Redes de Computadores

Camada de rede: protocolo ipv6

Versão 1.0
Abril de 2017

Prof. Jairo

jairo@uni9.pro.br
professor@jairo.pro.br

http://www.jairo.pro.br/

Sumário

1 – Protocolo ipv6

1.1 – Necessidade de usar ipv6 ao invés de ipv4

Desde 1981 que é usada a versão 4 do protocolo IP (ipv4). Desde então, mesmo sofrendo correções como foi a alteração de *classfull* para *classless*, esta versão tem conseguido atender e se adequar às novas condições da internet que não tem parado de crescer. No entanto, por ser de apenas 32 bits, o número teórico máximo de endereços IP do ipv4 não atende mais à demanda, problema este que se agrava a cada dia que passa. Técnicas como NAT[1] têm sido usadas para contornar a exaustão dos endereços públicos ipv4, mas não sabemos até quando ainda será possível continuar adiando a adoção definitiva do ipv6.

O ipv6 usa 128 bits para o endereço IP, que dá um número de undereços muitas ordens de grandeza maior que o ipv4:

ipv4: 2^{32} => $4{,}3x10^{9}$
ipv6: 2^{128} => $3{,}4x10^{38}$

Atualmente, a população da Terra já ultrapassou os 7 bilhões ($7x10^{9}$) de habitantes, portanto já existe muito mais gente do que disponibilidade de endereços IP na versão 4. Mesmo sem considerar a internet das coisas, está bastante claro que o futuro da internet exige uma nova versão, devido às limitações do ipv4.

É claro também que a nova versão não modificará radicalmente as coisas conforme vinham sendo feitas na versão anterior, apenas vai introduzir melhorias e algumas novidades.

1.2 – Mudanças mais importantes entre ipv4 e ipv6

Abaixo segue uma lista das mudanças mais importantes entre ipv4 e ipv6.

- **Aumenta o espaço de endereçamento**: de 32 para 128 bits;
- **Espaço de endereçamento hierárquico**: o tamanho do endereço foi expandido para permitir divisão hierárquica e prover um número grande de classes de endereços. Este tem sido um tema ainda bastante discutido, por remeter de volta ao *classfull*, pois não faz subnet menor que 64 bits;
- **Atribuição hierárquica de endereços *unicast***: foi criado um formato global de endereço *unicast* para permitir que os endereços sejam facilmente alocados na internet inteira. Permite múltiplos níveis de redes e sub redes para ISP (*Internet Service*

1 NAT: *Network Address Translation* é técnica de tradução de endereços IP ao passar de uma rede para outra. Por exemplo, ao sair da rede interna, o pacote de dados com endereço IP privado (192.168.1.10) é traduzido para o endereço público 186.251.39.91.

Provider, fornecedor de acesso à internet) e também para os demais níveis organizacionais. Também permite a geração de endereço IP baseado no endereço de hardware, tal como Ethernet MacAddress. Ao contrário do ipv4, em ipv6 não existe suporte a *broadcast*;

- **Melhor suporte para endereçamento não-*unicast***: além de melhorar o suporte a *unicast*, foi adicionado um novo tipo de endereçamento, que é o *anycast*. Este novo tipo de endereçamento basicamente diz para direcionar a mensagem para o membro do grupo mais fácil de alcançar. Isso tem o potencial de permitir novos tipos de funcionalidades de envio de mensagens. Conceitualmente, *anycast* pode ser considerado um intermediário entre *multicast* e *unicast*. Por exemplo, *unicast* diz "envie para este endereço específico", *multicast* diz "envie para cada membro deste grupo" e *anycast* diz "envie para qualquer um que seja membro deste grupo". Deste modo, *anycast* pode ser normalmente considerado como "envie para o membro mais próximo deste grupo";
- **Conectividade fim a fim**: após ipv6 ser completamente implementado, cada sistema terá um endereço IP único e poderá cruzar a internet sem uso de NAT ou outro componente de tradução. Cada *host* poderá acessar diretamente o outro;
- **Autoconfiguração e renumeração**: foi incluída uma provisão para permitir fácil autoconfiguração de *hosts* e renumeração de endereços IP em redes e sub redes, conforme for necessário. Um recurso implementado em ipv6 permite aos dispositivos se autoconfigurarem independentemente, sem necessidade de DHCP[2];
- **Novo formato de datagrama (cabeçalho simplificado)**: foi redefinido o formato do datagrama IP e incluídas novas capacidades. O principal cabeçalho de cada datagrama IP foi simplificado e também foi incluído suporte para facilmente estender o cabeçalho dos datagramas que necessitarem de mais informações de controle;
- **Suporte para qualidade do serviço**: foi incluída a funcionalidade QoS (*Quality of Service*, qualidade do serviço) nos datagramas ipv6 para permitir melhor suporte para multimídia e outras aplicações que requerem QoS;
- **Suporte à segurança**: o suporte à segurança foi projetado para o ipv6 pelo uso de autenticação e cabeçalhos com extensão de encriptação, além de outras funcionalidades. É usado IPSec (*IP Security Protocols*) similar ao ipv4;
- **Fragmentação atualizada e procedimentos de remontagem**: a nova maneira de trabalhar a fragmentação e remontagem de datagramas mudou com o ipv6 para incrementar a eficiência do roteamento e melhor refletir a realidade das redes atuais;
- **Modernizado o suporte ao roteamento**: o protocolo ipv6 foi desenvolvido para suportar os sistemas de roteamento modernos e permitir a expansão à medida que a internet cresce. O cabeçalho simplificado facilita a decisão de roteamento, tornando o encaminhamento de pacotes mais rápido;
- **Capacidades de transição**: como foi reconhecido desde o início que a mudança de ipv4 para ipv6 seria um grande passo, o suporte à transição ipv4/ipv6 foi providenciado em numerosas áreas. Isso inclui um plano de interoperação entre redes ipv4 e ipv6 e mapeamento entre endereços ipv4 e ipv6.

Algumas mudanças dignas de nota é substituição de ICMP por ICMPv6 e a adição do NDP (*Neighbor Discovery Protocol*, protocolo de descobrimento de vizinhança). O NDP realiza diversas

2 DHCP: *Dynamic Host Configuration Protocol* é um protocolo padrão para distribuir dinamicamente endereços IP para interfaces e serviços. Se não for usado DHCP, o endereço IP precisa ser configurado manualmente, e neste caso é dito endereço estático.

funções que antes eram feitas pelo ARP (*Address Resolution Protocol*) do ipv4.

Entre outras funcionalidades, o NDP tem o recurso de descobrir *hosts* e roteadores e criar uma lista de roteadores locais. Se não for usado NDP, a lista de roteadores locais precisa ser configurada manualmente.

1.3 – Cabeçalho (*header*) ipv4 e ipv6

O Protocolo da Internet (camanda OSI 3) divide os segmentos da camada de transporte (camanda 4 OSI) em datagramas IP (pacotes). Os pacotes encapsulam os dados recebidos da camada de cima e adicionam as suas próprias informações de cabeçalhos.

Os dados assim encapsulados são referenciados como carga útil IP (IP *payload*), e o cabeçalho IP contém toda a informação necessária para encaminhar o pacote até o seu endereço de destino.

1.3.1 – Cabeçalho ipv4

O cabeçalho ipv4 é mostrado na Tabela 1, abaixo:

<table>
<tr><td>Versão (4 bits)</td><td>IHL (4 bits)</td><td>DSCP (6 bits)</td><td>ECN (2 bits)</td><td colspan="2">Comprimento Total (16 bits)</td></tr>
<tr><td colspan="4">Identificação (16 bits)</td><td>Flags (3 bits)</td><td>Fragment Offset (13 bits)</td></tr>
<tr><td colspan="2">Time to Live (8 bits)</td><td colspan="2">Protocolo (8 bits)</td><td colspan="2">Checksum do cabeçalho (16 bits)</td></tr>
<tr><td colspan="6">Endereço de origem (32 bits)</td></tr>
<tr><td colspan="6">Endereço de destino (32 bits)</td></tr>
<tr><td colspan="6">Opcões [preenchimento]</td></tr>
</table>

Tabela 1: cabeçalho ipv4

Onde:

- **Versão**: ipv4;
- **IHL**: Comprimento total do cabeçalho Internet (*Internet Header Length*);
- **DSCP**:[3] Ponto de Código de Serviços Diferenciados (*Differentiated Services Code Point*), é o antigo Tipo do Serviço (*Type of Service* - TOS). Este campo é usado para classificar a precedência do pacote em acordo com a Qualidade do Serviço (*Quality of Service* - QoS);
- **ECN**: Notificação Explícita de Congestionamento (*Explicit Congestion Notification*), carrega informação sobre a congestão vista na rota;
- **Comprimento Total** (*Total Length*): é o comprimento inteiro do pacote IP, incluindo IP *Header* e IP *Payload*;

3 NOTA: Em 1998 DSCP e ECN substituiram o antigo campo Tipo do Serviço TOS (*Type of Service*), que era de 8 bits. Atualmente, o TOS é realizado pelo DiffServ (Serviços Diferenciados - *Differentiated services*), que provê Qualidade do Serviço (*Quality of Service* – QoS) com o uso dos campos DSCP e ECN.

- **Identificação** (*Identification*): se o pacote foi fragmentado durante a transmissão, todos os fragmentos contêm o mesmo número de identificação, isto para identificar o pacote IP original ao qual estes fragmentos pertencem;
- **Flags** (marca): caso o pacote seja muito grande, e se for requerido pelos recursos de rede, o campo *flags* indica se pode ser fragmentado ou não;
- **Fragment Offset** (Compensação de Fragmentação): indica a posição exata do fragmento no pacote original;
- **Time to Live** (TTL, Tempo De Vida): para evitar loop na rede, cada pacote é enviado com algum valor de TTL, que determina para a rede por quanto roteadores (saltos ou *hops*) este pacote pode cruzar. A cada salto este valor é reduzido de uma unidade, e quando atinge o valor zero o pacote é descartado;
- **Protocolo** (*Protocol*): indica para a camada de rede do *host* de destino a qual protocolo este pacote pertence. Por exemplo, o número do protocolo ICMP é 1, TCP é 6 e UDP é 17;
- **Checksum do Cabeçalho** (*Header Checksum*): este campo é usado para guardar o valor de checksum do cabeçalho inteiro, o qual é usado para verificar se o pacote foi recebido íntegro, isto é, sem erros;
- **Endereço de Origem** (*Source Address*): endereço IP (32 bits) da origem (remetente) do pacote;
- **Endereço de Destino** (*Destination Address*): endereço IP (32 bits) de destino do pacote;
- **Opções** (*Options*): este campo é opcional, usado caso o valor de IHL seja maior que 5. Se o IHL for maior que 5 (valor entre 6 e 15, pois IHL tem apenas 4 bits), isto sinaliza que o campo de Opções está presente e precisa ser considerado. Caso não esteja usando Opções, IHL será sempre 5. O campo Opções pode conter valores para opções tais como segurança, registro de rota, time stamp (registro de data/hora), etc;
- **Preenchimento** (*padding*): o preenchimento é necessário para que o tamanho do cabeçalho do pacote seja múltiplo de 32 bits, isso devido ao tamanho variável do campo Opções. Se forem incluídas uma ou mais opções, e se o número de bits usados não for múltiplo de 32, então são adicionados bits zero para preenchimento, isso para completar um múltiplo de 4 bytes.

1.3.2 – Cabeçalho ipv6

O formato do pacote ipv6 tem três partes: um cabeçalho ipv6 básico (ou fixo), um ou mais cabeçalhos de extensão e uma unidade de dados de protocolo de camada superior (*Protocol Data Unit* – PDU).

Um PDU de camada superior (*Upper-Layer* PDU) é composto de cabeçalho de protocolo de camada superior e sua carga (payload), tal como um pacote ICMP (versão 6), um pacote TCP ou um pacote UDP.

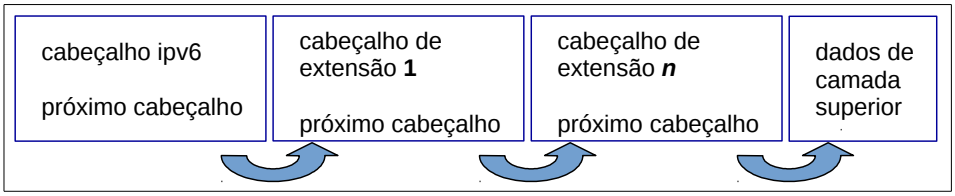
O cabeçalho ipv6 básico tem um tamanho fixo de 40 bytes (320 bits). Um esquema deste cabeçalho pode ser visto na Tabela 2, abaixo:

Versão (4 bits)	Classe de tráfego (8 bits)	Rótulo de fluxo (*Flow Label*) (20 bits)	
Extensão da carga (*Payload Length*) (16 bits)		Próximo cabeçalho (8 bits)	Salto limite (8 bits)
Endereço de origem (128 bits)			
Endereço de destino (128 bits)			
[próximo cabeçalho] [informaçoes do cabeçalho de extensão] (tamanho variável em bits)			

Tabela 2: Cabeçalho ipv6 fixo com 40 bytes.

Onde:

- **Versão**: ipv6 (número binário **0110**);
- **Classe de tráfego** (*Traffic Class*): os 8 bits deste campo estão divididos em duas partes. Os primeiros 6 bits são usados para o Tipo do Serviço (QoS), para informar ao roteador qual serviço deve ser providenciado para este pacote. Os dois últimos bits são usados para Notificação Explícita de Congestão (*Explicit Congestion Notification* – ECN);
- **Rótulo de Fluxo** (Flow Label): este rótulo é usado para manter o fluxo sequencial de pacotes pertencentes a uma comunicação. Na origem, a sequência de pacotes é rotulada para ajudar o roteador a identificar se um pacote em particular pertence a um fluxo específico de informação. Este campo ajuda a evitar o reordenamento de pacotes, e é projetado para transmissão de mídia em tempo real (*streaming* vídeo/áudio);
- **Extensão de carga** (*Payload Length*): este campo é usado para informar aos roteadores quanto de informação contém na carga (*payload*) de um pacote em particular. A carga (*payload*) é composta de Cabeçalhos de Extensão (*Extension Headers*) e dados de Camada Superior (*Upper Layer*). Cabeçalhos de Extensão são arranjados um após o outro, num modo de lista vinculada (*linked list manner*), conforme o diagrama abaixo:



- **Próximo cabeçalho** (*Next Header*): este campo é usado tanto para indicar o tipo do Cabeçalho de Extensão ou se o Cabeçalho de Extensão não está presente quanto indicar o PDU de camada superior. Os valores para o tipo do PDU de camada superior são os mesmos do ipv4;
- **Salto Limite** (*Hop Limit*): este campo é usado para impedir que o pacote permaneça indefinidamente em *loop* na rede. É o mesmo que TTL no ipv4. O valor do campo Salto Limite é decrementado em uma unidade toda vez que o pacote passa por um roteador (*hop*), e quando este valor é zerado o pacote é descartado;
- **Endereço de Origem** (*Source Address*): este campo indica o endereço IP (128 bits) da origem (remetente) do pacote;
- **Endereço de Destino** (*Destination Address*): endereço IP (128 bits) de destino do pacote;

Comparado com o cabeçalho do pacote ipv4, o cabeçalho ipv6 não carrega IHL, Identificação, *Flags*, Compensação de Fragmentação, *Checksum* do Cabeçalho, Opções e

Preenchimento, mas carrega o campo Rótulo de Fluxo. Esta simplificação facilita o processamento do pacote ipv6 e melhora a eficiência do roteamento.

Para suportar várias opções sem mudar o atual formato do pacote, o campo de informação Cabeçalho de Extensão foi adicionado ao cabeçalho do pacote, que aprimorou a flexibilidade do ipv6.

1.4 – *Network ID* e *host ID* ipv6

Um esquema do endereço ipv6 é mostrado abaixo:

```
     network ID                host ID
--------------------------  --------------------------
hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh
--------------------------  --------------------------
       64 bits                   64 bits
```

Onde **h** é um número hexadecimal. Cada número hexadecimal pode ser representado por 4 bits. Por exemplo:

binário	=	hexadecimal
0000	=	0
0001	=	1
0011	=	3
1000	=	8
1001	=	9
1010	=	A
1111	=	F

Pode ser notado que o endereço ipv6 é semelhante ao ipv4.

O *network* ID é atribuído administrativamente, já o *host* ID pode ser obtido de três maneiras:

1 – usando um número gerado aleatoriamente;
2 – usando DHCPv6;
3 – usando o formato EUI-64 (*Extended Unique Identifier*).

1.5 – *Extended Unique Identifier* (EUI-64)

O formato EUI-64 (*Extended Unique Identifier*) expande o endereço físico (MacAddress) de

48 para 64 bits pela inserção de **fffe** no meio do endereço e inverte o sétimo bit.

Por exemplo, dado o endereço MAC 44:8a:5b:94:63:9a, os passos seguidos para obter o formato EUI-64 são:

i. 44:8a:5b 94:63:9a <= divide ao meio
ii. 44:8a:5b **fffe** 94:63:9a <= insere **fffe**
iii. 44 = 0100 01**0**0 <= hexadecimal convertido para binário
iv. 46 = 0100 01**1**0 <= sétimo bit invertido
v. 46:8a:5b:ff:fe:94:63:9a <= reagrupando as partes
vi. 468a:5bff:fe94:639a <= *host* ID no formato EUI-64

1.6 – Regras de simplificação do endereço ipv6

Pelo fato da estrutura do endereço ipv6 ser muito grande, são usadas duas regras para remover zeros e simplificar o endereço. Tomando como exemplo o endereço abaixo, vamos aplicar estas regras:

2001:**0000**:**0000**:**00**b3:**0000**:5bff:fe94:639a

Regra 1: descartar os zeros à frente do número: no quarto bloco (00b3), os dois zeros devem ser omitidos. Isso leva o endereço para:

2001:0000:0000:**b3**:0000:5bff:fe94:639a

Regra 2: se dois ou mais blocos consecutivos contêm zeros, devem ser omitidos e substituídos por dois dois pontos. Isso leva o endereço para:

2001::**b3**:0000:5bff:fe94:639a

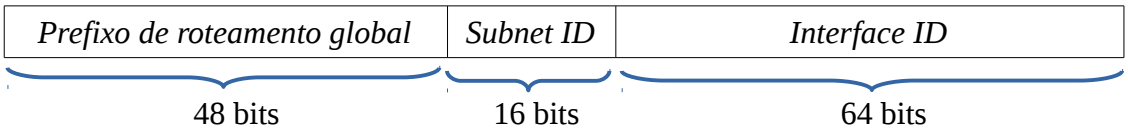
Depois disso, se ainda existirem blocos de zeros no endereço, ele apenas pode ser simplificado para um zero, nunca substituído por dois pontos. Isto leva o endereço para:

2001::**b3**:**0**:5bff:fe94:639a

1.7 – Tipos de endereços ipv6

O ipv6 define muitos tipos de endereços. Alguns exemplos são global *unicast*, *link local*, *multicast*, *anycast* e *loopback*.

Global unicast: é usado para identificar uma única interface. São endereços roteáveis na internet. Exemplo:

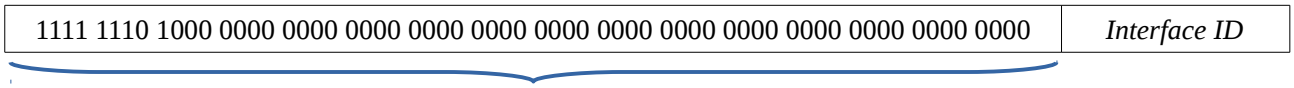


O **prefixo de roteamento global** foi dividido em 5 regiões na internet:

- APNIC (Asia/Região do Pacífico) => 2400
- ARIN (Canadá, EUA e algumas ilhas do Caribe) => 2600
- AFRINIC (África) => 2C00
- LACNIC (América Latina e algumas ilhas do Caribe) => 2800
- RIPE NCC (Europa, Oriente Médio e Ásia Central) => 2A00

Por exemplo, o endereço de internet ipv6 **2804:14c:139:9acb:267a:5bff:fe34:2035** está na região **LACNIC**, mais precisamente no Brasil, pois tem prefixo **2804**.

***Link* local**: são usados para permitir comunicação entre dispositivos na rede local. Estes endereços sempre iniciam por fe80 (1111 1110 1000 0000), e os 48 bits seguintes são zero. Exemplo:



Por exemplo, o endereço ipv6 **fe80::267a:5bff:fe34:2035** é um ***link* local**.

NOTA: uma mesma interface de rede normalmente pode conter mais de um endereço ipv6. Por exemplo, pode conter um IP global e também um IP local.

Multicast: a transmissão *multicast* envia datagramas de uma para todas as interfaces que são parte do grupo *multicast*. O grupo é representado pelo endereço de destino do datagrama. Os endereços *multicast* iniciam por **ff**. Exemplos:

ff02::1 => todos os nós no segmento local da rede

ff02::2 => todos os roteadores no segmento local da rede

Anycast: o endereço *anycast* identifica múltiplas interfaces de nós de destino. Uma transmissão *anycast* envia datagramas de um para somente uma das interfaces associada a um membro do grupo, e não para todos os membros do grupo. Esta interface é tipicamente a mais próxima, conforme definido pelo protocolo de roteamento.

Loopback: é usado por um nó para enviar o pacote para ele mesmo. Funciona do mesmo modo que no ipv4. Exemplo:

0000:0000:0000:0000:0000:0000:0000:0001/128, que é representado como **::1/128** ou simplesmente **::1**.

Em ipv6, o endereço especial que representa o *default gateway* (rota padrão) é:

::/0

Outro aspecto importante a ser notado é o formato usado com aplicações. Exempolo:

http://[2001:db8:f0b:1af0::1]/index.html	<= endereço em URL
http://[2001:db8:f0b:1af0::1]:443/index.html	<= endereço e porta em URL
[2001:db8:f0b:1af0::1]:21	<= porta TCP
2001:db8:f0b:1af0::1/64	<= endereço na notação CIDR
2001:db8:f0b:1af0::1%eth0	<= identificação de zona
ssh user@2001:db8:f0b:1af0::1%eth0	<= acesso SSH na zona
scp arquivo 2001:db8:f0b:1af0::1%eth0/diretorio	<= transferência scp

Mas nas redes internas os endereços privados ipv4 estão sendo usados com sucesso e sem previsão de exaustão mesmo para redes muito grandes. Desse modo, parece difícil que alguém queira alterar os endereços internos de ipv4 para ipv6, especialmente porque pode muito bem continuar sendo usado NAT com ipv4 nas redes internas, e migrado para ipv6 para endereços públicos.

Um ponto importante a ser considerado a respeito do ipv6 é que, embora já esteja sendo adotado gradualmente, ele ainda é um projeto em desenvolvimento. Portanto, alguns conceitos usados hoje poderão muito bem ser alterados amanhã caso não se mostrem adequados ao uso real na internet.