HUGO DOS SANTOS MORPANINI

PROTOCOLOS DA INTERNET: IPV4 X IPV6

Inconfidentes – MG
2016

HUGO DOS SANTOS MORPANINI

PROTOCOLOS DA INTERNET: IPV4 X IPV6

Trabalho de Conclusão de Curso apresentado como pré-requisito de conclusão do curso de Graduação Tecnológica em Redes de Computadores no Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Campus Inconfidentes, para obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: André Luigi Amaral Di Salvo

Inconfidentes-MG
2016

HUGO DOS SANTOS MORPANINI

PROTOCOLOS DA INTERNET: IPV4 X IPV6

Data da aprovação:_____de_____20___

André Luigi Amaral Di Salvo

Orientador

Alessandro de Castro Borges

Membro 1

Roberta Bonamiche Guide Garcia

Membro 2

RESUMO

As redes de computadores, sobretudo a Internet, utilizam um protocolo denominado IP, que identifica cada dispositivo conectado à rede e que contém informações importantes para o roteamento de uma mensagem entre a origem e o destino, possibilitando a comunicação entre dispositivos geograficamente distantes. Entretanto, com a grande variedade de dispositivos que conectam-se à rede, o protocolo original conhecido como IPv4 demonstrou-se ineficiente não sendo capaz de suprir a grande demanda por endereços, o que levou a necessidade da criação de um novo protocolo, IPv6. Essa nova versão tem como premissa básica suprir as deficiências de endereçamento apresentadas na versão anterior, além de disponibilizar novos serviços e mecanismos de controle. Este trabalho apresenta um estudo teórico dos dois protocolos analisando suas características, diferenças e semelhanças. Ao final, é apresentado um teste de desempenho entre os protocolos.

ABSTRACT

Computer networks, particularly the Internet, use a protocol called IP, which identifies each device connected to the network and that contains important information for routing a message between the source and destination, allowing communication between geographically distant devices. However, with the wide variety of devices that connect to the network, the original protocol known as IPv4 was demonstrated inefficient, not being able to meet the great demand for addresses, which led to the need to create a new protocol, IPv6 . This new version has as basic premise supply the addressing deficiencies presented in the previous version, in addition to providing new services and control mechanisms. This paper presents a theoretical study of the two protocols analyzing its characteristics, differences and similarities. Finally, a performance test between the protocols is displayed.

SUMÁRIO

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE QUADROS

1. INTRODUÇÃO

Atualmente, é impossível imaginar uma sociedade desenvolvida sem acesso às tecnologias de informação e comunicação (TIC). Neste cenário, a Internet é um dos principais canais de comunicação, interligando milhões de usuários por meio de uma rede de computadores interconectados entre si. A primeira rede de computadores foi desenvolvida no *Advanced Research Project Agency* (ARPA) nos Estados Unidos. Segundo Licklider (1960 e 1965), a ideia inicial era uma rede de computadores que permitisse o trabalho cooperativo em grupos, mesmo que fossem integrados por pessoas geograficamente distantes. Além disso, deveria permitir também o compartilhamento de recursos escassos, como por exemplo, o supercomputador ILLIAC IV em construção na Universidade de Illinois, com o patrocínio da própria ARPA. O projeto amadureceu até 1967, quando Lawrence Robert integrou a equipe da ARPA tornando o projeto uma realidade. Esse projeto foi denominado *Advanded Research Project Agency Network* (ARPANet).

Segundo Roberts (1988), o objetivo inicial da ARPANet era um sistema de comunicação que não fosse interrompido por avarias locais. No auge da guerra fria, a preocupação dos militares americanos era uma rede de telecomunicações que não pudesse ser destruída por um ataque localizado.

Em 1970, a ARPANET teve seu primeiro ensaio prático. Este envolveu quatro universidades: i) Universidade da Califórnia em Los Angeles, através do centro de desenvolvimento de "*software*"; ii) *Stanford Research Institute*; iii) Universidade da Califórnia em Santa Bárbara; iv) Universidade de Utah.

O sucesso dos testes iniciais da ARPANet, foram tão expressivos, que em 1972, a rede foi exposta à comunidade disponibilizando diversos serviços, entre eles, acesso remoto e autenticação de usuários. A Figura 1.1 mostra a expansão da rede nos seus primeiros anos.

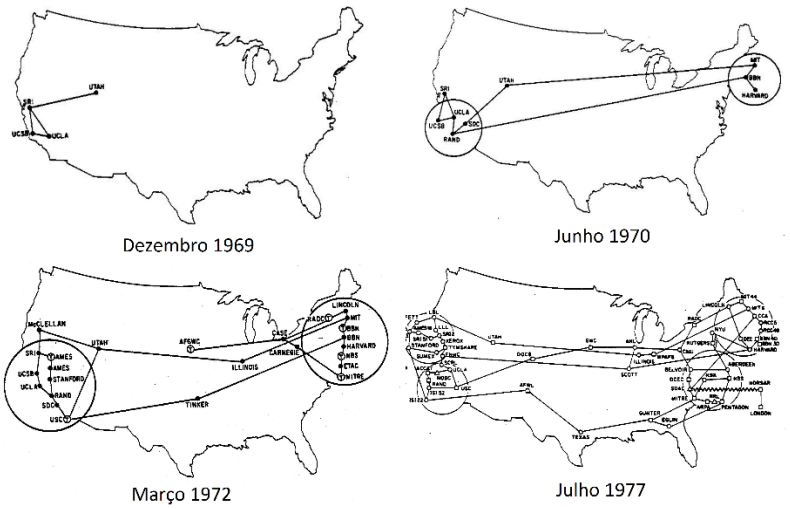


Figura 1.1 – expansão da ARPANet (Fonte, LICKLIDER, 1960)

Ainda na década de 1970, outras instituições que faziam trabalhos relacionados com a defesa americana tiveram permissão de conectar-se à ARPAnet, realizando então o primeiro experimento de suas funcionalidades. Essas empresas incluíram na rede computadores de diferentes plataformas de *hardware* e *software* demonstrando que a comunicação entre eles era possível. Logo rebatizaram a ARPANet para DARPAnet, inserindo um D que significava *Defense*, em referência ao Departamento de Defesa Americano.

Em 1973, a DARPAnet suportava uma grande variedade de serviços tais como: i) *login* remoto; ii) correio eletrônico. Esses dois serviços surpreenderam as expectativas de uso da rede e o número de conexões expandiu-se rapidamente. Isso fez com que a ARPANet tivesse que ser dividida em duas novas redes, a MILNet destinada a assuntos militares e a própria ARPANet, agora sem fins militares e destinada ao público civil. Essa segunda é a precursora da Internet utilizada nos dias atuais.

Com essa expansão, o protocolo *Network Control Protocol* (NCP) até então utilizado em todas as comunicações, tornou-se inadequado. Além de não possuir controle de erro fim-a-fim, ele poderia travar a rede caso algum pacote se perdesse no meio da comunicação. Frente a essa situação, um novo protocolo começou a ser desenvolvido. Esse novo protocolo, chamado *Transmission Control Protocol* (TCP), provia todo o transporte e serviço de encaminhamento da rede. Para um melhor controle, ele foi subdividido em dois protocolos, o TCP, que tinha por finalidade o controle de fluxo e recuperação de pacotes perdidos, e o IP,

que tratava apenas do endereçamento e encaminhamento de pacotes. Esse novo conjunto foi comumente chamado de TCP/IP.

Além do TCP/IP, um protocolo alternativo denominado *User Datagram Protocol* (UDP) foi também desenvolvido. Este era uma alternativa para aplicações que não necessitavam utilizar o TCP/IP.

Após a popularização dos serviços da ARPANet até os dias atuais, o protocolo TCP/IP tem sido amplamente utilizado em diversos dispositivos de comunicação conectados à Internet, porém, a sua capacidade de endereçamento está se esgotando. Diante disso surgiu, o IPv6. Esse protocolo tem como principal finalidade fornecer endereçamento para qualquer dispositivo que necessite conectar-se à Internet. Com base nesse novo protocolo, este trabalho tem como principal objetivo realizar um comparativo teórico mostrando as principais características e diferenças entre o protocolo IP originalmente desenvolvido, comumente chamado de IPv4, e a sua nova versão, o IPv6.

1.1. OBJETIVO GERAL

Realizar um estudo comparativo entre as versões IPv4 e IPv6 do protocolo IP, apresentando suas principais características e particularidades.

1.2. OBJETIVOS ESPECÍFICOS

- Apresentar um histórico sobre a evolução dos protocolos de Internet.
- Apresentar a estrutura do protocolo IPv4.
- Apresentar a estrutura do protocolo IPv6.
- Comparar as estruturas dos dois protocolos.
- Apresentar os testes de desempenho dos dois protocolos.
- Apresentar o panorama atual de migração no Brasil da versão 4 para a versão 6 do protocolo IP.

2. PROTOCOLO DA INTERNET

Desde os primeiros ensaios das redes de computadores até os dias atuais todo o processo de comunicação entre máquinas envolve protocolos, que são um conjunto de regras que padronizam as formas de comunicação entre máquinas. Com a ARPANet e, consequentemente, a Internet, isso não foi diferente. Inicialmente a ARPANet foi implementada utilizando o *Network Control Program* (NCP). Posteriormente, este protocolo foi substituído pelo *Internet Protocol* (IP). Atualmente, a nova versão do IP começa a ganhar espaço na rede mundial de computadores.

2.1. NETWORK CONTROL PROGRAM - NCP

No início do projeto da ARPANet não existiam procedimentos ou sistemas que permitissem o compartilhamento de informações entre os equipamentos que faziam parte da rede. Para resolver esse problema foi criado o *Network Working Group* (NWG), Grupo de Trabalho de Rede, para assumir o desafio de criar um protocolo de comunicação que interligasse as máquinas.

Além de interligar as máquinas, a equipe notou também a necessidade de mais duas funcionalidades: i) criar uma forma que usuários pudessem se conectar ao sistema remotamente; ii) tornar possível a transferência de arquivos entre máquinas. O acesso remoto ficou conhecido pelo protocolo Telnet, e a transferência de arquivos foi implementada pelo *File Transfer Protocol* (FTP). A equipe submeteu esses dois protocolos a Larry Roberts, que os achou pouco ambiciosos e que mais funções e processos deveriam ser inclusos. Foi então

que a equipe começou a trabalhar no *Network Control Program* (NCP), um protocolo fim-a-fim que permitia a comunicação de computadores dentro da rede. Além disso, este protocolo permita que a rede se expandisse. Entre suas funções, o NCP permitia o controle de caminho e o controle de fluxo de dados, estabelecia a prática de uso de endereços numéricos e foi o precursor do *Domain Name System* (DNS), que relaciona um endereço numérico a uma lista de nomes, tornando mais fácil a localização de um equipamento em uma rede. O NCP tornou possível o envio de dados a partir da comutação de pacotes, no qual uma mensagem é dividida em pedaços menores e pode ser transportada por caminhos diferentes, reduzindo assim o impacto na rede, e serviu de base para o protocolo TCP/IP (STRICKLAND,n.d.).

2.2. IPV4

O protocolo IPv4, é um serviço da camada de rede implementado pelo conjunto de protocolos TCP/IP. O protocolo IP fornece apenas as funções necessárias para enviar um pacote de uma origem a um destino através de um sistema de redes interconectadas. As características básicas do protocolo IP são: i) não orientado a conexão, ou seja, nenhuma conexão é estabelecida entre a origem e o destino dos pacotes antes de encaminhar os dados; ii) não confiável, ou seja, fornece um serviço de envio pelo menor esforço mas não garante a entrega dos pacotes.

Com essas características percebe-se que o IP não fornece nenhuma verificação, muito menos monitoramento de erros. Se a confiabilidade for importante, o IP deverá ser combinado com um protocolo confiável, como TCP. O protocolo IP opera em qualquer tipo físico, podendo ser utilizado em conexões metálicas, ópticas ou por redes sem fio.

Em uma rede de troca de pacotes que utilize a estratégia de datagramas, os mesmos são manipulados de maneira independente e podem seguir uma rota diferente entre a origem e o destino. Essa característica implica que datagramas enviados pela mesma origem ao mesmo destino podem chegar fora de ordem, e alguns deles podem ser perdidos ou corrompidos (TANENBAUN, 2003).

Apesar do protocolo IP, ser um grande sucesso, ele acabou sendo vítima de sua própria popularidade. Em sua implementação acreditava-se que a quantidade de endereços que ele podia oferecer seria capaz de suprir todas as requisições de endereços solicitadas, pois um endereço de 32 bits oferta mais de 4 bilhões de endereços únicos. Atualmente, sabe-se que a quantidade de dispositivos conectados à Internet, e que ainda continuarão a se conectar no futuro, ultrapassa tranquilamente esse número. Atento a isso, o *Internet Assigned Numbers*

Authority (IANA), entidade máxima que controla, organiza e distribui os endereços IP às organizações, tratou de criar mecanismos e protocolos que visavam resolver, ou ao menos minimizar, o problema de endereçamentos. Protocolos como CIDR, NAT, entre outros, foram desenvolvidos, o que ajudou a amenizar a situação. Mesmo assim, o IANA criou um grupo de pesquisadores com a finalidade de trabalhar no desenvolvimento de um novo protocolo que viria a substituir o atual IPv4, este protocolo recebeu o nome de *IP next genaretion* (IPng)**.** Posteriormente, esse protocolo foi denominado *Internet Protocol - Version* 6, (IPv6) sendo referenciado na RFC [2373; 2460] (KUROSE e ROSS, 2006).

2.3. SISTEMA DE CAMADAS – MODELO OSI X MODELO TCP/IPV4

Para garantir que o protocolo IPv4 pudesse se comunicar com qualquer sistema conectado à rede, e pudesse ser utilizado por qualquer fabricante de equipamentos, foi implementado seguindo os padrões da Organização Internacional de Normatização (*ISO - International Standards Organization*) que, no início dos anos 1980, aprovou o modelo de referência *Open System Interconnection* (OSI). Esse modelo, que é aplicado a qualquer tipo de rede, é um modelo que divide as redes de computadores em 7 (sete) camadas pré-definidas, que podem ser visualizadas na Figura 2.1.

Figura 2.1 – Camadas do Modelo OSI (Adaptado – FOROUZAN, 2008)

Cada camada do Modelo OSI possui uma função específica e serve de abstração para a camada superior. A Tabela 1 descreve resumidamente as funções de cada camada deste modelo.

Tabela 1 – Funções das camadas do Modelo OSI *(Adaptado – FOROUZAN, 2008)*

Camada	Função
Física	Coordena as funções exigidas para transportar um fluxo de bits por um meio físico, lida com especificações mecânicas e elétricas da interface e do meio de transmissão, além de definir os procedimentos e funções que os dispositivos físicos executam para que a transmissão ocorra.
Enlace	Responsável por mover quadros de um hop (nó) para o próximo, oferece, mecanismos de controle de acesso ao meio, controle de erros, controle de fluxo, endereçamento físico, divide o fluxo de bits recebidos da camada de rede em unidades de dados gerenciáveis chamadas de frames.
Rede	Esta camada é responsável pelo envio de um pacote da origem até o destino, passando possivelmente por várias redes (links). Tornado possível, a comunicação entre redes diferentes.
Transporte	Camada responsável pela transferência eficiente, confiável e econômica dos dados entre as máquinas origem e destino, independente da topologia da rede e da configuração garantido que estes cheguem na ordem e intactos ao destino.
Sessão	Esta camada estabelece, mantém e sincroniza a interação entre sistemas que se comunicam, permitindo assim um dialogo em ambas as direções (*full-duplex*) ou apenas uma direção de cada vez (*half-duplex*).
Apresentação	Responsável por converter os dados recebidos pela camada de aplicação, em um formato comum para sistemas independentes.
Aplicação	Esta é a camada mais próxima do usuário final, permitindo acesso à rede através de interfaces do usuário, fornecendo suporte a serviços como correio eletrônico, acesso remoto, transferência de arquivos dentre outras funções.

Segundo Forouzan (2008), o conjunto de protocolos TCP/IP foi desenvolvido antes do modelo OSI, o que significa que as camadas no conjunto de protocolos TCP/IP não correspondem exatamente às que aparecem no modelo OSI. Então, mesmo seguindo os padrões definidos pela ISO para comunicação de dados, o protocolo IPv4 possui apenas quatro 4 camadas, diferentemente do modelo OSI. Isso pode ser visualizado na Figura 2.2.

Figura 2.2 - Relação modelos OSI e TCP/IP (Adaptado – FOROUZAN, 2008)

A camada de aplicativo do modelo IPv4 engloba os serviços referentes às camadas Aplicação, Apresentação e Sessão do Modelo OSI. As camadas de Transporte e de Rede atuam respectivamente nas mesmas camadas. As camadas Física e de Enlace de dados no modelo IPv4, também conhecida como "camada de acesso à rede", engloba os serviços das camadas de Enlace de dados e Física do Modelo OSI. A tabela 2 descreve resumidamente as funções de cada camada do modelo TCP/IP.

Tabela 2 – Funções das camadas – Modelo TCP/IP (*Adaptado FOROUZAN, 2008*)

Camada	**Função**
Acesso à Rede	Nesta camada são realizados em conjuntos os serviços das camadas física e de enlace como endereçamento físico, controle de fluxo e erros, representação de bits etc.
Rede	Esta camada, mais precisamente camada de interconexão de rede, é onde atua IP e os demais protocolos de apoio.
Transporte	Nesta camada são definidos os protocolos de transporte como TCP para entrega confiável, UDP para entrega não confiável e SCTP para controle de transmissão de dados.
Aplicativo	Esta camada equivale às camadas de sessão, apresentação e de aplicativo do modelo OSI, é a camada mais próxima do usuário final e diversos protocolos são definidos nessa camada.

Dentre as camadas descritas acima, a camada de rede fornece os serviços, que permitem a dispositivos finais trocarem dados através da rede. Para realizar esse transporte denominado fim-a-fim, esta camada utiliza quatro serviços básicos. São eles:

- **Endereçamento de dispositivos finais** - Assim como um aparelho telefônico comum, que contém um número único e exclusivo que o identifica e o possibilita realizar ligações, um computador ou qualquer outro dispositivo que venha a se conectar à Internet deve ser

configurado com um endereço IP também exclusivo, para vir a ser identificado na rede e assim realizar suas transmissões.

- **Encapsulamento** - A camada de rede recebe uma unidade de dados de protocolo (PDU) da camada de transporte, neste processo a camada de rede adiciona informações do cabeçalho IP, como endereços IPs de origem e destino. Após a adição destas informações esta PDU recebe o nome de pacote.
- **Roteamento** - A camada de rede também tem como função direcionar os pacotes a um *host* de destino, para que isso aconteça os pacotes devem ser processados em dispositivos intermediários conhecidos como roteadores antes de chegar ao destino final. Cada rota ou dispositivo intermediário que o pacote passa e é processado é chamado de salto.
- **Desencapsulamento** – Assim que o pacote chega à camada de rede do *host* destino o dispositivo examina o cabeçalho IP do pacote, se o endereço IP do cabeçalho for correspondente ao seu próprio endereço IP o cabeçalho é removido do pacote, resultando na PDU gerada na camada 4 sendo esta então passada para o serviço apropriado na camada de transporte.

De acordo com COMMER (2006), na camada de rede a Internet pode ser vista como um conjunto de sub-redes ou sistemas autônomos como escritórios, *Lan houses*, Universidades, provedores de serviços de Internet (ISP) e outros diversos tipos de repartições públicas ou privadas conectadas entre si. Essas redes são denominadas *Local Área Network* (LANs), e por sua vez, estão conectados a um dos diversos *backbones*, que são linhas principais de comunicação construídas a partir de interconexões de redes de média e longa distância através de roteadores rápidos, que conectam Países e continentes e que formam a estrutura principal da rede mundial de computadores, a Internet.

2.4. IPV6

O protocolo IPv4 mostrou-se no começo muito eficiente, oferecendo ótimas funcionalidades e atendendo perfeitamente a todos os requisitos que uma rede de computadores necessita. Porém, a rápida expansão que ocorreu com a Internet nas duas últimas décadas tornou evidente que o protocolo IP, na sua versão atual, não seria capaz de suportar todos os dispositivos conectados à rede.

Quando o *Internet Engineering Task Force* (IETF), começou a trabalhar na nova versão do protocolo IP, atentou-se que o mesmo, além de possuir todas as funcionalidades da atual versão, deveria também atender uma série de pré-requisitos que o protocolo antigo não

atendia, entre eles, ser capaz de garantir o não esgotamento de endereços, o que permite o crescimento da rede, reduzir o custo do processamento em roteadores, oferecer suporte a cabeçalhos de extensão, a fim de permitir um roteamento mais eficaz, ser capaz de identificar fluxo de dados, o que permite a identificação de pacotes pertencentes a um determinado trafego de fluxo, além de oferecer suporte a mecanismos de autenticação e privacidade, o que garante a confidencialidade e integridade dos dados transmitidos (SANTOS et al., 2010). Deste ponto em diante o IETF solicitou aos interessados que apresentassem suas propostas na RFC 1550. Ao todo vinte uma propostas foram recebidas, sendo que apenas sete foram consideradas propostas completas e interessantes para estudo. No final, três propostas foram selecionadas e publicadas no *IEEE Network*. Depois de um período de muito estudo, discussão e disputa, uma versão combinada e modificada de Deering e Francis foi selecionada e recebeu o nome de *Simple Internet Protocol Plus* (SIPP), à qual foi atribuída a designação IPv6.

A nova versão do protocolo IP, o IPv6 atendeu a todos os objetivos propostos pela IETF, sendo capaz de aceitar bilhões de *hosts*, devido o espaço reservado para endereçamento ter passado de 32 bits para 128 bits, permitindo níveis mais específicos de agregação de endereços, e passando a implementar mecanismos de autoconfiguração. A nova versão do protocolo IP sofreu uma simplificação em seu cabeçalho em relação à versão antiga, o que propicia a redução dos custos do processamento dos pacotes nos dispositivos intermediários em que estes são processados. Passou a oferecer também suporte a cabeçalhos de extensão, eliminando as opções, isso permite que o cabeçalho tenha um tamanho fixo, o que torna o roteamento mais eficaz e que também é capaz de fornecer mecanismos de autenticação e integridade. Oferece também introdução a opções futuras, escalabilidade, e permite o crescimento da rede. Vale ressaltar que a exemplo do IPv4, o IPv6 é um protocolo que atua na camada de rede, implementado pelo conjunto de protocolos TCP/IP, e que nessa camada as unidades de dados que são tratadas pelos roteadores são denominados datagramas (SANTOS et al., 2010).

3. DATAGRAMA

Um datagrama ou células, como referenciado na RFC 1954, é uma unidade de dados completa e independente que contém informações suficientes para que seja roteada desde sua origem até seu destino sem a necessidade de confiar em permutas anteriores estre essas duas fontes. Assim como acontece com os pacotes na camada de transporte, cada datagrama é formado por um cabeçalho e uma área de dados. A operação no modo datagrama é uma comunicação não confiável, ou seja, não usa nenhum tipo de reconhecimento entre nós intermediários e muito menos qualquer tipo de controle de fluxo. No datagrama o caminho através da rede é definido individualmente e é possível ainda usar sempre o melhor caminho possível (KUROSE e ROSS, 2006).

3.1. DATAGRAMA IPV4

Na camada de rede, os pacotes são denominados datagramas. Um datagrama IPv4 consiste em um cabeçalho de tamanho fixo de 20 bytes e uma parte opcional de tamanho variável de 40 bytes, totalizando um datagrama com tamanho total de 60 bytes. O datagrama IPv4 contém campos de informação importantes e fundamentais para o encaminhamento e montagem das mensagens. A Figura 3.1 apresenta seu formato e seus campos segundo KUROSE e ROSS (2006) e FOROUZAN (2008).

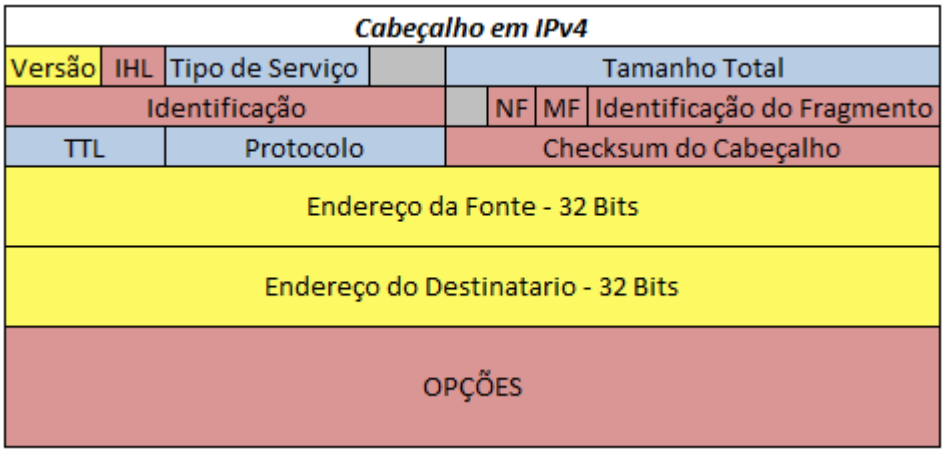


Figura 3.1 - Formato do datagrama IPv4 (CANNO, 2013)

- **Versão:** Esse campo contém 4 bits e indica qual versão do protocolo IP que foi utilizado para criar o datagrama. Ele é usado para verificar se o emissor, receptor e quaisquer roteadores entre eles concordam sobre o formato do datagrama. Todo IP precisa verificar o campo de versão antes de processar um datagrama, isso garante que ele combine com o formato que o software espera. Se os padrões mudarem, as máquinas irão rejeitar datagramas com versões de protocolo que diferem da sua.
- **Comprimento do cabeçalho (IHL):** Esse campo também contém 4 quatro bits e tem como principal função identificar onde realmente começam os dados no datagrama IP. A maioria dos datagrama IP não contém opções, portanto, o datagrama IP típico tem um campo de 20 bytes. Como o tamanho do cabeçalho não é constante, existe um campo IHL que informa seu tamanho em palavras de 32 bits, o valor mínimo é 5, quando não existe nenhuma opção presente, e o valor máximo é 15, o que limita o cabeçalho a 60 bytes e o campo *options* a 40 bytes.
- **Tipo de serviço**: Esse campo está incluso no cabeçalho do IPv4 com o intuito de diferenciar os diversos tipos de datagramas IP, ou seja distinguir datagramas de tempo real, como por exemplo os de arquivos FTP ou aplicações de telefonia IP, de datagramas que não requerem prioridade de serviço.
- **Tamanho total (*Total length*)**: Esse campo indica o tamanho total do datagrama IP medido em bytes, ou seja, cabeçalho mais os dados. Esse campo possui 16 bits de comprimento, o tamanho máximo de um datagrama IP é de 65535 bytes, no entanto, os datagramas raramente são maiores que 1500 bytes. O que determina o tamanho máximo de um datagrama é o *maximum transmission United* (MTU), unidade máxima de transmissão.

- **Identificador**: Esse campo também contém 16 bits e é necessário para permitir que o host de destino determine a qual datagrama pertence um fragmento recém-chegado. Todos os fragmentos de um mesmo datagrama contém o mesmo valor de identificação.
- ***Flags***: Neste campo há um bit não utilizado e dois campos de um bit cada. DF significa *Don't Fragment* (não fragmentar). Isso indica que a máquina de origem, não poderá fragmentar o datagrama a ser enviado, por que a máquina de destino não será capaz de juntar os fragmentos de um datagrama recém-chegado. MF significa *More Fragment* (mais fragmentos). Todos os fragmentos de um datagrama, exceto o último, tem esse conjunto de bits necessário para saber quando todos os fragmentos de um datagrama chegaram.
- **Deslocamento de fragmentação (*fragment offset*)**: esse campo contém 13 bits e informa a qual ponto do datagrama atual o fragmento pertence. Todos os datagramas, com exceção do último, devem ser múltiplos de 8 bits, a unidade elementar de fragmento. Como são fornecidos 13 bits, existem no máximo 8192 fragmentos por datagrama, resultando em um tamanho máximo de datagramas igual a 65.536 bytes, um a mais que o campo *total length*.
- **TTL (*Time to live* - tempo de vida do pacote)**: Esse campo tem como finalidade garantir que o datagrama não circule para sempre na rede, funcionando como um contador e é decrementado de uma unidade a cada vez que um datagrama é processado em um roteador, se o campo TTL chegar a zero e o datagrama não tiver chego ao seu destino este será descartado e um pacote de advertência será enviado ao host de origem.
- **Protocolo**: Utilizado somente quando um datagrama chega ao seu destino final, o valor desse campo indica ao protocolo da camada adjacente, ou seja, camada de transporte que o datagrama está utilizando. Por exemplo, o valor 17 indica que os dados serão passados ao UDP, e se valor for 6, o valor será passado ao TCP.
- **Soma e verificação de cabeçalho (*Header checksum*)**: Esse campo de 16 bits auxilia um roteador na detecção de erros de bits em um datagrama IP recebido. Esse total de verificação é útil para a detecção de erros gerados por palavras de memória incorretas em um roteador. O algoritmo tem como finalidade de somar todas as meias palavras de 16 bits à medida que elas chegam, utilizando a aritmética de complemento de 1, e depois calculando o complemento de um dos resultados.
- **Endereços IP de origem**: Esse campo de 32 bits define o endereço IP de origem de *host* específico e tem como finalidade identificar o mesmo na rede. Ele deve permanecer inalterado durante o tempo que o datagrama viajar de uma origem até o *host* de destino.

- **Endereços IP de destino**: Esse campo de 32 bits define o endereço IP de destino de host específico e tem como finalidade identificar o mesmo na rede. Ele deve permanecer inalterado durante o tempo que o datagrama viajar de uma origem até o *host* de destino.
- **Opções**: Este campo permite ampliar o cabeçalho IP. A intenção é que estas opções de cabeçalho sejam usadas raramente. A existência do campo opções já é um agravante, uma vez que cabeçalhos de datagramas podem ter comprimentos variáveis, além disso, o fato de datagramas requererem processamento de opções faz com que a quantidade de tempo de processamento de um datagrama IP em um roteador sofra muitas variações, o que é muito significativo em roteadores e hospedeiros de alto desempenho (FOROUZAN, 2008).

3.2. DATAGRAMA IPV6

O formato do datagrama IPv6 apresenta certas alterações em relação ao formato do datagrama IPv4. Alguns campos foram eliminados ou passaram a ser opcionais para utilizações especificas e pontuais. O novo formato é resultado da evolução do protocolo para atender as novas demandas das redes de computadores modernas, sobretudo a Internet. Além disso, esse datagrama foi desenvolvido possibilitando ofertar novos serviços e atender a qualquer demanda que no futuro venha surgir. A Figura 3.2 mostra o formato do datagrama IPv6, conforme TANENBAUM (2003).

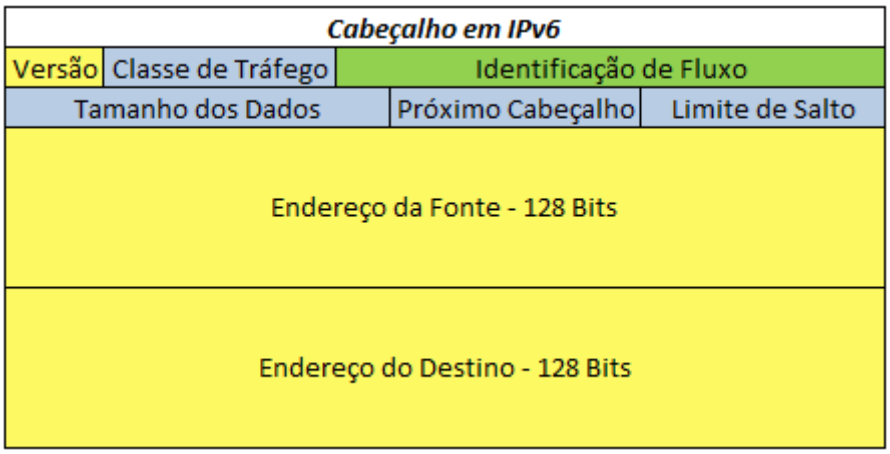


Figura 3.2 - O formato do cabeçalho IPv6 (CANNO, 2013)

- **Versão**: O campo versão contém 4 bits e identifica a versão do protocolo que está sendo usado pelo datagrama, no caso do IPv6 o valor do campo versão será seis, durante o período de transição que ainda pode levar um certo tempo para ser concluída. Os roteadores poderão usar este campo para identificar a versão do protocolo utilizado pelo datagrama recebido. A realização desse teste desperdiça algumas instruções no caminho

critico, o que leva muitas implementações a evita-lo, utilizando algum campo no cabeçalho de enlace de dados para diferenciar os pacotes IPv4 dos pacotes IPv6. Este tipo de ação possibilita que os pacotes sejam passados para o tratador da camada de rede correto, porém esta técnica de fazer com que a camada de enlace de dados tenha conhecimento do significado do bits passados a ela pela camada superior viola completamente o princípio de projeto.

- **Classe de tráfego**: Este campo contém 8 bits e tem função semelhante ao *Type of Services (*ToS*)* no IPv4, ou seja, distinguir pacotes com diferentes requisitos de tempo real daqueles que não tem tanta prioridade. Desde o início o protocolo IP possuía um campo destinado a este propósito, porém só era utilizado esporadicamente por roteadores, atualmente experiências estão sendo realizadas para definir a melhor maneira de utiliza-la para transmissão multimídia.
- **Identificação de Fluxo**: Esse campo contém 20 bits e é utilizado para identificar o fluxo de datagramas. Estando ainda em fase experimental permite que um fluxo de uma determinada conexão, que tenha severas restrições em termos de retardo e que necessite de uma determinada largura de banda, possa configurar com antecedência seu fluxo de dados e ter um identificador atribuído a ele. Assim quando um pacote aparecer com este campo diferente de zero, todos os roteadores podem verificar em suas tabelas internas que tipo de tratamento especial esse pacote precisa. Esses tipos de fluxos na prática tentam oferecer a flexibilidade de uma sub-rede de datagramas juntamente com uma sub-rede de circuitos virtuais.
- **Tamanho dos dados:** Este campo contém 16 bits e tem como função determinar o número de bytes que seguem o cabeçalho de 40 bytes de um pacote IPv6, ou seja, os 40 bytes deixaram de ser contados como parte do tamanho do pacote. No cabeçalho IPv4, esse campo era chamado de *Total length*.
- **Próximo cabeçalho:** Esse campo contém 8 bits e identifica à qual protocolo da camada de transporte (TCP ou UDP), o conteúdo do campo de dados de um datagrama IPv6 deverá ser entregue. Esse campo informa quais dos seis cabeçalhos de extensão seguem esse cabeçalho, se houver algum.
- **Limite de salto:** Esse campo é usado para impedir que um pacote tenha duração eterna. O seu conteúdo é decrementado cada vez que este é processado e repassado por um roteador, sendo descartado assim que este campo chegue a zero e ainda não chegou ao seu destino.

- **Endereços de fonte e destino:** Este é um campo de 16 bytes representado sob a forma de oito grupos de quatro dígitos hexadecimais, separado por sinais de dois-pontos entre os grupos, que tem como objetivo identificar o endereço do *host* de origem e o endereço do *host* de destino em um datagrama IPv6.
- **Cabeçalho de extensão:** Tendo em vista, que inicialmente seria necessária a utilização de alguns campos do cabeçalho IPv4, o IPv6 introduziu o conceito de um cabeçalho de extensão opcional, localizados entre o cabeçalho base e o cabeçalho da camada adjacente, não existindo nem quantidade nem tamanho fixo definido para estes tipos de cabeçalhos, podendo existir múltiplos cabeçalhos de extensão em um mesmo pacote. Caso isto ocorra, estes cabeçalhos deverão ser adicionados seguindo uma determinada ordem formando uma cadeia de cabeçalhos. As especificações do IPv6 definem seis cabeçalhos de extensão que devem seguir uma sequência definida no caso de vários existirem em um datagrama IPv6. São eles: *Hop-by-hop Options,* este tipo de cabeçalho de extensão é identificado pelo valor 0 no campo próximo cabeçalho, e carrega informações que devem ser processadas em todos os nós ao longo do caminho do pacote. Caso esta opção esteja ausente o roteador saberá que não será preciso processar nenhuma informação adicional e, assim, pode encaminhar o pacote até o destino final. *Destination Options,* identificado pelo valor 60 no campo próximo cabeçalho, carrega informações que devem ser processadas pelo nó de destino do pacote que está indicado no campo de Endereço de Destino do cabeçalho base, e é utilizado no suporte a mobilidade do IPv6 através da opção *Home Address,* que contém o endereço de origem do nó móvel. *Routing* este cabeçalho de extensão é identificado pelo valor 43 no campo próximo cabeçalho e foi desenvolvido inicialmente para listar um ou mais nós intermediários que devem ser visitados até o pacote chegar ao destino. *Fragmentation* identificado pelo valor 44 no campo próximo cabeçalho, este cabeçalho de extensão carrega informações sobre os fragmentos dos pacotes IPv6. *Authentication header,* este cabeçalho de extensão é identificado pelo valor 51 no campo próximo cabeçalho e é utilizado pelo IPSec para prover autenticação e garantia de integridade aos pacotes IPv6. *Encapsulating Security Payload,* identificado pelo valor 52 no campo próximo cabeçalho, também é utilizado pelo campo IPSec, para garantir a integridade e confidencialidade dos pacotes (SANTOS et. al., 2010).

4. ENDEREÇAMENTO IPV4

Na Internet, *hosts* e roteadores conectam-se uns aos outros através de *interfaces* que recebem um endereço IP. Uma *interface*, também conhecida como placa de rede, nada mais é do que um dispositivo eletrônico encontrado em computadores, roteadores e em vários outros tipos de dispositivos eletrônicos que possuem conectividade com qualquer tipo de rede. Na Internet e na maioria das redes baseadas em protocolo TCP/IP cada *interface* de rede recebe um endereço IP único e exclusivo que identifica o *host*. Esse endereço é composto pelo endereço da rede e o endereço da máquina (TANENBAUN, 2003).

O endereço IP, pode ser representado em notação decimal com quatro campos separados por "." pontos, que variam de 0 a 255, ou ser representado de forma binária, por meio de quatro octetos também separados por "." pontos. O quadro 1 apresenta as duas formas de representação de um endereço IP.

Quadro 1 - Formas de representação de um endereço IP

Representação decimal: 192.168.1.1
Representação binária: 11000000.10101000.00000001.00000001

Nos dispositivos de rede, a forma decimal é a mais utilizada, por ser mais fácil de ser lembrada, porém, ela nada mais é do que a conversão da forma binária em um sistema numérico mais amigável ao homem.

A Tabela 3 mostra como é feita a conversão do endereço binário para o endereço decimal.

Tabela 3 – conversão de binário para decimal (*Fonte: Adaptado TANENBAUN*)

Posição	7	6	5	4	3	2	1	0	Decimal equivalente
1º octeto	1	1	0	0	0	0	0	0	192
2º octeto	1	0	1	0	1	0	0	0	168
3º octeto	0	0	0	0	0	0	1	1	3
4º octeto	0	0	0	0	0	0	0	0	0

O decimal equivalente no endereço IP é obtido por meio de duas operações. Na primeira, eleva-se o número 2 (dois) à sua respectiva posição, quando o seu valor é igual a 1. A segunda, soma-se os valores obtidos em cada octeto. Exemplificando: o valor obtido no 1º octeto da Tabela 3 é resultado da operação $2^7+2^6+0^5+0^4+0^3+0^2+0^1+0^0 = 192$.

Um endereço IP não se refere realmente a um *host*. Na verdade ele se refere a uma interface de rede, assim, se um *host* estiver em duas redes ele precisará de dois endereços IP. Na maioria das vezes os *hosts* estão em uma única rede, então ele precisará ter apenas um endereço IP.

Quando o protocolo IP foi desenvolvido pelo IANA, foi dividido em cinco categorias, chamada de “endereçamento de classe completo”. Atualmente essa alocação não é mais utilizada, porém ainda continua sendo comum na literatura (TANENBAUN, 2003). Essas classes são demostradas na figura 4.1.

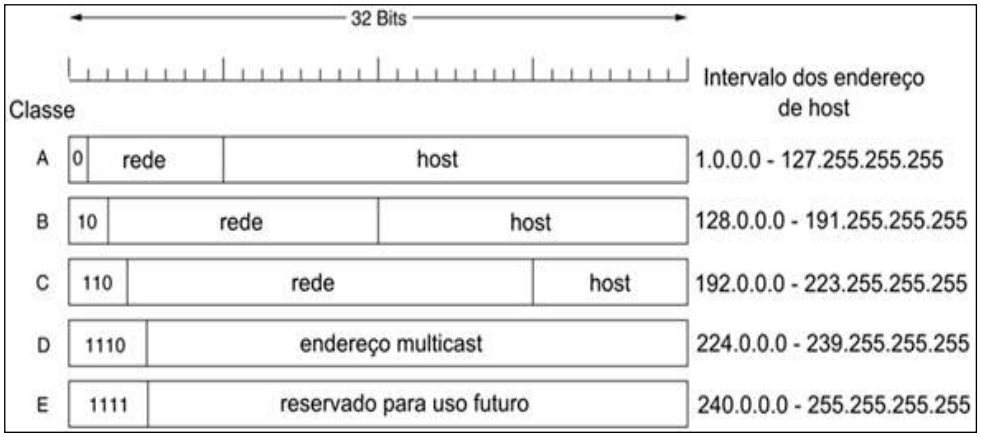


Figura 4.1 – Formatos de endereços IP (Fonte: Adaptado TANENBAUN)

Os endereços de classe A permitem a criação de 128 redes, cada uma com até 16.777.216 *hosts*, que vão da rede 1.0.0.0/8 à 127.255.255.255/8. Nessa classe, o primeiro campo ou octeto do endereço permanece inalterado e os outros três campos podem ser manipulados pelo administrador da rede de acordo com as suas necessidades. A classe B permite a criação de até 64 redes com no máximo 65.536 *hosts*. Seus endereços começam a partir da rede 128.0.0.0/16 e vão até 191.255.255.255/16. Nesta classe de endereços o

primeiro e o segundo octetos permanecem inalterados enquanto o terceiro e o quarto octeto podem ser manipulados pelo administrador da rede. A classe C permite a criação de aproximadamente “2 milhões” de redes, com até 256 *hosts* cada. Sua faixa de endereços vai da rede 192.0.0.0/24 até a rede 223.255.255.255. Na classe D, os endereços são de multidifusão, ou seja, datagramas são direcionados para vários endereços. Sua faixa de endereços inicia-se a partir da rede 224.0.0.0 e vai até 239.255.255.255. A classe E possui endereços reservados para uso futuro. Sua faixa de endereços começa a partir de 240.0.0.0 e termina em 255.255.255.255 (KUROSE e ROSS, 2006).

4.1. ENDEREÇOS IP ESPECIAIS

O primeiro e o ultimo endereço de cada rede são endereços especiais destinados ao endereço de rede e o de broadcast. O valor 0 representa à rede. Já o valor -1 é usado como endereço de difusão, que é um endereço no qual mensagens encaminhadas à ele, serão replicadas a todas as máquinas presentes na rede. A Figura 4.2 mostra o formato de um endereço IP.

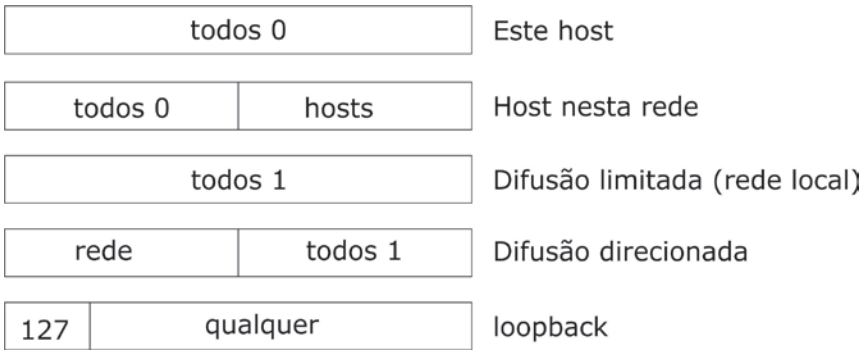


Figura 4.2 - Representação de endereços especiais 0, -1, e 1 (Fonte: Adaptado TANENBAUN)

Na figura podem ser visualizados os endereços especiais e suas aplicações. É possível observar que o primeiro endereço IP, onde todos os bits são 0, são usados pelos *hosts* quando eles estão sendo inicializados. Os endereços IP que tem 0 como número de rede estão referenciando a rede atual, ou seja, a rede em que o *host* está conectado no momento. Esses endereços permitem que os *hosts* façam referências às suas próprias redes sem saber seu número, mas ele precisa conhecer sua classe para saber quantos zeros devem ser incluídos. Os endereços IP que contém apenas dígitos 1 permite a difusão na rede local, geralmente uma LAN. Os endereços IP com um número de rede apropriado que contém apenas dígitos 1 em seu campo de *host*, permitem que os *hosts* enviem pacotes de difusão para LANs distantes em qualquer parte da Internet, no entanto administradores desativam essa função. Por último todos os endereços no formato 127.xx.yy.zz são reservados para testes de *loopback*, os

pacotes enviados para esse endereço não são transmitidos, eles são processados localmente tratados como pacote de entrada, isso permite que os pacotes sejam enviados para rede local sem que o transmissor saiba seu número Sub-Redes (TANENBAUN, 2003).

A partir de um endereço IP obtido através de um provedor de internet (ISP), é possível criar diversas redes pertencentes à rede principal, denominadas sub-redes. Essas redes são subdivididas a partir de um roteador interno ligado a um roteador ISP, onde uma das interfaces do roteador recebe conexão direta da rede externa, e disponibiliza uma rota para as sub-redes através de suas demais interfaces, A Figura 4.3 demonstra a topologia de uma organização educacional que dividiu sua rede interna de acordo com seus setores educacionais.

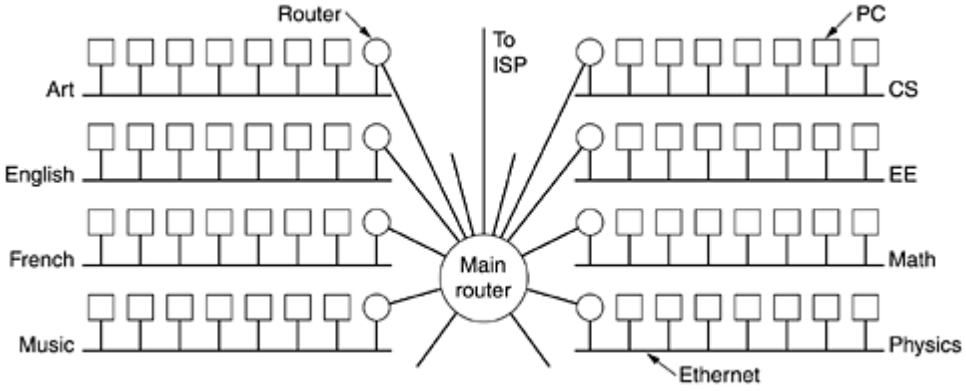


Figura 4.3 - Topologia de uma sub – rede (Fonte: Adaptado TANANBAUN)

Neste cenário, o roteador principal da rede recebe o LINK da rede externa “Internet” em uma de suas interfaces e distribui essa conexão para os demais *hosts*. Para que a divisão de sub-rede seja implementada o roteador principal, precisa de uma máscara de sub-rede, que irá indicar a divisão entre o número da rede, o número da sub-rede e o número do *host*. As máscaras de sub-rede também são descritas em notação decimal separadas por “.” pontos, e seguido de uma barra vertical e o número de bits pertencentes à rede mais os números de bits emprestados dos *hosts* para formar uma sub-rede. Uma rede que obtenha de seu provedor o endereço 192.168.3.0/24 teria sua máscara de rede igual a 255.255.255.0, e poderia subdividir essa rede em várias sub-redes de acordo com suas necessidades. Para se obter uma máscara de rede, primeiro converte-se o endereço IP obtido em decimal, no caso 192.168.3.0, que em binário corresponde a 11000000.10101000.00000011.00000000. Em seguida preenche em paralelo os octetos com bits 1 até o limite que corresponde a classe de endereço obtido através do ISP, neste caso o endereço é de classe C, o que significa que é um endereço /24, então os valores obtidos são :11111111.11111111.11111111.00000000, que corresponde em decimal

ao valor 255.255.255.0. A seguir realiza a operação *AND* exclusivo e se adquire então o endereço de sub-rede 11000000.10101000.00000011.00000000. A tabela 4 apresenta as máscaras e sub-redes para o endereço de rede 192.168.3.0.

Tabela 4 – Máscaras de rede e sub-redes

End. Decimal	192	168	3	0
End binário	11000000	10101000	00000011	00000000
Máscara de rede	11111111	11111111	11111111	00000000
Endereço de subrede	11000000	10101000	00000011	000|00000/27
Máscara de sub-rede	11111111	11111111	11111111	111|00000/27
Máscara de sub-rede em decimal	255	255	255	224
Sub-rede 1	11000000	10101000	00000011	000|00000/27
Sub-rede 2	11000000	10101000	00000011	001|00000/27
Sub-rede 8	11000000	10101000	00000011	111|00000/27

A tabela 4 indica que a rede 192.168.3.0/24 foi subdividida em oito sub-redes cada uma contendo 32 endereços, tendo tomado três bits emprestados da faixa de *host*s, estendendo a máscara de sub-rede para /27, que em decimal corresponde a 255.255.255.224. A primeira sub-rede é a 192.168.3.0/27 e a última sub-rede é a 192.168.3.224/27. Como foi mencionado anteriormente os endereços que contém somente valores 0 zero na faixa de endereços de *hosts*, são considerados endereços especiais, e são destinados endereçamento da rede, assim como os endereços que contém somente o valor 1 um na faixa de endereços de *hosts* também são considerados endereços especiais e são destinados para endereços de broadcast (TANENBAUN, 2003).

4.2. NAT – NETWORK ADDRESS TRANSLATION

Uma das soluções denominados paliativas, que foram desenvolvidas para amenizar a escassez de endereços IP, foi a utilização do *Network Address Translation* (NAT). A ideia básica por traz do NAT é atribuir a cada organização uma faixa de endereços IP, ou um único endereço para trafego da Internet. Com base nesse endereço, a organização configura sua rede interna de forma que todos os *hosts* acessem a Internet por meio desse IP. Em resumo, o NAT realiza uma tradução dos endereços IP da rede interna que é um endereço privado, e que portanto, não podem ser roteados fora da rede local, em um endereço público que possa ser reconhecido na Internet. A Figura 4.4 ilustra este cenário.

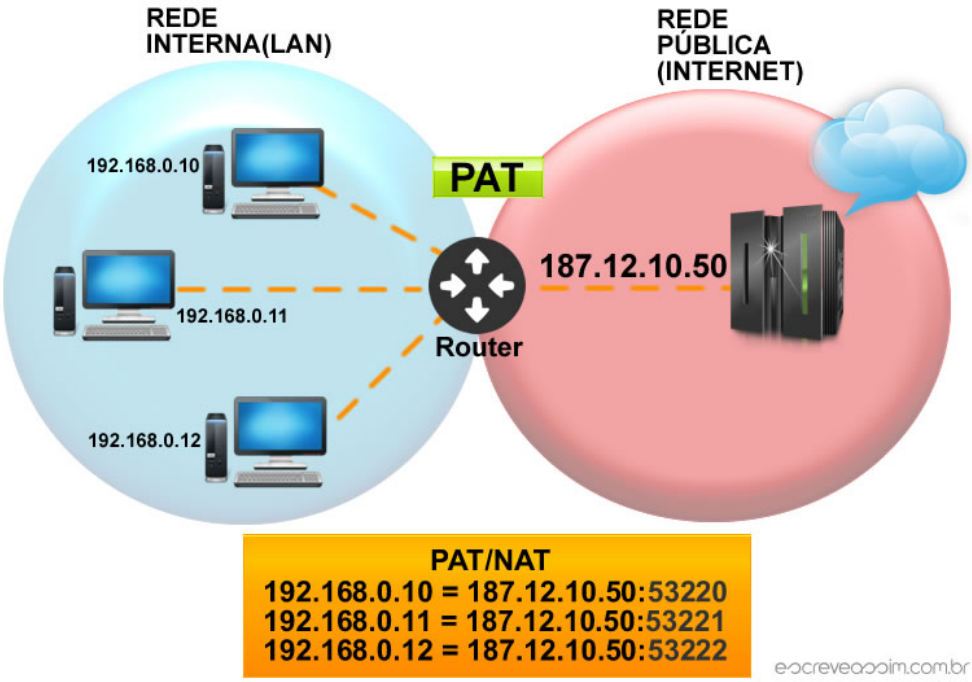


Figura 4.4 - Funcionamento NAT (Fonte: RUSSO, 2013)

Na figura observa-se que os *hosts* da rede interna (LAN) estão conectados a um roteador (*Router*). Estes *hosts* recebem endereços da rede interna, como por exemplo, 192.168.0.10, para que possam trocar dados entre si. Esses endereços não possuem a capacidade de enviar pacotes para a Internet, porém, utilizam o endereço IP configurado na interface do roteador que dá acesso à rede púbica junto com um número que o identifica para a realização desta tarefa. Já o PAT ou NAT *overload* traduz qual máquina entrou em qual site, direcionando os pacotes corretamente para as máquinas solicitantes. Em resumo, todos os pacotes que saem da rede interna para a rede externa saem com o endereço IP do roteador (TANENBAUN, 2003).

Existem três tipos de NATs: i) dinâmico, onde um conjunto de endereços públicos de (*pool*), são atribuídos a um grupo de máquinas que podem utilizar esses endereços; ii) estático, onde um endereço privado é traduzido em um endereço público; iii) NAT Overload (PAT), essa é a técnica mais utilizada. No cenário, acima observa-se o funcionamento da NAT/PAT, no qual utiliza-se um número de porta para cada *host*, utilizando um único endereço IP público.

4.3. CIDR – CLASSLESS INTERDOMAIN ROUTING

A divisão de endereços IP em classes ocasiona um desperdício muito grande de endereços, pois muitas vezes, as organizações obtém faixas de endereço maior do que realmente necessitam. Um bom exemplo disso é uma Empresa A que possui

aproximadamente 300 máquinas em sua rede e recebe uma faixa de endereços Classe B, que disponibiliza até 65.536 endereços. Neste caso, a faixa de endereços classe B disponibilizada à Empresa A é muito maior do que a necessidade real da empresa. Os demais endereços não utilizados ficam ociosos.

Para amenizar esse problema, algumas soluções foram desenvolvidas, entre elas, o protocolo *Classless InterDomain Routing* (CIDR). Este protocolo, descrito na RFC 1519, tem como princípio básico alocar os endereços restantes em blocos de tamanho variável, sem levar em consideração as classes pré-definidas. Em resumo, se uma organização necessita de 2000 endereços para uma rede, esta receberá uma faixa de 2048 endereços, ao invés dos 65.536, relativos à classe B (KUROSE e ROSS, 2006). Essa técnica permitiu um melhor aproveitamento da faixa de endereço IP. Além disso, as organizações podem ainda utilizar o NAT para cada um desses endereços poder rotear as outras máquinas.

5. ENDEREÇAMENTO IPV6

O IPv6, foi desenvolvido com o objetivo de sanar o problema de escassez de endereçamentos da versão 4 (IPv4). Essa nova versão possui um endereçamento com 16 bytes (octetos) que juntos contabilizam 128 bits de comprimento, disponibilizando assim mais de 340 undecilhões de endereços possíveis (valor 340 seguido de 36 zeros). De acordo com o NIC.br, instituição responsável pela distribuição e controle de endereços IP no Brasil, a nova versão do IP possui um espaço de endereçamento em torno de 79 octilhões (7,9x1028) de vezes a quantidade de endereço da versão IPv4, o que representa mais de 56 ocotilhões (5,6x1028) de endereços por ser humano na Terra (SANTOS et al., 2010).

Os endereços IPv6 são representados em notação hexadecimal de 0 à 8 e de A à F separados por “:” dois pontos Uma interface de rede configurada com o IPv6 pode ter o seguinte endereço IP: 2001:0dB8:AD1F:25E2:CADE:CAFE:F0CA:84C1. Pode-se observar nesta representação que o uso de cárteres maiúsculo e minúsculo são permitidos, além de regras de abreviação que podem ser aplicadas para facilitar a escrita de alguns endereços muito extensos, como, por exemplo, substituir uma sequência de dois zeros por “::”. O endereço IPv6 2001:0DB8:0000:0000:130F::140B pode ser escrito como 2001:DB8:0:0:130F::140B ou 2001:DB8::130F:0:0:140B. Nesta forma de escrita, é possível observar que a abreviação do grupo de zeros só pode ser realizada uma única vez, caso contrário poderá haver ambiguidades na representação do endereço. Além disso, o IPv6 usa o comprimento do prefixo para representar a porção de prefixo do endereço e não usa a notação de máscara de sub rede decimal com ponto. A maioria dos tipos de redes IPv6 são /64 o que

significa que a porção de prefixo típico de rede do endereço é de 64 bits para identificar a porção de host do endereço (SANTOS et al., 2010).

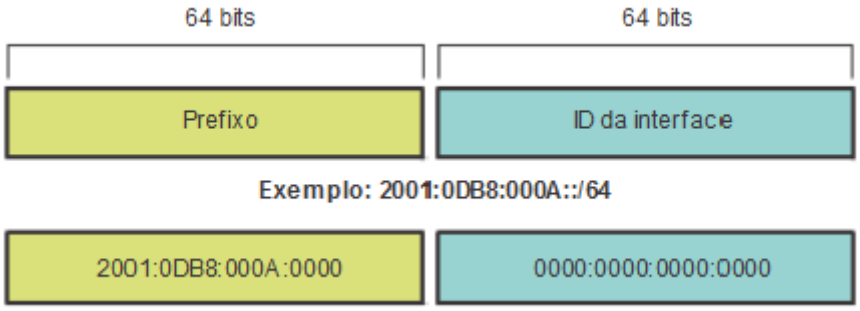


Figura 5.1 - identificação de prefixo e ID da Interface

Como pode ser observado na figura 5.1, os primeiros 64 bits do espaço reservado no cabeçalho IPv6 para o endereçamento, indicam o número da rede a quem o *host* emissor pertence, já o outro campo de 64 bits de Identificação da interface indica o número do *host* na rede a que este pertence.

5.1. TIPOS DE ENDEREÇOS IPV6

Diferente do IPv4, o IPv6 não possui endereço de *broadcast* responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6, esta função foi atribuída a três tipos de endereços definidos:

- ***Unicast***: Este tipo de endereço identifica uma única interface de um dispositivo, de modo que um pacote enviado a um endereço *unicast* é entregue a uma única interface. Endereços *unicast* são utilizados para comunicação entre dois nós, como por exemplo, telefones VoIPv6, computadores em uma rede privada, além de outros vários tipos de conexões *pear-to-pear*, a estrutura de um endereço *unicast* foi definida para permitir agregações com prefixos de tamanho flexível similar ao CIDR no IPV4.
- ***Global Unicast***: O endereço *Global unicast* é semelhante aos endereços públicos IPv4, sendo globalmente roteado e acessível na Internet IPv6. Este endereço é constituído de três partes: i) o prefixo de roteamento Local, que é utilizado para identificar o tamanho do bloco atribuído a uma rede, ii) a identificação da sub-rede utilizado para identificar um enlace em uma rede, e iii) a identificação da interface, que tem a função de identificar de forma única uma interface dentro de um enlace. 64 bits a esquerda de sua estrutura identifica a rede e os 64 bits a direita identifica o *host*.
- ***Link Local***: Este endereço pode ser utilizado apenas no enlace especifico onde a interface está conectada, o endereço de *link-local* pode ser atribuído a uma interface

automaticamente utilizando o prefixo FE80::/64. È importante ressaltar que os roteadores não devem encaminhar para outros enlaces pacotes que possuam como origem ou destino um endereço de link-local.

- ***Unique Local Address* (ULA)**: Este tipo de endereço tem grande probabilidade de ser globalmente único, sendo utilizado apenas para comunicações locais, ou seja, dentro de um mesmo enlace ou conjunto de enlaces. Um endereço ULA não deve ser roteado na Internet global e é composto por um Prefixo, *Flag Local*, identificador global de 40 bits e Identificador da Interface que possui 64 bits.
- **Endereço Não Especificado (*Unspecified*)**: Este endereço é representado pelo endereço 0:0:0:0:0:0:0:0 ou ::0 (que é equivalente no IPv4 ao endereço *uspecified* 0.0.0.0). Este endereço nunca deve ser atribuído a nenhum nó, sua função é identificar a ausência de um endereço e geralmente é usado no campo de endereço de um pacote IPv6 enviado por um *host* durante sua inicialização, antes que tenha obtido seu endereço exclusivo.
- **Endereço de *Loopback***: Este endereço é representado pelo endereço *unicast* 0:0:0:0:0:0:0:1 ou ::1 (equivalente ao endereço IPv4 *loopback* 127.0.0.1). Ele é utilizado [para referenciar a própria máquina e é muito utilizado para testes internos. Este tipo de endereço nunca deve ser atribuído a nenhuma interface física, nem usado como endereço de origem em pacotes IPv6 que são enviados para outros nós.
- ***Anycast***: Este endereço identifica um conjunto de interfaces. Um pacote quando é encaminhado a um endereço *anycas*t é entregue a interface pertencente ao conjunto mais próximo da origem de acordo com a distância medida pelos protocolos de roteamento. Este endereço é utilizado para comunicações um-para-um-de muitos.
- ***Multicast***: Este endereço também identifica um conjunto de interfaces, no entanto quando um pacote é enviado a um endereço *multicast* é entregue a um grupo de interfaces associadas a esse endereço. Este tipo de endereço é utilizado em comunicações de um-para-muitos. No Ipv4, o suporte *multicast* é opcional, já que foi introduzida apenas como extensão do protocolo. No entanto, no IPv6 é requerido que todos os nós suportem *muticast*, considerando que muitas funcionalidades do protocolo IPv6 utilizam esse serviço. O funcionamento do *multicast* no IPv6 é similar ao *broadcast* no IPv4, a diferença é que no broadcast o pacote é enviado para todos os hosts na rede, já no *multicast* o pacote é enviado apenas para um grupo especifico (KUROSE E ROSS, 2006).

6. COMPARAÇÃO ENTRE AS VERSÕES DO IP

O protocolo IPv6 sofreu muitas mudanças em relação ao seu antecessor IPv4, trazendo funcionalidades novas, eliminando aquelas que não tinham muita relevância e aperfeiçoando outras funções consideradas importantes. Em decorrência dessas mudanças, os cabeçalhos tornaram-se distintos, deixando a estrutura do protocolo IPv6 reduzida em relação ao seu antecessor. A Figura 6.1 ilustra as diferenças entre o cabeçalho IPv6 e IPv4.

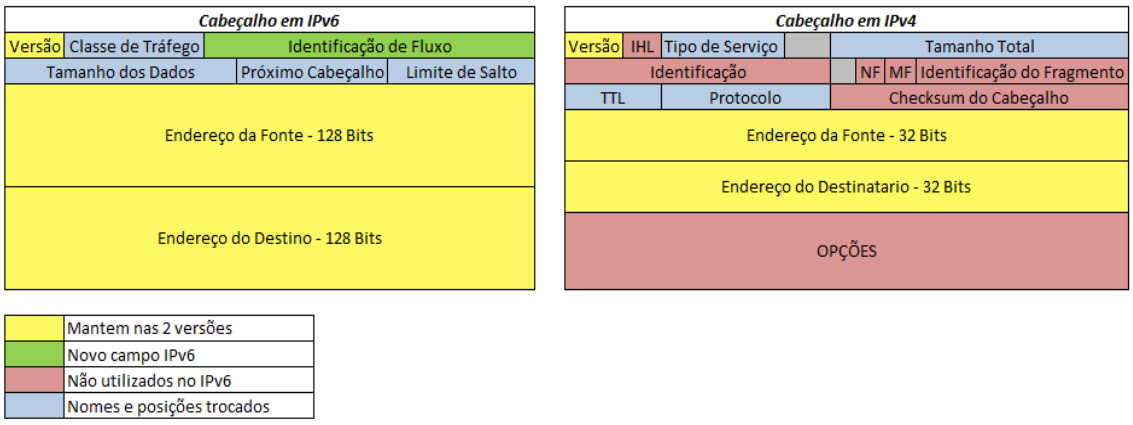


Figura 6.1 - Cabeçalhos IPv6 e IPv4 (CANNO, 2013)

Através das cores na Figura 6.1 pode-se ter uma noção exata de todos os campos em ambos os cabeçalhos, como aqueles que foram mantidos, substituídos, criados ou retirados de funcionamento na versão seis do protocolo IP pode-se verificar que os campos *Internet header length* (IHL), Identificação, NF, MF, Identificação do Fragmento, *Checksun* do Cabeçalho e Opções, existentes na versão quatro do protocolo, foram removidos, e não fazem parte do protocolo IPv6. Já os campos Tipo de serviço, Tamanho total, TTL e Protocolo

tiveram seus nomes modificados e suas posições alteradas, na versão seis esses protocolos são chamados de Classe de tráfego, Tamanho dos dados, Próximo cabeçalho e Limite de salto, já o campo Identificação de fluxo foi criado no protocolo IPv6.

Tabela 4 – Comparativo entre os protocolos IPv4 e IPv6 (CANNO, 2013)

IPv4	**IPv6**
Endereço de 32 bits	Endereço de 128 bits
Total de endereços 4.294.967.296 (2^{32})	Total de endereços 340 undecilhões (2^{128})
Suporte opcional de *IPsec*	Suporte obrigatório de *IPSec*
Nenhuma referência a capacidade de QoS *(Quality of Service)*	Introduz capacidade de QoS utilizando o campo *Flow Label* para este fim
Processo de fragmentação realizada pelo roteador	A fragmentação deixa de ser realizada pelos roteadores e passa a ser processada pelos hosts de origem
O cabeçalho inclui os campos de opção, que geralmente é pouco utilizável.	Todos os campos de opção foram transferidos para dentro do campo *extension header*
O *Address Resolution Protocol* (ARP), utiliza requisitos do tipo *broadcast*	O ARP deixa de ser utilizado, sendo substituído pelas mensagens *Neighbor Discovery*
Internet Resolution Management Protocol (IGMP) é utilizado para gerir relações locais de sub-redes	O IGMP foi substituído por mensagens *Multcast Listner Discovery*
Os endereços de *Broadcast* são utilizados para enviar trafego para todos os *hosts* de uma rede	Deixa de ser utilizado o endereço de Broadcast, para ser utilizado o endereço de *Multcast*
O endereço tem de ser configurado manualmente	Adição de funcionalidades de autoconfiguração
Suportam pacotes de 576 bytes, passíveis de serem fragmentados	Suporta pacotes de 1280 bytes, sem fragmentação

A tabela 4 mostra o comparativo entre os cabeçalhos IPv4 e IPv6. Neste comparativo é possível visualizar que a versão atualizada do protocolo se diferencia da antiga na quantidade de endereços muito extenso, e quase ilimitados. No IPv4, o suporte ao serviço IPsec é opcional, diferentemente do IPv6 em que é obrigatório. A fragmentação na versão 4 é feita nos roteadores enquanto na versão 6 a fragmentação e remontagem passa a ser feita nos *hosts* (origem e destino). Segundo (KUROSE E ROSS, 2006) essas operações ocupam muito tempo de processamento dos roteadores e coloca-las nos sistemas finais, aceleram consideravelmente o repasse (GOMES, 2012).

6.1. ICMPV4 X ICMPV6

O protocolo de mensagens de controle da Internet (ICMPv4), está especificado no RFC 792. Esse serviço foi projetado para compensar duas das deficiências do protocolo IP, que são reportar erros no processamento de pacotes e enviar mensagens sobre o status e as características da rede. Este protocolo é utilizado por *hosts* e roteadores para transmitir informações da camada de rede entre si.

O ICMP é frequentemente considerado parte do protocolo IP, mas em termos de arquitetura ele está localizado logo acima do IP, pois mensagens ICMP são carregadas dentro de datagramas IP no campo de carga útil do cabeçalho IP, exatamente como segmentos TCP ou UDP (KUROSE E ROSS, 2006).

Diversos tipos de mensagens ICMP foram definidas, sendo as mais importantes:

- ***Destination Unreachable*** - Essa mensagem é usada quando a sub-rede ou um roteador não consegue localizar o destino para um determinado datagrama, ou quando um bit DF não pode ser entregue por que há uma rede de pacotes relativamente pequena no caminho. O bit DF é um bit que está contido no campo de *flag* do cabeçalho IP.
- ***Time Exceeded*** - Essa mensagem é enviada quando o contador do datagrama chegou a zero, antes que ele chegasse ao seu destino. Esse tipo de evento indica que os pacotes estão entrando em *loop* ou que está havendo um congestionamento na rede.
- ***Parameter Problem*** - Essa mensagem indica que um valor inválido foi detectado em algum campo do cabeçalho, e que pode haver algum *bug* no *software* do *host* transmissor, ou possivelmente no *software* de algum roteador por onde o pacote tenha transitado.
- ***Source Quanch*** - Antes essa mensagem tinha como função ajustar *hosts* que enviavam mais pacotes do que a rede podia tratar, ocasionando o congestionamento. Ao receber essa mensagem o *host* deveria desacelerar sua operação. Atualmente raramente essa mensagem é utilizada porque, na maioria das vezes, o controle de congestionamento da Internet é feito na camada de transporte.
- ***Redirect*** - Essa mensagem é usada quando um roteador percebe que o pacote foi roteado incorretamente. Ao enviar essa mensagem o roteador alerta o *host* sobre o possível erro podendo este retransmiti-la.
- ***Echo e Echo reply*** - Essas mensagens são usadas para verificar se um determinado destino está ativo e acessível. Ao receber uma mensagem *echo*, o destino deve enviar uma mensagem *echo reply* anunciando que está pronto para receber os pacotes.

- ***Timestamp request e Timestamp reply***. - Essas mensagens são semelhantes às mensagens *echo* e *echo reply*, exceto pelo fato de que o tempo de chegada da mensagem e o tempo de saída da resposta serem registrados na mensagem de resposta. Esse recurso tem como objetivo medir o desempenho da rede (TANENBAUN, 2003).

O ICMP teve sua versão atualizada para ser utilizado com o IPv6. Definida na RFC 4443, o ICMPv6 apresenta as mesmas funcionalidades que o ICMPv4, como reportar erros no processamento de pacotes e enviar mensagens sobre status e características da rede. No entanto, ele não é compatível com seu antecessor e apresenta um número muito maior de mensagens e funções. O protocolo ICMPv6 é responsável por realizar funções do protocolo *Address resolution Protocol* (ARP), que mapeia os endereços de camada dois "enlace" para IP e vice-versa, e o *Internet Group Management Protocol* (IGMP), que gerencia membros de endereços dos grupos *multicast* no protocolo.

As mensagens ICMPv6 são divididas em duas classe: i) mensagens de erro; ii) mensagens de informação. A Tabela 5 e a Tabela 6 apresentam essas mensagens.

Tabela 5 – Mensagens de erro

Tipo	**Nome**	**Descrição**
1	*Destination Unreacheble*	Indica falhas na entrega do pacote como endereço ou porta desconhecida ou problemas na comunicação.
2	*Packt Too Big*	Indica que o tamanho do pacote é maior que a Unidade Máxima de Transmissão (MTU) de um enlace.
3	*Time exceeded*	Indica que o limite de encaminhamento ou tempo de remontagem do pacote foi excedido
4	*Parameter Problem*	Indica erro em algum campo de cabeçalho IPv6 ou que o tipo indicado no campo próximo do cabeçalho não foi reconhecido.
100-101		Uso experimental
102-126		Não utilizado
127		Reservado para expansão das mensagens de erro ICMPv6

Tabela 6 – Mensagens de informação

Tipo	Nome	Descrição
128	*Echo Request*	Utilizadas pelo comando *ping*
129	*Rccho Reply*	
130	*Muticast Listener Query*	
131	*Muticast Listener Report*	Utilizadas no gerenciamento de
132	*Multicast Listener Done*	grupos *Multicast*
133	*Router Sicitation*	
134	*Router Advertisement*	
135	*Neighbor Solicitation*	Utilizadas com o *protocol*
136	*Neighbor Advertisement*	Descoberta de Vizinhança.
137	*Redirect Meaage*	
138	*Router Renumbering*	Utilizada no mecanismo de reendereçamento (*Renumbering*) de roteadores.
139	*ICMP Node Information Query*	Utilizadas para descobrir
140	*ICMP Node Information Response*	informações sobre nomes e endereços, são atualmente limitadas a ferramentas de diagnóstico, depuração e gestão de redes.
141	*Inverse ND Solicitation Message*	Utilizada em uma extensão de
142	*Inverse NO Adversement Massage*	Descoberta de vizinhança.
143	*Version 2 Multicast Listner Report*	Utilizada no gerenciamento de grupos *Multicast.*
144	*HÁ Address Discovery Req. Massage*	
145	*HÁ Address Discovery Reply Massege*	
146	*Mobile Prefix solicitation*	Utilizada no mecanismo de
146	*Mobile Prefix Advertisement*	Mobilidade ipV6.
148	*Certification path solicitation Message*	Utilizadas pelo protocolo *Send*
149	*Cert. Path Advertisement Message*	
150		Utilizada experimentalmente com protocolos de mobilidade como o *Seamoby.*
151	*Muticast Router Adevertisement*	
152	*Muticast Router Solicitation*	Utilizadas pelo mecanismo
153	*Muticast Router Termination*	*Muticast Router Discovery.*
154	*FMIPv6 Messages*	Utilizada pelo protocolo de mobilidade *Fast Handovers.*
200-201		Uso Experimental
255		Reservado para expansão IPv6.

O protocolo ICMPv6 é um protocolo chave na arquitetura IPv6. Suas mensagens são essências para o funcionamento do protocolo de “Descoberta de Vizinhança” (*Neighbor Discovery*), que é responsável por localizar roteadores vizinhos na rede, determinar os

endereços MAC dos nós vizinhos, detectar mudanças de endereço no enlace, detectar endereços duplicados, oferece suporte a mobilidade ao gerenciar endereços de origem dos *hosts* dinamicamente, e também auxilia na descoberta do menor *Maximum Transmision Unit* (MTU) no caminho de um pacote até o destino (SANTOS et al., 2010).

6.2. QOS

A princípio, o protocolo IP trata todos os pacotes da mesma forma, sem nenhuma preferência na hora de encaminhá-los. O que pode acarretar em diversas implicações no desempenho de uma aplicação. Atualmente muitas aplicações, como voz e vídeo sobre IP, requerem transmissões de tempo real, e podem vir a ter suas qualidades diminuídas devido à ocorrência de perdas de pacotes, entrega fora de ordem, atraso ou variação do sinal. O conceito de (*Quality of service*) Qos, que em Português quer dizer qualidade de serviço, é empregado em protocolos para prover a transmissão de determinado tráfegos de dados com prioridade e garantia de qualidade. Atualmente existem duas arquiteturas principais de QOS. *Differentiated Services* (*DiffServ*) e a *Integrated Services* (*InterServ*). Ambas utilizam politicas de tráfego e podem ser combinadas para permitir QoS em redes locais ou de longa distâncias (SANTOS et al., 2010).

O *DiffServ* trabalha por meio de classes de serviços, agregando e priorizando pacotes com requisitos similares. Estes pacotes são identificados no IPv4 através dos oito bits contidos no campo tipo de serviço e no campo classe de trafego no IPv6. Ambos os campos possuem as mesmas definições, e as prioridades podem ser definidas tanto na origem quanto nos roteadores, e também podem ser redefinidas ao longo do caminho por roteadores intermediários. Pacotes que não necessitam de QoS possuem o campo Classe de tráfego com o valor 0 (zero). Comparado com *InterServ*, o *DiffServ* não exige qualquer identificação ou gerência dos fluxos, além de ser geralmente mais utilizado na rede devido à sua facilidade de implantação.

O *InterServ* atua na reserva de recursos de fluxo e sua utilização está associada ao protocolo RSVP, que é utilizado para reservar o recurso ao longo do caminho da fonte até o destino de um fluxo que requer Qos. No IPv6 fluxos de dados que requerem QoS são identificados utilizando 20 bits no campo identificador de fluxo, que são preenchidos com valores aleatórios entre 00001 e FFFFF, já os pacotes que não requerem QoS, devem marcar o campo identificador de fluxo com 0 (zero).

O protocolo RSVP utiliza alguns elementos do protocolo IPv6 como campo de identificação de fluxo e o cabeçalho de extensão *Hop-by-Hop*. Os pacotes RSVP são enviados com o mesmo valor no campo identificador de fluxo, junto com o cabeçalho de extensão *Hop-by-Hop* para transportar mensagens *Router Alert*, indicando para cada roteador no caminho do trafego QoS que o pacote deve ser processado (SANTOS et al., 2010).

6.3. TRANSIÇÃO DO IPV4 PARA O IPV6

Embora o protocolo IPv6, esteja pronto e definido há quase vinte anos, e seja visivelmente superior a sua versão antecessora em vários aspectos, vindo a suprir vários problemas que surgiram ao longo dos anos de funcionamento do IPv4, existe uma série de fatores que prorroga a implementação total do IPv6. Um desses fatores ocorre no fato de sistemas habilitados para IPv6 poderem ser inversamente compatíveis, ou seja, podem também receber e enviar datagramas IPv4, já os sistemas mais antigos habilitados para atuarem em IPv4 não podem tratar datagramas IPv6. A transição entre as duas versões do protocolo IP deve ocorrer de forma gradativa e sem causar impactos significativos na rede, havendo necessidade de um período de coexistência entre os protocolos IPv4 e IPv6. Enquanto o dia em que toda infraestrutura da rede pública esteja funcionando com a nova versão do protocolo IP não chega, foram descritas no RFC 2893 três abordagens que podem ser utilizadas juntas ou individualmente para a integração gradual dos hospedeiros e roteadores IPv4 ao universo IPv6, são elas: (SANTOS et al., 2010).

- **Pilha dupla**: técnica de pilha dupla possibilita introduzir nós habilitados ao IPv6, ou seja, nós IPv6 também pode conter uma implementação IPv4, sendo denominado nó IPv6/IPv4. Este nó está habilitado a enviar e receber ambos os datagramas. Nós IPv6/IPv4 contém tanto um endereço IPv4 quanto um endereço IPv6. Ao lidar com um nó IPv4, um nó IPv6 poderá usar datagramas Ipv4, e ao interagir com um nó IPv6 este poderá utilizar um datagrama IPv6. Nós IPv6/IPv4 devem determinar se um outro nó está habilitado para IPv6 ou somente para IPv4, nesse caso o DNS identifica se o nó é capacitado para receber datagramas IPv6, caso contrário ele retornará um endereço IPv4 (SANTOS et al., 2010).
- **Tradução:** Através desta técnica é possível fazer um roteamento transparente entre nós de uma rede estruturada somente com IPv6, com nós de uma rede que seja estruturada somente com IPv4 e vice-versa. Dentre as técnicas de tradução estão: i) tradução de cabeçalhos Ipv4 em cabeçalhos IPv6 e vice-versa; ii) realização de conversão de

endereços; iii) conversão de APIs de programação; iv) atuações na troca de tráfego TCP ou UDP;

- **Tunelamento**: Permite o trafego de pacotes IPv6 através de uma rede estruturada sobre IPv4. Nesta abordagem se o host emissor ou o host destino estiverem habilitados apenas para IPv4, um datagrama IPv4 deverá ser utilizado, contudo é possível que dois nós habilitados para atuarem em IPv6 venham a enviar datagramas IPv4 entre si, como pode ser notado na Figura 6.2.

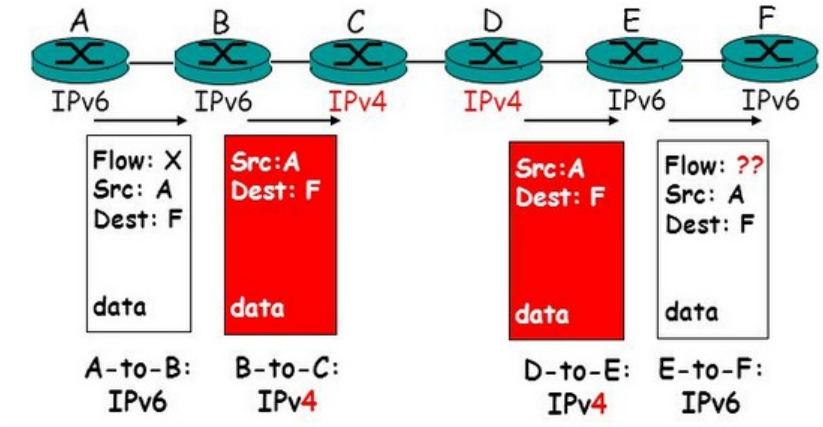


Figura 6.2 - Abordagem de Tunelamento (Adaptado TANENBAUN)

Neste diagrama o nó A está utilizando o protocolo IPv6 e está tentando enviar um datagrama ao nó F, que por sua vez também está utilizando IPv6. Os nó A e B podem trocar datagramas IPv6, no entanto o nó B deve criar um datagrama IPv4 para enviar este dado para o nó C. O campo de dados do datagrama IPv6 pode ser copiado para o campo de dados do datagrama IPv4, o que possibilita que o mapeamento de endereços adequado possa ser realizado, porém quando a conversão de versões for realizada haverá campos específicos do datagrama IPv6 que não terão contrapartes no datagrama IPv4, como, por exemplo, o campo identificador de fluxo, o que acarretará na perda das informações contidas nesses campos, o que significa que mesmo que E e F possam trocar datagramas IPv6, os datagramas IPv4 que chegarem a E e D não conterão todos os campos originalmente contidos no datagrama enviado por A (KUROUSE e ROSS, 2007).

6.4. TÉCNICAS DE TUNELAMENTO

A técnica de criação de túneis, ou tunelamento, permite a transmissão de pacotes IPv6 através de uma rede com infra-estrutura baseada em IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismo de roteamento, encapsulando o conteúdo IPv6 em um pacote IPv4. Essa técnica é referenciada na RFC 4213, e vem sendo a mais utilizada durante este período de implantação do protocolo IPv6, onde as rede ainda não estão

estruturadas para oferecer um tráfego IPv6. Existem diversas técnicas de tunelamento disponíveis;

- ***Tunnel Broker***: Essa técnica está descrita na RFC 3053 e permite que host IPv4/Ipv6 que estejam isolados em uma rede IPv4 possam acessar uma rede IPv6. Para obter esse serviço basta cadastra-se a um provedor de acesso *Tunnel Broker* e realizar o *download* de um *software* ou *script* de configuração. A conexão do túnel é estabelecida através da solicitação do serviço ao servidor *web* do provedor que após a autenticação, identifica qual o tipo de conexão o cliente está usando (NAT ou IPv4 público) e disponibiliza a ele um endereço IPv6. A partir deste estágio o cliente pode acessar qualquer dispositivo na Internet.
- ***6to4***: Definido na RFC 3056, está técnica de tunelamento automática *6to4* permite uma conexão ponto-a-ponto entre roteadores, sub-redes, ou computadores em uma rede IPv4, através de um endereço IPv6 único formado a partir de endereços IPv4.
- ***ISATAP***: Referenciada na RFC 5214, a técnica de transição *Intra-Site Automatic Tunnel Addessing Protocol* (ISATAP) baseia-se em túneis IPv6, criados automaticamente dentro de redes IPv4, e em endereços IPv6 associados aos clientes de acordo com o prefixo especificado no roteador ISATAP cliente IPv4.
- ***Teredo***: A técnica de tunelamento *Teredo* está definida na RFC 4380, e permite que nós localizados atrás de *Network Address Translation* (NAT), possam obter conectividade IPv6 utilizando protocolo UDP. A conexão é realizada através de servidor *Teredo* que inicializa, e determina o tipo de NAT que está sendo utilizada pelo cliente, em caso do *host* destino possuir um endereço IPv6 nativo, será usado um *Relay Teredo* para criar uma interface entre o cliente e o *host* destino. Está técnica não é muito eficiente devido ao *overhead* e a complexidade de seu funcionamento, no entanto quando um *host* está por traz de uma NAT, esta pode ser a única opção.
- **GRE**: (*Generic Routig Encapsulation*) trata-se de um túnel estático entre dois *hosts*. Originalmente essa técnica foi desenvolvida pela Cisco e tem como finalidade encapsular vários tipos diferentes de protocolos além do IPv6. Esta técnica de encapsulamento é suportada pela maioria dos sistemas operacionais e roteadores, através de um *link* ponta-a-ponto.

Como a coexistência ente IPv4 e IPv6 pode durar por um período de tempo indeterminado, a implementação de métodos que possam vir a possibilitar a interoperabilidade entre os dois protocolos, poderá garantir uma migração segura para a nova

versão do protocolo, através da realização de testes que possibilitam conhecer as opções que estes mecanismos oferecem a fim de evitar ilhas isoladas de comunicação (SANTOS et al., 2010).

7. DESEMPENHO DOS PROTOCOLOS

As mudanças significativas em relação às duas versões do protocolo IP aconteceram com a finalidade de melhorar diversos aspectos como endereçamento, segurança, desempenho de trafego entre outros serviços, levando-se em consideração o tempo de coexistência em que os dois protocolos atuarão juntos até que a nova versão do protocolo IP seja totalmente implantada. Frente a esse cenário, faz-se necessária a análise e comparação do trafego de dados utilizando tanto IPv4, quanto IPv6. Os testes a seguir foram realizados concentrando os estudos no desempenho do tráfego e as análises de coexistência entre as duas versões, utilizando-se para isso as técnicas de tunelamento. Os testes foram realizados em duas fases: i) a primeira analisando a diferença de velocidade "*Performance*" na transmissão dos pacotes (IPv4 e IPv6); ii) e a segunda, em relação ao roteamento, sendo assim possível analisar a diferença de velocidade, processamento e encaminhamento do IPv6 tunelado em relação ao IPv4.

Todos os resultados apresentados nesse capítulo foram obtidos na literatura (GOMES, 2012).

7.1. TESTE DE DESEMPENHO SEM UTILIZAÇÃO DE TÚNEL

Os primeiros testes foram realizados em um ambiente de rede local (LAN), interconectados através de portas *ethernet*, 100baseT, onde os dispositivos utilizados são independentes de meios externos como *Links* e roteadores. Este teste foi baseado na quantidade de tráfego transmitido, tendo em vista que o tempo de resposta é pequeno, devido

ao fato das duas máquinas se encontrarem no mesmo segmento de rede. A Figura 7.1 apresenta a topologia da rede utilizada no teste.

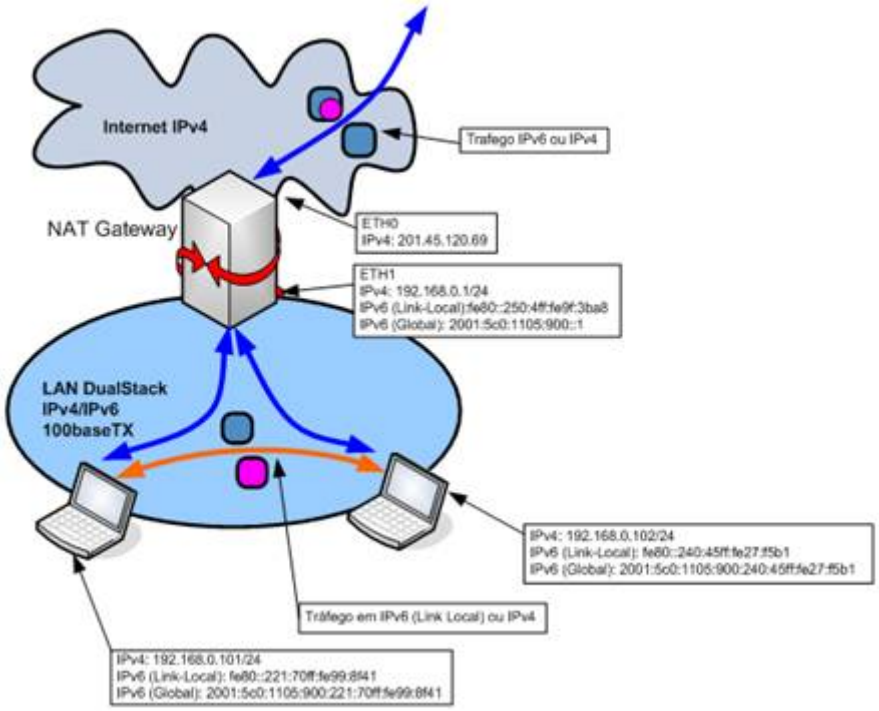


Figura 7.1: Topologia da rede – cabo (Fonte: GOMES, 2012)

A Figura 7.1 mostra a configuração realizada no laboratório para execução dos testes de desempenho na transferência de arquivos, sendo testados os protocolos da camada de rede IPv4 e IPv6. Inicialmente, os testes foram realizados com dispositivos configurados com IPv4 conectados via cabos através de um switch, com o protocolo IPv6 desabilitado. A transferência envolveu um arquivo de 113 MB da estação configurada com o endereço IP 192.168.0.102/24 para a estação 192.168.0.101/24. Nesse cenário, obteve-se uma taxa de transferência média de 14 MB/s. Em seguida, alterou-se as configurações das mesmas estações para IPv6 puro, desabilitando o protocolo IPv4. Transferindo o mesmo arquivo, obteve-se então uma taxa de transferência de 13 MB/s. Para cada um dos cenários, foram realizados quatro testes. A Figura 7.2 apresenta o comparativo desses testes.

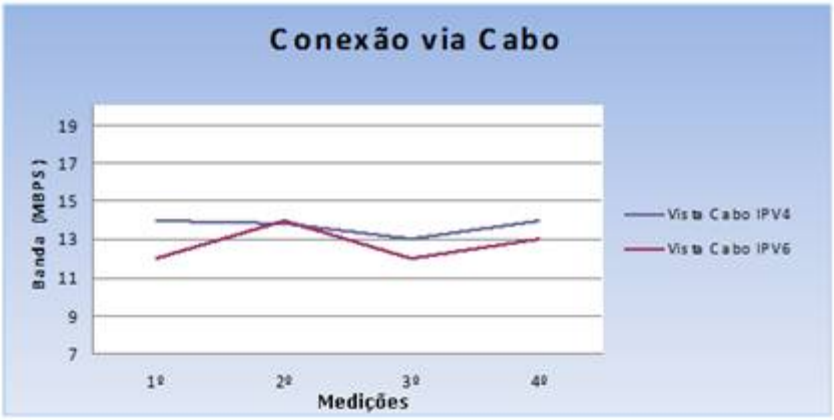


Figura 7.2: Comparativo IPv4 x IPv6 – Via Cabo (Fonte: GOMES, 2012)

Ao analisar os dados do teste de desempenho, pode-se concluir que os dois protocolos são basicamente equivalentes no quesito desempenho, tendo o IPv6 na segunda rodada de testes, superado o IPv4.

Em seguida, foi executado o mesmo teste com a adição de um *Access Point* (AP) em uma das portas do *switch*. Neste teste, o desempenho foi analisado com a comunicação sendo realizada por meio da rede wireless. A figura 7.3 demonstra a topologia após as novas configurações:

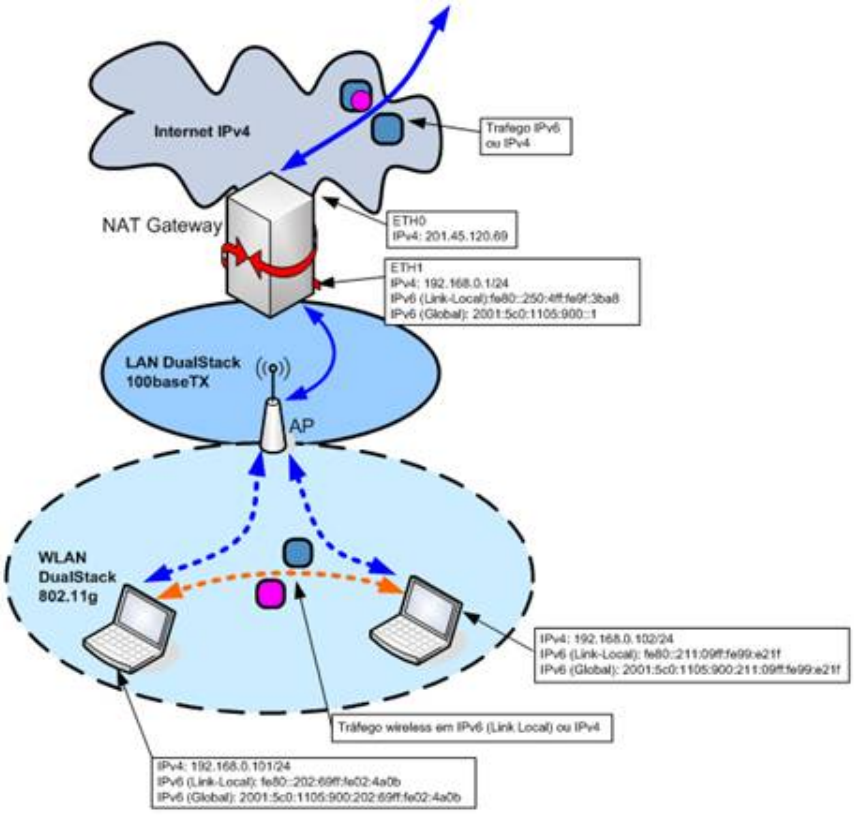
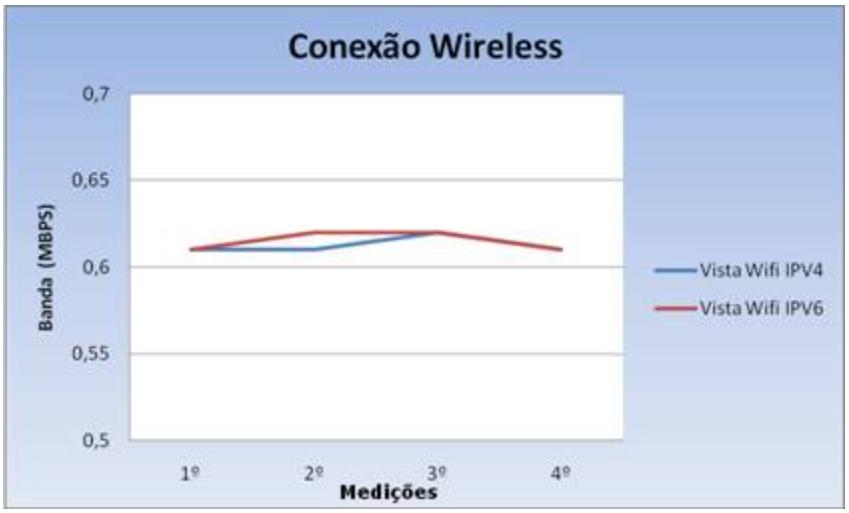


Figura 7.3: Topologia da rede – Wireless (Fonte: GOMES, 2012)

Semelhante ao teste anterior, pode-se perceber uma equivalência entre os dois protocolos, obtendo-se uma taxa média de transferência de 614 KB/s para o protocolo IPv4 e 615 KB/s para o IPv6. A Figura 7.4 apresenta os resultados obtidos.



7.4: Comparativo IPv4 x IPv6 – Wireless (Fonte: GOMES, 2012)

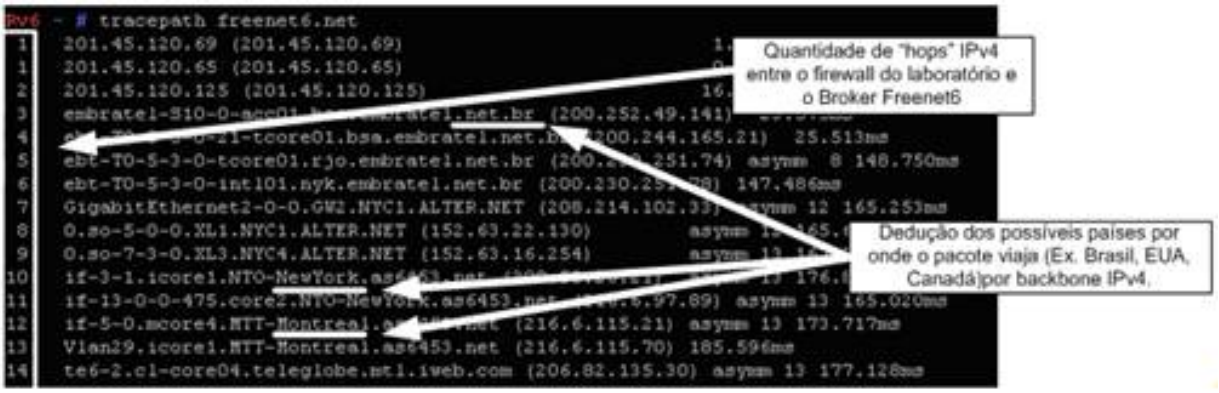
Ao analisar os resultados dos dois testes realizados (rede cabeada e *wireless*), é possível observar que o desempenho das duas versões do protocolo IP são equivalentes. Com base nesses resultados, é possível afirmar que o desempenho de uma rede local (LAN) não será afetado pela migração da versão 4 para a versão 6 do protocolo IP.

7.2. TESTES UTILIZANDO MECANISMO DE TUNELAMENTO

Os próximos testes utilizam os mecanismos de tunelamento. Como visto anteriormente, esses mecanismos são necessários para a comunicação entre redes configuradas com versões distintas do protocolo IP. Nestes testes foram levados em consideração apenas o tempo de latência, tendo em vista não ser possível controlar fatores externos tais como: i) disponibilidade e conectividade do link; ii) troca de trafego entre diversas operadoras, servidores, entre outros. Para realização dos testes foi utilizado o mecanismo de túnel *Broker*. O túnel utilizado foi o *Freenet6* da *HEXAGO*, situado fisicamente no Canadá. O primeiro teste realizado foi o teste de latência com base no comando *ping*, que mede o tempo de resposta de uma requisição ICMP. O comando *ping* foi executado apontando para o endereço do site *Freenet6* (www.freenet6.net), que está configurado em *dual-stack* (pilha dupla), aceitando requisições ICMPv4 e ICMPv6.

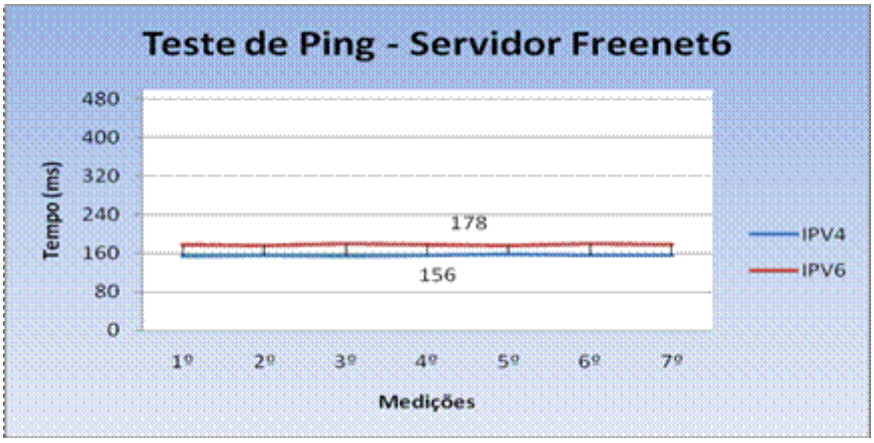
Para alcançar o endereço do *Freenet6*, o comando *ping* necessitou de 14 saltos, independentemente da versão do protocolo utilizado. Porém, ao analisar o caminho com base

no comando *tracepth6*, foi possível observar que quando utilizada a nova versão do protocolo, apenas um salto é realizado. Isso ocorre por que, o pacote transmitido via IPv6 foi transportado em um túnel através de uma rede IPv4. Para determinar o caminho e saltos percorridos pelo pacote do túnel na internet IPv4 do laboratório de testes até o *Broker*, foi utilizado o comando *tracepath*, que é para testes exclusivos para IPv4. A figura 7.5 apresenta os *hops* utilizados para alcançar o servidor *Ferenet6* onde é possível verificar o caminho percorrido pelo pacote IPv6 encapsulado com o protocolo 41 na Internet IPv4.



7.5: Hops para alcance do freenet6 (Fonte: GOMES, 2012)

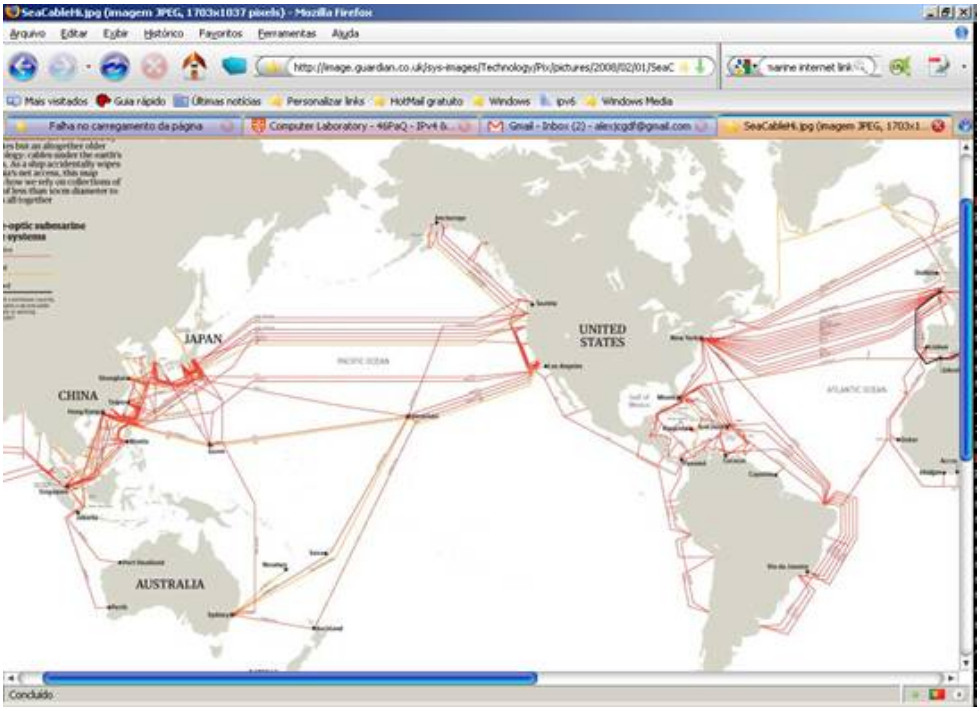
Um comparativo do tempo médio de um pacote ICMP (v4 e v6) é apresentado na figura 7.6, onde é possível verificar uma pequena diferença entre os dois protocolos. Esta diferença pode ser considerada pelo processamento do túnel, e pelo caminho utilizado entre o servidor de destino e o túnel *Broker*, porém, a diferença do processamento não é medida, já que os pacotes IPv6, por estarem encapsulados em IPv4, são roteados pela Internet como pacotes IPv4 até a ponta do *Broker*.



7.6: Teste de ping – comparação IPv4 x IPv6 – Servidor Freenet6 (Fonte: GOMES, 2012)

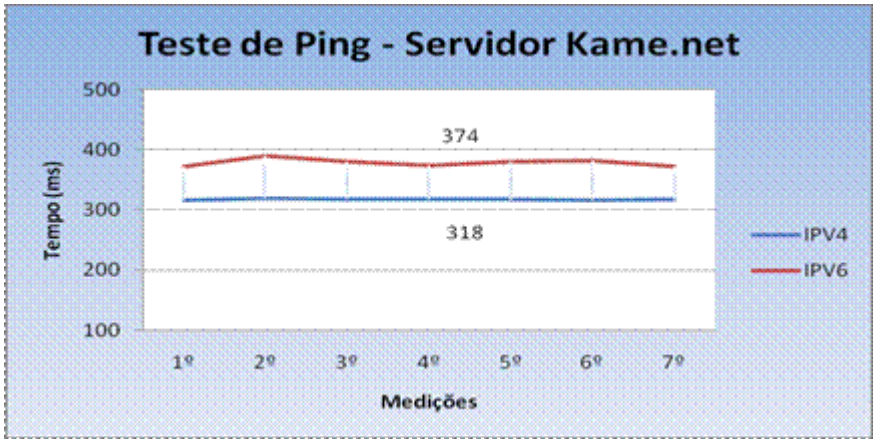
O próximo teste realizado teve como objetivo mensurar o tempo de processamento no roteamento entre os protocolos IPv4 e IPv6. Para este teste, foi utilizado um servidor

localizado no Japão. O servidor escolhido foi o www.kame.net, que suporta as duas versões do protocolo. A Figura 7.7 mostra como está distribuído os cabeamentos submarinos no entorno do teste. Ao analisar essa figura, observa-se que, após o pacote passar por um túnel do Canadá, ele será transmitido por um *backbone* IPv6 puro (sem encapsulamento), lado a lado com o *backbone* IPv4.



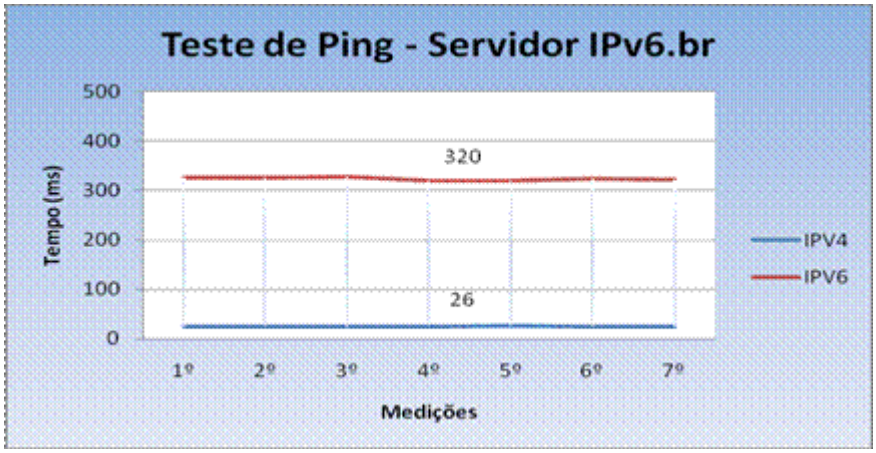
7.7: Mapa de interligação de redes – submarino (Fonte: GOMES, 2012)

Neste teste, a latência média aferida foi de 374 ms para IPv6 e 318 ms para IPv4. A diferença entre o primeiro teste (www.freenet6.com) e o segundo teste (www.kame.com) leva em consideração o percurso feito pelo pacote, já que, apesar de a saída utilizada tanto pelo pacote IPv4 quanto pelo IPv6 passar pelo mesmo percurso, o pacote IPv6 sai do tunelamento para a rede IPv6 somente no *Broker* origem, situado no Canadá, e, aí então, retorna para Seattle por onde sai para o Japão gerando um aumento no *delay*. Os resultados desse teste são visualizados na Figura 7.8.



7.8: Teste de ping – Comparação IPv4 x IPv6 – Servidor Kame.net (Fonte: GOMES, 2012)

Outro teste realizado considerou um servidor que suporta os dois protocolos IPv4 e IPv6 em pilha dupla localizado no Brasil. Este teste teve a finalidade de aferir o desempenho com destino aos sites e serviços brasileiros. O site utilizado foi o www.ipv6.br. A latência medida foi de 320ms para IPv6 e de 25ms para IPv4, obtendo uma diferença considerável em relação a ambos os protocolos. A explicação para essa grande diferença está ligado ao fato do IPv6 estar utilizando um *Broker* no Canadá. Sendo assim, só de latência para a utilização do *Broker*, foram gastos quase 300ms. Neste caso verificou-se que a utilização de *Broke*r IPv6 no Brasil só terá um desempenho próximo ao do IPv4 à partir do momento em que houver um serviço de *Broker* disponível no país, diminuindo assim o tempo gasto pelo pacote no túnel. A Figura 7.9 apresenta os resultados do testes no Brasil.



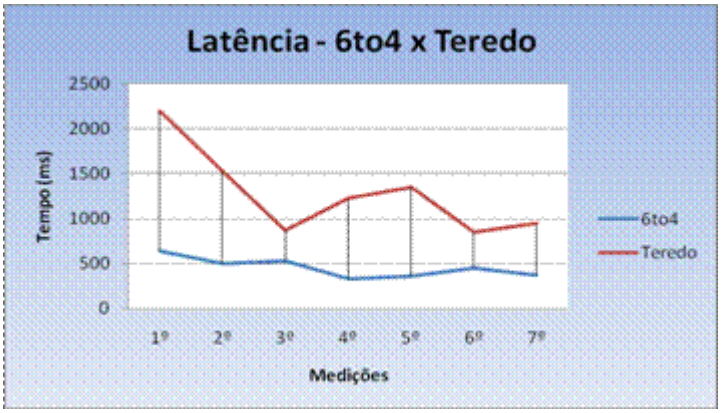
7.9: Teste ping – Comparação IPv4 x IPv6 – Servidor IPv6.br (Fonte: GOMES, 2012)

7.3. TUNELAMENTO – 6TO4 X TEREDO

O próximo conjunto de testes teve como objetivo analisar o desempenho dos mecanismos de tunelamento *6to4* e *Teredo*. Os testes foram realizados em máquinas configuradas com sistema operacional Windows XP. Inicialmente, as estações apresentavam as configurações de túneis desabilitadas e com endereço IPv4 público (válido na internet), sem a utilização de NAT, já que as conexões dos túneis *6to4* só são possíveis quando as estações estão configuradas com um endereço IPv4 válido.

O primeiro teste foi realizado habilitando-se o túnel *6to4*. O comando *ping* foi direcionado ao um *site* puramente em IPv6 (ipv6.google.com). O tempo médio de resposta obtido neste teste foi de 459 ms.

O próximo teste foi realizado habilitando o túnel *Teredo*. Neste teste, a máquina utilizada no experimento foi configurada com um IPv4 e seu acesso à rede externa foi realizado por meio de NAT. O comando *ping* foi direcionado ao mesmo *site*. Neste teste, o tempo de resposta foi muito superior ao realizado no *6to4*, sendo a latência média de 1278 ms. Esta diferença pode ser explicada com base no mecanismo de processamento e funcionamento do túnel *Teredo*, que opera atrás de NAT, diferentemente do *6to4*, que necessita de um endereço IP válido na Internet. A Figura 7.10 apresenta os resultados desses testes.



7.10: Teste ping – Comparação 6to4 X Teredo (Fonte: GOMES, 2012)

Ao analisar a Figura 7.10 observa-se que, além do túnel *Teredo* ser mais lento que o *6to4*, ele é menos consistente, oscilando bastante o tempo de latência.

8. IPV6 NO BRASIL

Segundo o Núcleo de informação e Coordenação do ponto BR (NIC.br), responsável pelo registro nacional de endereços IP para o Brasil, em conjunto com o Registro de endereçamento da Internet para a América Latina e o Caribe (LACNIC), o estoque de endereços IPv4 na Região da América Latina e Caribe chegou ao fim. O esgotamento desses endereços se deu três anos após Ásia e dois anos após a Europa. Com este esgotamento a região entra na chamada “fase de terminação gradual”, uma espécie de racionamento, em que serão distribuídos apenas mais dois milhões de endereços IPv4. A partir deste momento, as organizações no Brasil poderão receber no máximo, 1024 endereços IP, o que equivale a um (prefixo /22) a cada seis meses, mesmo que justifiquem a necessidade de blocos maiores.

Segundo a Cisco, o Brasil obtinha até junho de 2015 apenas 2,4% das conexões em IPv6, um percentual considerado baixo se comparado com os Estados Unidos que possuía até esta mesma data, 21% dos seus internautas navegando em IPv6. Mesmos com esse baixo percentual, o NIC.br considera um aspecto positivo, se comparado à situação meses antes, quando estes números eram quase nulos com apenas 0,11% das conexões utilizavam IPv6. (FIGUEREDO, 2015)

9. CONCLUSÃO

Ao longo do trabalho notou-se a importância do protocolo IP nos dias atuais. A Internet demostrou-se uma rede de redes, onde várias sub-redes, de diversas topologias e de tamanhos variados se interconectam para formar a grande rede mundial de computadores. Para que tudo isso aconteça, um conjunto de protocolos devem ser seguidos de forma rígida e padronizada. O protocolo IP foi desenvolvido para ser o mecanismo fundamental para que dados e informações possam trafegar na rede.

Com o decorrer do tempo, e com a demanda por serviços, notou-se a necessidade da evolução do protocolo, para que este pudesse suprir as necessidades de serviços e melhoria nas redes, além de permitir a sua expansão. O IPv6 chega com a proposta de solucionar a maioria desses problemas, como endereçamento, segurança, confidencialidade, diminuição do tempo de roteamento, entre outros. Diversos fatores, impedem uma migração rápida e definitiva, como o grande parque de equipamentos IPv4, que torna sua substituição extremamente cara e trabalhosa, e a criação de técnicas paliativas. No entanto, essa migração é inevitável para garantir a integridade e o futuro crescimento da rede, o que leva a criação de técnicas e ferramentas que venham a, pelo menos, garantir a interação entre os ambientes enquanto dura o período de migração entre as versões. Técnicas como tunelamento e tradução ajudam nesta interação, porém não resolvem o problema de forma definitiva, havendo mesmo que tardia a necessidade de migração.

De acordo com os resultados dos testes realizados entre as versões IPv4 e IPv6 observa-se que o desempenho dos protocolos são equivalentes quando em redes locais, porém as diferenças tendem a ser maiores quando necessitam utilizar os mecanismos de tunelamento.

Mesmo com essas diferenças, este estudo indicou a grande superioridade do IPv6 em relação ao IPv4. Sua implementação garantirá que novos serviços possam ser realizados de forma segura e confiável, o que ajuda não só o desenvolvimento de novas tecnologias, como também o desenvolvimento social, já que inúmeras instituições utilizam-se desse serviço para comunicação e disponibilização de conteúdo. Além disso, a nova versão permite que qualquer usuário utilizando qualquer tipo de dispositivo com suporte a IPv6 possa se conectar à rede, sem utilizar técnicas como NAT e CIDR. Contudo a migração entre as duas versões do protocolo é muito complexa e trabalhosa, e acontecerá de forma morosa, podendo perdurar por muito tempo até que aconteça por completo. Nesse período, ainda não será possível usufruir todas as funcionalidades e vantagens da nova versão do protocolo.

REFERENCIAS BIBLIOGRÁFICAS

CANNO, R.M., 2013. Redes IP I: Técnicas de Migração de Ambientes de Redes IPv4 para IPv6. Disponível em <http://www.teleco.com.br/tutoriais/tutorialredeip1/default.asp>. Acesso em Mar 2016.

COMMER, D.E. Interligação de redes com TCP/IP. Vol.1, 5 edição, Rio de Janeiro, Elsevier, 2006

FIGUEIREDE, P., 2015. IPv6 no Brasil: Anatel anuncia implantação do novo protocolo de Internet. Disponível em <http://www.techtudo.com.br/noticias/noticia/2015/03/ipv6-no-brasil-anatel-anuncia-implantacao-do-novo-protocolo-de-internet.html>. Acesso em março 2016.

FOROUZAN, B.A, Protocolo TCP/IP. 3º Edição, São Paulo, McGraw-Hill 2008

GOMES, A.J.C., 2012. Rede IP II: Melhores Práticas de Migração de Rede IPv4 para IPv6. Disponível em <http://www.teleco.com.br/tutoriais/tutorialredeipmig2/default.asp>. Acesso em Mar 2016.

KUROSE, J. F., ROSS, K. W. Redes de computadores e a Internet Uma abordagem top-down. 3º Edição, São Paulo, Pearson Addison Wesley, 2006

LICKLIDER, J.C.R., 1960. "Man-Computer Symbiosis". In: Transactions on Human Factors in Electronics, volume HFE-1, pag 4–11, Março 1960

LICKLIDER, J.C.R., 1965. "Man-Computer Partnership". In: International Science and Technology May 1965.

PEREIRA, A. P., 2009. O que é DHCP?. Disponível em <http://www.tecmundo.com.br/2079-o-que-e-dhcp-.htm>. Acesso em Fev 2016.

RFC 2460. Deering S., Hiden R., Internet Protocol, Version 6 (IPv6 Specification), Netwok Working Group, RFC 2460, Dezembro 1998.

RFC1519. Fuller, V., Li, T., YU, J., and K. Varadhan, “Classless Inter-Domein Routong (CIDR): an Address Assignment and Aggregation Strategy”, RFC 1519, Setembro 1993.

RFC1550. Brandner S., Mankin A., Ip Next Genaration (IPng) White Paper Solucutation, Network Working Gorup, RFC 1550, Dezembror 1993.

RFC1954. Newman P., Edwards L.W., Hiden R., Hoffman E., Liaw Ching F., Lyon T., Minshall G., Trnasmission of Flow Labelled IPv4 on ATM Links Ipsilon Version 1.0, Neworks Working Group, RFC 1954, Maio 1996.

RFC2373. Hiden R., Deering S., IP version 6 Addressing Architecture, Netwok Working Group, RFC 2373, Julho 1998.

RFC2883 Floyd S., Mahdavi J., Mathis M., Podolsky M., An Extension to the Selective Acknowlegement (SACK) Options for TCP.

RFC3053. Durand A., Fasano P., Guardini I., Lento D., IPv6 Tunnel Broker, Network Working Group, RFC 3053, Janeiro 2001.

RFC3315. Droms R., Bound J., Volz B., Lemon T., Perkins C., Carney M, Dynamic Configuration Protocol for IPv6 (DHCPv6), RFC 3315 Julho 2003

RFC4213. Nordmark E., Gilligan R., Basic Transition Mechanisms for IPv6 Hosts and Routers, Network Working Group, RFC 4213, Outubro 2005.

RFC4308. Swallow G., Drake J., Ishimatsu H., Reckter Y., Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI), Resource Reservation Protocol – Trafic Engineering (RSVP - TE) Suport for the overlay Medel, Network Working Group, RFC 4308, Outubro 2005.

RFC4380. Huitema C., Terede: Tunneling IPv6 Over UDP Through Network Address Translation (NATs), Network Working Group, RFC 4380, Fevereiro 2006.

RFC791. Postel, J., Information Science Institute Universety off Southern California, Defense Advanced Research Projects Agency Information Processing Techniques Office, “Internet Protocol – DARPA Internet Protocol Specification” RFC 791, Setembro 1981.

RFC792. Postel J., “Internet Message Control Protocol – DARPA Internet Protocol Specification”RFC 792, Setembro 1981.

ROBERTS, L. G., 1988. "The ARPANET and Computer Networks", in: A History of Personal Workstations, Autor: Adele Goldberg, Addison-Wesley Reading, Mass., 1988

RUSSO, R. (2013). Redes- Sabe o que é um PAT e NET?. Disponível em <http://escreveassim.com.br/2013/09/13/redes-nat-e-pat/>. Acesso em março 2016.

SANTOS, R.R., MOREIRAS, A.M., REIS, E.A., ROCHA, A.S., 2010. Curso IPv6 básico. Disponível em <http://ipv6.br/media/arquivo/ipv6/file/48/IPv6-apostila.pdf>. Acesso Jan 2016.

STRICKLAND, J. (n.d.). How ARPANET Works. Disponível em <http://computer.howstuffworks.com/arpanet1.htm>. Acesso em Fev 2016.

TANENBAUN, A.S., Redes de computadores 4º Edição Amsterdam, editora Campus.