ISSN 1518-5974

Boletim bimestral sobre tecnologia de redes
produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa
13 de novembro de 1998 | volume 2, número 8

Nesta edição:

NewsGeneration:

buscar

A Nova Geração de Protocolos IP

Frank Ned <frank@absoluta.org>

Rede Nacional de Ensino e Pesquisa (RNP)

Palavras chave: IPng, IPv6, Protocolos, Next Generation, 6bone

Este artigo trata de um tema cuja discussão tem extrapolado os ambientes acadêmicos ou as reuniões da IETF para ser discutido por um leque maior pessoas: o IPv6 ou IPng.

Assim, são brevemente apresentados aspectos introdutórios deste novo protocolo, como a parte de cabeçalho e endereçamento, bem como outros que incluem as novas potencialidades do mesmo, tais como: qualidade de serviço e segurança. Estes últimos, de uma forma mais detalhada. São ainda tratados a parte de roteamento e os mecanismos de transição do IPv4 (versão atual) para IPv6.

^

Introdução

Este documento foi fortemente baseado no artigo *IP Next Generation Overview*[1] de autoria do Prof. Robert M. Hinden (hinden@ipsilon.com), o qual autorizou esta adaptação para o português. O Prof. Hinden é um dos autores das **RFC 1883***Internet Protocol, Version 6 (IPv6) Specifications*[2] e ***RFC 1884*** *IP Version 6 Addressing Architecture*[3].

Apesar da data do referido documento, o assunto é atual e representa um marco na história da Internet. O nome formal do novo protocolo é IPv6 (onde "6" representa o número da versão) ou ainda IPng (*IP Next Generation*). A versão corrente do IP é a 4 (referenciada como IPv4). O número 5 foi atribuído a um protocolo experimental.

O IPv6 será importante, não neste ou no próximo ano, mas nos próximos três ou sete anos. Agora, o que norteia o desenvolvimento do IPv6 não é a possibilidade de mais endereços, isso está sendo resolvido com NAT, LAT entre outros. O foco dos trabalhos é o gerenciamento de endereços, qualidade dos serviços e segurança.

A qualidade de serviço e, em particular, o telefone via Internet, serão os grandes beneficiados. O IPng está sendo desenvolvido para rodar tanto em redes de alto desempenho, como em redes com baixa banda, além de prover uma plataforma para as novas funcionalidades da Internet que serão usadas no futuro. Na nova versão do protocolo IP, foi eliminado o *checksums* dos cabeçalhos, a fragmentação de pacotes e todos os pacotes IPv6 carregam *flow identifiers* que podem ser usados para reservar recursos para uma alta qualidade de serviço. A migração para o IPv6 levará um bom tempo. Pois, além da atualização das pilhas dos protocolos, as aplicações que trabalham com IPv4 deverão ser corrigidas além da atualização dos roteadores.

A boa noticia é que IPV6 e IPv4 poderão coexistir juntos até uma total migração para o novo endereçamento.

Este documento apresenta uma visão geral sobre a nova geração de IP (IPng).

^

Pontos em discussão

Existem alguns pontos que devem ser considerados. Alguns são muito diretos: o novo protocolo deve ser capaz de suportar grandes redes globais. Outros, menos óbvios: deve haver um modo claro para a migração da corrente base instalada (IPv4). O que adiantaria o novo protocolo (IPv6) ser bom se não existir uma forma prática de migração do IPv4 para o IPv6?

CRESCIMENTO

O crescimento **foi** o motivo básico que levou à definição de uma nova geração de IP. Uma lição que pode ser tirada da experiência com IPv4 é a de que o endereçamento e o roteamento devem suportar o crescimento futuro. É importante que tenhamos compreensão do crescimento passado e como será o crescimento futuro.

A atual base de IPv4 é o que poderia ser chamado de mercado de computadores. O mercado de computadores foi quem guiou o crescimento da Internet. Isto inclui a Internet atual e outras incontáveis "internets" que sequer estão conectadas à esta grande rede. Seu enfoque é conectar computadores de grandes empresas, do governo e escolas universitárias. Este mercado ainda está crescendo a uma taxa exponencial. A faixa de computadores ligados a Internet variam de PC's a supercomputadores. A maioria encontra-se conectado a redes locais (LANs) e não são móveis.

A próxima fase de crescimento, provavelmente, não será guiada pelo mercado de computadores. Enquanto este continuará crescendo a taxas significantes devido a expansão em outras áreas como escolas e negócios pequenos, deverá acontecer o desenvolvimento de outros tipos de negócios , em várias áreas, cuja principal característica é a grande exigência com relação a qualidade do serviço (QoS). Estas novas exigências não são evidentes na atual fase de desenvolvimento do IPv4.

O desafio enfrentado pela IETF no processo de escolha de um novo protocolo levou em conta um que atenda a demanda atual e a demanda dos novos mercados que estão surgindo. Estes mercados vão surgir com ou sem o IETF IPng. Se o IETF IPng for uma solução boa para estes novos mercados, provavelmente, ele será usado. Senão, estes mercados desenvolverão outro protocolo, incorrendo no risco de serem criadas soluções proprietárias. A IETF está tendo a oportunidade de selecionar um protocolo que deverá ser usado nestes novos mercados. Isto teria resultados positivos, pois seria possível a criação de uma imensa estrutura para uma rede mundial com um protocolo aberto. Outra alternativa é um mundo com várias redes separadas com protocolos controlados pelos fabricantes. A experiência nos mostra que esta não seria a melhor solução.

TRANSIÇÃO

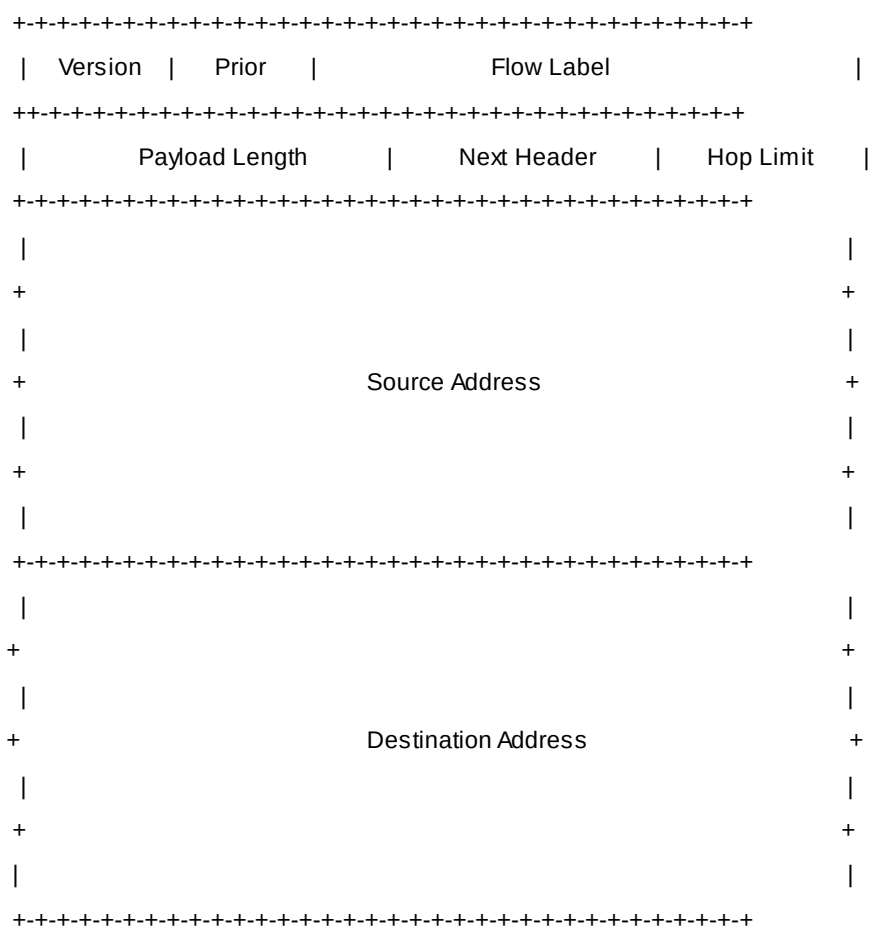
Em algum momento, nos próximos três ou sete anos, a Internet vai precisar de uma nova versão do protocolo IP (*internet protocol*). Dois fatores vão orientar esta necessidade: roteamento e endereçamento. O roteamento da Internet baseado em endereços de 32-bit (IPv4) está ficando limitado. O IPv4 não provê nenhuma flexibilidade para a construção de uma hierarquia eficiente que possa ser agregada. O desenvolvimento do CIDR (*Classless Inter-Domain Routing*) [5] está estendendo o tempo de vida do IPv4 por alguns anos. Os esforços para o gerenciamento do roteamento continuam aumentando. Não existe nenhuma duvida quanto a necessidade do IPng, mas somente uma questão: quando?

O desafio do novo protocolo é que a transição seja concluída antes que o endereçamento e o roteamento via IPv4 torne-se impossível. A transição será mais fácil se o endereçamento de IPv4 não estiver super-lotado. Assim, existem duas exigências importantes com relação a transição, que são: flexibilidade de desenvolvimento e habilidade de *hosts* com IPv4 comunicarem-se com *hosts* com IPv6. Existirão *hosts* com um único protocolo IPv6, bem como outros com IPv4.

A estratégia de desenvolvimento para o IPng deve ser tão flexível quanto possível. A Internet é muito grande e uma ação sem controle dificilmente terá êxito.

^

Formato do cabeçalho



Version - Com o tamanho de 4 bits, diz qual a versão do IP utilizado (6).

Prior - Diz o nível de prioridade (4 bits). Ver a seção Prioridade IPng.

Flow Label - Campo de 24 bist. Ver a seção Qualidade de Serviço.

Payload Length - Inteiro sem sinal (16 bits). Tamanho do *payload*, isto é, o resto do pacote que segue o cabeçalho IPng em octeto.

Next Header - Campo de 8 bits. Identifica o tipo de cabeçalho que segue o cabeçalho IPng. Usar o mesmo valor do protocolo IPv4 [6].

Hop Limit - Inteiro sem sinal (8 bits). Decrementado de 1 a cada *node* que passa o pacote. O pacote é descartado caso o *hop limit* seja igual a zero.

Source Address - Campo de 128 bits. O endereço do remetente original [7].

Destination Address - Campo também de 128 bits. Contém o endereço do destino do pacote (possivelmente não será o último destino caso um cabeçalho opcional de roteamento esteja presente).

^

Extensões do IPV6

O IPng possui um mecanismo de opções relativamente melhor que o do IPv4. As opções dele são colocadas em um cabeçalho de extensões separado, localizado entre o cabeçalho IPng e o da camada de transporte. A maioria dos cabeçalhos de extensões deste protocolo não são examinados ou processados pelos roteadores ao longo do caminho até que chegue ao destino final. Isto melhora o desempenho desses equipamentos para pacotes que contêm opções. No IPv4, a presença de qualquer opção obriga o roteador a examinar todas as outras opções.

Outra melhoria em relação ao IPv4 é que, no IPv6, os cabeçalhos de extensões podem ter um tamanho arbitrário e o total de opções transportadas em um pacote não é limitada a 40 octetos. Esta característica, aliada à forma pela qual são processados, permite que as opções do IPng sejam usadas para funções que não eram práticas no IPv4. Um bom exemplo são as opções de autenticação e encapsulamento de segurança.

Para melhorar o desempenho, quando está montando os cabeçalhos de opções subseqüentes e o protocolo de transporte que a segue, as opções IPng sempre são um múltiplo de um inteiro de 8 octetos. Isto mantém o alinhamento dos cabeçalhos seguintes.

Atualmente, são definidas as seguintes extensões de cabeçalhos:

Routing - roteamento estendido (IPv4 possui roteamento livre).

Fragmentation - Fragmentação e Remontagem.

Authentication - Integridade e Autenticação. Segurança.

Encapsulation - Confidencialidade.

Hop-by-Hop Option - Opção especial que requer processamento de *hop* para *hop*.

Destination Options - Informação opcional a ser examinada pelo destino.

^

Endereçamento no IPV6

Endereços IPv6 possuem tamanho de 128 bits e são identificadores de interfaces individuais e blocos de interfaces. Todos os tipos de endereços IPv6 são associados a interfaces não a nós. Desde que cada interface pertença a um único nó, quaisquer dos endereços de ***unicast*** das interfaces pode ser usado como um identificador para o mesmo. Uma única interface pode ser associada a múltiplos endereços IPv6 de qualquer tipo.

Existem três tipos de endereços IPng:

- ***Unicast*** - endereço que identifica uma única interface.
- ***Anycast*** - identifica um bloco de interfaces, de tal forma que um pacote enviado a um endereço de *anycast* será entregue a um elemento do bloco.
- ***Multicast*** - identifica um grupo de interfaces, tal que um pacote enviado a um endereço de *multicast* é entregue a todos elementos do grupo.

Não existe endereço de *broadcast* no IPv6, esta função foi substituída pelo endereço de *multicast*.

O IPng suporta endereços com número de bits 4 vezes maior que o endereço IPv4 (128 - [16 bytes] vs. 32 - [4 bytes]). Isto significa que o IPv6 é 4 bilhões (2^{96}) de vezes maior que o IPv4 (2^{32}), ou seja, a quantidade de endereços é de:

340.282.366.920.938.463.463.374.607.431.768.211.456

Esta é uma faixa de endereçamento extremamente grande. Teoricamente, isto representa aproximadamente 665.570.793.348.866.943.898.599 endereços por metro quadrado da superfície do nosso planeta (assumindo que a superfície da Terra seja de 511.263.971.197.990 m^2).

Em termos mais práticos, a tarefa de distribuição e roteamento de endereços requer a criação de hierarquias eficientes para o uso dos endereços. Christian Huitema fez uma análise [8] na qual avaliou a eficiência de outras arquiteturas de endereçamento (inclusive o sistema telefônico francês, o sistema telefônico dos E.U.A, a Internet atual que usa IPv4 e nós IEEE 802). Ele concluiu que o enderçamanto de 128 bits pode acomodar entre $8x10^{17}$ a $2x10^{33}$ nós, assumindo a eficiências de blocos semelhantes em outras arquiteturas de endereçamento. Até mesmo a sua estimativa mais pessimista assume que seria possível ter 1.564 endereços para cada metro quadrado da superfície do planeta Terra. A estimativa otimista permitiria 3.911.873.538.269.506.102 de endereços para cada metro quadrado.

O tipo de endereço IPng é indicado pelos bit mais significativo do endereço. A variação do tamanhos deste bit é chamado Prefixo de Formato (FP). A distribuição inicial destes prefixos é a seguinte:

Alocação	**Prefixo (binário)**	**Fração do espaço do Endereço**

reservado	0000 0000	1/256
não usado	0000 0001	1/256
reserved for NSAP Allocation	0000 001	1/128
reserved for IPX Allocation	0000 010	1/128
não usado	0000 011	1/128
não usado	0000 1	1/32
não usado	0001	1/16
não usado	001	1/8
Provider-Based Unicast Address	010	1/8
não usado	011	1/8
Reserved for *Neutra-Interconnect-Base Unicast Address*	100	1/8
não usado	101	1/8
não usado	110	1/8
não usado	1110	1/16
não usado	1111 0	1/32
não usado	1111 10	1/64
não usado	1111 110	1/128
não usado	1111 1110 0	1/512
Link Local Use Address	1111 1110 10	1/1024

Site Local Use Address	1111 1110 11	1/1024
Multicast Address	1111 1111	1/256

Esta estrutura suporta a distribuição direta para provedor de endereço, endereços de uso local e endereço de *multicast*. Existe espaço reservado para endereços NSAP, endereços IPX e *neutral-interconect address*. O espaço de endereço restante está reservado para uso futuro. Pode ser usado para expansão (por exemplo, provedor de endereço adicional, etc.) ou novos usos (por exemplo, identificadores). Observe que não foram tratados os endereços *anycast*. Isso porque eles são alocados fora do espaço de endereço de *unicast*.

Inicialmente será usado 15% do espaço do novo endereçamento, restando 85% para uso futuro.

^

Roteamento

O roteamento no IPng é semelhante ao roteamento no IPv4 com CIDR, a não ser pelo fato dos endereços do IPng serem de 128 bits em vez dos 32 bits do IPv4. Assim, com extensões muito simples, todos os algoritmos de roteamento do IPv4 (OSPF, RIP, IDRP, ISIS, etc.) podem ser usados para rotear pacotes IPng.

O IPng também inclui extensões simples de roteamento que permitem novas funcionalidades de roteamento poderosas, tais como:

- Seleção de provedor (baseado em política, desempenho, custo, etc.);
- Mobilidade de *host* (rotas para nova localização);
- Auto-reendereçamento (rota para novo endereço).

A nova funcionalidade de roteamento é obtida criando-se seqüências de endereços IPng usando as opções de roteamento do mesmo. As opções de roteamento são usadas pela origem do IPng para listar um ou vários nós intermediários (ou grupos de topologia) que devem ser "visitados" durante o transporte do pacote. Esta função é muito semelhante às opções do IPv4 *Loose Source* e *Record Router*.

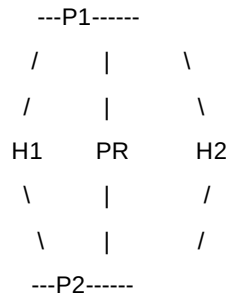
Para tornar o endereçamento seqüencial uma função geral, os *hosts* IPng são solicitados, em muitos casos, a fazer um roteamento reverso dos pacotes recebidos (se o pacote IPng for autenticado com sucesso usando a autenticação de cabeçalho), invertendo a seqüência de endereços para devolver o pacote a seu originador. Esta é a chave que permite aos *hosts* trabalharem com as novas características como seleção de provedor ou endereços estendidos.

Abaixo, três exemplos mostram como as sucessões de endereço podem ser usadas. Nestes exemplos, seqüências de endereços são mostradas por uma lista de endereços individuais separados por vírgula. Por exemplo:

SRC, I1, I2, I3, DST

O primeiro endereço é o endereço de fonte, o último é o endereço de destino, e os do meio são endereços intermediários.

Para estes exemplos, vamos assumir que dois *hosts,* (H1 e H2) desejam comunicar-se. Ambos estão conectados aos provedores P1 e P2. Um terceiro provedor PR (*wireless*), está conectado aos provedores P1 e P2 também.



O caso mais simples (sem o uso de seqüência de endereços) é quando H1 quer enviar um pacote para H2 contendo os endereços:

H1, H2

Quando H2 responder, este inverteria os endereços e construiria um pacote que contém os endereços:

H2, H1

Neste exemplo, poderia ser usado qualquer provedor, e H1 ou H2 não poderiam selecionar por qual provedor os pacotes seriam enviados e recebidos.

No entanto, se H1 decide usar uma política obrigando que toda comunicação entre ele e H2 devam ser transportadas via provedor P1, ele construiria um pacote com seqüência de:

H1, P1, H2

Isto garante que quando H2 respostas para H1, inverterá a rota e a resposta também seria transportada via P1. Os endereços de resposta em H2 seriam:

H2, P1, H1

Se H1 tornar-se móvel (um *laptop*) e mudasse para o provedor PR, poderia manter (sem quebrar qualquer conexão de transporte) a comunicação com H2, enviando pacotes que contêm a seqüência de endereço:

H1, PR, P1, H2

Isto garante que, quando H2 responder, ele usará a política de H1. A seqüência de endereços invertida seria:

H2, P1, PR, H1

A facilidade de seqüenciamento de endereço do IPng pode ser usada para selecionar o provedor, prover mobilidade e reendereçamento. Trata-se de uma característica simples, mas poderosa.

^

Qualidade do serviço

A Etiqueta de Fluxo (*Flow Label*) e os campos de prioridade no cabeçalho IPng podem ser usados por um *host* para identificar quais pacotes pedem manipulação especial através do roteador. Esta capacidade é importante para dar suporte a aplicações que requerem algum grau de processamento consistente, retardo e/ou velocidade. Estes tipos de aplicações são comumente descritos como multimídia ou aplicações em tempo real.

ETIQUETA DE FLUXO (*FLOW LABEL*)

O campo *flow label*, presente no cabeçalho do IPv6, possui 24 bits e pode ser utilizado para identificar pacotes que requerem tratamento especial pelos roteadores IPv6, como qualidade de serviço fora do padrão ou serviços de tempo real.

Esta funcionalidade do IPv6 está sendo pesquisada e pode sofrer mudanças. *Hosts* e roteadores que não suportam a funcionalidade de *flow label* devem preencher o campo com zeros quando originarem o pacote e ignorar o campo quando receberem um pacote.

Um fluxo (*flow*) é uma sucessão de pacotes enviada de uma origem para um destino (*unicast* ou *multicast*), e onde a origem define que os roteadores intermediários devem tratar o pacote de maneira especial. A forma de tratamento especial poderia ser carregada no roteador através de um protocolo de controle, como um protocolo de reserva de recursos ou por informações contidas dentro dos pacotes do fluxo, por exemplo, uma opção de *hop-by-hop*.

Pode haver múltiplos fluxos ativos de uma fonte para um destino, como também tráfego que não é associado a qualquer fluxo. Um fluxo é identificado exclusivamente pela combinação de um endereço da fonte e uma etiqueta de fluxo (*flow label*) preenchido com valores diferente de zeros.

Pacotes que não requerem tratamento especial, ou seja, que não pertencem a um fluxo possuem o campo *flow label* preenchido com zeros.

O campo *flow label* é preenchido pelo *host* que origina o fluxo. Devem ser escolhidas novas "etiquetas de fluxo" (randomicamente, entre 1 e FFFFFF). O propósito da alocação randômica é fazer com que qualquer conjunto de valores atribuídos dentro do campo *flow label* seja satisfatório para ser usado como uma chave *hash* pelo roteador, para verificar o estado associado ao fluxo.

Todos os pacotes que pertencem ao mesmo fluxo devem ser enviados com o mesmo endereço de origem, o mesmo endereço de destino e o mesmo *flow label*. Se algum pacote incluir em seu cabeçalho a opção de *hop-by-hop*, então todos os pacotes devem incluir a esta mesma opção em seus cabeçalhos (com exceção do próximo campo de *hop-by-hop* do cabeçalho). Se qualquer pacote incluir um cabeçalho de roteamento, então todos os pacotes devem incluir o mesmo cabeçalho (com exceção do campo próximo cabeçalho no cabeçalho de roteamento). A inclusão de roteador e destino é permitida, mas não requerida, para verificar se esta condição foi satisfeita. Se uma violação for detectada, a origem deverá ser informada através de um pacote de ICMP com o parâmetro de problema preenchido com o código 0, apontando o octeto de mais alta ordem do *flow label* (isto é, *offset* 1 dentro do pacote IPv6) [12].

Os roteadores são livres para "setar" um fluxo para qualquer estado, até mesmo quando não existir nenhum tipo de informação que explicitamente faça isto via um protocolo de controle, uma opção de *hop-by-hop* ou outro meio. Por exemplo, ao receber um pacote de uma fonte com um *flow label* desconhecido, um roteador pode processar seu cabeçalho IPv6 e qualquer cabeçalho de extensão como se o *flow label* fosse zero. Este processamento inclui determinar o próximo salto e outras ações como atualizar a opção de salto, avanço de ponteiro ou decidir como enfileirar os pacotes, baseado no campo prioridade. O roteador pode decidir, ainda, se vai armazenar estas informações em *cache*, usando o endereço de origem e o *flow label* como chave. Os pacotes seguintes como o mesmo endereço de origem e o mesmo *flow label* podem ser roteados a partir da informações amarzenadas no cache sem a necessidade de nova análise do cabeçalho.

PRIORIDADE

O campo prioridade, de 4 bits, permite que uma origem especifique a prioridade de entrega para determinados pacotes em relação a outros pacotes da mesma origem. Os valores do campo prioridade estão divididos em dois grupos:

- 0 a 7: são utilizados exclusivamente para definir a prioridade de tráfego para o qual a origem está provendo controle de congestionamento, ou seja, tráfego que volta devido ao congestionamento, como TCP.
- 8 a 15: são utilizados para especificar a prioridade de tráfego que não possuem resposta de volta. Ex.: pacotes de aplicações em tempo real, que são enviados a uma taxa constante.

Para o controle do congestionamento do tráfego, os seguintes valores de prioridade são recomendados:

0 *Uncharacterized traffic*;
1 *"Filler" traffic* (Ex.: netnews);
2 *Unattended data transfer* (Ex.: e-mail);
3 (Reservado)
4 *Attended bulk transfer* (Ex.: FTP, HTTP, NFS);
5 (Reservado)
6 *Interactive traffic* (Ex.: telnet, X);
7 *Internet control traffic* (Ex.: protocolos de roteamento, SNMP).

Para tráfego que não possuem controle de congestionamento, a prioridade mais baixa (valor 8) deve ser usada para pacotes que serão descartados caso exista um congestionamento (Ex.: tráfego de vídeo de alta fidelidade), e um valor mais alto (15) deve ser usado para pacotes que serão descartados com menor facilidade (Ex.: tráfego de áudio de baixa fidelidade). Não existe nenhuma relação entre os valores das prioridades do tráfego controlado e aquele não controlado.

^

Segurança

Atualmente, a Internet enfrenta vários problemas de segurança. Falta um mecanismo que garanta a privacidade de forma efetiva, e os protocolos não possuem mecanismos de autenticação para as camadas que estão abaixo da de aplicação.

Com o IPng, estas falhas serão corrigidas através de duas opções que provêem segurança [13]. Elas podem ser usadas isoladamente ou em conjunto para oferecer diferentes níveis de segurança. Isto é muito importante porque diferentes comunidades de usuários possuem diferentes necessidades no que diz respeito a este assunto.

O primeiro mecanismo é o *IPng Authentication Header*, que se trata de uma extensão de cabeçalho que provê autenticação e integridade (sem confidencialidade) para datagramas IPng [14]. Enquanto a extensão é um algoritmo independente e suporta várias técnicas diferentes de autenticação, foi proposto o uso de chaves MD5 para garantir a "interoperabilidade" na Internet. Este mecanismo pode ser usado para eliminar vários tipos de ataques, inclusive *spoof* de IP. A inclusão de tal mecanismo na Rede pode ser útil para os protocolos das camadas superiores no processo de autenticação da origem. Este mecanismo pode ser exportado pelos E.U.A. e por outros países que possuem as mesmas restrições de exportação, uma vez que ele provê somente autenticação e integridade e não confidencialidade. Isto encoraja o desenvolvimento e divulgação do *IPng Authentication Header*.

A segunda opção de segurança disponível é o *IPng Encapsulation Security Header* [15]. Este mecanismo provê integridade e confidencialidade para os datagramas IPng. Ele é mais simples que alguns protocolos de segurança similares (Ex.: SP3D, ISO, NLSP), possui flexibilidade e independência de algoritmo. Para prover "interoperabilidade" na Internet, o algoritmo padrão utilizado é o DES CBC.

^

Mecanismo de transição para IPV6

O objetivo principal dos mecanismos de transição é permitir a interoperabilidade entre IPv6 e IPv4. Um segundo objetivo é a distribuição de *hosts* e roteadores IPv6 de forma rápida e com alguma interdependência. Um terceiro ponto está relacionado com a facilidade de transição, ela deve ser simples para os usuários finais, administradores de sistemas e operadores de rede entre outros.

Os mecanismos de transição para o IPng são compostos de um grupo de protocolos implementados em *hosts* e roteadores, juntamente com algumas diretrizes operacionais com o objetivo de minimizar os impactos decorrentes da transição [16].

Algumas das características dos mecanismos de transição são:

- Pode-se migrar *hosts* e roteadores IPv4 para IPv6 sem a necessidade de migração de toda a rede, ou seja, um de cada vez. Da mesma forma, pode-se realizar a instalação de novos *hosts* e roteadores IPv6;
- Requisitos mínimos para migração. A única condição prévia para migração de *hosts* é que o servidor de DNS deve ser adequado para IPv6 antes disso. Para a migração de roteadores não existem pré-requisitos;
- Endereçamento fácil. Quando é realizada a migração de *hosts* e roteadores para IPv6, estes elementos podem continuar a utilizar seus antigos endereços IPv4. Eles não precisam ser configurados com os endereços novos;
- O custo inicial de migração é baixo. Necessita-se de pouco ou nenhum trabalho de preparação para migração de sistemas IPv4 para IPv6;
- Uma estrutura de endereçamento que encapsula os endereços IPv4 dentro do IPv6;
- Um modelo onde *hosts* e roteadores terão as duas pilhas de protocolos, IPv4 e IPv6, durante a fase de transição;
- Uma técnica de encapsulamento onde pacotes IPv6 serão embutidos dentro de cabeçalhos IPv4, permitindo o transporte dos pacotes por roteadores que ainda não migraram para IPv6.

Os mecanismos de transição, asseguram que *hosts* com IPv6 podem comunicar-se com *hosts* IPv4 a qualquer momento durante a fase de transição, e permite que, dentro de um âmbito limitado, o tempo de inter-operação seja indefinido. Esta característica protege os investimentos realizados em tecnologia IPv4 e garante que o mesmo não ficará obsoleto. Máquinas que utilizam conexões limitadas (por exemplo, impressoras) não precisam migrar para IPv6.

Este mecanismos permite que os fabricantes de *hosts* e roteadores implementem o IPng em suas linhas de produtos conforme suas prioridades. Permite também que usuários finais e administradores de redes implementem IPng conforme suas conveniências.

^

Conclusões

Conforme já foi dito, o IPv6 será importante, não neste ou no próximo ano, mas nos próximos três ou sete anos. Por enquanto, um *backbone* experimental com IPv6, o ***6bone*** , está sendo construído. O Brasil já está participando deste projeto através da RNP com recursos do CNPq. Agora, o que norteia o desenvolvimento do IPv6 não é a possibilidade de mais endereços, isso está sendo resolvido com NAT, LAT entre outros, mas o foco dos trabalhos é o gerenciamento de endereços, qualidade dos serviços e segurança.

^

Referências

[1] R. Hinden, "IPng Next Generation Overview", maio 1995.

[2] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specifications", RFC 1883, abril 1996.

[3] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", RFC 1884, abril 1996.

[4] S. Bradner, A. Mankin, "The Recommendation for the IP Next Generation Protocol", RFC 1752, janeiro 1995.

[5] V. Fuller, et al, "Supernetting: an Address Assignment and Aggregation Strategy", RFC 1338, julho 1992.

[6] J. Postel "Assigned Numbers", RFC-1700, outubro 1994.

[7] R. Hinden, Editor do "IP Version 6 Addressing Architecture", Internet *Draft*, abril 1995.

[8] C. Huitema, "The H Ratio for Addree Assignmente Efficiency" RFC-1715, novembro 1994.

[9] Y. Rekhter, T. Li, "An Archicture for IPv6 Unicast Address Allocation", Internet *Draft*, março 1995.

[10] Y. Rekhter, P. Lothberg, "An IPv6 Global Unicast Address Format", Internet *Draft*, março 1995.

[11] S. Thomson, "Ipv6 Address Autoconfiguration", Internet *Draft*, fevereiro 1995.

[12] A. Conta, S. Deering, "ICMP for the Internet Protocol Version 6 (IPv6)", Internet *Draft*, janeiro 1995.

[13] R. Atkinson, " IPv6 Security Architecture" Internet *Draft*, março 1995.

[14] R. Atkinson, "IP Authentication Header", Internet *Draft*, março 1995 .

[15] R. Atkinson, "IPng Encapsulating Security Payload (ESP)", março 1995.

[16] R. Gilligan, E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", março 1995.

^