Faculdade de Tecnologia de Americana

Curso de Segurança da Informação

Samir Salvador Camilo

Coexistência entre redes IPv4/IPv6

Americana, SP

2013

Faculdade de Tecnologia de Americana

Curso de Segurança da Informação

Samir Salvador Camilo

Coexistência entre redes IPv4/IPv6

Trabalho de conclusão de curso apresentada a Faculdade de Tecnologia de Americana como partes das exigências do Curso de Tecnologia em Segurança da Informação para obtenção de título de Tecnólogo em Segurança da Informação.

Orientador: Professor Rogério Nunes de Freitas

Americana, SP

2013

FICHA CATALOGRÁFICA elaborada pela

BIBLIOTECA – FATEC Americana – CEETPS

Samir Salvador Camilo

Coexistência entre redes IPv4/IPv6

Trabalho de Conclusão de Curso aprovado como requisito para obtenção do título de Tecnólogo em Segurança da Informação no curso de Tecnologia em Segurança da Informação da Faculdade de Tecnologia de Americana.

Banca Examinadora

Orientador: _____

Professor Rogério Nunes de Freitas

Convidado: _____

Professor Dr. José Luíz Zem

Convidado:_____

Professor Me. Diogo Robles

Americana, 06/06/13

Agradecimentos

A todos os docentes da Fatec Americana, pela dedicação em compartilhar os conhecimentos e experiências que adquiriam ao longo da vida, e a todos os demais funcionários, por proporcionarem um ambiente agradável e estimulante ao aprendizado. Ao Professor Rogério Nunes de Freitas, pelo esmero empregado na orientação, fundamental para o desenvolvimento e conclusão deste trabalho. À Professora Doutora Maria Cristina Aranda, por acompanhar de perto a elaboração do mesmo. Aos professores José Luís Zem e Diogo Robles, por agregar valor a este trabalho ao participarem da banca examinadora. Aos colegas de classe, pelo companheirismo nessa jornada. A todos os colegas de trabalho, especialmente Fatima França, que sanou muitas das minhas dúvidas técnicas sobre o tema desta monografia. Aos amigos, quer estejam perto, quer longe, particularmente a todos da RED e do PIX, pelas orações e força quando o fardo se tornou pesado. À minha família, por me ensinarem os valores que estão acima de qualquer conhecimento acadêmico. Finalmente, a Deus, que me deu a sua vida ao enviar Jesus, seu Filho, e, portanto, é digno de que eu lhe dê a minha.

Resumo

Este Trabalho de Conclusão de Curso tem como objetivo abordar o surgimento das redes de computadores e motivo de sua existência, além dos vários protocolos utilizados para viabilizar a comunicação entre sistemas diversos. Descrevem-se características básicas do funcionamento do Protocolo de Internet versão 4, usadas como base para o entendimento de sua sexta versão. Visa ainda explicar a motivação para a criação dessa nova versão, chamada de IPV6, e substituição do IPv4 como protocolo padrão utilizado na Internet para conectar as redes de computadores. São apresentadas diversas técnicas utilizadas para permitir a coexistência da versão 4 com a versão 6 da pilha de protocolos TCP/IP durante a transição de uma para a outra, até que a migração seja completa. Para tanto, farão parte do objeto de estudo as principais características de cada versão, algumas de suas peculiaridades e as diferenças entre elas. Por último, um modelo desenvolvido em laboratório será utilizado para simular um ambiente com redes mistas, e a comunicação entre elas através da transferência de arquivos de dados.

Palavras Chave: *IPv4; IPv6; esgotamento de endereços; Pilha Dupla; Tunelamento; Tradução de Endereços de Rede.*

Abstract

This monograph aims to address the emergence of computer networks and the reason for its existence, along with the various protocols used to enable communication between different systems. Basic features of the operation of Internet Protocol v4 are described and used as a basis for understanding its sixth version. It also aims to explain the motivation for creating this new version, known as IPv6, and the reason for replacing the IPv4 as the default protocol used on the Internet to connect computer networks. This paper also describes most of the techniques in use to allow coexistence of version 4 to version 6 of the TCP/IP protocol during the transition from one to the other, until the migration is complete. The main features of each version are examined, as well as some of its peculiarities and differences between them. Finally, a laboratory-developed model will be used to simulate an environment with mixed networks, and communication between them through the transfer of data files.

Keywords: *IPv4; IPv6; addresses exhaustion; Dual Stack; Tunneling; Network Address Translation.*

Sumário

Introdução

No princípio foram os computadores pessoais. Depois, computadores sem fio. Laptops e palmtops sendo usados com fins corporativos para agilizar a comunicação, facilitar os negócios e dar mobilidade a empregados conectados independentemente da distância que estivessem da base corporativa. Então, os telefones celulares, em particular os *smartphones*, passaram a fazer parte dessa imensa rede que interliga pessoas no mundo todo. E agora, os *tablets*, as televisões, geladeiras... e a lista segue.

Quando o primeiro computador eletrônico de uso geral surgiu, em 1946, o mundo começava, talvez sem ter consciência disso, o que talvez seja a maior revolução em toda sua história. Baseado nas máquinas mecânicas de calcular criadas por Leibniz, Pascal, Babbage, Hollerith (FONSECA FILHO, 2007), começou a ser projetado em 1943, com a finalidade de traçar com precisão a trajetória de projéteis e passou a ser utilizados para fins industriais e comerciais, já que a Segunda Guerra Mundial acabou um ano antes que fosse concluído.

Num ambiente de processamento centralizado, usuários se conectavam aos computadores de grande porte através de terminais. Isso moveu a tecnologia até que os computadores estivessem comunicando-se através das redes locais. Empresas distribuídas geograficamente conectavam-se através das redes metropolitanas e, dependendo de quão distantes os escritórios remotos estivessem, através das redes de longa distância. E, por fim, empresas se conectaram a outras empresas, órgãos governamentais, instituições de ensino, e cidadãos comuns, ao redor do mundo, através da Internet.

Entretanto, o que começou com fins governamentais, estudantis e comerciais, logo passou a ser explorado de outra forma. O computador havia se tornado "pessoal", ainda que tivesse um custo que o tornasse inacessível para a maioria dos indivíduos. Foi popularizando-se a medida que o custo

diminuía, e começou a fazer parte da vida das pessoas comuns, não só em seus empregos, mas em suas casas. Percebeu-se que a Internet poderia ser um instrumento de entretenimento para as pessoas, que enviavam mensagens para familiares distantes ou piadas para o colega da estação de trabalho vizinha, através do correio eletrônico. O número de *hosts* saltou de menos de 20 milhões em 1997 para mais de 160 milhões em 2003 (STALLINGS, 2005). A Web 2.0, por sua vez, trouxe a possibilidade de interação entre usuários através das redes sociais, criando um apelo que atinge pessoas que não tinham, até então, a mínima familiaridade com dispositivos computacionais.

Quando a versão 4 do protocolo IP foi projetada, não se imaginava que os 4 bilhões de endereços possíveis seriam utilizados. Mas, com tantas pessoas, cada uma com mais de um dispositivo conectado à rede simultaneamente e, com isso, mais e mais empresas disponibilizando conteúdo na Internet, o impacto no uso de recursos da "rede mundial" foi o esgotamento do que parecia ser um número infinito de endereços válidos.

Alguns métodos prolongaram a existência e utilização do IPv4 por um bom tempo, e é o que permite que ainda esteja ativo atualmente. Mais especificamente, o NAT, *Network Address Translation*[1], foi imprescindível para a sobrevida da versão 4 do protocolo IP. Entretanto, esforços por uma solução definitiva, até onde se pode imaginar, culminaram na nova versão desse mesmo protocolo, e que foi chamada de IPv6.

O protocolo IPv6 resolve o problema de demanda sofrido pela versão anterior, e ainda traz várias outras implementações para melhorar seu antecessor. Contudo, as coisas não são simples assim. Não se pode simplesmente mudar a chave "IPv4-IPv6" e instantaneamente adotar a versão 6 e abandonar a versão 4. Isso porque a maioria dos dispositivos e infraestrutura em produção ainda não está pronta para operar com o IPv6. E não é possível "desligar" a Internet e trocar tudo por uma inteiramente nova, construída já com base no novo modelo.

[1] Do inglês, Tradução de Endereço de Rede.

Portanto, as duas versões devem coexistir pacificamente, até que a transição esteja completa, e o IPv4 seja um capítulo encerrado da história da Internet. Para isso, várias técnicas foram desenvolvidas para conectar redes IPv4 às redes ou dispositivos IPv6. Essas técnicas de coexistência são objeto de estudo desse trabalho, que tem como objetivo a compreensão dessa nova tecnologia e dos desafios que devem ser enfrentados pelos profissionais envolvidos durante esse período de mudança.

Primeiramente, um breve relato é mostrado sobre o surgimento das redes de computadores, passando pelo funcionamento e características de redes locais e remotas, até a Internet.

No segundo capítulo, aborda-se o conceito de protocolos e o modelo OSI de camadas. Serão apresentados alguns dos primeiros protocolos de rede, entre eles protocolos proprietários, até chegarmos aos padrões atuais utilizados mundialmente.

O capítulo seguinte introduz características técnicas do IPv4, com foco no modelo de endereçamento, e explica por que a utilização dessa versão deixou de ser viável e a implementação do IPv6 é necessária.

O quarto capítulo apresenta a versão 6 do protocolo IP, suas características comparadas ao IPv4, a motivação para sua criação e utilização, e enfatiza as técnicas utilizadas para a coexistência de ambas as versões durante o período de transição.

No último capítulo um estudo de caso demonstra a aplicação da técnica de tradução de endereços entre as duas versões, simulando uma situação possível levando-se em conta o cenário mundial atual.

Finalmente, as conclusões obtidas através da pesquisa feita durante a elaboração deste material serão dispostas.

1- Redes de Computadores

> **“**Redes de computadores se tornaram um componente fundamental de quase todo tipo de negócios ao redor do mundo, mas as redes só existem para fornecerem um meio para o computador. Assim como as estradas e rodovias existem como meio para os carros, redes permitem que a informação trafegue de um sistema para o outro. O computador é a razão da existência das redes de dados.” (MCQUERRY, 2004, p. 5)**.**

1.1- Surgimento

Durante a Segunda Guerra Mundial, os generais alemães tentavam comunicar-se dos quartéis com os oficiais que estavam nos campos de batalha. Para isso, utilizavam a recente tecnologia de comunicação sem fio, o que permitia que as tropas se deslocassem rapidamente. Entretanto, as mensagens não podiam ser enviadas como texto limpo. Foram, então, usadas máquinas que eram vendidas comercialmente, conhecidas como Enigma, numa versão modificada pelos engenheiros alemães. Essas eram portáteis, alimentadas por baterias e enviavam mensagens curtas, de 200 a 250 caracteres, contendo instruções de quando avançar ou recuar, para onde a tropa devia se deslocar, o alvo a ser atacado, etc. Isso deu aos nazistas uma imensa vantagem estratégica.

O *Polish Cipher Bureau*, órgão polonês especializado em criptografia, foi capaz de decifrar as mensagens criptografadas pela máquina Enigma. Construíram então uma réplica da mesma e demonstraram como tinham obtido seus resultados com uma máquina mecânica chamada Bomba, que era usada para quebrar o código. Nessa fase, um time de cientistas e estudiosos de várias áreas se juntava em *Bletchley Park*, na Inglaterra, unindo esforços para decodificar as mensagens enviadas pelo exército alemão (FONSECA FILHO, 2007). De posse do trabalho realizado pelos poloneses, Alan Turing e Gordon

Welchman construíram uma máquina similar, prevendo alterações no método alemão e melhorando sua precursora.

Entretanto, as máquinas de decriptografia levavam até seis semanas para permitir que as mensagens fossem lidas. Na maioria dos casos, a mensagem já estava obsoleta, e não tinha valor algum. Tommy Flowers, um engenheiro dos correios, tinha familiaridade com eletrônica, que na época utilizava válvulas e comutadores (*switches*). Ele se propôs a empregar seus conhecimentos na construção de um aparelho que decriptografasse a comunicação alemã de forma que medidas de contra-ataque pudessem ser planejadas. Com o Colossus, como foi chamado, as mensagens levavam apenas seis horas para que pudessem ser lidas. Isso foi fundamental para a vitória do exército aliado.

Após o fim da guerra, esses estudiosos voltaram a seus países, cheios de novos conhecimentos e entendendo as possibilidades criadas pela tecnologia desenvolvida durante o conflito. O computador eletrônico poderia ser usado para diversas finalidades, e vários grupos independentes se dedicaram a construir equipamentos flexíveis. O ENIAC, concluído em 1946, é considerado o primeiro computador eletrônico com propósitos gerais (FONSECA FILHO, 2007), já que o Colossus tinha como único propósito decifrar mensagens, e o Z1, construído por Konrad Zuse em 1939, era eletromecânico.

Os primeiros sistemas para fins acadêmicos compreendiam computadores de grande porte, onde os serviços eram executados. Os operadores ou usuários utilizavam terminais que davam acesso aos *mainframes*[2] através de conectores seriais (RS232) ligados a uma porta serial de console, e assim inseriam dados, substituindo a técnica de se utilizar cartões perfurados para interagir com a máquina. Nesse contexto, o processamento de dados ocorria de forma centralizada, já que as aplicações se concentravam em um único hardware.

Para que o custo de um computador fosse justificado no orçamento, era preciso que seus recursos fossem explorados o tanto quanto fosse possível.

[2] Computador de grande porte com capacidade para processamento de grande volume de dados.

Para diminuir o tempo ocioso, o computador de grande porte tinha seu uso compartilhado por vários setores da universidade. Para ampliar esse uso, os terminais eram conectados ao *mainframe* através de linhas telefônicas. Portanto, poderia ser acessado de qualquer lugar, por exemplo, para maximizar sua utilização, desde que se conectassem a uma linha telefônica comum. Para ter acesso contínuo, o que era necessário para algumas funções críticas, as universidades ou empresas contratavam linhas telefônicas dedicadas, também chamadas de *leased lines*[3], o que tinha um alto custo.

1.2- Chaveamento de Pacotes

Até então, o técnica primária de comunicação era a comutação de circuitos, método utilizado pelas linhas telefônicas, onde a comunicação é estabelecida entre dois pontos e se mantém, com uma taxa constante e predeterminada, até que a transmissão termine (STALLINGS, 2005). Além do custo alto desse tipo de meio para a transmissão de dados, outra desvantagem é que a linha não pode ser utilizada enquanto o enlace não for desfeito. Portanto, o tempo ocioso entre um fluxo de dados e outro não poderia ser utilizado por outro sistema.

Alguns pesquisadores se dedicaram a estudar uma alternativa à comutação de circuitos. Separadamente, sem ter acesso à pesquisa uns dos outros, Leonard Kleinrock, doutorando do MIT, Paul Baran, do *Rand Institute* e Donald Davies e Roger Scantlebury do *National Physical Laboratory*, na Inglaterra, pesquisavam o assunto. Pouco tempo depois, J. C. R. Licklider e Lawrence Roberts seguiram em frente e lideraram o programa que resultou na ARPANET (Figura 1), a primeira rede de computadores a utilizar a comutação de pacotes, em 1969. Conectava apenas quatro nós: o *Stanford Research Institute* (SRI), a *University of California, Los Angeles* (UCLA), a *University of California, Santa Barbara* (USBC) e a *University of Utah*.

[3] Termo que descreve uma linha de comunicação privada de uso dedicado.

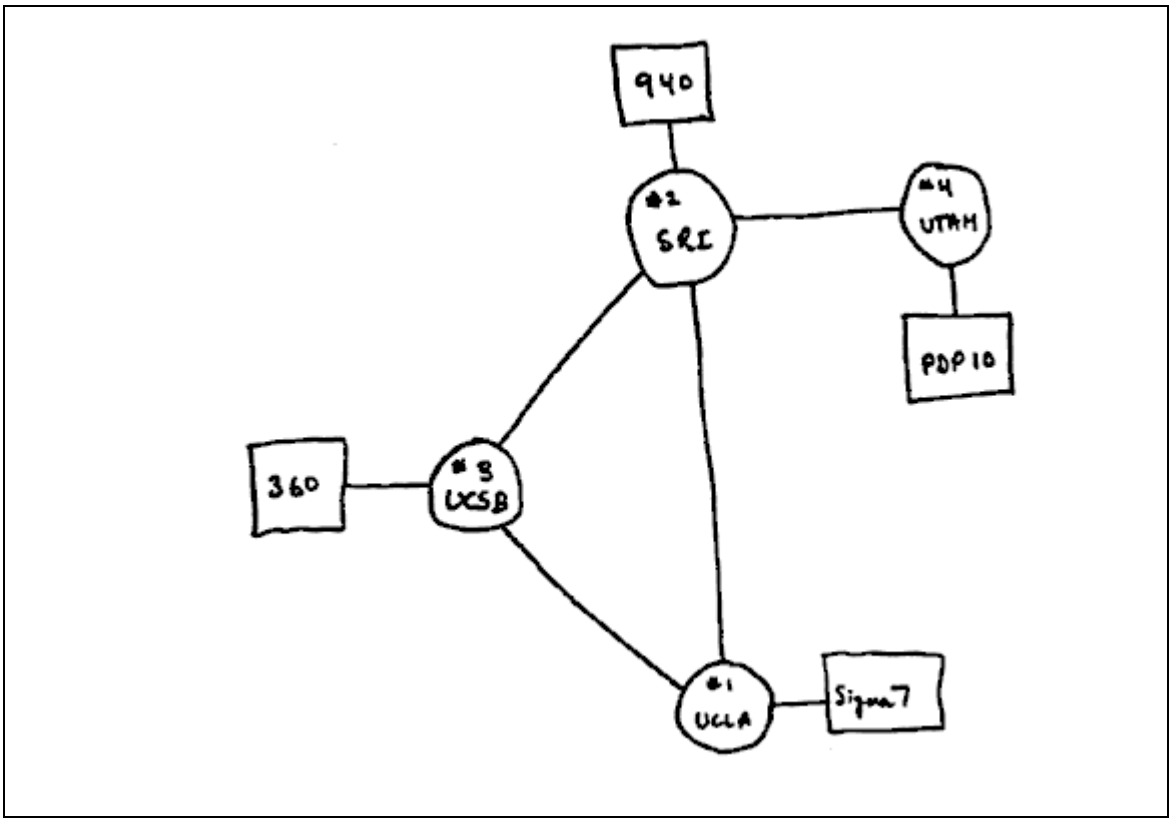


Figura 1. ARPANET em 1969.
Fonte: SRI. Disponível em: <http://www.sri.com/work/timeline/arpanet>. Acesso em: 15 mar. 2013.

1.3- Internet

Na década de 1970 surgiram algumas outras redes, como a ALOHAnet, utilizada para interligar as universidades nas diversas ilhas do Havaí através de microondas; a *Cyclades*, na França, sob a supervisão de Louis Pouzin; e a *SNA* da IBM (KUROSE, 2010). Entretanto, todas essas redes funcionavam de modo independente, isoladas, cada qual utilizando protocolos e tecnologia peculiares.

Nesse momento, a *Defense Advanced Research Projetcs Agency* (DARPA - Agência de Projetos de Pesquisa Avançada de Defesa) patrocinou o desenvolvimento de uma arquitetura que conectasse essas diferentes redes. Vinton G. Cerf e Robert E. Kahn elaboraram um trabalho chamado de CERF74,

que foi a base para o *Transmission Control Protocol*[4] (TCP) atualmente em uso. Já incluía conceitos como encapsulamento, segmentação de pacotes, retransmissão, controle de fluxo e um esboço do bloco de controle de transmissão (Figura 2). O termo "*internetwork*" é mencionado repetidas vezes nesse documento, e deu origem ao nome Internet.

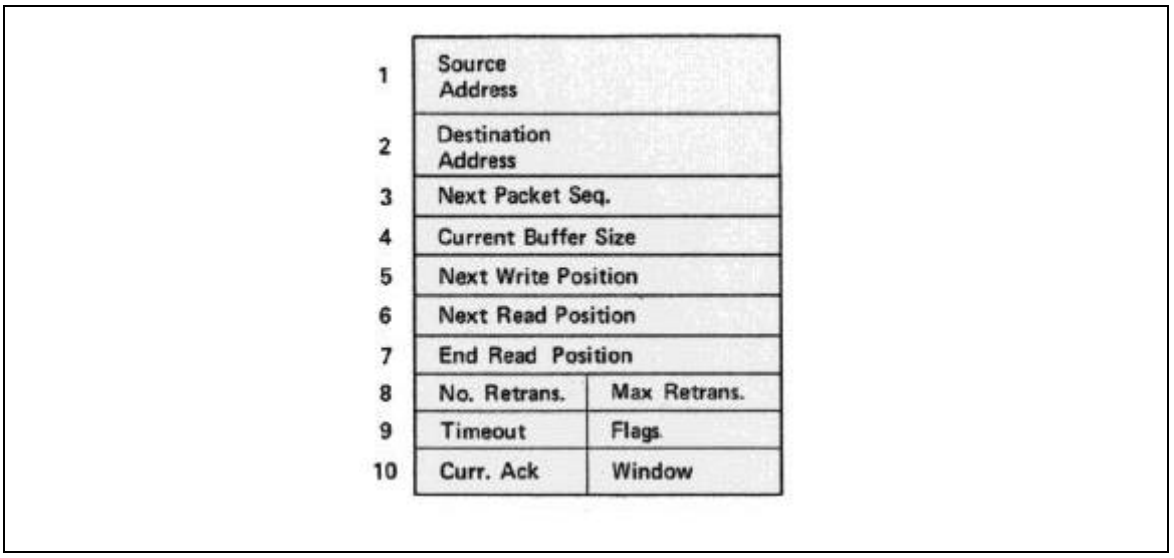


Figura 2. Bloco de Controle de Transmissão.
Fonte: CERF e KAHN (1974). Disponível em: < http://ece.ut.ac.ir/Classpages/F86/ECE571/Papers/CK74.pdf >. Acesso em: 18 mai 2013.

Atualmente, a Internet compreende milhares de redes locais, remotas entre si, com uma infinidade de estações computacionais interligadas por *switches*, roteadores e outros dispositivos gerenciados por ISPs[5], aproximando culturas, facilitando negócios, descentralizando o conhecimento de uma forma totalmente nova. Informações são mantidas “nas nuvens”. A Web, criada por Tim Bernes-Lee, já em sua segunda versão, é viabilizada, permitindo a existência das redes sociais, e agora esperamos pela versão 3.0, uma Web inteligente, com uma maior capacidade de organização de toda a informação compartilhada (FALCÃO, 2011), graças à infraestrutura global criada pela Internet.

[4] Protocolo de Controle de Transmissão
[5] *Internet Service Providers*, Provedoras de Acesso à Internet.

2- Protocolos de Rede

> "Nas redes de computador, a comunicação ocorre entre entidades de diferentes sistemas. Entretanto, duas entidades não podem simplesmente enviar fluxos de dados e esperar que sejam entendidas. Para que a comunicação ocorra, as entidades devem estar de acordo com um protocolo. Um protocolo é um conjunto de regras que governa a comunicação de dados." (FOROUZAN, 2008, pag. 6).

2.1- TCP/IP

Ao final da década de 1970, a ARPANET conectava cerca de 200 estações. O número de máquinas interligadas aumentaria para mais de cem mil em 10 anos segundo Kurose (2010), numa confederação de redes públicas que pode ser considerado o embrião da Internet que temos hoje. Isso porque os acadêmicos americanos se esforçavam para interligar suas universidades.

A Bitnet (acrônimo para "*Because it's there Net*[6]"), por exemplo, inicialmente interligava a *City University of New York* à *Yale University*, e era usada principalmente para troca de emails. Essa rede era composta por *Mainframes* IBM, e usava como protocolo de comunicação o *Network Job Entry*[7] (NJE)(RFC 1440). Ao mesmo tempo, a NSFNET, patrocinada pela *National Science Foundation*, e gerenciada pela Merit, um consórcio de universidades de Michigan, foi fundada como parte de um programa para promover a acessibilidade a supercomputadores, que era menos custosa que comprar um supercomputador para cada universidade. Outra rede, chamada CSNET (*Computer Science Network,* Rede de Ciência da Computação), interligava pesquisadores que não tinham acesso a ARPANET. Por fim, a ARPANET, que era a rede de computadores do departamento de defesa americano, que operava com um protocolo chamado NCP, *Network Control Protocol*[8], criado pelo *Network Working Group* (NWG, Grupo de Trabalho de

[6] Pode ser traduzido como "Rede 'Porque está lá'".
[7] Entrada de Processo de Rede
[8] Protocolo de Controle de Rede

Redes, em português), liderados por Steve Crocker, o também inventor das RFCs[9], *Request For Comments*, em português, pedido de comentários.

Em outubro de 1977, baseando-se no conceito de *gateway* apresentado por Cerf e Kahn, uma internet composta por três redes com tecnologias diferentes (ARPANET, rádio de pacotes e satélite de pacotes) demonstrou com êxito que esse tipo de comunicação era possível e viável (FOROUZAN, 2008). O *gateway* eliminava os problemas de diversos tamanhos de pacotes, interfaces diferentes e taxas de transmissão peculiares a cada dispositivo, funcionando como um intermediário na transmissão entre uma rede e outra.

Nessa ocasião decidiu-se separar os protocolos TCP e IP. O primeiro deveria gerenciar a segmentação, remontagem de pacotes e correção de erro (retransmissão), enquanto o IP (*Internet Protocol,* Protocolo de Internet) seria responsável pelo endereçamento de pacotes e roteamento dos mesmos (FOROUZAN, 2008). Ao mesmo tempo, a preocupação com aplicações de tempo real transmissão de voz levaram a criação de uma alternativa ao TCP, já que deviam priorizar o tempo de resposta em detrimento da garantia de que um determinado pacote chegaria ao seu destino. A esse protocolo chamou-se *User Datagram Protocol*[10] (UDP).

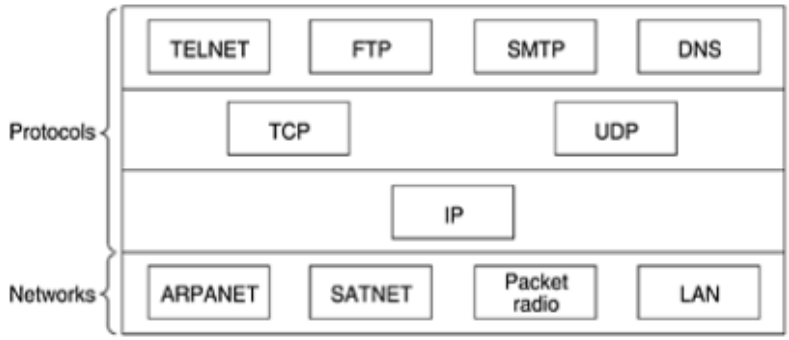


Figura 3. Protocolos e redes no modelo TCP/IP inicial.
Fonte: TANENBAUM (2010).

[9] O repositório de RFC é mantido pelo IETF – *Internet Engineering Task Force*
[10] Protocolo de Datagramas de Usuário. Datagrama é a unidade dos fragmentos do UDP e correspondem aos segmentos de dados do TCP.

Poucos anos depois, o Unix foi modificado pela *UC Berkeley* para incluir o TCP/IP, fazendo com que um sistema operacional contivesse um software de redes, o que contribuiu para torná-lo ainda mais popular, até que a ARPANET adotou-o como protocolo oficial, em 1983.

A pilha de protocolos TCP/IP é composta por uma série de protocolos que permitem a interação entre sistemas de diferentes modelos, funções e fabricantes, já que foi desenvolvida através de um esforço coletivo de voluntários, sem vínculos comerciais com empresas e corporações.

Tais protocolos estão classificados de acordo com camadas definidas pela arquitetura do modelo TCP/IP. Segundo Forouzan (2008) e Kurose (2007), essas camadas são cinco: física, enlace de dados, rede, transporte e aplicativo (ou aplicação), como se vê na Figura 4. Outros autores, como Tanenbaum (2010) e Odom (2008), concordam com a RFC 1122, de 1989, e citam apenas quatro, mesclando a camada física com enlace de dados. O primeiro modelo, entretanto, possuía apenas três (Figura 3).

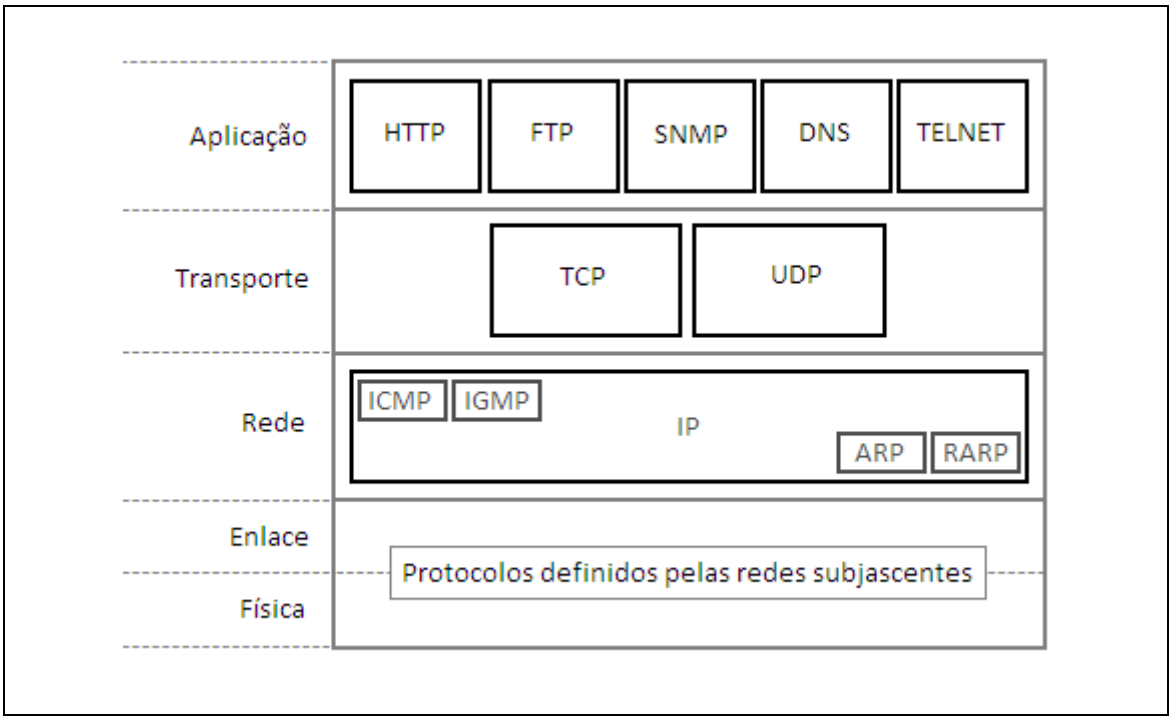


Figura 4. Camadas vs. Protocolos do modelo TCP/IP.
Fonte: FOROUZAN (2008), adaptado.

2.2- Modelo de Referência ISO OSI

O modelo OSI – *Open Systems Interconnection*[11] – foi criado pela ISO (*Internacional Standards Organization*[12]), com o intuito de permitir que sistemas diferentes pudessem ser interconectados sem a necessidade de alterações na lógica do software ou do hardware do sistema subjacente. Em outras palavras, cada fabricante poderia criar hardware com seu respectivo software sabendo que seria compatível com o sistema a ser conectado a ele, independentemente do fabricante desse outro *hardware*, se simplesmente seguissem os padrões definidos.

Todavia, esse modelo nunca foi totalmente posto em prática, embora tivesse sido "encomendado" pelo governo dos Estados Unidos. Isso se deu por alguns motivos, mas principalmente porque sua versão refinada foi publicada apenas em 1984, um ano depois que a ARPANET oficializou o uso do TCP/IP, e muitos fabricantes estavam desenvolvendo produtos com base nos protocolos dessa pilha.

O modelo OSI descreve a transferência entre *hosts* utilizando camadas para dividir funções e serviços, e se apoia no conceito de que cada camada deve prover serviços para a camada imediatamente superior, e se comunica com a mesma camada na outra extremidade. Por exemplo, a camada "n" provê serviços para a camada "n+1", pois encapsula os dados recebidos, e se comunica com a camada "n" do outro lado, quando tem seu cabeçalho lido para que o *host* verifique se aquele conteúdo é destinado a ele. Esse modelo apresenta sete camadas: aplicação, apresentação, sessão, transporte, redes, enlace de dados e, por fim, física (Figura 5).

A pilha TCP/IP é comparada ao modelo OSI, apesar de não ser um modelo de referência, pelo fato de ambos se basearem no conceito de uma pilha de protocolos independentes distribuídos em camadas, e por essas

[11] Interconexão de Sistemas Abertos.
[12] Organização de Padrões Internacionais.

camadas apresentarem praticamente as mesmas funções. Lado a lado, se correspondem como mostrado na Figura 5.

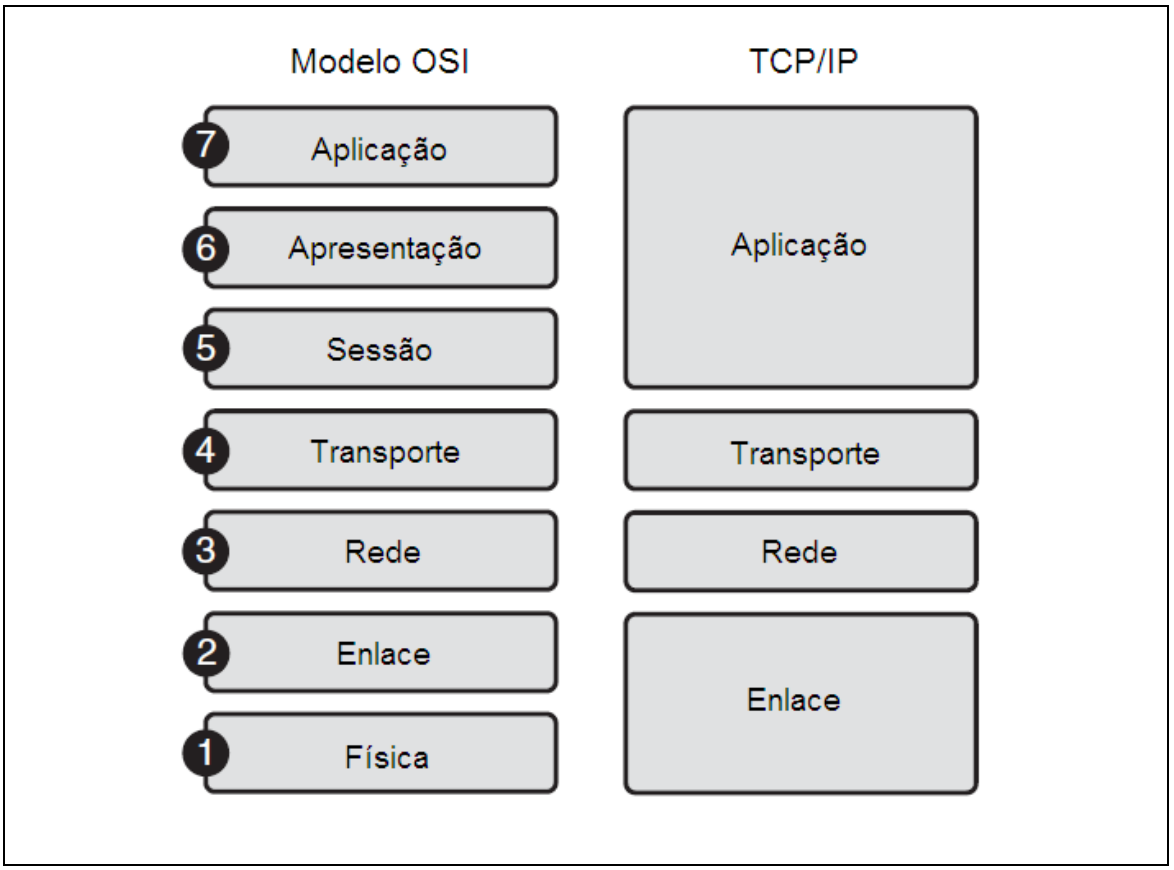


Figura 5. Comparação entre Modelo OSI e TCP/IP.
Fonte: JOHNSON (2009), adaptado.

2.3- Camada de Rede

Nesta monografia, trataremos especificamente da Camada de Rede, terceira do modelo OSI e segunda na arquitetura TCP/IP. Essa camada define como os pacotes enviados alcançarão seu destino e o trajeto de volta com a informação solicitada, sempre que os dois *hosts* envolvidos na comunicação estiverem em domínios de *broadcast*s diferentes, ou seja, em redes ou sub-redes diferentes. Para desempenhar essa função, são designados endereços lógicos de origem e destino, e um caminho entre esses dois pontos (ODOM, 2008).

Alguns protocolos foram desenvolvidos para isso. Entre eles, o IPX, parte da pilha IPX/SPX (*Internetwork Packet Exchange/Sequenced Packet Exchange*[13]), desenvolvido pela Novell, baseado no XNS[14], a suíte de protocolos da Xerox (CISCO, 2012). Essa pilha é similar à pilha TCP/IP, com o IPX servindo a camada três do modelo OSI, podendo ser comparado ao IP, e o SPX operando na camada quatro, assim como o TCP. Outro protocolo da camada de rede foi o *Datagram Delivery Protocol*[15], parte da pilha de protocolos *AppleTalk*, desenvolvido conjuntamente com o computador *Macintosh* pela Apple Computer (CISCO, 2012).

O mais importante entre eles, e o que se tornou padrão de fato, é o *Internet Protocol*, parte da pilha TCP/IP descrita por Cerf e Kahn, como visto anteriormente. Esse será visto com maior detalhamento no próximo capítulo.

[13] Troca de Pacotes de Rede/Troca de Pacotes Sequenciais.
[14] *Xerox Network Systems*, Sistemas de Redes Xerox.
[15] Protocolo para Entrega de Datagramas

3- IPv4

> "A função ou finalidade do Protocolo Internet é mover datagramas através de um conjunto de redes interconectadas. Isto é feito fazendo passar os datagramas de um módulo de internet para o outro até o destino for atingido. Os módulos de internet residem em *hosts* e *gateway*s no sistema de internet. Os datagramas são encaminhados a partir de um módulo de internet para outro através de redes individuais com base na interpretação de um endereço de internet. Assim, um importante mecanismo do protocolo de internet é o endereço de internet." (POSTEL, 1981, p.2)[16]

O *Internet Protocol* é o principal entre os protocolos que satisfazem os requisitos descritos para a camada de Rede da pilha TCP/IP. É considerado *connectionless*[17], ou seja, não estabelece nenhum tipo de sessão para que a comunicação ocorra. Também é classificado como *unreliable*[18], por não garantir a entrega dos pacotes, motivo pelo qual se considera que faz o que se chama de "*best effort"* ("melhor esforço"). Isso significa que o protocolo tenta entregar todos os pacotes, mas atrasos podem ocorrer, pacotes podem ser perdidos ou duplicados, ou entregues fora de sequência, e a correção desses erros fica a cargo de outros protocolos, como o TCP, por exemplo.

A primeira versão do *Internet Protocol* realmente utilizada foi a quarta desenvolvida, conhecida como IPv4, é ainda é a predominante nas redes de todo o mundo. Determina o formato de endereços lógicos utilizados na comunicação "fim a fim" entre redes e subredes física ou logicamente separadas, além de cuidar da fragmentação de pacotes que excedem o tamanho máximo. Os mesmos são divididos em pacotes menores e remontados ao alcançarem o destino.

Alguns outros protocolos realizam funções de extrema importância nessa mesma camada. Entre eles, estão os seguintes:

[16]Disponível em: <http://www.ietf.org/rfc/rfc791.txt>. Acesso em: 02 mai 2013.
[17] Pode ser traduzido por "não-orientado à conexão".
[18] Do Inglês, 'não confiável'.

- ARP – *Address Resolution Protocol* (Protocolo de Resolução de Endereço), que associa o endereço MAC (endereço físico utilizado pela camada dois) de um *host* para um endereço IP (lógico) de destino conhecido.
- DHCP – *Dynamic Host Configuration Protocol* (Protocolo de Configuração Dinâmica de *Host*), cuja função é prover configuração automática de endereço IP e máscara de rede a um *host*.
- ICMP – *Internet Control Message Protocol* (Protocolo de Mensagem de Controle de Rede), que permite que mensagens sejam usadas para controle e diagnóstico ("*ping*", por exemplo).
- IGMP – *Internet Group Management Protocol* (Protocolo de Gerência de Grupos de Internet), responsável pela gerência de grupos de *multicast*[19].

3.2- Principais características

O IPv4 define endereços lógicos com quatro octetos separados por pontos, totalizando 32 bits, representados em números decimais que vão de zero a 255 (MCQUERRY, 2004), onde a primeira parte representa o endereço lógico de uma rede ou subrede, e a segunda parte, combinada com a primeira, identifica um *host* único daquela rede. Esses endereços estão divididos em cinco classes, das quais as três primeiras disponibilizam endereços válidos, e as outras duas são reservadas para fins específicos, como visto na Figura 6.

Os endereços pertencentes à **classe A** servem a redes que necessitam de endereços disponíveis para muitos *hosts,* ou seja, redes extremamente grandes. Sendo assim, reserva apenas o primeiro octeto para o endereço da rede, e os três octetos seguintes para endereços dos dispositivos conectados a ela. Seus endereços têm sempre o primeiro bit igual à zero, logo variam de 00000000_2 (0_{10}) a 01111111_2 (127_{10}). Todavia, as redes 0.0.0.0 e 127.0.0.0 são

[19] Método de endereçamento que entrega pacotes a um grupo específico de *hosts* utilizando apenas um endereço lógico.

reservadas, restando os valores entre 1 e 126 no primeiro octeto. Um endereço *32.0.0.1* é um exemplo de um endereço IP classe A.

Endereços **classe B** suprem redes de médio à grande porte, destinando dois octetos para a rede e os outros dois para *hosts*. Seu primeiro octeto pode assumir valores entre 128 e 191, já que, nessa classe, os endereços começam com os bits 10, e variam de 10000000_2 (128_{10}) a 10111111_2 (191_{10}). Exemplo: *191.178.1.1* corresponde a um endereço IP classe B.

A **classe C**, por sua vez, define 24 bits para o endereço da rede, sempre iniciados em 110 (de 11000000_2, ou $192_{10,}$ até 11011111, ou 223_{10}), e o último octeto para *hosts*. Um endereço IP *202.10.254.255* está na classe C.

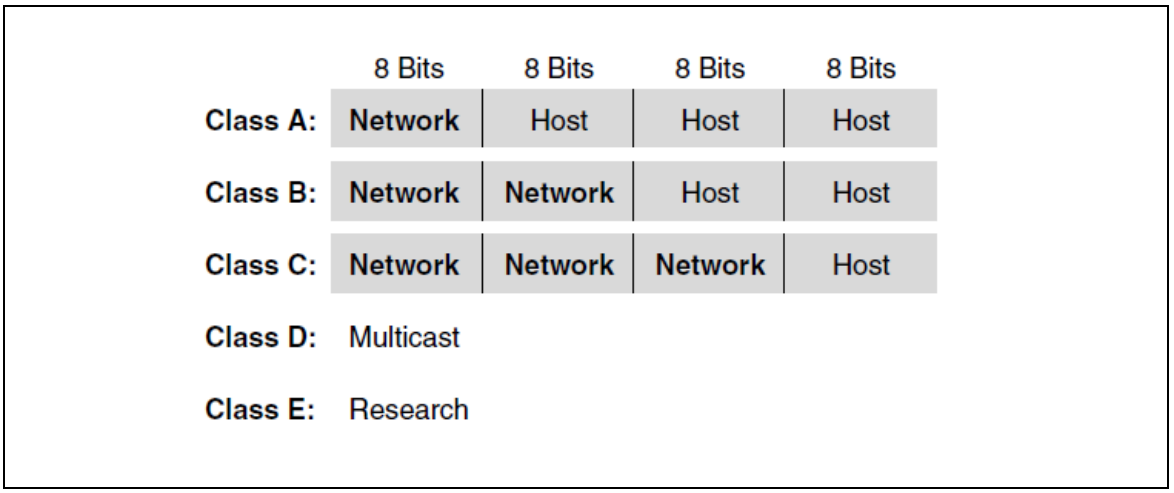


Figura 6. Classes de Endereços IP.
Fonte: MCQUERRY (2004).

A **classe D** é reservada para endereços *multicast,* com os quatro primeiros bits iguais a 1110, resultando num primeiro octeto variando entre 11100000_2 (224_{10}) e 11101111_2 (239_{10}). Exemplo: *224.0.0.1*.

Finalmente, a **classe E** é reservada para pesquisas. Tem os quatro primeiros bits iguais a 1111, portanto pode começar com valores entre 11110000_2 e $11111111_{2,}$ ou entre os decimais 240 e 255. Estes são reservados pelo IETF (*Internet Engineering Task Force,* Força-Tarefa de Engenharia para Internet) para pesquisas, e nunca foram disponibilizados para uso público.

Para as classes A, B e C, o primeiro endereço de cada rede é o endereço dessa rede, e o último é o endereço de *broadcast*[20] da mesma. Assim, uma rede classe C, que destina oito bits variando entre 0 e 1, totalizando 256 possibilidades (2^8), pode ter até 254 *hosts*, descontando-se um endereço para a rede (todos os bits de *hosts* em 0) e um para *broadcast* (todos os bits de rede em 1). Exemplificando, uma rede classe C com os bits de rede iguais a *191.178.255* teria:

- Endereço de rede: 191.178.255.0;
- Endereço de Broadcast: 191.178.255.255;
- Endereços de *host* possíveis: 191.178.255.1 a 191.178.255.254.

Portanto, podemos resumir as características das classes A, B e C da seguinte forma:

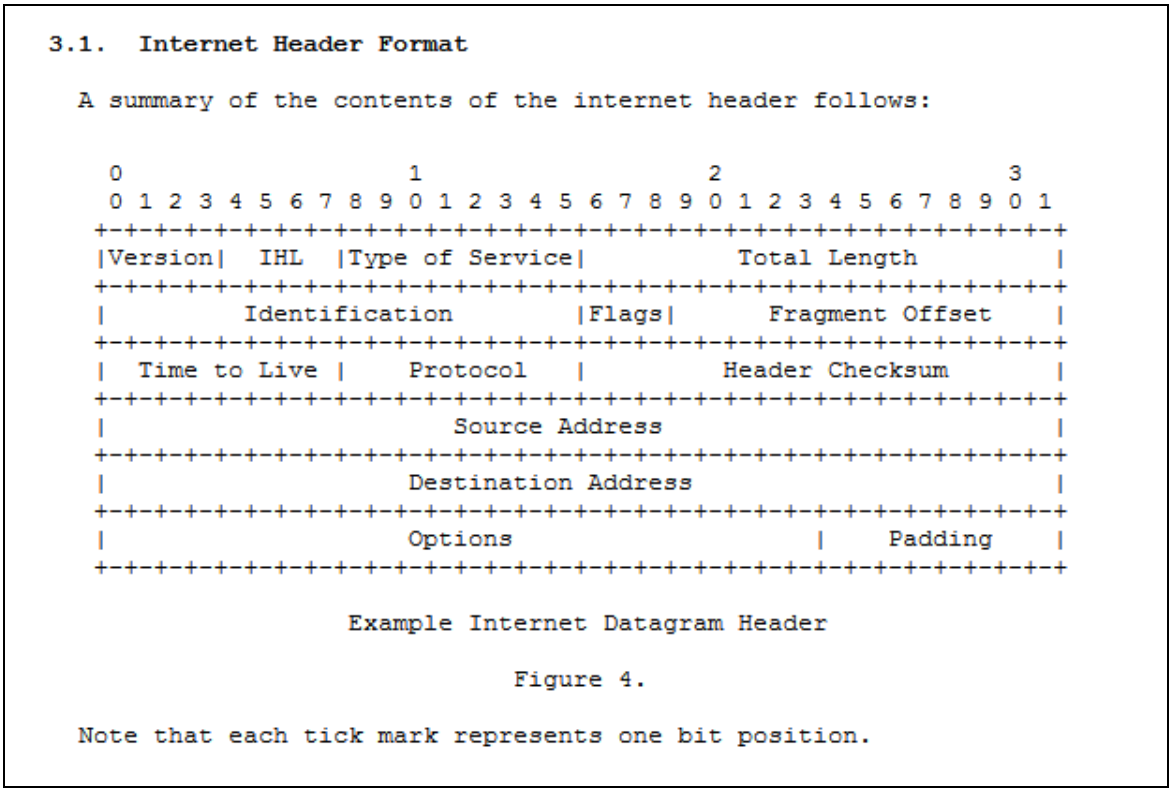
Tabela 1. Propriedades das classes de endereços IP.
Fonte: MCQUERRY (2009).

Tipo de endereço	**Classe A**	**Classe B**	**Classe C**
Bit(s) inicial(is)	0xxxxxxx	10xxxxxx	110xxxxx
Range de endereços de redes	1.0.0.0 a 126.0.0.0	128.0.0.0 a 191.255.0.0	192.0.0.0 a 223.255.255.0
Número de redes possíveis	127	16.384	2.097.152
Número possível de *hosts*[21]	16.777.216	65.536	256

O esquema de comunicação de redes em camadas propõe que cada uma delas se comunique com as camadas imediatamente adjacentes em uma extremidade do sistema, e com a camada correspondente a ela mesma no outro lado. Por exemplo, a camada de rede se comunica com os protocolos das camadas de transporte (imediatamente superior) e de enlace (imediatamente inferior) quando do início da comunicação, e com a camada de rede no lado

[20] Método de endereçamento que entrega os pacotes com tal endereço de destino a todos os *hosts* de determinada rede.
[21] Em cada rede/sub-rede subtraem-se dois *hosts* devido aos endereços reservados para rede e *broadcast* .

oposto, através de um cabeçalho contendo informações de controle. Por meio desse cabeçalho, consegue realizar suas funções primordiais: troca informações como endereços IP de origem e destino e numeração em caso de fragmentação de pacotes. A Figura 7 mostra esse cabeçalho da maneira como foi representado na RFC 791.



3.1. Internet Header Format

A summary of the contents of the internet header follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Example Internet Datagram Header

Figure 4.

Note that each tick mark represents one bit position.

Figura 7. Cabeçalho IPv4.
Fonte: POSTEL (1981). Disponível em: <http://www.ietf.org/rfc/rfc791.txt>. Acesso em: 02 mai 2013.

A interação com as camadas adjacentes se dá seguindo o conceito de encapsulamento, onde a camada imediatamente inferior gera um cabeçalho e encapsula os dados gerados pela camada imediatamente superior. Neste caso, o cabeçalho IP é adicionado ao segmento de dados (TCP) ou datagrama (UDP), formando um pacote IP. Este pacote IP, por sua vez, recebe um novo cabeçalho, dessa vez contendo os endereços MAC, e passa a ser chamado de quadro de dados, ou *frame*, no original. Cada um desses cabeçalhos também informa o tipo de dados que carrega, através do campo “Protocolo”. Quando a camada de transporte do destinatário recebe o pacote IP, sabe se este contém um segmento de dados (TCP) ou um datagrama (UDP), por exemplo.

3.3- Evolução/Esgotamento

"A Internet cresceu além de todas as expectativas" (Rekhter, 1996). Assim começa o texto explicando a motivação da criação da RFC 1918. Dos apenas pontos iniciais da ARPANET, em 1969, passou a ter 200 mil *hosts* distribuídos em 3000 redes em 1990. Em 1992, o milionésimo computador se conectou a rede. Apenas um ano depois, aproximadamente 15 milhões de usuários têm acesso à Internet. Em 2003, atingia 160 milhões (STALLINGS, 2005).

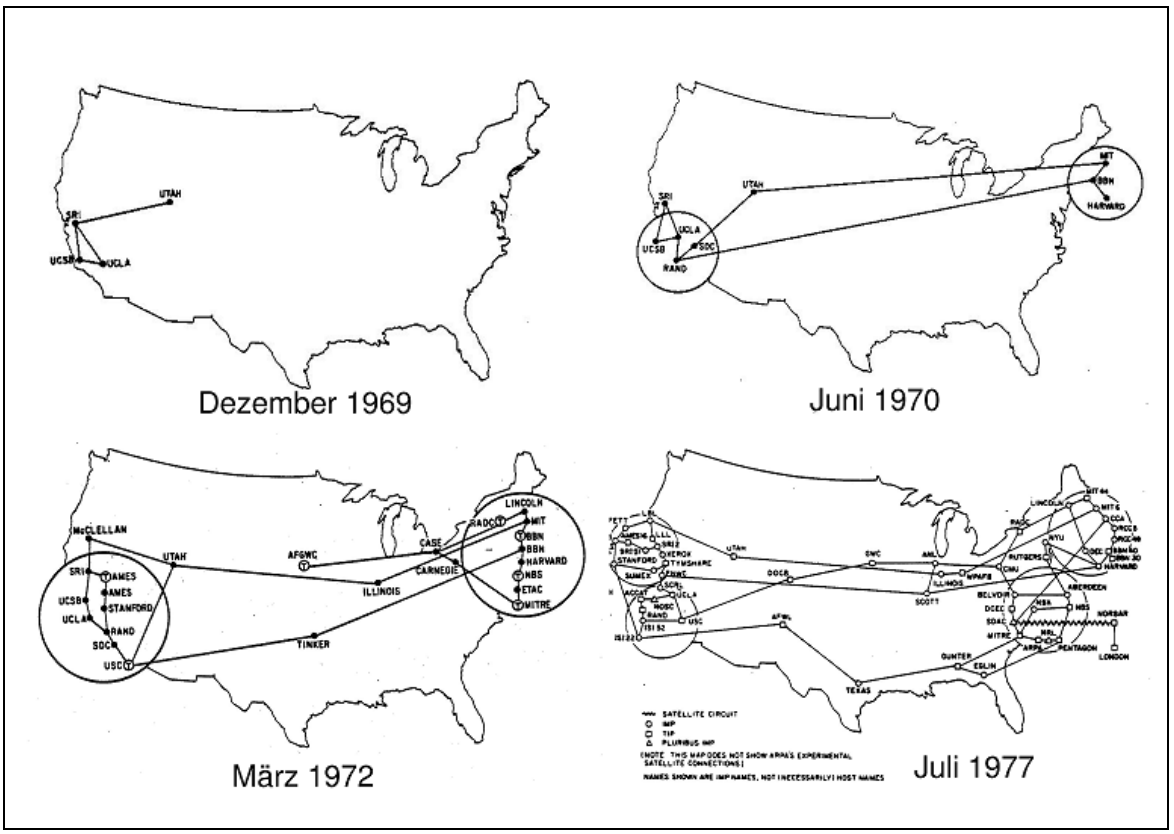


Figura 8. Progressão da ARPANET.
Fonte: FIBEL (2004), Disponível em: <http://www.fibel.org/linux/lfo-0.6.0/node457.html>. Acesso em: 02 mai 2013.

Até certo momento, todo *host* que utilizava o protocolo TCP/IP recebia um endereço de IP único, atribuído pela IANA[22], que identificaria aquele dispositivo globalmente. Mas com o aumento exponencial de estações se

[22] *Internet Assigned Numbers Authority*, entidade fundada em 1988 responsável pela atribuição de endereços IP e números de portas de serviços.

conectando, a preocupação com o esgotamento do número de IP levou à criação do conceito de *endereços privados* (Tabela 2), explicado na RFC 1597, de março de 1994, substituída pela sua versão definitiva, a RFC 1918, dois anos mais tarde.

Esses endereços seriam utilizados por estações que não necessitassem se comunicar diretamente com a Internet. Os endereços públicos seriam únicos globalmente, como já acontecia, e os endereços privados, ou locais, seriam únicos dentro das organizações, mas poderiam ser ambíguos em relação a outras organizações. Portanto, não seriam endereços IP válidos para roteamento na Internet. Assim, se um computador com um IP privado quisesse se comunicar com outro computador fora da rede de sua organização, deveria passar por um processo de tradução, realizado pelo *gateway* da rede, para ser alterado temporariamente para um endereço válido. A técnica utilizada para isso está descrita na RFC 1631, intitulada "*The IP Network Address Translator (NAT)*", em português, Tradução de Endereços de Redes IP (NAT).

Tabela 2. Endereços de Redes Privadas (RFC 1918).
Fonte: REKHTER et al. (1996). Disponível em: <http://www.ietf.org/rfc/rfc1918.txt>. Acesso em: 02 mai 2013.

Classe	Faixa de Endereços	Número de redes
A	10.0.0.0 - 10.255.255.255	1
B	172.16.0.0 - 172.31.255.255	16
C	192.168.0.0 - 192.168.255.255	256

Outra medida tomada no mesmo sentido foi a adoção de CIDR, *Classless Inter-domain Routing*[23], descrito pela RFC 4632. Convencionou-se que os endereços das redes deviam estar agrupados de forma contígua, o que diminuiria brutalmente o tamanho das tabelas de roteamento das provedoras de Internet. Permitiria também que os endereços fossem distribuídos para diversas redes de acordo com a real necessidade de cada organização. O uso de máscaras de rede diferentes das máscaras padrão de cada classe

[23] Roteamento Interdomínio Independente de Classe.

possibilitaria que a faixa de endereços de uma classe fosse subdividida em redes menores, o que racionalizaria o uso de endereços IP globais.

O *Dynamic Host Configuration Protocol*[24], mais conhecido por DHCP, contribuiu na conservação de endereços provendo endereçamento temporário a usuários finais. Dessa forma, quando alguém não estivesse conectado à Internet, o IP que estava em uso poderia agora ser atribuído a outro *host*. A RFC 1541, mais tarde feita obsoleta pela RFC 2131, explicava o uso desse protocolo.

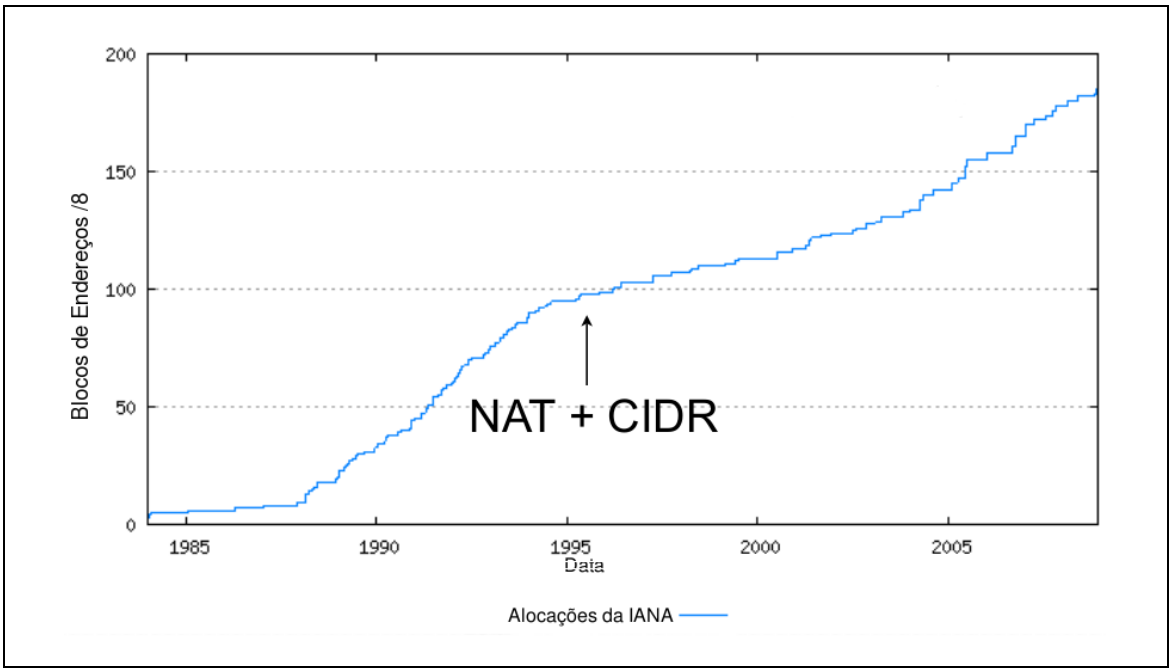


Figura 9. Alocação de endereços.
Fonte: IPV6.BR (2012). Disponível em <http://ipv6.br/entenda/introducao/>. Acesso em 10 mai 2013.

Com a utilização de endereçamento privado e o uso de NAT, a segurança das redes aumentou, já que os *hosts* nas redes internas não tinham seus endereços lógicos divulgados, dificultando a ação de possíveis invasores. O CIDR, por sua vez, deu flexibilidade para os engenheiros de redes definirem o endereçamento nas redes locais, e aumentou o número de possibilidades para a criação de subredes. Mais que isso, essas técnicas somadas atingiram seu propósito primordial: que a extinção dos endereços fosse adiada por tempo suficiente até que uma solução definitiva fosse posta em prática.

[24] Protocolo de Configuração Dinâmica de Estação.

4- IPv6

> "O IPv6 é uma nova versão do Internet Protocol, projetado como um passo evolutivo, em vez de revolucionário, do IPv4. Funções que se consideram como funcionando no IPv4 foram mantidas no IPv6. Funções que não funcionam ou são raramente utilizadas foram removidas ou tornadas opcionais. Alguns novos recursos foram adicionados, onde a funcionalidade foi considerada necessária." (BRADNER, MANKIN, 1995, p. 20)[25]

Numa cerimônia formal no dia três de fevereiro de 2011, a IANA alocou os últimos cinco blocos de endereços disponíveis, um para cada bloco regional (*Regional Internet Registries* (RIRs)), concretizando o que pode ser chamado de exaustão de endereços IPv4. A ARIN, *American Registry for Internet Numbers*, ainda tem endereços não utilizados, que serão distribuídos de acordo com políticas preestabelecidas. Sendo assim, começa a era do IPv6, ou ainda, a transição da versão 4 para esta última.

Inicialmente chamado de IPng, ou "*IP new generation*", o IPv6 começou a ser desenvolvido a partir da RFC 1550, de 1993, a qual socilitava propostas para o novo modelo, e o padrão foi definido na RFC 1752, publicada em 1995. Entre as principais preocupações estavam escalabilidade, tempo necessário para desenvolvimento, transição e segurança.

4.1- Principais diferenças entre IPv4 e IPv6

Como mencionado anteriormente, o IPv6 foi construido como uma evolução da versão anterior, e não como uma revolução. Isso quer dizer que existem muitas similaridades entre eles, e a versão 4 pode ser usada como base para o entendimento da versão mais recente, apontando-se a diferença entre eles.

[25] Disponível em: <http://www.ietf.org/rfc/rfc1752.txt>. Acesso em: 04 mai 2013.

O ponto que mais chama a atenção, e fundamentalmente resolve o problema de escassez, é o número de bits que forma o endereço lógico. Enquanto o IPv4 tem 32 bits, possibilitando aproximadamente 4 bilhões de *hosts* ($4x10^9$), o IPv6 usa 128 bits, em oito grupos de 16, representados por caracteres hexadecimais e separados por “dois pontos”. Com esse formato, possibilita a alocação de aproximadamente $340x10^{36}$ de endereços(JAIN, SHARMA, 2010), ou seja, $85x10^{27}$ vezes a quantidade de endereços que os 32 bits da versão 4 permitiam, ou ainda, aproximadamente 48,6 $x10^{30}$ endereços para cada habitante do planeta. O sufixo nos mesmos moldes do CIDR (“/xx”) indica quantos dos bits formam o endereço de rede. Exemplo:

2001:0DB8:130F:0000:0000:7000:0000:140B /64

Como notação alternativa, podemos agrupar campos com todos os bits em zero e representá-los por “**::**”, contanto que isso ocorra uma única vez. Os bits com valor zero podem ser suprimidos se estiverem à esquerda de algum bit válido. O endereço abreviado fica da seguinte maneira:

*2001**:**DB8**:**130F**::**7000**:**0**:**140B /64*

Quanto ao método de transmissão, existem três tipos de endereços:

- ***Unicast**:* os pacotes são transmitidos para um único destinatário;
- ***Multicast**:* os pacotes são transmitidos para **todos** os *hosts* um grupo predeterminado;
- ***Anycast**:* os pacotes são entregues a **um** *host* de um conjunto determinado;

Segundo Jain e Sharma (2010), uma diferença fundamental é que na versão 4, um único endereço IP é atribuído para cada placa de rede, enquanto espera-se que cada interface IPv6 tenha mais que um endereço. Por padrão, a interface possui um endereço de *multicast* e dois de *unicast (loopback e link-local).* Para *unicast*, existem vários tipos de endereço, sendo que o escopo de cada um deles varia de acordo com seu tipo. Podem ser:

***Link-local**:* é um endereço válido apenas no segmento onde a interface está conectada, logo, pacotes destinados a esses endereços não são roteados. Toda interface com IPv6 habilitado recebe automaticamente um endereço *link-local*, com o prefixo $FE80_{16}$, ou $1111\ 1110\ 10_2$.

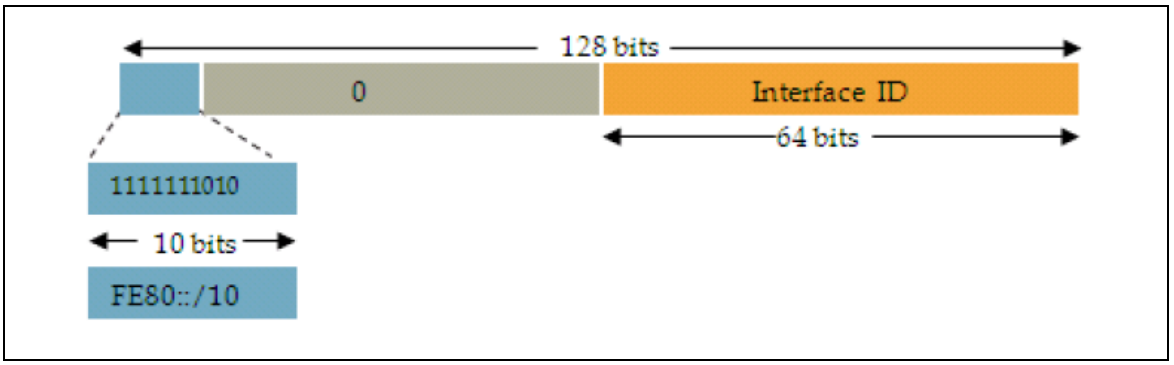


Figura 10. Estrutura de endereço IPv6 *Link-Local*.
Fonte: JAIN e SHARMA (2010).

O endereço *link-local* é geralmente gerado de forma automática assim que o IPv6 é habilitado numa interface, e pode ser comparado ao IP de APIPA[26] (169.254.0.0/16) usado pelo *Windows (*MICROSOFT, 2005)[27]. O identificador da interface, que corresponde à porção do *host* no IPv4, contendo, por padrão, 64bits, é extraído do *MAC-Address* da mesma*.* O *MAC-Address* é um número de 48 bits formado pelo *Organizationally Unique Identifier*[28] (OUI) em conjunto com um número também único atribuído a cada interface de rede, de 24 bits. Após a expansão, é chamado de *Extended Unique Identifier* (Identificador Único Estendido), ou EUI-64, o que corresponde ao novo padrão definido pelo IEEE (que usa 24 bits para o OUI mais 40 bits de identificação).

O processo para obter esse identificador é o seguinte: de posse do *MAC-Address*, separa-se o entre as duas porções, com 24 bits cada, é inserido o valor "*FFFE*" (Figura 11-a), um valor reservado pelo IEEE que não pode ser usado em EUI-64 para interfaces físicas. Depois, inverte-se o sétimo bit, que, inicialmente em "0", indica que o endereço é administrado pelo IEEE, ou localmente, se for "1" (Figura 11-b). Para uma interface com *MAC-Address*

[26] *Automatic Private IP Addressing*, endereço IPv4 atribuído automaticamente a interfaces que não conseguem estabelecer comunicação com um servidor DHCP e não tem um IP válido configurado.
[27] Disponível em < http://technet.microsoft.com/en-us/library/cc759208%28v=ws.10%29.aspx>, acesso em 14 mai 2013.
[28] Identificador Organizacional Único. Identifica os fabricantes de Interfaces de rede.

igual a **00:12:7F:EB:6B:40**, o EUI-64 é igual a **02:12:7F:FF:FE:EB:6B:40**. Por ser um endereço do tipo *link-local*, recebe o prefixo FE80/10, com os 54 bits da porção da rede com valor igual a “0”.

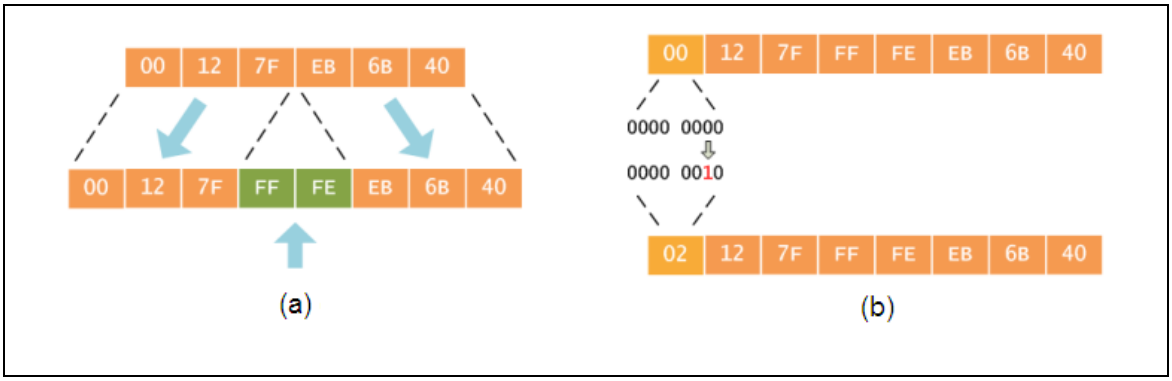


Figura 11. Processo de composição do EUI-64.
Fonte: STRETCH (2008) Disponível em: <http://packetlife.net/blog/2008/aug/4/eui-64-ipv6/>. Acesso em: 11 mai 2013.

Aplicando-se as regras de notação abreviada, obtêm-se o seguinte endereço:

FE80::212:7FFF:FEEB:6B40/64

Unique Local: é o tipo de endereço que deve ser utilizado somente localmente, assim como os endereços privados (RFC 1918). Tem como prefixo FC00::/7, ou seja, 1111 110_2, logo, varia entre *FC00* e *FD00* (1111 1100_2 e 1111 1101_2).

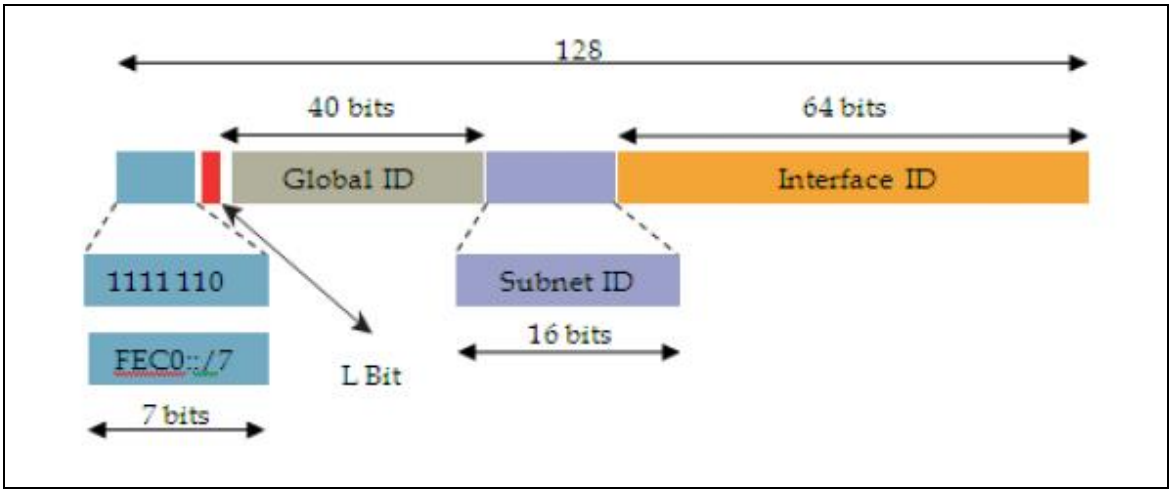


Figura 12. Estrutura de endereço IPv6 *Unique Local.*
Fonte: JAIN e SHARMA (2010).

O oitavo bit é chamado de bit “L”, de “*local”.* Quando for igual a “1” indica que o endereço foi atribuído localmente. O uso do bit “L” em “0” ainda não foi definido, e fica reservado para uso futuro. O *Global ID* é um valor pseudorrandômico, ou seja, gerado por um algoritmo (proposto na seção *3.2.2* da RFC 4193) para, propositalmente, ser único no mundo e, ao mesmo tempo, não ter nenhuma relação de continuidade com os endereços *unique-local* atrubuídos em uma mesma rede. A composição desse endereço foi discutida na RC 4193, de outubro de 2005, mostrado na Figura 12.

Global: comparado ao “endereço público” do IPv4, deve ser único no mundo para que o roteamento na Internet seja possível. São distribuídos pela IANA para as RIRs (*Regional Internet Registry,* Registro Regional da Internet), como a ARIN, por exemplo, e a LACNIC (*Latin America and Caribbean Network Information Centre*)[29], que administram a concessão de endereços válidos. Até agora, todos os endereços disponibilizados estão no bloco *2000::/3*. O *Global Routing Prefix* (Prefixo de Roteamento Global) segue um modelo hierárquico, agregando os endereços por região, desenhado para aperfeiçoar as tabelas de roteamento, melhorando o desempenho e evitando o aumento das mesmas.

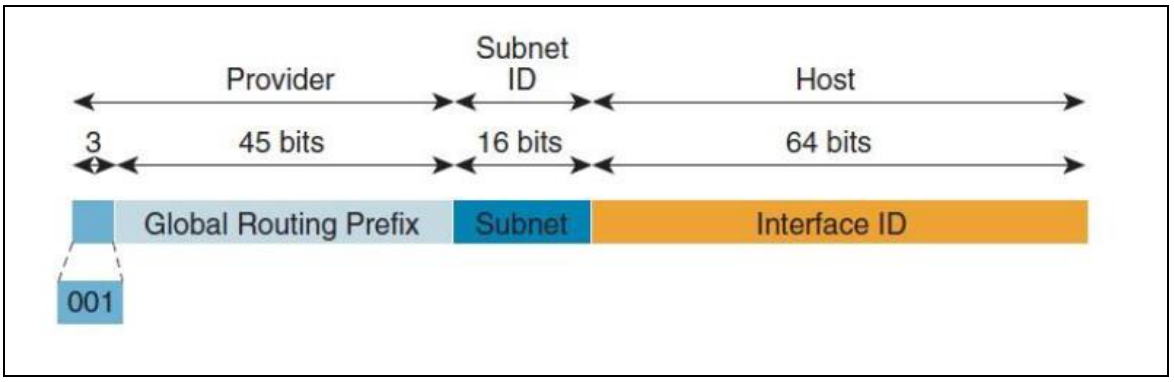


Figura 13 Estrutura de endereço IPv6 *Global*.
Fonte: JAIN e SHARMA (2010).

O endereço *global* pode ser autoconfigurado em *hosts* e interfaces de roteadores, utilizando o protocolo *ND (Neighbor Discovery*[30], visto com mais detalhes logo adiante). Nesse caso, o *host* concatena o prefixo informado pelo roteador (64 bits iniciais) e utiliza o mesmo método de expansão para obter o

[29] Registro de Endereçamento da Internet para América Latina e Caribe.
[30] Pode ser traduzido literalmente por “descoberta de vizinhos”.

EUI-64. Outra opção é a configuração manual (apenas do prefixo, calculando-se o EUI-64 para os bits finais), ou o auxílio de um servidor de DHCP(v6).

O escopo dos endereços pode ser representado da seguinte forma:

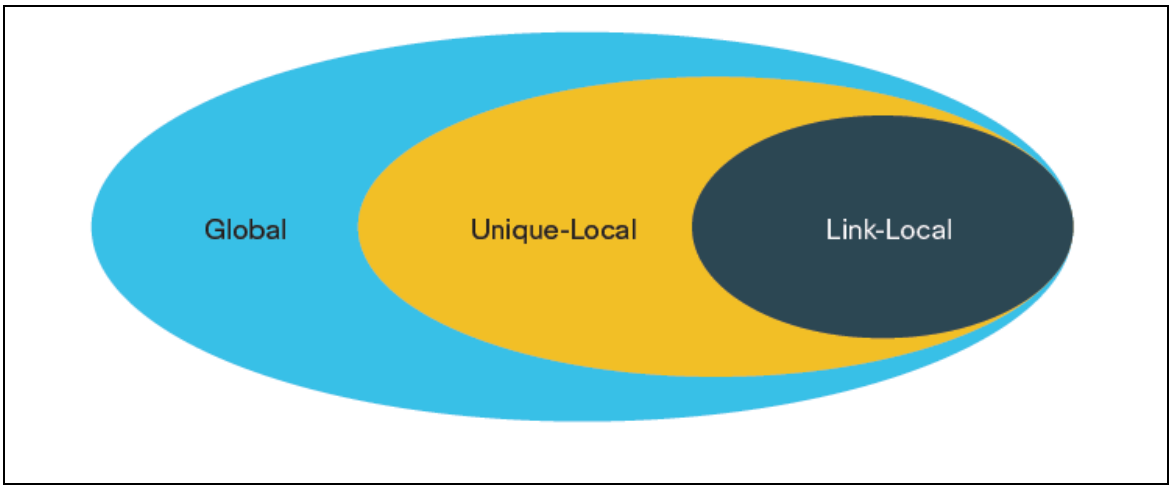


Figura 14. Escopo de endereços *Unicast*.
Fonte: CISCO (2012).

Endereços *unicast* não especificados, ou seja, quando o *host* não tem um IPv6 válido, são representados pelo bit "0" em todas as posições, ou simplesmente por "::/128". O endereço de *loopback* "::1/128" substitui o antecessor "127.0.0.1".

Endereços de *multicast* são utilizados para enviar a mesma mensagem para um grupo específico de interfaces. Cada uma delas já tem um IP atribuído de acordo com seu tipo, sempre com o prefixo "FF00/8".

Tabela 3. Escopo de endereços *Multicast*.
Fonte: RAZA, K. e ASADULLAH, S. (2012).

Address	Scope	Meaning
FF01::1	Node-Local	All Nodes
FF02::1	Link-Local	All Nodes
FF01::2	Node-Local	All Routers
FF02::2	Link-Local	All Routers
FF05::2	Site-Local	All Routers

A Tabela 3 mostra a abrangência de cada um deles. *Link-Local tem* escopo similar ao do endereço de *unicast link-local; Node-Local* se compara ao escopo do endereço *unique local; Site-Local* abrange todos os roteadores dentro da organização. Fazem parte de *All Nodes:* computadores, *switches, access points*, etc.

Anycast é o terceiro tipo de endereço definido para IPv6. Permite que servidores com uma mesma função (DHCP ou DNS, por exemplo) utilizem o mesmo endereço de IP (JAIN, SHARMA, 2010). Dessa forma, o *host* que origina o tráfego estabelece comunicação com apenas um deles, considerado ser o mais próximo (definido por algoritmos de roteamento). Caso esse servidor esteja indisponível, outro assume o lugar de "mais próximo", e evita que o serviço seja interrompido.

O campo "*subnet*" aparece nas figuras acima dedicando 16 bits para isso, pois o prefixo atribuído a uma companhia tem uma máscara padrão /48 para organizações de grande porte e /56 para as de médio porte (ODOM, 2010). No primeiro caso, temos 2^{16} endereços de subrede (65536), e 2^{8} para o segundo (256). No IPv6, não há preocupações em se reservar o endereço da subrede ou o endereço de *broadcast* como no IPv4. A organização pode optar em não dividir os endereços em subredes, resultando num total de 80 bits para *hosts* ($1{,}2 \times 10^{24}$), mas isso acarreta limitações para autoconfiguração de endereços, que se baseia numa porção de endereços de *host* com 64 bits.

Outra diferença é a substituição do ARP pelo protocolo ND (RFC 2461), parte do ICMPv6. O *host* sendo inicializado ou juntando-se à rede envia mensagens solicitando informações sobre o prefixo local. Além disso, usa mensagens para descobrir o endereço link-local dos dispositivos adjacentes. Os roteadores, por sua vez, informam os demais dispositvivos de sua presença na rede e proveem as informações solicitadas.

Finalmente, o novo cabeçalho IPv6 sofreu várias alterações em relação ao utilizado pela versão 4: alguns campos foram excluídos, outros tiveram seu nome e posição alterados e outros foram adicionados.

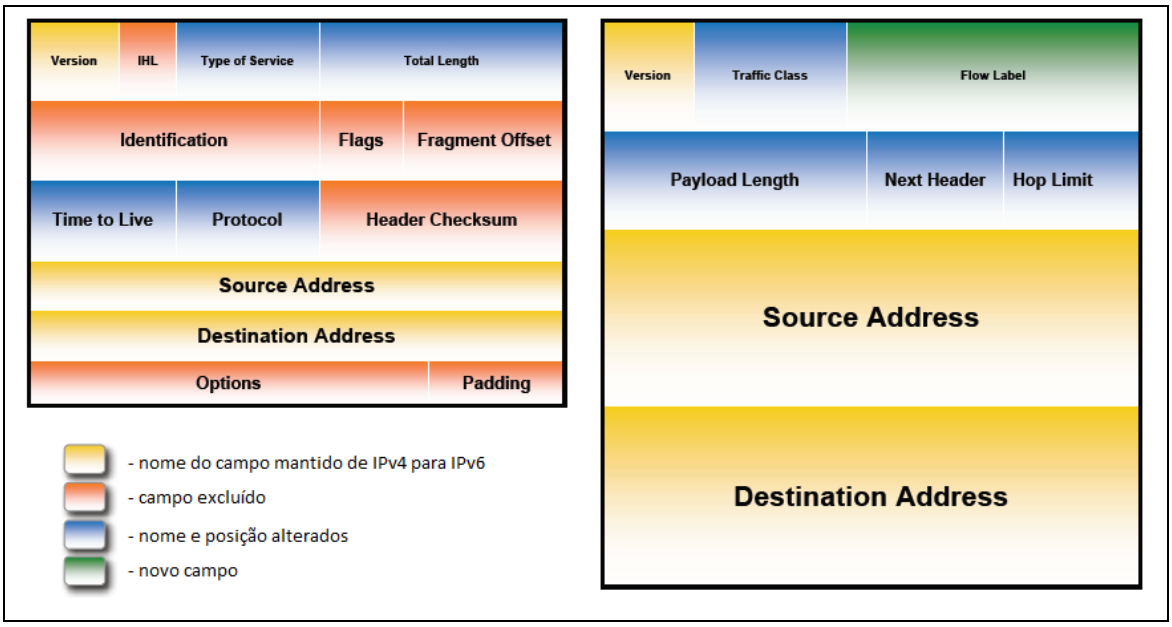


Figura 15. Comparação entre cabeçalho IPv4 e IPv6.
Fonte: CISCO (2012).

O cabeçalho IPv4 pode variar em tamanho de 20 bytes até 80 bytes. Para a nova versão, foi fixado em 40 bytes, tornando desnecessário o campo *IHL (Internet Header Length*, ou Tamanho do Cabeçalho de Internet). As informações contidas nos campos *Identification* (Identificação), *Flags* (marcação), *Fragment Offset* (Deslocamento de Fragmento), *Options/Padding* (Opções e Complementos) são transmitidas dentro de cabeçalhos de extensão. *Header Checksum* (Soma de Verificação) foi extinto, levando em conta que os protocolos de camadas superiores realizam validações da quantidade de *bytes* (IPV6.BR, 2012).

Type of Service (Tipo de Serviço) passou a se chamar *Class of Traffic* (Classe de Tráfego), usado para QoS, em conjunto com o novo campo *Flow Label* (Identificador de Fluxo). Como o cabeçalho tem tamanho fixo, Total *Length* (Tamanho Total) considera apenas o *Payload Length* (Tamanho dos Dados). Na versão 6, *Time to Live* (Tempo de Vida) passa a ser chamado de *Hop Limit* (Limite de Encaminhamento). O campo *Protocol* aparece como *Next Header* (Próximo Cabeçalho), indicando o que está encapsulado pelo cabeçalho IP.

Os demais campos continuam com a mesma denominação, mas tem tamanho diferente em relação à versão 4. Todas essas modificações foram feitas com o intuito de diminuir o tamanho e o processamento destinado ao cabeçalho ("*overheading*"). Como resultado, não existe a interoperabilidade entre os cabeçalhos das duas versões, exigindo que técnicas auxiliares sejam utilizadas para que redes IPv6 se comuniquem com redes operando com IPv4.

4.2- Cenários Possíveis

Backer (2011) descreve na RFC 6144 que será inevitável que os dois protocolos coexistam durante um período de transição, e aponta os cenários possíveis, com foco nos quais se aplicam soluções de tradução. A intenção, segundo ele, era que a maioria dos *hosts* utilizasse IPv6 antes do esgotamento de endereços IPv4, mas sua previsão se confirmou, já que o esgotamento ocorreu antes que a transição alcançasse um estágio avançado.

- Cenário 1: *rede IPv6 para IPv4 na Internet:* organização com uma rede totalmente IPv6 que necessita acessar conteúdo na Internet via IPv4.

Figura 16. Cenário 1.
Fonte: IPV6.BR (2012)[31].

- Cenário 2: *IPv4 na Internet para rede IPv6:* similar ao anterior, mas com a comunicação partindo de um IPv4 na Internet acessando recursos na rede IPv6 nativa.

[31] Figuras de 16 a XX: Disponíveis em: <http://ipv6.br/entenda/transicao/#transicao-coex>. Acesso em 20 mai 2013.

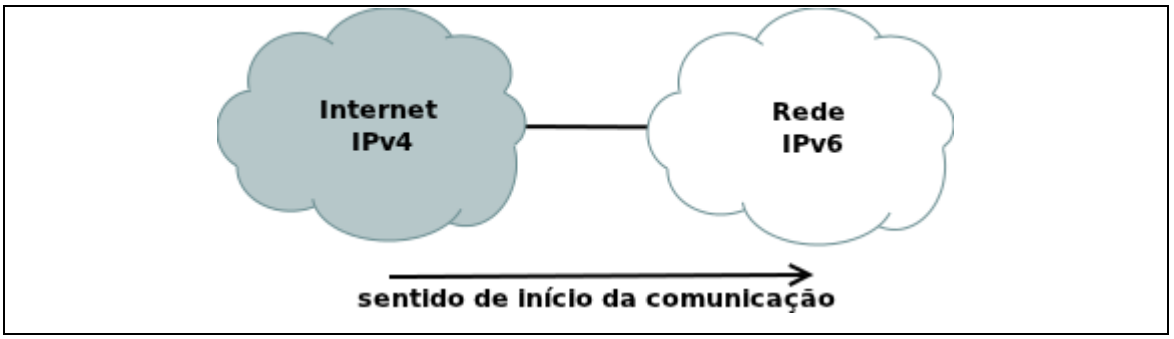


Figura 17. Cenário 2.
Fonte: IPV6.BR (2012).

- Cenário 3: *IPv6 na Internet para rede IPv4:* esse cenário se tornará comum à medida que mais *hosts* utilizarem IPv6 e estiverem acessando redes legadas IPv4.

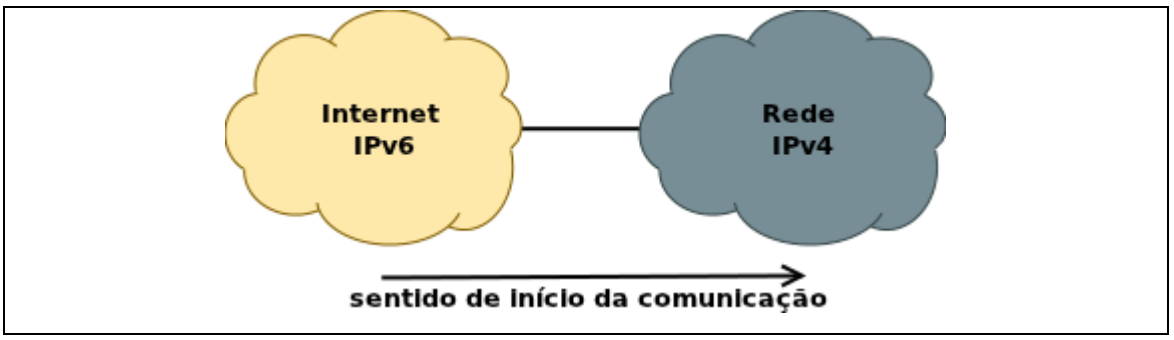


Figura 18. Cenário 3.
Fonte: IPV6.BR (2012).

- Cenário 4*: rede IPv4 para IPv6 na Internet:* situação que deve ser vista mais frequentemente nos últimos estágios da transição, onde a maior parte dos *hosts* utilizará IPv6.

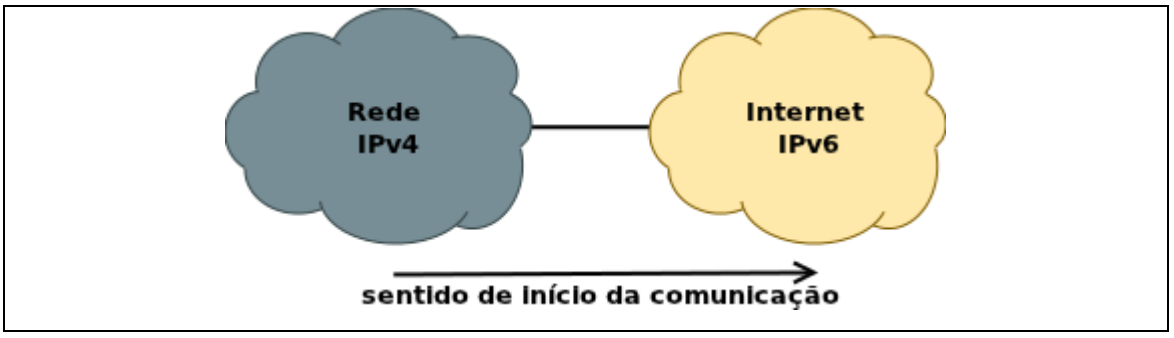


Figura 19. Cenário 4.
Fonte: IPV6.BR (2012).

- Cenário 5*: rede IPv6 para rede IPv4:* deve ocorrer dentro de uma mesma organização, e tem soluções similares ao Cenário 1.

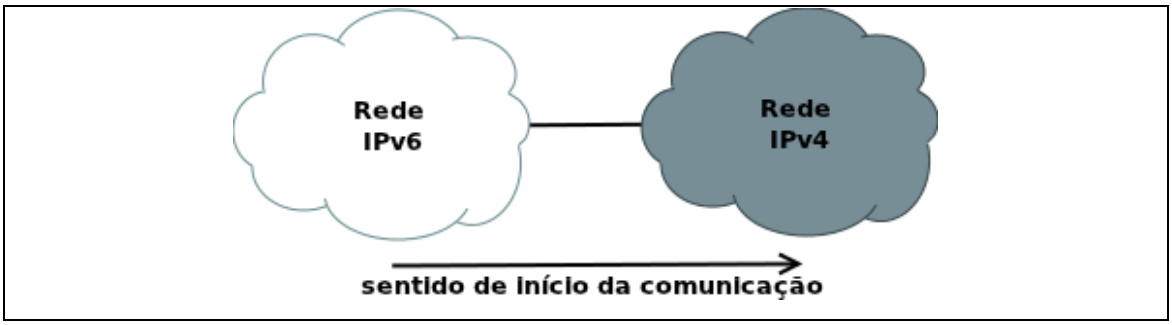


Figura 20. Cenário 5.
Fonte: IPV6.BR (2012).

- Cenário 6: *rede IPv4 para rede IPv6:* também diz respeito a redes em uma mesma organização, e tem soluções similares ao Cenário 2.

Figura 21. Cenário 6.
Fonte: IPV6.BR (2012).

- Cenário 7: *IPv6 na Internet para IPv4 na Internet:* considerado o mais complexo, já que nenhuma técnica de tradução seria viável devido à grande diferença na quantidade de endereços de cada versão.

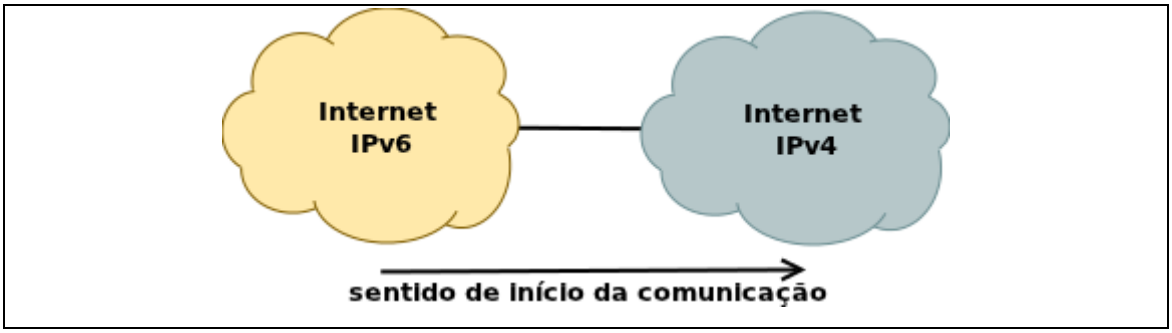


Figura 22. Cenário 7.
Fonte: IPV6.BR (2012).

- Cenário 8: *IPv4 na Internet para IPv6 na Internet:* similar ao anterior.

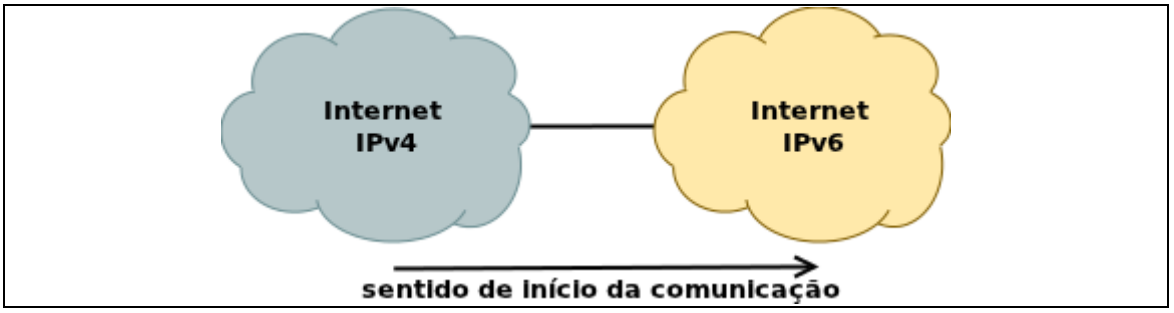


Figura 23. Cenário 8.
Fonte: IPV6.BR (2012).

- Cenário 9: *redes IPv6 utilizando transporte IPv4:* dois extremos utilizando IPv6 com uma rede IPv4 completando a conexão entre eles.

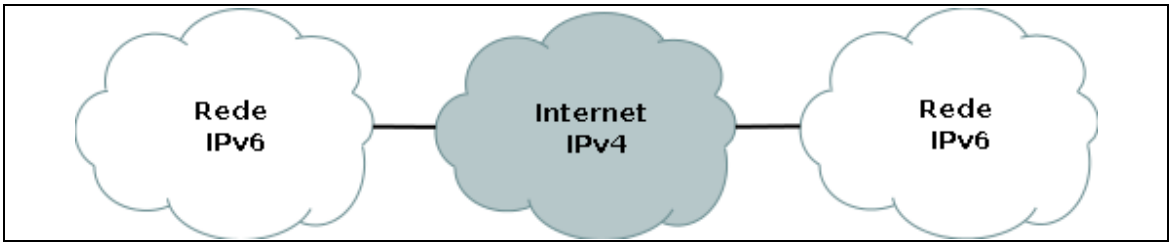


Figura 24. Cenário 9.
Fonte: IPV6.BR (2012).

- Cenário 10: *redes IPv4 utilizando transporte IPv6:* dois extremos utilizando IPv4 com uma rede IPv4 completando a conexão entre eles.

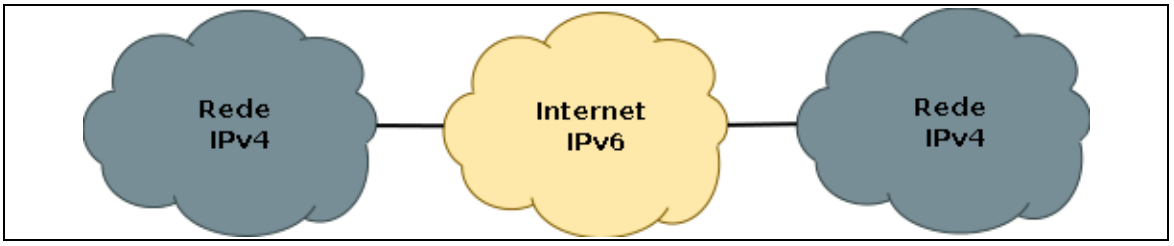


Figura 25. Cenário 10.
Fonte: IPV6.BR (2012).

Cada um deles apresenta peculiaridades que restringem o uso de determinadas técnicas e encorajam outras. Cada caso deve ser analisado separadamente, já que uma única solução não resolve todos os cenários.

4.3- Métodos de Coexistência

Como dito no capítulo anterior, diferentes cenários exigem soluções diferentes. Inúmeros métodos foram propostos, sendo que alguns deles foram rejeitados devido a sua complexidade, ou mesmo ineficiência. Ainda assim, vários estão sendo utilizados e serão úteis durante o período de transição. Quanto à funcionalidade, essas técnicas podem ser classificadas em *Dual Stack, Tunneling* e *Translation*[32].

4.3.1- Pilha Dupla

Pilha Dupla (*Dual Stack)* refere-se à utilização de ambas as pilhas dos protocolos IPv4 e IPv6 operando simultaneamente em um equipamento. Nesse caso, para se comunicar com outro nó configurado apenas com a pilha IPv4, o dispositivo com *dual stack* utiliza pacotes IPv4. Caso a comunicação seja com um nó IPv6, o mesmo utiliza essa versão (NORDMARK; GILLIGAN, 2005).

Quando ambos os sistemas envolvidos na comunicação operam com *dual stack,* a preferência será dada ao IPv6. Um algoritmo chamado *Happy Eyeballs*[33] se encarregará disso. Equipamentos Cisco possuem suporte nativo à pilha dupla (é necessário habilitar características de IPv6 via configuração), assim como o sistemas operacionais da Microsoft (*Windows 7* em diante) e *MAC OS da* Apple Computers.

Essa solução é a mais simples, embora tenha algumas restrições. Por exemplo, configurações de Firewall devem considerar as duas versões, pois não são replicadas automaticamente entre elas. Alguns protocolos de roteamento, como o OSPFv2, não suportam IPv6; portanto deve-se migrar para

[32] Pilha Dupla, Tunelamento e Tradução, consecutivamente.
[33] Pode-se entender a expressão "*happy eyeballs*" como "uma expressão de alegria nos olhos".

um protocolo que tenha esse serviço ou utilizar o OSPFv3, por exemplo, paralelamente.

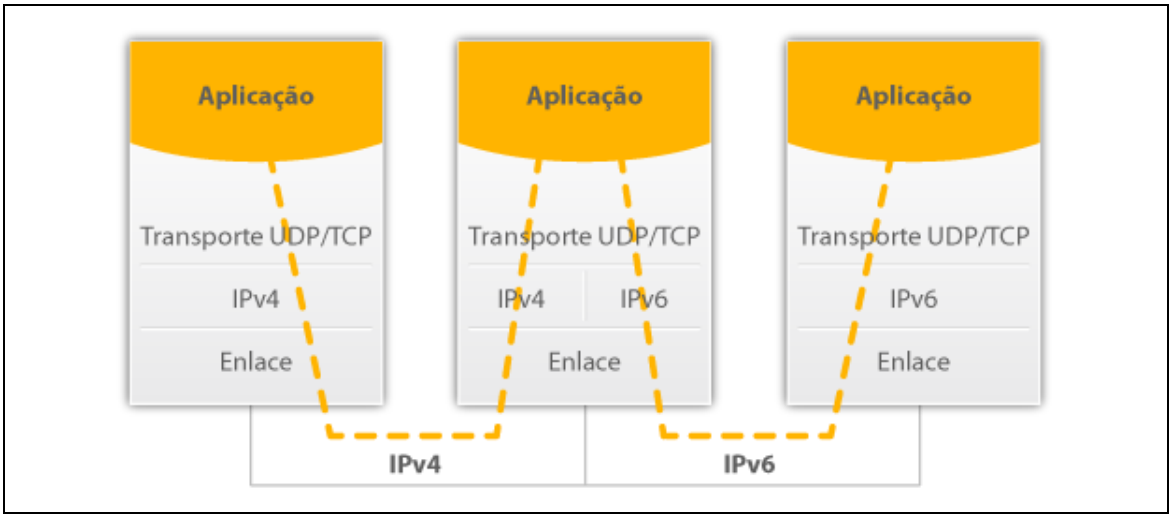


Figura 26. *Dual Stack*.
Fonte: CICILEO (2013). Disponível em <http://portalipv6.lacnic.net/pt-br/mecanismos-de-transi-o>. Acesso em 20 mai 2013.

Apesar de ser o método preferencial de transição, a utilização desse modelo é inviável em alguns casos. Se uma nova organização disponibiliza conteúdo na Internet, mas não pode adquirir um endereço IPv4 válido devido ao esgotamento, sua rede não suportará *dual stack*. Outro problema é que alguns equipamentos em ambientes de produção não também não operam com pilha dupla, e alguns deles não podem ser facilmente substituídos, ou por motivos financeiros ou por implicações no desenho da rede. Em tais situações, pode-se utilizar um dos métodos seguintes.

4.3.2- Tunelamento

Tunneling, ou simplesmente tunelamento, consiste na técnica de encapsular um pacote IPv6 dentro de um pacote IPv4. Portanto, os equipamentos na rede de transporte operando em IPv4 encaminham o pacote, ignorando o fato de que o campo onde são transmitidos os dados contém, na verdade, um pacote IPv6 (ODOM, 2010). Na outra extremidade da

comunicação, um dispositivo deve fazer o processo inverso, ou seja, retirar o cabeçalho IPv4 para que o destinatário final receba o pacote IPv6. Esse modelo é usado para a comunicação entre dois *hosts* IPv6 que precisam se comunicar através de uma rede IPv4. O mesmo pode ser feito quando existirem duas redes IPv4 que necessitem trafegar por uma rede IPv6, encapsulando pacotes v4 dentro de pacotes v6. Tal cenário é improvável no estágio atual de implantação do IPv6.

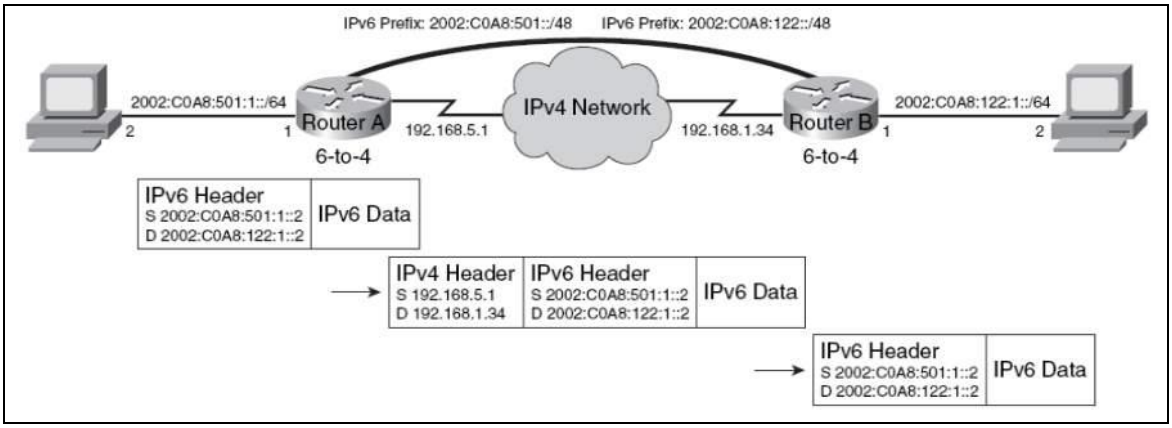


Figura 27. Encapsulamento *6to4.*
Fonte: BENTOW (2009). Disponível em <http://www.bentow.com.br/category/tunneling/>. Acesso em: 21 mai 2013.

Existem duas classificações para túneis: estáticos e dinâmicos. Os primeiros são configurados manualmente, com o intuito de formar um circuito ponto a ponto. Adéquam-se a projetos que necessitem de túneis permanentes. Túneis dinâmicos são conexões do tipo multiponto apropriadas para quando o tráfego é esporádico. Exemplos de túneis estáticos e dinâmicos são abordados na próxima seção deste capítulo.

4.3.2.1- Túneis estáticos

Existem alguns tipos de túneis estáticos, entre os quais os principais são o *6over4* e o Túnel GRE (*Generic Routing Encapsulating*[34]). Esses, também chamados de túneis manualmente configurados, provêm conexão permanente

[34] Encapsulamento de roteamento genérico.

para duas redes IPv6 que percorram um caminho onde existe algum dispositivo que não esteja apto a gerenciar tráfego desse protocolo.

O encapsulamento segue as especificações presentes na RFC 4213, que diz que a entrada do túnel cria um encapsulamento IPv4, e determina via configuração os endereços de origem e de destino (NORDMARK; GILLIGAN, 2005). Os mesmos devem ser refletidos na configuração no outro extremo do túnel, ou seja, o endereço de origem de um dos lados deve ser configurado como endereço de destino no outro, e vice-versa.

Quando o pacote atravessa o túnel, o dispositivo que recebe o pacote precisa saber de alguma forma que o *payload*[35] do pacote IPv4 é, de fato, um pacote IPv6. Para tanto, o campo "Protocolo", que informa o tipo de conteúdo sendo carregado pelo pacote, de conter o número "41" (29_{16}). Essa técnica de encapsulamento é chamada de *6in4*. No momento que o dispositivo recebe o pacote e percebe o esse código, desencapsula o mesmo e trata o *payload* como um pacote IPv6, aplicando as regras de roteamento.

A única diferença de conceito entre o *6over4* e o túnel GRE é que o segundo tipo pode carregar outros tipos de protocolos. Isso se dá através de um campo de protocolo adicional no cabeçalho IPv4 (ODOM, 2010), que informa qual o protocolo contido. Embora esses túneis sejam usados para transportar IPv6, o túnel GRE provê flexibilidade nesse sentido.

4.3.2.2- Túneis Dinâmicos

Os túneis dinâmicos, assim como os túneis estáticos, encapsulam pacotes IPv6 dentro de pacotes v4. Entretanto, formam túneis multiponto, ou seja, não são atrelados a um único dispositivo na outra extremidade. Do ponto de vista lógico, funcionam como uma LAN. Do ponto de vista prático, não há nenhuma vantagem em relação aos túneis estáticos.

[35] Campo do cabeçalho que contém os dados transmitidos.

A grande diferença é a forma como o roteador enviando o pacote determina o caminho que o mesmo vai percorrer (ODOM, 2010). Após receber o pacote em sua interface LAN, o roteador entende que tem que enviar o pacote pela interface de entrada do túnel multiponto. O endereço IPv4 do outro extremo do túnel é derivado a partir do endereço v6 de destino. O pacote IPv6 é então encapsulado com um cabeçalho v4, com o endereço de origem de sua própria interface, e o de destino com o IPv4 do roteador que completa o túnel.

Túneis automáticos **6to4** seguem o raciocínio descrito acima, e funcionam da seguinte forma: o prefixo IPv6 é escolhido, podendo ser um endereço global ou o número reservado (2002::/16). O endereços IPv4 de origem dos túneis são embutidos nos quartetos 3 e 4, definindo os primeiros 48 bits do endereço. Os próximos 16 bits definem as subredes, e cada *host* recebe os últimos 64 bits para formar seu endereço IPv6. Por exemplo, se os endereços IPv4 *10.100.100.11, 10.100.100.12* e *10.100.100.13* serão usados, os prefixos dos endereços IPv6 derivados serão, respectivamente, *2002:A64:640B::/48, 2002:A64:640C::/48* e *2002:A64:640D::/48*.

Uma rota estática deve ser configurada no roteador, para que todos os pacotes com destino 2002::/16 sejam encaminhados para a interface túnel. Como a interface tem o tipo 6to4 também previamente configurado, o roteador sabe que tem que adicionar um cabeçalho v4, usando o IPv4 (embutido no endereço v6) como destino. Se os *hosts* têm endereços globais ao invés de utilizar o prefixo reservado 2002::/16, algumas rotas estáticas devem ser adicionadas. A rota para um determinado *host* deve apontar para o túnel do roteador como interface de saída, e o próximo nó deve ser o endereço IPv6 do túnel do roteador remoto, (que ainda terá o prefixo 2002::/16).

As diferenças entre os túneis **ISATAP** (*Intra-Site Automatic Tunnel Addressing Protocol*[36]) e 6to4 são bem pontuais, por se tratar também de um túnel dinâmico, ou automático, por assim dizer, a começar pelo processo de como o endereço IPv4 é embutido no endereço v6. Nesse caso, definido um prefixo global de 64 bits (não se utiliza o prefixo reservado 2002::/16, usado

[36] Protocolo de Endereçamento de Túnel Automático de Intranet.

pelo 6to4) comum a todas as interfaces de LAN e de túnel, o roteador utiliza o IPv4 configurado na interface de saída e insere o mesmo nos últimos dois quartetos do IPv6. Dessa maneira, temos os primeiros 64 bits e os últimos 32. Os demais bits (quartetos 5 e 6) são preenchidos com o valor *0000:5EFE*. Um detalhe é que todas as interfaces de túnel devem estar na mesma subrede, diferentemente do modelo 6to4.

Outro fator de diferenciação é que o ISATAP pode ser usado para a comunicação entre dois *hosts* IPv6 em uma intranet IPv4. Por padrão, os sistemas operacionais Windows Server (a partir do 2003) e XP, da Microsoft, configuram automaticamente um endereço no padrão do túnel para o *host* assim que a pilha IPv6 é iniciada. Para tanto, é usado o prefixo da interface link-local (FE80) concatenado aos quartetos 5 e 6 com valor 0:5EFE. O IPv4 desses *hosts* completa o endereço de túnel ISATAP (MICROSOFT, 2013). Exemplificando, um *host* com IPv4 *10.5.2.14* passa a ter um endereço *FE80::0:5EFE:A05:2E*. Como mencionado, essa comunicação tem escopo local, pois endereços do tipo "*FE80*" não são encaminhados pelos roteadores.

Assim como os demais túneis dinâmicos, túneis **Teredo** também têm um endereço IPv4 embutido para formar o endereço IPv6. O prefixo reservado pela IANA, *2001:0000:/32*, é concatenado ao endereço IPv4 do servidor Teredo, formando os primeiros 64 bits. Os próximos 16 bits são *flags* de controle, seguidos pelo número da porta UDP invertida. Por último, o endereço IPv4 do *host* Teredo, também invertido através de uma operação XOR com o valor "*FFFFFFFF*" (HUITEMA, 2006).

Também permitem conexão entre duas estações finais de trabalho, e deve ser usado para permitir a comunicação entre redes IPv6 interligadas por dispositivos IPv4 como um último recurso (MICROSOFT, 2013), só em casos em que 6to4 e ISATAP não forem viáveis. Geralmente usa-se Teredo quando o pacote tem que passar por NAT ou Firewalls. Isso porque túneis 6to4 e ISATAP utilizam o campo "*protocol*" do cabeçalho IPv4 para informar que o pacote carrega um pacote IPv6 em seu *payload*, sinalizado pelo valor "41". Entretanto, a maioria de dispositivos realizando NAT e firewalls apenas encaminham

segmentos do tipo TCP ou UPD, esperando, portanto, que o valor do campo "*protocol*" seja "6" ou "17", consecutivamente..

Para "burlar" os sistemas de NAT e firewall, os túneis Teredo encapsulam o pacote v6 dentro de um cabeçalho UDP, e então dentro do v4. Segundo Zucchi (2011), esse nome vem de um molusco marisco comum na Ilha de Marajó, que perfura o casco de embarcações de madeira, análogo ao comportamento dos pacotes passando através de NAT e firewalls.

Os túneis são muito úteis em cenários como os descritos acima, mas, segundo Backer (2011), existem algumas razões para não se utilizar túneis. Basicamente, os usuários não fazem uso da infraestrutura IPv4, já que os túneis provêm apenas serviço de transporte, e não permite que usuários da versão 6 se comuniquem com os usuários v4. Tendo vista essas restrições, podem ser usadas, alternativamente, traduções de endereços, tópico do próximo capítulo.

4.3.3- Tradução

A primeira solução para permitir que *hosts* IPv4 se comunicassem com *hosts* IPv6 foi o *Network Address Translation - Protocol Translation* (NAT-PT), uma tradução de endereços similar ao NAT44 (usado para traduzir endereços IPv4 privados para endereços IPv4 públicos), que permite uma rede IPv6 comunicar-se com um *host* (geralmente um servidor) IPv4 na Internet. Baseia-se no mapeamento de endereços v4 para os endereços v6 dos *hosts* da rede, numa relação de 1:1. Foi considerado obsoleto pela RFC 4966 devido a problemas graves, segundo Aoun e Davis (1997). Como substituta, foi apresentada a técnica NAT64, para prover comunicação entre uma rede IPv6 e *hosts* IPv4 na Internet. Pode ser classificada em "*Stateless*", como a antecessora NAT-PT, e "*Stateful*".

4.3.3.1- Tradução de Endereços de Rede *64 (NAT64)*

A NAT64 ***Stateless*** recebe esse nome porque não precisa manter nenhuma tabela com informações sobre determinada comunicação. A RFC 6145 (LI, 2011) descreve seu funcionamento: O tráfego entre o sistema IPv6 e o sistema IPv4 se estabelece através de tradutor (um roteador, por exemplo), que traduz o cabeçalho de IPv6 para IPv4 (ou vice-versa)[37]. As alterações mais significativas se dão no campo do endereço. Um prefixo IPv6, chamado de *Network-Specific Prefix*[38] (NSP), é escolhido pelo administrador do sistema (convenciona-se o uso do valor 64:ff9b::/96 (BAO, et al, 2010)). Usando esse prefixo, basta concatená-lo aos 32 bits do IPv4, que pode ser representado no formato decimal (ex: 64:ff9b::192.0.2.33).

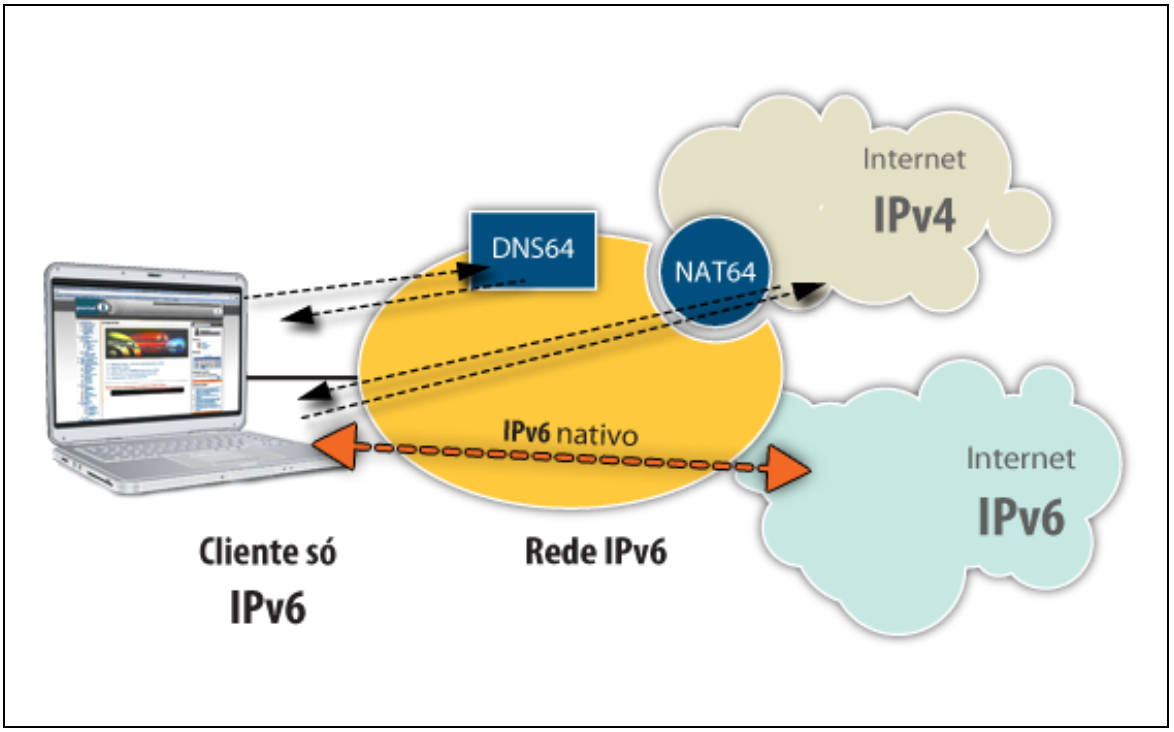


Figura 28. NAT64.
Fonte: CICILEO (2013). Disponível em <http://portalipv6.lacnic.net/pt-br/mecanismos-de-transi-o>. Acesso em 20 mai 2013.

[37] Devido à diferença no tamanho dos mesmos, algumas questões sobre fragmentação devem ser levadas em consideração. Essas não serão abordadas nesse trabalho.
[38] Prefixo de Rede Específica.

Nesse modo, um intervalo específico de endereços v6 representarão dispositivos IPv4 (v4 convertidos para v6), e os dispositivos IPv6 têm um endereço que pode ser traduzido e mapeado para endereços IPv4 válidos através de um algoritmo. Em ambos os casos, os endereços v4 podem ser extraídos ou embutidos no formato v6, tornando desnecessária uma tabela de estado.

É fundamental que o tradutor funcione paralelamente a um servidor de *Domain Name System64*[39] (DNS64). O *host* v6 que deseja acessar a Internet faz uma requisição do tipo "AAAA". No caso, o IP do servidor de destino será IPv4, com formato "A". O DNS64 se encarrega de traduzir o endereço IPv4 utilizando o prefixo determinado (64:ff9b::, por exemplo). O campo do endereço de destino passa a ter o formato de 128 bits, e é enviado para o tradutor. Nesse momento os endereços v6 (tanto da origem quanto do destino) são substituídos com o uso do algoritmo, e modificados para a versão 4. Quando o servidor da Internet responde, o processo inverso ocorre, com o tradutor usando o algoritmo para compor o endereço v6 e traduzir o cabeçalho, dessa vez de IPv4 para IPv6.

No modo ***stateful***, o processo é bem parecido, mas o tradutor utiliza somente um endereço IPv4 válido para o tráfego que sai em direção à Internet. Para tanto, faz uso de portas de rede TCP, assim como o NAT44. Para que o trafego de retorno encontre o *host* específico que fez aquela requisição (todos retornam com o endereço mesmo IPv4 no campo de destino), é necessário manter uma tabela de estado, contendo detalhes sobre a conexão (endereços de porta). Os detalhes de seu funcionamento são explicados por Bagnulo (2011) na RFC 6146.

[39] Serviço que traduz nomes para endereços IP. O número 64 se refere à capacidade de atender requisições também no formato v6.

Estudo de Caso

Foram demonstradas diversas características de funcionamento do protocolo IPv6 em comparação à sua versão anterior, e abordar as diversas técnicas de transição disponíveis para atender os diversos cenários existentes. Agora, apresenta-se uma demonstração prática de utilização de duas dessas soluções através de uma simulação criada com o auxílio do GNS3[40] de uma rede operando com as duas versões.

No primeiro modelo, temos os cenários mais prováveis nos primeiros estágios da transição: uma rede de uma organização que implantou a pilha IPv6 em seus dispositivos e precisa comunicar-se com redes ou *hosts* IPv4 e IPv6 na Internet. O problema foi resolvido com o uso de pilha dupla em todos os dispositivos, ou seja, adicionando-se endereços IPv6 aos dispositivos que antes operavam somente com IPv4. Essa solução é a mais recomendada, e pode ser utilizada nos cenários de 1 a 8 apresentados no capítulo anterior.

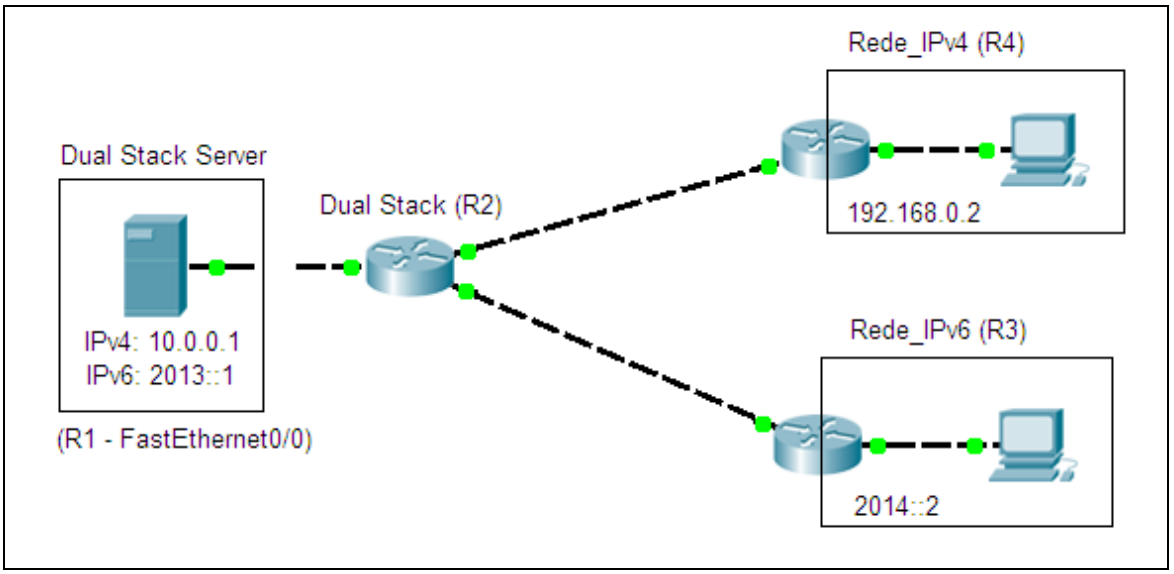


Figura 29. Rede utilizando Pilha Dupla como solução.
Fonte: Autor

Temos um servidor (*Dual Stack Server*) representado por R1, com dois endereços, um v4 e outro v6. Assim, quando a comunicação se der entre o

[40] *Software* utilizado para simulação de ambientes de rede.

servidor e a rede IPv4, o mesmo utilizará o endereço **10.0.0.1**, e o endereço **2013::1** para trocar informações com a rede IPv6 (R3). A Figura 30 mostra a resposta de pacotes ICMP (*"pings"*) a requisições enviadas a partir da rede IPv4 utilizando o endereço v4 e a resposta de pacotes ICMPv6 (*"pings" v6*) a requisições originadas na rede IPv6.

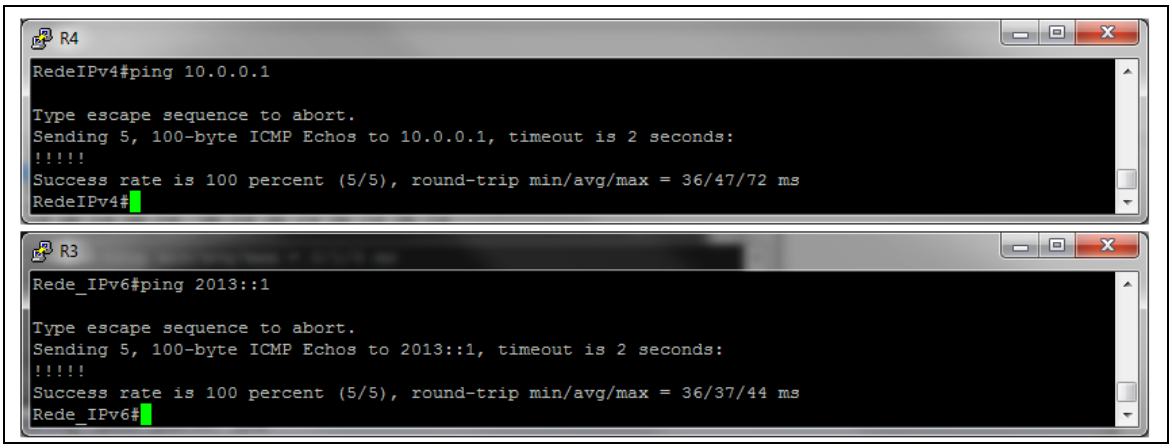


Figura 30. Pacotes do tipo ICMP (*"ping"*) respondidos **pelo** servidor (R1).
Fonte: Autor.

Adiante, o sentido do tráfego é o inverso, com pacotes do tipo *"echo request"* disparados pelo servidor (R1) em direção às duas redes (v4 e v6).

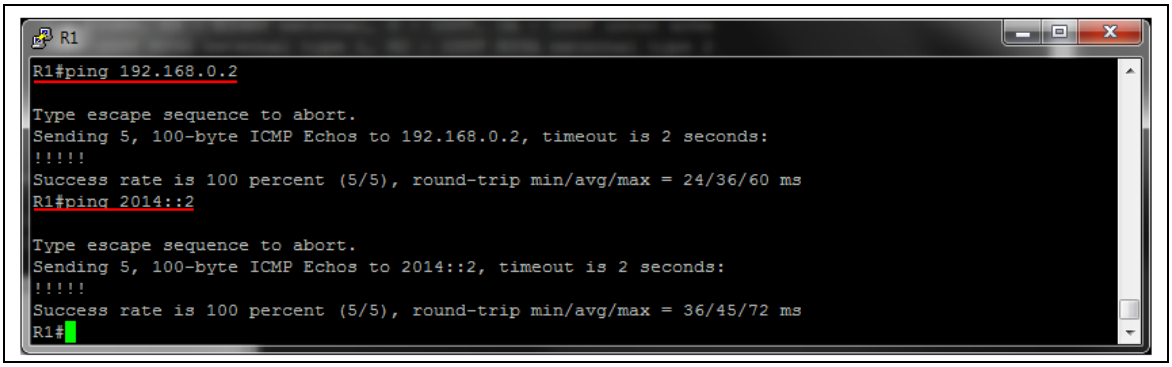


Figura 31. Pacotes do tipo ICMP ("*ping*") respondidos **ao** servidor (R1).
Fonte: Autor.

A seguir, a captura de pacotes mostra claramente que os pacotes originados em um *host* que é parte de uma rede IPv4 (***192.168.0.2***, nesse caso) são respondidos pelo endereço IPv4 (***10.0.0.1***) do sistema que opera com pilha dupla (Figura 32(a)). Pacotes de uma rede IPv6 (***2014::2***) com destino à rede operando com pilha dupla são respondidos pelo endereço IPv6 (***2013::1***) desse sistema (Figura32(b)).

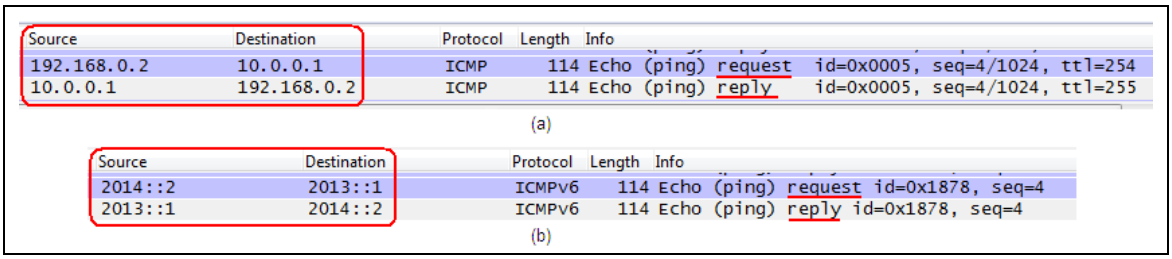


Figura 32. Captura de pacotes ICMP **destinados** ao dispositivo com pilha dupla.
Fonte: Autor.

Quando o pacote parte do sistema IPv4/IPv6, o mesmo faz a escolha do endereço de origem de acordo com o endereço de destino. Em outras palavras, caso o pacote seja destinado à rede IPv4 (no caso, ***192.168.0.2***), o endereço de origem será v4 (***10.0.0.1***). Se o destino for um endereço do tipo IPv6 (***2014::2***), o servidor pilha dupla utiliza um cabeçalho IPv6 com origem igual ao valor do endereço v6 configurado em sua interface (***2013::1***) (Figura 33(b)).

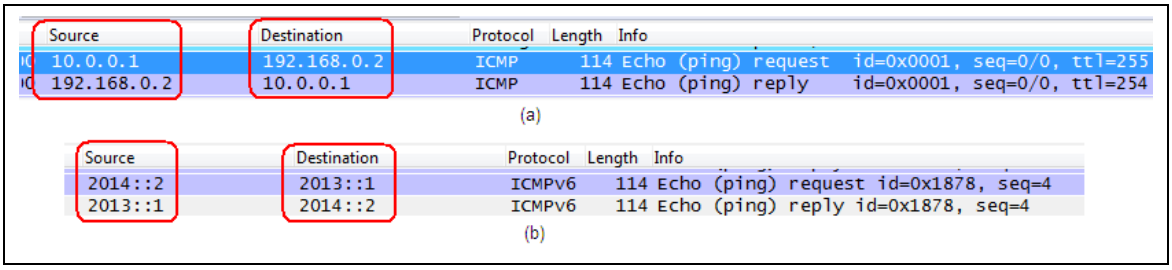


Figura 33. Captura de pacotes ICMP **originados** no dispositivo com pilha dupla.
Fonte: Autor.

Neste segundo caso temos duas redes IPv6 de uma mesma empresa que devem comunicar-se, mas o tráfego necessita atravessar dispositivos sem capacidade de gerenciar tráfego v6, como no cenário 9 (p.41). Para isso, um túnel manualmente configurado do tipo *6over4*, também chamado de *IPv6IP*, será utilizado. A topologia está representada logicamente como na Figura 34.

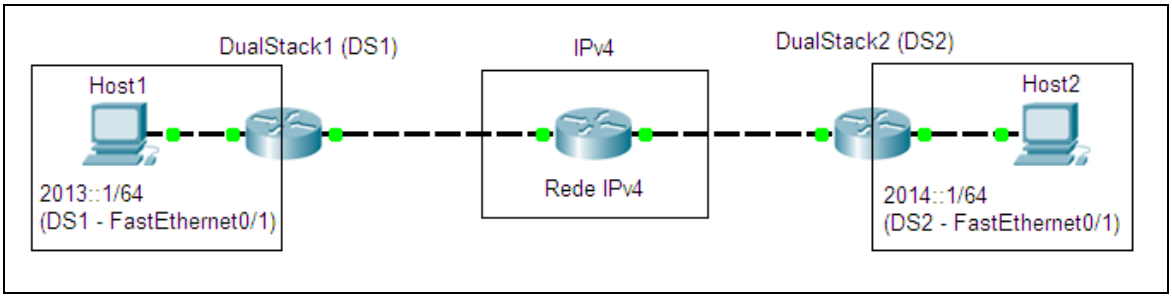


Figura 34. Topologia para aplicação da técnica de Tunelamento.
Fonte: Autor.

Devido a algumas restrições de licença de *software*, a simulação foi feita utilizando apenas três roteadores: *Dual Stack 1* (**DS1**), *Dual Stack 2* (**DS2**), e **IPv4** como intermediário entre os dois, encaminhando apenas pacotes v4. Os *hosts* são substituídos por interfaces dos roteadores. As interfaces que simulam os hosts recebem *endereços IPv6 globais* configurados manualmente (**2013::1**; **2014::1**). Nota-se um segundo endereço, atribuído automaticamente (gerado a partir do *MAC-Address* da interface). O mesmo ocorre com a interface túnel em ambos os extremos (Figura 36).

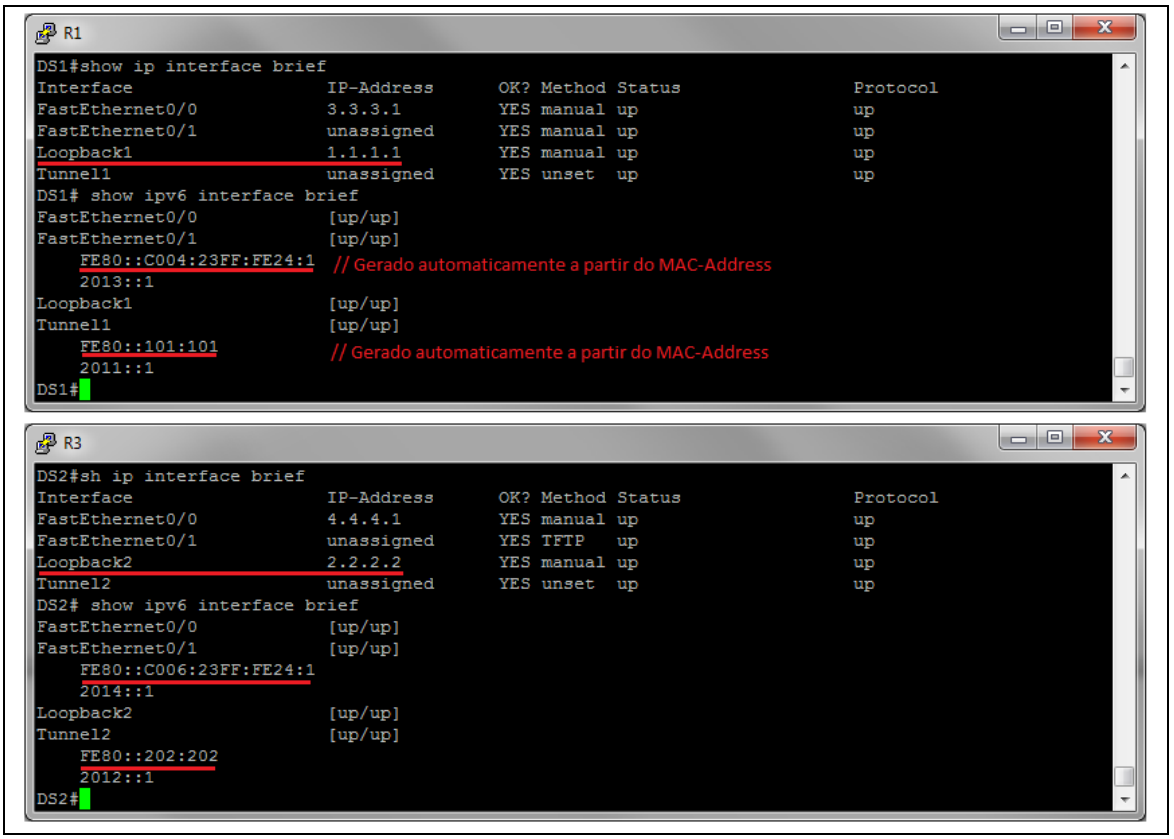


Figura 35. Endereços IPv6 atribuídos automaticamente.
Fonte: Autor.

A configuração do túnel propriamente dito se dá a partir de uma interface virtual (*Loopback1,* em **DS1**, e *Loopback2*, em **DS2,** Figura 36). Em **DS1**, a interface *Loopback1* (***1.1.1.1***) é usada como origem do túnel (***tunnel source Loopback1***), e o endereço (IPv4) da *Loopback2* (***2.2.2.2***, Figura 37) é usado como destino. Em **DS2**, a mesma lógica é utilizada, invertendo origem e destino. O comando ***tunnel mode ipv6ip*** define o tipo de túnel e o endereço IPv6 a ser usado como origem é configurado logo em seguida.

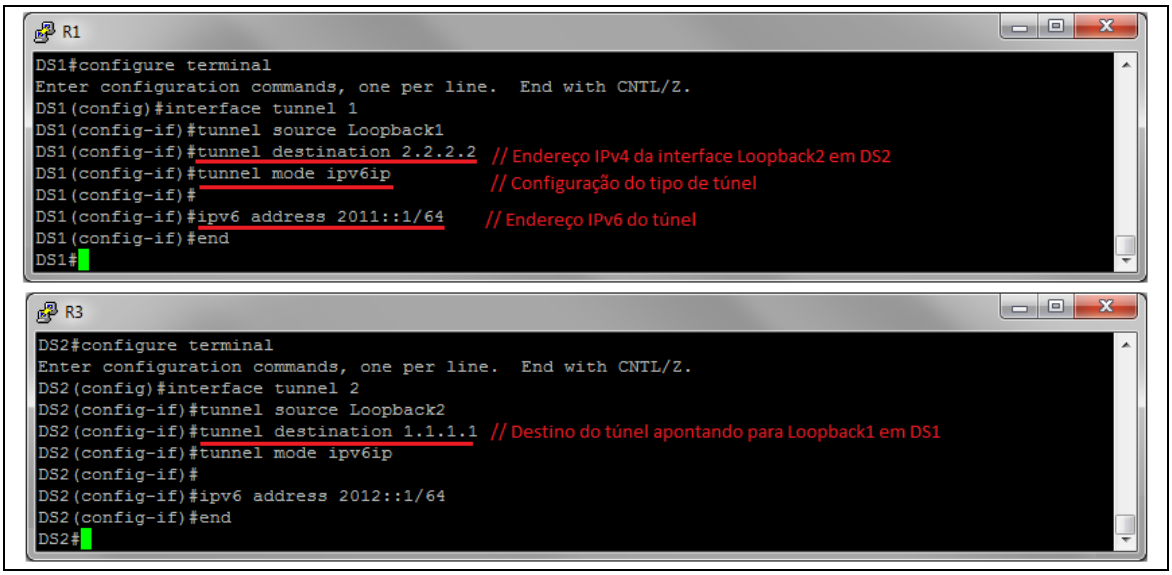


Figura 36. Configuração do túnel IPv6IP (6over4).
Fonte: Autor.

As rotas IPv4 são divulgadas via RIPv2 (*Routing Information Protocol*), e para IPv6, rotas estáticas apontam para o endereço do túnel por onde o tráfego sairá. Aplicadas essas configurações, o tráfego gerado pelo *Host1* alcança o *Host2*, ainda que o roteador **IPv4** não tenha nenhum tipo de configuração da versão 6, provando a funcionalidade do túnel *6over4*.

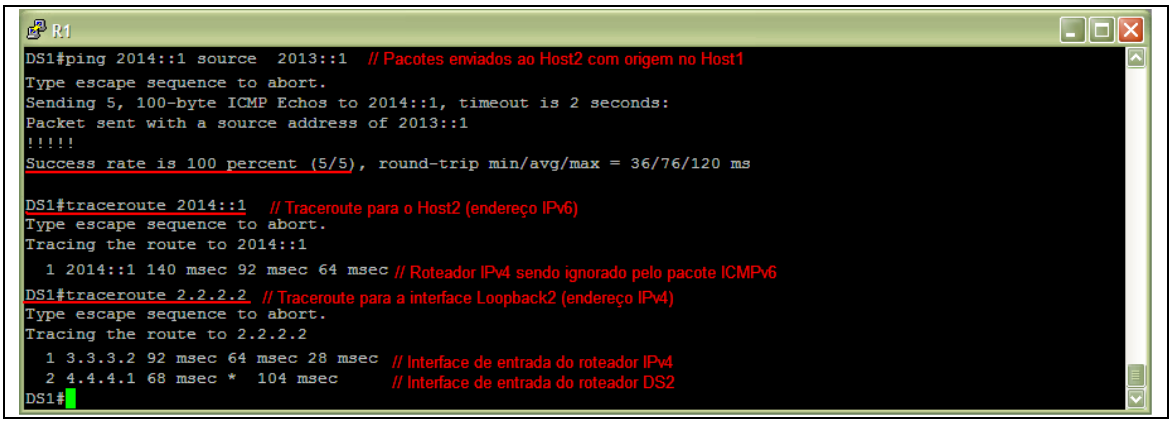


Figura 37. Pacotes ICMPv6. Traceroute v6 vs. v4.
Fonte: Autor.

Como pode ser visto, o comando *traceroute* mostra a diferença do caminho lógico entre pacotes IPv4 e IPv6 (Figura 38). Para pacotes v6, o roteador **IPv4** é completamente transparente. Essa troca de pacotes foi capturada com o auxilio do Wireshark, um conhecido examinador de tráfego, permitindo que o cabeçalho dos pacotes seja observado. O tipo de

encapsulamento é mostrado em ordem decrescente, ou seja, o mais externo aparece mais acima dos mais internos (Figura 39).

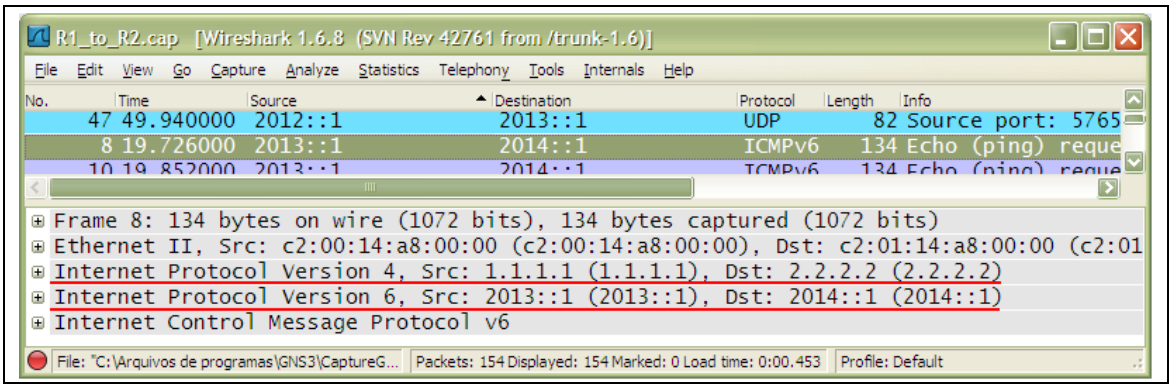


Figura 38. Captura de pacotes *6in4*.
Fonte: Autor.

O *Frame 8* mostra um pacote do tipo *echo request* (ICMPv6 *ping*) partindo do *Host1* (**2013::1**) em direção ao *Host2* (**2014::1**).

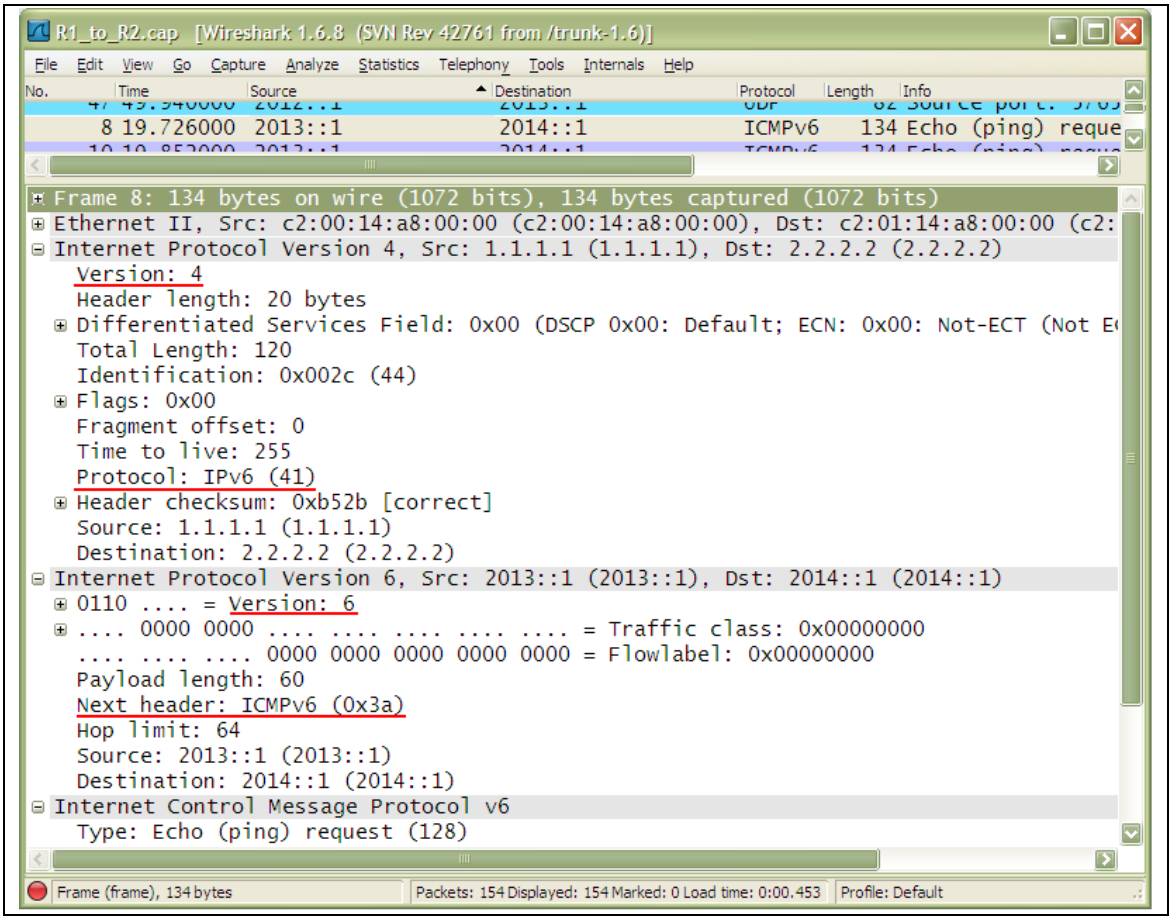


Figura 39. Cabeçalhos expandidos.
Fonte: Autor.

Este *frame* está dentro de um pacote IPv6, que por sua vez está encapsulado por um cabeçalho IPv4, com endereços de origem e destino como os configurados no túnel (***Src: 1.1.1.1, Dst: 2.2.2.2***). Expandindo os cabeçalhos, encontram-se os campos "*version*" (***Version: 4***) e "*protocol*" marcado com o valor "***41***", informando que este pacote carrega um pacote IPv6 e deve ser desencapsulado (Figura 40), e ainda o campo *"next header"* no cabeçalho IPv6, substituto do campo *"protocol"* da versão 4, comunicando que o próximo cabeçalho é do tipo ICMPv6.

Analisando os dados coletados, é possível visualizar as características do funcionamento dessa nova versão de protocolo em comparação com a versão anterior, e que a coexistência entre eles é totalmente viável e funcional, ainda que algum esforço quanto ao planejamento e configuração seja necessário.

6- Conclusão

Na elaboração deste trabalho foram utilizados livros de autores conceituados e com vasta experiência, bem como materiais de estudo desenvolvidos por companhias líderes de mercado, além de textos redigidos pelos próprios engenheiros que determinaram os padrões a serem seguidos, disponibilizados pelos órgãos reguladores da Internet (IETF, IANA, entre outros). Como resultado da pesquisa e experimentação realizadas de acordo com a proposta do mesmo, as conclusões são apresentadas a seguir.

No tocante à Pilha Dupla, é o método preferencial, e deve ser utilizado sempre que possível, já que no momento em que se encontra a transição entre os protocolos, ainda existem muitos *hosts* operando apenas com IPv4. Serve como solução para os cenários 1 até 8 descritos pro Baker. Equipamentos que possuem ambas as pilhas de protocolos (v4 e v6) são também utilizados nas outras técnicas de transição. O único caso que impossibilita sua utilização é quando não existem endereços IPv4 disponíveis para tais servidores ou *hosts* (que provavelmente estão sendo adicionados à rede).

Quanto às técnicas de tunelamento, são muito úteis para a comunicação entre redes IPv6 cujo tráfego percorrem ambientes onde apenas a pilha de protocolos IPv4 está instalada. Sua restrição está no fato de que não permite a comunicação entre *hosts* IPv4 e IPv6, mas apenas entre computadores operando com a nova versão. Podem ser aplicadas aos cenários 9 e 10.

Para os cenários 1 a 6, os quais serão mais comumente encontrados (*hosts* IPv4 comunicando-se com *hosts* IPv6 e vice-versa), as técnicas de tradução também são apropriadas. Entretanto, observa-se que em caso de tradução *stateful* (NAT64 *Stateful*, por exemplo), tráfego iniciado em um sistema IPv4 (cenários 2 e 4) não é capaz de prever o endereço IPv6 de um determinado *host*, mas é eficaz para o tráfego iniciado no sentido oposto. Por outro lado, a necessidade de configuração manual em tradutores stateless traz problemas de escalabilidade.

Pode-se dizer que o funcionamento do IPv6 e seus componentes representa um campo de estudo muito amplo, tornando a plenitude de seu entendimento uma tarefa extremamente árdua. O domínio das tecnologias empregadas para a utilização do IPv4 são de grande auxílio na compreensão da nova pilha de protocolos, por se tratar de uma evolução. Contudo, apesar de tamanha complexidade, muitos de seus conceitos podem ser abstraídos, permitindo que profissionais com níveis diversos de conhecimento e experiência interajam com os novos sistemas, desde que o escopo seja definido.

Por último, há que se considerar que, devido à visão de alguns cientistas que anteviram o esgotamento dos endereços IPv4, houve tempo hábil para o planejamento da transição, tornando desnecessária a interrupção dos serviços disponíveis na Internet, promovendo uma mudança suave e totalmente transparente para os usuários finais.

Referência bibliográfica

CISCO. ***Cisco SBA borderless networks:*** *IPv6 addressing guide.* San Jose: Cisco Systems, Inc. 2012.

FALCÃO, M. A. **Web 3.0:** A web inteligente. Guarulhos, 2012. 44f. Trabalho de Graduação em Bacharelado em Sistemas de Informação. Faculdades Eniac.

FONSSECA FILHO, C. **História da computação:** O Caminho do Pensamento e da Tecnologia. Porto Alegre: EDIPUCRS, 2007. Disponível em: <http://www.pucrs.br/edipucrs/online/historiadacomputacao.pdf>. Acesso em: 11 abr 2013.

FOROUZAN, B. A**. Protocolo TCP**. Tradução da 3ª edição. São Paulo: McGraw-Hill Interamericana do Brasil Ltda., 2008.

JAIN, R.; SHARMA, S. ***IPv6 Addressing Strategy.*** San Jose: Cisco Systems, Inc. 2010.

KUROSE, J. F.; ROSS, K. W. **Redes de Computadores e a Internet**: Uma Abordagem *Top-Down*. Tradução da 5ª ed. São Paulo: Addison Wesley, 2003.

MCQUERRY, S. ***CCNA Self-Study:*** *Introduction to Cisco Network Technologies (INTRO).* Indianapolis: Cisco Press, 2004.

_____. ***CCNA Self-Study:*** *Interconnecting Cisco Network Devices (ICND).* 2ª Ed. Indianapolis: Cisco Press, 2004.

ODOM, W. ***CCNP Route 642-902 Official Certification Guide***. Indianapolis: Cisco Press, 2010.

_____. ***CCNA Official Certification Guide Library***. 3ª Ed. Indianapolis: Cisco Press, 2010.

RAZA, K.; ASADULLAH, S. ***IPv6 Tutorial***. Karachi: Cisco Systems, Inc. 2006.

STALLINGS, W. **Redes e Sistemas de Comunicação de Dados**. Tradução da 5ª edição. Rio de Janeiro: Elsevier Editora Ltda, 2005.

TANEMBAUM, A. **Redes de Computadores**. Tradução da 4ª ed. Rio de Janeiro: Editora Campus 2003. Disponível em <http://www-usr.inf.ufsm.br/~rose/Tanenbaum.pdf>. Acesso em: 11 abr 2013.

ZUCCHI, W. L. Túneis IPv6. **Revista RTI**. São Paulo, nº 133, p. 138-143, jun 2011.

Links:

AOUN, C.; DAVIES, E. ***Reasons to Move the Network Address Translator:*** *Protocol Translator (NAT-PT) to Historic Status*, RFC 4966. 2007. Disponível em: http://www.ietf.org/rfc/rfc4966.txt Acesso em: 5/18/2013

ARIN. ***The IANA IPv4 address free pool is now depleted***. Disponível em: <https:// www.arin.net/announcements/2011/20110203.html>. Acesso em: 10 mai 2013.

BAGNULO, M et al. ***Stateful NAT64:*** *Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers,* RFC 6146. 2011. Disponível em: <http://tools.ietf.org/rfc /rfc6146.txt>. Acesso em: 17 mai 2013.

BAKER, F. et al. ***Framework for IPv4/IPv6 Translation***, RFC 6144. 2011. Disponível em: <http://www.ietf.org/rfc/rfc6144.txt>. Acesso em: 17 mai 2013.

BAO, C et al. ***IPv6 Addressing of IPv4/IPv6 Translators***, RFC 6052. 2010. Disponível em: <http://tools.ietf.org/rfc/rfc6052.txt>. Acesso em: 18 mai 2013.

BRADEN, R. ***Requirements for Internet Hosts:*** *Communication Layers,* RFC 1122. 1989. Disponível em: <http://www.ietf.org/rfc/rfc1122.txt>. Acesso em: 04 mai 2013.

BRADNER, S et al. ***The Recommendation for the IP Next Generation Protocol***, RFC 1752. 1995. Disponível em: <http://www.ietf.org/rfc/rfc1752.txt>. Acesso em: 04 mai 2013.

CISCO. ***Securing IPv6 Transition Technologies***. Disponível em: <http://blogs.cisco. com/security/securing-ipv6-transition-technologies>. Acesso em: 11 mai 2013.

_____. ***Apple Talk***. Disponível em: <http://docwiki.cisco.com/wiki/AppleTalk>. Acesso em: 01 mai 2013.

_____. ***Xerox Network Systems***. Disponível em: <http://docwiki.cisco.com/wiki/ Xerox_Network_Systems>. Acesso em 01 mai 2013.

_____. ***NAT64 Technology:*** *Connecting IPv6 and IPv4 Networks.* Disponível em: < http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/white_paper_c11-676278.html>. Acesso em: 17 mai 2013.

FULLER, V. et al. ***Classless Inter-domain Routing (CIDR):*** *The Internet Address Assignment and Aggregation Plan,* RFC 4632. 2006. Disponível em: <http://www. ietf.org/rfc/rfc4632.txt>. Acesso em: 04 mai 2013.

HUITEMA, C. "***Teredo:*** *Tunneling IPv6 over UDP through Network Address Translations (NATs)***.** RFC 4380. Disponível em: <http://tools.ietf.org/rfc/rfc6145.txt>. Acesso em: 26 mai 2013.

LI, X. et al. ***IP/ICMP Translation Algorithm***, RFC 6145. 2011. Disponível em: <http:// tools.ietf.org/rfc/rfc6145.txt>. Acesso em: 17 mai 2013.

MICROSOFT**.** ***Unicast IPv6 addresses***. Disponível em: <http://technet.microsoft.com/ en-us/library/cc759208 (v=ws.10). aspx>. Acesso em: 14 mai 2013.

_____. ***TCP/IP Core Protocols***. Disponível em: <http://technet.microsoft.com/en-us/library/cc958827.aspx>. Acesso em: 02 mai 2013.

NORDMARK, E; GILLIGAN, R. ***Basic IPv6 Transition Mechanisms***, RFC 4213. 2005. Disponível em: <http://www.ietf.org/rfc/rfc4213.txt>. Acesso em: 17 mai 2013.

POSTEL, J. ***Internet Protocol***, RFC 791. 1981. Disponível em: <http://www.ietf .org/rfc/rfc791.txt>. Acesso em: 02 mai 2013.

REKHTER, Y. et al. ***Address Allocation for Private Internets***, RFC 1597. 1994. Disponível em: <http://www.ietf.org/rfc/rfc1597.txt>. Acesso em: 02 mai 2013.

_____. ***Address Allocation for Private Internets***, RFC 1918. 1996. Disponível em: <http://www.ietf.org/rfc/rfc1918.txt>. Acesso em: 02 mai 2013.

TROTH, R. ***SIFT/UFT:*** *Sender-Initiated/Unsolicited File Transfer*, RFC 1440. 1993. Disponível em: <http://www.ietf.org/rfc/rfc1440.txt>. Acesso em: 04 mai 2013.