Adam Victor Nazareth Brandizzi, Paulo Roberto Ramos Santos, Lauro Ivan da Costa

Internet Protocol Version 6 — IPv6

2006

Adam Victor Nazareth Brandizzi, Paulo Roberto Ramos Santos, Lauro Ivan da Costa

Internet Protocol Version 6 — IPv6

Trabalho realizado pelos alunos Adam Brandizzi, Laurivam Costa e Paulo Roberto Ramos Silva, referente à disciplina de Transmissão de Dados do Departamento de Ciências da Computação da Universida de Brasília, ministrada pelo prof. Jacir Bodin durante o primeiro semestre de 2006

UNIVERSIDADE DE BRASÍLIA
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE CIÊNCIAS DA COMPUTAÇÃO

2006

1 *Introdução – Histórico dos Motivos das Mudanças para o IPv6*

Na década de 90, engenheiros e cientistas começaram a perceber que a pilha de protocolos TCP/IP se tornaria ultrapassada para novas aplicações da Internet, como voz e vídeo. [MSL97], já em 1997, mostrou que o número de *hosts* na Rede dobrava a cada 14 meses e logo esgotaria o conjunto de endereços disponíveis.

Desde então, dois fatos ficaram claros: aplicações multimídia funcionam relativamente bem pela Internet existente na época, mas provavelmente a base atual tornar-se-ia obsoleta para aplicações mais exigentes; e, mesmo usando alternativas como o modelo de endereçamento CIDR (*Classless InterDomain Routeing* [FLYV93]) ou NAT (*Network Adress Translator* [EF94]), que fornecem uma certa margem ao número de endereços necessários, as projeções atuais sugerem que teremos endereços suficientes para algo entre quatro anos, segundo [Hai05], e vinte anos, segundo [Hus06], i.e., os endereços IP disponíveis atualmente estarão atribuídos a curto ou médio prazo[1].

A conclusão é evidente: precisamos de uma alternativa ao protocolo IP atual — o protocolo IPv4.

1.1 Apresentação do IPv4

A versão 4 do *Internet Protocol* (IPv4) foi a primeira versão largamente utilizada do protocolo IP; ela permanece quase inalterada desde o final da década de 1970 — época de seu lançamento. A longevidade da versão 4 mostra que o projeto é flexível e poderoso. Porém, desde o momento em que o IPv4 foi projetado, o desempenho do processador aumentou por três ordens de grandeza, os tamanhos típicos da memória aumentaram por um fator maior que 400, a largura de banda dos enlaces de maior velocidade na Internet aumentou por um fator de 150 mil. As tecnologias de LAN emergiram e o número de *hosts* na Internet aumentou de

[1] Para uma breve mas esclarecedora análise do por quê de tamanha discrepância, veja [Sen05]

alguns para centenas de milhões.

O protocolo IPv4 usa, para endereçamento, 32 bits, podendo, portando, endereçar mais de 4 bilhões de *hosts* na Internet. Quando o IP foi projetado, um espaço de endereços de 32 bits foi mais do que suficiente. Somente algumas das organizações usavam uma LAN, e nenhuma tinha uma *workstation*. Agora, porém, até mesmo corporações pequenas possuem LANs e vários computadores. Segundo [Tel05], no mundo, em dezembro de 2005, existiam cerca de 2 bilhões de celulares; se, a cada telefone celular atribuirmos um endereço IP, (como vem sido feito) os endereços serão esgotados rapidamente, sobrariam menos da metade do número total de endereços IPs disponíveis.

Outro problema do IPv4 é a total falta de segurança. Quando IPv4 foi projetado, acesso à Internet (ou, à época, ARPANET) era feito através de terminais em bases militares vigiadas por soldados. Os próprios desenvolvedores do TCP/IP não tinham muita noção do que fazer neste sentido. Nos tempos atuais, onde um enorme número de transações financeiras é executado por uma miríade de usuários, muitas vezes lidando com valores gigantescos, na Internet, agora pública, esta situação começa a se tornar um problema sério.

1.2 Proposta do IPv6

Tendo em mente isto, o *Internet Engeneering Task Force* (IETF) solicitou propostas de soluções para estes impasses [BA93]. O objetivo era encontrar um protocolo que satisfizesse as seguintes condições [Tan96]:

1. suportasse bilhões de *hosts* com endereços inequívocos;
2. reduzisse o tamanho das tabelas de roteamento;
3. especificasse pacotes mais fáceis de serem processados;
4. provisse meios de assegurar melhor privacidade e autenticação;
5. fosse mais flexível quanto à análise do *tipo de serviço* (i.e, fosse capaz de alterar parâmetros do transporte como velocidade ou qualidade de serviço dependendo do serviço prestado pelo pacote);
6. facilitasse a transmissão através de *multicasting*;
7. permitir que *hosts* em geral pudessem se deslocar no espaço sem precisar mudar de endereço IP;

8. permitir a evolução futura do protocolo; e, por último mas não menos importante

9. permitir a coexistência entre a nova versão e o IPv4.

Após algum tempo, conseguiram-se 21 propostas, das quais sete foram selecionadas como prováveis aceitas. Destas, duas propostas foram combinadas em uma solução para o que na época chamava-se *SIPP* (*Simple Internet Protocol Plus*). A este novo protocolo deu-se o nome de IPv6 — pois o nome IPv5 já havia sido usado [IPv06a].

2 Endereçamento

Certamente, a diferença mais visível e importante entre o protocolo IPv4 e o protocolo IPv6 é o modo de endereçamento.

No IPv6, cada endereço ocupa 16 bytes, quatro vezes o tamanho de um endereço IPv4. Com isto, obtemos 340282366920938463463374607431768211456 endereços, mais de $3,4 \times 10^{38}$. O espaço de endereços grande garante que o IPv6 pode tolerar qualquer esquema de atribuição de endereço razoável. Na verdade, se os projetistas decidirem mudar o esquema de endereçamento mais tarde, o espaço de endereços é suficientemente grande para acomodar uma reatribuição.

É difícil compreender o tamanho do espaço de endereços do IPv6. Um modo de examinar isso relaciona a magnitude ao tamanho da população: o espaço de endereços é tão grande que cada pessoa no planeta pode ter endereços suficientes para ter sua própria internet, tão grande quanto a Internet atual. A superfície da terra tem aproximadamente $5,1 \times 10^8 km^2$, significando que existem mais de $6,7 \times 10^{23}$ endereços por metro quadrado da superfície da terra. Segundo [Tan96], estaríamos próximos de atribuir um endereço IPv6 para cada molécula sobre a superfície da terra! Todavia, dada a separação dos endereços IPv6 em categorias como suporte a protocolos antigos, regiões ou empresas, este número não será bem distrubuído, como se vê na tabela 2.3. Não que isto seja um problema.

2.1 Notação do IPv6

A nova notação utilizada para os endereços IPv6 divide os 128 bits em oito grupos de 16 bits cada, ou seja, oito grupos de 4 dígitos, na forma hexadecimal e separados com “ : ”:

```
FECD:0008:0000:0000:0000:1600:45BA:0010
```

Devido a enorme quantidade de endereços possíveis proporcionados pelo IPv6, torna-se evidente que endereços semelhantes ao mostrado acima, com muitos “zeros”, sejam bastante comuns. Para facilitar e otimizar o trabalho com os bits convencionou-se que os zeros à es-

querda podem ser omitidos, deixando pelo menos um dígito no grupo de bits. O exemplo acima, então, ficaria assim:

`FECD:8:0:0:0:1600:45BA:10`

Ainda assim, teremos grupos de "zeros" encadeados e sua omissão também pode ser realizada, porém substituindo a "cadeia" de zeros por "::". Desta forma, nosso endereço exemplo passaria a ser:

`FECD:8::1600:45BA:10`

Note que, para evitar ambiguidade, a omissão acima pode ser realizada apenas uma vez no mesmo endereço. Deste modo,

`FECD:0008:0000:0000:0000:45BA:0000:0000`

poderia ser representado por

`FECD:8::45BA:0:0`

mas não por

`FECD:8::45BA::`

Como a transição dos protocolos requer que o IPv6 mantenha certa compatibilidade com endereços IPv4, convencionou-se representá-los na forma IPv6 preenchendo os primeiros 96 bits à esquerda com "zeros" e os 32 restantes com os bits do endereço IPv4. Sendo assim, um suposto endereço IPv4, digamos

`10.1.1.10`

seria representado em IPv6 por

`0000:0000:0000:0000:0000:0000:10.1.1.10`

ou

`::10.1.1.10`

Apenas ter um modo de codificar um endereço IPv4 em um endereço IPv6 não soluciona o problema de tomar as duas versões interoperáveis, porém. Além de resolver a codificação, a tradução é necessária. Para usar um tradutor, um computador IPv6 gera um datagrama que contém a codificação IPv6 do endereço de destino IPv4. O computador IPv6 envia o datagrama a um tradutor, que usa IPv4 para se comunicar com o destino. Quando o tradutor recebe uma resposta do destino, ele traduz o datagrama IPv4 para IPv6 e o envia de volta à origem IPv6.

2.2 Três tipos de endereçamento do IPv6

Assim como o IPv4, o IPv6 associa um endereço a uma conexão de rede específica, e não a um computador específico. Assim, as atribuições de endereço são semelhantes ao IPv4: um roteador IPv6 possui dois ou mais endereços, e um *host* IPv6 com uma conexão de rede só precisa de um endereço. O IPv6 também retém (e estende) a hierarquia de endereços do IPv4 em que uma rede física recebe um prefixo. Porém, para tornar a atribuição e a modificação mais fáceis, o IPv6 permite que vários prefixos sejam atribuídos a determinada rede e que um computador tenha vários endereços simultâneos atribuídos a determinada interface.

Além de permitir vários endereços simultâneos por conexão de rede, o IPv6 expande e, em alguns casos, unifica os endereços especiais do IPv4. Em geral, um endereço de destino em um datagrama cai em uma das três categorias [HD98]:

Unicast Um endereço é atribuído a uma única interface. Funciona de forma similar ao endereçamento ponto-a-ponto, ou seja, um pacote destinado à um endereço *unicast* será entregue diretamente a inteface associada a este endereço.

Multicast Um endereço é atribuído a um grupo de interfaces que geralmente pertecem a nodos diferentes. Um pacote destinado a um endereço *multicast* será entregue a todas as interfaces associadas, pelo grupo, a esse endereço. Esta função suprimiu o *broadcast* do IPv4 e já vinha sendo implementada, em especial nos *backbones*. Contudo, as complicações inerentes a necessidade desta implementação não existirão no IPv6, visto que todos os *hosts* e roteadores reconhecerão multicasting originariamente.

Anycast Provavelmente o mode de endereçamento mais original em IPv6. Aqui, um endereço também é atribuído a um grupo de intefaces. Contudo, um pacote destinado a um endereço *anycast* será entregue a apenas uma interface assoaciada aquele endereço e especificada nele como a mais próxima, considerando a distância segundo protocolos de roteamento. Este tipo de endereço só pode ser atribuído a roteadores, segundo determinação da própria IETF na RFC 2373.

2.3 Atribuição do espaço de endereços IPv6

A questão de como particionar o espaço de endereço IPv6 gerou muita discussão. Existem duas questões centrais: como gerenciar a atribuição de endereço e como mapear um endereço

a uma rota. A primeira questão trata do problema prático de criar uma hierarquia de autoridade. Ao contrário da Internet atual, que usa uma hierarquia de dois níveis de prefixo de rede (atribuída por um ISP) e sufixo de *host* (atribuído por uma organização), o espaço de endereços grande no IPv6 permite uma hierarquia multinível ou hierarquias múltiplas. A segunda questão trata da eficiência computacional. Independente da hierarquia de autoridade que atribui endereços, um roteador precisa examinar cada datagrama e escolher um caminho até o destino. Para manter baixo o custo dos roteadores de alta velocidade, o tempo de processamento exigido para escolher um caminho precisa ser minimizado.

Prefixo (binário)	Uso	Fração
0000 0000	Reservado (incluindo IPv4)	1/256
0000 0001	Não atribuído	1/256
0000 001	Endereços OSI NSAP	1/128
0000 010	Não atribuído	1/128
0000 011	Não atribuído	1/128
0000 1	Não atribuído	1/32
0001	Não atribuído	1/16
001	Não atribuído	1/8
010	Endereços baseados em provedores	1/8
011	Não atribuído	1/8
100	Endereços baseados em localização geográfica	1/16
101	Não atribuído	1/8
110	Não atribuído	1/8
1110	Não atribuído	1/16
1111 0	Não atribuído	1/32
1111 10	Não atribuído	1/64
1111 110	Não atribuído	1/128
1111 1110 0	Não atribuído	1/512
1111 1110 10	Endereço local à rede	1/1024
1111 1110 11	Endereço local à máquina	1/1024
1111 1111	Não atribuído	1/256

Tabela 2.1: Atribuição de espaços de endereços IPv4 (tirado de [Tan96])

2.4 Autoconfiguração

IPv6 foi elaborado para dar suporte à autoconfiguração sem servidor (*serverless autoconfiguration*), que permite que os computadores se comuniquem sem exigir que um administrador especifique um endereço e sem exigir um servidor de atribuição de endereços, como DHCP. O intuito desta funcionalidade é dar mobilidade ao usuário, que poderia por exemplo usar seu *laptop* para se conectar em diversas redes diferentes. Basicamente, à medida que um *host* se movimentasse de uma rede para outra, seu número de IP se autoconfiguraria, alterando-se para

ser reconhecido pela rede específica. O pensamento é de que a comunicação não é quebrada por esta “máscara”, pois independentemente de ser móvel ou não, host deve possuir um endereço local de sua rede de origem (*home adress*) que é fixo. Dessa forma, os pacotes continuariam sendo destinados a esse endereço e encaminhados ao “novo” endereço *host*, que avisaria sua rede original sempre que houvesse essa mudança de endereço IP.

3 Características gerais do IPv6

O protocolo IPv6 proposto retém muitas das características que contribuíram para o sucesso do IPv4. Na verdade, os projetistas caracterizaram o IPv6 como sendo basicamente o mesmo que o IPv4, com algumas pequenas modificações. O IPv6, por exemplo, ainda admite entrega sem conexão (ou seja, cada datagrama é roteado independentemente), permite que o emissor escolha o tamanho de um datagrama e exige que o mesmo especifique o número máximo de saltos que um datagrama pode fazer antes de ser terminado. Como veremos, o IPv6 também retém a maior parte dos conceitos fornecidos pelas opções do IPv4, incluindo facilidades para fragmentação e roteamento de origem.

Apesar de muitas semelhanças conceituais, o IPv6 muda a maior parte dos detalhes do protocolo, como por exemplo o uso de endereços. Examinaremos sucintamente estas alterações, depois de considerarmos as principais mudanças e a motivação básica para cada um.

As maiores mudanças introduzidas pelo IPv6 podem ser agrupadas em sete categorias:

1. Endereços maiores. O novo tamanho do endereço é a mudança mais observável. O IPv6 quadruplica o tamanho de um endereço IPv4 de 32 bits para 128 bits.

2. Hierarquia de endereço estendida. O IPv6 usa o espaço de endereço maior para criar níveis adicionais de hierarquia de endereçamento (por exemplo, para permitir que um ISP aloque blocos de endereços a cada cliente).

3. Formato de cabeçalho flexível. O IPv6 usa um formato de datagrama completamente novo e flexível, que inclui um conjunto de cabeçalhos opcionais.

4. Opções avançadas. O IPv6 permite que um datagrama inclua informações de controle opcionais; as opções do IPv6 fornecem facilidades adicionais não disponíveis no IPv4.

5. Previsão para extensão de protocolo. Em vez de especificar todos os detalhes, a capacidade de extensão do IPv6 permite que o IETF adapte o protocolo ao novo hardware de rede e novas aplicações.

6. Suporte para autoconfiguração e renumeração. O IPv6 permite que os computadores em uma rede isolada atribuam endereços locais automaticamente; o projeto também permite que um gerente renumere redes em um site dinamicamente.

7. Suporte para alocação de recurso. O IPv6 inclui uma abstração de fluxo e bits para a especificação de serviço diferenciado (*DiffServ*). O último é idêntico ao DiffServ do IPv4.

3.1 O Datagrama IPv6

O IPv6 muda completamente o formato do datagrama. Como mostra a figura 3.1, um datagrama IPv6 possui um cabeçalho básico de tamanho fixo seguido por zero ou mais cabeçalhos de extensão, seguidos pelos dados. Os cabeçalhos de extensão são opcionais e fornecem informações sobre os dados que não se encontram no caso comum e precisam de algum tratamento especial.

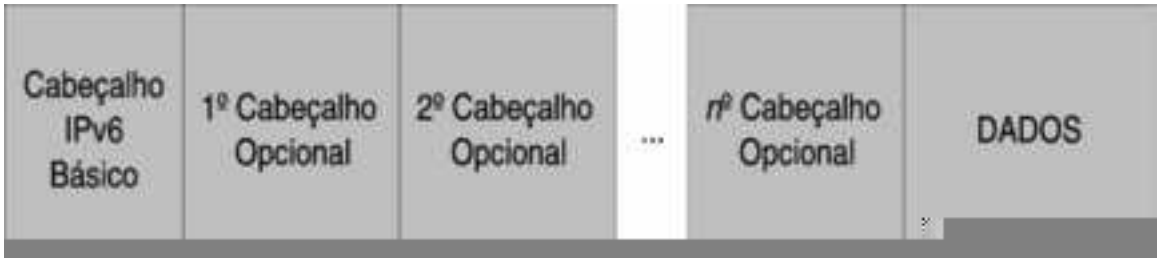

Figura 3.1: Diagrama de um pacote IPv6 genérico

3.1.1 Formato do Cabeçalho Básico no IPv6

Embora deva acomodar endereços maiores, um cabeçalho básico IPv6 contém menos informações do que um cabeçalho de datagrama IPv4. As opções e alguns dos campos fixos que aparecem em um cabeçalho de datagrama IPv4 foram movidos para cabeçalhos de extensão no IPv6. Em geral, as mudanças no cabeçalho do datagrama refletem as mudanças no protocolo:

- o alinhamento foi alterado de múltiplos de 32 bits para 64 bits;
- um campo de tamanho de cabeçalho foi eliminado, e o campo de tamanho do datagrama foi substituído por um campo de *Payload Length*, que informa o tamanho total do pacote;
- o tamanho dos campos de endereço de origem e destino foi aumentado para 16 *bytes* cada um;

- a informação de fragmentação foi movida para fora dos campos fixos no cabeçalho básico para um cabeçalho de extensão;
- o campo *Time to Live* foi substituído pelo campo *Hop Limit*, já que mesmo o antigo *Time to Live* guardava, na prática, o número de *hops*[1] percorridos;
- o campo *Service Type* teve o nome alterado para *Traffic Class* e extendido com um campo *Flow Label*;
- o campo *Protocol* foi substituído por um campo que especifica o tipo do próximo cabeçalho.

3.2 Campos do cabeçalho padrão IPv6

Vamos falar do conteúdo e do formato de um cabeçalho IPv6 básico. Vários campos em um cabeçalho básico do IPv6 correspondem diretamente aos campos em um cabeçalho IPv4. Assim como no IPv4, o campo *Version* de 4 bits inicial especifica a versão do protocolo; *Version* sempre contém 6 em um datagrama IPv6. Assim como no IPv4, os campos Endereço de Origem (*Source Address*) e Endereço de Destino (*Destination Address*) especificam os endereços do emissor e destinatário desejados. Porém, no IPv6, cada endereço requer 16 *bytes*.

O campo *Hop Limit* corresponde ao campo *Time to Live* do IPv4. A mudança de nome tem causa conceitual: teoricamente, o tempo de vida de uma datagrama é determinado, em IPv4, por um *delay* temporal máximo menor ou igual a 255 segundos), mas, na prática, o número armazenado no campo *Time to Live* de um pacote IPv4 é usado para denermnar o limite de *hops* que o datagrama pode percorrer antes de ser descartado, sendo decrementado em cada salto. Então, o IPv6 adaptou o nome do campo para sua real funcionalidade.

O IPv6 trata de especificações de tamanho de datagrama de uma nova maneira. Primeiro, como o tamanho do cabeçalho básico é fixado em 40 *bytes*, o cabeçalho básico não inclui um campo para o tamanho do cabeçalho. Em segundo lugar, o IPv6 substitui o campo de tamanho do datagrama do IPv4 pelo campo *Payload Lenght*, que especifica o número de *bytes* transportados no datagrama, excluindo o próprio cabeçalho. Este campo possui 16 *bits*, de modo que um datagrama IPv6 padrão pode conter até 64K *bytes* de dados. Entretanto, IPv6 suporta um cabeçalho de extensão que permite a especificação de tamanhos maiores, de modo a gerar o que comumente se chama de *jumbogramas*: datagramas com tamanhos bem maiores que o padrão, geralmente utilizados por supercomputadores distribuídos.

[1] Um *hop* é uma transferência entre um *host* e outro, incluindo roteadores, executada para se alcançar o computador alvo

Dois campos no cabeçalho básico são usados na tomada de decisões de encaminhamento. O campo *Type of Service* do IPv4 foi renomeado como *Trafic Class*. Além disso, um novo mecanismo no IPv6 admite reserva de recurso e permite que um roteador associe cada datagrama a determinada alocação de recurso. A abstração básica, um fluxo, consiste em um caminho por uma internet junto à qual roteadores intermediários garantem uma qualidade de serviço específica. O campo *Flow Label* no cabeçalho básico do IPv6 contém informações que os roteadores utilizam para associar um datagrama a um fluxo e prioridade específicos. Por exemplo, duas aplicações que precisam enviar vídeo podem estabelecer um fluxo em que o atraso e a largura de banda sejam garantidos. Como alternativa, um provedor de rede pode exigir que um assinante especifique a qualidade de serviço desejada e depois use um fluxo para limitar o tráfego que um computador ou aplicação específica envia. Observe que os fluxos também podem ser usados dentro de determinada organização para gerenciar recursos de rede e garantir que todas as aplicações recebam uma fatia justa da banda. Um roteador usa a combinação de endereço de origem do datagrama e identificador de fluxo ao associar um datagrama a um fluxo específico.

Resumindo: cada datagrama IPv6 começa com um cabeçalho básico de 40 *bytes*, que inclui campos para os endereços de origem e destino, o limite máximo de saltos, a classe de tráfego, o rótulo de fluxo e o tipo do próximo cabeçalho (*Next Header*), sendo que o último cabeçalho opcional indica para a camada de transporte qual o protocolo adequado para tratar o dado. Deste modo, um datagrama IPv6 precisa conter pelo menos 40 *bytes* além dos dados.

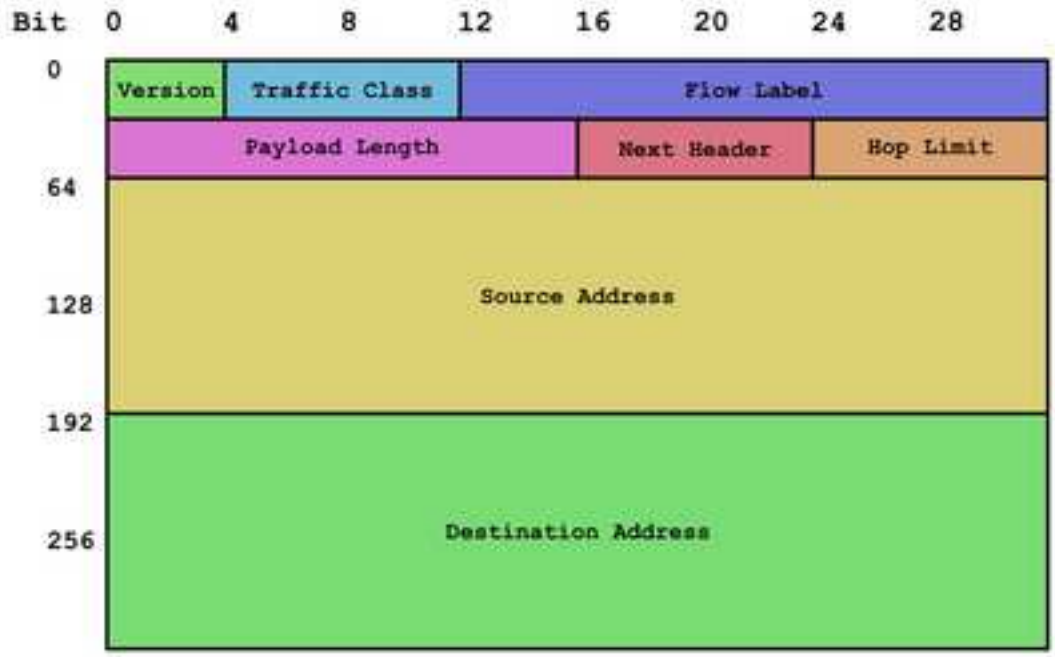

Figura 3.2: Diagrama de um pacote IPv6 – tirado de [IPv06b]

Para agilizar o processamento, o IPv6 exige que os cabeçalhos de extensão utilizados por roteadores intermediários sejam colocados antes dos cabeçalhos de extensão usados pelo destino final. O IPv6 usa o termo cabeçalho salto-a-salto (*hop-by-hop header*) para se referir a um cabeçalho de extensão que um roteador intermediário precisa processar. Assim, os cabeçalhos *hop-by-hop* precedem os cabeçalhos de fim-a-fim.

3.3 Fragmentação e remontagem do IPv6

A fragmentação de datagramas IPv6 é permitida; um cabeçalho de extensão é usado para especificar que um datagrama é um fragmento. Assim como no IPv4, o IPv6 providencia para que o destino final realize a remontagem do datagrama. Porém, os projetistas escolheram fazer mudanças que evitam a fragmentação por roteadores. Lembre-se de que o IPv4 requer que um roteador intermediário fragmente qualquer datagrama que seja muito grande para a MTU (*Maximum Transfer Unit*) da rede que ele precisa atravessar. No IPv6, a fragmentação é de fim-a-fim; nenhuma fragmentação ocorre nos roteadores intermediários. A origem, que é responsável pela fragmentação, tem duas escolhas: ela pode usar a MTU míníma garantída de 1280 *bytes* ou realizar a descoberta de MTU do caminho (*Path MTU Discovery*) para identificar a MTU mínima ao longo do caminho até o destino. De qualquer forma, a origem fragmenta o datagrama de modo que cada fragmento seja menor que a MTU esperada do caminho.

IPv6 retém a funcionalidade de fragmentação básica. Cada fragmento precisa ser um múltiplo de 8 *bytes*. No IPv4, o único *bit* no campo *More Fragments* marca o próximo ou último fragmento, e o campo *Identification* transporta uma ID exclusiva que o receptor usa para agrupar fragmentos (o IPv6 expande este campo 32 *bits*, a fim de acomodar redes de maior velocidade).

3.4 A conseqüência da fragmentação de fim-a-fim

A motivação para usar a fragmentação de fim-a-fim está em sua capacidade de reduzir o *overhead* em roteadores e permitir que cada roteador trate de mais datagramas por tempo unitário. Na realidade, a sobrecarga de CPU exigida para a fragmentação IPv4 pode ser significativa - em um roteador convencional, a CPU pode atingir 100% de utilização se o roteador fragmentar todos os datagramas que ele recebe. Porém, a fragmentação de fim-a-fim tem uma conseqüência importante: ela altera a suposição fundamental do IPv4 de que as rotas mudam dinamicamente.

Para entender a conseqüência da fragmentação de fim-a-fim, lembre-se de que o IPv4 foi projetado para permitir que as rotas mudem a qualquer hora. Por exemplo, se uma rede ou roteador falhar, o tráfego pode ser roteado por um caminho diferente. A principal vantagem desse sistema é a flexibilidade — o tráfego pode ser roteado ao longo de um caminho alternativo sem atrapalhar o serviço e sem informar a origem ou o destino. Porém, no IPv6, as rotas não podem ser alteradas tão facilmente, pois uma mudança em uma rota também pode alterar a MTU do caminho. Se a MTU do caminho ao longo de uma nova rota for menor que a MTU do caminho ao longo da rota original, então um roteador intermediário precisa fragmentar o datagrama ou a origem precisa ser informada.

Para resolver o problema de mudanças de rota que afetam a MTU do caminho, o IPv6 inclui uma nova mensagem de erro do ICMP. Quando um roteador descobrir que a fragmentação é necessária, ele enviará a mensagem de volta à origem. Ao receber tal mensagem, a origem realizará outra descoberta de MTU do caminho para determinar uma nova MTU mínima e depois fragmentará os datagramas de acordo com o novo valor.

3.5 Roteamento de origem IPv6

O IPv6 retém a capacidade para um emissor especificar uma rota de origem solta. Diferente do IPv4, em que o roteamento de origem é fornecido por opções, o IPv6 usa um cabeçalho de extensão separado. Os quatro primeiros campos do Cabeçalho de Roteamento são fixos. O tipo de roteamento (*Routing Type*) especifica o tipo de informação de roteamento; o único tipo que foi definido, tipo O, corresponde ao roteamento de origem solto. O campo *Type-Specific Data* contém uma lista de endereços de roteadores através dos quais o datagrama precisa passar. O campo *Seg Left* especifica o número total de endereços na lista. Finalmente, o campo *Header Extention Length* especifica o tamanho do cabeçalho de roteamento.

3.6 Opções do IPv6

Pode parecer que os cabeçalhos de extensão do IPv6 substituem completamente as opções do IPv4. Porém, os projetistas propõem dois cabeçalhos de extensão adicionais do IPv6 para acomodar informações diversificadas não incluídas nos outros cabeçalhos de extensão. Os cabeçalhos adicionais são um cabeçalho de extensão salto-a-salto e um cabeçalho de extensão de fim-a-fim. Como o nome sugere, os dois cabeçalhos separam o conjunto de opções que devem ser examinados em cada salto do conjunto que são apenas interpretados no destino. Cada

opção começa com um campo *Type* de um *byte*, seguido por um campo *Lenght* de um *byte*. Se a opção exigir dados adicionais, os *bytes* que constituem o *Value* vêm após o *Lenght*.

Bits	Significado
00	Pular esta opção
01	Descartar datagrama; não enviar mensagem ICMP
10	Descartar datagrama; enviar mensagem ICMP à origem
11	Descartar datagrama; enviar ICMP se não *multicast*

Tabela 3.1: Combinação de *bits* no campo *Type*

Os *bits* de alta ordem de cada campo *Type* da opção especificam como um *host* ou roteador deve descartar um datagrama se não entender a opção.

Além disso, o terceiro *bit* no campo *Type* especifica se a opção pode mudar em trânsito. É importante ter essa informação para autenticação — o conteúdo de uma opção que pode mudar em trânsito é tratado como zeros, para fins de autenticação.

4 *Críticas e Migração para IPv6*

4.1 Críticas a IPv6

Obviamente, IPv6 não conseguiu ser a primeira unanimidade da Humanidade: muitas críticas surgiram a vários dos seus aspectos.

Por exemplo, um dos pontos que mais atraiu críticas é, não surpreedentemente, o novo tamanho de endereços. Para muitos, 16 *bytes* é simplesmente muito *overhead* para pouca necessidade. Entretanto, como é evidente, o time do *overhead* ganhou.

Uma crítica de certo modo inversa a esta é a que se faz à manutençaõ tamanho do campo *Hop Limit*. Muitos consideram 255 *hops* um limite muito restrito para um pacote. Os argumentadores a favor do campo *Hop Limit* de oito *bits*, porém, conseguiram manter o tamanho do campo em um *byte*, em especial porque se considera que, à medida em que a rede cresce, mais conexões de longa distância são feitas, reduzindo o número de *hops* necessários.

Os fabricantes e usuários de supercomputades, por sua vez, reclamavam do minúsculo tamanho máximo dado aos pacotes: 64K *bytes*. Entretanto, considerou-se que habilitar pacotes muito maiores que este resultaria em redes com alto *delay* resultante da grande ocupação da banda por um só pacote. A resolução neste caso foi manter o tamanho máximo de 64K *bytes* e oferecer os cabeçalhos opcionais para jumbogramas.

Outro ponto importante foi a abolição do *checksum* dos pacotes IPv6. Entretanto, ficou mais ou menos entendido[1] que com os protocolos abaixo do protocolo de rede já fazendo a verificação de integridade e com os protocolos de cima tendo esta opção, não faz sentido gastar processamento de um roteador com mais *checksums*.

Houve, naturalmente, muito mais controvérsias. Por exemplo, os dispositivos móveis são um pomo da discórdia insolúvel. A principal questão era como se faria para atribuir endereços a eles, pois que eles inevitavelmente percorreriam o espaço. O endereço IPv6 deles deveria

[1] Pois nada pode ficar mais entendido que "*mais ou menos entendido*" na IETF...

mudar para a faixa do local onde estão? Não há consenso sobre isto.

Outro exemplo foi a questão da segurança: como seria feita? Muitos apoiavam a idéia de que as próprias aplicações deveriam criptografar seus dados, enquanto outros presumiam que a camada de rede deveria ser responsável por isto. Ganhou a idéia de que os dados seriam criptografados por padrão, mas que seria possível desabilitar a criptografia de um pacote.

Notoriamente, isto não foi suficiente para acalmar os ânimos. A questão agora era: que algoritmo de criptografia utilizar? Se usarem um algoritmo muito seguro, pode se tornar muito eficiente; se usarem um muito eficiente, as transmissões podem se tornar inseguras. A solução foi simples: assim como é possível desabilidar a criptografia, é possível alterar o algoritmo. Por paddrão, porém, ficaria um algoritmo mais poderoso.

Para dados mais precisos sobre estas controvérsias, além dos próprios RFCs da IETF, veja [Tan96], p. 447—449.

4.2 O caminhar da migração

Como se pode perceber, o protocolo IPv6 traz alterações estruturais significativas se comparado ao protocolo IPv4. Entretanto, como explicamos ainda no primeiro capítulo, era propriedade inalienável do protocolo a desbancar IPv4 a compatibilidade retrógrada com a atual versão do IP, e IPv6 é compatível. As vantagens disto tornam-se claras com o andamento do processo migratório.

A migração para IPv6 já está acontecendo, e tem sido bem sucedida. Várias interredes já estão suportando IPv6, como e.g. a RNP [dEeP06]. A maioria dos sistemas operacionais modernos mais utilizados também está preparada para a migração [IPv03], além de diversos *sites* de grande acesso, como os listados em [IPv03].

Resumindo: a migração já está acontecendo, e continuará assim suavemente, imperceptívelmente. Como diria [San05]:

> “Não haverá dia D”.

5 *Conclusão*

A necessidade e a iminência de não se ver os atuais endereços IP esgotados e atender a crescente demanda por endereços não é a única motivação para a transição IPv4 – IPv6. Os usuários domésticos e corporativos estão demandando uma nova leva de serviços inovadores para os quais IPv4 começa a ficar impróprio, desde jumbogramas para supercomputadores até *video streamming* e VoIP. IPv6 proporciona flexibilidade suficiente para suprir as novas demandas, e certamente grande parte das que estão por vir.

Além disso, cada vez mais a redes de computadores têm convergido para o desenvolvimento de tecnologias que possibilitem mobilidade ao usuário, e este por sua vez demanda de forma igual que seu dispositivo esteja conectado à Internet independente da rede em que ele se encontra. Não estamos muito distantes de um futuro onde cada usuário não possuirá em seu bolso apenas um telefone celular (como já vem acontecendo), mas um dispositivo com endereço IP único que ofereça conexão transparente à Internet de forma simplificada à semelhança do que ocorre em sua casa ou trabalho, e esse futuro está apoiado sobre o IPv6.

De fato, o protocolo está longe de ser uma quebra de paradigma e este foi um dos muitos fatores que geraram críticas de técnicos especializados na época de sua concepção, mas hoje com as RIRs (*Regional Internet Registries* - responsáveis pela distribuição de endereções IPv6) consolidadas e com a transição em curso ninguém duvida da sua larga adoção iminente.

Referências Bibliográficas

[BA93] S. Bradner and Mankin A. Ip: Next generation (ipng) white paper solicitation. http://www.ietf.org/rfc/rfc1550.txt, 1993.

[dEeP06] Rede Nacional de Ensino e Pesquisa. Ipv6 na rnp. http://www.rnp.br/ipv6/ipv6-rnp.html, abril 2006.

[EF94] K. Egevang and P. Francis. The ip network address translator (nat). http://www.ietf.org/rfc/rfc1631.txt, 1994.

[FLYV93] V. Fuller, T. Li, J. Yu, and K. Varadhan. Classless inter-domain routing (cidr): an address assignment and aggregation strategy. http://www.ietf.org/rfc/rfc1519.txt, 1993.

[Hai05] Tony Hain. A pragmatic report on ipv4 address space consumption. *The Internet Protocol Journal*, 8(3):2—9, setembro 2005. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipv4.html.

[HD98] R. Hinden and S. Deering. Ip version 6 addressing architecture. http://www.ietf.org/rfc/rfc2373.txt, 1998.

[Hus06] Geoff Huston. Ipv4 address report. http://bgp.potaroo.net/ipv4/, junho 2006.

[IPv03] Ipv6 information page. http://www.ipv6.org/, abril 2003.

[IPv06a] Ipv5 – wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/IPv5, julho 2006.

[IPv06b] Ipv6 – wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/IPv6, julho 2006.

[MSL97] Arnaldo Mangel, Imre Simon, and Jorge L. de Lyra. Informação: Computação e comunicação. http://www.ime.usp.br/ is/abc/abc/abc.html, julho 1997.

[San05] Robinson Nelson dos Santos. Quem precisa do ipv6? http://old.computerworld.com.br/AdPortalv5/adCmsDocumentShow.aspx?GUID=B9E7C58
9CD6-4751-9867-897799F12B72&ChannelID=21, julho 2005.

[Sen05] James Seng. When will we run out of ipv4? http://www.circleid.com/posts/when_will_we_run_out_of_ipv4/, outubro 2005.

[Tan96] Andrew S. Tanenbaum. *Computer Networks*. Prentice Hall, 3 edition, 1996.

[Tel05] Teleco.com.br. Brasil se consolida entre os 5 países com mais celulares no mundo. http://www.teleco.com.br/comentario/com142.asp, 2005.