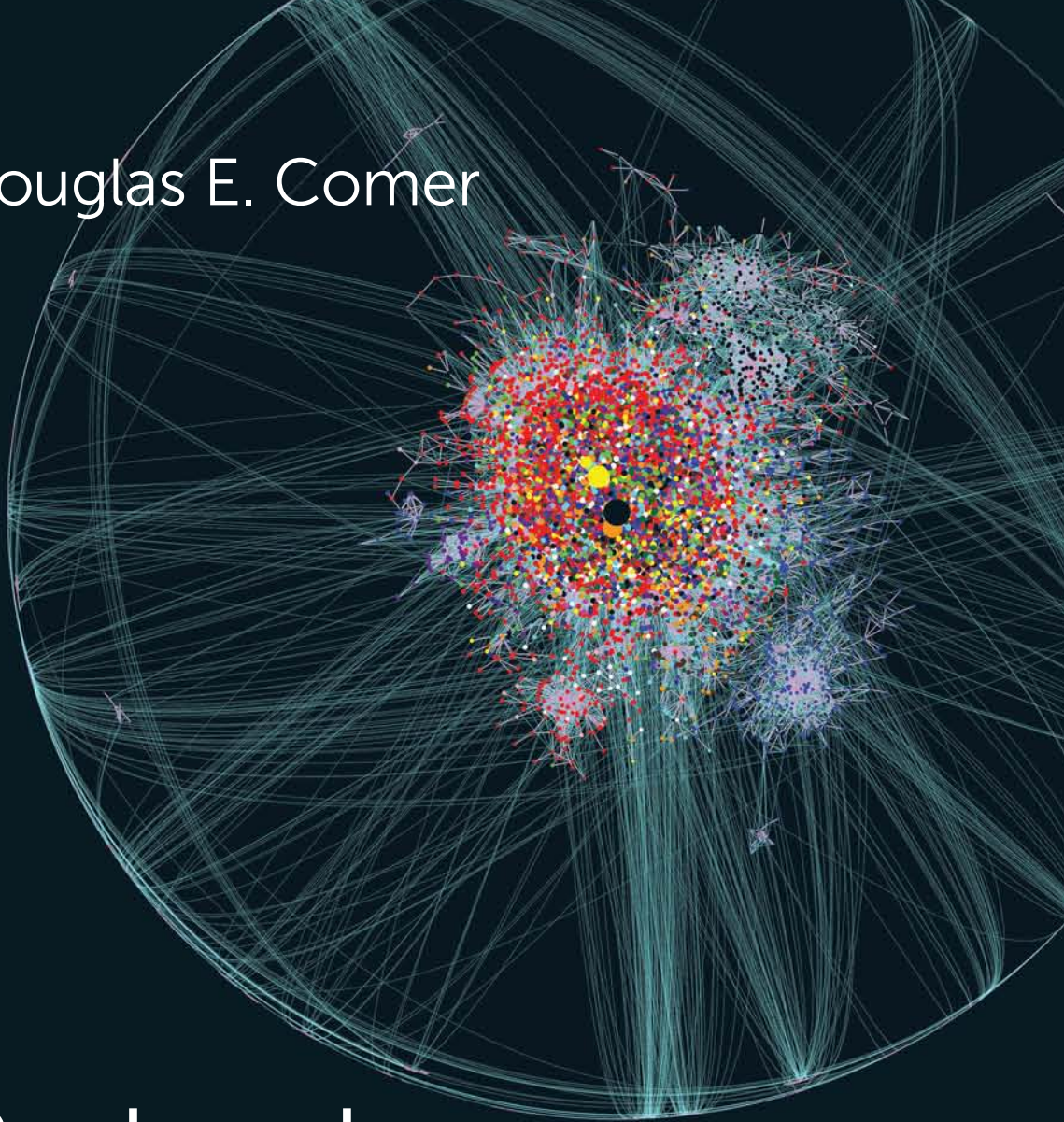


Douglas E. Comer



Redes de Computadores e Internet



6ª EDIÇÃO

O autor

Dr. Douglas Comer é um internacionalmente reconhecido especialista em redes de computadores, protocolos TCP/IP e Internet. Foi um dos pesquisadores que contribuíram com a formação da Internet no fim dos anos 1970 e nos anos 1980, sendo membro do *Internet Architecture Board*, o grupo responsável por guiar o desenvolvimento da Internet. Também foi presidente do comitê técnico CSNET, membro do comitê executivo CSNET e presidente do Distributed Systems Architecture Board da DARPA (*Defense Advanced Research Projects Agency*). Foi ainda Vice-Presidente de Pesquisa na Cisco Systems.

Comer é consultor de projeto de redes de computadores para empresas e palestrante frequente em ambientes acadêmicos e profissionais ao redor do mundo. Seu sistema operacional, Xinu, e a implementação de protocolos TCP/IP (ambos documentados em seus livros) são utilizados em produtos comerciais. É professor honorário de Ciências da Computação na Purdue University, onde leciona redes de computadores, redes de internet, arquitetura de computadores e sistemas operacionais. Lá desenvolveu laboratórios de informática inovadores que dão aos alunos a oportunidade de ter experiências práticas na operação de sistemas, redes de computadores e protocolos.

Além de escrever livros técnicos *best-sellers*, já traduzidos para 16 idiomas, atuou como editor norte-americano do periódico *Software – Practice and Experience* por 20 anos. Comer é membro da ACM. Informações adicionais podem ser encontradas em: www.cs.purdue.edu/homes/comer.



C732r Comer, Douglas E.
Redes de computadores e internet [recurso eletrônico] /
Douglas E. Comer ; tradução: José Valdeni de Lima, Valter
Roesler. – 6. ed. – Porto Alegre : Bookman, 2016.

Editado como livro impresso em 2016.
ISBN 978-85-8260-373-4

1. Redes de computadores. 2. Internet. I. Título.

CDU 004.7

IP: endereçamento da Internet

- 21.1 Introdução, 301
- 21.2 A mudança para o IPv6, 302
- 21.3 O modelo de amпуheta e a dificuldade de mudar, 302
- 21.4 Endereços para a Internet virtual, 302
- 21.5 O esquema de endereçamento IP, 304
- 21.6 A hierarquia do endereço IP, 304
- 21.7 Classes originais de endereços IPv4, 304
- 21.8 Notação decimal pontilhada IPv4, 306
- 21.9 Autoridade para endereços, 306
- 21.10 Sub-rede IPv4 e endereçamento classless, 307
- 21.11 Máscaras de endereço, 308
- 21.12 A notação CIDR usada com o IPv4, 309
- 21.13 Um exemplo CIDR, 310
- 21.14 Endereços nos hosts CIDR, 311
- 21.15 Endereços especiais IPv4, 311
- 21.16 Resumo dos endereços especiais do IPv4, 313
- 21.17 Forma de endereço Berkeley broadcast para o IPv4, 314
- 21.18 Roteadores e princípios de endereçamento IPv4, 314
- 21.19 Multihomed hosts, 315
- 21.20 Multihoming no IPv6 e renumeração, 316
- 21.21 Endereçamento IPv6, 316
- 21.22 Notação hexadecimal com separação através de “:” do IPv6, 317
- 21.23 Resumo, 318

21.1 Introdução

O capítulo anterior explica a arquitetura física da Internet, na qual os roteadores interconectam as redes físicas. Este capítulo começa com uma descrição do software de protocolo que faz a Internet parecer um único sistema de comunicação integrado. O capítulo apresenta o esquema de endereçamento usado pelo *protocolo de Internet* e discute o uso de máscaras de endereço. A Internet está em transição entre a versão 4 do IP (*IPv4*) e a versão 6 do IP (*IPv6*)¹. Consequentemente, o capítulo abrange ambas as versões. O texto apresenta princípios gerais que se aplicam a ambas as versões e, em seguida, apresenta detalhes sobre IPv4 e IPv6.

Os próximos capítulos expandem a descrição do IP. Cada um deles considera um dos aspectos do protocolo em detalhe. Tomados como um grupo, os capítulos definem o protocolo IP e explicam como o software permite aos computadores trocar pacotes através da Internet.

¹ Por razões políticas e históricas, a versão 5 não foi implementada.

21.2 A mudança para o IPv6

Antes de considerarmos endereçamento em IPv4 e em IPv6, é importante entender a mudança que está ocorrendo. O IPv4 tem sido extremamente bem-sucedido. O projeto permitiu que a Internet acomodasse redes heterogêneas, mudanças dramáticas na tecnologia de hardware e aumentos extremos na escala. A versatilidade e a escalabilidade do IPv4 são evidentes a partir das aplicações que o utilizam e do tamanho da Internet global. Para resumir:

O sucesso do IPv4 é incrível – o protocolo tem acomodado as mudanças de tecnologia de hardware, redes heterogêneas e de escala extremamente larga.

Se o IP funciona tão bem, por que mudar? Quando o IPv4 foi definido, apenas alguns computadores existiam nas redes. Os projetistas decidiram usar endereço de 32 bits para o IP, pois isso permite que a Internet inclua mais de 1 milhão de redes. No entanto, a rede Internet global continua a crescer exponencialmente, com o tamanho duplicando em menos de um ano. Todos os endereços IPv4 já foram atribuídos. Assim, a principal motivação para a definição de uma nova versão do IP foi a limitação de espaço de endereço – eram necessários endereços maiores para acomodar o crescimento contínuo da Internet.

21.3 O modelo de ampulheta e a dificuldade de mudar

Embora a aparente escassez de endereços restantes tenha sido considerada crucial, quando o trabalho começou, visando a obtenção de uma nova versão do IP, em 1993, nenhuma situação de emergência ocorreu, e as organizações estavam relutantes em mudar para uma nova versão. Para entender o porquê, é preciso pensar na importância do IP e no custo da mudança. Em termos de importância, o IP é o centro da comunicação via Internet – todos os aplicativos usam o IP e ele funciona sobre todas as tecnologias de redes. Profissionais de rede dizem que a comunicação Internet segue um *modelo de ampulheta* e que o IP está na posição em que a ampulheta é fina. A Figura 21.1 ilustra o conceito.

Um ponto importante decorre da dependência do IP e da consequência da inércia que ele introduz.

Como o IP é central para todas as comunicações realizadas pela Internet, substituí-lo requer uma mudança na Internet inteira.

21.4 Endereços para a Internet virtual

Lembre-se do que vimos no Capítulo 20: o objetivo da ligação inter-redes é fornecer um sistema integrado de comunicações. Para atingi-lo, o software de protocolo deve esconder os detalhes das redes físicas e oferecer a ilusão de se tratar de uma única grande rede. Do ponto de vista de um aplicativo, a Internet virtual funciona como qualquer rede, permitindo que os computadores enviem e recebam pacotes. A principal diferença entre a Internet e uma rede física é que aquela é uma abstração imaginada por seus projetistas e criada inteiramente por software de protocolo. Assim, os projetistas escolhem endereços, formatos de pacotes e técnicas de distribuição independentes dos detalhes do hardware.

O endereçamento é um componente fundamental da abstração Internet. Para aparentarem ser uma única rede, todos os computadores hosts devem usar um esquema de endereçamento uniforme, e cada endereço deve ser exclusivo. Embora cada computador tenha um endereço MAC, tais endereços não são suficientes, porque a Internet pode incluir várias tecnologias de rede e cada uma delas define seus próprios endereços MAC.

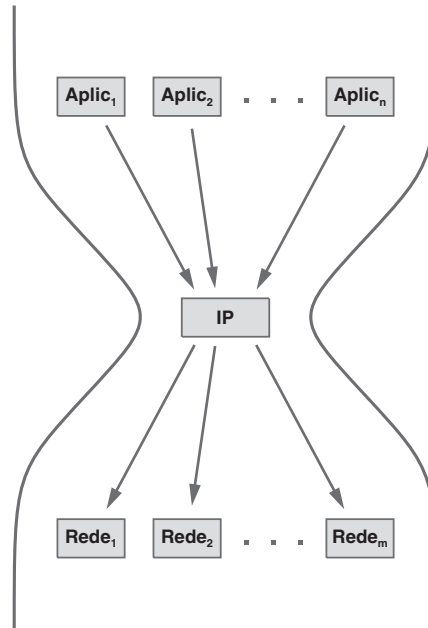


Figura 21.1 O modelo amulheta de comunicação Internet com o IP ao centro.

Para garantir um endereçamento uniforme, o IP define um esquema de endereçamento que é independente dos endereços MAC. Os endereços IP são usados como destinos na Internet assim como os endereços MAC são utilizados como destinos em uma LAN. Para enviar um pacote através da Internet, o remetente coloca o endereço IP do destino no pacote e passa o pacote ao software do protocolo IP para encaminhamento. O software do protocolo IP usa o endereço IP de destino quando encaminha o pacote através da Internet para o computador de destino.

A vantagem do endereçamento IP é a uniformidade: um par arbitrário de aplicativos pode se comunicar sem saber o tipo de hardware de rede ou os endereços MAC usados. A transparência é tanta que alguns usuários ficam surpresos ao saber que os endereços IP são fornecidos pelo software do protocolo e não pela rede. Curiosamente, nós veremos que muitas camadas do software do protocolo usam endereços IP. Em síntese:

Para fornecer endereçamento uniforme na Internet, o IP define um esquema de endereçamento abstrato que atribui a cada host um endereço de protocolo único; aplicativos usam endereços IP para se comunicar.

21.5 O esquema de endereçamento IP

O IP especifica que para cada host é atribuído um número exclusivo conhecido como *endereço do protocolo Internet*, *endereço IP* ou *endereço Internet*². O IPv4 usa endereços de 32 bits e o IPv6 usa endereços de 128 bits. Ao enviar um pacote através da Internet, o remetente deve especificar seu próprio endereço IP (endereço de origem), bem como o endereço do destinatário (endereço de destino).

Para resumir:

Um endereço IP é um número binário atribuído ao host e usado durante toda a comunicação com o host. O IPv4 usa endereços de 32 bits e o IPv6 usa endereços de 128 bits.

21.6 A hierarquia do endereço IP

Assim como o endereçamento hierárquico utilizado nas WANs, cada endereço IP é dividido em duas partes: um prefixo e um sufixo. Ao contrário de uma WAN tradicional, a Internet não usa comutadores de pacotes. Em vez disso, um prefixo IP identifica a rede física à qual o host está conectado e um sufixo IP identifica um computador específico na rede. Ou seja, a cada rede física na Internet é atribuído um *número de rede* exclusivo. O número de rede aparece como um prefixo do endereço IP de cada computador conectado à rede, e a cada computador em uma determinada rede física é atribuído um sufixo único.

Para garantir a unicidade, o mesmo número de rede não pode ser atribuído a duas redes na Internet, e um gerente de rede deve ter certeza de que não há dois computadores de uma determinada rede com o mesmo sufixo. Por exemplo, se uma internet contém três redes, a elas podem ser atribuídos os números de rede 1, 2 e 3. A três computadores conectados à rede 1 podem ser atribuídos os sufixos 1, 3 e 5, enquanto a três computadores conectados à rede 2 podem ser atribuídos os sufixos 1, 2 e 3. Os valores atribuídos não precisam ser contíguos.

O mais importante é que o esquema de endereços IP garante duas propriedades:

- A cada computador é atribuído um endereço único (isto é, um único endereço nunca é atribuído a mais de um computador).
- Embora as atribuições do número de rede devam ser coordenadas globalmente, os sufixos podem ser atribuídos localmente sem uma coordenação global.

A primeira propriedade é garantida porque um endereço IP contém um prefixo e um sufixo. Se dois computadores estão conectados a redes físicas diferentes, os prefixos atribuídos a seus endereços serão diferentes. Se dois computadores estão ligados à mesma rede física, os sufixos atribuídos aos respectivos endereços serão diferentes. Assim, o endereço atribuído a cada computador é único.

21.7 Classes originais de endereços IPv4

Uma vez que escolheram um tamanho para os endereços IP e decidiram dividir cada endereço em duas partes, os projetistas do IPv4 tiveram que determinar quantos bits

² Os três termos são usados como sinônimos.

teria cada parte. O prefixo precisaria ter bits suficientes para permitir que um número de rede único fosse atribuído a cada rede física na Internet. O sufixo precisaria ter bits suficientes para permitir que a cada computador conectado a uma rede fosse atribuído um sufixo único. Nenhuma escolha simples foi possível, porque adicionar bits em uma parte significaria subtrair bits da outra. Escolher um prefixo grande significa ter muitas redes, mas limita o tamanho delas; escolher um sufixo grande significa ter redes físicas com muitos computadores, mas limita o número total de redes.

Como a Internet inclui tecnologias para quaisquer redes, ela contém algumas redes físicas grandes e muitas redes pequenas. Consequentemente, os projetistas optaram por um esquema de endereçamento que acomodasse uma combinação de redes grandes e pequenas. O esquema original, conhecido como *classful IP addressing*, dividiu o espaço de endereço IPv4 em três *classes* primárias, cada uma com prefixo e sufixo de tamanhos diferentes.

Os primeiros quatro bits de um endereço determinaram a classe a que pertencia um endereço e especificaram como a parte restante do endereço foi dividida em prefixo e sufixo. A Figura 21.2 ilustra as cinco classes de endereços, os bits principais usados para identificar cada classe e a divisão em prefixo e sufixo. A figura segue a convenção usada em protocolos TCP/IP de numeração de bits da esquerda para a direita e de utilização de zero para o primeiro bit.

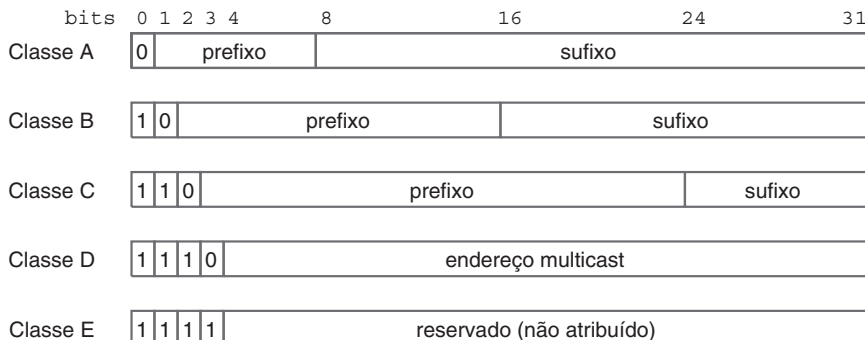


Figura 21.2 As cinco classes do endereço IPv4 no esquema original *classful*.

Embora o esquema *classful* tenha sido substituído, os endereços de classe *D* ainda são usados para multicasting; eles permitem a entrega para um conjunto de computadores. Cada endereço de multicast corresponde a um grupo de computadores. Uma vez que um grupo multicast tenha sido estabelecido, uma cópia de qualquer pacote enviado para o endereço de multicast será entregue a cada host do grupo. Na prática, a Internet multicasting nunca esteve disponível globalmente, o que significa que o multicasting é restrito aos locais individuais.

Podemos resumir:

O esquema de endereçamento IPv4 original dividiu endereços em classes. Os endereços da classe D ainda são usados para multicasting, mas este não está disponível em toda a Internet global.

21.8 Notação decimal pontilhada IPv4

Embora os endereços IPv4 sejam números de 32 bits, os usuários não entram ou leem os valores em binário. Em vez disso, ao interagir com um usuário, o software usa uma notação que é mais conveniente para a compreensão humana. Chamada *notação decimal pontilhada*, a forma expressa cada seção de 8 bits de um número de 32 bits como um valor decimal e usa um ponto decimal para separar as seções. A Figura 21.3 ilustra exemplos de números binários e a notação decimal equivalente.

Número binário de 32 bits	Notação decimal pontilhada equivalente
10000001 00110100 00000110 00000000	129.52.6.0
11000000 00000101 00110000 00000011	192.5.48.3
00001010 00000010 00000000 00100101	10.2.0.37
10000000 00001010 00000010 00000011	128.10.2.3
10000000 10000000 11111111 00000000	128.128.255.0

Figura 21.3 Exemplos de números binários de 32 bits e seus equivalentes na notação decimal pontilhada usados com o IPv4.

A notação decimal pontilhada trata cada *octeto* (valor de 8 bits) como um binário inteiro sem sinal³. Como exemplo final, na figura é mostrado o menor valor possível, 0, que ocorre quando todos os bits de um octeto são iguais a zero, e o maior valor possível, 255, que ocorre quando todos os bits de um octeto são iguais a 1. Assim, os endereços decimais pontilhados variam de 0.0.0.0 até 255. 255. 255. 255. Os endereços multicast, classe D, ocupam a faixa de 224.0.0.0 até 239. 255. 255. 255.

Para resumir:

A notação decimal pontilhada é uma forma sintática que o software IPv4 usa para expressar valores binários de 32 bits ao interagir com seres humanos. O decimal pontilhado representa cada octeto em decimal e usa um ponto para separar os octetos.

21.9 Autoridade para endereços

Cada prefixo atribuído a uma rede individual na Internet deve ser único. Portanto, uma organização central deve distribuir os prefixos. Atualmente, a responsabilidade recai sobre a *Internet Corporation for Assigned Names and Numbers* (ICANN). Com o crescimento da Internet além de suas fontes de pesquisa, a ICANN foi criada especificamente para lidar com a atribuição de endereços e julgar conflitos.

A ICANN não atribui prefixos individuais diretamente. Em vez disso, ela autoriza o uso de um conjunto de *registradores*. Cada região geográfica tem um registrador (por exemplo, há um para a América do Norte, um para a Europa e assim por diante). Os

³ Os protocolos de Internet usam o termo *octeto* mais frequentemente do que o termo *byte*, porque este depende do computador utilizado. Assim, embora bytes de 8 bits sejam o padrão de fato, o termo octeto não é ambíguo.

registradores possuem grandes blocos de endereços disponíveis para os ISPs principais, que, por sua vez, tornam-os disponíveis para os ISPs menores. Os ISPs conectam assinantes e fornecem a eles um conjunto de prefixos para suas redes. Assim, para obter um prefixo de rede, uma organização ou um indivíduo contata um ISP.

21.10 Sub-rede IPv4 e endereçamento classless

Com o crescimento da Internet, o esquema de endereçamento IPv4 *classful* original tornou-se uma limitação. Dois novos mecanismos foram criados para superar a limitação:

- Endereçamento de sub-rede
- Endereçamento classless

Os dois mecanismos estão tão intimamente relacionados que podem ser considerados parte de uma única abstração: em vez de ter três classes distintas de endereço, permitem a ocorrência de divisão entre o prefixo e o sufixo em um limite de bits qualquer. O endereçamento da sub-rede foi inicialmente usado dentro de grandes organizações que, ao se conectarem à Internet global, estenderam a mesma abordagem de endereçamento classless para toda a Internet. A ideia foi também adotada pelo IPv6.

Para entender os motivos da utilização de um limite arbitrário, considere um ISP que distribui prefixos. Suponha que um cliente do ISP solicita um prefixo para uma rede que contém 35 hosts. Quando o endereçamento classful era usado, o ISP atribuía um prefixo de classe C. De fato, apenas 6 bits do sufixo do host são necessários para representar todos os valores dos 35 hosts, o que significa que 219 dos 254 possíveis sufixos nunca seriam atribuídos aos hosts⁴. Em outras palavras, a maior parte do espaço do endereço da classe C é desperdiçada.

Infelizmente, com o crescimento da Internet tornou-se óbvio que todos os endereços poderiam, eventualmente, ser necessários – não poderíamos deixar endereços sem uso. O endereçamento classless resolveu o problema permitindo a um ISP atribuir um prefixo de tamanho mais apropriado. No nosso exemplo, um ISP que usa o endereçamento classless pode atribuir um prefixo que tem 26 bits de comprimento. Como um endereço IPv4 contém 32 bits, o sufixo é de 6 bits de comprimento, o que significa que 62 sufixos são possíveis. Como resultado, apenas 27 endereços ficarão sem uso.

Outra maneira de verificar a situação é assumir que o ISP possui um prefixo classe C. O endereçamento classful atribui o prefixo a uma organização. Com o endereçamento classless, no entanto, o ISP pode dividir o prefixo em vários prefixos mais longos e atribuir cada um deles a um assinante. A Figura 21.4 ilustra como um endereçamento classless permite a um ISP dividir um prefixo classe C em quatro prefixos mais longos que podem acomodar uma rede de até 62 hosts.

Na figura, a parte do host de cada prefixo é mostrada em cinza. O endereço de classe C original tem 8 bits de sufixo, e cada um dos endereços classless tem 6 bits de sufixo. Assumindo que o prefixo original de classe C é único, cada um dos prefixos classless também será único. Assim, em vez de desperdiçar os endereços, o ISP pode atribuir cada um dos quatro prefixos classless a um assinante com 62 ou menos hosts.

⁴ O número 254 surge porque um endereço de classe C tem 256 sufixos possíveis e todos os sufixos 0s e todos os sufixos 1s são reservados para transmissão de sub-rede, como descrito posteriormente neste capítulo.

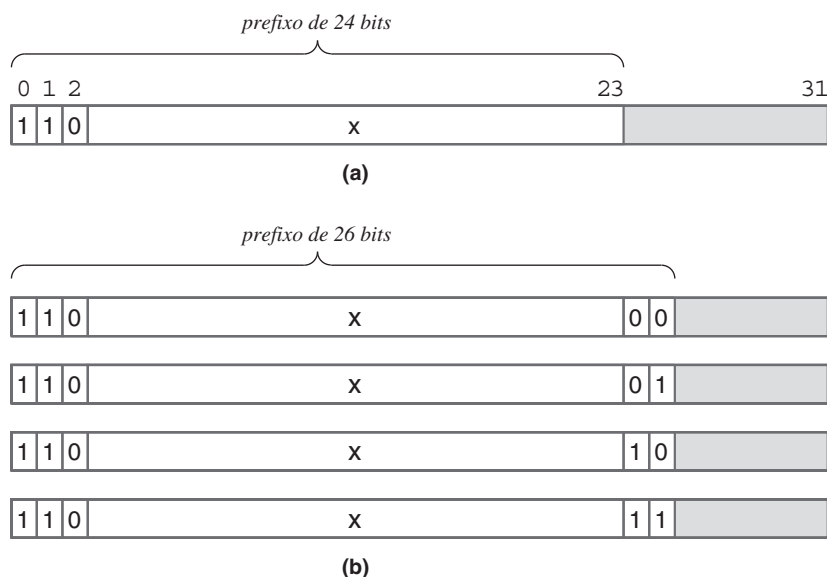


Figura 21.4 (a) Um prefixo classe C do IPv4 e (b) o mesmo prefixo dividido em quatro prefixos classless.

21.11 Máscaras de endereço

Como um endereço IP pode ser dividido em partes de tamanhos arbitrários? Os esquemas de endereçamento classless e de sub-rede exigem hosts e roteadores que processem os endereços para armazenar uma peça adicional de informação: um valor que especifique o limite exato entre o prefixo da rede e o sufixo do host. Para marcar o limite, o IPv4 utiliza um valor de 32 bits (e o IPv6 usa um valor de 128 bits), conhecido como máscara de endereço, que foi originalmente chamado de *máscara de sub-rede*. Uma *máscara de endereço* tem bits “1” para marcar o prefixo de rede e bits “0” para marcar a parte do host.

Por que utilizar uma máscara de bits? Uma máscara torna o processamento eficiente. Em particular, vamos ver que, quando lidam com um pacote IP, hosts e roteadores precisam comparar a parte do prefixo da rede do endereço com um valor em suas tabelas de encaminhamento. A representação através de uma máscara de bits torna a comparação eficiente. Para compreender como, suponha que a um roteador usando o IPv4 é dado um endereço D de destino, um prefixo de rede representado por um valor N de 32 bits e uma máscara de endereço M de 32 bits. Ou seja, assuma que os bits mais altos de N contêm um prefixo de rede e que os bits restantes estão zerados. Para verificar se o destino está na rede especificada, o roteador testa a condição:

$$N == (D \& M)$$

Isto é, ele utiliza a máscara com uma operação lógica *and* para definir os bits do host do endereço D para zero e então compara o resultado com o prefixo de rede N .

Como exemplo, utilizando o IPv4, considere o seguinte prefixo de rede de 32 bits:

10000000 00001010 00000000 00000000

Ele tem o valor decimal pontilhado *128.10.0.0*. Considere também uma máscara de 32 bits que tem 16 bits 1 seguidos por 16 bits 0, que pode ser representada em decimal pontilhado como *255.255.0.0*:

11111111 11111111 00000000 00000000

Agora, considere o endereço de destino de 32 bits *128.10.2.3*, que tem um equivalente binário de:

10000000 00001010 00000010 00000011

Um *and* lógico do endereço de destino e a máscara de endereço extraem os 16 bits de alta ordem, o que produz o resultado binário:

10000000 00001010 00000000 00000000

que é igual ao prefixo de rede *128.10.0.0*.

21.12 A notação CIDR usada com o IPv4

O esquema de endereçamento classless é formalmente conhecido como *Classless Inter-Domain Routing* (CIDR). O nome não é adequado, porque CIDR especifica apenas endereçamento e encaminhamento. Quando o esquema de endereçamento CIDR foi criado, os projetistas queriam tornar mais compreensível para um ser humano a especificação de uma máscara. Para compreender a dificuldade, considere a máscara necessária para o exemplo na Figura 21.4 (b), que tem 26 bits 1 seguidos de 6 bits 0. Em notação decimal pontilhada, a máscara é:

255.255.255.192

Para tornar mais compreensível para os seres humanos a especificação e a interpretação dos valores de máscara, a notação decimal foi estendida. Na versão estendida, conhecido como *notação CIDR*, um endereço e uma máscara podem ser especificados dando um endereço decimal pontilhado seguido por uma barra e um número decimal que especificam o número de bits 1 ajustado pela esquerda na máscara. Ou seja, a forma geral é:

ddd.ddd.ddd.ddd / m

onde *ddd* é o valor decimal para um octeto do endereço e *m* é o número de bits 1 na máscara. Assim, a configuração do roteador pode ser inserida como segue:

192.5.48.69 / 26

que especifica uma máscara de 26 bits. A Figura 21.5 lista as máscaras de endereços em notação CIDR, juntamente com a notação decimal pontilhada equivalente de cada uma. Note que alguns dos endereços de máscaras CIDR correspondem às atribuições originais classful.

Comprimento (CIDR)	Máscara de endereço							Observações
/0	0	.	0	.	0	.	0	Todos os 0s (equivalente a nenhuma máscara)
/1	128	.	0	.	0	.	0	
/2	192	.	0	.	0	.	0	
/3	224	.	0	.	0	.	0	
/4	240	.	0	.	0	.	0	
/5	248	.	0	.	0	.	0	
/6	252	.	0	.	0	.	0	
/7	254	.	0	.	0	.	0	
/8	255	.	0	.	0	.	0	Máscara classe A original
/9	255	.	128	.	0	.	0	
/10	255	.	192	.	0	.	0	
/11	255	.	224	.	0	.	0	
/12	255	.	240	.	0	.	0	
/13	255	.	248	.	0	.	0	
/14	255	.	252	.	0	.	0	
/15	255	.	254	.	0	.	0	
/16	255	.	255	.	0	.	0	Máscara classe B original
/17	255	.	255	.	128	.	0	
/18	255	.	255	.	192	.	0	
/19	255	.	255	.	224	.	0	
/20	255	.	255	.	240	.	0	
/21	255	.	255	.	248	.	0	
/22	255	.	255	.	252	.	0	
/23	255	.	255	.	254	.	0	
/24	255	.	255	.	255	.	0	Máscara classe C original
/25	255	.	255	.	255	.	128	
/26	255	.	255	.	255	.	192	
/27	255	.	255	.	255	.	224	
/28	255	.	255	.	255	.	240	
/29	255	.	255	.	255	.	248	
/30	255	.	255	.	255	.	252	
/31	255	.	255	.	255	.	254	
/32	255	.	255	.	255	.	255	Todos os 1s (máscara específica de host)

Figura 21.5 Uma lista de máscaras de endereço em notações CIDR e decimal pontilhada.

21.13 Um exemplo CIDR

Como um exemplo de CIDR, assuma que um ISP tenha o seguinte bloco de endereço para atribuir:

128.211.0.0 / 16

Além disso, suponha que o ISP tenha dois clientes, um deles precisa de 12 endereços IP e outro precisa de nove. O ISP pode atribuir o prefixo CIDR a um cliente:

128.211.0.16 / 28

e pode atribuir a outro cliente:

128.211.0.32 / 28

Embora ambos os clientes tenham o mesmo tamanho de máscara (28 bits), os prefixos diferem. O valor binário atribuído a um cliente é:

10000000 11010011 00000000 0001 0000

e o valor binário atribuído ao outro cliente é:

10000000 11010011 00000000 0010 0000

Assim, não há ambiguidade – cada cliente tem um prefixo único e pode alocar 14 endereços IP. Mais importante, o ISP mantém a maior parte do bloco de endereço original, que ele pode alocar para outros clientes.

21.14 Endereços nos hosts CIDR

Considere calcular o intervalo de endereços em um bloco CIDR IPv4. Uma vez que um ISP atribui a um cliente um prefixo CIDR, o cliente pode atribuir endereços aos hosts. Por exemplo, suponha que seja atribuída a uma organização o prefixo *128.211.0.16 / 28*, como descrito acima. A Figura 21.6 ilustra que a organização terá 4 bits para usar como um campo de endereço de host e mostra os endereços mais altos e os mais baixos nas notações binária e decimal pontilhada. O exemplo evita atribuir endereços host todos em 1 e todos em 0.

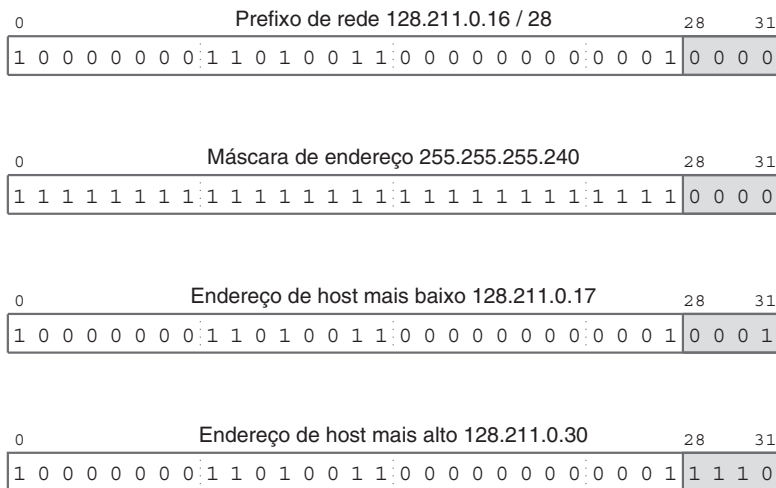


Figura 21.6 Ilustração de endereçamento CIDR IPv4 para um exemplo do prefixo /28.

A Figura 21.6 ilustra uma desvantagem do endereçamento classless – como o sufixo do host pode começar em um limite arbitrário, os valores não são fáceis de ler em notação decimal pontilhada. Por exemplo, quando combinados com o prefixo de rede, os 14 possíveis sufixos do host resultarão em valores decimais pontilhados de *128.211.0.17* até *128.211.0.30*.

21.15 Endereços especiais IPv4

Além de atribuir um endereço para cada computador, é conveniente ter endereços que possam ser atribuídos a redes ou conjuntos de computadores. O IP define um conjunto

de formas de endereços especiais que são *reservados*. Ou seja, endereços especiais nunca são atribuídos a hosts. Esta seção descreve tanto a sintaxe quanto a semântica de cada forma de endereço especial.

21.15.1 Endereços de rede IPv4

Um dos motivos para a definição de formas especiais de endereço pode ser visto na Figura 21.6 – é conveniente ter um endereço que pode ser atribuído ao prefixo de uma determinada *rede*. O IP reserva o endereço de host 0 e usa-o para designar uma rede. Assim, o endereço *128.211.0.16/28* denota uma rede, pois os bits além do 28º são zeros. Um endereço de rede nunca deve aparecer como o endereço de destino em um pacote⁵.

21.15.2 Endereço de broadcast direcionado do IPv4

Às vezes, é conveniente enviar uma cópia de um pacote para todos os hosts em uma rede física. Para simplificar a difusão, o IPv4 define um *endereço de broadcast direcionado* para cada rede física. Quando um pacote é enviado para o endereço de broadcast direcionado de rede, uma única cópia do pacote viaja através da Internet até que atinja a rede especificada. O pacote é então entregue a todos os hosts da rede.

O endereço de broadcast direcionado para uma rede é formado pela adição de um sufixo que consiste em todos os bits 1 para o prefixo de rede. Assim, o sufixo do host que consiste em todos os bits 1 é reservado – se um administrador inadvertidamente atribui o sufixo com todos os bits 1 a um computador específico, o software pode funcionar mal.

Como o broadcast funciona? Se o hardware de rede suporta broadcast, um broadcast direcionado será entregue usando a capacidade de transmissão broadcast do hardware. Se uma rede particular não tem suporte de hardware para broadcast, o software deve enviar uma cópia em separado do pacote a cada host na rede.

21.15.3 Endereços de broadcast limitados do IPv4

O termo *broadcast limitado* se refere a uma transmissão broadcast em uma rede conectada diretamente; informalmente, dizemos que a transmissão é limitada a um “único fio”. A difusão limitada em broadcast é usada durante a inicialização do sistema por um computador que ainda não sabe o número da rede.

O IPv4 reserva o endereço que consiste em 32 bits 1 para se referir ao broadcast limitado. Assim, o software IP irá transmitir em broadcast qualquer pacote enviado para o endereço com todos os bits 1 através da rede local.

21.15.4 Os endereços destes computadores do IPv4

Como cada pacote da Internet contém o endereço do remetente, bem como o do destino, um computador precisa saber seu endereço IPv4 antes de poder enviar ou receber pacotes da Internet. No Capítulo 23, nós aprenderemos que o TCP/IP contém protocolos que um computador pode usar para obter seus endereços IP automaticamente quando é inicializado. Curiosamente, os protocolos de inicialização usam o IP para se comunicar.

⁵ A Seção 21.17 aborda a forma de endereço Berkeley broadcast para o IPv4, que é uma exceção ao padrão.

Quando tais protocolos de inicialização são usados, um computador não pode fornecer um endereço IP do remetente correto. Para lidar com esses casos, o IPv4 reserva o endereço composto por zeros para atribuí-lo a *esse computador*⁶.

21.15.5 O endereço de loopback do IPv4

O IP define um *endereço de loopback* usado para testar aplicações de rede. Os programadores costumam usar o loopback para depuração preliminar após uma aplicação de rede ter sido criada. Para executar um teste de loopback, um programador deve ter dois aplicativos que têm como objetivo comunicarem-se através de uma rede. Cada aplicativo inclui o código necessário para interagir com o software de protocolo TCP/IP. Em vez de executar cada aplicativo em um computador separado, o programador executa ambos em um único computador e os instrui para usar um endereço de loopback para a comunicação. Quando um aplicativo envia dados para outro, os dados trafegam para baixo na pilha de protocolos para o software IP, que encaminha-os de volta através na mesma pilha de protocolos para o segundo aplicativo. Assim, o programador pode testar a lógica do aplicativo de forma rápida, sem a necessidade de dois computadores e sem o envio de pacotes através de uma rede.

O IP reserva o prefixo de rede *127/8* para uso com o loopback. O endereço da máquina usada com *127* é irrelevante – todos os endereços dos computadores são tratados da mesma maneira. Por convenção, os programadores costumam usar número host 1, fazendo com que *127.0.0.1* seja o mais popular dos endereços de loopback.

Durante o teste de loopback, nenhum pacote sai de um computador – o software IP encaminha pacotes de um aplicativo para outro. Consequentemente, o endereço de loopback nunca aparece em um pacote que trafega através de uma rede.

21.16 Resumo dos endereços especiais do IPv4

A Figura 21.7 resume as formas dos endereços especiais IP.

Prefixo	Sufixo	Tipo de endereço	Objetivo
tudo-0	tudo-0	este computador	usado durante a inicialização
rede	tudo-0	rede	identificar uma rede
rede	tudo-1	broadcast direcionado	broadcast em rede específica
tudo-1	tudo-1	broadcast limitado	broadcast em rede local
127 / 8	todos	loopback	testar

Figura 21.7 Resumo das formas de endereço especial IP.

Nós dissemos que endereços especiais são reservados e nunca devem ser atribuídos a computadores host. Além disso, cada endereço especial é restrito para determinado

⁶ O significado especial somente se aplica quando o endereço aparece como um endereço de origem em um pacote; uma entrada com zeros também pode aparecer como a rota padrão em uma tabela de encaminhamento.

uso. Por exemplo, um endereço de broadcast nunca deve aparecer como um endereço de origem, e um endereço com todos os valores *zerados* não deve ser utilizado depois que um host completa o procedimento de inicialização e obtém um endereço IP.

21.17 Forma de endereço Berkeley broadcast para o IPv4

A Universidade da Califórnia, em Berkeley, desenvolveu e distribuiu uma das primeiras implementações de protocolos TCP/IP como parte do BSD UNIX⁷. A implementação BSD continha um recurso fora do padrão que afetou muitas implementações subsequentes. Em vez de usar um sufixo do host com todos os valores 1s para representar um *endereço de broadcast direcionado*, a implementação de Berkeley usa um sufixo do host com todos os valores 0s (ou seja, idênticos ao endereço de rede). A forma de endereço é conhecida informalmente como *Berkeley broadcast*.

Infelizmente, muitos fabricantes de computadores implementaram seu software TCP/IP tendo como base a implementação de Berkeley, e alguns sites ainda usam o Berkeley broadcast. O software comercial TCP/IP muitas vezes inclui um parâmetro de configuração que permite a escolha entre o padrão TCP/IP e a forma de transmissão de Berkeley; muitas implementações são construídas para aceitar ambas as formas de endereço de transmissão: padrão e Berkeley. Assim, se o *broadcast direcionado* é permitido, um gerente de rede deve escolher a forma de endereço a ser usada em cada rede.

21.18 Roteadores e princípios de endereçamento IPv4

Além de atribuir um endereço IP para cada host, o protocolo de Internet especifica que também devem ser atribuídos endereços IP aos roteadores. De fato, cada roteador recebe dois ou mais endereços IP, um para cada rede que ele conecta. Para entender por que, lembre-se dos dois fatos a seguir:

- Um roteador tem conexões com várias redes físicas.
- Cada endereço IPv4 contém um prefixo que especifica uma rede física.

Assim, um único endereço IPv4 não é suficiente para um roteador, pois cada roteador se conecta a várias redes, e cada rede tem um prefixo único. O esquema IPv4 pode ser explicado por um princípio fundamental:

Um endereço IPv4 não identifica um computador específico. Em vez disso, cada endereço IP identifica uma conexão entre um computador e uma rede. Um computador com várias conexões de rede (por exemplo, um roteador) deve ter um endereço IPv4 para cada conexão.

A Figura 21.8 ilustra a ideia com um exemplo que mostra endereços IPv4 atribuídos a dois roteadores que conectam três redes.

⁷ BSD, *Berkeley Software Distribution*.

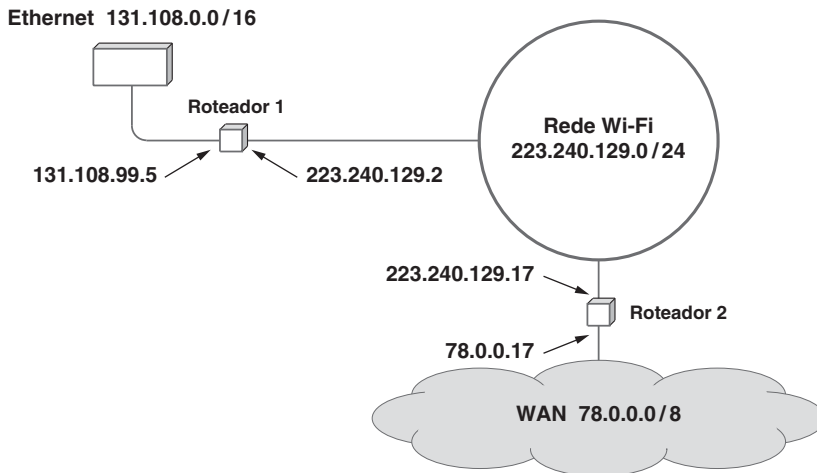


Figura 21.8 Um exemplo de endereços IPv4 atribuídos a dois roteadores.

O IP não exige que o mesmo sufixo seja atribuído a todas as interfaces de um roteador. Na figura, por exemplo, o roteador que conecta a Ethernet e a rede Wi-Fi tem sufixos 99.5 (conexão com a Ethernet) e 2 (conexão com a rede Wi-Fi). No entanto, o IP não impede o uso do mesmo sufixo para todas as conexões. Assim, o exemplo mostra que o administrador decidiu usar o mesmo sufixo, 17, para ambas interfaces do roteador que conecta a rede Wi-Fi à WAN. Na prática, usar o mesmo sufixo pode ajudar os seres humanos que gerenciam as redes porque um único número é mais fácil de memorizar.

21.19 Multihomed hosts

Um host pode conectar-se a várias redes? Sim. Um computador host conectado a várias redes é chamado de *multihomed*. O *multihoming* é por vezes utilizado para melhorar a confiabilidade – se uma rede falha, o host ainda pode estar na Internet através da segunda conexão. Alternativamente, o multihoming é usado para aumentar o desempenho – a conexões com várias redes permite o envio do tráfego diretamente, evitando roteadores que estão, às vezes, congestionados. Como um roteador, um host multihomed tem vários endereços de protocolo, um para cada conexão de rede.

No IPv4, o multihoming sempre foi uma parte complicada do projeto do protocolo, porque aumenta o esforço de gerenciamento de um computador com vários endereços. Questões são levantadas, tais como: se um pacote proveniente de uma rede chega, mas tem o endereço do host de outra rede, ele deveria ser aceito? Uma das razões para tais questionamentos está relacionada com a segurança (*spoofing* pelo envio de um pacote através de uma rota ilegal).

21.20 Multihoming no IPv6 e renumeração

Curiosamente, em vez de proibir o multihoming, o IPv6 eleva-o a uma posição de destaque: um host IPv6 implica várias conexões e vários endereços. Mais importante, o IPv6 permite a uma organização atribuir vários prefixos IPv6 para cada rede.

O motivo para permitir que uma rede tenha vários prefixos é a necessidade de *renumerar* as redes. Se uma organização muda o seu fornecedor de serviços, o prefixo de rede atribuído à organização também pode mudar. Os projetistas do IPv6 queriam tornar tais mudanças fáceis. Portanto, os protocolos foram projetados para que o novo prefixo pudesse ser acrescentado enquanto os aplicativos em execução continuassem a usar o prefixo antigo. Quando um aplicativo fosse executado, ele deveria usar o novo prefixo. Depois de um curto período de tempo, todos os aplicativos deveriam usar o novo prefixo, e o antigo prefixo poderia ser removido. Infelizmente, apesar de anos de trabalho na renumeração de redes no IPv6, a renumeração automática ainda não é prática.

21.21 Endereçamento IPv6

Como o IPv4, o IPv6 atribui um endereço exclusivo para cada conexão entre um computador e uma rede física. Assim, se um roteador se conecta com três redes físicas, a ele são atribuídos pelo menos três endereços IPv6 (lembre-se de que o IPv6 permite que vários prefixos sejam atribuídos a uma determinada rede). Também como o IPv4, o IPv6 separa cada endereço em um prefixo que identifica a rede e um sufixo que identifica um computador particular na rede.

Apesar de adotar a mesma abordagem para atribuir endereços aos computadores, o endereçamento IPv6 difere do IPv4 de maneira significativa. Primeiro, os detalhes do endereço são completamente diferentes. Como nos endereços CIDR, a divisão entre prefixo e sufixo no IPv6 pode ocorrer em um limite arbitrário de bits. Diferentemente do IPv4, no entanto, o IPv6 inclui endereços com três níveis de hierarquia. Um prefixo inicial do endereço é um valor único e global usado para roteamento na Internet. Pensamos no prefixo como algo atribuído a uma única organização. A parte seguinte do endereço identifica uma *sub-rede* (ou seja, uma rede) da organização e a terceira parte corresponde a um computador específico na rede.

Tal como os prefixos IPv4, o prefixo de um endereço IPv6 é de tamanho variável e é escolhido por um ISP, dependendo do tamanho de um assinante. No entanto, a terceira parte de um endereço IPv6 – a parte que identifica um computador específico – é de tamanho fixo. Por convenção, a terceira parte usa 64 bits. Assim, o prefixo global e a sub-rede sempre formam um prefixo /64. Ou seja, se um ISP atribui a uma organização um prefixo global de K bits, a porção da sub-rede dos endereços IPv6 na organização deve ter $64 - K$ bits de comprimento. A Figura 21.9 ilustra a divisão de um endereço IPv6.

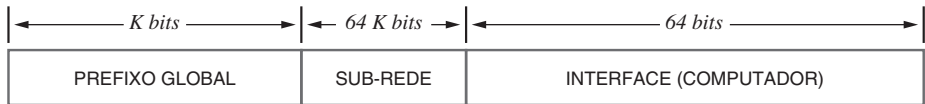


Figura 21.9 A divisão de um endereço IPv6 de 128 bits em seções prefixo, sub-rede e interface. A interface é de 64 bits de comprimento.

Como o IPv4, o IPv6 define um conjunto de endereços especiais. No entanto, as duas versões diferem completamente no tipo de endereços especiais utilizados. Por exemplo, o IPv6 fornece endereços com *alcance* limitado (por exemplo, aqueles que só podem ser usados em uma única rede e aqueles que estão limitados a uma organização). Mais importante, o IPv6 não inclui quaisquer endereços especiais para broadcasting. Em vez disso, usa multicast. Cada endereço IPv6 é um dos três tipos básicos listados na Figura 21.10.

Tipo	Objetivo
unicast	O endereço corresponde a um único computador. Um datagrama enviado para o endereço é roteado pelo caminho mais curto até o computador
multicast	O endereço corresponde a um grupo de computadores, e a filiação ao grupo pode mudar a qualquer momento. IPv6 entrega uma cópia do datagrama para cada membro do grupo
anycast	O endereço corresponde a um grupo de computadores que compartilham um prefixo em comum. Um datagrama enviado para o endereço é entregue para exatamente um dos computadores (p.ex., o computador mais próximo do remetente)

Figura 21.10 Os três tipos de endereços IPv6.

Como mostra a figura, o IPv6 mantém os endereçamentos unicast e multicast. Para lidar com o broadcast limitado (transmitido na rede local), ele define um grupo multicast especial que corresponde a todos os hosts e roteadores da rede local.

O endereçamento *anycast* era originalmente conhecido como endereçamento *cluster*. Ele surgiu do desejo de permitir a replicação de serviços. Por exemplo, uma organização que oferece um serviço através da rede atribui um endereço de anycast para vários computadores que oferecem o serviço. Quando um usuário envia um datagrama para o endereço de anycast, o IPv6 roteia o datagrama para um dos computadores do conjunto (ou seja, do *cluster*). Se um usuário de outro local envia um datagrama para o endereço de anycast, o IPv6 pode optar por encaminhar o datagrama para um membro diferente do conjunto, permitindo que os computadores do grupo processem o pedido ao mesmo tempo.

21.22 Notação hexadecimal com separação através de “:” IPv6

Como um endereço IPv6 ocupa 128 bits, escrever tais números pode ser complicado. Por exemplo, considere um número de 128 bits escrito na forma decimal, que o IPv4 usa:

105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

Para reduzir o número de caracteres usados para escrever um endereço, os projetistas do IPv6 escolheram uma forma sintática mais compacta conhecida como *notação hexadecimal com separação através de “:”*, no inglês geralmente abreviada como *colon hex*. Nessa notação, cada grupo de 16 bits é escrito em hexadecimal com dois pontos separando os grupos. Por exemplo, quando o número apresentado anteriormente é escrito em colon hex, torna-se:

69DC:8864:FFFF:FFFF:0:1280:8C0A:FFFF

Como o exemplo ilustra, a notação colon hex requer menos caracteres para expressar um endereço. Uma otimização adicional conhecida como *zero compression* reduz ainda mais o tamanho. Ela substitui sequências de zeros com dois pontos. Por exemplo, o endereço:

FF0C:0:0:0:0:0:B1

pode ser escrito:

FF0C::B1

O grande espaço ocupado pelo endereço do IPv6 e o esquema proposto de atribuição de endereços tornam a *zero compression* especialmente importante, porque os projetistas esperam ter muitos endereços IPv6 com sequências de zeros. Em particular, para ajudar na transição para o novo protocolo, os projetistas mapearam os endereços IPv4 existentes no espaço do endereço IPv6. Qualquer endereço IPv6 que começa com 80 bits 0 seguidos de 16 bits 1, contém um endereço IPv4 de 32 bits de baixa ordem.

Diferentemente do IPv4, o IPv6 não reserva endereços especiais de broadcast. Em vez disso, usa um conjunto de endereços multicast para lidar com casos especiais. Por exemplo, no lugar do endereço de broadcast com todos bits 1 limitado do IPv4, o IPv6 define um endereço de multicast que corresponde a *todos os nós da rede local*. O IPv6 também define endereços multicast que vão além de casos especiais do IPv4. Por exemplo, ele define um endereço de multicast para *todos os roteadores da rede local*.

21.23 Resumo

Para ter a aparência de uma grande rede, integrada como um todo, a Internet usa um esquema uniforme de endereçamento. A cada computador é atribuído um endereço IP único; todos os aplicativos da Internet usam esse endereço ao se comunicar com ele.

O protocolo de Internet especifica o endereçamento. O IPv4 divide cada endereço IP em uma hierarquia de dois níveis: um prefixo que identifica a rede à qual o computador está conectado e um sufixo que identifica um computador específico na rede; o IPv6 usa uma hierarquia de três níveis: prefixo, sub-rede e computador. Para garantir que os endereços permaneçam únicos para uma determinada internet, uma autoridade central atribui os prefixos de rede. No IPv4, uma vez que um prefixo tenha sido atribuído, um administrador da rede local atribui a cada host na rede um sufixo único. Nós veremos que, no IPv6, os sufixos host únicos podem ser gerados automaticamente.

Um endereço IPv4 é um número de 32 bits; e um endereço IPv6 é um número de 128 bits. O esquema de endereçamento original do IPv4 dividiu os endereços em classes; a classe multicast do IPv4 ainda é usada. O endereçamento classless e o de sub-rede do IPv4 permitem que a fronteira entre o prefixo e o sufixo ocorra em um limite arbitrário de bits. Para isso, o endereçamento de sub-rede e o classless (CIDR) armazenam uma máscara de 32 bits de tamanho junto com cada endereço. A máscara tem valor 1 para cada bit no prefixo e valor 0 para cada bit no sufixo. O IPv6 mantém a abordagem classless, mas utiliza uma máscara de 128 bits.

O IPv4 especifica um conjunto de endereços reservados que têm significado especial. Os endereços especiais do IPv4 podem ser usados para especificar o loopback (usado para testes), o endereço de uma rede, o broadcast na rede física local e o broadcast em

uma rede remota. O IPv6 define um conjunto de endereços multicast, tal como um endereço para todos os nodos em uma rede e um endereço para todos os hosts em uma rede.

Embora seja conveniente pensar em um endereço IP como um computador, cada endereço IP identifica uma conexão entre um computador e uma rede. Os roteadores e os hosts multihomed, que têm conexões com diversas redes físicas, têm vários endereços IP.

Exercícios

- 21.1 O IP poderia ser reprojetoado para usar endereços de hardware em vez dos endereços IP que são usados atualmente? Por quê?
- 21.2 O que a hierarquia de endereço da Internet permite a um gerente local fazer?
- 21.3 No esquema original de endereço classless do IPv4, era possível determinar a classe do endereço? Explique.
- 21.4 Escreva um aplicativo que aceite um endereço com notação decimal pontilhada (*dotted decimal*) e imprima um string de 32 bits.
- 21.5 Escreva um aplicativo que aceite um endereço colon hex como entrada e imprima um string de 128 bits.
- 21.6 Escreva um aplicativo que leia um endereço IPv4 na forma de notação decimal pontilhada e determine se ele é um endereço de *multicast*.
- 21.7 Escreva um aplicativo que traduza a notação com barra CIDR para a equivalente na notação decimal pontilhada.
- 21.8 Se um ISP atribuir para você um bloco de endereço IPv4 /28, quantos computadores poderão ser atribuídos com endereços do bloco?
- 21.9 Se um ISP atribuir para você um bloco de endereço IPv6 /28, quantos computadores poderão ser atribuídos com endereços do bloco?
- 21.10 Se um ISP oferece um bloco de endereço /17 por N dólares por mês e um bloco de endereço /16 por 1,5 N dólares por mês, qual deles tem o custo mais barato por computador?
- 21.11 O prefixo CIDR 1 . 2 . 3 . 4 / 29 é válido? Por quê?
- 21.12 Suponha que você tenha um ISP com o bloco de endereço IPv4 /24. Explique se você pode acomodar um pedido de um cliente que necessita de endereços para 255 computadores. (Dica: considere os endereços especiais.)
- 21.13 Suponha que você tenha um ISP que possui um bloco de endereço IPv4 /22. Mostre a alocação CIDR que você poderia usar para alocar blocos de endereço para quatro clientes que necessitam de endereços para 60 computadores.
- 21.14 Suponha que você tenha um ISP que possui um bloco de endereço IPv4 /22. É possível acomodar pedidos de seis clientes que necessitam de endereços para 9, 15, 20, 41, 128 e 260 computadores, respectivamente? Se sim, como? Se não, explique por que.
- 21.15 Escreva um aplicativo que leia um endereço IPv4 em notação CIDR e imprima o endereço resultante e a máscara em binário.
- 21.16 Escreva um aplicativo que leia como entrada um prefixo de rede IPv4 em notação CIDR e um pedido por um número de host. Assuma que o pedido foi dado para o ISP que possui o prefixo e atribua um prefixo CIDR que acomode o pedido sem desperdiçar endereços.
- 21.17 Escreva um aplicativo que leia um endereço host IPv4 de 32 bits e uma máscara de host de 32 bits em notação CIDR. Depois, diga se o endereço é um dos endereços especiais.

- 21.18** Escreva um aplicativo que leia um endereço host IPv6 de 128 bits e uma máscara de 128 bits em notação CIDR e informe se o endereço é de multicast. (Dica: o IETF publica normas que especificam as atribuições de endereços IPv6.)
- 21.19** O que é um endereço Berkeley broadcast?
- 21.20** O IPv6 usa endereços de broadcast? Explique.
- 21.21** Quantos endereços IPv4 são atribuídos a um roteador que conecta N redes? Explique.
- 21.22** Quantos endereços IPv6 são atribuídos a um roteador que conecta N redes? Explique.
- 21.23** Um host pode ter mais do que um endereço IPv4? Explique.
- 21.24** Se um host IPv6 está conectado a cinco redes, qual termo é usado para descrevê-lo?
- 21.25** Quando um endereço anycast pode ser útil?

Encerra aqui o trecho do livro disponibilizado para esta Unidade de Aprendizagem. Na Biblioteca Virtual da Instituição, você encontra a obra na íntegra.

