UNIPAC
UNIVERSIDADE PRESIDENTE ANTÔNIO CARLOS
FACULDADE DE CIÊNCIA DA COMPUTAÇÃO E
COMUNICAÇÃO SOCIAL DE BARBACENA

CURSO DE CIÊNCIA DA COMPUTAÇÃO

Cláudio Discacciati Silveira

PROTOCOLO IPV6: *a nova geração do protocolo IP*

BARBACENA
DEZEMBRO DE 2004

CLÁUDIO DISCACCIATI SILVEIRA

PROTOCOLO IPV6: a nova geração do protocolo IP

Trabalho de Conclusão de Curso apresentado à Universidade Presidente Antônio Carlos, como requisito parcial para obtenção do Título de Bacharel em Ciência da Computação.

ORIENTADOR: Prof. Luís Augusto Mattos Mendes

BARBACENA
DEZEMBRO DE 2004

Cláudio Discacciati Silveira

PROTOCOLO IPV6: *a nova geração do protocolo IP*

Trabalho de Conclusão de Curso apresentado à Universidade Presidente Antônio Carlos, como requisito parcial para a obtenção do Título de Bacharel em Ciência da Computação.

Aprovado em _____/_____/_____

BANCA EXAMINADORA

_____

Prof. Luís Augusto Mattos Mendes (Orientador)
Universidade Presidente Antônio Carlos

_____

Prof. Ms. Eliseu César Miguel
Universidade Presidente Antônio Carlos

_____

Prof. Ms. Gustavo Campos Menezes
Universidade Presidente Antônio Carlos

Dedico este trabalho a meus pais Clara e Ronaldo, aos meus irmãos Carla e Rodrigo, a minha querida Kelly e também a todos aqueles que estiveram ao meu lado.

Agradeço ao meu orientador Luís Augusto pelas orientações recebidas, pela seriedade, dedicação e apoio com que este trabalho foi conduzido.

RESUMO

Há algumas décadas, a *Internet* estava dando seus passos iniciais em direção à sua concepção atual. Era somente utilizada em meios acadêmicos, industriais e órgãos do governo (especialmente o Departamento de Defesa dos Estados Unidos) ficando restrita a poucas pessoas que detinham conhecimentos para utilizá-la. Durante a década de 90, houve uma grande difusão deste incrível meio de comunicação, fazendo com que muitos tivessem acesso às informações distribuídas por todo o planeta. Atualmente, a *Internet* utiliza como protocolo de rede o *Internet Protocol Version 4*, ou comumente conhecido como IPv4. Devido a problemas como o crescimento do número de internautas, utilização cada vez maior de serviços multimídia (som e vídeo sob demanda), novas tecnologias e necessidade de segurança na *Internet*, é importante que ocorra uma evolução do protocolo IP para uma versão que contemple e atenda a essas necessidades. Com a visão voltada para o futuro, desenvolvedores iniciaram em 1990 o projeto de um novo protocolo que iria revolucionar a *Internet* em diversos aspectos. Este novo protocolo inicialmente recebeu o nome de *IP Next Generation* e, posteriormente, o nome IPv6. É essencial que tenhamos um conhecimento aprofundado sobre IPv6 para verificar suas vantagens e desvantagens em relação à versão 4, permitindo avaliarmos a viabilidade de sua implantação.

Palavras chave: IPv6, Protocolo, Redes ,TCP/IP , Segurança, *6BONE*.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

Atualmente a *Internet* vem estando cada vez mais próxima da população mundial, podendo ser encontrada distribuída por uma malha que atinge até mesmo as mais longínquas localidades. O fato de estar tão presente em nosso dia a dia originou uma crescente necessidade por comunicação, impulsionada por meios facilitadores que foram criados com o evoluir de nossas tecnologias. Portanto, podemos facilmente notar como os serviços distribuídos por redes de computadores se tornaram importante e indispensáveis no contexto mundial que nos encontramos inseridos.

Os serviços que possuímos e fazemos uso, são todos fornecidos por computadores conectados à grande rede mundial de computadores que conhecemos pelo nome de Internet. Para que um computador possa comunicar com outro, provendo serviços e enviando dados, é necessário que o mesmo possua uma identificação individual que o possibilite de ser o único a utilizar aquele endereço, àquela identidade. A identidade de um computador é fornecida pela sua associação natural a um número que denominamos de número IP.

Como o funcionamento da *Internet* e demais serviços de rede estão intimamente ligados a distribuição de números IP´s pelo planeta, é necessário que existam números IP´s suficientes para todas as máquinas que se encontrem conectadas. Nossa situação atual não é muito boa, pois os números IP´s estão se esgotando, nos forçando a encontrar meios alternativos para manter a *Internet* funcionando. Apesar do desenvolvimento de técnicas que permitam que os endereços IP´s sejam melhor reaproveitados e redistribuídos, o número de máquinas e *sites* que se conectam e são criados estão aumentando rapidamente.

Para solucionar este e demais problemas ligados à distribuição de serviços via *Internet,* grupos da IETF (*Internet Enginering Task Force*) concentraram esforços para o desenvolvimento de uma nova versão de IP com a finalidade de substituir o nosso atual IP versão 4 mais conhecido como IPv4. Deste trabalho surgiu um protótipo, o IP versão 5, porém, esta versão do IP não foi adotada como versão que viria por sua vez a atualizar a versão 4. Então foi trabalhada uma nova versão, esta viria a ter as qualidades necessárias para ser adotada em um futuro próximo para substituir a nossa atual versão do IP. Foi então desenvolvido o IPv6 (*Internet Protocol Version 6)*, mantendo muitas das características que contribuíram para o

sucesso do IPv4. A todas as propostas de versões que viriam substituir o IPv4 foram denominadas de IPng (*IP Next Generation)*.

Este trabalho tem como finalidade apresentar alguns conceitos da *Internet*, bem como apresentar as características, vantagens, arquitetura e fatores de segurança do IPv6 incluindo algumas técnicas para a transição de nosso atual Protocolo de rede o IPv4 para a sua próxima versão, o IPv6.

2 HISTÓRIA E NOÇÕES SOBRE A *INTERNET*

A história da comunicação de dados se iniciou por volta dos anos 60, quando houve a descentralização de alguns terminais de computadores que deixaram seus centros de processamento de dados para serem instalados à distância. Desta forma, surgiu o conceito de Teleprocessamento que, por sua vez, é baseado em um computador principal dotado de alto poder de processamento, que armazenava todas as aplicações, que eram acessadas por vários terminais remotos. Com a visão voltada para as potencialidades do Sistema de Teleprocessamento, em 1968 o Departamento de Defesa dos Estados Unidos iniciou estudos quanto a viabilidade do desenvolvimento de redes de computadores. Em 1972 iniciava o desenvolvimento do projeto ARPA (*Advanced Research Project Agency*). Com o surgimento deste projeto iniciou a era da tecnologia das redes de computadores. A partir deste momento de implantação das redes de computadores permitiu que os computadores conectados a rede possuíssem suas próprias aplicações e estrutura de teleprocessamento (W2K, 2004).

Com o projeto ARPA surgiram vários serviços de redes que utilizamos até a presente data e que são de extrema valia para o funcionamento de nossas redes de computadores atuais. O projeto ARPA contribuiu para o surgimento da comutação de pacotes e também para o método de divisão em várias camadas das tarefas envolvendo aplicações em redes. Também foi pioneira no desenvolvimento de protocolos de aplicações como o de transferência de arquivos FTP (*File Transfer Protocol*).

No inicio da década de 80, foi criada nos Estado Unidos o que viria a ser a espinha dorsal de nossa redes de computadores atual. Baseada no potencial instalado da rede ARPA posteriormente denominada de *Internet*. À *Internet* foram atribuídas as principais aplicações do ARPA, como o protocolo de transferência de arquivo FTP e o protocolo virtual *Telnet*, e foi adotada para o seu gerenciamento uma estrutura técnico organizacional denominada IAB (*Internet Activities Board*). Foi de responsabilidade da IAB a criação do principal protocolo de rede que utilizamos atualmente o TCP/IP.

Após uma década a *Internet* experimentou uma altíssima taxa de crescimento que superou todas as expectativas previstas na sua criação. Devido a esta alta taxa de crescimento a *Internet* começou a apresentar alguns problemas que não estavam previstos. Tais problemas

tiveram como fator principal a enorme quantidade de *hosts*[1] conectados e os endereços IP disponíveis começaram a se tornar escassos rapidamente. O problema da falta de endereços também pode ser atribuído a má distribuição dos endereços IP em classes realizado durante a criação da *Internet,* desta forma os endereços IP foram desperdiçados. Todos estes fatores contribuíram para o aumento das tabelas de roteamento que tornou esta atividade lenta e ineficiente.

Juntamente ao amadurecimento da *Internet* começaram a surgir serviços que inicialmente em sua concepção não existiam. Estes serviços foram produzidos a partir da evolução natural dos computadores, ou seja, a partir de que os computadores pessoais se tornaram mais velozes e robustos, fizeram com que a rede se adaptasse para poder dar suporte aos mesmos. A nossa *Internet* atual não está capacitada para fornecer, por exemplo, serviços de tempo real como para transmissão de sons e vídeos com alta performance e qualidade, pois inicialmente ela não foi projetada para isso. Não podemos deixar de fora a questão de segurança. Nos primórdios da *Internet*, era utilizada pelo meio universitário e por militares, principalmente para transmitir arquivos textos de um lugar para outro. Devido ao interesse inicial de que ela somente funcionasse bem para estes fins o fator de segurança passou a ser implementado posteriormente na *camada de aplicação*, que a torna uma tarefa não muito eficiente.

Não restam dúvidas que o protocolo IPv4 (*Internet Protocol Version 4*) necessita ser substituído para o melhor funcionamento de nossa rede mundial de computadores. Foi com foco nesta idéia que em 1990 o *Internet Enginering Task Force* - IETF começou a trabalhar para o desenvolvimento de um novo protocolo de rede o IPv6. Na época foram apresentados vários projetos de protocolos que receberam o nome de IPng (*IP Next Generation*). A versão 5 do protocolo era somente uma versão para experimentos. Em 1995, a fase de desenvolvimento estava terminada e o protocolo IPv6 já estava definido para ser implementado.

[1] *Host* – Terminal de computador que está conectado a uma rede.

2.1 Noções sobre o Funcionamento dos Protocolos

Para que haja uma comunicação entre computadores é necessário que os mesmos se comuniquem utilizando uma mesma linguagem. Estas linguagens precisam possuir uma padronização para posteriormente serem denominadas protocolos de rede (W2K, 2004).

A principal função dos protocolos na interconexão em redes é estabelecer regras de comunicação entre computadores. Estas regras vão controlar diversos processos que irão permitir que um determinado pacote saia de sua origem e chegue ao seu destino com uma alta margem de segurança.

Além de definir a linguagem com a qual estes computadores vão se comunicar é necessário estabelecer a forma com que eles serão interligados para a troca de informações. Para atingir tal finalidade existem duas formas. A primeira seria estabelecer uma conexão direta entre os computadores comunicantes, que recebe o nome de comutação por circuitos. Uma segunda forma e mais difundida atualmente, seria a comutação de pacotes, que consiste em encaminhar as informações para computadores intermediários que estariam retransmitindo esta informação até outras máquinas para que ela chegue ao seu destino.

Foi percebido que a implantação da comutação entre circuitos geraria um custo muito elevado, uma rede frágil, e no caso de um nó[2] de ligação deixar de existir a rede deixaria de funcionar por falta de ligações redundantes. No protocolo TCP/IP foi implementada a tecnologia de comutação de pacotes permitindo um alto grau de interoperabilidade apresentando uma solução para tais problemas. O TCP/IP foi adotado como padrão no mundo todo como protocolo de comunicação na *Internet*. É permitido a uma organização que projete seus próprios protocolos para que sejam utilizadas dentro de suas redes internas, mas em relação com a comunicação através da *Internet*, as suas redes têm de se adaptar para que consigam utilizar o padrão TCP/IP.

O protocolo TCP/IP é uma junção de dois protocolos, o protocolo TCP e o Protocolo IP. Eles trabalham lado a lado para garantir a dois ou mais computadores conectados na rede, comunicação e transparência de dados.

A Figura 01 mostra o posicionamento do protocolo TCP e do protocolo IP na arquitetura de *Internet* TCP/IP por meio de suas camadas conceituais. As informações são

[2] Nó – Qualquer computador (*Host*) ou equipamento que seja um ponto de interconexão de uma rede.

trocadas na forma vertical seguindo uma hierarquia que começa de cima para baixo. A camada superior solicita um serviço da camada inferior correspondente. A idéia de se ter as camadas predispostas desta forma sugerem que cada uma delas utilizem e prestem serviços a sua camada vizinha. Na camada de Inter-rede, encontran-se os protocolos de conexão como é o caso do protocolo IP. Na camada de transporte encontramos os protocolos de transmissão como o TCP e o UDP (*User Datagram Protocol*) este último é responsável pelas transmissões que não precisam de controle de fluxo fazendo uma entrega imediata, é muito usado para transmissão de sons e vídeos em tempo real, justamente por não questionar este mesmo fluxo acaba ganhando em rapidez de entrega, mas perde em integridade por ser um protocolo de conexão não confiável. A camada de aplicação é constituída por protocolos de alto nível como o *Telnet*, http, Ftp dentre outros.

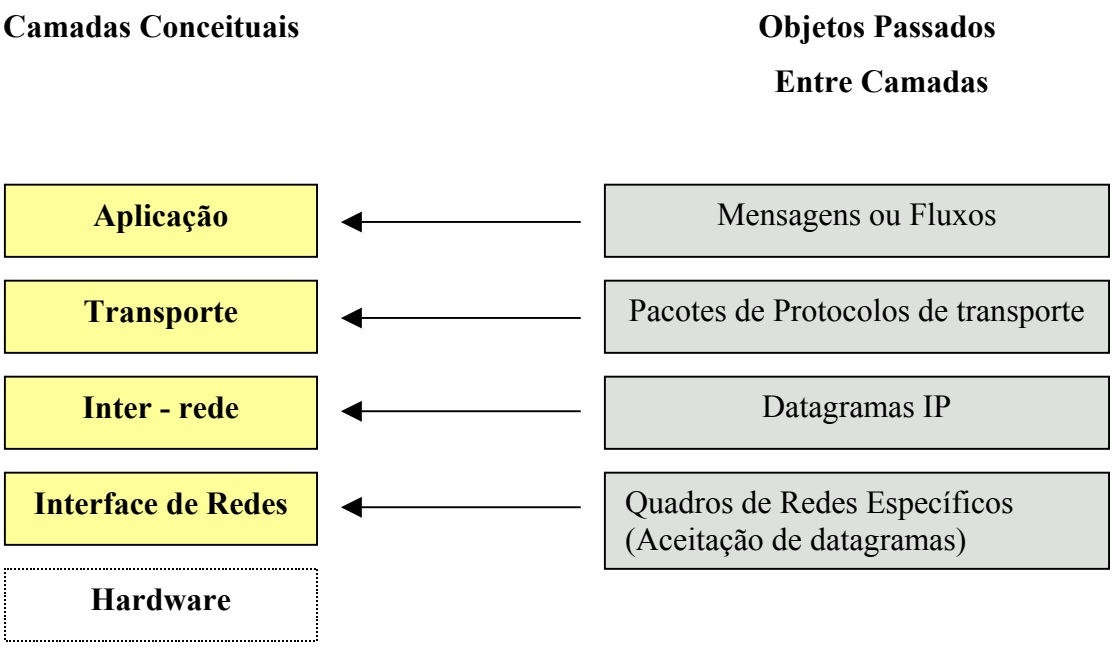


Figura 01 – Camadas conceituais do protocolo de *Internet* TCP/IP.
(COMER, 1998, p.185).

O TCP (*Trasmission Control Protocol*) ou Protocolo de Controle de Transmissão garante que os pacotes contendo os dados a serem enviados entre computadores, cheguem ao seu destino conservando a sua integridade. O TCP é constituído de bibliotecas de rotinas que se

encontram instaladas nos computadores de origem e destino permitindo o uso de serviços como Telnet, http e outros.

Segundo Comer (1998, p.211) embora o TCP seja apresentado como parte de uma pilha de protocolos TCPI/IP da *Internet*, ele é um protocolo independente e de finalidade geral que pode ser adaptado para utilização com outros sistemas de transmissão. Como, por exemplo, o TCP pouco questiona sobre a rede básica, é possível utilizá-lo em uma rede individual como a *Ethernet*, e também em uma interligação em redes complexa.

O gerenciamento de uma rede por meio do TCP se faz através da quebra dos dados em pedaços menores chamados pacotes. O TCP garante que estes dados transmitidos cheguem ao seu destino evitando qualquer tipo de perda de pacotes durante o trajeto fazendo a junção no *host* destino reconstituindo os dados originais.

Para que pacotes de informação cheguem a seus destinos é necessário definir um caminho, caminho este pré-definido pelo protocolo IP. Os pacotes deverão sair do computador de origem chegando até o computador destino podendo passar por uma ou mais redes para atingir tal objetivo. Segundo Soares (1995, p.316) o serviço oferecido pelo IP é sem conexão. Portanto, cada pacote IP é tratado como uma unidade independente que não possui nenhuma relação com qualquer outro pacote. A comunicação é não-confiável, não sendo usados reconhecimentos fim-a-fim[3] ou entre nós intermediários. Nenhum mecanismo de controle de erros nos dados transmitidos é utilizado, exceto um *checksum* do cabeçalho que garante que as informações nele contidas, que são usadas pelos *gateways* (roteadores) para encaminhar os pacotes estão corretas. Nenhum mecanismo de controle de fluxo é empregado.

O endereço IP é o responsável pela identificação de cada equipamento conectado à rede fazendo com que cada um deles possuam um endereço IP único em toda a rede. Por serem endereços únicos, possibilitam que ocorra uma comunicação entre dois computadores distintos. Atualmente nos utilizamos a versão 4 deste protocolo conhecido como IPv4.

2.2 Limitações do IP versão 4

Quando olhamos o nosso atual protocolo de rede mais de perto percebemos que ele além de nos oferecer serviços valiosos para conexão, possui certas imperfeições que merecem

[3] Entende-se por fim-a-fim a mesma definição de ponto-a-ponto.

maior atenção. Tais imperfeições são encontradas quando é abordada a questão de segurança e a falta de endereços IP disponíveis para a contínua expansão da *Internet*. Muitos dos relacionados problemas de segurança surgiram porque o protocolo IPv4 não foi projetado para ser seguro. Desta forma, o protocolo IPv4 está sujeito a vários ataques[4] a serviços de *Internet* como o *Telnet*, FTP, SMTP (*E-mail*). Tais serviços também estão sujeitos a ataques passivos como captura de tráfego por meio de *sniffers*[5] e ataques ativos como o roubo de informações. Os problemas quanto a questão do esgotamento de endereços disponíveis são originários à limitação de geração de endereços pelo fato do campo de endereçamento do IPv4 possuir apenas 4 bytes (32 bits). Este problema ainda pode ser agravado pela má divisão dos endereços em classes para a divisão da *Internet* em redes. É fácil imaginar que dentro de poucos anos não haverá mais endereços IPv4 suficientes para identificar todos os computadores que queiram se conectar a esta grandiosa rede mundial de computadores. Devido a estes e outros fatores o atual protocolo de rede o IPv4 deverá ser substituído pela sua versão mais recente o IPv6 que foi desenvolvido voltado a questão da segurança.

[4] Ataque é definido como sendo qualquer tipo de ação realizada em um computador conectado a uma rede que não tenha sido autorizada pelo administrador deste mesmo computador.

[5] *Sniffer* – Programa especializado em "escutar" o que se passa na rede. Sua função é capturar pacotes de um determinado tráfego da rede. Caso o *sniffer* esteja instalado em uma máquina qualquer, ele somente poderá capturar o trafego desta máquina.

3 PROTOCOLO IPV6

No início da década de 90, a *Internet Engenering Task Force* conhecida pela sigla IETF, por meio de um grande esforço, começou a desenvolver um novo protocolo que viria a substituir o atual protocolo IPv4. Este grande esforço realizado pela IETF foi motivado pela escassez crescente de números IP de 32 bits existentes, que na época se fez evidente pela grande velocidade de conexão de redes de computadores à *Internet*.

Para suprir a necessidade de alocação de novos endereços IP, um novo protocolo IP foi desenvolvido. Este novo protocolo foi batizado com o nome de IPv6, nome que inclusive foi dado por não ter sido utilizado um protótipo de protocolo de cujo nome era IPv5.

A equipe de projetistas que estavam desenvolvendo este novo protocolo aproveitou a oportunidade para adicionar novos aspectos ao IPv6, baseando-se nas observações feitas durante todos esses anos em que foi utilizado o protocolo IPv4 como principal protocolo de interconexão em rede.

Com o esgotamento dos endereços IP existentes, mais nenhuma rede poderia ser adicionada à rede mundial de computadores. Foi com base nesta deficiência que o protocolo IPv6 surgiu como uma evolução necessária motivada principalmente pela necessidade de se criar uma grande quantidade números IP que suprissem esta grande demanda que anda aumentando gradativamente ano após ano.

Para termos uma idéia mais abrangente sobre o protocolo IPv6 e também do que ele virá a se tornar, devemos ter de antemão o conhecimento de suas funcionalidades, características e arquitetura.

Na seção seguinte será abordado as principais características do IPv6 para permitir uma melhor avaliação deste protocolo.

3.1 Características do Protocolo IPv6

O protocolo IPv6 que está sendo proposto preserva muitas características que garantiram sucesso ao IPv4. Na realidade, os projetistas atribuíram a este novo protocolo basicamente as mesmas características do protocolo IPv4, mas realizaram algumas alterações significativas para contribuir em seu melhoramento em relação ao IPv4 (COMER, 1998, p.548).

É importante citar algumas importantes modificações que foram incorporadas ao IPv6, como: simplificação de cabeçalho, suporte nativo a *multicasting*, criação do tipo de endereçamento *anycast*, suporte nativo a autenticação e privacidade, hierarquias nos tipos de fluxos de dados.

Algumas de suas funcionalidades foram mantidas com as mesmas características. Um exemplo que podemos citar é a entrega sem conexão. Ela permite que cada datagrama seja roteado independentemente, possibilitando ao transmissor que determine o tamanho de cada datagrama e o número de passos de rota que um datagrama pode percorrer antes de ser descartado.

Segundo Comer e W2K (1998, p.548 ; 2004), em relação às características deste protocolo, algumas tiveram importância significativa até mesmo para a criação do IPv6. A criação de endereços maiores que permitirá em um futuro próximo que existam tantos números IP que até mesmo eletrodomésticos se conectem à rede. Mais importante, foi tornar os campos de opções de comprimento variável por cabeçalhos de tamanho fixo que tornará este novo protocolo mais dinâmico que o IPv4. Podemos citar algumas das principais mudanças introduzidas pelo IPv6:

- *Endereços Maiores* - O tamanho de endereçamento gasto de 32 bits no IPv4 passa para 128 bits no IPv6, que permitirá a criação de bilhões de endereços IP. A capacidade de endereçamento do IPv6 é tão grande que não há previsões de quando irá se esgotar.
- *Formato de Cabeçalho Flexível* - Ao contrário do IPv4 que possui um formato de cabeçalho fixo em todos os campos, exceto o de opções, o IPv6 usa um formato de datagrama totalmente novo e compatível. O IPv6 utiliza um conjunto de cabeçalhos adicionais que são chamados de cabeçalhos de extensão.
- *Opções Aprimoradas* - Como o IPv4, o IPv6 fornece suporte a inclusão de informações de controles adicionais. O IPv6 oferece a adição de novas opções de recursos que não estão disponíveis no IPv4.
- *Autoconfiguração*.- O IPv6 possui mecanismos destinados a facilitar a configuração de ambientes IP através de mecanismos de autoconfiguração. A autoconfiguração ajudará bastante ao usuário livrando-o da tarefa de configurar os protocolos de rede manualmente a fim de permitir que, ao conectar o computador à rede, a configuração

seja feita de uma maneira fácil e transparente. Esta técnica permite que o computador também passe de uma rede para outra sem perder a sua referência.

- *Seleção de rota pelo originador* - Tem por objetivo a seleção de rota pelo originador fazendo que o pacote percorra um caminho pré-estabelecido através de roteamento. Este mecanismo permite também a possibilidade de aumentar a segurança durante a transmissão da informação. Baseado no endereço de destino os roteadores escolhem a melhor rota para o datagrama. A rota é fixada preenchendo os cabeçalhos de extensão com os endereços que devem ser percorridos, para realizar o caminho de retorno do datagrama, basta inverter a ordem dos cabeçalhos de extensão e enviar o datagrama para quem o originou.
- *Suporte para Alocação de Recursos* - O IPv6 permite a pré-alocação de recursos de rede para a utilização de certos serviços, por exemplo, transmissão de som e vídeos em tempo real. Tais aplicativos requerem garantias de largura de banda e retardo de transmissão.
- *Provisão para Extensão de Protocolo* - Ao analisarmos as mudanças que foram feitas no IPv6, talvez a mais significativa tenha sido a transição de um protocolo que possui um cabeçalho que fornece todos os detalhes para seu normal funcionamento, por outro protocolo com cabeçalho fixo e simples que permita recursos adicionais. Esta capacidade de extensão permite que a IETF modifique o protocolo de acordo com mudanças de hardware de rede ou para fornecer serviços a novos aplicativos.
- *Suporte a Jumbogramas* - Capacidade de envio de pacotes com tamanho superior a 64Kb e podendo alcançar um limite de 4Gb. Podendo ser muito útil se empregadas em redes que disponibilizem uma grande largura de banda.

3.2 Formato Geral de um Datagrama IPv6

O datagrama IPv6 possui um cabeçalho básico de tamanho fixo, seguido ou não por cabeçalho de extensão e posteriormente por dados, conforme apresentado na Figura 02.

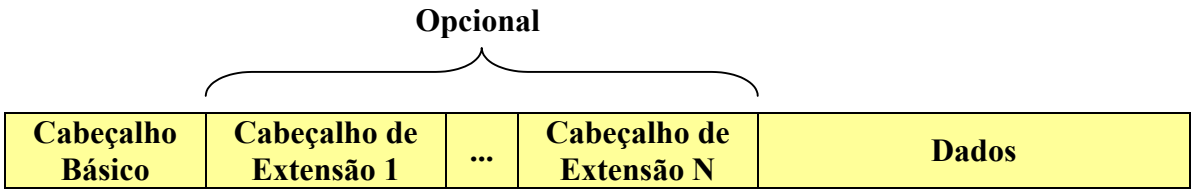


Figura 02 - Datagrama Básico IPv6. (COMER, 1998, p.549).

O IPv6 proporcionou várias mudanças no datagrama com objetivo de corrigir imperfeições de arquitetura do IPv4. Tais modificações tornam o datagrama IPv6 mais eficiente em sua forma de processamento pelos roteadores, sendo mais detalhado na seção seguinte.

3.2.1 Simplificação de cabeçalho

Com a finalidade de se otimizar o processamento de pacotes do protocolo IPv6, foi realizada uma redução significativa de tamanho de cabeçalho. Esta redução de tamanho é possível porque alguns campos que existiam no cabeçalho dos pacotes IPv4 foram eliminados ou se tornaram opcionais. O cabeçalho resultante, com tamanho fixo de 40 bytes, irá permitir o processamento mais veloz dos datagramas IPv6.

Apesar de acomodar campos de endereçamentos maiores, um cabeçalho básico IPv6, contém uma quantidade menor de informações que um cabeçalho IPv4, isto se refere à eliminação de alguns campos já mencionados anteriormente. Alguns campos de opções que se encontravam como campos fixos no datagrama IPv4 passaram a fazer parte de um cabeçalho de extensão no datagrama IPv6. A Figura 03 mostra que os campos que constituem o cabeçalho IPv6 são os seguintes:

- *Version* – Contém a informação de qual versão do IP está sendo utilizada. Se a versão usada for a versão IPv6 esta campo irá conter o número binário 0110.
- *Priority* – Fornece a prioridade de tratamento com o qual o pacote será tratado. Permite que uma origem especifique a prioridade de entrega para determinados pacotes em relação a outros pacotes da mesma origem. Tem como função gerar uma prioridade para determinado tráfego.

- *Flow Label* – Identifica, juntamente com a associação dos campos *Sourse Address e Destination Address*, o fluxo ao qual o pacote pertence. Utilizado para identificar pacotes que requerem tratamento especial pelos roteadores IPv6, como na qualidade de serviço fora do padrão ou serviços de tempo real como a transmissão de vídeo e som.
- *Payload Length* – Este campo é responsável pelo armazenamento do tamanho do pacote após o cabeçalho. Os 40 bytes do cabeçalho não são incluídos, como acontecia no IPv4.
- *Next Header* – Indica o tipo de cabeçalho de extensão que estará contido após o cabeçalho IPv6. Se não houver cabeçalho de extensão a ser passado, neste campo estarão as informações de qual protocolo de transporte que este pacote deve ser repassado.
- *Hop limit* – Este campo é muito necessário na arquitetura IPv6, pois impede que pacotes tenham vida eterna. O tempo de vida e determinado pelo limite de passos através da rede.
- *Sourse Address* – Indica o endereço de quem enviou o pacote.
- *Destination Address* – Indica o endereço de destino do pacote.

Para se ter uma idéia melhor de como é um cabeçalho IPv6, na Figura 03 se encontra a representação deste cabeçalho, contendo o tamanho específico de cada campo bem como suas descrições:

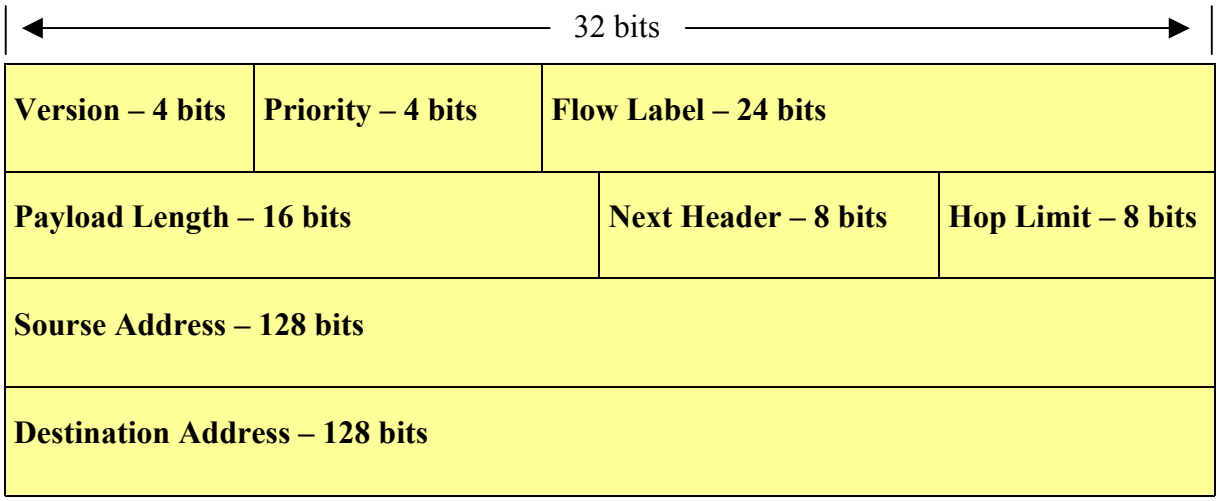


Figura 03 – Cabeçalho de tamanho fixo do datagrama IPv6.
(TANENBAUM, 1997, p.501; DEERING).

É importante perceber que, no cabeçalho básico do IPv6, vários campos correspondem aos campos de um cabeçalho IPv4, estes campos foram mantidos pelo fato do IPv6 ter sido criado com base na arquitetura do IPv4.

Abaixo serão apresentados algumas mudanças no cabeçalho do datagramas e que refletem diretamente como alterações no protocolo:

- O alinhamento para múltiplos de 64 bits o que antes se fazia com 32 bits.
- O campo de *Comprimento de Cabeçalho* foi eliminado pelo motivo de que o cabeçalho assumirá tamanho fixo de 40 bytes e o nome do campo *Comprimento de Datagrama* foi trocado por *Comprimento de Payload.*
- O campo de endereçamento de origem e endereçamento de destino teve o seu tamanho aumentado para 128 bits armazenados em 16 octetos cada.
- As informações de fragmentação foram movidas para o Cabeçalho de Extensão.
- O campo *Tempo de Vida* foi substituído por um campo chamado *Limite de Passos de Rota(Hop Limit).*
- O campo *Tipo de Serviço* foi substituído por um novo campo *Rótulo de Fluxos(Flow Label)*.
- O campo *Protocolo* foi substituído pelo campo *Próximo Cabeçalho(Next Header)*. (Verificar mais sobre as informações acima)

3.2.2 Cabeçalho de extensão

O IPv6 possui um mecanismo de opções que ao compararmos ao do IPv4 concluímos que é relativamente melhor. As opções no datagrama IPv6 são colocadas em cabeçalhos de extensão que se localizam entre o cabeçalho fixo e os dados a serem transportados. A maioria dos cabeçalhos de extensão do IPv6 são processados e analisados ao longo de seu percurso pelos roteadores até que chegue ao seu destino. Isto melhora o desempenho dos roteadores. No IPv4 acontece de maneira diferente, em cada momento que aparece um pacote que contenha alguma opção, o roteador passa a verificar todas as outras opções que este possua.

Uma grande vantagem dos cabeçalhos de extensão é que eles podem ter tamanhos arbitrários e o total de opções transportadas pode ser superior a 40 octetos. Estas características, se usadas em conjunto, podem proporcionar a utilização de funções que não eram práticas do IPv4, como as opções de autenticação e encapsulamento de segurança.

Para aumentar seu desempenho o protocolo monta os cabeçalhos de opções subseqüentes em múltiplos de um inteiro de 8 octetos. Isto mantém uma padronização de alinhamento dos cabeçalhos seguintes.

Em resumo, o cabeçalho de extensão do IPv6 é semelhante às opções do IPv4. Cabe ao protocolo incluir nos datagramas transmitidos os cabeçalhos de extensão que necessitar.

Segundo Comer (1998, p.552) cada cabeçalho básico e de extensão contém um campo "Próximo Cabeçalho". O software em roteadores intermediários e no destino final que precisa processar o datagrama deve usar o valor no campo "Próximo Cabeçalho" de cada cabeçalho, para analisar o datagrama. Para extrair todas as informações de cabeçalho de um datagrama IPv6, é necessário uma pesquisa seqüencial através dos cabeçalhos. Por exemplo, a Figura 04 mostra os campos "Próximo Cabeçalho" do datagrama que contêm dois cabeçalhos de extensão.

Cabeçalho Básico **PRÓXIMO = ROTA**	**Cabeçalho de Rota** **PRÓXIMO = AUTORIDADE**	**Cabeçalho de Autoridade** **PRÓXIMO = TCP**	**Segmento TCP**

Figura 04 – Datagrama constituído de um cabeçalho básico e dois de extensão. (COMER, 1998, p.553).

3.3 Endereçamento no IPv6

Uma das maiores vantagens do IPv6, é a sua constituição de 128 bits para armazenamento de endereços enquanto o IPv4 utilizava apenas 32 bits. Esta quantidade maior de bits permitem que existam uma quantidade equivalente a bilhões de endereços por cada habitante do planeta. É como se atribuíssemos a cada pessoa uma quantidade de endereços igual ao total utilizada pela *Internet* atual. É até mesmo complicado pensarmos em quanto tempo esta quantidade de endereços vão se esgotar. Na verdade não se tem estimativas para tal

acontecimento. Se formos passar este número binário de 128 bits para a notação decimal que utilizamos em nosso cotidiano, obteríamos o seguinte número: 3,4x10^38 que seria o mesmo que dizer que após o número 3, haveria mais 38 casas decimais acompanhando este número.

3.3.1 Tipos básicos de endereçamento

No IPv6 o sistema de endereçamento Broadcast foi eliminado, por ser ineficiente se comparado aos novos tipos criados no IPv6. Podemos englobar os endereços em três categorias:

- ***Unicast*** **-** É o novo nome dado ao endereçamento ponto-a-ponto[6] do IPv4. Neste tipo de endereçamento foram mantidas as mesmas características anteriores do ponto-a-ponto, ou seja, um datagrama é enviado apenas para uma determinada interface que possui o endereço especificado.
- ***Multicast*** **-** O multicast possui algumas familiaridades com o sistema de broadcast utilizado no IPv4. No multicast os pacotes são enviados a um grupo de interfaces. Os pacotes que serão enviados para o grupo, serão enviados diretamente a todos os membros constituintes do grupo. Podemos até arriscar a dizer que o multicast seria um aperfeiçoamento do antigo e ultrapassado broadcast.
- ***Anycast*** **-** O *anycast* teria a sua forma de funcionamento similar ao multicast, em que o destino é um grupo de endereços, porém, ao invés de tentar fazer a entrega de pacotes para todos os endereços, o anycast tenta enviar o pacote para apenas um endereço, este endereço seria o mais próximo. Normalmente ele envia o pacote para o roteador, e este se encarrega de retransmití-lo para o *host* ideal. Isto acontece quando alguém tenta fazer uma cópia de um arquivo, neste caso ele pode se conectar a um grupo de servidores de arquivos utilizando o anycast para alcançar o servidor mais próximo, sem se preocupar em saber qual deles se trata.

> *Como o IPv4, o IPv6 associa um endereço a uma conexão de rede específica, não a um computador específico. Assim, atribuições de endereço são semelhantes ao IPv4: um roteador IPv6 tem dois ou mais endereços, e um host IPv6 com uma conexão de rede precisa de apenas um endereço. O IPv6 também retém (e estende) a hierarquia*

[6] Ponto-a-ponto – terminologia usada para definir a comunicação entre um ponto de origem a um ponto de destino dentro da rede.

> *de endereço de IPv4 em que um prefixo é atribuído a uma rede física. Entretanto, para facilitar a atribuição e a modificação de endereço, o IPv6 permite que vários prefixos sejam atribuídos a determinada rede e permite que um computador tenha vários endereços simultâneos atribuídos a determinada interface (COMER, 1998, p.559).*

3.3.2 Simplificação de endereçamento

Com a utilização de endereços maiores, o IPv6 conseguiu solucionar o problema de escassez de endereços IP, mas esta solução proporcionou um novo problema. Este problema teve origem em como se daria a compactação do próprio endereço de 128 bits que o IPv6 iria utilizar, que por sua vez é muito extenso e gastaria muito espaço para o seu armazenamento. Segundo Comer (1998, p.558) para melhor entendimento da simplificação de endereçamento consideraremos que um endereço IPv6 de 128 bits seja escrito na forma decimal pontuada que é adotada no IPv4 :

100.123.23.10.200.255.255.255.255.0.0.144.13.128.255.255

Desta forma o endereço de 128 bits faria com que o IPv6 desperdiçasse espaço demasiado. Para contornar este problema, foi proposto que fosse usado no endereçamento uma notação *hexadecimal de dois pontos,* em que cada conjunto de 16 bits fosse representado por uma notação hexadecimal separada por dois pontos. Se fizermos esta transformação no endereço de 128 bits acima ele tomaria a seguinte forma:

647B:17A:C8FF:FFFF:FF:0:90:D80:FFFF

É evidente que ao adotarmos a notação hexadecimal de dois pontos adquirimos uma vantagem óbvia, que é a de utilizarmos menos caracteres do que a forma decimal de dois pontos. A notação hexadecimal de dois pontos também possui mais uma técnica muito importante que ajuda na compactação do endereçamento que é a capacidade de suprimir os zeros repetidos substituindo por pares de dois pontos, por exemplo:

: :A23:10:44D3:1

3.4 Roteamento IPv6

O roteamento tem como função permitir e possibilitar que um determinado pacote trafegue por uma rota até que chegue ao seu destino escolhido previamente. Ao contrário do IPv4, o IPv6 permite que se especifique uma rota livre que leve os pacotes a serem roteados da origem até o destino. Esta funcionalidade é possível graças aos cabeçalhos de extensão que contêm listas de endereços especificando os roteadores intermediários através do qual os pacotes devem trafegar. Entre os campos do cabeçalho de roteamento os mais importantes são os que indicam o número de endereços a serem percorridos e o campo *próximo endereço*, que diz qual será o próximo endereço que o pacote será enviado. O caminho a ser percorrido por cada pacote é predeterminado em cada máquina de origem. Desta forma há a possibilidade de ter maior controle sobre qual caminho os pacotes irão tomar. Haverá assim uma grande redução no processamento dos roteadores, pois a origem realizará esta função que antes era exclusiva dos roteadores.

O roteamento do IPv6 é semelhante ao do IPv4, o que altera é que o IPv6 utiliza endereços de 128 bits e o IPv4 de 32 bits. Basicamente todos os algoritmos que constituíam o roteamento de pacotes IPv4, podem ser empregados para rotear pacotes IPv6.

O IPv6 também possui extensões simples de roteamento que permitem que seus pacotes sejam roteados de uma melhor forma. Tais extensões agregaram funcionalidades poderosas, por exemplo:

- Seleção de provedor – seleção do provedor baseando em desempenho e custo;
- Mobilidade de *host* – é a capacidade de mudar de rede sem perder a referência com o endereço anterior*;*
- Auto-reendereçamento – possibilita o direcionamento automático para um novo endereço;

Existe um fator principal para que *hosts* trabalhem com novas características como seleção de provedor ou endereços extendidos. Este fator consiste em solicitar o roteamento reverso de pacotes recebidos. Esta técnica tende a criar seqüências de endereços usando as

opções de roteamento. As opções são usadas para listar um ou mais *hosts* intermediários (ou grupos de topologias) que devem ser percorridos pelos pacotes até o seu destino.

Para tornar o endereçamento seqüencial uma função geral, os *hosts* são solicitados para se fazer o roteamento reverso, invertendo seqüências de endereçamento para que o pacote retorne à sua origem, permitindo assim que os *hosts* trabalhem com seleção de provedor e endereços estendidos.

4 SEGURANÇA

Atualmente, a população mundial cada vez mais vem utilizando a *Internet* para diversas finalidades como uma simples consulta a bancos de dados a até mesmo transações bancárias envolvendo altos valores monetários. Por isso, a *Internet* tem uma necessidade primordial por segurança. Foi pensando nisto, que foram criados vários mecanismos que contribuíram para que o IPv6 fosse tão conciso no que se refere a questão da segurança e de seu aperfeiçoamento em relação ao IPv4.

No IPv6 existem mecanismos que utilizados individualmente ou em conjunto podem garantir uma segurança efetiva que torne a *Internet* um ambiente mais hospitaleiro para quem faz seu uso. Foi pensando nos diversos problemas com a segurança que foram implementados mecanismos localizados na camada de rede para eliminar a necessidade de verificações de segurança nas camadas superiores, em particular na camada de aplicação.

No IPv6, os dados contidos nos datagramas são encriptados em toda trajetória, da origem até o destino, enquanto no IPv4 somente são encriptados entre roteadores na camada de distribuição.

Mais à frente serão abordadas arquiteturas e métodos necessárias para a implementação de tais mecanismos que tornam o IPv6 tão eficiente e bem estruturado na parte que se refere a segurança.

4.1 O Problema de Segurança no IPv4

Segundo Puttini (2004) o relatório anual do "*Computer Emergency Response Team*", uma entidade pertencente ao governo Norte Americano que pesquisa sobre segurança na *Internet*, listou aproximadamente 2.500 (dois mil e quinhentos) acidentes com segurança os quais atingiram 12.000 (doze mil) redes em 1995. Os ataques relatados de conseqüências mais graves incluíam *IP Spoofing*[7], E*avesdropping*[8] e *Packet Sniffing*[9]. Os fatos citados deixam claro a necessidade de implementar mecanismos de segurança eficazes os quais necessariamente

[7] *IP Spoofing* - ataque que se utilizam de pacotes IP com endereços falsos
[8] E*avesdropping* - analise não autorizada dos pacotes que trafegam na rede
[9] *Packet Sniffing* - ataque no qual um intruso pode diretamente ler as informações transmitidas e conteúdo de base de dados

devem cobrir áreas tais como proteção da infra-estrutura contra monitoramento não autorizado e controle de tráfego de rede. Além disso, torna-se necessário defender o tráfego entre usuários finais usando mecanismos de autenticação e criptografia.

Conforme mostrado anteriormente, começamos a ter uma idéia da fragilidade de nosso sistema de segurança utilizado atualmente no protocolo IPv4, e demais aplicações de segurança situadas na camada de aplicação. É necessário uma mudança imediata na arquitetura de protocolo atual por uma mais especializada, para que tais problemas mencionados se minimizem, ou melhor, não retornem a acontecer novamente. A segurança implementada para o protocolo IP é a solução para estes fatos.

4.1.1 Solução para o problema

A solução para esses problemas e deficiências veio com o desenvolvimento do IPv6, Outra forma de referenciarmos o IPv6 é chamando-o de *IpSecurity* ou simplesmente IPSEC. Sua proposta é implementar segurança no próprio nível IP, fazendo com que não seja mais necessário criar mecanismos de segurança em nível de aplicativo ou serviço. Assim, todos os serviços existentes em uma rede estariam seguros. Esta solução pode ser útil não só para LANs[10] mas para WANs[11] públicas e por toda a *Internet*. Resumidamente, pode-se dizer que todos os dados que trafegam em uma rede, sejam eles aplicações distribuídas, *login* remotos, modelos cliente/servidor, e-mail, ftp, http podem estar finalmente seguros, sem precisar de mais nenhum mecanismo adicional de proteção. Assim, resta apenas proteger os equipamentos, por exemplo, os de uma LAN contra acessos não autorizados, com a utilização de *firewalls*[12], para alcançar um nível de proteção satisfatório (ANDREOLI, 2000). Diversas áreas se beneficiarão com o IPSEC, por exemplo:

- Trafego de correio eletrônico.
- Proteção contra ataques do tipo "*IP Spoofing*"
- Para troca de informações de forma segura na *Internet*:

[10] LAN (*Local Area Networks*) - Rede local geralmente envolvendo poucas maquinas.
[11] WAN (*Wide Area Networks*) – Rede com abrangência mundial (*Internet)*.
[12] Firewall – Software ou equipamento que tem como principal função proteger uma rede ou uma máquina contra acessos não autorizados.

- Evitar análise do trafego de dados em uma rede qualquer.
- Evitar o reconhecimento de informações que por ventura seja interceptada.

Mais a frente abordaremos os mecanismos que serão necessários para a implementação da segurança em nível IP.

4.2 Segurança no Nível IP

Atualmente cada vez mais se investe em segurança em nível de aplicação. A forma que é realizada a segurança em nível de aplicação se dá por meio de mecanismos que atuam especificamente para garantir segurança para determinado tipo de aplicação específica. Podemos citar como exemplo e para melhor entendimento o serviço de *e-mail* atual. Dois dos mecanismos que promovem a segurança nos serviços de *e-mail* são: *PEM - Privacy Enhanced Mail* (Privacidade de Correspondência Otimizada) *e PGP - Pretty Good Privacy* (Privacidade Razoável).

No entanto foi verificado que é mais importante se utilizar da segurança em nível IP do que somente promover segurança em nível de aplicação. Esta segurança em nível IP se faria de diversas formas na camada de rede, como:

- Implementação um mecanismo de Autenticação e Integridade dos datagramas transmitidos e recebidos;
- Implementação de mecanismos que permitam confidencialidade da informação nos datagramas;

Desta maneira podemos assegurar uma conexão confiável não apenas para aplicações seguras, mas também para muitas daquelas que desconhecem segurança. Por exemplo, se implementássemos um sistema de segurança ao nível de IP em uma empresa que possua duas redes corporativas confiáveis e distantes entre si. Utilizando a *Internet* como via de intercambio de informações podemos garantir que, com o IPv6 a troca de *e-mails* seria totalmente confiável uma vez que se garante através dos mecanismos de segurança autenticidade, integridade e confidencialidade aos datagramas transmitidos e recebidos.

4.3 Associações de Segurança

Um conceito em comum que aparece relacionado aos mecanismos existentes de autenticação e privacidade para o IPv6 é a Associação de Segurança. Associação de Segurança é um conjunto de instruções que permitem negociar quais os algoritmos serão utilizados para cálculo da criptografia.

De acordo com Puttini (2004)**,** uma associação de segurança é uma relação de sentido único entre um emissor e um receptor que descreve quais serão os mecanismos de segurança a utilizar para estabelecer uma comunicação segura. Se uma relação que se processa em dois sentidos então são necessárias duas associações de segurança. Uma associação de segurança é unicamente identificada por um endereço *Internet* e um índice de parâmetro de segurança (*Security Parameter Index - SPI*). Desta forma, em qualquer pacote IP, a associação de segurança é unicamente identificada pelo endereço de destino e pelo SPI. Uma associação de segurança é definida pelos seguintes parâmetros:

- Algoritmo de autenticação e modo do algoritmo usado com cabeçalho de autenticação IP (requerido para implementações AH - Authentication Header).
- Chave(s) usada no algoritmo de autenticação utilizado com o cabeçalho de autenticação (necessário para implementações AH).
- Algoritmo de criptografia, modo do algoritmo, e transformação usada no cabeçalho de encapsulamento de dados de segurança - ESP - Encapsulating Security Payload (necessário às implementações ESP).
- Chave(s) usada no algoritmo de criptografia utilizados no cabeçalho de encapsulamento de dados de segurança (necessário às implementações ESP).
- Presença / ausência e tamanho do campo do vetor de inicialização ou sincronização criptográfica para o algoritmo de criptografia (necessário às implementações ESP).
- Algoritmo de autenticação e modo usados com a transformação do cabeçalho de encapsulamento de dados de segurança ESP, se algum estiver em uso (recomendada para implementações ESP).

- Chave(s) de autenticação usada com o algoritmo de autenticação, a qual é parte do cabeçalho transformado ESP, caso haja algum (recomendada para implementações ESP).
- Tempo de vida da chave ou tempo para o qual deverá ocorrer mudança da mesma (recomendado para todas as implementações).
- Tempo de vida da associação de segurança (recomendado para todas as implementações).
- Endereço origem da associação de segurança divide a mesma associação de segurança com o destino (recomendado para todas as implementações).
- Nível de sensibilidade (por exemplo, "secreto" ou "não classificado") dos dados a serem protegidos (requerido para todos os sistemas que necessitam prover segurança em níveis múltiplos, recomendado para todos os outros sistemas).

Na associação de segurança são empregados algoritmos de criptografia que utilizam chaves para promover a encriptação e desencriptação da informação a ser transmitida. Uma chave é um conjunto de instruções que associada a um algoritmo de criptografia em poder do emissor e receptor da informação, permite que se possa fazer a codificação e decodificação dos datagramas IPv6.

> *O mecanismo chave de gerência, que é usado para distribuir chaves, é acoplado aos mecanismos de autenticação e privacidade apenas por meio do índice de parâmetros de segurança (SPI). Desta forma, autenticação e privacidade são especificadas de forma independente de qualquer mecanismo específico de gerência de chaves (PUTTINI, 2004).*

4.3.1 Áreas funcionais

A aplicação da segurança em nível IP tem uma abrangência sobre duas áreas funcionais que são:

- Autenticação - O cabeçalho de extensão para autenticação é conhecido como cabeçalho de Autenticação - *Authentication Header (*AH);

- Privacidade - Cabeçalho de extensão correspondente à privacidade é conhecido como cabeçalho de encapsulamento de dados de segurança - *Encapsulating Security Payload* (ESP).

Nos dois casos as características de segurança são implementadas como cabeçalhos de extensão que seguem o cabeçalho IPv6, que no caso do IPv4, é realizado através do campo "*options*". No IPv4 estas características são opcionais, no IPv6 já se encontram nativas, não necessitando de ser implementado.

4.4 Autenticação

Um dos principais mecanismos de segurança é o Cabeçalho de Autenticação, ou comumente conhecido como *Authentication Header (AH).* Este novo mecanismo trata os datagramas de forma a promover autenticação e a integridade, mas sem adicionar confidencialidade aos mesmos. O IPv6 será muito útil no processo de autenticação de origem. Existe um fato que encorajou os projetistas na produção e divulgação deste mecanismo, a razão deste não confidencializar as informações dos datagramas. Isto se deve ao fato de muitos países não admitir que as informações que trafegam na *Internet* sejam confidenciais, como o caso da França, Iraque, dentre outros. O *Authentication Header* gera um cabeçalho IPv6 autenticado, garantindo a identidade do remetente, e que o datagrama não foi alterado durante o tráfego.

Autenticação assegura que um pacote recebido foi realmente transmitido pela origem identificado no cabeçalho do pacote. Adicionalmente, a autenticação assegura que nada foi alterado no conteúdo da informação transmitida, ou seja, o que é recebido é o que realmente foi enviado. O cabeçalho de autenticação provê suporte à autenticação e integridade dos dados no pacote do protocolo IP (PUTTINI, 2004).

O cabeçalho de autenticação, apresentado na Figura 05, é um cabeçalho de extensão e é constituídos dos seguintes campos:

- ***Próximo Cabeçalho (Next header)*** - Identifica o tipo de cabeçalho que segue imediatamente depois .
- ***Tamanho (Length*) -** Comprimento do campo de autenticação em palavras de 32 bits.

- ***Reservado (Reserved*) -** Será utilizado caso se faça necessário no futuro.
- ***Índice de Parâmetros de Segurança (Security Parameters Index*) -** Identifica a associação de segurança.
- ***Autenticação de dados (Authentication Data*) -** Valor de no máximo 32 bits.

***Next Header* - 8 bits**	***Reserved* – 16 bits**	***Length* – 32 bits**
***Authentication Data* – Tamanho variável**		
***Security Parameters Index* - 32 bits**		

Figura 05: Cabeçalho de Autenticação. (PUTTINI, 2004).

> *O campo de autenticação de dados dependerá do algoritmo de autenticação especificado. De qualquer forma, o dado de autenticação é calculado sobre todo o pacote IP, excluindo-se qualquer campo que possa mudar durante o trânsito na rede. Tais campos são tornados nulos para propósitos de cálculo tanto na fonte quanto no destino. O cálculo de autenticação é executado antes de uma fragmentação na fonte e depois da remontagem do pacote no destino. Daí, os campos relacionados com fragmentação podem ser incluídos no cálculo. Para o IPv4, os campos de "Checksum" e "Time-to-live" estão sujeitos a modificações e, desta forma, são tornados nulos para o cálculo da autenticação. As "Options" no IPv4 têm que ser manipuladas de acordo com as regras para quaisquer "Options" para as quais o valor poderia mudar durante o trânsito na rede, ou seja, não podem ser incluídas no cálculo. Para o IPv6, o campo "Hop Limit" é o único campo no cabeçalho base do IPv6 sujeito a mudanças; daí, o mesmo é anulado para efeitos de cálculo. Para os cabeçalhos "Destination Option" e a opção "Hop-by-Hop", o campo "Option Type" para cada "Option" contém um bit que indica se o campo "Option Data" para esta opção pode mudar durante o trânsito; caso isso ocorra, esta "option" é excluída do cálculo de autenticação (PUTTINI, 2004).*

4.4.1 Autenticação usando o algoritmo MD5

De acordo com Puttini (2004), o algorítmo MD5 é executado sobre o pacote IP mais uma chave secreta na fonte e, então, é inserido no pacote IP. No destino, o mesmo cálculo é executado sobre o pacote IP e a chave secreta é comparada com o valor recebido. Este

procedimento provê tanto a autenticação quanto a integridade dos dados. Especificamente, o cálculo MD5 é executado na seguinte seqüência:

Chave, "Keyfill", Pacote IP, Chave, MD5 fill

Onde:

- chave = chave secreta para esta associação de segurança
- keyfill = "padding" tal que chave + keyfill é um múltiplo inteiro de 512 bits
- pacote IP = pacote IP com os campos adequados anulados
- MD5fill = "padding" fornecido pelo MD5 tal que todo o bloco seja um múltiplo inteiro de 512 bits.

Na Figura 06 são mostrados duas formas onde são utilizados o serviço de autenticação. Em uma das situações, a autenticação é fornecida por um servidor e um cliente. As estações de trabalho podem estar ou não em uma mesma rede (Autenticação Fim-a-Fim).

O processo de troca de pacotes IP pode ser determinado seguro se a medida que o servidor e as estações de trabalho compartilham uma chave secreta. Na outra situação o servidor não suporta características de autenticação então as estações de trabalho remotas possuem algumas opções que autenticam a si mesmas para um “firewall” ou para acesso a toda rede interna. O processo de autenticação seria realizado por meio de um nó intermediário neste caso o roteador (Autenticação Fim-Intermediário).

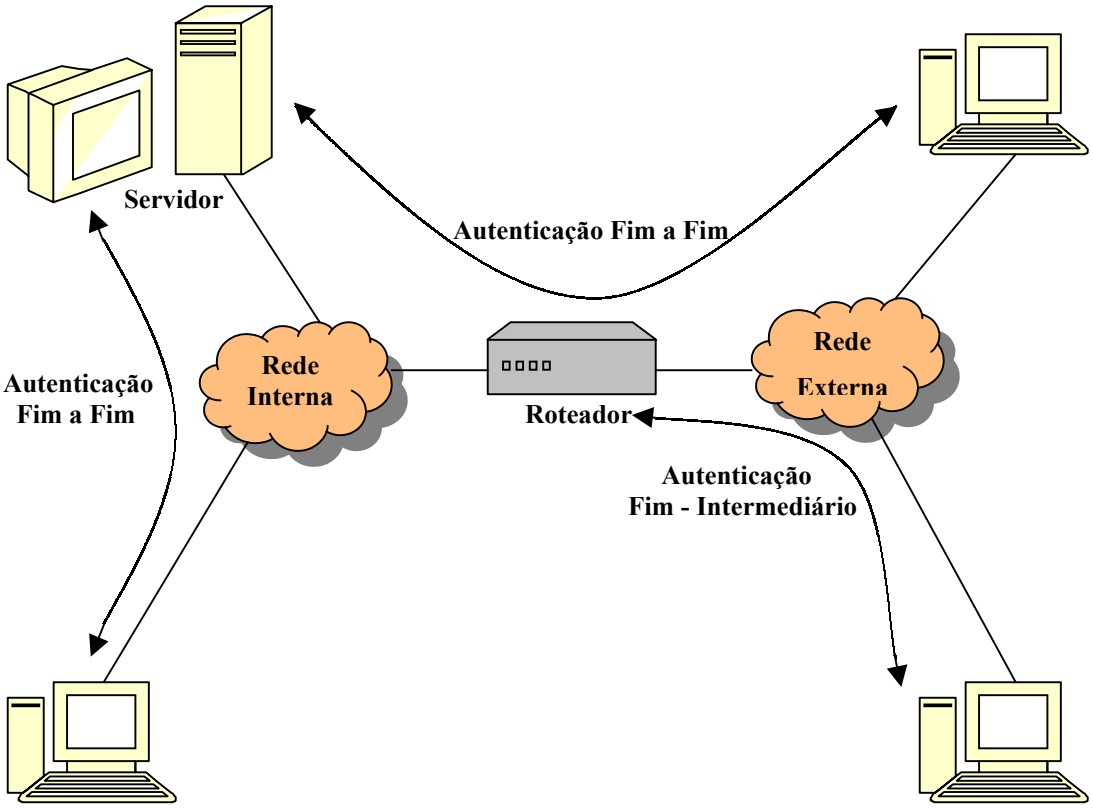


Figura 06: Modos de autenticação fim a fim e intermediário. (PUTTINI, 2004).

4.5 Privacidade

O principal mecanismo que fornece segurança sobre os datagramas IPv6 é chamado de cabeçalho ESP (*Encrypted Security Payload).* Através dele é implementado criptografia aos dados enviados em todo o *payload*, armazenando informações no próprio cabeçalho de extensão ESP. Desta forma, os datagramas transmitidos não poderão ser lidos e compreendidos por outras pessoas que porventura o interceptem em seu percurso. Este mecanismo promove a segurança de forma a permitir a integridade e confidencialidade dos datagramas IPv6, sendo totalmente independente de algoritmos de criptografia, fazendo com que ele possa evoluir seus métodos criptográficos para métodos mais seguros.

4.6 Autenticação e Privacidade

Podemos ter o nível de segurança aumentado quando juntamos estes dois mecanismos de segurança baseados em IP. Eles podem ser combinados de modo a transmitir um pacote IP com ambos os mecanismos de privacidade e autenticação. Utilizamos duas formas para fazer uso desta técnica:

- Criptografia antes da autenticação;
- Autenticação antes da criptografia;

4.6.1 Criptografia antes da autenticação

De acordo com Puttini (2004)**,** na técnica de se empregar a criptografia antes da autenticação, todo o pacote IP transmitido é autenticado, incluindo ambas as partes criptografadas e não criptografadas. Neste caso, o usuário aplicou em primeiro lugar aos dados a serem protegidos o mecanismo ESP e depois o mecanismos de autenticação associado ao cabeçalho base IP conforme mostrado na Figura 07. Neste modelo existem ainda duas possibilidades:

- Modo de transporte ESP: O mecanismo de autenticação se aplica a todo o pacote IP que é enviado ao destino final, mas apenas o segmento da camada de transporte é protegido pelo mecanismo de privacidade.
- Modo túnel ESP: A autenticação se aplica ao pacote IP inteiro ao endereço IP externo (um *firewall* por exemplo), e a autenticação é executada no destino final. Todo o pacote IP "interior" é protegido pelo mecanismo de privacidade, para entrega do pacote IP interior.

Criptografado - Modo de Transporte ou Túnel

IP-H	AH	ESP-H	Segmento de transporte do pacote	E-T

Escopo da aplicação

Figura 07: Criptografia aplicada antes da autenticação sobre o pacote IP. (PUTTINI, 2004).

Onde:

- IP-H: Cabeçalho IP mais os cabeçalhos de extensão
- E-T: Campos "*trailing*" do ESP
- ESP-H: Cabeçalho ESP
- AH: Cabeçalho de identificação

4.6.2 Autenticação antes da criptografia

Nesta técnica é recomendada apenas para modo túnel. Podemos empregar a autenticação antes da criptografia da seguinte forma:

1° - O cabeçalho de autenticação é colocado dentro do pacote IP interior;

2° - O Pacote IP interior é autenticado e protegido pelo mecanismo de privacidade.

As funções de autenticação e criptografia podem ser aplicadas em ambos os casos para o modo túnel ESP, conforme mostra a Figura 08. O uso da autenticação antes da criptografia poderia ser preferível por várias razões. Primeiro, por causa do AH ser protegido pelo ESP, é impossível interceptar a mensagem e alterar o AH sem detecção. Em segundo lugar, seria desejável armazenar informação de autenticação com a mensagem e o destino para referências em outra ocasião. É mais conveniente executar esta armazenagem se a informação de autenticação se aplicar a uma mensagem não criptografada; por outro lado, poderia haver a necessidade de criptografar mais uma vez a mensagem para verificar a informação de autenticação (PUTTINI, 2004).

Criptografado - Modo Túnel

IP-H	ESP-H	IP-H	AH	Segmento do nível de transporte	E-T

Escopo da Autenticação — Pacote IP interno

Figura 08: Autenticação aplicada antes da criptografia sobre o pacote IP. (PUTTINI, 2004).

5 TRANSIÇÃO DO PROTOCOLO IPV4 PARA O PROTOCOLO IPV6

Como já apresentado, a cada ano de uso de nossa Rede Global de Computadores os números de IP existentes vem se esgotando gradativamente, assim é necessário que haja uma transição urgente de protocolo para que este problema seja solucionado. O Protocolo IPv6 possui capacidade muito superior de endereçamento que o seu antecessor o IPv4, que irá nos trazer diversas novidades e facilidades para um futuro próximo. Com base nesta concepção, é fácil termos uma idéia de como esta transição de protocolos se faz necessária.

Como a Rede Mundial de Computadores atual é muito extensa, e nem todos os usuários estão familiarizados com o protocolo IPv6, as dificuldades para colocá-lo em funcionamento são muito grandes. Uma transição de protocolo em quase toda a *Internet* pode se estender por um tempo indeterminado devido ao alto investimento recente na compra de equipamentos e roteadores especializados em trabalhar com datagramas IPv4.

Para que a transição do protocolo IPv4 para o IPv6 seja realizada de forma segura é preciso que seja feita de forma gradual e lenta. Uma segunda opção seria a de determinar um dia e horário para que todos os computadores da *Internet* fossem desligados e atualizados com o novo protocolo. Ocorreu por volta de 20 anos atrás uma troca de serviço quando a *Internet* ainda era usada somente por um pequeno grupo de especialistas. A rede naquela época era bem menor que hoje, e a transição dos serviços NPC para o TCP, nos mostrou que escolher um dia para tal atualização seria impossível. Não é possível marcar um dia para a troca de protocolos, devido ao próprio tamanho que a nossa Rede Mundial de Computadores tem alcançado atualmente.

Veremos, a seguir, algumas técnicas que foram desenvolvidas para que esta transição se faça possível, tornando-a bem natural e transparente a todos que a adotarem.

5.1 Técnicas de Integração IPv6

Para que haja uma transição de protocolos de maneira mais amigável e de forma mais natural, é necessário que o protocolo IPv6 possua um fator muito importante. Este fator refere-se à compatibilidade entre o IPv6 e o IPv4. Sem esta compatibilidade de protocolos teríamos que realizar a transição em hora e dias marcados, pois quem não atualizasse sua máquina ficaria impossibilitado de se comunicar com a rede.

Para que a compatibilidade se estabeleça ao IPv6 foram desenvolvidas técnicas que fazem uso de diversas funcionalidades e semelhanças entre os dois protocolos. Aliadas a novas metodologias irão permitir que o IPv4 e o IPv6 tenham uma convivência amistosa durante os muitos anos de duração deste processo.

Como vimos a chave para uma transição para o IPv6 é a compatibilidade. Esta compatibilidade deverá ser implementada tanto em *hosts* como em roteadores de IPv4.

Os mecanismos que serão vistos foram desenvolvidos para que o protocolo IPv6 possa interagir com redes IPv4. É esperado que a rede utilize destas ferramentas de compatibilidade por muito tempo ou indefinidamente. No entanto apesar do IPv6 ter sido projetado para ser utilizado em tais ambientes de interação com o IPv4 ele pode ser perfeitamente em ambientes puramente IPv6. Nas redes IPv6 não aparecerão problemas de incompatibilidade com o IPv4, pois ele já possui estes mecanismos incorporados.

Os mecanismos utilizados para integração dos protocolos IPv4 e IPv6 são o de Pilha Dupla, tradução e Tunelamento.

5.1.1 Mecanismo de Pilha Dupla (*Dual-Stack*)

O mecanismo de Pilha Dupla ou *Dual-Stack*[13], consiste em fazer com que *hosts* e roteadores da rede estejam habilitados para trabalharem sobre datagramas (pacotes) IPv4 e IPv6. Ou seja, estes roteadores e *hosts* estariam rodando sobre a mesma interface, tanto para pilhas IPv4, quanto para IPv6. Desta forma, um nodo[14] *Dual-Stack* (ponto de interconexão da rede utilizando a metodologia *Dual-Stack*), poderá receber e transmitir pacotes dos dois protocolos.

Em uma situação normal, que tivéssemos somente nodos *Dual-Stack* rodando em uma parte da rede, poderíamos trafegar tanto datagramas IPv6 quanto IPv4 naturalmente, pois os nodos da rede estariam habilitados a receber e enviar datagramas IPv6 e IPv4. Portanto estando um datagrama inserido neste contexto não iríamos precisar nos preocuparmos se este sofrer alguma alteração pois todos os datagramas irão ter tratamentos distintos.

[13] Dual-Stack – Técnica que permite fazer com que um roteador da rede trabalhe com pacotes IPv4 e IPv6.
[14] Nodo pode ser entendido como sendo um nó, ou seja, equipamento que serve como ponto de interconexão de uma rede.

5.1.2 Mecanismo de tradução

O mecanismo de tradução consiste em possibilitar uma conversão do datagrama IPv6 em IPv4 quando houver a necessidade de trafegar datagramas IPv6 em roteadores IPv4. O mesmo ocorre ao tentar trafegar datagramas IPv4 em roteadores IPv6. Tal circunstância ocorre pelo fato do roteador trabalhar com apenas um destes protocolos, impossibilitando-o de realizar uma alternância de serviços como no caso da metodologia *Dual-Stack*. Por meio da tradução de pacotes máquinas e redes com versão de IP diferentes poderão se comunicar e trocar informações, como por exemplo, havendo uma máquina que interaja com outras duas que trabalhem com protocolos diferentes, esta por sua vez poderá acessar dados tanto de uma quanto da outra.

Existe uma circunstância de utilização da metodologia de tradução que poderá ocasionar alguma situação indesejável. Segundo Kurose (2003, p.270) na abordagem de Pilha Dupla, se o remetente ou o destinatário forem habilitados apenas ao IPv4, um datagrama IPv4 deverá ser usado. Como resultado, é possível que dois nós habilitados para IPv6 acabem enviando datagramas IPv4 um para o outro. Isso é ilustrado na Figura 09. Suponha que o nó A com IPv6 queira enviar um datagrama IP ao nó F que também possui IPv6. Os nós A e B podem trocar um pacote IPv6. Contudo, o nó B deve criar um datagrama IPv4 para enviar a C. É certo que o campo de dados do pacote IPv6 pode ser copiado para o campo de dados do datagrama IPv4 e o mapeamento do endereço adequado pode ser feito. No entanto, ao realizar a conversão de IPv6 para IPv4, haverá campos IPv6 específicos no datagrama IPv6 (por exemplo, o campo do identificador do fluxo) que não terão contrapartes em IPv4. As informações contidas nesses pacotes serão perdidas. Assim, mesmo que E e F possam trocar datagramas IPv6, os datagramas IPv4 que chegarem a E e F não conterão todos os campos que estavam no datagrama IPv6 original enviado de A.

Uma possível alternativa para resolver este tipo de problema, será abordado quando falarmos de mecanismos de tunelamento.

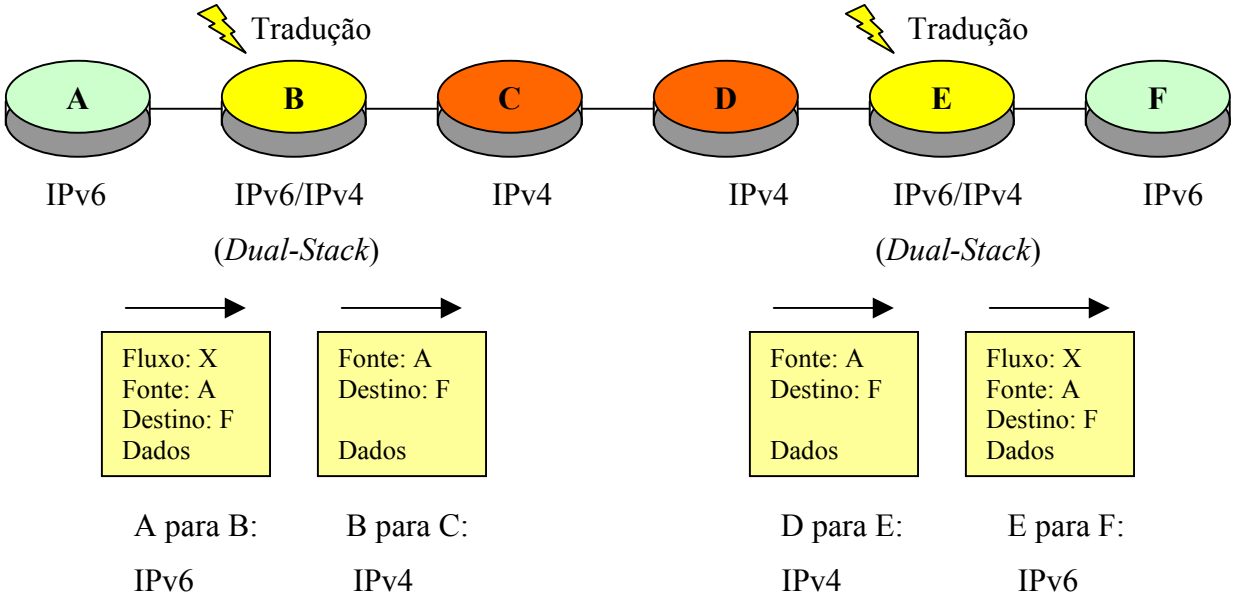


Figura 09 – Remetente e destinatário habilitados a IPv6 trafegando pacotes por nós IPv4. (KUROSE, 2003 , p.271).

5.1.3 Mecanismo de Tunelamento

Durante o período de implantação do IPv6 na rede, será necessário o uso de um mecanismo que solucione problemas de compatibilidade e que seja realmente eficiente, proporcionando uma convivência harmoniosa entre os dois protocolos. O mecanismo que já esta sendo implantado e utilizado com sucesso é a técnica de tunelamento. Esta técnica já se encontra bastante utilizada atualmente no projeto *6BONE* que consiste em formar ilhas de IPv6 funcionando em meio ao nosso grande mar de nós IPv4. O projeto *6BONE* será abordado posteriormente para melhor entendermos como o processo de atualização da rede esta sendo realizado.

O tunelamento consiste em encapsular um datagrama IPv6 dentro de um datagrama IPv4 permitindo a acessibilidade de nós e serviços IPv6 em meio a uma rede IPv4. Desta forma os pacotes passam por roteadores IPv4 sem que eles saibam que estão transportando protocolos IPv6. O método de transporte via túnel resolve o problema encontrado no exemplo anterior quando abordamos o emprego da metodologia de tradução. Vale a pena lembrar que a técnica de

tunelamento também faz uso do mecanismo de Pillha-Dupla (*Dual-Stack*), onde roteadores que trafegam tanto pacotes IPv6 quanto IPv4 são inseridos nas fronteiras entre as redes IPv6 e IPv4, permitindo desta maneira que se formem ilhas de IPv6. O objetivo é que estas ilhas de IPv6 se expandam até se encontrarem umas com as outras proporcionando uma atualização total da rede.

Segundo Dalazoana (2002, p.03), tunelamento pode ser usado em uma variedade de modos:

- **Roteador para Roteador** (*Router-to-router*). Roteadores *Dual-Stack* (IPv6/IPv4) interconectados por uma infra-estrutura IPv4 podem tunelar pacotes IPv6 entre eles. Neste caso, o tunelamento encaminha um segmento fim-a-fim que os pacotes IPv6 escolhem.
- **Hospedeiro para Roteador** (*Host-to-router*). *Hosts Dual-Stack* podem tunelar pacotes IPv6 para um roteador intermediário *Dual-Stack* que é alcançável via rede IPv4. Este tipo de tunelamento encaminha o primeiro segmento do caminho fim-a-fim do pacote.
- **Hospedeiro para Hospedeiro** (*Host-to-host*)**.** *Hosts Dual-Stack* que são interconectados por uma rede IPv4 podem tunelar pacotes IPv6 entre eles. Neste caso, é feito tunelamento do caminho inteiro em um segmento do caminho fim-a-fim dos objetos de pacote.
- **Roteador para Hospedeiro** (*Router-to-host*). Roteadores *Dual-Stack* podem tunelar pacotes IPv6 para o destino final do *host Dual-Stack*. Este túnel encaminha só o último segmento do caminho fim-a-fim.

> *Técnicas de tunelamento normalmente são classificadas de acordo com o mecanismo pelo qual o nó encapsulador determina o endereço do nó de destino do túnel. Nos primeiros dois métodos de tunelamento que são descritos acima (router-to-router e host-to-router) o pacote IPv6 está sendo tunelado para um roteador. O ponto final deste tipo de túnel é um roteador intermediário que deve desencapsular os pacotes IPv6 e encaminhar isto para seu destino final. Quando tunelado para um roteador, o ponto final do túnel é diferente do destino do pacote que é tunelado inicialmente. Assim o endereço no pacote IPv6 que é tunelado não provê o endereço IPv4 do ponto final do túnel. O endereço do ponto final do túnel deve ser determinado da informação de configuração sobre o nó que executa o tunelamento (DALAZOANA, 2002, p.04).*

Nos últimos dois métodos (*host-to-host* e *router-to-host*) o pacote IPv6 é tunelado inteiro para o seu destino final.

Para permitir a implementação do mecanismo de tunelamento podemos empregar duas técnicas que são:

- **Tunelamento Configurado.** É a forma de se estabelecer que tipo de túnel onde o ponto final é configurado. Segundo Telepac (2004) o endereço IPv6 é configurado manualmente numa interface de tunelamento. Os endereços IPv4 também são configurados manualmente nas extremidades desse túnel. As extremidades devem suportar transporte IPv4 e IPv6 e podem ser roteadores ou *hosts*.
- **Tunelamento Automático.** Segundo Dalazoana (2002, p.04) Determina-se o endereço do ponto final do túnel derivando-o a partir do endereço IPv4 embutido no pacote IPv6. Quando o endereço de ponto final do túnel é o mesmo do pacote IPv6 o endereço de ponto final do túnel adota este endereço de destino. Esta técnica evita a necessidade de se configurar explicitamente o endereço de ponto final do túnel.

Para melhor entendimento, na Figura 10 é mostrado como é a organização de uma rede que implemente o mecanismo de tunelamento.

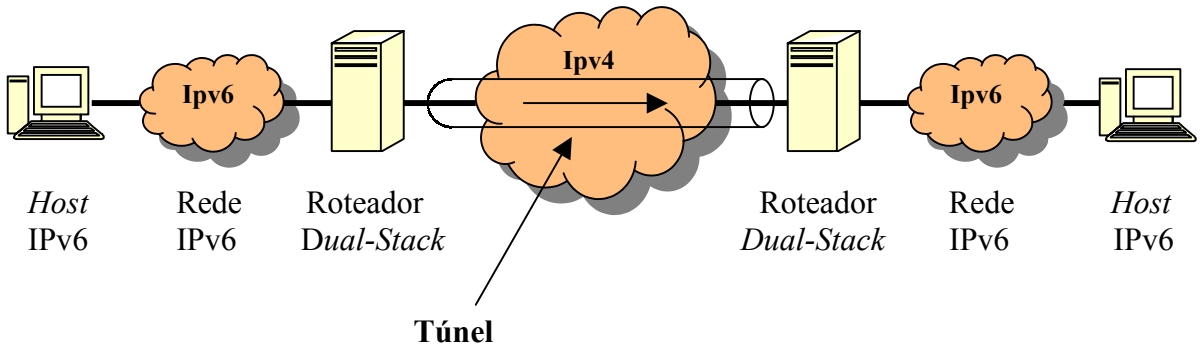
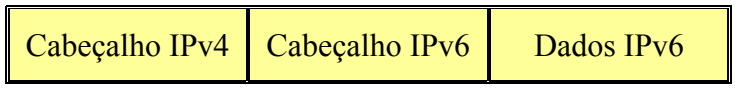


Figura 10 - Tunelamento de pacotes IPv6 inseridos em pacotes IPv4. (TELEPAC, 2004).

È mostrado na figura 11 a forma que um datagrama IPv6 assume após sofrer o encapsulamento para posteriormente ser tunelado.



Datagrama IPv6 encapsulado para trafegar
em meio a uma rede IPv4

Figura 11 - Datagrama IPv6 encapsulado dentro de um datagrama IPv4. (TELEPAC, 2004).

Como observado acima, o datagrama IPv6 após o encapsulamento tem o seu tamanho aumentado, o que pode gerar um aumento de fragmentação e carga na rede IPv4. O nó que encapsula o pacote IPv6 obtém informações do túnel e registra alguns parâmetros como o comprimento máximo que cada datagrama (MTU - *Maximum Transfer Unit*) pode atingir em cada túnel, possibilitando o processamento dos datagramas IPv6. Esta funcionalidade evita que datagramas sejam fragmentados nos roteadores reduzindo o processamento (W2K, 2004; GOMES, 2004).

5.2 Transição para o Protocolo IPv6 e o Projeto *6BONE*

A transição atualmente no mundo está se fazendo de uma forma lenta e gradativa. Segundo Martini (2003, p.07), em 1996 foi iniciado o projeto denominado *6BONE*, que é um *backbone*[15] internacional formado por *sites* IPv6 conectados através de túneis IPv4, visando servir como suporte a testes de implementação do protocolo IPv6 em diversas plataformas, além de servir como ponto de partida para a implementação do protocolo na *Internet*.

Segundo Martini (2003, p.07) atualmente, o projeto *6BONE* consiste em uma rede virtual que permite o transporte de pacotes IPv6 sobre redes físicas IPv4, formando um cenário composto por ilhas IPv6 que suportam diretamente o protocolo e comunicam-se entre si através de ligações virtuais ponto a ponto (túneis). As máquinas com protocolo IPv4 que compõem os túneis possuem um sistema operacional com suporte para IPv6 e utilizam protocolos de roteamento adequados à nova versão.

[15] *Backbone* - Representa a conexão principal entre dois ou mais grupos de rede de uma ou mais regiões diferentes.

O *6BONE* é conhecido mundialmente por ter servido de ponto inicial para a disseminação do protocolo IPv6, sendo que este projeto se tornou uma fonte muito importante para pesquisas e informações sobre o novo protocolo.

No Brasil, projetos similares ao *6BONE* internacional foram iniciados a um bom tempo. Estes projetos estão sendo difundidos pela RNP – Rede Nacional de Pesquisa e ainda se encontram em processo de consolidação, sendo a maio parte destes projetos realizadas em instituições de ensino e laboratórios de pesquisa por meio de pesquisas acadêmicas.

A RNP (Rede Nacional de Pesquisa) atualmente possui dois projetos relacionados ao uso do IPv6:

- *Backbone* RNP2 - Utiliza uma ligação com vários pontos da rede na presença da RNP. Porém, o diferencial é que somente são utilizadas ligações por meio do protocolo IPv6 em modo nativo, ou seja, nesta ligação somente é utilizado o protocolo IPv6 para interconexão em rede.
- Br6Bone - Projeto que visa o envolvimento de instituições que se interessem em implementar o uso desta nova tecnologia em suas redes internas. O funcionamento desta é feita pelo emprego de tunelamento através de nossa estrutura IPv4 atual.

Segundo Martini (2003, p.07) a disponibilidade destes serviços oferecidos pela RNP, abre novas perspectivas para o desenvolvimento do IPv6 no país, a medida que permite à mesma estabelecer parcerias com instituições, inclusive do setor privado, possibilitando explorar novos protocolos, serviços e aplicações em ambientes IPv6. Estas instituições ligadas a RNP podem participar de uma rede de pesquisas com alcance internacional. Diversas universidades como Unicamp, UFRGS e UFBA, além de provedores comerciais, como a Rede Pegasus, participam do projeto.

Para contribuir com a expansão do IPv6 basta tomar a posição adotada por estas organizações que acreditaram e desenvolveram com auxílio do projeto *6BONE*, uma rede IPv6 pura em suas redes internas. Com o aumento destas redes IPv6 puras, será possível começar a investir em novos equipamentos adequados para este novo protocolo.

5.3 Implantação do Protocolo IPv6

Para que ocorra uma significativa implantação do protocolo IPv6 na *Internet,* é necessário que também seus equipamentos sejam trocados por equipamentos especializados em IPv6. Uma transição de protocolo em quase toda a *Internet* pode se estender por um tempo indeterminado, devido ao alto investimento recente na compra de *hardware* e *software* especializados em trabalhar com datagramas IPv4.

Atualmente, realizar um grande investimento em *hardware* e s*oftware* especializados IPv6 seria demasiadamente caro para as empresas, devido ao fato de que na maioria dos casos, ter sido realizado um grande investimento em equipamentos IPv4. Contudo foi visto que o protocolo IPv6 possui a técnica de tunelamento para que a transição seja possível sem que haja a necessidade imediata da troca de equipamentos. Uma desvantagem do IPv6 é o alto custo de *hardware* para atualizar sistemas e redes.

6 CONCLUSÃO

Vemos nos dias atuais como é crescente a demanda por recursos de rede que proporcionem um bom serviço de comunicação. A comunicação envolvendo redes de computadores está presente nas mais diversificadas áreas de trabalho. A cada ano, mais pessoas se conectam a *Internet* para desfrutar de suas potencialidades bem como suas facilidades.

Para que a *Internet* não pare de crescer necessitamos que haja números de IP suficientes para que este serviço continue expandindo. Várias técnicas foram implantadas para retardar o esgotamento dos endereços IP. Os principais fatores que impulsionaram o surgimento do protocolo IPv6 foram as deficiências em segurança do protocolo IPv4 e a escassez de endereços IP, que, aliás, é um protocolo que foi criado principalmente voltado para segurança.

Diversas características tornaram o IPv6 um grande avanço em relação ao IPv4. Destaca-se o formato de cabeçalho simplificado e de tamanho fixo que diminuíram o tempo de processamento do mesmo pelos roteadores da rede, suporte a cabeçalhos de extensão, o aumento de capacidade para bilhões de endereços IP, suporte a autoconfiguração, controle de fluxo e de hierarquia de datagramas, dentre outros. Quando falamos de segurança, o IPv6 já a possui em sua implementação. Desta forma ele pode realizar uma proteção mais eficaz agindo diretamente na camada de rede ao invés de atuar na camada de aplicação como o IPv4.

Devido ao alto investimento realizado a alguns anos na compra de equipamentos e roteadores especializados em trabalhar com o protocolo IPv4, o processo de transição para o IPv6 ainda deve durar algumas décadas. Por meio da utilização da técnica de tunelamento será possível trafegar datagramas IPv6 através de redes IPv4 até chegarmos ao ponto em que todos os computadores passem a utilizar o IPv6. É essencial que todos se mobilizem para esta transformação que a *Internet* está sofrendo e comecem desde já a atualizar seus computadores adotando este novo protocolo, pois, somente desta forma a rede estará apta para uma troca definitiva de protocolo. Gradativamente, os equipamentos deverão ser trocados por equipamentos específicos para trabalhar em cima do protocolo IPv6, neste momento iremos saber que a *Internet* estará se tornando mais segura e fornecendo serviços de forma mais eficiente aumentando a qualidade de comunicação no mundo todo.

6.1 Trabalhos Futuros

Como sugestão para realização de Trabalhos Futuros, alguns pontos poderiam ser abordados, dentre eles:

1. Implementação do Protocolo IPv6 em uma rede interna;
2. Transmissão em tempo real de vídeo e áudio utilizando o protocolo IPv6;
3. Segurança em redes sem fio utilizando IPv6;
4. Técnicas de invasão sobre IPv6;
5. Integração dos protocolos IPv6 e ATM em redes de alta performance;
6. Análise de performance do protocolo IPv6 em relação ao IPv4.

BIBLIOGRAFIA

ANDREOLI, Andrey Vedana. IP Security (IPSEC). **Internet Protocol Journal,** March 2000, V.3, N.1, FCCN - Fundação para a Computação Científica Nacional de Portugal. Disponível em: <http://www.cert-rs.tche.br/docs_html/ ipsec.html>. Acesso em: 17 de maio 2004

ANTON, Eric Ricardo. **Protocolo IPv6**. UFRJ - Universidade Federal do Rio de Janeiro. Disponível em: <http://www.gta.ufrj.br/grad/99_2/eric/seguranca.htm> Acesso em: 27 de mar. 2004.

COMER, Douglas E. **Interligação em Rede com TCP/IP**. 5.ed. Rio de Janeiro: Campus, 1998. 672 p.

COSTA, Julio Soares Firmo da; FIALHO, Sergio Viana. **Implementação de um mecanismo de tradução de protocolos (IPv4 e IPv6) - NAT-PT/DNS-ALG**. RNP - Rede Nacional de Ensino e Pesquisa - Universidade Federal do Rio Grande do Norte (UFRN) 30 de julho de 2003. Disponível em: <http://www.rnp.br/newsgen/0303/trad_protocolo.html**>.** Acesso em: 23 de maio 2004.

DALAZOANA, Paulo Roberto; RYMSZA, Rodrigo; SAVA, Ewerton Luis. **Técnicas de integração IPv4 e IPv6**. Universidade Católica do Paraná, 2002. Disponível em: <http://www.ppgia.pucpr.br/~jamhour/Download/pub/ArtigosPos/Projeto_ipv4_ipv6.pdf>. Acesso em: 10 de abr. 2004.

DEERING, S; Hinden, R.. **RFC1883:**Internet Protocol Version 6 (Ipv6). Disponível em: <http://www.ietf.org/rfc/rfc1883.txt?number=1883>.

DOTTI, Fernando Luis. **Redes de Computadores**. Faculdade de Informática – PUCRS. Disponível em: <http://www.inf.pucrs.br/~fldotti/redes/aulas/redes4b-nivelrede-ipv6.pdf>. Acesso em: 13 maio 2004.

GOMES, Ader Artur Pereira. **Introdução ao IPv6**. Laboratório de Sistemas Integráveis Escola Politécnica - Universidade de São Paulo, São Paulo. Disponível em: <http://www.lsi.usp.br/ ~ader/ introducaoipv6.pdf>. Acesso em: 15 de jun. 2004.

HINDEN, R.; Deering, S.. RFC1884: **IP Version 6 Addressing Architecture**. Disponível em: <http://www.ietf.org/rfc/rfc1884.txt?number=1884>.

KUROSE, James F.; ROSS, Keith W.. **Redes de Computadores e a Internet: Uma Nova Abordagem**. São Paulo: Addison Wesley, 2003.

MARTINI, Fernando Zacuni; BOGO, Madianita. **Análise e Proposta de Implantação de um Ambiente de Rede utilizando o Protocolo IPv6**. Centro Universitário Luterano de Palmas; Encontro de Estudantes de Informática do Tocantins. Palmas, TO. outubro, 2003. pp. 381-390. Disponível em: <http://www.ulbra-to.br/ensino/43020/artigos/anais2003/anais/ipv6-encoinfo 2003.pdf>. Acesso em: 13 de maio 2004.

MOREIRA, Edson dos Santos; MARTINS, Luciano. **Uso do Protocolo IPv6 e de Multicasting para Transmissão de Vídeo**. ICMC - Instituto de Ciências Matemática e de Computação - Universidade de São Paulo - São Carlos – SP. Disponível em: <http://www.rnp.br/wrnp2/2001/palestras_engenharia/res_engen_13.pdf>. Acesso em: 10 de abr. 2004.

NEED, Frank. **A Nova Geração de Protocolos IP**. Disponível em: <http://www.absoluta.org/tcp/tcp_ipv6.htm#p7>. Acesso em: 10 de abr. 2004.

OLIVEIRA, Frank Ned Santa Cruz de. **A Nova Geração de Protocolo IP**. RNP - REDE NACIONAL DE PESQUISA. Disponível em: <http://www.rnp.br/newsgen/9811/intr-ipv6.html> Acesso em: 27 de mar. 2004.

PUTTINI, Ricardo S; SOUZA, Rafael T. de**. IPSEC - Internet Protocol Security.** UnB - Departamento de Engenharia Elétrica. Disponível em: <https://www. redes.unb.br/security/firewall/ipsec.html#areas%20funcionais>. Acesso em: 13 de abr. 2004.

RODRIGUES, Adriane Pires. **Comparação do Protocolo IPv4 com o IPv6**. Disponível em: <http://docentes.uportu.pt/darioc/cdr/Ipv6%20versus%20Ipv4.html>. Acesso 10 de maio 2004.

SILVA, Adailton J. S.. O IPv6 na RNP e no Brasil. **Revista RNP NewsGeneration**, V.2, N.7, 14 de outubro de 1998. Disponível em: <http://www.6bone.rnp.br/ipv6-artigo.html>. Acesso em: 01 de out. 2004.

SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sergio. **Redes de Computadores: das LANS, MANS e WANS as redes ATM**. 2.ed. Rio de Janeiro: Campus, 1995. 705 p.

SOUZA,Gilberto. **IPv6 - Características do IP Next Generation**. Clube das Redes - Rio de Janeiro 27 de Maio de 2004. Disponível em: <http://www.clubedasredes.eti.br/ rede0019.htm>. Acesso em: 23 de maio 2004.

TANENBAUM, Andrew S. **Redes de Computadores**. 3.ed. Rio de Janeiro: Campus, 1997. p.923.

TELEPAC. O novo nome da internet. **IPv6 - Caracteristicas do IP Next Generation**. Disponível em: <http://www.ipv6.telepac.pt/info.php>. Acesso em: 17 de maio 2004.

UNIVERSIDADE DE SÃO PAULO. **Introdução ao IPv6**. Disponível em: <http://www.lsi.usp.br/~ader/introducaoipv6.pdf**>.** Acesso em: 17 de maio 2004.

W2K. **Material sobre IPv6 e ATM, só mesmo na W2K**. Disponível em: <http://w2k.com.br/images/SID/IPV6_ATM/ipv6atm.htm>. Acesso em: 20 de maio 2004.