento e transmite dados mais rapidamente na rede. Aplicações de Voz sobre IP (VoIP – *Voice Over IP*) são exemplos que utilizam o protocolo UDP. Esses são os principais protocolos desta camada (ODOM, 2007, tradução nossa).

- **Camada de Rede** *(Internet Layer)***:** Está camada tem as mesmas particularidades e funções da camada de Rede do modelo OSI, sendo responsável pelo endereçamento lógico, roteamento e definição de caminhos após designação dos endereços IP. O principal protocolo que opera nesta camada e o Protocolo de Internet (IP – *Internet Protocol*) atualmente rodando nas versões 4 (IPv4) e versão 6 (IPv6) onde são responsáveis por endereçar e rotear pacotes entre computadores e segmentos de rede locais ou remotos (HUNT, 2002, tradução nossa).
- **Camada de Host a Rede** *(Network Access Layer)***:** Está camada inclui as particularidades e funções das camadas de Enlace de Dados e Física do modelo OSI, na primeira parte ela descreve um conjunto específico de regras ou protocolos que definem cabeçalho e rodapé para os mesmos conforme a mídia de transmissão definida (NORTHRUP; MACKIN, 2009, tradução nossa). A segunda parte tem a função de identificar vários padrões que lidam com as características físicas da mídia de transmissão escolhida incluindo modelos de conectores e sequencia de ligação, corrente elétrica, modulação de luz, e parâmetros que possibilitam a ativação ou desativação da mídia (ODOM, 2007, tradução nossa).

3 PROTOCOLO IPv4

O Protocolo IP, definido pela RFC 791, foi concebido para possibilitar a interligação de sistemas que possibilitam a comunicação por comutação de pacotes em uma rede de computadores. Essa comunicação acontece através de blocos de dados que podem ser transmitidos via datagrama onde os *hosts* de destino e o de origem, devem ser identificados por endereçamento lógico de comprimento fixo, função do protocolo IP. Caso esse datagrama ultrapasse um tamanho pré-definido o mesmo sofre uma fragmentação e remontagem de datagramas quando entregue ao seu destino. O protocolo IP passa a ser conhecido um protocolo de melhor esforço onde o mesmo não oferece confiabilidade, nem controle de fluxo ou sequenciamento, essas funções são atribuídas aos protocolos da camada de transporte (POSTEL, 1981, tradução nossa).

3.1 VERSÕES DO PROTOCOLO IP

Atualmente existem duas versões do protocolo IP, a versão 4 publicado pela RFC 791, conhecida como IPv4 sendo a mais utilizada atualmente e a versão 6 publicado pelas RFC 2373 e 2460 ou simplesmente IPv6, já foi desenvolvida há alguns anos e se encontra em fase de implantação por todo o mundo, com a finalidade de substituir a versão anterior trazendo melhorias de operação, segurança.

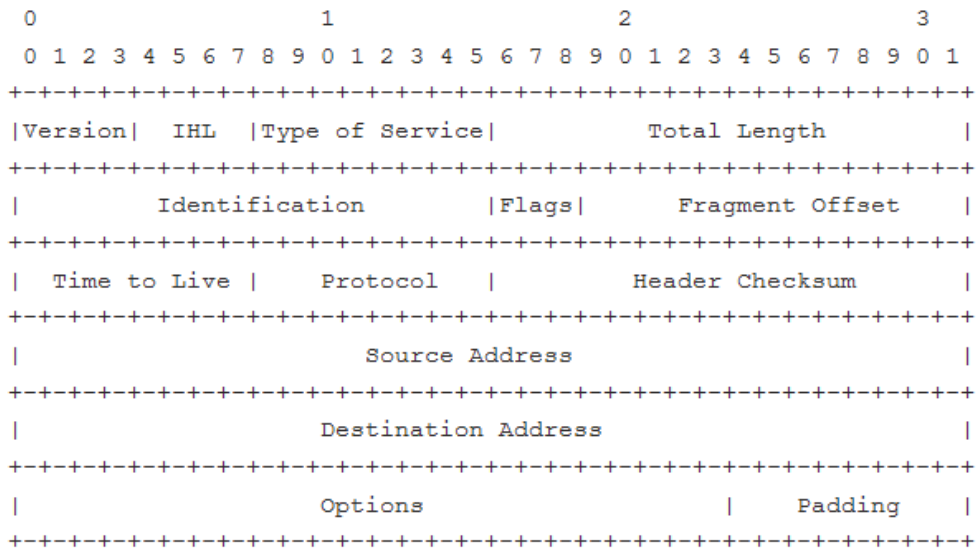
3.2 FUNCIONABILIDADES DO PROTOCOLO IPv4

A função do IPv4, definido pela RFC 791 e mover datagramas por um grupo de redes interconectadas, encaminhando os módulos por cada segmento até que o seu destino seja alcançado, tendo como características (HUNT, 2002, tradução nossa; POSTEL, 1981, tradução nossa):

3.2.1 Cabeçalho IPv4

Podemos considerar que o cabeçalho IPv4 consiste em duas partes sendo uma para o cabeçalho com tamanho fixo de 20 bytes e outra parte para dados com tamanho

variável (TANENBAUM; WETHERALL, 2011). O esquema 3 demonstra o formato do cabeçalho (POSTEL, 1981, tradução nossa):



Esquema 3: *Internet Datagram Header*.

Fonte: Postel, 1981.

- **Versão** (*Version*)**:** Define a versão do protocolo, atualmente a versão 4, tamanho de 4 *bits*.
- **IHL:** Informa o seu tamanho em palavras de 32 bits. Onde o valor mínimo e 5,quando não há nenhuma opção presente, tamanho de 4 *bits*.
- **Tipo de Serviço** (*Type of Service*)**:** Indica a qualidade do serviço tamanho de 8 *bits*. É destinado a identificar classes de serviços permitindo várias combinações entre velocidade e confiabilidade.

  Os primeiros 3 *bits* (*Bits* 0-2) definem as seguintes:

  Precedências

  - 000 – Rotina;
  - 001 – Prioridade;
  - 010 – Imediato;
  - 011 – Flash;
  - 100 – Anulação do Flash;
  - 101 – Crítico;
  - 110 – Controle;
  - 111 – Controle de Rede;

  Os 3 *bits* (*Bits* 3-5) seguintes definem:

Tipo de Serviço

- 0000 – Serviço Normal;
- 0001 – Baixo custo;
- 0010 – Alta confiabilidade;
- 0100 – Alto Rendimento;
- 1000 – Baixo atraso;

Os dois últimos *bits* (*Bits* 6-7) foram reservados para uso futuro (ATAKAN et al., 2000; POSTEL, 1981; TANENBAUM; WETHERALL, 2011).

- **Comprimento Total** (*Total Length*)**:** Inclui todo o datagrama, considerando cabeçalho mais os dados onde seu tamanho máximo e de 65.535 bytes, tamanho de 16 *bits*.
- **Identificação** (*Identification*)**:** Valor único para identificação do pacote onde todos os fragmentos de um datagrama têm o mesmo valor, tamanho de 16 *bits*.
- ***Flag*****:** Define se a fragmentação deve ou não ocorrer, tamanho de 3 *bits*. Onde as opções deste campo são (ATAKAN et al., 2000)**:**
  - 0 – Reservado
  - DF – Não fragmentar.
  - MF – Mais fragmentos.
- **Deslocamento do Fragmento** (*Fragment Offset*)**:** Garante a fragmentação e remontagem de um pacote se o mesmo for muito extenso e estiver dentro de um único quadro (*frame*). E possível também definir diferentes Unidades Máximas de Transmissão (MTU – *Maximum Transmission Units*), tamanho de 13 *bits* (FILIPPETTI, 2006; POSTEL, 1981, tradução nossa).
- **Tempo de Vida** (*Time to Live*)**:** E considerado um contador para limitar o tempo de vida útil do pacote no máximo de 255 segundos, caso o mesmo chegue a marca de 0 ele é descartado e um pacote advertência e enviado para o *host* de destino. Isso técnica ajuda a prevenir *loopings* na rede, tamanho de 13 *bits* (POSTEL, 1981, tradução nossa; TANENBAUM; WETHERALL, 2011).
- **Protocolo** (*Protocol*)**:** Carrega o número do protocolo de camada superior para quem o IP irá entregar os dados contidos no pacote, tamanho de 8

bits. Alguns dos números mais importantes são (ATAKAN et al., 2000; POSTEL, 1981, tradução nossa).

- 0 – Reservado;
- 1 – ICMP;
- 4 – IP;
- 6 – TCP;
- 17 – UDP;
- 41 – IPv6;

- **Verificação de Soma** (*Header Checksum*)**:** Um algoritmo de soma e verificação e aplicada apenas ao cabeçalho, assumindo que o valor do *checksum* seja 0. Se o valor do *checksum* não for igual ao do conteúdo o datagrama e descartado, tamanho de 16 *bits* (ATAKAN et al., 2000; POSTEL, 1981, tradução nossa).
- **Endereço de Origem** *(Source Address***):** Carrega o endereço IP de origem, tamanho de 32 *bits*.
- **Endereço de Destino** (*Destination Address*)**:** Carrega o endereço IP de destino, tamanho de 32 *bits*.
- **Opções** (*Options*)**:** Foi concebido inicialmente para execução de testes de rede suportando versões posteriores do protocolo, tamanho variável (TANENBAUM; WETHERALL, 2011).
- ***Padding*:** Caso seja usada alguma opção, o datagrama será preenchido com zeros ate a próxima palavra de 32 *bits*, tamanho variável.

3.2.2 Endereçamento IPv4

Segundo Filippetti (2006) o endereço IPv4 e um endereçamento lógico que foi concebido para permitir a comunicação de dispositivos em redes distintas independentes das tecnologias de “Camada de Host a Rede” envolvidas, atuando como um identificador numérico único atribuído a cada dispositivo conectado a uma rede IPv4, isso permite identificar de maneira única um dispositivo em uma rede local ou na Internet.

Os endereços IPv4 são hierárquicos e compostos de 32 bits, divididos em duas partes: A primeira parte e designada para *ID de rede* e a segunda parte e designada para *ID de host*, possuindo tamanhos variáveis. O endereço IPv4 utiliza como forma de escrita a notação

decimal com ponto, nesse formato os endereços IPv4 de 32 bits são subdivididos em 4 octetos de 8 bits cada, onde são escritos em decimal, de 0 a 255 separados por ponto, por exemplo (ATAKAN et al., 2000; TANENBAUM; WETHERALL, 2011):

- Notação binário nativa de um endereço IPv4, 32 bits:
  10000000000000100000011100001001
- Formato binário nativa de um endereço IPv4 de 32 bits divididos em 4 octetos:
  10000000 00000010 00000111 00001001.
- Formato decimal com pontos deste mesmo endereço:
  128.2.7.9.

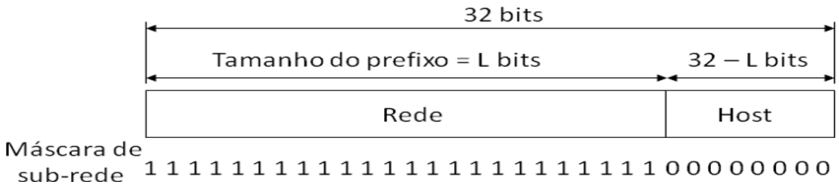
3.2.2.1 Máscaras de sub-redes ou Prefixo

A máscara de sub-rede e um parâmetro de configuração do IPv4 que permite saber qual parte de um endereço IPv4 e designado *ID de rede* e para o *ID de host.* Também e escrita na forma de notação decimal com ponto, nesse formato as máscaras de sub-redes são compostas por 32 bits, subdivididos em 4 octetos de 8 bits cada e que diferentemente do endereçamento IPv4 cada octeto ser formado apenas por dois valores decimais, 0 ou 255. Com isso temos três máscaras padrões (NORTHRUP; MACKIN, 2009, tradução nossa):

FORMATO DECIMAL	FORMATO BINÁRIO
255.0.0.0	11111111.00000000.0000000.00000000
255.255.0.0	11111111.11111111.00000000.00000000
255.255.255.0	11111111.11111111. 11111111.00000000

O bloco designado como *ID de rede* tem o mesmo valor para todos os *hosts* de uma mesma rede, esse bloco e classificado com o nome de **prefixo,** e o seu tamanho determinado pela quantidade de bits na parte de *ID de rede.* Podendo ser descrito pelo seu tamanho ´/16´ que é pronunciado como ´barra 16´ que significa que os 16 primeiros bits foram utilizados como *ID de rede* e os outros 16 bits com *ID de host*, essa termologia e muito utilizada na área de operações, rede e roteamento (ATAKAN et al., 2000; TANENBAUM; WETHERALL, 2011):

O esquema 4 descreve o exemplo de um prefixo é uma máscara de sub-rede.

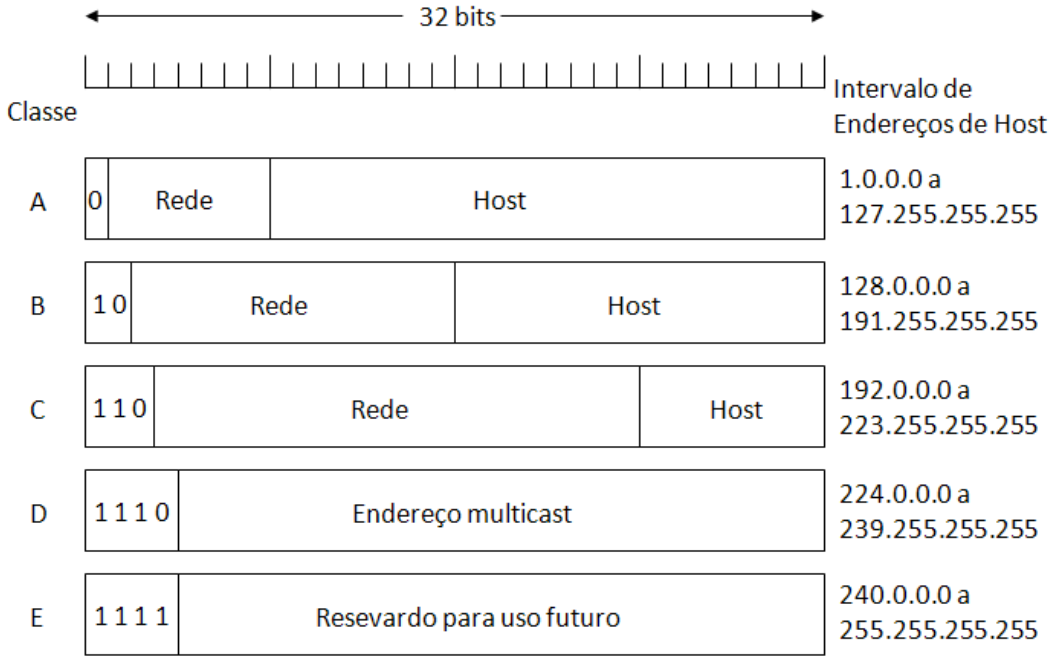


Esquema 4: Um prefixo IP é uma máscara de sub-rede.

Fonte: Tanenbaum; Wetherall, 2011.

3.2.2.2 Endereçamento em Classes

O IPv4 trabalha em uma estrutura de tamanhos fixos, classificada como "endereçamento em classes", sendo divididas em cinco categorias descritas no esquema 5 (TANENBAUM; WETHERALL, 2011):



Esquema 5: Formatos de endereços IP.

Fonte: Tanenbaum; Wetherall, 2011.

Com a divisão de classes e possível a padronização, organização, comunicação e roteamento de redes distintas, permitindo (ATAKAN et al., 2000; FILIPPETTI 2006; ODOM, 2007):

- **Classe A:** Para endereços pertencentes à “Classe A” o primeiro *byte* (8 *bits*) e reservado para rede e os outros três *bytes* (24 *bits*) para endereçamento de *hosts*, porém o primeiro *bit* e definido sempre como 0:

0nnnnnnn.hhhhhhhh.hhhhhhhh.hhhhhhh

Com isso e possível termos 128 redes ou 2^7 e mais de 16 milhões de endereços para *hosts* 2^{24} ou precisamente 16.777.216 endereços para *hosts* por rede, e válido lembra que temos que diminuir sempre dois endereços, sendo o de rede para identificação da própria rede e o de *broadcast* para identificação de todos os *hosts* da mesma rede:

Rede: **0nnnnnnn.hhhhhhhh.hhhhhhhh.00000000**

Broadcast: **0nnnnnnn.hhhhhhhh.hhhhhhhh.11111111**

Possibilitando 16.777.216 - 2 = 16.777.214 de *hosts* válidos por rede. Ainda temos que desconsiderar o uso de dois *ranges*, são elas:

0.0.0.0 - Definida originalmente para broadcast.

127.0.0.0 - Definida para testes e *loopback.*

Possibilitando 128 - 2 = 126 redes válidas. Tendo como máscara padrão 255.0.0.0.

- **Classe B:** Para endereços pertencentes à “Classe B” os dois primeiros *bytes* (16 *bits*) e reservado para rede e os outros dois *bytes* (16 *bits*) para endereçamento de *hosts*, porém os dois primeiros *bits* e definido sempre como 10:

10nnnnnn. nnnnnnnn.hhhhhhhh.hhhhhhh

Com isso e possível termos mais de dezesseis mil redes 2^{14} ou precisamente 16.384 redes e mais de sessenta mil endereços para *hosts* 2^{16} ou precisamente 65.536 endereços para *hosts* por rede, e válido lembra que temos que diminuir sempre dois endereços, sendo que o de rede para identificação da própria rede e o de *broadcast* para identificação de todos os *hosts* da mesma rede:

Rede: **10nnnnnn.nnnnnnnn.hhhhhhhh.00000000**

Broadcast: **10nnnnnn.nnnnnnnn.hhhhhhhh.11111111**

Possibilitando 65.536 - 2 = 65.534 de *hosts* válidos por rede. Tendo como máscara padrão 255.255.0.0.

- **Classe C:** Para endereços pertencentes à “Classe C” os três primeiros *bytes* (24 *bits*) e reservado para rede e o último *byte* (8 *bits*) para

endereçamento de *hosts*, porém os dois primeiros *bits* e definido sempre como 110:

110nnnnn.nnnnnnnn.nnnnnnnn.hhhhhhh

Com isso e possível mais de dois milhões de rede 2^{21} ou precisamente 2.097.152 redes e apenas 256 endereços para *hosts* 2^{8} por rede, e válido lembra que temos que diminuir sempre dois endereços, sendo o de rede para identificação da própria rede e o de *broadcast* para identificação de todos os *hosts* da mesma rede:

Rede: **110nnnnn.nnnnnnnn.nnnnnnnn.00000000**

Broadcast: **110nnnnn.nnnnnnnn.nnnnnnnn.11111111**

Possibilitando 256 - 2 = 254 *hosts* válidos por rede. Tendo como máscara padrão 255.255.255.0.

- **Classe D:** Para endereços pertencentes à "Classe D" os quatro primeiros *bits* são reservados. Essa classe e utilizada para transmissão com uma área limitada conhecida como *multicasting*, e apenas para *hosts* que estejam na mesma classe podem se comunicar (HUNT, 2002, tradução nossa).
- **Classe E:** Para endereços pertencentes à "Classe E" os quatro primeiros *bits* são reservados. Essa classe de endereçamento foi designada para uso futuro (HUNT, 2002, tradução nossa).

3.2.2.3 Sub-redes

O endereçamento IPv4 possui 32 *bits* subdivididos em *ID de host* e *ID de rede*, inicialmente a utilização das máscaras de sub-redes padrões pode não comporta o tamanho da rede ou simplesmente desperdiça endereçamento causando ainda problemas para administração, gerenciamento e ainda aumentando o tamanho de domínios de *broadcasts*. A prática de subdividir logicamente uma máscara de sub-rede padrão, pegando-se *bits* reservados da parte do *ID de host* e movendo para o *ID de rede*, e conhecida como sub-redes (*subnetting*), isso possibilita criar redes mais específicas onde podemos simplesmente aumentar ou diminuir o tamanho da rede possibilitando que a rede comporte mais ou menos *hosts* e se adequando a necessidade real. Podendo ter como principais vantagens (MOGUL, 1984, tradução nossa):

- Redimensionamento lógico da rede física;

- Controle e limitação do tráfego de *broadcast*;
- Administração simplificada;
- Segurança.

3.2.2.4 Endereçamento Público

O processo de atribuição e gerenciamento de endereços IP válidos na Internet e responsabilidade da IANA e as suas organizações membros. Quando uma empresa solicita um bloco de endereçamento ela antes precisa comprovar a real necessidade e preencher os pré-requisitos estabelecidos pelos órgãos responsáveis. Após a aceitação do processo a empresa recebe um bloco de endereçamento/prefixo válido na Internet e de uso exclusivo, o próximo passo e divulgar rotas para os roteadores da Internet, assim tornando-se acessível a quaisquer *hosts* da Internet. Após isso essas redes passam a ser classificadas de rede públicas e os endereços de endereços públicos (ODOM, 2007). O Esquema 6 demonstra a distribuição das organizações membros da IANA.

Registry	Area Covered
AfriNIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	North America Region
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

Esquema 6: Organizações Membro da IANA.
Fonte: IANA, 2011.

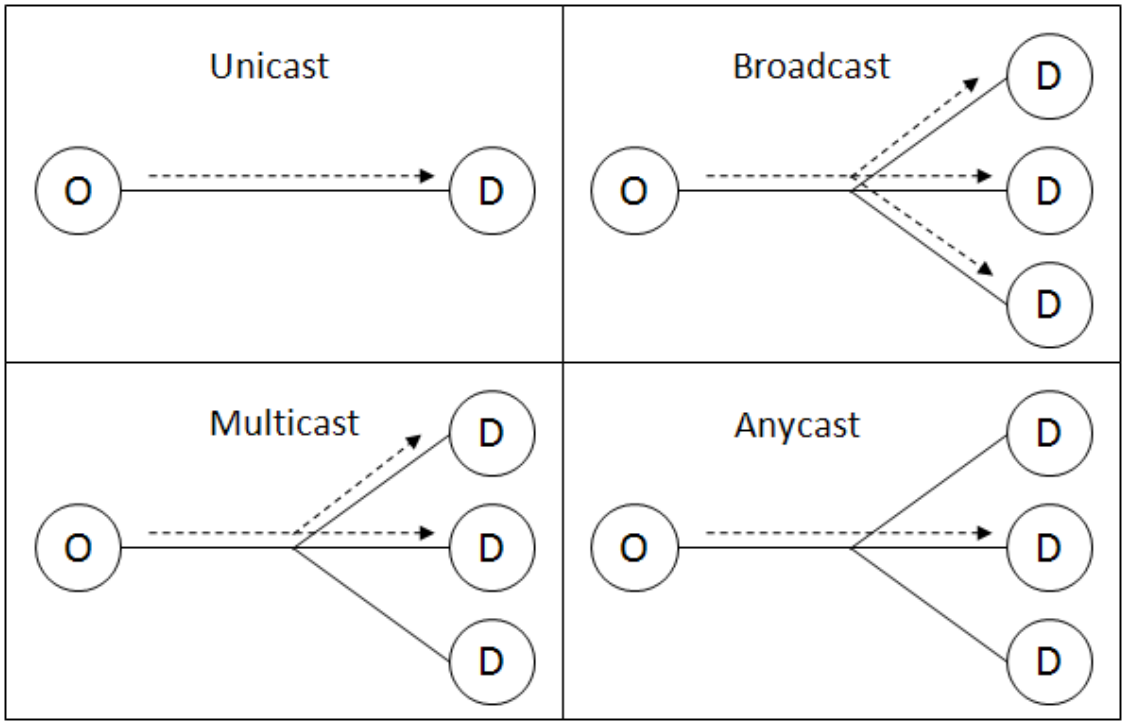
3.2.2.5 Métodos de Entrega

O IPv4 utiliza quatro métodos de entrega descritos a seguir e representado visualmente no esquema 7 (BRITT et al., 2006, tradução nossa):

- ***Unicast*:** Este método e utilizado por dispositivos para estabelecer conexões apenas para um dispositivo dentro da rede.
- ***Broadcast*:** Este método e utilizado por dispositivos ou aplicações para estabelecer conexões e enviar mensagens a todos dispositivos da rede.

Todos os *bits* do endereço IPv4 e representado por 1 binário ou 255.255.255.255 e sempre são válidos somente como endereço de destino e nunca como endereço de origem.

- ***Multicast*:** Este método e utilizado por um dispositivo para estabelecer conexões para um grupo de dispositivos da rede, onde cada grupo e representado por um número de 28 *bits* expressado por um endereço de classe D.
- ***Anycast*:** Este método atribui o mesmo endereçamento em mais de um dispositivo de rede pertencendo a *hosts* diferentes e possibilitando a distribuição dos dados. Quando um dispositivo estabelece uma conexão com intuito de obter dados, o *host* mais próximo e com melhor desempenho responde e realiza a entrega os dados solicitados.



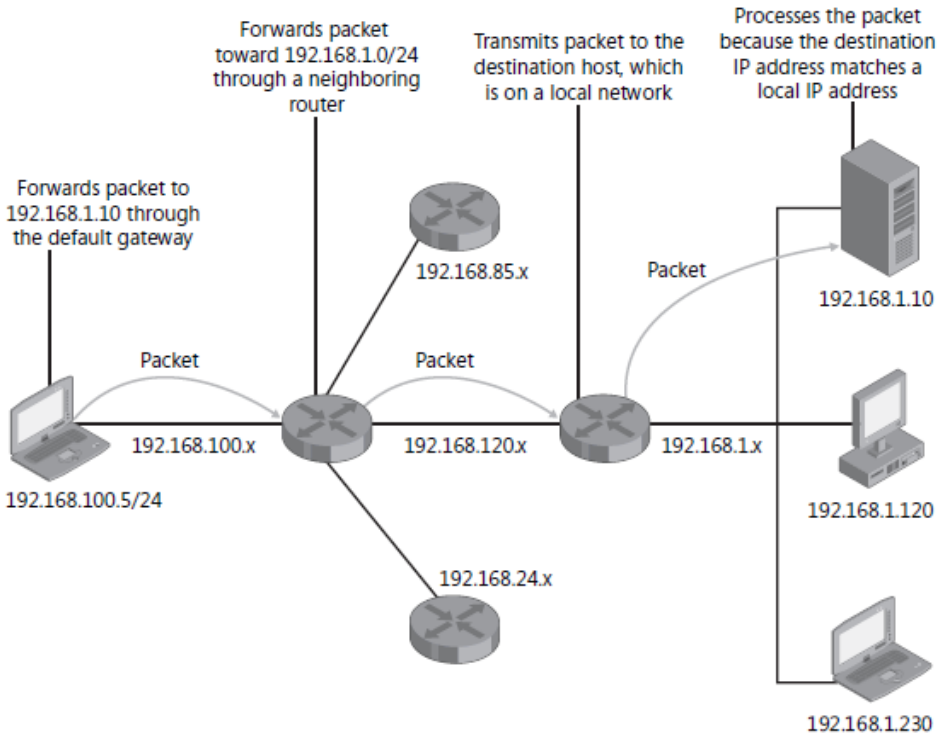
Esquema 7: *IP: Packet Delivery Modes*.

Fonte: Britt et al., 2006.

3.2.3 Gateways

Os *gateways* são dispositivos que permitem a comunicação entre redes distintas. Quando um computador em uma determinada rede tenta enviar um pacote para outro

computador que pertence a uma rede diferente, o mesmo encaminha o pacote primeiramente ao roteador local (*gateway default)* que por sua vez encaminha o pacote IPv4 de acordo com a tabela de roteamento existente no mesmo, essa rota pode ter sido atribuída dinamicamente através de protocolos de roteamento ou estaticamente. O esquema 8 demonstra a quando um computador na rede 192.168100.0/24 tenta estabelecer a comunicação com o servidor localizado na rede 192.168.1.0/24, porém para que essa comunicação exista foi necessário o encaminhamento do pacote para o seu *gateway default* e após a realização de uma consulta a sua tabela de roteamento encaminhou o pacote para o roteador vizinho que conhece e possui uma rota para a rede de destino e este por sua vez encaminha o pacote para o servidor (NORTHRUP; MACKIN, 2009, tradução nossa; POSTEL, 1981, tradução nossa):



Esquema 8: *Routing an IP packet over an Internetwork*.

Fonte: Northrup; Mackin, 2009.

3.2.4 Fragmentação

O processo de fragmentação consiste na divisão de um pacote grande em pacote de tamanhos menores, essa técnica e aplicada quando um pacote originado dentro de uma rede local tem um tamanho maior que o comportado pela rede física e possui a necessidade de cruzar redes físicas diferentes. Uma regra aplicada nas redes físicas e não ultrapassar o

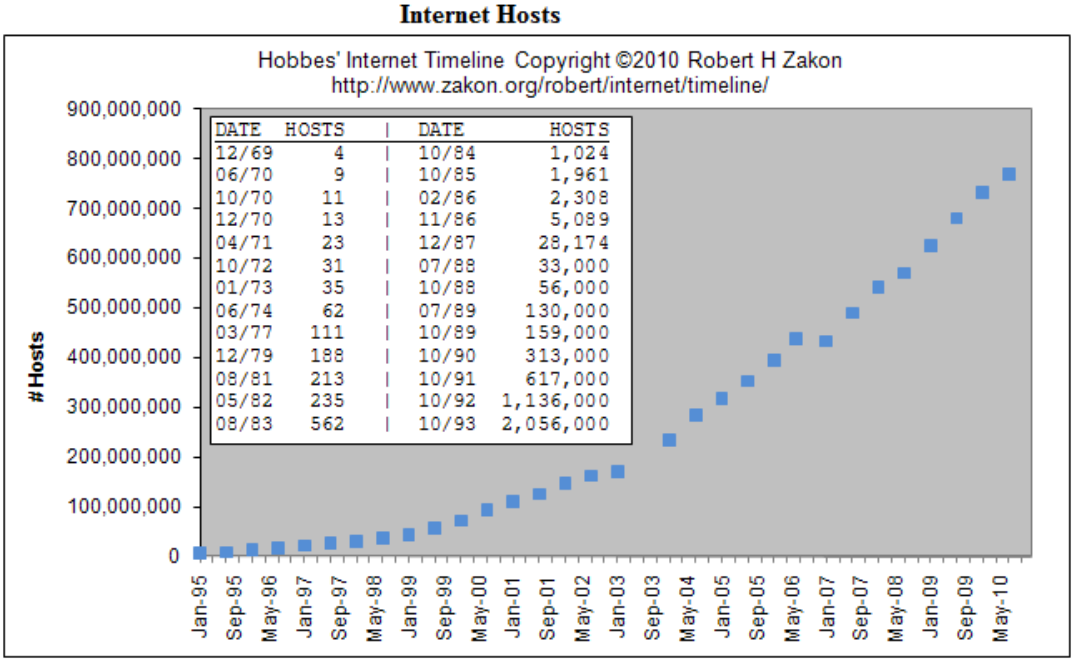
tamanho máximo do frame, também conhecido como Unidade Máxima de Transmissão (MTU – *Maximun Transmission Unit*). Quando um computador necessita se comunicar com outro computador em uma rede diferente e começa a encaminhar pacotes com a MTU maior que o comportado pela rede o roteador que recebeu o pacote quebra eles em tamanhos menores conhecidos como fragmento e os encaminha para o seu próximo salto e finalmente para o computador de destino, ao receber esses fragmentos a função do IPv4 do computador de destino e agrupá-los para remontar o pacote novamente. Caso algum fragmento seja perdido todos os outros são descartados, não sendo função do IPv4 realizar o reenvio de fragmentos perdidos (BRITT et al., 2006, tradução nossa).

3.3 ESGOTAMENTO DOS ENDEREÇOS IPv4

A concepção original do protocolo IPv4 não sofreu muitas alterações desde seu lançamento, na década de 70, o projeto surpreendeu as expectativas no início porém, ao passar dos anos mesmo sendo muito flexível apresentava limitações quando o assunto era:

- Novas tecnológicas de comunicações e dispositivos;
- Novos aplicativos;
- Segurança;
- QoS.

Mesmo com essas limitações o principal ponto que motiva adoção da nova versão do protocolo e que a versão 4 mesmo oferecendo endereço com 32 *bits* o que possibilita pouco mais de 4 bilhões de endereços possíveis, não comporta mas, o crescimento da Internet Global. Analisando o gráfico 1, observa-se o ritmo de crescimento da Internet nos últimos quinze anos e a quantidade aproximada de *hosts*, conectados.



DATE	HOSTS	DATE	HOSTS
12/69	4	10/84	1,024
06/70	9	10/85	1,961
10/70	11	02/86	2,308
12/70	13	11/86	5,089
04/71	23	12/87	28,174
10/72	31	07/88	33,000
01/73	35	10/88	56,000
06/74	62	07/89	130,000
03/77	111	10/89	159,000
12/79	188	10/90	313,000
08/81	213	10/91	617,000
05/82	235	10/92	1,136,000
08/83	562	10/93	2,056,000

Gráfico 1: *Internet Hosts.*

Fonte: Zakon, 2011.

Durante os últimos anos as seguintes técnicas paliativas foram adotas com intuito de contornar o problema de endereçamento do IPv4 (COMER, 1998):

3.3.1.1 CIDR

O Roteamento Interdomínio sem Classes (CIDR – *Classless Inter-Domain Routing*) tem como objetivo principal permite a alocação de blocos conforme a necessidade de cada rede sendo que para isso e necessário trabalhar com endereçamento sem classes alterando o formato de endereço IP da rede para (endereço IPv4 / Tamanho do prefixo), uma segunda vantagem e a redução da tabela de roteamento da Internet (NAUGLE, 2001).

3.3.1.2 DHCP

O Protocolo de configuração de host dinâmico (DHCP – *Dynamic Host Configuration Protocol*) realiza a distribuição e o gerenciamento de endereços IPv4 automaticamente, com isso *hosts* ou dispositivos locais ou remotos podem utilizar recursos disponíveis naquela rede por um período determinado pelo servidor. Além do endereço IPv4 o DHCP fornece também máscara de sub-rede, *gateway default*, endereço do servidor DNS. Essa técnica e muito utilizada em provedores de Internet (ISP – *Internet Service Provider*),

pois garante a atribuição de endereçamento IPv4 válidos na Internet temporariamente para *hosts* remotos, evitando a alocação definitiva e desnecessária (SANTOS; MOREIRAS; ROCHA, 2010).

3.3.1.3 Endereçamento Privado

A RFC 1918 define um conjunto de redes privativas que podem ser utilizadas para endereçamento de redes locais não roteáveis, ou seja, nenhum pacote originado dessas redes pode trafegar via Internet e nenhuma estação que tenha recebido um IP privado possa navegar na internet sem o uso da tradução de endereço de rede. Com isso e possível endereçar e prover comunicação com vários *hosts*, sem a necessidade de endereços públicos. A IANA não atribuíra esse endereçamento a nenhuma organização, porém podem ser utilizadas livremente por empresas, organizações, instituições de ensino, etc. O esquema 9 definem os blocos de endereçamento privativo, reservados pela IANA (GROOT, et al., 1996, tradução nossa):

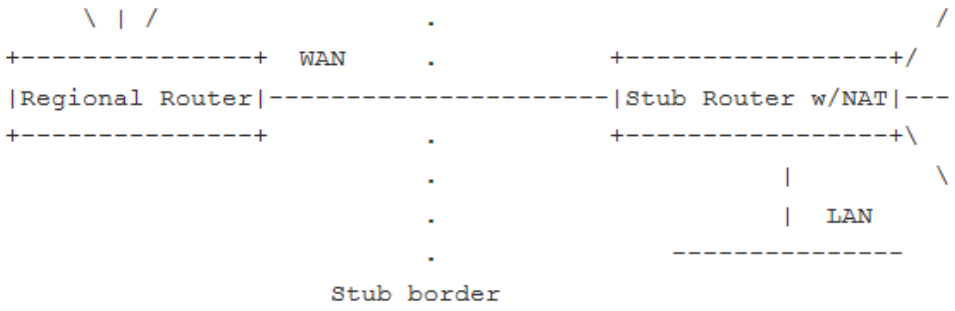
```
10.0.0.0        -   10.255.255.255  (10/8 prefix)
172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

Esquema 9: Private Address Space.

Fonte: Groot et al., 1996.

3.3.1.4 NAT

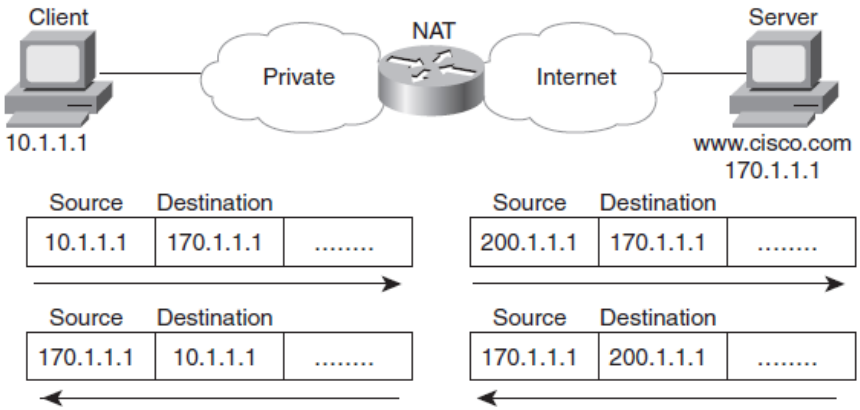
A Tradução de endereços de rede (NAT – *Network Address Translation*) possibilita que os *hosts* pertencentes às redes privativas comuniquem-se e trafeguem pela Internet, usando como técnica um grupo de endereços IP públicos ou apenas com um único endereço IP público. O esquema 10 demonstra uma configuração de NAT tradicional (EGEVANG; SRISURESH, 2001).



Esquema 10: *Traditional NAT Configuration.*

Fonte: Egevang; Srisuresh, 2001.

No esquema 11 podemos ver o momento da troca do endereçamento IP privativo pelo IP publico utilizando NAT (ODOM, 2008).



Esquema 11: *NAT IP Address Swapping: Private Addressing.*

Fonte: Odom, 2008.

As vantagens e desvantagens oferecidas na utilização do NAT são (SANTOS; MOREIRAS; ROCHA, 2010):

- Vantagens:
  - Reduz a necessidade de endereços públicos;
  - Facilita a administração do endereçamento interno;
  - Oculta a topologia;
  - Só permite a entrada de pacotes se forem originados pela rede;
- Desvantagens:
  - Quebra o modelo fim-a-fim da Internet;
  - Dificulta o funcionamento de inúmeras aplicações;
  - Não é escalável;

- Demanda de mais recursos de hardware;
- Falsa sensação de segurança;
- Impossibilita rastreamento do pacote;
- Impossibilita utilização de algumas técnicas do IPSec.

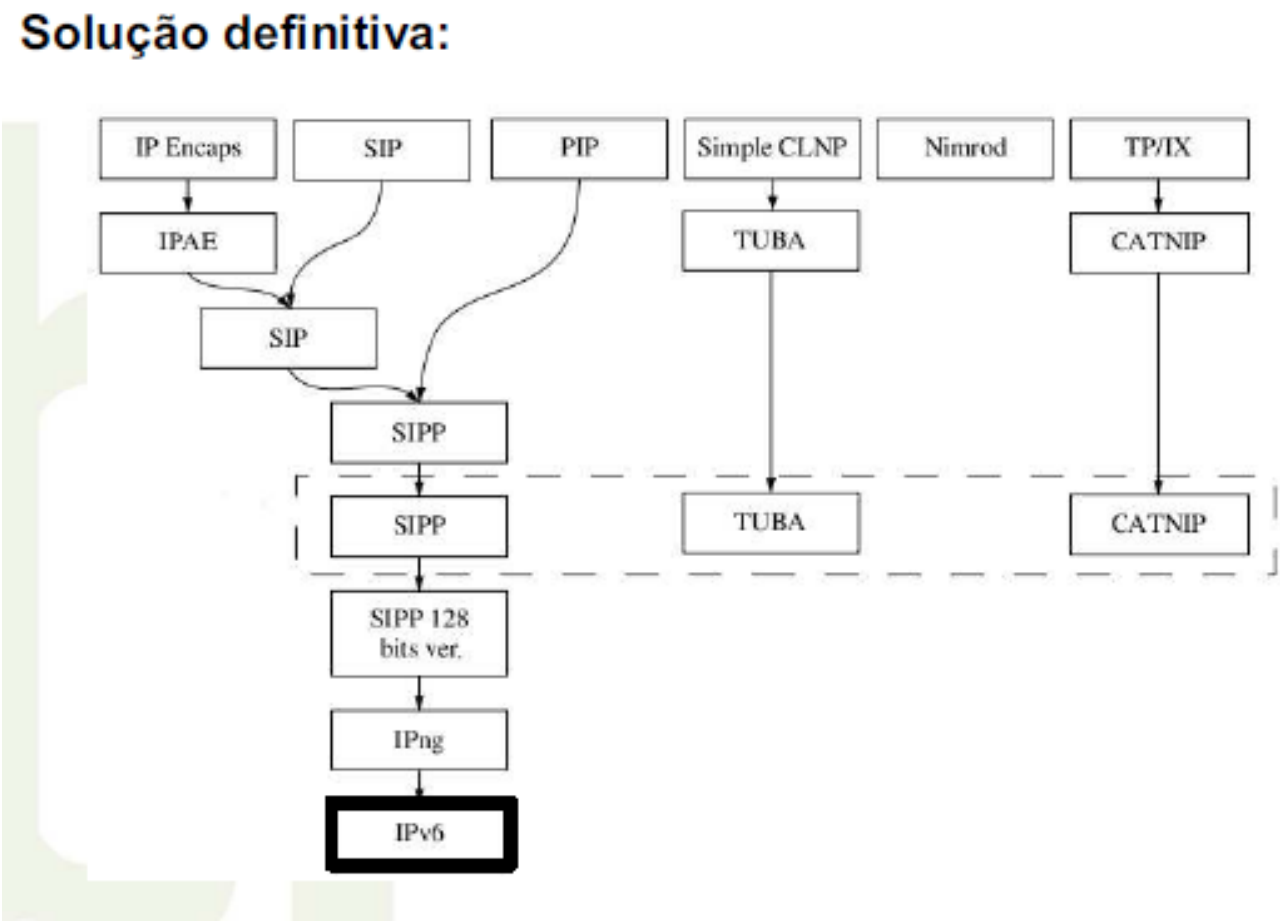
A utilização do NAT atingiu bons resultados com relação à economia de endereçamento IP, mesmo com várias vantagens a adoção do NAT trás muitos inconvenientes onde para alguns acaba não justificando sua utilização. Mesmo com todas essas técnicas, esforços e os 4 bilhões de endereçamentos possíveis oferecidos pelo IPv4, o último bloco de endereçamento público foi atribuído pela IANA ao APNIC em 2011 (MACHADO, 2011).

4 PROTOCOLO IPv6

O Protocolo IPv6, definido pelas RFC 2460, foi concebido para suprir as deficiências apresentada pela versão anterior do protocolo e ao mesmo tempo trazendo inúmeras mudanças (DEERING; HINDEN, 1998, tradução nossa). No início da década de 90 o IETF, criou um grupo chamado de Nova Geração do Protocolo de Internet (IPng – *Internet Protocol Next Generation*) com o propósito de pesquisar e desenvolver uma nova geração do protocolo de Internet, conforme descrito e formalizado na RFC 1550, podendo ser abordado como questões relevantes no processo de desenvolvimento do IPng (BRADNER; MANKIN, 1993, tradução nossa):

1. Escalabilidade;
2. Escala de tempo;
3. Transição e implantação;
4. Segurança;
5. Administração, configuração e operação;
6. Mobilidade;
7. Fluxo e Reserva de recursos;
8. Política de roteamento;
9. Topologia flexível;
10. Aplicabilidade;
11. Serviço de datagrama;
12. Contabilidade;
13. Suporte aos meios de comunicação;
14. Robusto e Tolerante a falha;
15. Influência com outras tecnologias;
16. Itens de ação.

Diversos modelos de projetos foram lançados e estudados buscando atender o problema de endereçamento e o crescimento da Internet global, porém apenas os projetos: CATNIP, TUBA e SIPP foram publicadas na RFC 1752. O esquema 12 demonstra a cadeia evolutiva do projeto (SANTOS; MOREIRAS; ROCHA, 2010):



Esquema 12: Solução definitiva IPng.

Fonte: Santos; Moreiras; Rocha, 2009.

Após as pesquisas, análises e comparações feitas nos três projetos, à RFC 752 descarta o projeto CATNIP, e propõe a integração de funcionalidades apresentadas nos projetos TUBA e SIPP, surgindo à versão revisada do projeto SIPP possibilitando endereçamento de 128 *bits.* Essa versão passou a ser chamado inicialmente de IPng e depois oficialmente de IPv6. E possível visualizar essas comparações no esquema 13 (BRADNER; MANKIN, 1995, tradução nossa; SANTOS; MOREIRAS; ROCHA, 2010).

	CATNIP	SIPP	TUBA
	---	---	---
complete spec	no	yes	mostly
simplicity	no	no	no
scale	yes	yes	yes
topological flex	yes	yes	yes
performance	mixed	mixed	mixed
robust service	mixed	mixed	yes
transition	mixed	no	mixed
media indepdnt	yes	yes	yes
datagram	yes	yes	yes
config. ease	unknown	mixed	mixed
security	unknown	mixed	mixed
unique names	mixed	mixed	mixed
access to stds	yes	yes	mixed
multicast	unknown	yes	mixed
extensibility	unknown	mixed	mixed
service classes	unknown	yes	mixed
mobility	unknown	mixed	mixed
control proto	unknown	yes	mixed
tunneling	unknown	yes	mixed

Esquema 13: *IPng Proposal Reviews.*

Fonte: Bradner; Mankin, 1995.

4.1 FUNCIONABILIDADES DO PROTOCOLO IPv6

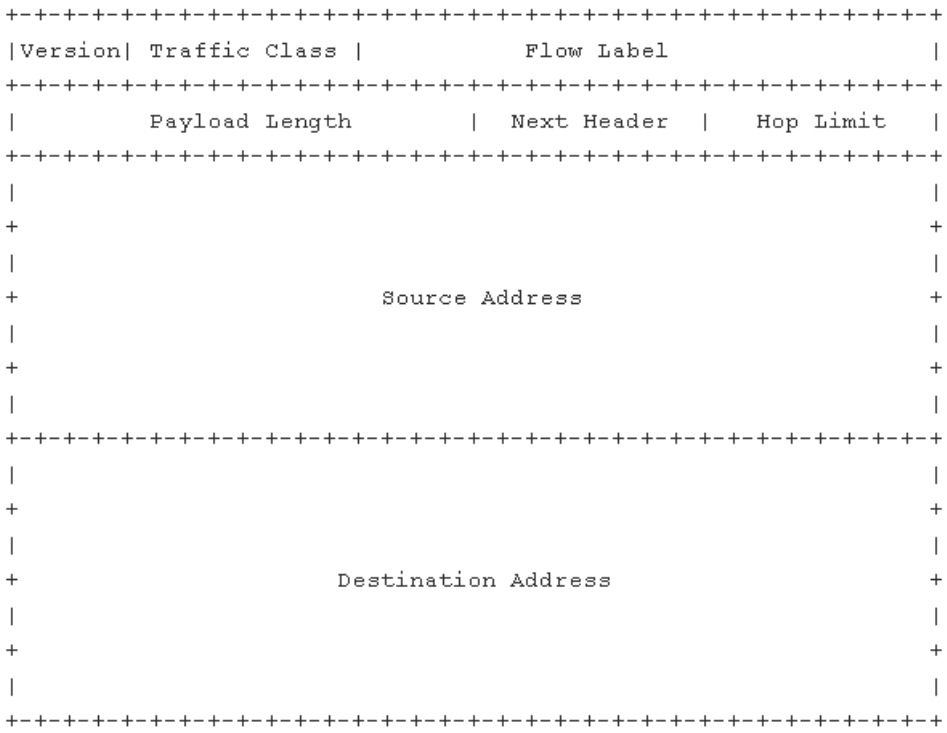
Para Comer (1998), o IPv6 foi concebido preservando várias características e conceitos do IPv4, contudo várias modificações foram necessárias e vários detalhes do protocolo sofreram alteração, tendo como principais vantagens:

- **Endereços maiores:** O tamanho do endereçamento passou de 32 para 128 *bits.*
- **Formato flexível do protocolo:** O formato de datagrama do IPv6 e inteiramente novo e incompatível.
- **Opções aprimoradas:** O IPv6 inclui novas opções possibilitando a inclusão de informações de controle opcionais.
- **Suporte para alocação de recursos:** Substitui a específicação de tipo de serviço do IPv4 para uma nova técnica possibilitando a pré-alocação de recursos de rede.

- Provisão para extensão de protocolo: Permite a transição entre protocolos se adaptando a novos hardwares ou aplicativos.
- **Formato datagrama IPv6:** O datagrama IPv6 passou a ser composto por três partes:
  - Cabeçalho básico;
  - Cabeçalhos de extensão, opcionais;
  - Dados.

4.1.1 Cabeçalho IPv6

Mesmo suportando endereços maiores o tamanho do cabeçalho IPv6 e menor do que o seu antecessor, e vários campos fixos foram removidos e são adicionados se necessários como cabeçalhos de extensão. O esquema 14 demonstra o formato do cabeçalho IPv6 (DEERING; HINDEN, 1998, tradução nossa):



Esquema 14: *IPv6 Header Format.*
Fonte: Bradner; Mankin, 1993.

- **Versão** (*Version*)**:** Define a versão do protocolo, atualmente a versão 6, tamanho de 4 *bits*.

- **Classe de tráfego** (*Traffic Class*)**:** E utilizado para informar as classe dos pacotes para diferentes serviços, possibilitando aplicações em tempo real, tamanho de 8 *bits* (LOSHIN, 2004, tradução nossa).
- **Rótulo de Fluxo** (*Flow Label*)**:** E utilizado para diferenciar e identificar pacotes com o mesmo fluxo, tamanho de 20 *bits*.
- **Tamanho dos Dados** (*Payload Length*)**:** Contém o tamanho inteiro em *Bytes*, apenas dos dados enviados após o cabeçalho básico IPv6. Os cabeçalhos de extensão também são adicionados neste campo para fins de cálculo, tamanho de 16 bits (LOSHIN, 2004, tradução nossa).
- **Próximo Cabeçalho** (*Next Header*)**:** Define e identifica o cabeçalho que segue o cabeçalho IPv6, contendo valores referentes a cabeçalhos de extensão e outros protocolos de camada mais alta como TCP ou UDP, tamanho de 8 *bits* (LOSHIN, 2004, tradução nossa).
- **Limite de Saltos** (*Hop Limit*)**:** Este campo marca o número máximo de saltos que um pacote IPv6 pode dar antes de ser descartado. Toda vez que um pacote e analisado por um roteador ele e decrementado e se o limite de hop chegar à zero, o pacote e descartado (LOSHIN, 2004, tradução nossa).
- **Endereço de Origem** *(Source Address*)**:** Carrega o endereço IP de origem, tamanho de 128 *bits*.
- **Endereço de Destino** (*Destination Address*)**:** Carrega o endereço IP de destino, tamanho de 128 *bits*.

4.1.2 Cabeçalhos de extensão

Para Tanenbaum (2011), mesmo com a simplificação do cabeçalho do IPv6 alguns campos originários do IPv4 ainda são necessários para gerarem informações extras e opcionais e foram agregados ao cabeçalho básico do IPv6 como cabeçalhos de extensão, atualmente existem seis tipos de cabeçalhos, são eles (LI; JINMEI; SHIMA, 2007, tradução nossa):

- ***Hop-by-hop options*:** Este cabeçalho carrega informações complementares e devem ser processados por todos os roteadores.

    - Identificado pelo valor 00 no campo de “Próximo Cabeçalho” do cabeçalho IPv6 básico.
- ***Destination options:*** Este cabeçalho carrega opções adicionais e devem ser processadas pelo roteador de destino do pacote.
    - Identificado pelo valor 60 no campo de “Próximo Cabeçalho” do cabeçalho IPv6 básico.
- ***Routing:*** Este cabeçalho lista parcialmente um ou mais roteadores que deveriam ser visitados pelo pacote ate o seu destino final.
    - Identificado pelo valor 43 no campo de “Próximo Cabeçalho” do cabeçalho IPv6 básico.
- ***Fragmentation:*** Este cabeçalho carrega e gerencia os fragmentos dos datagramas IPv6.
    - Identificado pelo valor 44 no campo de “Próximo Cabeçalho” do cabeçalho IPv6 básico.
- ***Authentication:*** Este cabeçalho possibilita a verificação da identidade, autenticidade e autenticação do transmissor.
    - Identificado pelo valor 51 no campo de “Próximo Cabeçalho” do cabeçalho IPv6 básico.
- ***Encapsulantion Security Payload:*** Este cabeçalho carrega informações de criptografia, integridade e confiabilidade de pacotes.
    - Identificado pelo valor 50 no campo de “Próximo Cabeçalho” do cabeçalho IPv6 básico.

Quando não existem cabeçalhos de extensão o campo e identificado pelo valor 59 no campo de “Próximo Cabeçalho” do cabeçalho IPv6 básico.

4.1.3 Endereçamento IPv6

Segundo Comer (1998), o endereçamento IPv6 ocupa 16 octetos binários ou 128 *bits*, sendo quatro vezes maior do que o seu antecessor o endereçamento IPv4, que tem o tamanho de 4 octetos binários ou 32 *bits*. Com isso e possível obter o equivalente a 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços IPv6 ou 2^{128}, endereços possíveis. Considerando que a população da Terra hoje esteja estimada em 6 bilhões de

pessoas, o IPv6 disponibiliza mais de 56 octilhões ($5,6x10^{28}$) de endereços por ser humano (SANTOS; MOREIRAS; ROCHA, 2010).

4.1.3.1 Representação do endereçamento IPv6

A representação do endereçamento IPv6 e composta por 128 *bits* ou 32 dígitos hexadecimais podendo ser maiúsculos ou minúsculos, onde cada dígito hexadecimal equivale a 4 dígitos binários, sendo organizado e escrito em 8 quartetos de 4 dígitos hexadecimais separados por dois pontos, exemplo (LOSHIN, 2004, tradução nossa; ODOM, 2008, tradução nossa):

Na primeira parte foi escrito um endereço IPv6 no formato original hexadecimal:

- 2340:1111:AAAA:0001:1234:5678:9ABC

E na segunda parte, convertemos esse endereço em binário, para um melhor entendimento foram utilizadas quatro cores para diferenciar cada número hexadecimal dentro de cada quarteto, com isso e possível visualizar de forma simples e objetiva o endereçamento IPv6:

- 0010001101000000:1010101010101010:0000000000000001:0001001000110100:0101011001111000:1001101010111100

Desta forma e mais fácil escrever um endereço IPv6 no formato hexadecimal, podendo ainda utilizar duas convenções que permitem abreviação do endereço IPv6, são elas:

- Omitir os 0 na frente em qualquer octeto;
- Caso um ou mais quartetos apresente todos com 0s hexadecimais, o mesmo pode ser representado por "::", podendo ser utilizado apenas uma única vez, exemplo:
  - Formato original:
    - FE00:0000:0000:0001:0000:0000:0000:0056
  - Formato abreviado:
    - FE00::1:0:0:0:56 ou FE00:0:0:1::56
  - Formato de abreviação não aceito, pois gera ambiguidade:
    - FE00::1::56.

4.1.3.2 Outras representações importantes do endereçamento IPv6

O endereçamento IPv6 também e representado na forma de prefixos, utilizando a notação CIDR, onde e escrito “Endereço IPv6 / Tamanho do Prefixo”, desta forma o tamanho do prefixo e especificado pela quantidade de *bits* à esquerda do endereço, como podemos visualizar no esquema 15 (DEERING; HINDEN, 2003, tradução nossa).

```
12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60
```

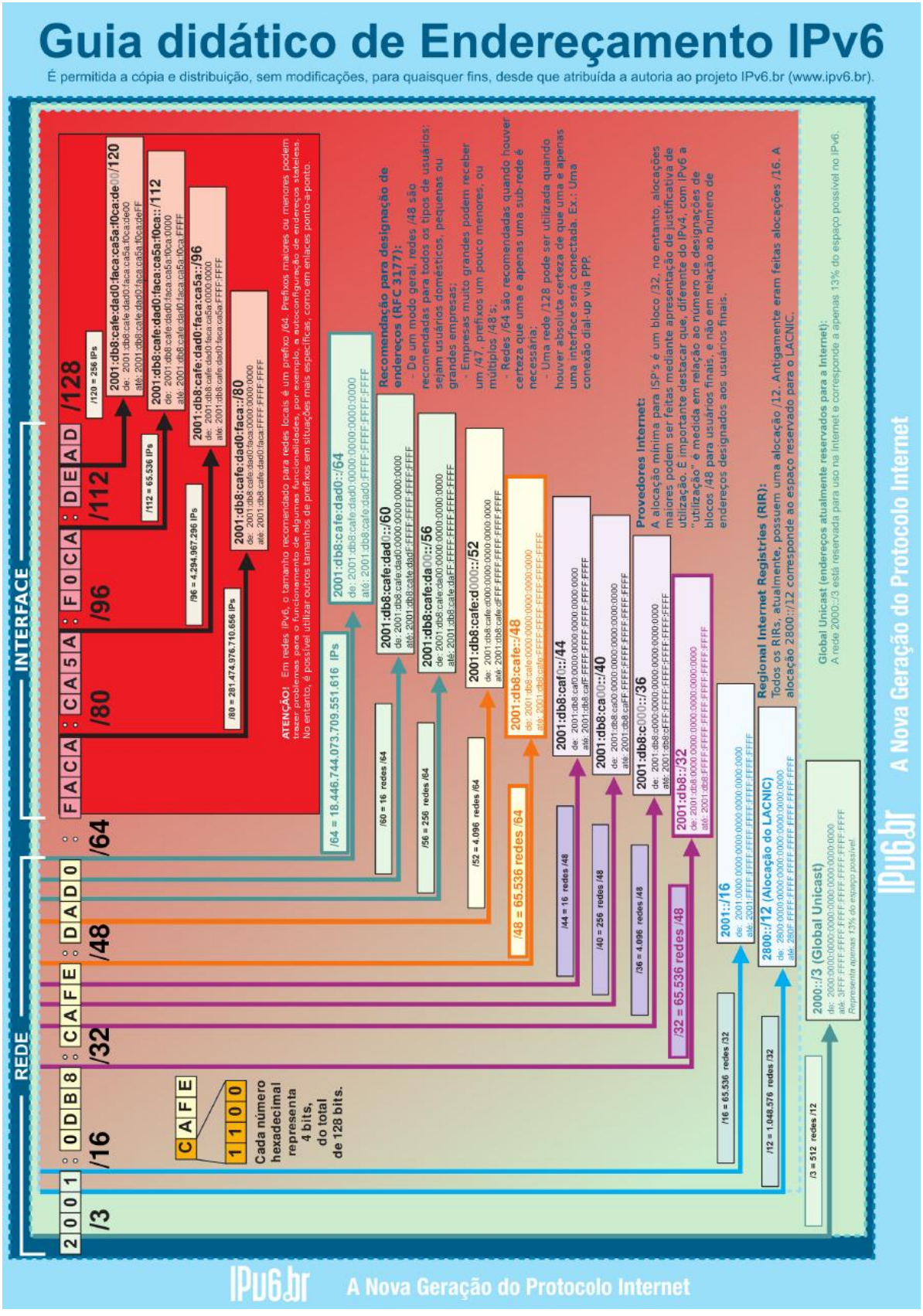
Esquema 15: Representations of the 60-bit prefix.
Fonte: Deering; Hinden, 2003.

Também e possível acessar os endereços IPv6 no formato de URL, sendo necessária a utilização de colchetes, demostrado no esquema 16 (SANTOS; MOREIRAS; ROCHA, 2010):

http://[**2001:12ff:0:4::22**]/index.html
http://[**2001:12ff:0:4::22**]:8080

Esquema 16: Representação do endereçamento IPv6 no formato de URL.
Fonte: Santos; Moreiras; Rocha, 2010.

No esquema 17, e possível visualizar um guia extremamente didático, disponibilizado pelo “Projeto IPv6.br” e que ajuda compreender de forma clara e objetiva a divisão de um endereço IPv6 em prefixos.



Esquema 17: Guia didático de Endereçamento IPv6.

Fonte: Projeto IPv6.br, 2010.

4.1.3.3 Tipos de endereçamento IPv6

Conforme publicado pela RFC 3513, existem três tipos de endereçamento IPv6 (DEERING; HINDEN, 2003, tradução nossa):

- ***Unicast:*** O endereçamento *unicast* serve para identificação individual, onde um pacote direcionado a um endereço *unicast* e entregue a uma única interface. Podemos classificar o endereçamento *unicast*, como (COMER, 1998; LOSHIN, 2004, tradução nossa; NORTHRUP; MACKIN, 2009, tradução nossa).
    - ***Global Unicast***: São conhecidos como *unicast* globais agregáveis, sendo equivalentes aos endereços públicos do IPv4, esses endereços podem ser encaminhados através da Internet IPv6 e são globalmente únicos.
      Prefixo de identificação: **2000::/3** tendo como intervalo **2000::** à **3fff.ffff.ffff.ffff.ffff.ffff.ffff.ffff**.
    - ***Link-local***: Esses endereços são atribuídos automaticamente e validos apenas localmente dentro da mesma rede, podendo ser utilizado para descoberta de vizinhança, autoconfiguração e quando não houver roteadores presentes na comunicação (DEERING; HINDEN, 2003, tradução nossa). São equivalentes ao endereçamento *APIPA* do IPv4 tendo como principal diferença, que mesmo após atribuição de um endereço roteável pela interface o mesmo permeasse atribuído como um endereçamento secundário.
      Prefixo de identificação: **FE80::/64**.
    - ***Unique-local:*** Esses endereços são utilizados para comunicações locais numa rede ou em um grupo de redes, são equivalentes aos endereços privados do IPv4 podendo ser roteáveis entre sub-redes privadas, mas não sendo roteável na Internet, também são globalmente únicos.
      Prefixo de identificação: **FC00::/7**.

- ***Loopback:*** Esse endereço e utilizado para identificação da própria interface, sendo equivalente ao endereço de *loopback* 127.0.0.1 do IPv4 (DEERING; HINDEN, 2003, tradução nossa).
  Prefixo de identificação: **1/128 (0:0:0:0:0:0:0:1 ou ::1)**.
- ***Unspecified***: Esse endereço indica a ausência de um endereço, sendo equivalente ao endereço 0.0.0.0 do IPv4 (DEERING; HINDEN, 2003, tradução nossa).
  Prefixo de identificação: :: /128 (**0:0:0:0:0:0:0:0** ou **::0)**.
- **IPv4 mapeado em IPv6**: Esse endereço combina um endereço IPv6 com um endereço IPv4 convertido em hexadecimal. São usado técnicas de transição.
  Prefixo de identificação: **FFFF.wxyz** (**0:0:0:0:0:FFFF:wxyz)**.
- ***Site Local:*** Esse endereço foi projetado para endereçar *hosts* dentro de uma mesma rede sem a necessidade de um prefixo global. Também fornecendo roteamento privado nas redes IPV6. Porém recentemente o mesmo foi preterido conforme descrito no RFC 3879 (HUITEMA; CARPENTER, 2004, tradução nossa).
  Prefixo de identificação: **FECO::/10**.
- ***Interface Identifiers:*** Esse endereço foi projetado para endereçar interfaces em um link, tendo que ser únicos dentro da própria sub-rede. O IID pode ser gerado automaticamente, porém recomendasse que o mesmo fosse constituído baseando no endereço MAC da interface no formato EUI-64 (DEERING; HINDEN, 2003, tradução nossa).

- ***Multicast:*** O endereçamento *multicast* serve para identificação um grupo de interfaces pertencentes a diferentes *hosts*. Quando um pacote e destinado a um endereço *multicast* o mesmo é enviado para todas as interfaces do grupo. O *broadcast* do IPv4 foi descontinuado sendo substituídos no IPv6 pelo *multicast*, com isso todos os *hosts* endereçados com IPv6 tem que oferecer suporte a *multicast* (DEERING; HINDEN, 2003, tradução nossa).
  Prefixo de identificação: **FF00::/8** .
- ***Anycast:*** O endereçamento *anycast* atua com uma identificação seletiva, identificando um conjunto de interfaces. Quando um pacote e destinado a

> um endereço *anycast* o mesmo é entregue a interface mais próxima. A determinação de interface mais próxima e definida pelos protocolos de roteamento (DEERING; HINDEN, 2003, tradução nossa).

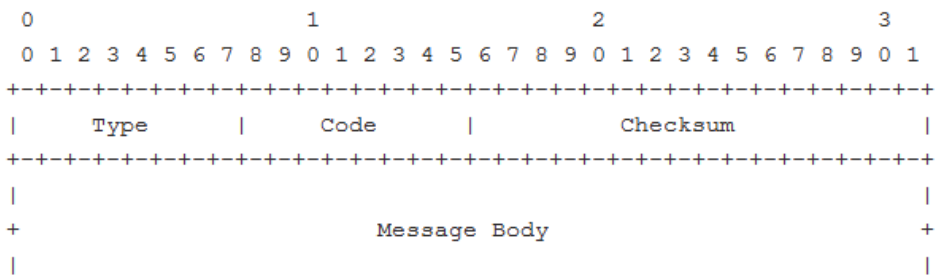
4.1.4 ICMPv6

O Protocolo de Mensagem de Controle da Internet (ICMP – *Internet Control Message Protocol*), originário do IPv4 foi atualizado e definido pela RFC 4443 como ICMPv6, mantendo a mesma estrutura do seu antecessor, um ponto relevante e que o ICMP não e compatível com o ICMPv6. Sua função e relatar erros de processamento de pacotes e enviar mensagens sobre o *status* da rede, podendo também funções de “Camada de Rede” como diagnósticos ICMPv6 "*ping*". No protocolo IPv6 o protocolo ICMPv6 e identificado pelo valor 58 no campo “Próximo Cabeçalho” (CONTA; DEERING; GUPTA, 2006).

Foram adicionadas ao ICMPv6 as funções do Protocolo de Resolução de endereços (ARP – *Address Resolution Protocol*) e do Protocolo de Gerenciamento de Grupo de Internet (IGMP – *Internet Group Management Protocol*), sendo essências nos serviços:

- Descoberta de Vizinhança;
- Descoberta de *Path* MTU;
- Gerenciamento de Multicast;
- Mobilidade.

O cabeçalho ICMPv6 apresenta uma estrutura simples conforme demonstrado pelo esquema 18 (BRITT et al., 2006, tradução nossa; CONTA; DEERING; GUPTA, 2006):



Esquema 18: *The ICMPv6 messages have the following general format.*

Fonte: Conta; Deering; Gupta, 2006.

- **Tipo** (*Type*)**:** Índica o tipo da mensagem, o seu valor influenciará no formato da mensagem, tamanho de 8 *bits*. No ICMPv6 suas mensagens são agrupadas em duas classes:
    - **Mensagens de erro:** São mensagens identificadas pelos valores entre 0 a 127, exemplo:
        - 1 – *Destination Unreachable.*
        - 2 – *Packet Too Big.*
        - 3 – *Time Exceeded.*
        - 4 – *Parameter Problem.*
    - **Mensagens de Informação:** São mensagens identificadas pelos valores entre 128 a 255, exemplo:
        - 128 – *Echo Request.*
        - 129 – *Echo reply.*
        - 130 – *Group Membership Query.*
        - 133 – *Router Solicitation.*
        - 134 – *Router Advertisement.*
        - 135 – *Neighbor Solicitation.*
        - 136 – *Neighbor Advertisement.*
        - 137 – *Redirect.*
- **Código** (*Code*)**:** Esse campo depende do campo "Tipo" onde e utilizado para criar um nível de informações adicionais, tamanho de 8 *bits*.
- **Soma de Verificação** (*Checksum*)**:** É utilizado para encontrar dados corrompidos no cabeçalho ICMPv6 e em parte da mensagem, tamanho de 16 *bits*.
- **Corpo de Mensagens** (*Message Body*)**:** Contém as informações de *status* e erros levando em consideração o tipo da mensagem.

4.1.5 Descoberta de vizinhança

Conforme descrito na RFC 4861, a função do Protocolo de Descoberta de Vizinhança (NDP – *Neighbor Discovery Protocol*) e facilitar o processo de configuração de redes IPv6. Dispositivos como *hosts* e roteadores utilizam o protocolo de Descoberta de Vizinhança, para (NARTEN et al., 2007, tradução nossa):

- Descobrir endereços MAC dos *hosts* da rede;
- Encontrar roteadores vizinhos;
- Detectar endereços duplicados;
- Redirecionamento de pacotes;
- Autoconfiguração de endereços;

4.1.5.1 Mensagens ICMPv6 utilizadas pelo NDP

O Protocolo de Descoberta de Vizinhança utiliza cinco mensagens ICMPv6 para execução das suas funcionalidades, são elas (NARTEN et al., 2007, tradução nossa):

- ***Router Solicitacion:*** São mensagens enviadas por *hosts* com destino aos roteadores requisitando mensagens *Router Advertisement*. Essa mensagem e identificada pelo tipo 133 no cabeçalho ICMPv6.
- ***Router Advertisement:*** São mensagens enviadas constantemente, podendo ser uma resposta para um *Router Solicitacion* ou simplesmente anunciando rapidamente a presença de roteadores em links locais ou na Internet. Essa mensagem e identificada pelo tipo 134 no cabeçalho ICMPv6.
- ***Neighbor Solicitation:*** São mensagens *multicast* enviadas por um *host* buscando determinar o endereço de camada de enlace e ao mesmo tempo informar o seu endereço físico para o *host* de destino. Também possibilita identificar endereços duplicados e detectar a acessibilidade de um vizinho na rede. Essa mensagem e identificada pelo tipo 135 no cabeçalho ICMPv6.
- ***Neighbor Advertisement:*** São mensagens enviadas como resposta para um *Neighbor Advertisement* ou simplesmente anunciando rapidamente a mudança de estado de um endereço de enlace dentro da rede. Essa mensagem e identificada pelo tipo 136 no cabeçalho ICMPv6.
- ***Redirect:*** São mensagens enviadas por roteadores para informar aos *hosts*, o roteador mais próximo e de melhor métrica para alcançar o seu destino. Essa mensagem e identificada pelo tipo 137 no cabeçalho ICMPv6.

4.1.5.2 Soluções de problemas

Uma das principais funcionalidades do NDP e ajudar na solução de problemas relacionados a *hosts*, nós e roteadores na rede, definindo mecanismos para resolução dos seguintes problemas (LOSHIN, 2004, tradução nossa; NARTEN et al., 2007, tradução nossa):

- ***Router Discovery*:** Esta técnica e utilizada por *hosts* para localizar roteadores no mesmo *link*.
- ***Prefix Discovery*:** Esta técnica e utilizada por nós para localizar endereços de prefixos no mesmo segmento, com isso podem determinar se o destino e alcançado por um roteador.
- ***Parameter Discovery*:** Esta técnica e utilizada por nós de rede para aprender parâmetros físicos do enlace de comunicação.
- ***Address Autoconfiguration*:** Este mecanismo permite que nós a configuração automática de endereçamento nas suas interfaces de rede. ***Address resolution*:** Esta técnica e utilizada por *hosts* para descobrir o endereço de camada de enlace dos *hosts* vizinhos.
- ***Next-hop determination*:** Esta técnica utiliza um algoritmo para mapear endereços IP de destino em endereços IP dos vizinhos, possibilitando o envio de tráfego ao destino.
- ***Neighbor Unreachability Detection*:** Esta técnica e utilizada por nós de rede para determinar se um vizinho ainda e acessível.
- ***Duplicate Address Detection*:** Esta técnica e utilizada pelos nós da rede para identificar se existem endereços duplicados no mesmo segmento de rede
- ***Redirect*:** Esta técnica e iniciada pelos roteadores ao redirecionarem os *hosts*, a um roteador mais próximo.

4.1.6 Autoconfiguração

A autoconfiguração do IPv6 torna mais simples o processo de atribuição de endereçamento para dispositivos de rede. A capacidade de se configurar automaticamente, mesmo em a utilização de protocolo de configuração de endereço, facilita muito a implantação de uma rede IPv6 já que a oferta de endereçamento do IPv6 e de 2^{128} endereços. Usando funcionalidades do NDP um *host* pode automaticamente configurar endereços locais e remotos para cada interface. As configurações automáticas utilizadas pelo protocolo IPv6 são (DAVIES, 2008, tradução nossa):

- **Endereços *Stateless*:** Permite a atribuição de endereços automaticamente aos nós da rede, sem a necessidade de configurações manuais ou utilização de servidores, sendo necessárias apenas as configurações básicas de roteadores.
- **Endereços *Stateful*:** Permite a atribuição de endereços dinamicamente, utilizando servidores, o protocolo utilizado para configuração de endereços dinamicamente e DHCPv6, que possibilita obter endereços e outras configurações de rede.

4.1.7 DHCPv6

O Protocolo de configuração de host dinâmico (DHCP – *Dynamic Host Configuration Protocol*), originário do IPv4 também foi atualizado e descrito pela RFC 3315 como DHCPv6, mantendo o conceito inicial proposto pelo projeto, porém na parte operacional passou por mudanças significativas, tendo como principais mudanças (BOUND et al., 2003, tradução nossa):

- A comunicação entre servidor e *hosts* passou a ser via *multicast.*
- E incompatível com a versão anterior.
- Possui menos opções de configuração interna comparado com o DHCPv4.
- Pode ser utilizado em conjunto com a autoconfiguração de endereços *stateless*.
- Com apenas uma única solicitação um hosts pode configurar todas as suas interfaces, com opções independentes para cada uma delas.

4.1.8 *Path MTU Discovery*

O Protocolo *Path MTU Discovery*, descrito na RFC 1981 e responsável pela fragmentação dos pacotes em redes IPV6, o PMTU analisa todo o caminho que será percorrido pelo pacote, coletando o tamanho da MTU de cada circuito e dinamicamente atribui o tamanho máximo permito ao pacote. Essa fragmentação ocorre apenas na origem, e não e aceito a modificação durante o transporte do pacote (MCCANN; DEERING; MOGUL, tradução nossa).

4.1.9 *Jumbograms*

O IPv6 utiliza o cabeçalho de extensão conhecido como *Hop-By-Hop* chamado de *Jumbo Payload* ou *jumbograms*, ele permite o envio de pacotes com tamanho entre 65.536 e 4.294.967.295 Bytes de comprimento conforme descrito pela RFC 2675. Os protocolos de camada superior também recebem leves modificações para permitir o tamanho máximo do pacote (BORMAN; DEERING; HIDEN, 1999, tradução nossa).

4.1.10 Mobilidade

Segundo Loshin (2004), o suporte à mobilidade oferecido pelo IPv6, permite que um dispositivo móvel transite livremente entre redes distintas sem sofrer a mudança do seu endereçamento IP de origem, tornando este processo invisível para aplicações e protocolos de camadas superiores, independente de sua localidade o dispositivo continuará recebendo e enviando dados normalmente.

5 ANÁLISE E ESTRATÉGIAS DE MIGRAÇÃO PARA IPv6

Este capítulo apresenta um estudo que demonstra e comprova a necessidade de adoção da versão 6 do protocolo de IP. Inicialmente e realizada uma análise evolutiva dos protocolos de Internet abordados no trabalho, em seguida são descritas as principais técnicas de migração e implantação utilizadas atualmente no mercado.

5.1 ANÁLISE EVOLUTIVA DOS PROTOCOLOS

É interessante observar, que o protocolo IPv6, é uma evolução do seu antecessor, o IPv4, com isso não podemos realizar uma comparação direta, mais sim uma análise evolutiva, sendo essa uma das principais motivações para o estudo em questão. Com quase 40 anos de existência, o IPv4, e o principal protocolo de Internet atualmente e se mantem firme ao seu proposito original, que e de possibilitar a interligação de redes e dispositivos móveis muitas vezes complexas, porém de forma simples e direta. Por outro lado, o principal problema apresentado pelo IPv4 e a falta de endereçamento publico, já que conforme dados divulgados recentemente pela IANA, em fevereiro deste ano esgotou-se o estoque central de endereçamento IP público, sendo esse um fator determinante para adoção da nova versão do protocolo e assim garantindo o crescimento da Internet de forma globalizada (MACHADO, 2011).

5.1.1 Endereçamento

Demais, o endereçamento IPv4, oferece um espaço de 2^{32} (4.294.967.296 endereços), ou seja pouco mais de 4 bilhões de endereços IPv4, já a nova versão o IPv6 oferece um espaço de endereçamento de 2^{128}, cerca de 79 octilhões de endereços IP a mais do que no IPv4 ou precisamente (340.282.366.920.938.463.463.374.607.431.768.211.456 endereços) (KUROSE; ROSS, 2006; MOREIRAS, 2009).

5.1.2 Cabeçalho

Segundo Naugle (2001), o novo cabeçalho foi simplificado, e passou a ter o tamanho fixo de 40 *bytes*, sendo independente do tamanho do datagrama, essa mudança o

torna mais eficiente, pois reduz bastante a carga de processamento dos roteadores de borda da Internet e facilita o processo de convergência entre eles. Em outra perspectiva, analisando os dois cabeçalhos podemos identificar que o cabeçalho do IPv4, e composto por campos fixos, porém o tamanho do cabeçalho pode variar entre 20 e 60 *bytes* e contem os seguintes campos:

- Versão, IHL, Tipo de Serviço, Comprimento Total, Identificação, *Flag*, Deslocamento do Fragmento, Tempo de Vida, Protocolo, Verificação de Soma, Endereço de Origem, Endereço de Destino, Opções, e *Padding.*

Quando comparado com o seu antecessor, o cabeçalho do IPv6, apresenta as seguintes modificações:

- Três campos foram preservados do seu antecessor, são eles:
    1. Versão.
    2. Endereço de Origem.
    3. Endereço de destino.
- Quatro campos foram preservados do seu antecessor, porém sofreram alteração de nome, são eles:
    1. De “Tipo de serviço” para “Classe de Tráfego”.
    2. De “Comprimento Total” para “Tamanho dos Dados”.
    3. De “Protocolo” para “Próximo Cabeçalho”.
    4. De “Tempo de Vida” para “Limite de Saltos”.
- Seis campos foram removidos, são eles:
    1. IHL.
    2. Identificação.
    3. *Flag.*
    4. Deslocamento do Fragmento.
    5. Verificação de Soma.
    6. Opções e *Padding.*

E por fim, um novo campo foi adicionado, com a função de diferenciar e identificar pacotes com o mesmo fluxo é chamado de “Rótulo de Fluxo”.

5.1.3 Vantagens

Podemos destacar como principais vantagens (DAVIES, 2008, tradução nossa):

- Autoconfiguração;
- Descoberta de vizinhança;
- Mobilidade;
- O IPv6 permite *jumbograms*.
- Fácil integração com os atuais servidores de DNS, sendo necessário apenas oferecer suporte aos registros AAAA de tamanho fixo ou ao registros A6 de tamanha variável.
- Várias opções do IPv4 foram atribuídas a cabeçalhos de extensão.
- A opção de fragmentação não faz mais parte do cabeçalho básico do IPv6, essa função foi incorporada aos cabeçalhos de extensão.
- Capacidade de identificar fluxos de dados.
- Sistemas operacionais da Microsoft, Apple, Linux e Unix já oferecem suporte nativo para cliente final.
- Segurança nativa oferecendo suporte a autenticação e garantia de integridade.

5.1.4 Desvantagens

Uma dos principais desvantagens relacionado com a adoção do IPv6, e a utilização em Redes Locais (LAN – *Local Area Network*), pois nem todos os dispositivos de redes e aplicações oferecem suporte nativo ao protocolo, e muitos *hardwares* não oferecem possibilidade de atualização de *firmware*. Com isso a adoção do IPv6 deva ocorrer em larga escala nas Redes de Longa Distância (WAN – *World Area Network*), mais precisamente nas operadoras e provedores de Internet devido a alta demanda por endereçamento IP público.

Outra questão relevante e a falta de mão de obra qualificada, onde será necessário investir em treinamentos técnicos, isso ajuda a aumentar a relação “Custo x Benefício” e muitas vezes se torna um fator limitante.

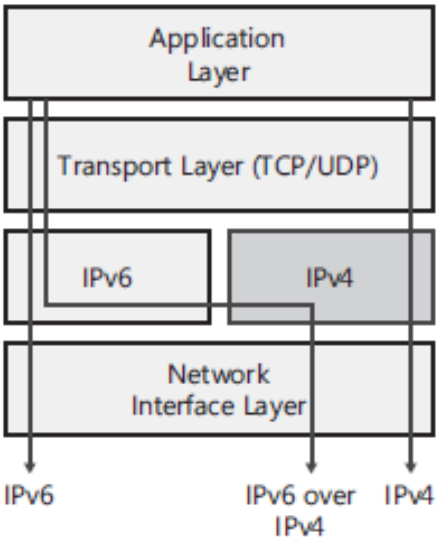
5.2 TRANSIÇÃO

A implantação do IPV6 se torna necessária para garantir o crescimento da Internet e principalmente a correção dos problemas apresentados pelo IPv4, e para que isso ocorra faz-se necessário a utilização de técnicas de transição que ocorrera em etapas, com a

finalidade de garantir e possibilitar a coexistência dos dois protocolos nesse primeiro momento. Mesmo sendo uma evolução do seu antecessor, o IPv6 não oferece compatibilidade com o mesmo. De qualquer forma, já era previsto um longo período de transição que devera ocorrer de forma transparente e com menor impacto possível, já que hoje bilhões de dispositivos funcionalidade do protocolo IP em suas aplicações ou em sua totalidade. Com isso podemos classificar as técnicas de transição em três categorias (SANTOS; MOREIRAS; ROCHA, 2010):

5.2.1 Pilha Dupla

Esta técnica possibilita que qualquer *host* opere com as duas pilhas de protocolo, IPv4 e IPv6. Deste modo ele passa a operar nas duas redes independentemente utilizando a mesma infraestrutura, conforme demostrado no esquema 19 (DAVIES, 2008, tradução nossa).

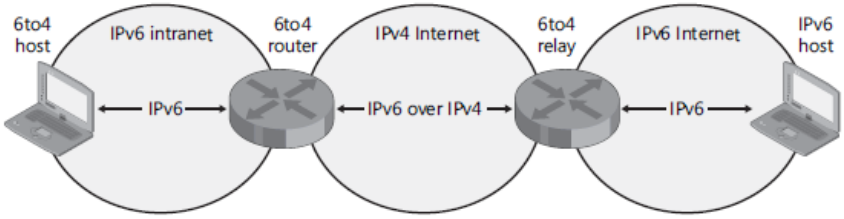


Esquema 19: *Type of packets with a dual IP layer architecture.*
Fonte: Davies, 2008.

5.2.2 Tunelamento

Esta técnica permite a criação de túneis, que possibilitam trafegar pacotes IPv6 encapsulados dentro dos pacotes IPv4 utilizando a infraestrutura IPv4 existente. Uma das vantagens não e necessário realizar criticas na rede. As principais técnicas de tunelamento utilizadas são (DAVIES, 2008, tradução nossa):

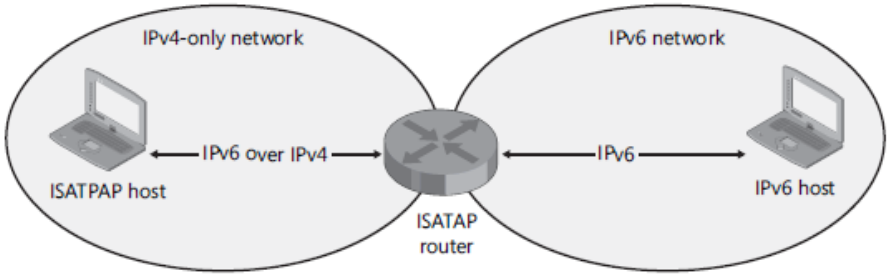
- **6to4:** Este técnica consiste em aplicar o tunelamento roteador-a-roteador, conforme demostrado no esquema 20 (Northrup; Mackin, 2009, tradução nossa).



Esquema 20: *6to4.*

Fonte: Northrup; Mackin, 2009.

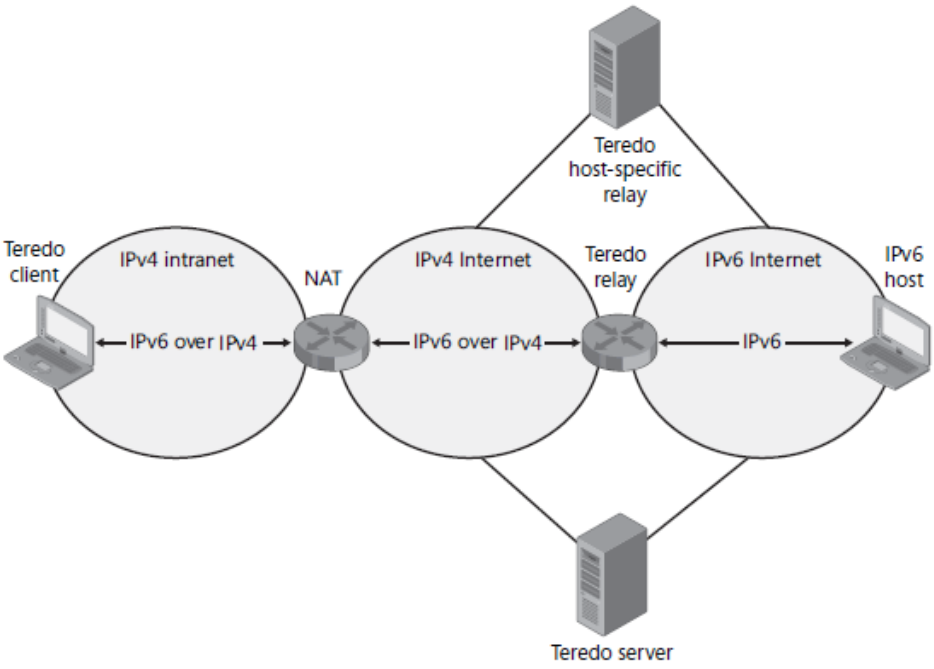
- ***ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)*:** Esta técnica consiste na conversão de endereços IPv4 para IPv6 ou IPv6 para IPv4, geralmente ocorre dentro do roteador, conforme exemplo do esquema 21 (Northrup; Mackin, 2009, tradução nossa).



Esquema 21: *ISATAP.*

Fonte: Northrup; Mackin, 2009.

- ***Teredo*:** Esta técnica possibilita que clientes pertencentes a uma rede que utiliza um roteador com NAT IPv4, utilizem o IPv6 na Internet. E importante lembrar que essa técnica só e utilizada quando nenhuma outra tecnologia de transição e oferecida. O esquema 22, demostra a infraestrutura complexa necessária para utilização do tunelamento *Teredo* (Northrup; Mackin, 2009, tradução nossa).



Esquema 22: *Teredo.*

Fonte: Northrup; Mackin, 2009.

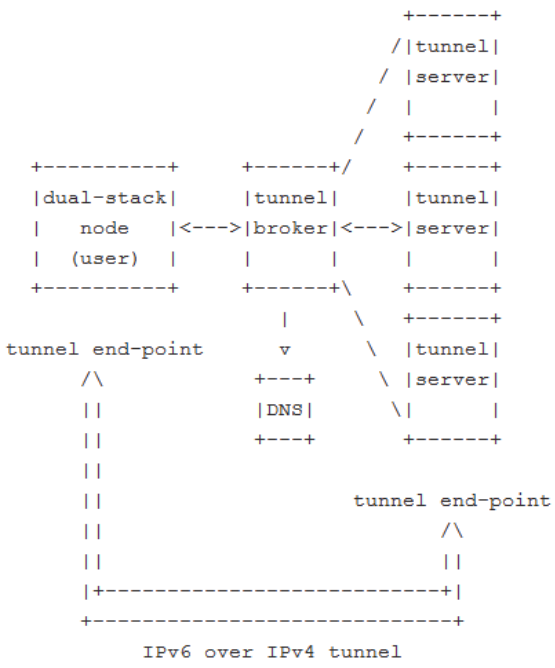
- **GRE (*Generic Routing Encapsulantion*):** Esta técnica possibilita criar um túnel estático entre dois *hosts*, para que eles possam estabelecer comunicação. O campo "GRE *Header*" demostrado no esquema 23, e utilizado para encapsulamento do protocolo IPv6 (FARINACCI et al., 2000, tradução nossa).

```
---------------------------------
|                               |
|       Delivery Header         |
|                               |
---------------------------------
|                               |
|       GRE Header              |
|                               |
---------------------------------
|                               |
|       Payload packet          |
|                               |
---------------------------------
```

Esquema 23: *Packet GRE.*

Fonte: FARINACCI et al., 2000.

- ***Tunnel Broker*:** Esta técnica possibilita que *hosts*, localizados dentro de uma rede IPv4 acessem redes IPv6, mediante utilização de *softwares* para criação dos túneis. O esquema 24 demostra o modo de operação desta esta técnica (DURAND et al., 2001).



Esquema 24: *Tunnel Broker*.

Fonte: DURAND et al., 2001.

5.2.3 Tradução

Nesta técnica de tradução e possível realizar o roteamento transparente para comunicação de *hosts* que apresente apenas um protocolo IP, ou *hosts*, que utilizem a pilha dupla. Após a escolha do método de tradução sua operação pode trabalhar apenas com o cabeçalho, com o endereçamento, utilizando o cabeçalho mais o endereçamento ou diretamente com uma ou mais camadas do modelo OSI.

6 CONCLUSÃO

O presente trabalho abordou os principais tópicos referentes ao protocolo de Internet mais utilizado atualmente e a sua nova versão.

O objetivo, deste estudo foi apresentar inicialmente os principais pontos relacionados com os protocolos IPv4 e IPv6, relacionando conceitos, fundamentos, evolução e tecnologias para possibilitar a compreensão dos próximos capítulos. Com isso possibilita ao leitor dar continuidade na leitura do trabalho independente da sua familiarização com o assunto.

Por fim, depois de compreendidas as funcionalidades dos protocolos de Internet IPv4 e IPv6, foi realizado uma análise com intuito de detalhar as principais características evolutivas dos protocolos, tendo como destaque as principais técnicas de transição utilizadas atualmente no mercado, são elas:

- **Pilha Dupla:** Possibilita a utilização dos dois protocolos em qualquer *host.*
- **Tunelamento:** Permite a criação de túneis, para trafegar os pacotes IPv6 encapsulados dentro dos pacotes IPv4 utilizando a infraestrutura existente
- **Tradução:** E possível realizar a comunicação e o roteamento transparente na rede.

É importante ressaltar as dificuldades encontradas na busca por matérias sobre o assunto, foram encontrado vários livros e artigos que tratavam a nova versão do protocolo IP (IPv6) ainda como *draft* (Em desenvolvimento), não sendo muito útil pois fugia do foco principal do trabalho. Portanto, além dos livros, foram utilizados muitos documentos com especificações técnicas, conhecido como RFC (*Request for Comments*) disponíveis na Internet.

Pode-se, concluir que não e necessário a adoção da nova versão do protocolo IP e que não existe um modelo de transição ideal para realizar um implantação de uma rede IPv6, pois torna-se extremamente necessário um planejamento buscando definir um modelo que se inicie primeiramente na capacitação técnica de todos envolvidos, seguido por um levantamento completo das reais necessidades, impactos, custo, e sempre considerando legados de *hardware* e *software* e por fim combinar técnicas de transição com intuito de

possibilitar não só a comunicações de *hosts*, mas também garantir que aplicações funcionem transparente independente da versão do protocolo escolhido.

REFERÊNCIAS

ATAKAN, Orcum; BRETZ, Stefan; PUGH, R. Larry; MURHAMMER, W. Martin; SUSUKI, Kazunari; WOOD, H. David. *TCP/IP Tutorial e Técnico.* 1. ed. São Paulo: Makron Books, 2000.

BORMAN, David A.; DEERING, Stephen E.; HIDEN, Robert M. *RFC 2975 – Ipv6 JUMBOGRAMS*. 1999. Disponível: <http://www.faqs.org/ rfcs/rfc2675.html>. Acesso em: 18 ago. 2011.

BOUND, Jim; VOLZ, Bernie; LEMON, Ted; PERKINS, Charles E.; MIKE, Carney. *RFC 3315 - Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. 2003. Disponível: <http://www.faqs.org/rfcs/rfc3315.html>. Acesso em: 20 jul. 2011.

BRADNER, Scott; MANKIN, Allison. *RFC 1550 - IP: Next Generation (IPng) White Paper Solicitation*. 1993. Disponível: <http://www.faqs.org/rfcs/rfc1550.html>. Acesso em: 20 mai. 2011.

BRADNER, Scott; MANKIN, Allison. *RFC 1752 - The Recommendation for the IP Next Gerenation Protocol*, 1995. Disponível: <http://www.faqs.org/rfcs/rfc1752.html>. Acesso em: 22 mai. 2011.

BRITT; David T.; DAVIS, Chuck; FORRESTER, Jason; LIU, Wei; MATTHEWS, Carolyn; PARZIALE; Lydia; ROSSELOT, Nicolas. *TCP/IP Tutorial and Technical Overview*. 8. ed. New York: IBM, 2006.

COMER, Douglas E. *Interligação em rede com TCP/IP*. 2. ed. Rio de Janeiro: Campus, 1998.

CONTA, Alex; DEERING, Stephen E.; GUPTA, Mukesh Ed.. *RFC 4443 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*. 2006. Disponível: <http://www.faqs.org/rfcs/rfc4443.html>. Acesso em: 15 jul. 2011.

DAVIES, Joseph. *Unrderstanding IPv6.* 2 .ed. Washington: Microsoft Press, 2008.

DEERING, Stephen E.; HINDEN, Robert M. *RFC 2460 - Internet Protocol, Version 6 (IPv6)*. 1998. Disponível: <http://www.faqs.org/rfcs/rfc2460.html>. Acesso em: 15 mai. 2011.

DEERING, Stephen E.; HINDEN, Robert M. *RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture*. 2003. Disponível: <http://www.faqs.org/rfcs/rfc3513.html>. Acesso em: 20 jun. 2011.

DURAND, Alain; FASANO, Paolo; GUARDINI, Ivano; LENTO, Domenico. *RFC 3053 - IPv6 Tunnel Broker*. 2001. Disponível: <http://www.faqs.org/rfcs/rfc3053.html>. Acesso em: 01 abr. 2011.

EGEVANG, Kjeld Borch; SRISURESH, Pyda. *RFC 3022 - Traditional IP Network Address Translator (Traditional NAT).* 2001. Disponível: <http://www.faqs.org/rfcs/rfc3022.html>. Acesso em: 05 mai. 2011.

FARINACCI, Dino; LI, Tony; HANKS, Stan; MEYER, David. *RFC 2784 - Generic Routing Encapsulation (GRE)*. 2000. Disponível: <http://www.faqs.org/rfcs/rfc2784.html>. Acesso em 01 set. 2011.

FILIPPETTI, Marco Aurélio. *CCNA 4.0 Guia Completo de Estudo***.** Florianopolis: Visual Books, 2006.

GROOT, Geert Jan de; KARRENBERG, Daniel; LEAR, Eliot; MOSKOWITZ, Robert G.; REKHTER, Yakov. *RFC 1918 - Address Allocation for Private Internet*. 1996. Disponível: <http://www.faqs.org/rfcs/rfc1918.html>. Acesso em: 01 mar. 2011.

IPv6.br. Guia didático de Endereçamento IPv6. 2010. Disponível: <http://www.ipv6.br/pub/IPV6/MenuIPv6CursoPresencial/enderec-v6.pdf> Acesso em: 02 jun. 2011.

HAGEN, Silvia. *IPv6 Essentials***.** 1. ed. Sebastopol: O'Reilly, 2002.

HUITEMA, Christian; CARPENTER, Brian. *RFC 3879 - Deprecating Site Local Addresses*. 2004. Disponível: <http://www.faqs.org/rfcs/rfc3879.html>. Acesso em: 05 jul. 2011.

HUNT, Craig. *TCP/IP Network Admnistration.* 3. ed. Washington: O'REILLY, 2002.

IANA. Number Resources. 2001. Disponível em: <http://www.iana.org/numbers/>. Acesso em 02 mar. 2011.

KUROSE, James F.; ROSS, Keith W. *Redes de Computadores Uma abordagem top-dpwn*. 3. ed. Rio de Janeiro: Pearson, 2006.

LI, Qing; JINMEI, Tatuya; SHIMA, Keiichi. *IPv6 Core Protocols Implementation.* San Francisco: Elsevier, 2007.

LOSHIN, Pete. *IPv6: Theory, Protocol, and Practice.* 2. ed. San Francisco: Elsevier, 2004.

MACHADO, Francine. *Últimos blocos IPv4 são alocados pela IANA.* 2011. Disponível: <http://www.nic.br/imprensa/clipping/2011/midia135.htm>. Acesso em: 10 mar. 2011.

MCCANN, Jack; DEERING, Stephen E.; MOGUL, Jeffrey. *RFC 1981 - Path MTU Discovery for IP version 6*. 1996. Disponível: <http://www.faqs.org/rfcs/rfc1981.html>. Acesso em: 18 jul. 2011.

MOGUL, Jeffrey. *RFC 917 - Internet Subnets*. 1984. Disponível: <http://www.faqs.org/rfcs/rfc917.html>. Acesso em: 18 fev. 2011.

MOREIRAS, Antônio Marcos. *Entenda o esgotamento do IPv4*. 2009. Disponível: <http://www.ipv6.br/IPV6/ArtigoEsgotamentoIPv4#A_Internet_e_os_n_meros_IP>. Acesso em: 22 fev. 2011.

NARTEN, Thomas; NORDMARK, Erik; SIMPSON, William Allen; SOLIMAN, Hesham. *RFC 4861 - Neighbor Discovery for IP version 6 (IPv6).* 2007. Disponível: <http://www.faqs.org/rfcs/rfc4861.html>. Acesso em: 28 jul. 2011.

NAUGLE, Matthew. *Guia Ilustrado do TCP/IP*. 1. ed. São Paulo: Berkeley, 2001.

NORTHRUP, Tony; MACKIN, J.C. *MCTS Self-Paced Training Kit (Exam 70-642): Configuring Windows Server 2008 Network Infrastructure***.** Washington: Microsoft Press, 2008.

ODOM, Wendell. *CCENT/CCNA ICND1 Official Exam Certification Guide***.** 2. ed. Indianapolis: Cisco Press, 2007.

ODOM, Wendell. *CCNA ICND2 Official Exam Certification Guide***.** 2. ed. Indianapolis: Cisco Press, 2008.

POSTEL, Jon. *RFC 791 – Internet Protocol*. 1981. Disponível: <http://www.faqs.org/rfcs/rfc791.html>. Acesso em: 28 jan. 2011.

SANTOS, Rodrigo Regis do; MOREIRAS, Antônio Marcos; ROCHA, Ailton Soares da. *Curso IPv6 Básico.* São Paulo: Comitê Gestor da Internet no Brasil, 2010.

STARLIN, Gorki. *TCP/IP***.** Rio de Janeiro: Book Express, 2001.

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

TANENBAUM, A. S; WETHERALL, David. *Redes de Computadores*. 5. ed. São Paulo: Pearson, 2011.

ZACON, Robert Hóbbes. *Hobbes' Internet Timeline 10.1*. 2011. Disponível: <http://www.zakon.org/robert/internet/timeline/>. Acesso em: 01 set. 2011.