Índice

1.0 - Introdução

O protocolo IP, Internet Protocol, provê funções de endereçamento e roteamento e sua padronização é feita através de RFCs – Request for Comments, que são documentos que indicam as funções básicas de qualquer protocolo. Atualmente a versão do IP que é utilizada é a versão 4 (Ipv4), porém o que se verifica é que esta versão está chegando ao seu limite de utilização e que possui uma série de restrições que citaremos a seguir:

- **Crescimento e popularização da Internet**

O protocolo IP possui 32 bits para endereçamento, o que fornece cerca de 4 bilhões de endereços possíveis. Esses dados levavam a pensar que esse número de endereços era suficiente para todos os hosts na internet, porém com o crescimento fenomenal da Internet ocasionado principalmente pela sua grande popularização nesta década, chegará num ponto que eles não serão suficientes, mostrando-se um recurso baixo devido ao crescimento exponencial de hosts conectados à Rede.

- **Novas Aplicações**

Com a utilização crescente da Internet, uma grande quantidade de aplicações foram criadas e pensadas. As aplicações necessitaram de facilidade e serviços que não poderiam ser providos pelo IP atual. Um exemplo deste tipo de serviço é a multimídia, que necessita de transmissões de vídeo e som pela rede. Isto implica em um protocolo que permita uma taxa de entrega de dados em intervalos regulares.

- **Negócios na Internet**

Com o crescimento de trocas comerciais na Rede Mundial surge a necessidade de que os dados transmitidos tenham autenticação, privacidade e integridade. Na verdade a definição atual do protocolo em questão, permite que um usuário com conhecimentos básicos utilize ferramentas e técnicas que faz o ambiente da rede, totalmente inseguro por permitir que os dados transmitidos possam ser capturados ou por não se ter certeza se o host em contato é mesmo aquele que diz ser.

Devido a essas limitações começou-se a verificar que uma nova versão do IP fazia-se necessária para suportar um endereçamento muito maior e prover suporte ao problema de escalabilidade, logo, em meados de 1994 foi sugerido o novo protocolo IP. Este protocolo teria 128 bits e se chamaria Ipv6.

2.0 - Objetivos

O Ipv6, também conhecido como IPng (IP Next Generation) é um incremento natural do Ipv4, essa nova versão introduz melhoramentos significativos, verificados a partir da utilização do Ipv4, a nível de endereçamento, encaminhamento e segurança e apresenta os seguintes objetivos:

- solucionar problemas de endereçamento do IPv4 (reserva e utilização de espaço, divisão de redes, eliminação de parâmetros não utilizados);
- evitar saturação das tabelas de encaminhamento na Internet;
- introduzir mecanismos de transição para uma passagem transparente e gradual do protocolo IPv4 para IPv6;
- introduzir mecanismos de segurança na camada de rede;
- providenciar suporte para aplicações multimédia e em tempo-real.

Vale ressaltar que o novo protocolo mantêm as características que contribuíram para o sucesso do IPv4. Exemplo dessas características são: serviço não orientado a conexão, decisão de escolha do tamanho do pacote, o número máximo de roteadores a serem utilizados, facilidade de fragmentação e roteamento.

3.0 - Características

As características mais importantes do IPv6 são:

- **Extensão das capacidades de endereçamento**

O tamanho de endereços passa de 32 bits na versão 4 para 128 bits no IPv6, o que permite o suporte de um número muito superior de nós finais e uma melhor hierarquização do espaço de endereçamento essencial à escalabilidade.

- **Simplificação do cabeçalho**

Alguns campos do cabeçalho IPv4 foram retirados ou passaram a ser opcionais de forma a simplificar o tratamento de um pacote comum. Embora os endereços IPv6 sejam 4 vezes maiores do que endereços IPv4 o cabeçalho é apenas duas vezes maior (40 bytes).

- **Suporte para autenticação e privacidade**

O protocolo IPv6 inclui as definições de extensões que permitem a autenticação e confidencialidade de comunicações ao nível de rede.

- **Suporte de auto-configuração**

Quando se instala uma estação cliente numa rede Netware, automaticamente, é assinalado um endereço IPX para este cliente. Esta característica de autoconfiguração, denominada "stateless autoconfiguration", estará presente no IPv6. Isso eliminará a necessidade de se configurar manualmente as estações da rede.

- **Suporte para seleção de rota pelo originador**

O IPv6 inclui uma extensão que permite a especificação de rota pelo originador desenhada para se integrar com a utilização do protocolo “Source Demand Routing Protocol” (SDRP). Este protocolo tem por objetivo a seleção de rotas pelo originador de forma a completar o encaminhamento de pacotes com base na informação fornecida pelos protocolos de routing intra e inter-domínio correntes. Esta opção permite não só, controlar o tráfego na rede, como também aumentar a segurança na transmissão da informação.

- **Transição simples e flexível**

Uma das características chave do protocolo IPv6 é um plano de transição simples que permita a instalação incremental de nós IPv6 no ambiente atual. Este plano contempla a instalação de nós IPv6 sem exigir qualquer dependência em relação a outros nós e permitindo o endereçamento de nós IPv6 com base nos endereços IPv4 já atribuídos.

- **Suporte para tráfego com garantia de qualidade de serviço**

O cabeçalho IPv6 contém um campo de fluxo destinado a ser utilizado em conjunto com um protocolo de reserva de recursos de forma a permitir a utilização de qualidade de serviço garantida.

- **Suporte para Jumbograms**

Possibilidade de enviar pacotes com dimensão superior a 64Kb. O limite de um pacote Jumbogram é de 4Gb. Esta propriedade é útil para as redes com grande largura de banda.

- **Segurança**

As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho (authentication header) ou autenticação IP, e a segurança do encapsulamento IP (encrypted security payload).

A autenticação de cabeçalho assegura ao destinatário que os dados IP são realmente do remetente indicado no endereço de origem, e que o conteúdo foi entregue sem modificações. A autenticação utiliza um algoritmo chamado MD5 (Message Digest 5), especificado em [RFC1828].

A segurança do encapsulamento IP permite a autenticação dos dados encapsulados no pacote IP, através do algoritmo de criptografia DES (Data Encryption Standard) com chaves de 56 bits, definida em [RFC1829].

Os algoritmos de autenticação e criptografia citados acima utilizam o conceito de associação de segurança entre o transmissor e o receptor. Assim, o transmissor e o receptor devem concordar com uma chave secreta e com outros parâmetros relacionados à segurança, conhecidos apenas pelos membros da associação. Para gerenciar as chaves provavelmente será utilizado o IKMP (Internet Key Management Protocol), desenvolvido pelo grupo de trabalho em Segurança IP.

- **Suporte a Servicos em Tempo Real**

Os campos "priority" e "flow label" foram criados especialmente para facilitar o desenvolvimento de protocolos para controle de trafego em tempo real, como o RSVP (Resource Reservation Protocol), de forma a permitir a implementação de uma Internet com aplicações multimídia e com a integração de serviços de dados, voz e vídeo em tempo real.

4.0 - O pacote IPv6

O IPv6 modifica totalmente o formato do pacote. A figura abaixo mostra o formato geral. O pacote é formado por uma parte fixa, o cabeçalho base, seguido de zero ou mais extensões de cabeçalho, logo depois vem o dado (carga útil ou payload).

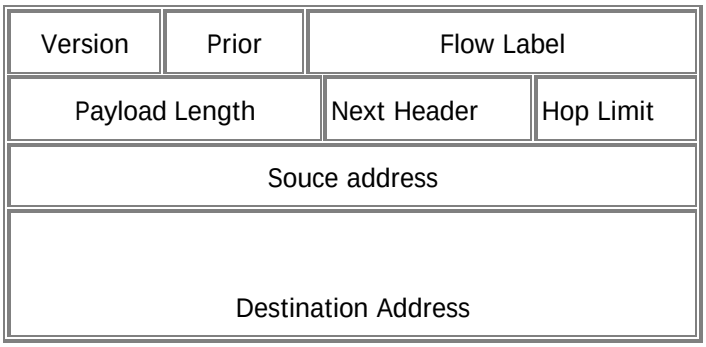
Cabeçalho Base	Extensão de Cabeçalho	...	Extensão de Cabeçalho	Dados

Apesar de prover mais endereçamento o cabeçalho do IPv6 contém menos informações que o de IPv4. As principais mudanças ocorridas no cabeçalho foram:

- algumas informações que aparecem no cabeçalho do IPv4 foram colocadas como opcionais, visando diminuir o processamento;
- o tamanho do campo de endereços foi alterado para dezesseis octetos, contra os quatro da versão anterior;
- os campos de fragmentação passam a fazer parte das opções, através dos cabeçalhos de extensão. Existe um grande esforço para que ela ocorra somente fim a fim, ou seja, da origem para o destino;

4.1 - Cabeçalho base Ipv6

Outra característica importante do IPv6 é o seu novo e simplificado formato de cabeçalho. O cabeçalho IPv6 é constituído por um cabeçalho inicial de 64 bits, seguido dos endereços de origem e destino de 128 bits, totalizando 40 bytes. A simplificação no formato do cabeçalho está na remoção de alguns campos ou a simples locomoção dos mesmos para outros cabeçalhos opcionais, chamados cabeçalhos de extensão. A redução ocorreu nas informações de controle. Esta simplificação otimiza o tempo de processamento por pacote em um roteador.



, onde:

O campo de *Version* (4 bits) tem a mesma função do IPv4. Ele é sempre 6 para IPv6.

O campo *Priority* (4 bits) é utilizada para dar prioridade distintas aos pacotes. Ele diferencia os pacotes que podem ter controle de fluxo, dos que não podem. Os valores de 0 a 7 dão destinados a protocolos capazes de diminuir o fluxo de envio caso ocorra o congestionamento. Para pacotes de aplicações em tempo real que são enviados a taxa constante, valores de 8 a 15 dizem quais pacotes podem ser descartados com prioridade maior para valores mais altos.

Os roteadores baseados no IPv4, normalmente, tratam todo o tráfego de forma igual. Já os roteadores IPv6 devem analisar a prioridade do tráfego para decidirem o que fazer:

Valor da Prioridade	Ação
0 – 7	Iniciar a eliminação (drop) dos pacotes quando a rede estiver congestionada (Congestionamento controlado)
8 – 15	Tentar despachar os pacotes, mesmo que os pacotes de menor prioridade estejam sendo eliminados (dropped)

O campo *Flow Label* - Identificador de fluxo (24 bits). Consiste num valor arbitrário que pode ser utilizado pelo originador para identificar pacotes para os quais tenha requerido uma determinada qualidade de serviço por meios externos ao protocolo IP em si. Um fluxo é uma sequência de pacotes enviados por um determinado originador a um destino específico para o qual o originador deseja um tratamento especial no encaminhamento de pacotes.

O campo *Payload Lenght* (16 bits) determina o tamanho do pacote, em octetos, excluindo-se o cabeçalho base . O *total Length* do IPv4, dava o valor total do pacote incluindo o cabeçalho.

O campo *Next Header* (8 bit's) indica a existência de cabeçalho adicionais ou caso não exista o protocolo da camada superior (TCP ou UDP). Esta característica inclui dois compromissos: a generalização e a eficiência. A generalização é conseguida com a inclusão de funções adicionais, como fragmentação, roteamento na origem e autenticação. A eficiência é conseguida a partir do momento que se não forem preciso estas características os seus campos não necessitam estar presentes.

A figura abaixo mostra como são utilizados os cabeçalhos de extensão. Cada cabeçalho contém o campo *Next Header* que aponta para o próximo campo, o ultimo cabeçalho indica qual protocolo da camada de transporte será utilizado. É utilizado o mesmo princípio de uma lista encadeada.

Cabeçalho Base NEXT=ROUTER	Cabeçalho de Roteamento NEXT=AUTH	Cabeçalho de autenticação NEXT=TCP	Segmento TCP (dados

Exemplo de cabeçalho com duas extensões

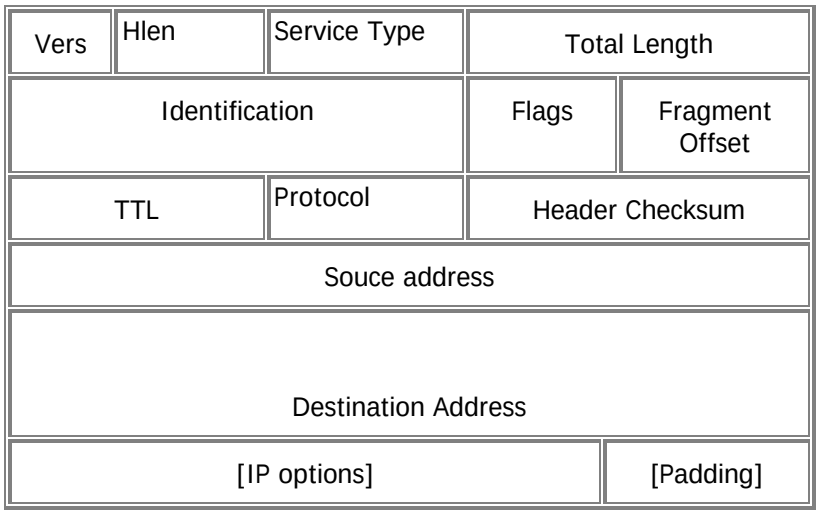
Hop Limit (8-bits, inteiro, sem sinal) e é decrementado de 1 para cada nó que segue o pacote. Este campo é semelhante ao campo TTL, mas agora com a medida em hops e não em segundos. Isto foi trocado por duas razões:

- O IP, normalmente, despacha pacotes mais rápido do que a freqüência de um hop por segundo e o campo TTL é sempre decrementado em cada hop, tal que na prática ele é medido em hops e não em segundos;
- Muitas implementações IPv6 não descartam pacotes na base do tempo transcorrido. O pacote é descartado se o Hop Limit for decrementado para zero.

O campo *Source e Destination Address* indicam respectivamente o endereço de origem e de destino do pacote, como diferencial do IPv4 tem o fato de se usar 128 bits ao invés de 32 bits daquela versão.

4.2 - Comparação entre o cabeçalho do IPv4 e IPv6

Como dito anteriormente, o cabeçalho IPv4 foi simplificado no IPv6. Uma comparação entre os formatos dos cabeçalhos IPv4 e IPv6 mostrará que o número de campos do cabeçalho IPv4 não tem uma equivalência direta no cabeçalho IPv6.



Cabeçalho IPv4

Enquanto o cabeçalho do IPv4 possui 10 campos de cabeçalho, dois endereços de 32 bits cada, e algumas opções, o cabeçalho IPv6 compõe-se apenas de 6 campos de cabeçalho e dois endereços 128 bits cada. Os seis campos de cabecalho sao: version (4 bits), priority (4 bits), flow label (28 bits) e length of the payload (16 bits).

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

- Type of Service - será manipulado pelo IPv6 usando-se o conceito de fluxos;
- Identification, os flags de Fragmentação e Fraggment Offset – no IPv6, os pacotes fragmentados têm um cabeçalho de extensão, ao invés de constituirem-se como informações de fragmentação no cabeçalho-base IPv6. Desde que os protocolos de nível mais alto, particularmente o TCP, tendem evitar a fragmentação dos pacotes, isto reduzirá o overhead do cabeçalho-base para os casos normais. Como será visto adiante, o IPv6 não fragmenta pacotes na rota até ao destino, e sim, somente na origem;

- Header Checksum – Devido aos protocolos de transporte já implementarem o checksum e porque o IPv6 já inclui um cabeçalho de Autenticação (que pode ser usado para garantir a integridade), o IPv6 não fornece o monitoramento checksum dos pacotes IP. Ambos, TCP e UDP incluem um pseudo-cabeçalho IP em seus checksums, tal que nestes casos, o cabeçalho IP no IPv4 está sendo checado duas vezes. Os protocolos TCP e UDP e quaisquer outros protocolos que usam o mesmo mecanismo de checksum, rodando sobre o IPv6, continuarão a usar um pseudo-cabeçalho IPv6, apesar de que, obviamente, o pseudo-cabeçalho será diferente do pseudo-cabeçalho IPv4. O ICMP e o IGMP e quaisquer outros protocolos que não usem um pseudo-cabeçalho IP sobre IPv4 usam um pseudo-cabeçalho IPv6 em seus checksums.

As simplificações mais consideráveis do IPv6 foram a alocação de um formato fixo para todos os cabeçalhos, a remoção do checksum de cabeçalho e remoção dos procedimentos de segmentação "hop-by-hop".

A remoção de todos os elementos opcionais não significa que não se possa configurar serviços especiais. Estes poderão ser obtidos através de cabeçalhos denominados "extension headers", que são anexados ao cabeçalho principal.

A cada salto de um pacote IPv6, os roteadores não precisarão se preocupar com o calculo do tamanho do cabeçalho, que é fixo, com o calculo do checksum do cabeçalho, e nem com as tarefas de fragmentação, que serão realizadas pelos hosts. Todas estas modificações aumentarão substancialmente o desempenho dos roteadores.

5.0 - Cabeçalhos de Extensão [RFCs 1883, 1826 e 1827]

Os campos do cabeçalho IPv6 são significativamente menos do que os do IPv4, note-se por exemplo a ausência de qualquer tipo de informação relativamente a fragmentação. O que acontece é que muitos campos passaram a ser opcionais sob a forma de cabeçalhos de extensão. Trata-se de cabeçalhos adicionais que circulam "encapsulados" no "pacote" IPv6.

Cada pacote IPv6 inicia-se com um cabeçalho-base. Na maioria dos casos, este será o único cabeçalho necessário para transmitir o pacote. Algumas vezes, entretanto, são necessárias informações adicionais para serem conduzidas com o pacote até o seu destino final ou até sistemas intermediários na rota (informações que deveriam, previamente, ter sido carregadas no campo Option do pacote IPv4) A informação respeitante a opções é codificada, no IPv6, em cabeçalhos separados que podem ser colocados entre o cabeçalho IPv6 e o cabeçalho do protocolo de transporte, esses são os cabeçalhos de extensão.

No IPv6, as informações opcionais da camada Internet são codificadas em cabeçalhos separados que podem ser colocados entre o cabeçalho-base IPv6 e um cabeçalho de camada-superior em um pacote. O número de cabeçalhos de extensão é pequeno, cada um é identificado por um valor distinto de Next Header. Como ilustrado abaixo, um pacote IPv6 pode carregar zero, um, ou mais cabeçalhos de extensão, cada um identificado pelo campo

Next Header do cabeçalho precedente. Os cabeçalhos de extensão são contados como parte do tamanho da carga útil (payload length).

Exemplo 1

Cabeçalho IPv6 Next Header = TCP	Cabeçalho TCP + dados

Exemplo 2

Cabeçalho IPv6 Next Header = 43 (cabeçalho de Roteamento)	Cabeçalho de Roteamento Next Header = TCP	Cabeçalho TCP + dados

Exemplo 3

Cabeçalho IPv6 Next Header = 43 (cabeçalho de Roteamento)	Cabeçalho de Roteamento Next Header = 44 (cabeçalho de Fragmento)	Cabeçalho de Fragmento Next Header = TCP	Cabeçalho TCP + dados

Os cabeçalhos de extensão devem ser processados, estritamente, na ordem em que eles aparecem no pacote: o receptor não deve, por exemplo, examinar através do pacote procurando por um tipo específico de cabeçalho de extensão e processá-lo com prioridade aos seus precedentes. Todos os cabeçalhos de extensão são opcionais.

O tamanho de cada cabeçalho varia, dependendo de seu tipo, mas é sempre um múltiplo de 8 bytes. Há um número limitado para cabeçalhos de extensão; eles devem aparecer somente uma vez em cada pacote (com exceção do cabeçalho de Opções de Destino que pode aparecer mais do que uma). A ordem dos cabeçalhos, importante para o processamento eficiente dos roteadores, é estabelecida pelos nós que originam os pacotes. Esta ordem é de acordo com os números (ordem crescente, com exceção do cabeçalho 60). Os roteadores, geralmente, só se interessam pelos cabeçalhos de Opções Hop-by-Hop e de Roteamento, portanto, após lê-los, eles não precisam prosseguir na leitura do pacote, podendo despachá-lo imediatamente.

O IPv6 permite o encapsulamento do próprio IPv6, denominando esta ação de tunneling. Isto é feito, usando-se um Next Header igual a 41 (o cabeçalho-base). Com exceção do cabeçalho de Opções Hop-by-Hop e, algumas vezes, do cabeçalho de Opções de Destino, os cabeçalhos de extensão não são processados por todos os nós ao longo da rota do pacote.

Eles carregam informações que devem ser examinadas e processadas por cada nó ao longo do caminho de transmissão do pacote, incluindo os nós nó-origem e nó-destino. O cabeçalho de Opções Hop-by-Hop, quando presente, deve seguir imediatamente o cabeçalho-base IPv6. Sua presença é indicada pelo valor zero no campo Next Header do cabeçalho-base IPv6.

Se, como resultado de um processamento de um cabeçalho, um nó é requisitado para processar para o próximo cabeçalho, mas o valor do Next Header no corrente cabeçalho não é reconhecido pelo nó, este deverá descartar o pacote e enviar uma mensagem de erro ao originador por ICMP - Internet Control Message Protocol.

5.1 - Ordem dos Cabeçalhos de Extensão [RFC 1883]

Quando existe todas as opções de cabeçalho de extensão no pacote, a ordem deve ser a seguinte:

(41) Cabeçalho-base IPv6

(0) Cabeçalho de Opções Hop-by-Hop

(60) Cabeçalho de Opções de destino

(43) Cabeçalho de Roteamento

(44) Cabeçalho de Fragmento

(51) Cabeçalho de Autenticação

(50) Cabeçalho de Encapsulamento de Segurança do Payload
(nota 2)

(60) Cabeçalho de Opções de destino

Cabeçalho de camada-superior

Cada cabeçalho deveria ocorrer apenas uma vez, exceto para o cabeçalho de Opções de Destino que deveria ocorrer no máximo duas vezes (uma vez antes do cabeçalho de Roteamento e uma vez antes do cabeçalho de camada-superior).

Se o cabeçalho da camada-superior é outro cabeçalho-base IPv6 (neste caso, o IPv6 está sendo tunneled - ou encapsulado – sobre o IPv6), ele pode ser seguido por seus próprios cabeçalhos de extensões, que são, separadamente, sujeitos às mesmas recomendações de ordenação.

Quando outros cabeçalhos de extensão forem definidos, suas restrições de ordenação relativas aos cabeçalhos listados acima devem ser especificadas.

Os nós IPv6 devem aceitar e tentar processar cabeçalhos de extensão em qualquer ordem e que ocorram qualquer número de vezes no mesmo pacote, exceto, somente, para o cabeçalho de Opções Hop-by-Hop que é restrito para aparecer imediatamente após o cabeçalho-base IPv6. De qualquer forma, é extremamente aconselhado que as origens dos pacotes IPv6 sigam à ordem recomendada acima até que outras especificações revisem esta recomendação.

5.2 - Descrição dos Cabeçalhos de Extensão

Os cabeçalho de extensão foram criados com a finalidade de fornecer informações adicionais relativas as facilidades utilizadas por um determinado Datagrama. A tabela abaixo mostra os seis cabeçalhos atualmente definidos. Uma descrição de cada um é dado logo a seguir.

Cabeçalho de extensão	Descrição
Hop-by-hop	Informações diversas para os rotedores
Routing	Rota parcial ou integral a ser seguida
Fragmentation	Fragmentação do pacote IP
Authentication	Verificação da identidade do pacote
Encrypted security payload	Informações sobre o conteúdo encriptado
Destination options	Informações adicionais para o destino

Cabeçalhos de extensão do IPv6

5.2.1 - Hop-by-hop Options e Destination Options

Os cabeçalhos *Hop-by-Hop e Destination Options* possuem o mesmo formato, como mostrado na figura abaixo:

0	8	16 31
NEXT HEADER	HEADER LENGTH	
ONE OR MORE OPTIONS		

Formato do Hop-by-hop e Destination Options

O campo *Next Header* diz o tipo de cabeçalho que vem a seguir.

O campo *Header Lenght* indica o tamanho total do cabeçalho, pois este cabeçalho não possui tamanho fixo.

A área *ONE OR MORE OPTIONS* representa uma seqüência de opções individuais. Cada opção é composta pelos campos *TYPE, LENGTH e VALUE* segundo pode ser visto na figura abaixo:

0	8	16
TYPE	LENGTH	VALUE **...**

Formato das opções individuais dos cabeçalho de opções

Os dois bits de mais alta ordem do campo *TYPE* especifica como os roteadores irão tratar as opções, se estas não forem compreendidas conforme a tabela abaixo.

Dois bits de mais alta ordem	Ação
00	Desconsidere esta opção
01	Descarte o pacote e não envie uma mensagem ICMP
10	Descarte o pacote e envie uma mensagem ICMP
11	Descarte o pacote e envie uma mensagem ICMP para endereços não Multicast

Tratamento das opções que não forem compreendidas pelo roteador

Os 5 bits de mais baixa ordem do campo TYPE indicam a opção propriamente dita. O terceiro bit de mais alta ordem indica se os dados desta opção poderão mudar ou não durante o percurso do pacote.

A diferença entre *Hop-by-Hop e Destination*, é que o primeiro deve ser processado por todos os roteadores, enquanto o segundo somente pelo destino.

Hop-by-Hop é usado para transportar informação opcional que tem de ser examinada por cada nodo ao longo do caminho do pacote.

Destination Options é usado para transportar informação opcional a ser analisada apenas no destino do pacote.

5.2.2 - Fragmentation

O IPv6, assim como o IPv4, implementa a fragmentação do pacote. A grande diferença se dá na maneira com que isto ocorre. No IPv4 cada roteador intermediário deveria fragmentar e reorganizar pacotes. No IPv6, a fragmentação é feita na origem, antes de enviar um

pacote, e não ocorre nos roteadores intermediários. Caso haja a necessidade de uma fragmentação não esperada nos rotedores intermediários (mudança de rotas) eles encapsulam o datagrama em um novo e o fragmenta. A figura abaixo mostra o formato do cabeçalho de fragmentação.

0	8	16	29	31
NEXT HEADER	RESERVED	FRAGMENT OFF SET	RES	MF
IDENTIFICATION				

Formato do cabeçalho de fragmentação

O campo *Next Header* indica como foi explicado anteriormente, o próximo cabeçalho de extensão.

O campo *Reserved* foi reservado para uso futuro

O campo *Fragment Off Set* indica a que ponto do pacote original o fragmento pertence.

O campo *Res* reserva-se para o futuro.

O *Flag Mf* indica se existem mais fragmentos ou se este trata-se do último.

Identification identifica unicamente o fragmento assim como o IPv4. O número de bits deste campo foi ampliado devido as redes de alta velocidade.

5.2.3 - Routing

Este cabeçalho lista um ou mais roteadores que devem ser visitado durante o percurso do pacote. Pode-se utilizar os dois tipos de roteamento, assim como no IPv4, *Strict e Loose*, com a variação de poderem ser combinados. A figura abaixo indica seu formato.

0	8	16	24 31
NEXT HEADER	ROUTING TYPE	NUMBER ADDRESS	NEXT ADDRESS
RESERVED	BIT MAP		
1 - 24 ADDRESS			

Formato do cabeçalho de extensão

O campo *Next Header* possui a mesma função de todos os outros cabeçalhos, ou seja, indica o próximo tipo de cabeçalho.

O campo *Routing Type* indica o tipo de roteamento, atualmente está definido em 0.

O campo *Number Address* indica o número de endereços presentes neste cabeçalho (de 1 a 24).

O campo *Next Address* indica o próximo endereço para o qual o pacote poderia ser enviado. Este campo inicia com 0 e é incrementado cada vez que um endereço é visitado.

O campo *Bit Map* é um mapa de bits que serve para indicar qual dos tipos de tratamento deve ser tomado a cada um dos roteadores. O endereço pode ser visitado diretamente depois do que o antecede (Strict) ou fazê-lo indiretamente, podendo existir roteadores intermediários (Loose).

5.2.4 - Authentication (AH)

O cabeçalho de autenticação oferece um mecanismo que permite que o host de origem saiba se o pacote enviado é mesmo de quem diz ser. Neste tipo de serviço, a privacidade da comunicação é garantida mas sem confidencialidade, isto é, os dados não são encriptados. Um dos objetivos da autenticação de pacotes é evitar ataques de máquina conhecido como IP *spoof*. O IP spoof consiste em utilizar o endereço de uma máquina em outra. Se a máquina de destino confiar neste endereço (isto é possivel no UNIX) é aberta então uma possibilidade de invasão.

Antes de ser iniciada uma comunicação, é necessário que o transmissor e o receptor defina uma ou mais chaves secretas, conhecidas somente por eles, criando uma associação. A associação é um relacionamento unidirecional entre o transmissor e o receptor, identificada pelo endereço do transmissor e um Security Parameter Index, presentes no cabeçalho de segurança. Os parâmetros desta associação são os algoritmos de autenticação e suas chaves de criptografia. Como algoritmo padrão do IPv6 foi definido o MD5 (Message Digest 5) mas outros poderão ser utilizados.

A autenticação no IPv6 é feito através de um cabeçalho de segurança que suporte a integridade e autenticação dos dados. O formato deste encontra-se na figura abaixo.

0	8	16	24 31
NEXT HEADER	PAYLOAD LENGTH	RESERVED	
SECURITY PARAMETER INDEX			
SEQUENCY NUMBER			

Formato do cabeçalho de autenticação.

O *Next Header* identifica o próximo cabeçalho.

O campo *Lenght* indica o comprimento do cabeçalho em palavras de 32 bits.

O campo *Security Parameter Index* é o número chave de 32 bits que em conjunto com os endereços de destino identifica unicamente a associação segura. De posse deste número o receptor localiza a chave secreta e calcula a soma de verificação do pacote confirmando ou não a associação segura.

O campo *Sequence Number* contém um contador que é incrementado a cada transmissão. O transmissor e o receptor são setados em 0 quando uma associação segura é iniciada. Este número é utilizado para evitar um replay de pacotes. Um replay consiste em capturar o datagrama e enviar um outro montado com informações modificadas. Este numero não é cíclico, e quando chegar o seu valor máximo o receptor e o transmissor devem colocá-lo em zero e iniciar uma nova associação segura.

O campo *Authentication* identifica os dados da autenticação em palavras de 32 bits. O que este campo contém vai depender do algoritmo de autenticação utilizado. Ele é calculado utilizando o pacote todo e atribuindo zero, àqueles campos que se modificam durante o percurso.

5.2.5 - Encrypted Security Payload (ESP)

Este cabeçalho provê a integridade e confidencialidade aos pacotes. Se utilizado em conjunto com o de autenticação forma uma solução completa de segurança. O serviço de segurança pode ser aplicado entre dois roteadores , entre dois hosts ou entre um host e um roteador. A figura 5.2.5.0 mostra o formato do cabeçalho de encriptação de dados.

O princípio básico deste cabeçalho é de enviar dados encriptados utilizando para isto um algoritmo, que deverá ser conhecido pelo transmissor e pelo receptor, bem como as chaves utilizadas para gerá-los. Por questão de compatibilidade um algoritmo padrão foi escolhido, o DES-CBC (Data Encryption Standard in Cipher-Block Chaining). Poderão ser usados, no entanto, outros algoritmos.

O ESP pode ser utilizado de dois modos. O primeiro é conhecido como *Tunnel-Mode*, que encapsula o datagrama inteiro no cabeçalho. O segundo é o *Transpot-Mode*, que encapsula os dados vindos da camada superior (TCP e UDP) dentro do cabeçalho.

O processamento de um cabeçalho ESP deverá aumentar o tempo de latência nos roteadores. Isto acontecerá devido ao tempo necessário para processar os complexos algoritmos de encriptacao utilizados, o que pode requerer roteadores com um maior poder

de processamento e uma implementação dos algoritmos em hardware. Entretanto, o uso de ESP não deverá impactar nos roteadores intermedários que não participarão desta associação de segurança.

<table>
<tr><td>0</td><td>8</td><td>16</td><td>24 31</td></tr>
<tr><td colspan="4">SECURITY PARAMETERS INDEX</td></tr>
<tr><td colspan="4">SEQUENCE NUMBER</td></tr>
<tr><td colspan="4">PAYLOAD DATA</td></tr>
<tr><td colspan="2"></td><td colspan="2">PADDING (0 - 255 bytes)</td></tr>
<tr><td colspan="2"></td><td>PAD LENGTH</td><td>NEXT HEADER</td></tr>
<tr><td colspan="4">AUTHENTICATION DATA</td></tr>
</table>

Figura 5.2.5.0 - Formato do cabeçalho de encriptação de dados

O campo *Security Parameters Index* é um número de 32 bits que identifica juntamente com os endereços de destino uma associação segura para o datagrama.

O campo *Sequence Number* contém um contador que é incrementado a cada transmissão. O transmissor e o receptor são setados em 0 quando uma associação segura é iniciada. Este número é utilizado para evitar um replay de pacotes assim como no cabeçalho de item anterior.

O campo *Payload Data* é o dado descrito pelo campo Next Header. Este campo deverá ser múltiplo de 8 bytes e corresponder a carga útil encriptada a ser transmitida. Se o algoritmo usado necessitar de sincronização de dados, um vetor de inicialização se faz necessário e é colocado no início deste campo.

O campo *Padding* é utilizado para incluir valores ao campo anterior caso o algoritmo necessite que o mesmo seja múltiplo de um número.

O campo *Pad Length* indica o número de octetos utilizados no campo anterior. Um valor 0 indica que nenhum *Padding* foi incluído.

O *Next Header* indica o tipo de dado contido no campo *Payload Data*, por exemplo, se neste campo contém TCP, indica que a carga útil é o dado vindo da camada de transporte.

O campo *Authentication Data* é opcional e, é incluído somente se houver uma necessidade de autenticação.

6.0 - *Endereçamento no IPv6*

Como já foi visto anteriormente, cada endereço do IPv6 ocupa 16 octetos (128 bits), isto faz com que o IPv6 suporte um número bem maior de níveis de hierarquia de endereços e de nós endereçáveis. Segundo Tanenbaum [TAN 96], se for colocado um computador em cada pedaço do planeta, incluindo a água, o IPv6 permitiria que fosse colocado 7×10^{23} endereços IP por metro quadrado. A quantidade de endereços no IPv6 possui quatro vezes o numero de bits utilizados para endereçamento no IPv4, tanto que engloba todos estes endereços para manter a compatibilidade.

Assim como a versão anterior o IPv6 associa um endereço a uma conexão de rede e não a um computador, permitindo, por exemplo, a um host ou a um roteador ter mais de um endereço associado a uma mesma interface física. Além disto o IPv6 amplia o endereçamento em três categorias:

- *Unicast* – o endereço de destino é associado a somente um computador;
- *Multicast* –o endereço de destino é um grupo de computadores possivelmente em locais diferentes. Uma cópia do pacote é dado para cada membro do grupo;
- *Anycast* – o destino é um conjunto de computadores. O pacote é entregue a somente um dos computadores, normalmente o mais próximo. Cabe ao roteador decidir qual deles.

6.1 - Notação de endereços no IPv6

O IPv6 usa uma notação diferente para seus endereços. Enquanto o IPv4 agrupa seus bits em oito e os representa em forma decimal, O IPv6 agrupa seus bits em 16 e os representa sob a forma hexadecimal. A notação decimal se fez ineficiente devido a dificuldade de tratá-la. Dessa maneira uma notação em decimal para um endereço IPv6 seria: 104.230.140.100.255.255.255.255.0.0.17.128.150.10.255.255.

O mesmo endereço usando a notação padrão do IPv6 é: 68E6:8C64:FFFF:FFFF:0:1180:96 A: FFFF. Esta notação tem a vantagem de requerer poucos dígitos e poucos pontos para separação dos campos agrupados.

Uma simplificação ainda é possível no caso de haver muitos zeros no endereçamento. Uma seqüência repetida de zeros é simplificada por um par de ":" por exemplo, citamos o endereço: FF05:0:0:0:0:0:0:B3. Este endereço poderia ser escrito da seguinte forma : FF05: :B3. Esta redução somente poderá ser usada uma vez para impedir valores ambíguos.

6.2- Tipos de endereçamento no IPv6

No IPv6, foram especificados apenas três tipos de endereços: Unicast, Anycast e Multicast. Sendo assim, diferente do IPv4, não mais existem endereços Broadcast. Esta função passa a ser provida pelo endereço Multicast.

6.2.1- Endereço Unicast

Identifica apenas uma interface. Um pacote destinado a um endereço unicast é enviado diretamente para a interface associada ao endereço. Foram definidos vários tipos de endereços unicast, que são:

* Global Provider-based, ou baseado no Provedor: é o endereço unicast que será globalmente utilizado. Seu plano inicial de alocação baseia-se no mesmo esquema utilizado no CIDR (Classless InterDomain Routing, [RFC1519]) definido em [RFC1887]. Seu formato possui um prefixo de 3 bits (010) e cinco campos: registry ID, para registro da parte alocada ao provedor; provider ID, que identifica um provedor especifico; subscriber ID, que identifica os assinantes conectados a um provedor; e infra-subscriber, parte utilizada por cada assinante.

* Unspecified: definido como 0:0:0:0:0:0:0:0 ou "::", indica a ausência de um endereço e nunca deverá ser utilizado em nenhum node. Este endereço só poderá ser utilizado como endereço de origem (source address) de estações ainda não inicializadas, ou seja, que ainda não tenham aprendido seus próprios endereços.

* Loopback: representado por 0:0:0:0:0:0:0:1 ou "::1". Pode ser utilizado apenas quando um node envia um pacote para si mesmo. Não pode ser associado a nenhuma interface.

* IPv4-based, ou baseado em IPv4: um endereço IPv6 com um endereço IPv4 embutido. Formado anexando-se um prefixo nulo (96 bits zeros) a um endereço IPv4 como, por exemplo, ::172.16.25.32. Este tipo de endereço foi incluído como mecanismo de transição para hosts e roteadores tunelarem pacotes IPv6 sobre roteamento IPv4. Para hosts sem suporte a IPv6, foi definido um outro tipo de endereço (IPv4-mapped IPv6) da seguinte forma: ::FFFF:172.16.25.32.

* NSAP: endereço de 121 bits a ser definido, identificado pelo prefixo 0000001. Endereços NSAP (Network Service Access Point) são utilizados em sistemas OSI.

* IPX: endereço de 121 bits a ser definido, identificado pelo prefixo 0000010. Endereços IPX (Internal Packet eXchange) são utilizados em redes Netware/Novell.

* Link-Local: endereço identificado pelo prefixo de 10 bits (1111111010), definido para uso interno num único link. Estações ainda não configuradas, ou com um endereço provider-based ou com um site-local, poderão utilizar um endereço link-local.

* Site-Local: endereço identificado pelo prefixo de 10 bits (1111111011), definido para uso interno numa organização que não se conectará à Internet. Os roteadores nao devem repassar pacotes cujos endereços origem sejam endereços site-local.

Também está reservado 12,5% de todo espaço de endereçamento IPv6 para endereços a serem distribuídos geograficamente (geographic-based).

6.2.2- Endereço Anycast

Identifica um grupo de interfaces de nodes diferentes. Um pacote destinado a um endereço anycast é enviado para uma das interfaces identificadas pelo endereço. Especificamente, o pacote é enviado para a interface mais próxima de acordo com a medida de distancia do protocolo de roteamento.

Devido à pouca experiência na Internet com esse tipo de endereço, inicialmente seu uso será limitado:

* Um endereco anycast não pode ser utilizado como endereço de origem (source address) de um pacote IPv6;

* Um endereço anycast não pode ser configurado num host IPv6, ou seja, ele deverá ser associado a roteadores apenas.

Este tipo de endereçamento será útil na busca mais rápida de um determinado servidor ou serviço. Por exemplo, pode-se definir um grupo de servidores de nomes configurados com

um endereço anycast; o host acessará o servidor de nomes mais próximo utilizando este endereço.

6.2.3- Endereço Multicast

Igualmente ao endereço anycast, este endereço identifica um grupo de interfaces, mas um pacote destinado a um endereço multicast é enviado para todas as interfaces do grupo.

As funcionalidades de multicasting foram formalmente incorporadas ao IPv4 em 1988, com a definição dos endereços classe D e do IGMP (Internet Group Management Protocol), e ganhou forca com o advento do MBONE (Multicasting Backbone) mas seu uso ainda não é universal. Desta vez, estas funcionalidades foram automaticamente incorporadas ao IPv6. Isto significa que não mais será necessário implementar túneis MBONE, pois todos os hosts e roteadores IPv6 deverão suportar multicasting.

7- Conclusão

A principal lição tirada do IP é que uma solução é amplamente adotada quando ela supre as necessidades de quem a deseja. A flexibilidade do IP e sua natureza aberta o tornou sucesso mundial. Hoje, ao final da sua “adolescência”, percebe-se que o mesmo não está apto para as novas exigências.

A IETF e mais especificamente o grupo de trabalho IPng tem hoje a oportunidade de oferecer ao mundo uma solução para várias restrições do IP atual (IPv4), com a vantagem da migração poder de acordo com cada necessidade e mantendo também a convivência harmoniosa entre as duas versões dos protocolos.

Por meio deste trabalho, podemos perceber como o IPv6 soluciona o problema de falta de endereços IP, diminuindo também o problema de grandes tabelas de roteamento.

Devemos atentar para o suporte nativo a segurança e a *multicast*, assim como a possibilidade de oferecer tratamento diferenciados para diferentes tipos de serviços e/ou fluxos.

A implementação de mecanismos de autoconfiguração é outra vantagem evidente que permite a mobilidade, eliminando problemas de configuração.

A utilização dos *extension headers* permitiu não só a simplificação do cabeçalho como também a possibilidade de evolução do protocolo. Este eventualmente se tornará obsoleto e necessitará ser substituído, no entanto, pela maneira como foi projetado, deverá apresentar uma vida útil bastante longa.